Technology Landscape for Digital Identification

WORLD BANK GROUP

dial Digital Impact Alliance

1818 H Street, NW, Washington, D.C., 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

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

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

Rights and Permission

Attribution—Please cite the work as follows: World Bank. 2018. *Technology Landscape for Digital Identification*, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO)

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

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

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

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

Contents

Figures

About ID4D

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

The mission of ID4D is to enable all people to access services and exercise their rights, by increasing the number of people who have secure, verifiable, and officially recognized identification. ID4D makes this happen through its three pillars of work:

- Thought leadership and analytics to generate evidence and fill knowledge gaps;
- Global platforms and convening to amplify good practices, collaborate and raise awareness; and
- Country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive and responsible digital identification systems that are integrated with civil registration.

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

To find out more about ID4D, visit worldbank.org/id4d.

Acknowledgments

This report was prepared as part of the Identification for Development (ID4D) initiative, the World Bank Group's cross-sectoral effort to support progress toward identification systems using 21st century solutions. It was made possible through the generous support of Digital Impact Alliance (DIAL) and the partners of the ID4D Multi-Donor Trust Fund (Bill & Melinda Gates Foundation and Omidyar Network).

The Accenture team who contributed to this paper as authors or reviewers include: Dan Bachenheimer, Dan Baker, Sebabrata Banerjee, Craig Chatfield, Ilkka Hyvonen, Akshay Iyer, Mrinal Jha, Suneeta Kudaravalli, Christine Leong, Sabareesh Madhav, Rahul Malik, Nilanjan Nath, Juhi Saxena, Luca Schiatti, and Srijan Singh.

This report benefited greatly from the inputs by Anita Mittal and reviews of the World Bank Group staff including Seth Ayres, Luda Bujoreanu, Susan David Carevic, Kamya Chandra, Tina George, Jonathan Marskell, Anna Zita Metz, and David Satola under the supervision of Vyjayanti Desai.

The findings in the report are based on the research, consultations, and detailed assessments of identification and authentication technologies during late 2017. As a result, the information presented here represents a snapshot of technologies at the time the report was written, and may not reflect recent developments.

The report would not have been possible without the insights and reviews by Dr. Joseph Atick, ID4Africa & Identity Counsel; Jérôme Buchler, HSB identification; Dasha Cherepennikova, One World Identity; Sanjay Dharwadker, WCC; Rebecca Distler, Element Inc; Alan Gelb, Centre for Global Development; Marta Ienco, GSMA; Sanjay Jain, iSprit; Brett McDowell, FIDO Alliance; Monica Monforte, GSMA; C. Maxine Most, Acuity Market Intelligence; Wameek Noor, DIAL; Adam Perold, Element Inc; Kris Ranganath, NEC; Yiannis Theodorou, GSMA; Don Thibeau, The Open Identity Exchange; Colin Wallis, Kantara Initiative; Anne Wang, Gemalto; Dr. Jim Wayman, San Jose State University (Director of Biometric Identification Research Program); Matt Wilson, GSMA; and Jeff Wishnie, DIAL.

Key Terms and Definitions

Authentication: The process of proving an identity. Occurs when subjects provide appropriate credentials, often as a prerequisite to receiving access to resources.[1]

Biometrics: A measurable physical characteristic or personal behavioral trait used to recognize an applicant's identity, or verify his or her claimed identity. Facial images, fingerprints, and iris scan samples are all examples of biometrics.[2]

Credential: An object or data structure that authoritatively binds an identity—via an identifier or identifiers—and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.[3]

De-duplication: In the context of identification systems, it is a technique to identify duplicate copies of identity data. Biometric data—including fingerprints and iris scans—are commonly used to de-duplicate identities in order to identify false or inconsistent identity claims and to establish uniqueness.

Digital identification: The process of validating a person's attributes and characteristics, including uniqueness, to establish his or her digital identity.[4]

Digital identity: The terminology used throughout this document to refer to a set of electronically captured and stored attributes and credentials that can uniquely identify a person.[5]

Foundational identification system: Identification system created for general public administration and identification—including civil registries, national IDs, and national population registers. May serve as the basis for a wide variety of public and private transactions, services, and derivative identity credentials. Common examples include digital IDs or civil registers.

Functional identification system: Identification system created in response to a demand for a particular service or transaction. May issue identity credentials such as voter IDs, health and insurance records, and bank cards. These may be commonly accepted for broader identification purposes, but may not always bestow legal identity.

Identification: The determination of identity and recognition of who a person is; the action or process of determining what a thing is; or the recognition of a thing as being what it is.

Identity: A unique set of features and characteristics that individualize a person, including biographical and biometric attributes.

[1] Darril (December 2011). *Identification, Authentication, and Authorization*. Get Certified Get Ahead Retrieved from: http://blogs.getcertifiedgetahead.com/identification-authentication-authorization/

[2] Richard Kissel (May 2013). *Glossary of Key Information Security Terms*. NIST Retrieved from: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[3] Grassi, P.A, Fenton, J.L., et al. (June 2017). *Digital Identity Guidelines*. NIST Retrieved from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[4] World Bank (2016). *Digital Identity: Towards shared principles for public and private sector cooperation (English)*. World Bank Group. Retrieved from: https://openknowledge.worldbank.org/bitstream/handle/10986/24920/Digital0identi0e0sector0cooperation.pdf?sequence=1&isAllowed=y

[5] World Bank (2016). *Digital Identity: Towards shared principles for public and private sector cooperation (English)*. World Bank Group. Retrieved from: https://openknowledge.worldbank.org/bitstream/handle/10986/24920/Digital0identi0e0sector0cooperation.pdf?sequence=1&isAllowed=y

Protocol: Set of rules and formats, semantic (meaning), and syntactic (format), that enable information systems to exchange information.[6]

Revocation: The process of prematurely ending the operational period of a certificate or credential effective at a specific date and time.[7]

User: Individual or (system) process authorized to access an information system.[8]

Verification: Confirmation and establishing of a link between a claimed identity and the actual, living person presenting the evidence.[9]

[6] Richard Kissel (May 2013). *Glossary of Key Information Security Terms.* NIST Retrieved from: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[7] Richard Kissel (May 2013). *Glossary of Key Information Security Terms.* NIST Retrieved from: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[8] Richard Kissel (May 2013). *Glossary of Key Information Security Terms.* NIST Retrieved from: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[9] Grassi, P.A, Fenton, J.L., et al. (June 2017). *Digital Identity Guidelines.* NIST Retrieved from: https://pages.nist.gov/800-63-3/sp800-63a.html

Abbreviations

AAL	Authenticator Assurance Level
AI	Artificial Intelligence
API	Application Programming Interface
BN	Billion
BSoC	Biometric System on Card
CNIC	Computerized National Identity Card
CRL	Certificate Revocation List
CSP	Credential Service Provider
DLT	Distributed Ledger Technology
DNA	Deoxyribonucleic Acid
DNI	Documento Nacional de Identidad
ECG	Electrocardiography
eID	Electronic Identification
eIDAS	Electronic Identification, Authentication and Trust Services
EMS	Enterprise Mobility + Security
EMV	Europay, MasterCard, and Visa
EU	European Union
FAR	False Acceptance Rate
FIDO	Fast Identity Online
FRR	False Rejection Rate
FTE	Failure to Enroll
GSM	Global System for Mobile
GSMA	Groupe Spéciale Mobile Association
HTTP	Hyper Text Transfer Protocol
IAL	Identity Assurance Level
ICAO	International Civil Aviation Organization
ID	Identification
ID4D	Identification for Development
IETF	Internet Engineering Task Force
IMDB	In-Memory Database
IoT	Internet of Things
ISO	International Organization for Standardization
KYC	Know Your Customer
LDA	Linear Discriminant Analysis
MN	Million
MRTD	Machine Readable Travel Document
MRZ	Machine-Readable Zone
N/A	Not Applicable
NADRA	National Database and Registration Authority
NFC	Near-Field Communication
NIR	Near Infrared
NIST	National Institute of Standards and Technology

OAuth	Open Authorization
OCR	Optical Character Recognition
OTP	One-Time Password
PCA	Principal Component Analysis
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
QR	Quick Response
RAM	Random-Access Memory
RF	Radio Frequency
RFC	Remote Function Call
RFID	Radio Frequency Identification
RSA	Rivest-Shamir-Adleman
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SDK	Software Development Kit
SIM	Subscriber Identification Module
SMS	Short Message Service
TPM	Trusted Platform Module
UAF	Universal Authentication Framework
UHF	Ultra-High Frequency
UI	User Interface
USB	Universal Serial Bus
USD	US Dollars

1. Introduction

Robust, inclusive, and responsible identification systems can increase access to finance, healthcare, education, and other critical services and benefits. Identification systems are also key to improving efficiency and enabling innovation for public- and private-sector services, such as greater efficiency in the delivery of social safety nets and facilitating the development of digital economies. However, the World Bank estimates that more than 1.1 billion individuals do not have official proof of their identity.[10] New technologies provide countries with the opportunity to leapfrog paper-based systems and rapidly establish a robust identification infrastructure. As a result, the countries are increasingly adopting nationwide digital identification (ID) programs and leveraging them in other sectors.[11]

Whether a country is enhancing existing ID systems or implementing new systems from the ground up, technology choices are critical to the success of digital identification systems. A number of new technologies are emerging to enable various aspects of ID lifecycle. For some of these technologies, no large-scale studies have been done; for others, current speculation makes objective evaluations difficult.

This report is a first attempt to develop a comprehensive overview of the current technology landscape for digital identification. It is intended to serve as a framework for understanding the myriad options and considerations of technology in this rapidly advancing agenda and in no way is intended to provide advice on specific technologies, particularly given there are a number of other considerations and country contexts which need to be considered. This report also does not advocate the use of a certain technology from a particular vendor for any particular application.

While some technologies are relatively easy to use and affordable, others are costly or so complex that using them on a large scale presents daunting challenges. This report provides practitioners with an overview of various technologies and advancements that are especially relevant for digital identification systems. It highlights key benefits and challenges associated with each technology. It also provides a framework for assessing each technology on multiple criteria, including length of time it has been in use, its ease of integration with legacy and future systems, and its interoperability with other technologies.

The practitioners and stakeholders who read this are reminded to bear in mind that the technologies associated with ID systems are rapidly evolving, and that this report, prepared in early 2018, is a snapshot in time. Therefore, technology limitations and challenges highlighted in this report today may not be applicable in the years to come.

The report comprises the following sections:

- **Section 1: Introduction.** The Introduction sets the context and outlines the technology challenges that practitioners and stakeholders may have to address while evaluating or implementing digital ID systems. The list of challenges is not exhaustive but addresses insights gained from the implementation of digital ID systems in different countries around the world. The list of challenges

[10] World Bank (2017). *Identification for Development*. Retrieved from World Bank: http://www.worldbank.org/en/programs/id4d

[11] World Bank (2015). *Identification for Development (ID4D) Integration Approach*. Retrieved from World Bank: http://pubdocs.worldbank.org/en/205641443451046211/ID4D-IntegrationAproachStudyComplete.pdf

has also been framed in the context of developing countries that often have rapidly growing populations and limited budgets for identification systems.

- **Section 2: Understanding the Identity Lifecycle.** This section groups the identity process into its main steps and briefly explains the sub-processes in each step. It also provides the framing for a discussion of how the different technologies can enable different stages of the identification lifecycle.
- **Section 3: Introducing the Technology Assessment Framework.** This section details the parameters used to evaluate the technologies, including maturity, performance, scalability, adoption, security, and affordability. Each parameter has multiple sub-parameters, and these are rated on a 3-point scale of high, medium, or low. The section also lists the technologies evaluated using this framework and the identity lifecycle steps they can enable or affect.
- **Sections 4 through 6**: These provide an overview of each technology examined through the assessment framework and highlight challenges that the technology could solve, challenges it does not solve, and any new challenges that its adoption could present. Through these analyses, practitioners can better understand the key considerations involved in choosing digital ID technologies.
- **Section 7: Other Considerations.** This concluding section describes some important considerations that practitioners should keep in mind while making technology choices.

The main focus of the report is to assess technologies related to the digital ID lifecycle. However, this in no way infers that technology is the only or the most critical consideration for practitioners seeking to maximize the benefits of identification systems while mitigating the risks. The "Principles on Identification for Sustainable Development: Toward the Digital Age" highlight a range of critical considerations.[12] These Principles have been endorsed by more than 20 organizations and are briefly listed below for the benefit of readers.

Principles

Inclusion

1. Ensuring universal coverage for individuals from birth to death, free from discrimination
2. Removing barriers to access and usage and disparities in the availability of information and technology

Design

3. Establishing a robust—unique, secure, and accurate—identity
4. Creating a platform that is interoperable and responsive to the needs of various users
5. Using open standards and ensuring vendor and technology neutrality
6. Protecting user privacy and control through system design
7. Planning for financial and operational sustainability without compromising accessibility

Governance

8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework

[12] The World Bank (February 2017). *Principles on Identification for Sustainable Development: Toward the Digital Age.* The World Bank. Retrieved from: http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples.pdf

9. Establishing clear institutional mandates and accountability
10. Enforcing legal and trust frameworks though independent oversight and adjudication of grievances

A detailed discussion of these principles is in The World Bank report titled Principles on Identification for Sustainable Development: Toward the Digital Age.

Although this report is focused on technologies, the World Bank's Identification for Development initiative is working across the issues listed in the Principles. For example, given the importance of open and interoperable standards for secure and efficient digital identify platform for effective services delivery, further work on standards is in progress. A report titled *Technical Standards for Digital Identity*, prepared in 2017, is available on ID4D website here.[13]

Additionally, the emergence of new digital technologies and the increase in a number of state and non-state actors who are using those technologies for the collection, storage, and processing of data of and about individuals, raises a number of data protection, privacy, and consent issues that need to be considered as part of the design and implementation of digital ID systems. The Principles, above, include protecting user privacy (in design) and safeguarding data privacy, security, and user rights (in the governance of a system).

Privacy and data protection regimes establish predictable rights and obligations regarding the treatment of individual data and personally identifiable information (PII) that are an important part of establishing trust in digital systems—trust that then encourages use.[14] Given the importance of this agenda, and to assist countries identify gaps in legal and regulatory framework for privacy, data protection, and inclusion, the ID4D initiative is developing the ID Enabling Environment Assessment (IDEEA) tool to be rolled out in several countries in 2018.

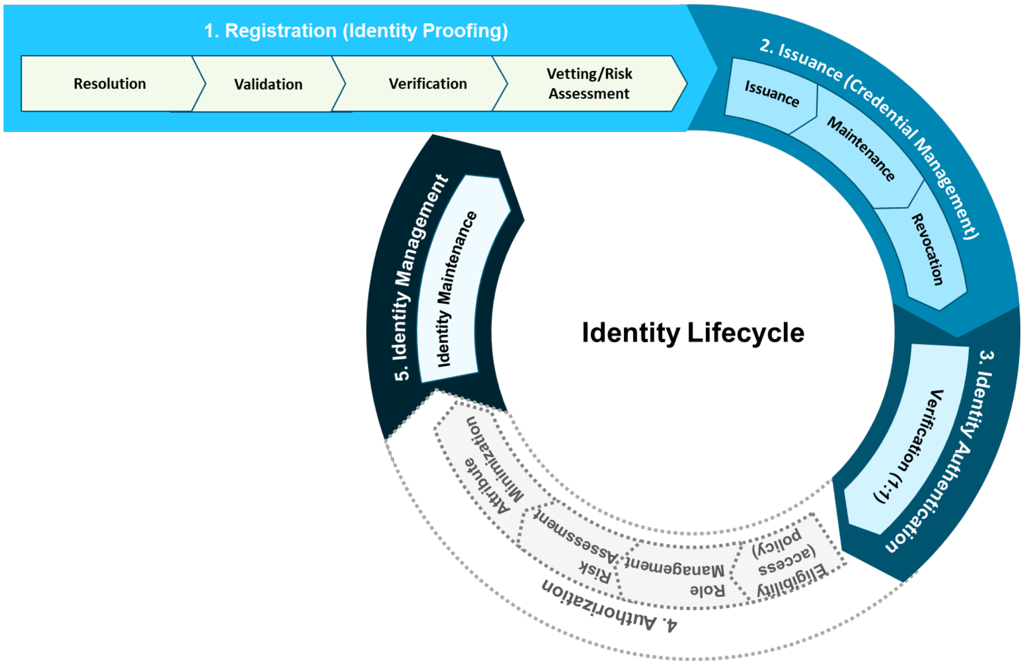
[13] National Institute of Standards and Technology, U.S. Department of Commerce (June 2017). *Digital Identity Guidelines: Enrollment and Identity Proofing*. Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

[14] See Digital Dividends, The World Development Report 2016, at page 222 et seq., The World Bank; available at: http://www.worldbank.org/en/publication/wdr2016

2. Understanding the Identity Lifecycle

The identity lifecycle, as the name implies, is not a onetime event; rather, it's a process—one that starts when a person applies for a digital ID and ends when the record is removed, and the ID is invalidated owing to death, request for removal by the individual, or some other event.[15] Figure 1 depicts the events and activities that take place at each step in the lifecycle. Authorization is implemented and enforced by relying parties and is included in Figure 1 only for the sake of completeness. The technologies pertaining to authorization are not within the scope of this report, and are therefore not discussed in the subsequent sections.

Figure 1: Identity Lifecycle



2.1. Registration (Identity Proofing)[16]

The foundational aspect of one's identity is established during the registration process, when an applicant provides evidence of his or her identity to the credential-issuing authority. (See "Key Terms and Definitions" for the definition of *credential*.) If the person reliably identifies himself or herself, the authority can assert that identity with a certain level of identity assurance. In developing countries, and in cases like those of displaced persons or refugees, it is not uncommon for applicants to lack fundamental documents (birth

[15] The terminologies used in this framework align with NIST standards and existing ID4D literature published by the World Bank.

[16] National Institute of Standards and Technology, U.S. Department of Commerce (June 2017). *Digital Identity Guidelines: Enrollment and Identity Proofing*. Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

certificate, passport, utility bill, driving license). And in some situations, even if some form of an identity document (typically, a breeder document, such as a birth certificate)[17] is available, it may not be trustworthy. In such situations, identification systems may use an introducer[18] who is tasked with verifying the applicant's identity and address. Once verification is completed, biometric registration and de-duplication will bind the applicant to his or her identity claim, which will then be used during subsequent identity interactions.

Ideally, a digital identification system should be integrated with civil registration, which is the official recording of births, deaths, and other vital events including marriages, deaths, divorces, annulments, separations, adoptions, legitimations, and recognition.[19] What this means in practice is that a person's record in the digital ID system and his or her unique ID number are first generated through registration of their birth. Digital ID system is notified of a person's death as soon as possible after death registration. Aside from promoting coverage and sustainability of a digital identification system, this integration provides an opportunity to produce real-time vital statistics, such as on population, fertility, and mortality.

Registration may start with ***Resolution***,[20] the process of uniquely distinguishing an individual in a given population or context. The first step in resolution is pre-enrollment. Here, the applicant provides the issuing authority with biographic information, breeder documents (such as birth certificates, marriage certificates, and social security documents), and photographs. The applicant can present these in person or provide the information online or offline. This is followed by enrollment, which typically happens in person, so pre-enrollment information can be validated and augmented by the registration authority as needed.

In-person proofing is required for the highest identity assurance level (IAL3).[21] When the demographic and biometric information is validated and enrolled, identity proofing typically continues with de-duplication to ensure that the individual did not register under a different claim of identity. This can be accomplished with an identification (1: N) search of the entire biometric database using one or more biometric identifier (physiological and/or behavioral characteristics that are used to identify an individual).[22] This process can be especially challenging with large populations.

The next step is ***Validation***, where the authority determines the authenticity, validity, and accuracy of the identity information the applicant has provided, and relates it to a living person. This is followed by ***Verification***, the establishing of a link between a claimed identity and the real-life subject presenting the evidence. The final step is ***Vetting/Risk Assessment***, assessing the user's profile against a watch list or a risk-based model. Per National Institute of Standards and Technology (NIST) Special Publication 800-63A, identity proofing enables the authority to:

- Resolve a claimed identity to a single, unique identity within the context of the population of users the Credential Service Provider (CSP) serves.
- Validate that all supplied evidence is correct and genuine (that is, not counterfeit or misappropriated).

[17] "Breeder documents are documents used for access to other forms of legitimate identification, such as a driver's license, for the purpose of establishing a false identity." *Breeder Document Law and Legal Definition*. Retrieved from: https://definitions.uslegal.com/b/breeder-document/

[18] Aadhaarcard.net.in (07 November 2016). *Apply for Aadhaar Card without any Documents*. Retrieved from: https://uidai.gov.in/component/fsf/?view-faq&catid=36

[19] United Nations Department of Social and Economic Affairs (2014). *Principles and Recommendations for a Vital Statistics System, Revision 3.* Retrieved from: https://unstats.un.org/unsd/demographic/standmeth/principles/M19Rev3en.pdf

[20] National Institute of Standards and Technology, U.S. Department of Commerce (June 2017). *Digital Identity Guidelines: Enrollment and Identity Proofing*. Retrieved from NIST: https://pages.nist.gov/800-63-3/sp800-63a.html

[21] National Institute of Standards and Technology, U.S. Department of Commerce (June 2017). *Digital Identity Guidelines*. Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[22] Jain, Hong and Pankanti (2000). *Biometric Identification.* Communications of the ACM, 43(2), p. 91–98. Retrieved from ACM: https://dl.acm.org/citation.cfm?doid=328236.328110

- Validate that the claimed identity exists in the real world.
- Verify that the claimed identity is associated with the real person supplying the identity evidence.

For developing countries, multiple challenges may arise during the registration process:

- The hardware and software used for registration activities needs to be accurate, affordable and usable.
- The system must be inclusive, and must include members of marginalized groups such as the poor, the elderly, women, and infants. Some individuals may have poor biometric features (like poor fingerprint ridge structure) that make accurate enrollment difficult.
- The scope of the process must be clearly defined, including the population whose data will be collected, the attributes that will be collected, and the corresponding performance of the registration system. For instance, will registration be for residents of that country only, or for visitors as well? Will the information required for registration include name, birth details, or fingerprints? What are the accuracy and confidence levels of the registration process? Clearly defining the scope of the population whose data will be collected and the attributes that will be collected will mitigate any future issues related to privacy and consent.

2.2. Issuance (Credential Management)[23]

Credential Management starts with ***Issuance***, which is the process of creating and distributing virtual or physical credentials like decentralized identity proofs, e-passports, digital ID cards, and driver's licenses; and a unique identifier (with central biometric authentication), such as the Aadhaar system in India. The other steps are ***Maintenance*** (the retrieval, update, and deletion of credentials) and ***Revocation*** (the removal of the privileges assigned to credentials).

Interoperability of these credentials for authentication is becoming increasingly important for intra-country and inter-country service delivery, as can be seen in the European Union (EU), East African Community (EAC), and West Africa regions. In the EU, for example, electronic identification (eID) and electronic Trust Services (eTS) provide the interoperability framework for secure cross-border electronic transactions of the Digital Single Market under the electronic IDentification, Authentication and Trust Services (eIDAS)[24] regulation.

2.3. Identity Authentication[25]

Authentication is the process of verifying an identity claim against the registered identity information. Such information could be a personal identification number (PIN), a password, biometric data such as a fingerprint, a photo—or a combination of these. Challenges in this phase include how to reduce processing time, improve accuracy of matching for authentication, ensure a seamless experience for applicants, mitigate challenges with network connectivity, counter fraudulent behavior, and find affordable hardware and software solutions.

[23] Entrust Datacard Corporation. *Credential Lifecycle Management*. Retrieved from: https://www.entrustdatacard.com/solutions/credential-lifecycle-management

[24] European Commission (25 February 2015). *Trust Services and eID*. Retrieved from European Commission: https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification

[25] National Institute of Standards and Technology, U.S. Department of Commerce (May 2013). *Glossary of Key Information Security Terms*. Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

2.4. Authorization

Authorization typically takes place after an individual's claim of identity is authenticated and defines access rights (or grants) that a Relying Party has associated with the identity aligned to the relationship between the individual and the Relying Party (e.g., a financial institution)—independent of the Identity Provider (e.g., the National Identification Authority). In more advanced authorization schemes the grants are contextual and dynamic. Because this report is focused on Identity Providers and the provisioning of identities, not Relying Parties and the authorizations that they may associate with an identity, it will not explore the various authorization processes and technologies emerging in the market today.

2.5. Identity Management (Identity Maintenance)

Identity management or maintenance is the ongoing process of retrieving, updating, and deleting identity attributes or data fields and policies governing users' access to information and services. Identity retrieval involves fetching a user's identity attributes. Security policies should be used to enforce access privileges to ensure that only authorized individuals can access, alter, or delete identity information, and to ensure that the actions are audited and cannot be repudiated. This approach ensures that resources are made available only to authorized users according to rules of access that are defined by attributes and policies.[26] Credentials may be deactivated, revoked, or made dormant as a result of certain events, and identity information may be updated or deleted. Identity Management challenges include how to make system maintenance cost-effective, use data analysis to improve the system's performance (including its efficiency), ensure that databases are updated to reflect major life events (such as birth and death), and maintain privacy and security controls.

2.6. Example of a User's Journey through the Identity Lifecycle

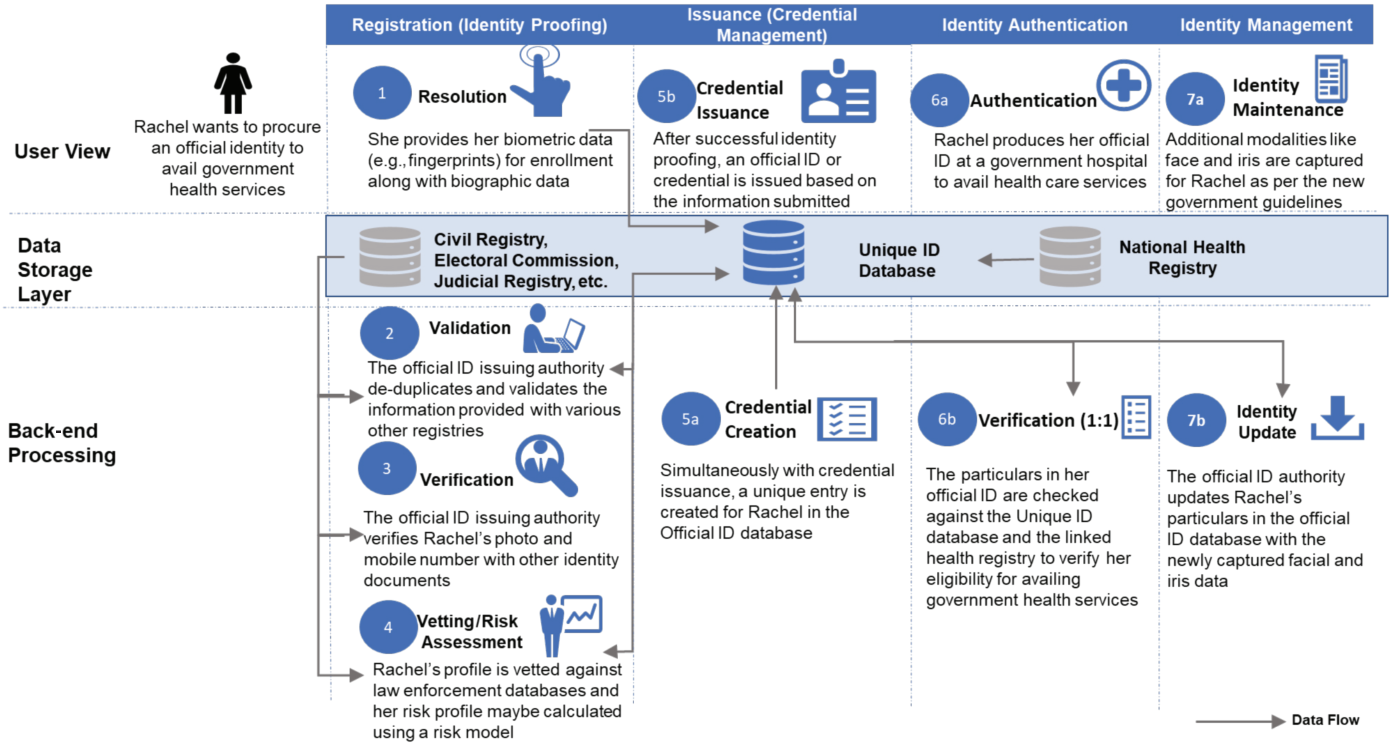
What is it like for digital ID system users to travel through the Identity Lifecycle? Take the example of Rachel. She wants to enroll in the system so that she can be assured access to government-provided health services. As she advances through the different stages in the lifecycle (see Figure 2), a whirlwind of activity takes place behind the scenes.[27] Employees working in various parts of the system draw on data, technologies, and back end processes to ensure that Rachel is who she says she is, and that she does indeed get the credentials or identification document she'll need to gain access to the services she requires.[28]

[26] National Institute of Standards and Technology, U.S. Department of Commerce (March 2010). *A report on the Privilege (Access) Management Workshop.* Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7657.pdf

[27] The user journey shown in Figure 2 aligns with the journey described in the USAID report *Identity in the Digital Age.*

[28] Figure 2 does not include Authorization as a step. That's because authorization is not the responsibility of the foundational identification system. Rather, it's the responsibility of the various functional identification systems to authorize applicants to the system. Steps during authorization include eligibility (access policy), role management, risk assessment, and attribute minimization.

Figure 2: Rachel’s Journey through the Identity Lifecycle



Rachel wants to procure an official identity to avail government health services

1 Resolution: She provides her biometric data (e.g., fingerprints) for enrollment along with biographic data

5b Credential Issuance: After successful identity proofing, an official ID or credential is issued based on the information submitted

6a Authentication: Rachel produces her official ID at a government hospital to avail health care services

7a Identity Maintenance: Additional modalities like face and iris are captured for Rachel as per the new government guidelines

2 Validation: The official ID issuing authority de-duplicates and validates the information provided with various other registries

3 Verification: The official ID issuing authority verifies Rachel’s photo and mobile number with other identity documents

4 Vetting/Risk Assessment: Rachel’s profile is vetted against law enforcement databases and her risk profile maybe calculated using a risk model

5a Credential Creation: Simultaneously with credential issuance, a unique entry is created for Rachel in the Official ID database

6b Verification (1:1): The particulars in her official ID are checked against the Unique ID database and the linked health registry to verify her eligibility for availing government health services

7b Identity Update: The official ID authority updates Rachel’s particulars in the official ID database with the newly captured facial and iris data

3. Introducing the Technology Assessment Framework

3.1. Six Assessment Parameters

Understanding the Identity Lifecycle helps implementers grasp the various processes and technologies involved in provisioning the credentials that enable identification and authentication. Some technologies—like fingerprint recognition—are fairly mature and have seen wide adoption already. Others are emerging, and include contactless fingerprint recognition, rapid deoxyribonucleic acid (DNA) profiling, and blockchain. Such newer technologies are still in the pilot testing stage. With multiple technologies available, an assessment framework can help implementers compare them, gaining a sense of how the technologies work, what their advantages and disadvantages are, and how they might be most useful for managing each stage in the Identity Lifecycle. The assessment parameters are presented below:

Maturity: How long has the technology been in use? How well is it understood?

- *Longevity:* How long has the technology been available and in use (regardless of adoption)
- *Interoperability:* Is the technology based on Standards (preferably open)? How interoperable is the technology with the other technologies in the identity ecosystem?

Performance: How well suited is the technology for performing the required task?

- *Throughput:* How many identity service requests can the technology process per unit of time?
- *Response time:* How quickly can the system respond to an individual request?
- *Accuracy:* How frequently does the technology generate false matches or false rejections during matching or how often does the technology fail to enroll a specific percentage of the population?
- *Stability:* To what degree will the technology be resistant to change in the face of external forces such as age, environmental conditions, pace of development, and others?

Scalability: Can use of the technology be scaled as needed?

- *Data scalability:* How well can the technology adapt to an increase or decrease in the volumes of data being processed or the number of people in the system?
- *Simplicity of computational resources:* How easily can system architects procure and install the necessary hardware and software?
- *Simplicity of network infrastructure:* How easily can system architects establish data transfer channels especially in bandwidth constrained domains?

Adoption: To what degree do system operators and users accept the technology?

- *Integration:* Can we integrate the technology with legacy and future systems?
- *Ease of learning:* How easily can system operators learn to use the technology?
- *User interface (UI) simplicity:* How complex are the technology's software and hardware interfaces?

- *Simplicity of training:* How easy is it to train someone to use the technology?
- *Cultural acceptance:* What are users' feelings and thoughts about the technology?

Security: How secure is the technology against unauthorized access and usage?

- *Circumvention resistance:* How well protected is the technology from hackers and other attacks?
- *Resilience:* How quickly and effectively can the technology recover from an attack or breach?
- *Transmission security:* How secure is the information-exchange channel?

Affordability: How economical is the technology?

- *Hardware affordability:* How cost-effective is the dedicated hardware?
- *Software affordability:* How cost-effective is the dedicated software?
- *Revenue opportunities:* To what degree could we recoup our investment in the technology through interoperability arrangements such as fees from private-sector service providers for conducting e-KYC (Know Your Customer) using the government unique ID database?
- *Time cost savings:* How cost-effective is the technology based on time required to be fully functional?

3.2. A Three-Point Scale

The Technology Assessment Framework uses a three-point scale of "high," "medium," and "low" to represent responses to each of the above questions. "High" is the maximum score or best outcome for a particular parameter, while "low" is the worst outcome or lowest score for a parameter.

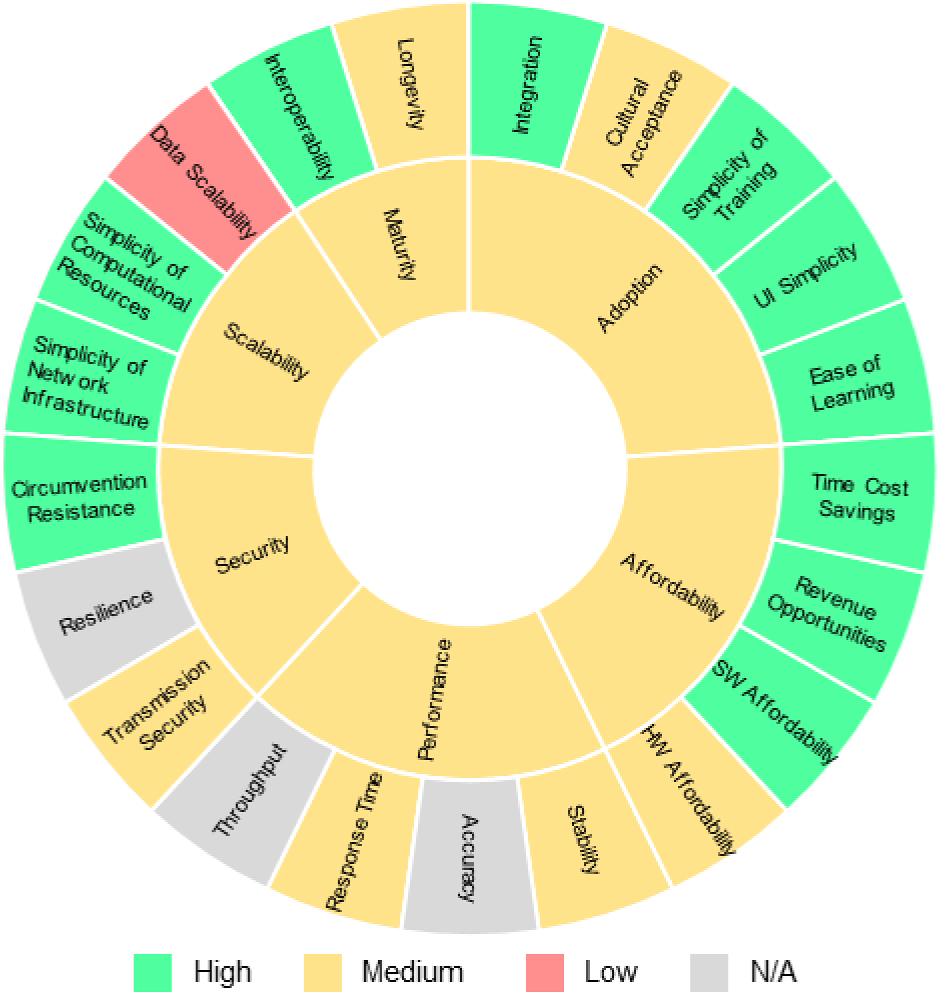
Some of the technologies evaluated through this framework are very new, so information available on them is sparse. In such cases, informed predictions were made for both the score and direction of growth for this technology, drawing on analysis of the technology, trends in identification and authentication, and insights from subject matter experts.

Before delving into ratings for the various technology evaluations, readers may find it helpful to view an example of what the Technology Assessment Framework's output looks like. (See Figure 3.)

The following process was used to decide the ratings for the inner elements of the circle:

1. If all sub-parameters or outer elements are rated High, then the respective inner element is rated High.
2. Conversely, if all sub-parameters are rated Low, then the inner element is rated Low.
3. For all other combinations, the rating for the inner element is Medium.
4. If a certain sub-parameter is not applicable (N/A) for rating, it is excluded from the rating process.

Figure 3: Example Output from the Technology Assessment Framework



Maturity

Performance

Scalability

Adoption

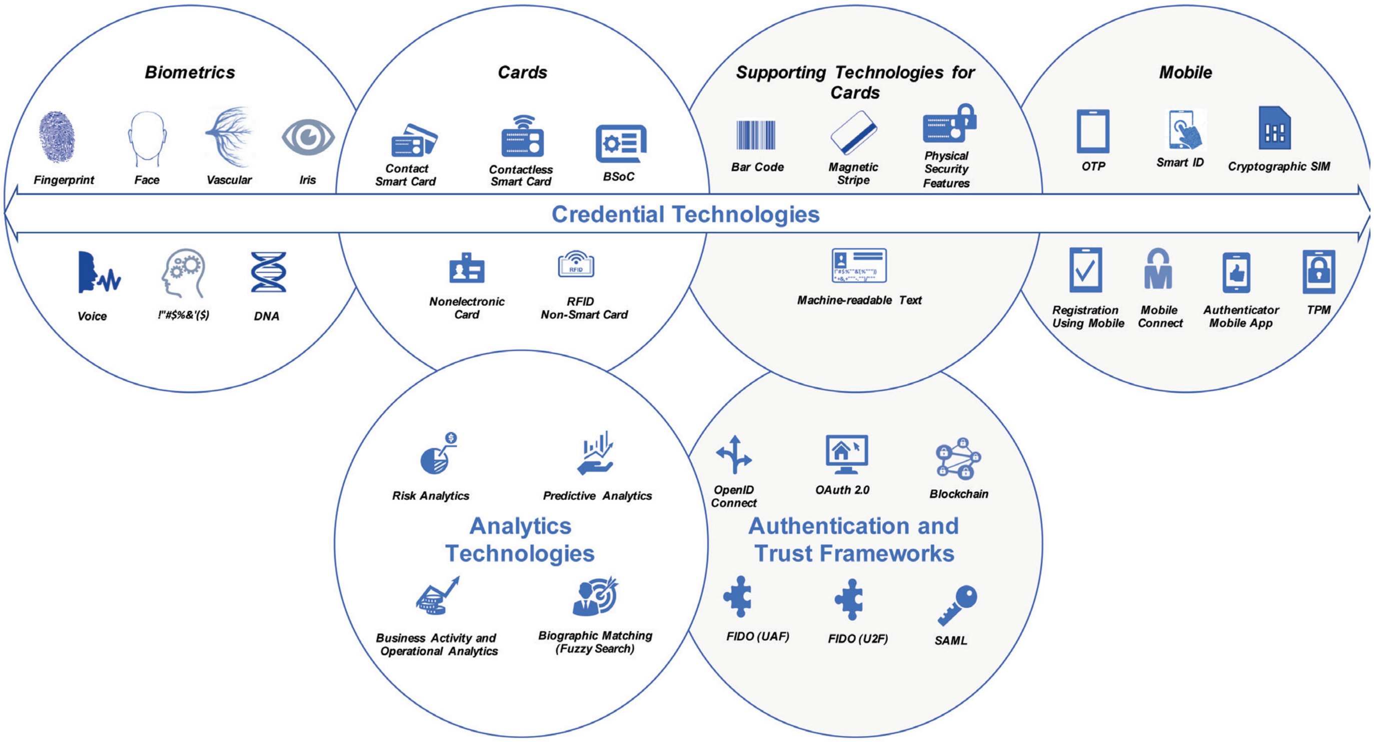
Security

Affordability

3.3. Assessing Technologies Used in Identification and Authentication

Figure 4 below presents technologies covered in the assessment. The report groups the technologies into six broad categories.

Figure 4: Identification and Authentication Technologies

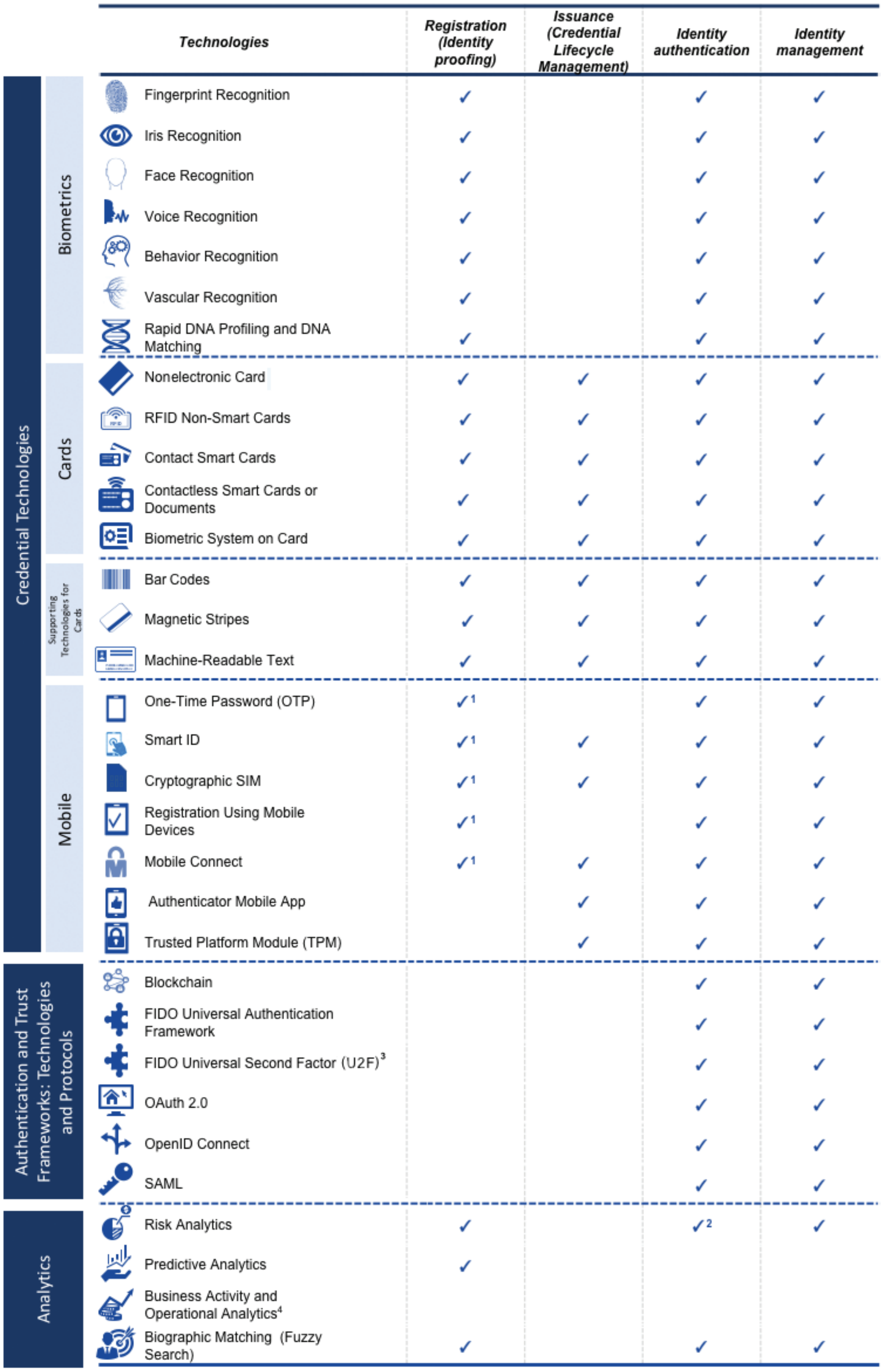


For each category, the technology's current capabilities and future growth trajectory are considered. Some applicable large-scale rollouts and limited pilots where these technologies are used to support identification or authentication are also highlighted. Though the focus of this report is on applications in digital ID programs, some examples of how a technology is being used in the private sector are also presented.

3.4. Mapping Technologies to the Identity Lifecycle

Before getting into the detailed assessments of the technologies, Figure 5 indicates which technologies can enable or affect a certain step in the Identity Lifecycle. For example, fingerprint and vascular capture and matching technologies are applicable in Registration, Authentication and Identity Management, but not in Issuance. Likewise, blockchain is applicable only after Identity Proofing. The following sections will provide a description of each and highlight the problems a particular technology can or cannot solve.

Figure 5: Technologies Mapped to the Identity Management Lifecycle



		Technologies	Registration (Identity proofing)	Issuance (Credential Lifecycle Management)	Identity authentication	Identity management
Credential Technologies	Biometrics	Fingerprint Recognition	✓		✓	✓
		Iris Recognition	✓		✓	✓
		Face Recognition	✓		✓	✓
		Voice Recognition	✓		✓	✓
		Behavior Recognition	✓		✓	✓
		Vascular Recognition	✓		✓	✓
		Rapid DNA Profiling and DNA Matching	✓		✓	✓
	Cards	Nonelectronic Card	✓	✓	✓	✓
		RFID Non-Smart Cards	✓	✓	✓	✓
		Contact Smart Cards	✓	✓	✓	✓
		Contactless Smart Cards or Documents	✓	✓	✓	✓
		Biometric System on Card	✓	✓	✓	✓
	Supporting Technologies for Cards	Bar Codes	✓	✓	✓	✓
		Magnetic Stripes	✓	✓	✓	✓
		Machine-Readable Text	✓	✓	✓	✓
	Mobile	One-Time Password (OTP)	✓[1]		✓	✓
		Smart ID	✓[1]	✓	✓	✓
		Cryptographic SIM	✓[1]	✓	✓	✓
		Registration Using Mobile Devices	✓[1]		✓	✓
		Mobile Connect	✓[1]	✓	✓	✓
		Authenticator Mobile App		✓	✓	✓
		Trusted Platform Module (TPM)		✓	✓	✓
Authentication and Trust Frameworks: Technologies and Protocols		Blockchain			✓	✓
		FIDO Universal Authentication Framework			✓	✓
		FIDO Universal Second Factor (U2F)[3]			✓	✓
		OAuth 2.0			✓	✓
		OpenID Connect			✓	✓
		SAML			✓	✓
Analytics		Risk Analytics	✓		✓[2]	✓
		Predictive Analytics	✓			
		Business Activity and Operational Analytics[4]				
		Biographic Matching (Fuzzy Search)	✓		✓	✓

[1] Applicable only if the technology is used to assert identity or make an identity claim.

[2] Applicable to authentication by using thresholding schemes.

[3] FIDO U2F not mapped to issuance because the second factor is managed by a different issuing authority.

[4] Business Activity and Operational Analytics monitor the identification system performance and not the user.

4. Credential Technologies

This report categorizes credentials into three sub-technologies: biometrics, cards, and mobile. A biometric identifier can be used as a credential once it has been registered with the issuing authority. For example, after a traveler completes the registration process with the Canadian Border Services Agency, their irises are the only credential required for NEXUS Air. Cards, smart cards, and mobile devices can be used to store identity information and can be used as evidence to support an identity claim.

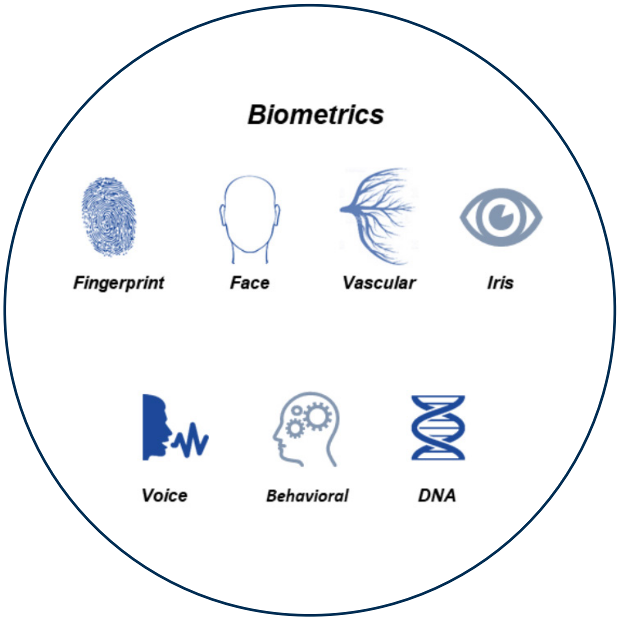
Credentials were originally designed for traditional computing devices (such as desktop and laptop computers) where the Personal Identity Verification (PIV) card can be used for identity authentication through integrated readers. However, with the emergence of a newer generation of computing and mobile devices, use of PIV cards has proved to be challenging. Mobile devices lack integrated smart card readers. This is where developments in biometrics and near-field communication (NFC) are enabling users to authenticate themselves using a phone's integrated biometric sensors and NFC-enabled mobile devices and cards.

4.1. Biometrics

Biometric recognition uses an individual's unique physiological and behavioral attributes to identify and authenticate his or her identity. Physiological attributes include elements related to shape or composition of the body, such as fingerprints ridges, iris patterns, and facial characteristics. Examples of behavioral attributes include gait, signature, keystroke patterns, and mouse usage. The type of attribute collected and matched is called modality. For example, fingerprint and iris are different biometric modalities.

In the sections that follow, a number of biometric modalities are reviewed—including iris, fingerprint, face, voice, behavior, vascular, and DNA. (See Figure 6.)

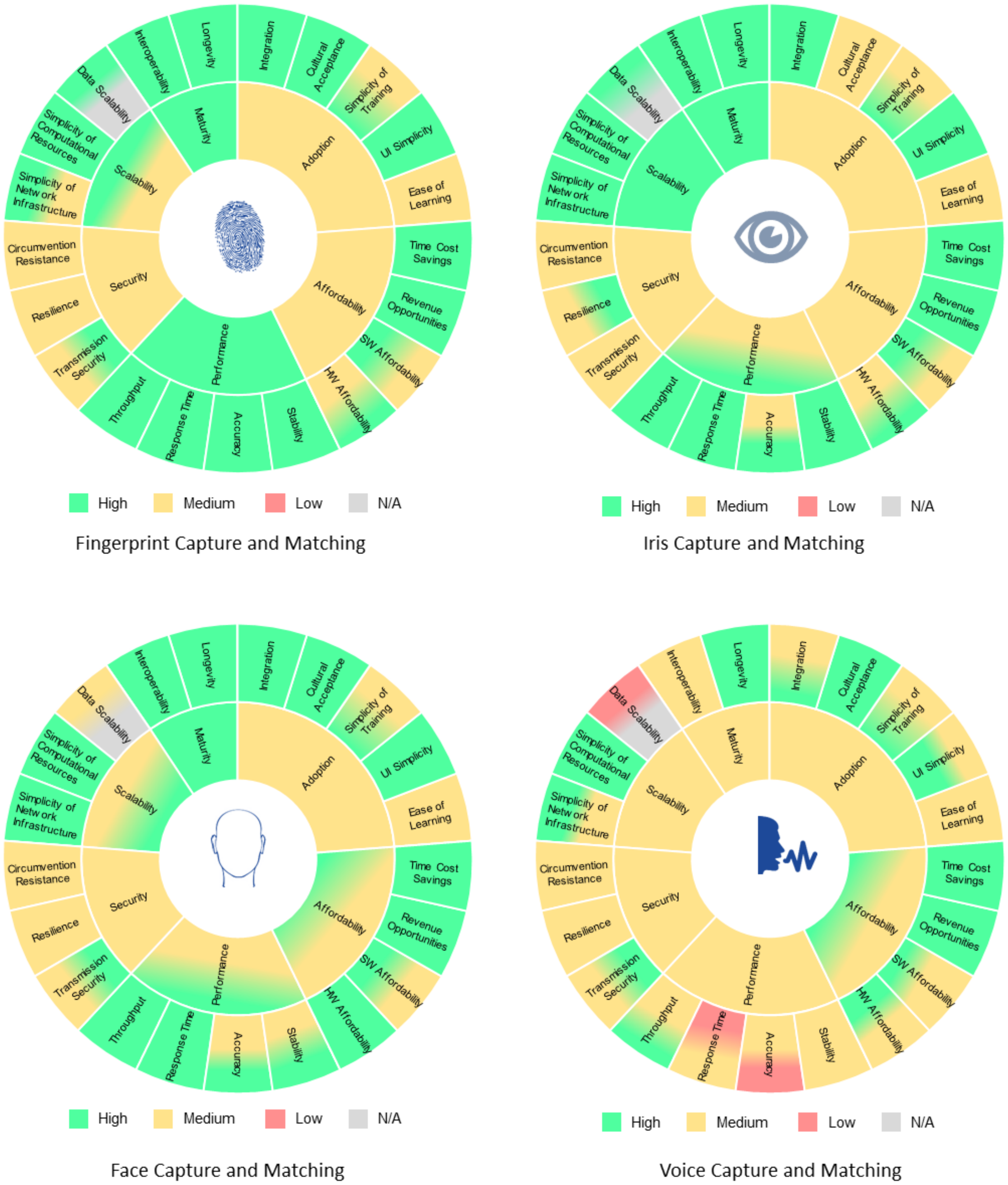
Figure 6: Biometric Sub-Technologies



In the assessment, biometric capture and matching are distinguished from each other. The reason is that the technologies are maturing at different rates. And although they are related, they are selected based on specific needs that may not be related. For example, ease of capture has little to do with matching speed. Capture is the process of collecting the biometric data from the user. Matching is the process where an individual's probe biometric record is matched against the stored record (candidate) when an end user requests access to any biometrically protected system (such as for authentication), or is matched against all candidates during a de-duplication (i.e., identification) search. Certain modalities also have different levels of maturity and technology advancement for capture and matching. Moreover, the ratings are an average of different devices and subjects. The devices may vary in terms of cost, speed, features, and other characteristics, while subjects may vary based on age, profession, and other factors that make the capture process easier or difficult for the specific demographic group.

Even though the capture and matching technologies for each modality have been evaluated separately, in the biometrics assessment summary shown in Figure 7, the different assessments for capture and matching are combined into one graph using gradients. The inner color represents the rating for the respective modality's capture technology, and the outer color represents the rating for matching technology.

Figure 7: Biometric Capture and Matching Assessment

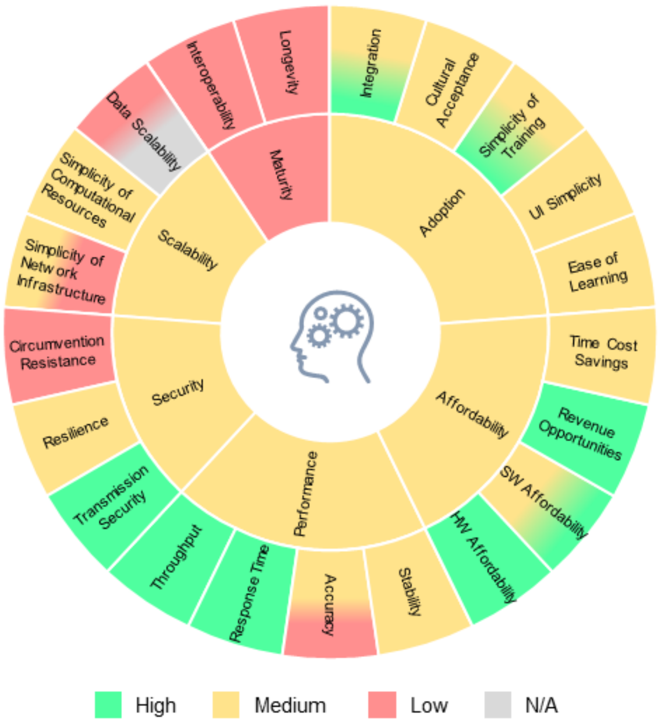


Fingerprint Capture and Matching

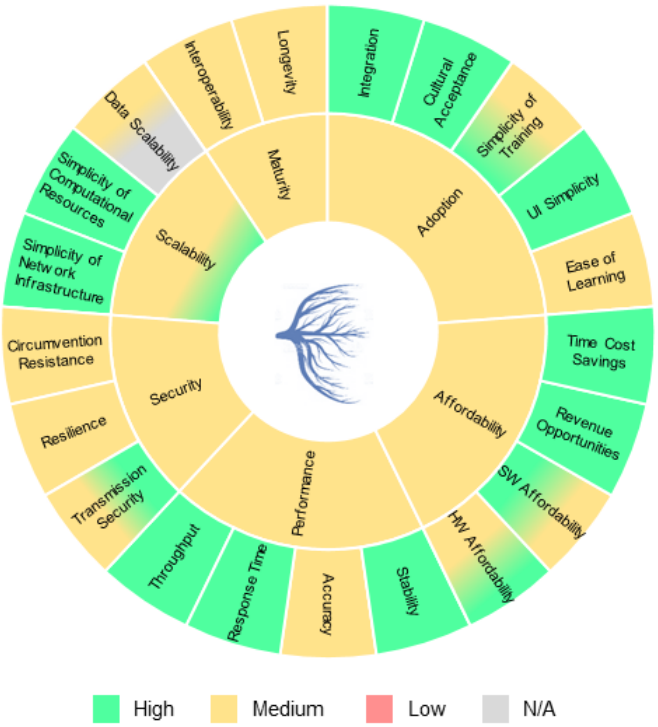
Iris Capture and Matching

Face Capture and Matching

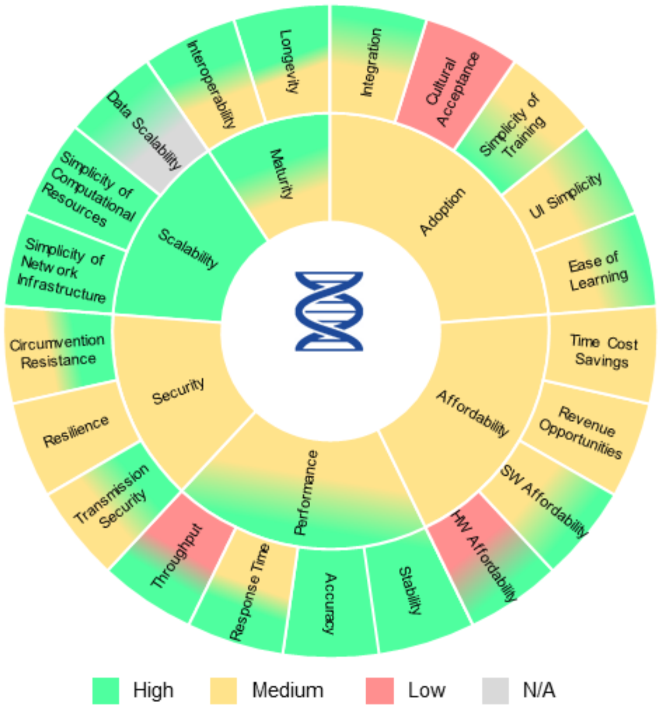
Voice Capture and Matching



Behavioral Capture and Matching



Vascular Capture and Matching



DNA Profiling and Matching

In determining which modalities to incorporate in a biometric-recognition system, decision makers must consider the following criteria:

- **Accuracy:** false acceptance rate (FAR) and false rejection rate (FRR) under operational conditions
- **Universality:** presence of the trait in members of the relevant population—important because certain traits (like fingerprints) may be poor or damaged in certain demographics and can lead to a failure to enroll (FTE) the individual
- **Stability:** permanence of the trait over time or after disease or injury
- **Collectability:** ease with which good quality samples can be acquired
- **Resistance to circumvention:** vulnerability of the modality to fraud
- **Acceptability:** degree of public openness for use of the modality
- **Usability:** ease with which individuals can interact with the technology used to capture the biometric data
- **Cost:** costs of sample collection and matching; namely, hardware, and software costs

In evaluating how well different biometrics meet these criteria for effectiveness, the biometrics can be thought of as falling into two major categories:

- **Primary biometrics** are associated with modalities such as fingerprint, face, and iris recognition, and have relatively low FARs and FRRs. Identification systems that must search across large galleries of biometric samples use primary biometrics because they yield more accurate results.
- **Soft biometrics** relate to an individual's behavioral characteristics, such as keystroke patterns, signature, and gait. Error rates are typically too high for identification searches, but these modalities are used for continuous authentication to verify the identity of the user throughout a session. Through analysis of a user's behaviors and interactions with a device, continuous authentication can detect anomalies during a session.

The following sections will examine each biometric modality in more detail.

4.1.1. Fingerprint Recognition

The presence and location of distinctive features on the surface of a fingertip, on what are known as friction ridges, are unique to an individual. Friction ridges include bifurcations and ridge endings, and the location and direction of these characteristics are called minutiae.[29] Other features are classified as pattern-based where patterns are categorized as islands, deltas, loops, whorls, and pores. Biometric matching algorithms derive and compare templates from images that include some or all of these fingerprint features (minutiae and patterns) to identify and authenticate individuals.

Depending on business needs and the level of assurance needed, the number of fingerprints captured and matched for an individual can be from 1 to all 10 fingers (or more for physical abnormality, such as polydactyls). Authorities can use a number of different sensors to capture fingerprints:

- **Optical sensors** capture an image, essentially a photograph, and use algorithms to detect unique patterns by analyzing the lightest and darkest areas of the image.[30]

[29] Naser Zaeri (2011). *Minutiae-based Fingerprint Extraction and Recognition, Biometrics*. Dr. Jucheng Yang (Ed.). InTech. DOI: 10.5772/17527. Retrieved from: https://www.intechopen.com/books/biometrics/minutiae-based-fingerprint-extraction-and-recognition

[30] Robert Triggs (09 July 2016). *How fingerprint scanners work: optical, capacitive, and ultrasonic variants explained.* Retrieved from Android Authority: https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

- **Capacitive sensors** use electrical current to form an image of the fingerprint. Capacitance of fingerprint valleys differs from that of ridges, owing to air pockets in valleys.
- **Swipe sensors** take readings after an individual swipes his or her finger across a small capacitive stripe. The technology "stitches" together several individual images to create an image of the fingertip.
- **Ultrasonic sensors** use a transmitter to send high-frequency sound waves that get absorbed or bounced back based on the fingerprint pattern. A receiver then analyzes this pulse to construct the pattern.
- **Thermal sensors** read the temperature differences on the contact surface between fingerprint ridges and valleys.
- **Multispectral sensors** capture multiple images of the fingertip under different illumination conditions such as wavelength, illumination orientation, and polarization.
- **Light-emitting sensors**, an emerging technology, reportedly work in direct sunlight on dry or moist fingers and resist abrasion. The devices are much smaller and lighter than traditional optical scanners.[31]
- **Optical thin-film transistor sensors,** another emerging technology, use light-sensitive pixels and a graphical display to illuminate the capture surface, and to guide users in placing their fingertips. The technology is smaller and lighter than traditional fingerprint scanners as well as easier for individuals to interact.[32] Specifically, it can display graphical elements, animations, or videos on the surface where individuals place their fingertips.

Fingerprint matching is the process of comparing an individual's fingerprint(s) templates against fingerprint(s) templates stored in the identity store for that user to verify an identity claim or against all users for an identification search. The result of fingerprint searching is a list of candidates whose similarity score is above the threshold defined for the operation. In some implementations, similarity scores are provided for all comparisons; in others, scores are provided for only the top 'N' candidates.

Evaluating fingerprint matching is important, given its widespread applications. Recent advancements in fingerprint matching technology have achieved very high accuracy rates, with false negative identification rates (FNIRs) as low as 1.9% for single index fingers matching and 0.09% for ten fingers matching.[33] Accuracy of fingerprint matching improves with prints of more fingers captured for every individual.

Fingerprint recognition is now increasingly being used for online authentication. This is already in practice in banking applications. For example, Bank of America customers can save their fingerprints on their phones and use them to access their accounts. This may also eliminate the need for passwords or PINs.[34] Fingerprint capture and matching has high market penetration, with many countries using fingerprints as the primary modality in their digital ID systems. What's more, capturing and matching fingerprints requires little training for operators and for individuals being fingerprinted.

What problems can it solve?

- **Performance.** Fingerprint matching accuracy is sufficiently good to warrant use on a national scale. Inclusivity is high; in the Aadhaar program, for example, the FTE rate for fingerprint biometrics was

[31] Integrated Biometrics, LLC. Retrieved from: https://integratedbiometrics.com/technology/

[32] Jenetric GmbH. Retrieved from: http://www.jenetric.com/technology.html

[33] National Institute of Standards and Technology, U.S. Department of Commerce (December 2014). *Fingerprint Vendor Technology Evaluation.* Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf

[34] Danny Thakkar. *Biometrics in Banking—for Identification and Verification.* Bayometric. Retrieved from: https://www.bayometric.com/biometrics-banking-identification-verification/

only 2%.[35] Fingerprint matching technology has also advanced to the point where some matching algorithms can perform more than a billion matches per second,[36] and high resolution 1000+ dpi scanners are being piloted for infant biometrics.

- **Maturity.** Fingerprint matching is fairly mature and has well-established standards for interoperability, making it well suited for inter-agency and cross-border applications.
- **Affordability.** Fingerprint matching technology is cost-effective, on the order of biometric matching technologies of many other modalities. Fingerprint-capture technologies range from well under $100 for a single finger, mass-produced capture device to thousands of dollars for a contactless, four-finger capture device.

What problems does it not solve?

- **Performance (stability).** Fingerprint capture is not universally inclusive, given that some friction ridges are unreadable, damaged, or worn, especially in people who work with caustic chemicals and in agriculture or manual labor, the elderly, infants, and persons with small fingertips.
- **Adoption.** Some people still view contact-based fingerprint-capture sensors as unhygienic, and these perceptions could limit willingness to use the technology. In cases where administrators are required to physically assist subjects through the capture process, some may perceive this as invasive or inappropriate. In addition, some still associate fingerprinting with criminal behavior and oppose it. However, emerging contactless scanner technology could help alleviate such concerns.
- **Security.** The technology is not immune to circumvention, which raises some worries about security and privacy. Nevertheless, technologies for detecting presentation attacks are emerging, as defined in ISO 30107.

What problems could it create?

- **Affordability.** Contactless fingerprint capture scanners could cost significantly more than traditional scanners.

4.1.2. Iris Recognition

Iris recognition uses the unique features of the iris, which include the pigmented portion of the eye separating the dark pupil at the center of the eye from the white sclera around the pigment. Near infrared (NIR) light is typically used to illuminate the iris during the capture process, bringing out the patterns by diminishing the spectrum (color variation) in the area of interest. The camera captures an image of one or both eyes and an algorithm then processes the image, detecting the sclera and pupil boundaries, and segmenting them accordingly. After segmentation, an algorithm derives a template (an iris code) based on the features in the iris.

Key advantages of iris-recognition technology include speed of matching; high accuracy; and stability of the iris's shape, color, and texture. Iris-matching technology typically employs mathematical models for pattern recognition to compare the iris templates. The iris is highly inclusive, secure, and accurate, with FRRs of 0.2% (fingerprint has 1%) and FARs of 0.0001% (fingerprint has 0.00002%).[37] In terms of capture rate, in a UNHCR project in Malawi, iris scored a 98% capture rate for one good iris, versus an 87% capture rate for four good fingers in individuals aged 4 and above. For young children and infants aged 0 to 3

[35] Based on SME discussion with Sanjay Jain, former Chief Product Manager of UIDAI.

[36] Innovatrics (10 August 2017). *Innovatrics Algorithm Processes 1 Billion Matches per Second.* Retrieved from: http://www.marketwired.com/press-release/innovatrics-algorithm-processes-1-billion-matches-per-second-2229791.htm

[37] Thakkar, D. *Top Five Biometrics: Face, Fingerprint, Iris, Palm, and Voice*. Bayometric. Retrieved from: https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/

years, the capture rate for one good iris was 14% versus 2% for four good fingerprints. Thus, iris scored higher than fingerprints in terms of ease of use, speed, and overall preference.[38]

Iris recognition can be used for authentication in online applications, and research efforts have focused on how to use this biometric for authentication in banking and e-commerce applications.[39,40]

What problems can it solve?

- **Performance.** Iris matching is highly suited for identity de-duplication because of its relatively low error rates for one-to-many matching during searches across large galleries (more than 1 million identities).[41] In Aadhaar, for example, FTE rates for iris scans is only 0.2% to 0.5 %.[42] What's more, the iris is more stable than some other modalities (namely face and fingerprint). Thus, operators don't have to frequently re-enroll this modality.
- **Scalability.** Matching speeds are high, with certain algorithms matching at a rate of 200,000 iris templates per second.[43] The technology can therefore be scaled to large populations.

What problems does it not solve?

- **Adoption.** Iris-capture technology may not be as user-friendly as face or contactless fingerprinting, because some iris-capture devices require highly specific positioning of the subject. There is also some cultural stigma associated with the iris scanner. But newer iris scanners are overcoming these challenges by being much easier to operate and requiring less operator or subject interaction than the older devices. New iris-at-a-distance technology also enables iris capturing at farther distances from the device, such as 0.8 to 1.2 meters.[44]
- **Affordability.** Iris-capture hardware and software typically costs more than that of fingerprinting. Iris matching technology, on the other hand, typically requires less computing power than that of fingerprinting.

4.1.3. Face Recognition

Face recognition uses the features of the face that do not change significantly with age or through surgery. These include the eyebrow ridge, cheekbones, edges of the mouth, distance between the eyes, width of the nose, and shape of the jawline and chin.

Currently, face-recognition technology is used mainly in security (such as in automated border clearance systems and surveillance) as well as to govern individuals' physical access to facilities.

[38] Gelb, A., Mukherjee, A., and Diofasi, A. (01 August 2016). *Iris Recognition: Better than Fingerprints and Falling in Price*. Center for Global Development. Retrieved from: https://www.cgdev.org/blog/iris-recognition-better-fingerprints-and-falling-price

[39] Lawal, A. and Chukwu, R.O. (November 2014). *Application of Iris Biometric Technology to Banking Industry in Nigeria*. International Journal of Soft Computing and Artificial Intelligence Vol-2, Issue-2, pp. 17–22. Retrieved from: http://www.iraj.in/journal/journal_file/journal_pdf/-141544422317-21.pdf

[40] Vangala, R.R. and Sasi, S. (2004). *Biometric authentication for e-commerce transaction.* 2004 IEEE International Workshop on Imaging Systems and Techniques, IST. pp. 113–116. Retrieved from: https://www.researchgate.net/publication/4125406_Biometric_authentication_for_e-commerce_transaction

[41] NIST. *Performance of Iris Identification Algorithms.* Retrieved from: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=910350

[42] Based on SME Interview with Sanjay Jain, former Chief Product Manager of UIDAI.

[43] Neurotechnology. Retrieved from: http://www.neurotechnology.com/megamatcher-technical-specifications.html

[44] Morpho. *Iris at a Distance: the power behind the iris.* Retrieved from: https://www.morpho.com/en/media/iris-distance-power-behind-iris-20140311

Facial-recognition systems and algorithms fall into two main categories: two-dimensional (2D) and three-dimensional (3D). Currently, 2D systems outperform 3D, but this is expected to change soon.[45] 2D uses principal component analysis (PCA) to improve accuracy by reducing the dimensionality of the data (reducing the number of random variables under consideration by obtaining a set of principal variables), while retaining as much as possible of the variation present in the original dataset. Operators can achieve significant improvements by first mapping the data into a lower dimensional subspace.[46] Linear discriminant analysis (LDA) is another 2D technique. It also aims to reduce dimensionality and preserve data variations. However, it is better able to distinguish image variation stemming from factors such as illumination and facial expression. Apple has bundled facial recognition that it calls Face ID with the latest iPhone X. Face ID is a form of biometric authentication that relies on unique characteristics of the face. It uses a combination of an infrared emitter and sensor to project 30,000 points of infrared light on and around the face. The camera then calculates depth and angle for each dot and constructs a depth map which is then used for matching. This feature improves matching accuracy and makes presentation attacks easier to detect because depth is used along with other characteristics to determine whether the subject is genuine or is being manipulated in some fashion.

As face-recognition solutions become more prevalent, they can also be used to authenticate users in online transactions. Several facial-recognition trials have been conducted recently by financial services institutions to investigate the technology's efficacy; for instance, in credit card payments.[47] MasterCard even ran a trial to approve online purchases using a facial scan.[48]

What problems can it solve?

- **Performance.** This technology can be used in large-scale identification systems, including in inter-agency and cross-border identification cases, because the accuracy of three-dimensional face matching has improved substantially. Today, FAR and FRR rates are on par with those of fingerprint-recognition systems for authentication (1-to-1 matching).[49] Facial-recognition-system accuracy is affected by the quality and size of the gallery being searched and does not perform as well as iris and fingerprint at large-scale identification (one-to-many searches).
- **Adoption.** Face-recognition capture technology is relatively easy to use**.** Taking a photograph requires minimum training for operators and little behavioral change on the part of users, although the quality of the image merits attention. With the increased use of covert facial-recognition technologies (such as those used for marketing or security without subjects' permission or notification), privacy concerns have increased.[50]
- **Affordability.** Facial recognition has become increasingly affordable, owing to a rise in bundling of the technology with smartphone camera systems. It could therefore rival the success of the smartphone-based fingerprint sensor for personal authentication. Where facial-recognition systems are used for automated identification searches (1: N) on large databases with poor- to medium-quality of input photos (which is often the case), system owners can expect higher operational costs owing to a higher rate of manual adjudications.

[45] Scheenstra, A., Ruifrok, A., and Veltkamp, R. C. (2005). *A Survey of 3D Face Recognition Methods.* In Lecture Notes in Computer Science, pp. 891–899. Retrieved from: http://www.cs.uu.nl/groups/MG/multimedia/publications/art/avbpa05.pdf

[46] Bebis G. (2016). Biometrics. Lecture Notes. Retrieved from: https://www.cse.unr.edu/~bebis/CS790Q/Lect/FR_PCA_LDA.ppt

[47] G. Jetsiktat, S. Panthuwadeethorn and S. Phimoltares (2015). *Enhancing user authentication of online credit card payment using face image comparison with MPEG7-edge histogram descriptor.* 2015 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), Okinawa, pp. 67–74. Retrieved from IEEE: http://ieeexplore.ieee.org/document/7439481/

[48] Jose Pagliery (01 July 2015). *MasterCard will approve purchases by scanning your face*. CNN. Retrieved from: http://money.cnn.com/2015/07/01/technology/mastercard-facial-scan/index.html

[49] SME Input from Dr. Joseph Atick, Executive Chairman, ID4Africa & Identity Counsel.

[50] (03 October 2017). *Privacy is under threat from the facial recognition revolution*. Financial Times. Retrieved from: https://www.ft.com/content/4707f246-a760-11e7-93c5-648314d2c72c

What problems does it not solve?

- **Performance.** Although performance of facial-recognition software has improved significantly, it yields satisfactory performance only under controlled scenarios. Performance degrades with aging, poor illumination, and variations in subject poses.[51] In addition, there is opportunity for greater standardization.
- **Security.** The technology is not immune to circumvention. For example, using a technique called morphing, individuals can create a photo ID containing a graphical representation of several faces, which enables multiple individuals to share credentials. This risk worsens in unsupervised environments.

What problems could it create?

- **Adoption.** If facial-recognition systems are optimized for recognition of the majority of ethnic groups in a multiethnic society, they may make more errors in evaluating faces of people who are members of minority groups.[52] This could worsen the exclusion and marginalization of such individuals.
- **Adoption (cultural acceptance).** Facial recognition could be used for surveillance of a country's individuals without their consent. These systems gather feeds from numerous closed-circuit television (CCTV) cameras and perform real-time face recognition to identify offenders or other persons of interest. Countries like China[53] and Russia[54] have already deployed such systems in large-scale pilots.
- **Adoption (vendor lock-in).** There is a need for greater standardization. This is especially true in defining facial templates to remove potential vendor lock-ins and to reduce storage requirements, as most implementers must store images that often require more storage space than fingerprints' compressed International Organization for Standardization (ISO) templates.[55]

4.1.4. Voice Recognition

Voice-recognition technology interprets voice patterns to recognize individuals based on their voice. In these systems, collected voice samples are converted into a spectrograph—a visual representation of the acoustic properties of a sound. This spectrograph is then used for verification or identification purposes.

Voice is both a physiological and behavioral biometric modality. Indeed, the acoustic properties of an individual's speech are determined by anatomical features such as the shape of the person's mouth and the length and quality of the vocal cords (physiological)—along with his or her unique intonations while talking. Using more than 100 physical and behavioral factors (including pronunciation, emphasis, speed of speech, accent, vocal tract, and mouth and nasal passages), voice-recognition technologies can create a unique voice signature of an individual.

Use of this modality starts with voice registration, the process of capturing an individual's voice sample for the first time, assessing its quality, and creating and storing the resulting model. Voice verification and

[51] M. Hassaballah and S. Aly (30 July 2015). *Face recognition: challenges, achievements and future directions.* IET Computer Vision, vol. 9, no. 4, pp. 614–626. Retrieved from: http://ieeexplore.ieee.org/document/7172641/

[52] Garvie, et al. (2016). *The Perpetual Line-up: Unregulated Police Face Recognition in America.* Georgetown Law Center on Privacy & Technology

[53] Chin, J. and Lin, L. (26 June 2017). *China's All-Seeing Surveillance State Is Reading Its Citizens' Faces.* Wall Street Journal. Retrieved from: https://www.wsj.com/articles/the-all-seeing-surveillance-state-feared-in-the-west-is-a-reality-in-china-1498493020

[54] Gianluca Mezzofiore (28 September 2017). *Moscow's facial recognition CCTV network is the biggest example of surveillance society yet.* Mashable. Retrieved from: http://mashable.com/2017/09/28/moscow-facial-recognition-cctv-network-big-brother/#GzhBgoBDd8qy

[55] SME Input from Jérôme Buchler, International Business Development Manager at HSB identification.

potentially identification, is the process of comparing a probe (test) sample against the registered sample for authenticating an individual.

There are two types of voice-matching systems: speaker verification and speaker identification. Speaker-verification systems verify whether the voice sample presented by a person matches the voice sample stored in the database. This is a 1:1 matching process. Speaker-identification systems try to match a given sample voice with the samples in a database to identify the speaker. This is a 1: N matching process.

Two types of speaker-verification systems predominate: text-dependent, which requires the speaker to exactly say the enrolled or given password, and text-independent, where the speaker's identity can be verified without a constraint on the speech content. While text-independent is more convenient because individuals can speak freely to the system, it requires more extensive training of the algorithm and testing of speakers' utterances to deliver maximum accuracy.[56]

Voice recognition is now being used by many banks as an authentication biometric, especially while providing banking services to customers over the telephone.[57,58] Research is also being conducted on the use of voice recognition in e-commerce applications.[59,60]

What problems can it solve?

- **Adoption.** Voice recognition is readily adopted because people are familiar with it, and it's easy to use. It also doesn't raise concerns about hygiene or cultural appropriateness, since the voice-capture process requires no physical contact between individuals and a device, and no physical intervention by operators. Voice can also be used to remotely authenticate users. For example, it can be used in call centers to authenticate the identity of a customer.
- **Affordability.** Setting up a voice-based ID system is cost-effective because it requires little capture hardware beyond a simple microphone for recording voices, and associated matching technology is on par with other modalities.

What problems does it not solve?

- **Performance.** The voice-capture process requires recording about 10 seconds of a normal conversation when using text-independent voice recognition. Capture for enrollment requires about 30 seconds of speech. In both cases, quality of the recording affects matching accuracy. In addition, any extensive background noise, along with compression schemes that degrade sample quality, increases error rates. Other factors such as aging and illness, along with microphone or channel quality, signal amplitude and duration of the sample, can also erode sample quality. Voice matching typically has higher error rates compared to face, fingerprint, and iris recognition.
- **Scalability.** Compared to fingerprint and iris systems, which can perform millions of matches per second, common voice-recognition systems can process only a million records per day.

[56] Zhengyou Zhang (20 August 2006). *Speaker Verification: Text-Dependent vs. Text-Independent.* Microsoft Retrieved from: https://www.microsoft.com/en-us/research/project/speaker-verification-text-dependent-vs-text-independent/

[57] Kevin Peachey (01 August 2016). *Banks Turning to Voice Recognition*. BBC. Retrieved from: http://www.bbc.com/news/business-36939709

[58] ICICI Bank (25 May 2015). *ICICI Bank introduces voice recognition for biometric authentication.* ICICI Bank Retrieved from: https://www.icicibank.com/aboutus/article.page?identifier=news-icici-bank-introduces-voice-recognition-for-biometric-authentication-20152505124050634

[59] Shaji, N. A., Murali, S., et al. (Nov 2016). *A Survey on Biometrics Authentication for Online Transactions.* International Journal of Engineering and Computer Science, Volume 5, Issue 11, pp. 19241–19243. Retrieved from: https://www.ijecs.in/issue/v5-i11/93%20ijecs.pdf

[60] W. Yang, Y. Wu, and G. Chen (2011). *Application of Voice Recognition for Mobile E-Commerce Security*. Third Pacific-Asia Conference on Circuits, Communications and System (PACCS), Wuhan, pp. 1–4. Retrieved from: http://ieeexplore.ieee.org/document/5990286/

What problems could it create?

- **Security.** Since voice matching can be performed remotely, these systems could be circumvented using a voice sample from an individual. Also, because background noise and other factors can impede voice-recognition accuracy, this modality can be used only in environments where the level of assurance needed for an identity claim is low. Circumvention may be mitigated through text-dependent voice recognition, which includes a dynamic pass-phrase.

4.1.5. Behavior Recognition

Behavioral biometrics uses human behavior patterns to authenticate an individual, and is typically combined with one or more other physiological modalities in a multimodal system. Behavioral biometrics includes signature dynamics (such as the speed and pressure with which a person signs his or her name), gait, keystroke dynamics, mouse usage, and touchscreen interactions. Devices like smartphones can be configured to passively capture behavioral data through the touchscreen, accelerometer, and gyroscope. Increasingly, organizations are using social media footprint (also called metadata) to prevent and track identity theft and fraud, and to support continuous authentication of a user over a session.

Behavioral biometrics are currently being deployed in online banking, e-commerce, payments, and high-security authentication markets.[61] Technology is now being developed to identify users based on behaviors such as cursor movements, click patterns, typing speed, swipe patterns, and geographical location.[62] Behavioral analytics in conjunction with machine learning is now also being used to deliver identity assurance.[63]

What problems can it solve?

- **Performance.** Operators can use behavioral biometrics for real-time, continuous authentication along with legacy authentication mechanisms such as password entry. For behavioral matching, numerous data points are collected, and operators can use any combination of them to identify an individual.
- **Adoption.** In dynamic signature verification (one type of behaviorial recognition enrollment), results are independent of the user's native language. This makes the technology more socially and legally acceptable, boosting the likelihood of adoption.

What problems does it not solve?

- **Maturity.** Behavioral-recognition technology has not yet been fully studied, and standards for data collection and exchange are still being developed. Thus, the technology may not be suitable for use as a stand-alone system for digital identification.
- **Performance.** Accuracy of dynamic signature verification is not high enough for use as a stand-alone modality for digital ID systems. Though multiple parameters (such as pen-tip pressure, number of strokes, and pen angle) are considered, such verification is only 97.47% accurate.[64] As with using a biometric like finger or iris to lock a smartphone, a pattern lock that is a behavioral biometric is less secure.

[61] International Biometrics + Identity Association. *Behavioral Biometrics.* IBIA. Retrieved from: https://www.ibia.org/download/datasets/3839/Behavioral%20Biometrics%20white%20paper.pdf

[62] Alton, L. (23 August 2015). *Next-Gen Cybersecurity Is All About Behavior Recognition.* TechCrunch. Retrieved from: https://techcrunch.com/2015/08/23/next-gen-cybersecurity-is-all-about-behavior-recognition/

[63] Oeltjen, J. (06 November 2017). *Authentication and Machine Learning: Taking Behavior Recognition to a New Level.* RSA Security LLC. Retrieved from: https://www.csoonline.com/article/3209917/identity-management/article.html

[64] Schmidt, T., Riffo, V., and Mery, D. (2011). *Dynamic Signature Recognition Based on Fisher Discriminant.* Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications, pp. 433–442. Retrieved from: https://link.springer.com/chapter/10.1007/978-3-642-25085-9_51

- **Scalability.** The technology is not highly scalable because the metadata associated with behavioral recognition is typically captured and analyzed at a centralized location over a period of time. By contrast, other systems are enrolled just once and authenticated locally against the enrolled pattern immediately. Additionally, training an operator to use behavioral biometrics systems usually takes days or weeks. Finally, behavioral authentication cannot be performed locally on devices and needs to be connected to a back-end server, unlike other modalities like fingerprint and face.

What problems could it create?

- **Adoption.** The technology could raise concerns about privacy and surveillance, because the background data required for behavioral authentication is captured continuously and, in some cases, without individuals' awareness or permission.

4.1.6. Vascular Recognition

Every person has a distinct pattern of veins. Vascular (vein) pattern recognition uses this physiological biometric trait for identity recognition such as back of the hand, in the palm, or in the fingers. NIR light is used to illuminate veins just under the skin, which show up as dark and distinct against a lighter background of arteries. A sensor then reads the image to capture or match the vein pattern. Palm-vein was used as an example for the assessment presented in this section.

A few companies offer vascular-recognition technologies for authentication, and the technology is gradually being adopted for identification. A notable example is NYU Langone Medical Center, which uses a vein-matching system to identify patients and obtain their previous medical records from the database. This system has proved useful for identifying even unconscious and uncommunicative patients.[65] Japan's financial services sector has also implemented the technology to verify customers in retail channels.[66] This approach has reduced financial service providers' dependency on handheld cards or documentation, which have been frequently lost in the island nation owing to earthquakes.

Vascular recognition has been used since the 1980s but has not achieved high-market penetration. One potential reason for this could be the lack of large-scale studies of this modality.

What problems can it solve?

- **Performance.** Some vascular-matching systems can accommodate transactions for as many as 100,000[67] individuals. The systems also tend to be accurate, reporting FRRs of just 0.01% and FARs of unauthorized users of 0.00008%.[68]
- **Adoption.** Newer vascular-capture technologies accommodate more variability in hand positioning. The increased user-friendliness improves the likelihood of adoption.
- **Security.** Contactless vascular-capture technology offers better security than traditional contact fingerprint scanners do. That's because contactless vascular scanning does not leave latent prints during the capture process, reducing the possibility of someone tricking the system. Additionally, unlike face, iris, and fingerprints, remote capture of vascular patterns is impossible without the subject's knowledge.

[65] Plasencia, A. (25 July 2011). *Hospital Scans Patient Hands to Pull Medical Info*. NBC. Retrieved from: https://www.nbcnewyork.com/news/local/Hospital-Scans-Patient-Hands-to-Pull-Medical-Info-126142628.html

[66] Shimbun, A. (14 September 2016). *Japanese Bank to Let Customers Use Palm Vein Biometrics Instead of Cards*. Find Biometrics. Retrieved from: https://findbiometrics.com/japanese-bank-palm-vein-biometrics-30142/

[67] *PV1000-Palm Vein.* Indiamart.com. Retrieved from: https://www.indiamart.com/proddetail/pv1000-palm-vein-9918273197.html

[68] Fujitsu. *PalmSecure® Palm Vein Authentication Solution.* Retrieved from: https://www.fujitsu.com/us/Images/palmsecure_datasheet.pdf

What problems does it not solve?

- **Affordability.** Vascular-capture technology is more expensive than technologies used for fingerprinting, and costs about US$400-500.[69]

What problems could it create?

- **Maturity.** No leading independent organization (such as NIST) has yet tested vascular biometric technology's performance on large-scale identification and authentication. The technology is thus not well understood, and the lack of understanding could pose challenges related to integration and interoperability when implemented.

SPOTLIGHT: PRIVACY

Biometric data is one form of PII. The Biometrics Institute, an independent and impartial international forum for the sharing of knowledge and information about biometrics, has published the following guidelines for handling of biometric information:[70]

1. *All staff members and managers in an organization using biometrics should commit to protecting subjects' privacy, demonstrate respect for privacy, and systematically control the use of biometric and other personal data.*
2. *Where possible, organizations must respect a person's right to give informed consent to having biometric data collected from him or her. To give informed consent, the subject must understand:*
    - ○ *Why and when the biometric information is being collected*
    - ○ *Who is collecting it*
    - ○ *Who else will have access to it*
    - ○ *How it will be protected, stored, transmitted, and accessed*
    - ○ *What the time limits are on its use and storage*
    - ○ *How it will be removed or deleted from the identity database*
3. *Biometric data should be protected through privacy-impact assessments, privacy audits, clear privacy policies, and procedures and technical controls to prevent unauthorized access, accidental loss, or misuse of personal data.*
4. *Organizations should aim to ensure that no person will be denied service or access to benefits owing to his or her inability or unwillingness to provide biometric data or use a biometric system. An alternative should be offered where possible, and system design should include alternative processes for those unable to access the system, including providing the opportunity to access the system at a later date.*
5. *All individuals/data subjects should be informed of circumstances where data may be shared with other parties, whether for law enforcement purposes, fraud investigations, or other purposes relating to law or commerce.*
6. *Organizations should establish complaints and enquiry systems that include transparent avenues for redress and a sympathetic approach that accepts the possibility of procedural or technical faults in their biometrics system.*

[69] *Fujitsu PalmSecure Scanner with Shell.* Fulcrum Biometrics, LLC. Retrieved from: https://www.fulcrumbiometrics.com/

[70] Biometrics Institute (May 2017). *Privacy Guidelines—A Best Practice Guide for Biometrics and Privacy Guidelines.* Biometrics Institute. Retrieved from: https://www.biometricsinstitute.org/privacy-charter

4.1.7. Rapid DNA Profiling and DNA Matching

DNA is the genetic code that is unique to every organism, and has traditionally been used in law enforcement and paternity testing. DNA can also be used to establish kinship.

The technology works by measuring short-term repeat sequences in DNA. Measuring these sequences' length provides a highly accurate attribute that uniquely identifies the individual among the entire human population.

Before the introduction of Rapid DNA sequencing technology, DNA processing had to be performed in laboratories with trained technicians and specialized laboratory instruments. Generation of the final analysis took several days. Rapid DNA technology has reduced the processing time to about 90 minutes. Rapid DNA analysis involves creating a DNA profile from a reference sample swabbed from a person's mouth or inside the cheek in a fully automated manner. Additionally, the devices required have been miniaturized and made portable, strengthening the case for using DNA as a modality for identification.

DNA profiling generates a visual representation of DNA that features columns of dark colored parallel bands and is equivalent to a fingerprint lifted from a smooth surface. To identify the owner of a DNA sample, the DNA "fingerprint," or profile, must be matched, either to DNA from a known individual (1:1) or to a DNA profile stored in a database (1: N).[71] As much as 99.9% of the DNA from two people will be identical. The 0.1% of DNA code sequences that vary from person to person are what make each individual unique. The key to DNA matching is knowing where to look in the billions of letters of genetic code to find the genetic markers that will identify the important similarities or differences between people. For matching, DNA is isolated from the cells and millions of copies are made, using a method called polymerase chain reaction (PCR). PCR uses a naturally occurring enzyme to copy a specific stretch of DNA repeatedly. Having plenty of DNA to work with makes analyzing the genetic code easier. The DNA molecules are then split at particular locations to separate them into known sections, and the code at those specific points is analyzed to create a DNA fingerprint. The fingerprints from the two different samples are then compared to see whether they match.[72]

What problems can it solve?

- **Performance.** Because DNA contains patterns of genetic material that are present in every human being and unique in almost every individual (except identical twins), it can be used to uniquely identify a person even in very large populations.
- **Security.** DNA-based matching systems are highly resistant to circumvention. Though scientists have shown that it's possible to fabricate DNA evidence, doing so requires a sophisticated process and thus is out of the reach of average criminals, according to some experts.[73]

What problems does it not solve?

- **Performance.** Developing a DNA-based unique identifier takes a while—about 90 minutes—even in a Rapid DNA machine. The technology therefore has limited use in a digital identification system.
- **Affordability.** Hardware for rapidly developing a DNA profile is expensive (about US$250,000),[74] and profiling each sample costs roughly US$350. However, costs are coming down, with some Rapid

[71] Harris, W. *How DNA Evidence Works.* HowStuffWorks. Retrieved from: https://science.howstuffworks.com/life/genetic/dna-evidence4.htm

[72] *How Does DNA Testing Work?* (01 February 2013). BBC. Retrieved from: http://www.bbc.co.uk/science/0/20205874

[73] Pollack, A. (17 August 2009). *DNA Evidence Can Be Fabricated, Scientists Show.* New York Times. Retrieved from: http://www.nytimes.com/2009/08/18/science/18dna.html

[74] Butkus, B. (04 October 2012). *Rapid DNA Forensic Testing Systems from IntegenX, NetBio/GE Healthcare Hit Market.* GenomeWeb LLC. Retrieved from: https://www.genomeweb.com/pcrsample-prep/rapid-dna-forensic-testing-systems-integenx-netbioge-healthcare-hit-market

DNA systems available for only US$150,000 and sample-processing costs falling to just US$150. Once the DNA samples are profiled (for instance, through Rapid DNA sequencers), DNA matching is relatively simple. It requires minimal computing and storage capacity, resulting in much lower matching costs than other biometric matching systems.

What problems could it create?

- **Adoption.** Use of DNA for identification could lead to increased discrimination against people seeking to access services, because providers can identify users' race, gender, medical history, and familial relationships based on DNA. Resulting concerns about ethical aspects and privacy could discourage adoption of the technology. Indeed, a major controversy surrounding use of DNA is that it enables government agencies to learn much more about an individual than just his or her identity.

4.1.8 Key Trends in Biometrics

While the underlying capture and recognition technologies continue to evolve for fingerprint, face, and iris recognition, no major technology disruptions are anticipated. For instance, sensors have become more accurate and can read data from longer distances, such as through contactless fingerprinting and iris-at-a-distance scanners. Fingerprint matching technology has advanced to the point where some matching algorithms can perform more than 1 billion matches per second. High-resolution (1000+ dpi) scanners are being piloted for infant biometrics, and facial biometrics algorithms are advancing to better accommodate off-axis, lower resolution, and poorly illuminated faces. Across all of these modalities, sensors are evolving in ways that make it more difficult to trick a biometric-recognition system.

Experts expect to see as many as 600 million devices with biometric authentication by 2021.[75] By 2020, 50 billion Internet of Things (IoT) devices are forecasted to be in use, and 500 million biometric sensors will be deployed for IoT by 2018.[76] Indeed, IoT will be a major enabler for combining analytics and continuous assessment to generate an adequate level of assurance, in real time, that an individual is who he or she claims to be.

Meanwhile, multimodal biometric systems using a combination of iris, fingerprint, and face modalities will likely be the most promising for identifying and authenticating an individual. With attention to photo quality as prescribed in the associated standards and best practices from ISO and International Civil Aviation Organization (ICAO), face-authentication technology is now almost as accurate as fingerprinting for authentication.[77] However, this is not always the case in developing countries where legacy data is of very poor quality and enrollment guidelines are poorly enforced.

For some applications, governments or organizations will use behavioral recognition as a means for continuous authentication to ensure that an individual who was authenticated at the start of the session remains the same throughout the session. Some of the earliest deployments of continuous authentication to date have been in the European banking industry.[78] To achieve continuous authentication, system operators could use multimodal biometrics as well as behavioral parameters like geolocation, commuting and work patterns, and passive voice and face recognition.

[75] Smith, S. (29 November 2016). *Voice and Facial Recognition to Be Used in Over 600 Million Mobile Devices by 2021.* Juniper Research. Retrieved from: https://www.juniperresearch.com/press/press-releases/voice-and-facial-recognition-to-be-used-in-over-60

[76] Badugu, N. (17 May 2017). *Biometrics in Internet of Things (IoT) Security.* IoT ONE. Retrieved from: https://www.iotone.com/guide/biometrics-in-internet-of-things-iot-security/g712

[77] Source: Kris Ranganath from NEC.

[78] Violino, B. (14 March 2017). *Continuous authentication: Why it's getting attention and what you need to know.* IDG Communications, Inc. Retrieved from: https://www.csoonline.com/article/3179107/security/continuous-authentication-why-it-s-getting-attention-and-what-you-need-to-know.html

SPOTLIGHT: INFANT BIOMETRICS

An effective digital ID system is inclusive. But all populations contain groups for whom capturing biometric information is difficult or even impossible, making it hard to register members in the system. Fingerprinting infants is a case in point. The limited available ridge structure, due to small fingers, and aversion to the capture process make it difficult for devices to capture images of sufficient detail and quality to extract usable templates from the sample.

Yet effective infant biometric capture and matching technologies are emerging that raise hopes for surmounting this inclusion challenge. Consider vaccination programs. In developing countries, billions of dollars are spent each year to vaccinate children, but only about 50% of possible immunizations are administered because of unreliable vaccination records.[79] *A biometric system inclusive of children could enable clinicians to match children with their vaccination schedules, which usually start one month after an infant is born. This approach could also improve provision of welfare services (such as maternal and child welfare benefits) and trace infants who drop out of these public services.*

Current Limitations

While infant biometric technology is being piloted in various countries, solutions for infant enrollment in digital ID systems are still evolving. Moreover, technologies for biometric modalities such as fingerprints as well as ear and foot shapes present challenges when it comes to infant biometrics. That's because these biometric identifiers change substantially as a child grows. Researchers have studied template aging to a degree (algorithmically applying the aging process to templates to simulate aging), but this technique has not yet been proven effective. The iris modality also is not feasible for newborns, who can't look directly into a scanning device. Additionally, the iris pattern *typically doesn't stabilize until after a child has reached the age of two.*

It is also expensive and raises ethical concerns about its use in purposes other than law enforcement.[80]

Some countries—including India, Peru, Indonesia, Malaysia, and Thailand—are enrolling children in their ID systems without biometric information. Instead, they capture demographic information and associate children to their adult next of kin. In these cases, biometric information is captured and processed once the modalities stabilize, which is usually after the age of five. Information on a child can be updated and refreshed, including adding biometric details from iris and fingerprints. In the Indian state of Haryana, for example, children are registered for Aadhaar with the biometric data of one of their parents, along with that adult's Aadhaar number. The biometric data for the child needs to be uploaded when the child is five years old.[81] *Meanwhile, Peru's national identity document for children uses infants' biometric information (such as footprints and a photo) in combination with parents' fingerprints.*

A Way Forward

To overcome challenges inherent in infant biometrics, experts are working to develop and test biometric capture devices specifically tailored for infants. For instance, researchers are testing the use of additional modalities such as foot geometry and ear shape to enhance matching accuracy.[82] *Global Good Fund and*

[79] LaMonica, M. (04 September 2014). *Fingerprinting Infants Helps Track Vaccinations in Developing Countries.* MIT Technology Review. Retrieved from: https://www.technologyreview.com/s/530481/fingerprinting-infants-helps-track-vaccinations-in-developing-countries/

[80] Secure Insights SME Discussions.

[81] Sural, A. (30 April 2015). *Babies in Haryana will have Aadhaar cards.* Times of India. Retrieved from: https://timesofindia.indiatimes.com/good-governance/haryana/Babies-in-Haryana-will-have-Aadhaar-cards/articleshow/47111358.cms

[82] One World Identity SME Discussions.

Element Inc. are using the common camera on smartphones to image a range of infant modalities, including palms, feet, and ears, and are currently running longitudinal trials in Bangladesh and Cambodia. Using artificial intelligence (AI) and deep learning algorithms, aim to develop a non-touch solution for infant biometrics that can be deployed on common mobile devices, and run in areas of low connectivity.[83]

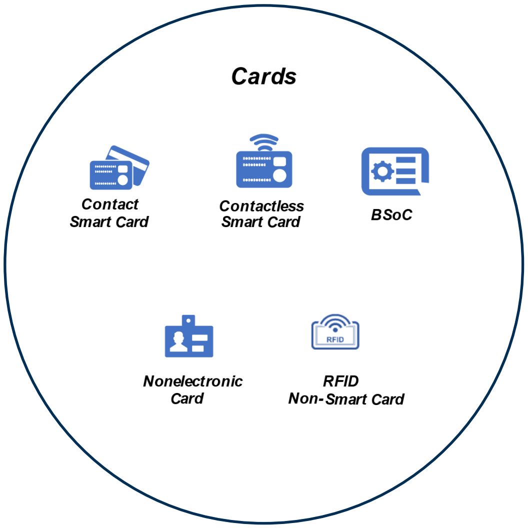
Additionally, NEC and Dr. Anil Jain, a professor at Michigan State University, have developed a high-resolution infant-fingerprint scanner that uses machine learning algorithms. In a pilot conducted in India, the scanner was used to capture fingerprint images of 300-plus children, 100 of whom were infants. The scanner delivered 99% accuracy for children older than six months but only 80% accuracy for four-week-old infants. As part of the same pilot, fingerprint recognition is also being piloted with infants in Benin for the purpose of tracking vaccination records. However, since fingerprints change over time, children need to be re-enrolled more frequently than adults.

Infant biometric-recognition technologies are expected to enter the mainstream thanks to technology advancements that improve accuracy and lower costs. Capturing and using biometrics of children is an emerging issue. Apart from the technical challenges, there are significant ethical considerations that require further examination, which UNICEF has recently launched research on.

4.2. Cards

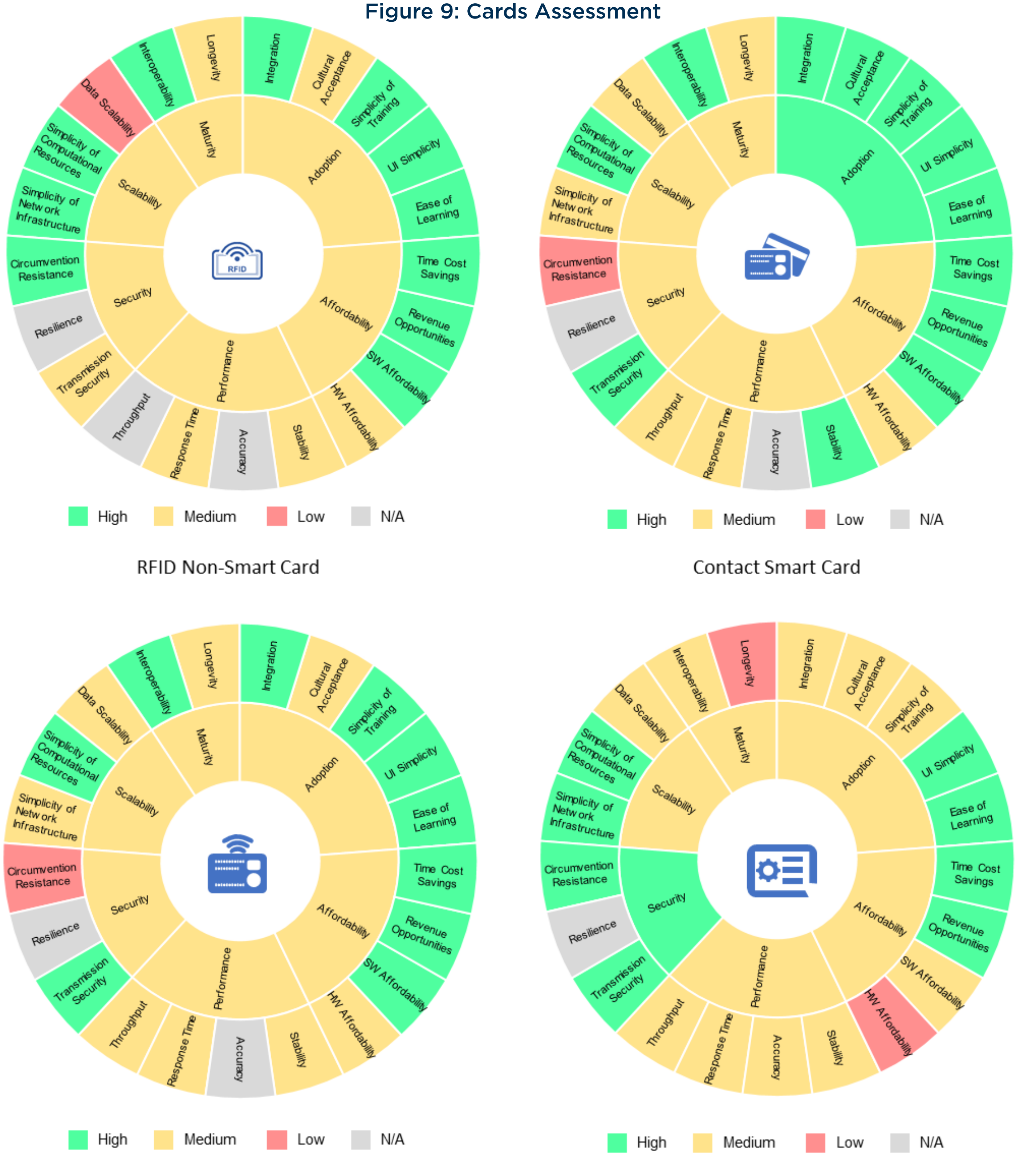
Cards in various formats can be read by specialized data input devices or card readers that use technologies that can capture and interpret bar codes or text through optical character recognition (OCR), magnetic-stripe readers, contact and contactless smart card readers, and other RFID readers. In the sections that follow, the assessments are presented for five forms of cards.

Figure 8: Cards



[83] *Global Good Fund and Element Inc. to Develop Biometric Identification Technology for Infants and Children.* (31 October 2017). One World Identity. Retrieved from: https://oneworldidentity.com/element-inc-global-good-fund-create-biometric-health-id-system-infants-children/

Figure 9: Cards Assessment

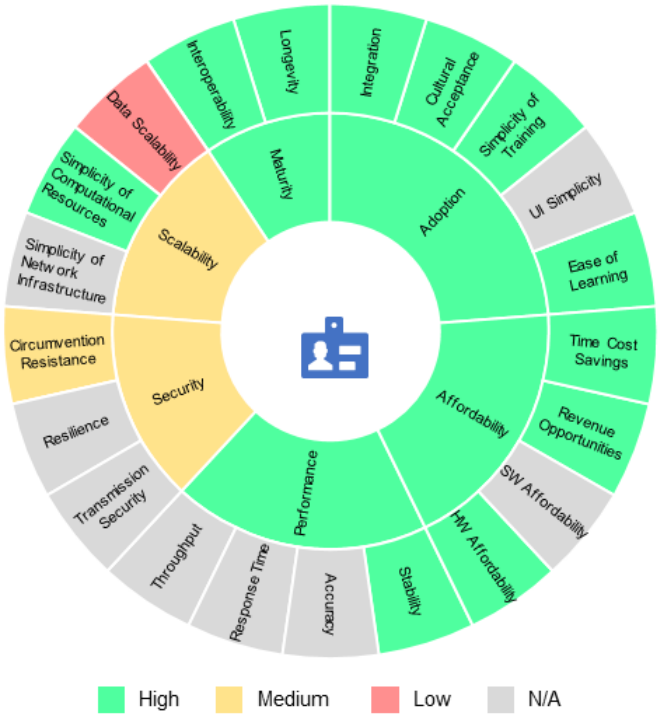


RFID Non-Smart Card

Contact Smart Card

Contactless Smart Card

Biometric System on Card (BSoC)



Nonelectronic Card

4.2.1. Nonelectronic Card

Nonelectronic ID cards can be plastic cards, typically made from PVC or polycarbonate, representing basic demographic information such as name, address, date of birth, digital ID number, photograph, signature image, and names of close family members. A nonelectronic ID card can be used as a photo identity proof where visual security features are used to detect fraud. Alternatively, the card can be used to validate an identity claim by using the unique identification number to reference a record in a central database. In South Africa, for example, a national identity number read from the national ID card and a fingerprint is sent to the Home Affairs National Identification System (HANIS) for authentication.[84]

Bar codes (including 1D: Code39, Codabar; 2D: PDF417, QR) are used in nonelectronic cards to automate the data-capture process and to reduce keypunch errors.

With limited use cases for on-spot validation, nonelectronic cards are not completely impersonation proof, unless they are linked to a central database. Additionally, with no processing or storage power on the card itself, the technology has limited scalability for local operations.

What problems can it solve?

- **Maturity.** Nonelectronic cards have been in use for a long time and is one of the simplest way of authenticating individuals. Bar codes or quick response (QR) codes make them easy to integrate with other technologies and thus fostering a high level of interoperability.

[84] *NEC AFIS created the world's largest civilian fingerprint identification database for HANIS.* NEC. Retrieved from: http://www.nec.com/en/case/sa/pdf/catalogue.pdf

- **Affordability.** Nonelectronic cards come with high affordability unless they have high security features. Their ease of implementation delivers time and cost savings as well. These cards do not require any specific software installation or embedding to operate, though QR or bar code readers are needed in some specific cases.
- **Adoption.** Being mostly a display card of individual information, nonelectronic cards are easy to use, fostering ready adoption. In a majority of countries, many people are already aware of how these cards work and how to use them.

What problems does it not solve?

- **Security.** The cards' security features are limited to optical and mechanical elements that are not as robust or scalable as electronic security features. Lost cards can be used by anyone carrying them, unless there is a parallel physical biometric validation present.
- **Scalability.** Nonelectronic cards do not provide an effective means for local biometric authentication. Although a biometric template could be encoded as a bar code on the card to support such local use, such templates are seen as insufficiently secure because they are not encrypted or insufficiently scalable because any encrypted templates require keys that must be distributed and secured.

What problems could it create?

- **Security.** The two major issues with the technology are around security and scalability. Whereas a smart card has a crypto processor and local storage, a nonelectronic card must rely on printed data limited by the size of the card and the bar code technology used. Although the bar coded data can be encrypted, it would be a static encryption scheme because there is no crypto engine. Use cases that involve implementation of local validation using biometric factors might not be achieved. Further, security threats are higher with a nonelectronic cards, especially as multifactor validation is not implementable.

4.2.2. RFID Non-Smart Cards

Radio frequency identification (RFID) uses electromagnetic energy to read information stored in RFID tags. Depending on the application, RFID tags are selected based on a number of parameters, including reading distance; amount and speed of data to be transferred; and security, size of documents, and cost. For many identification applications, passive RFID tags are preferred, whereby the electromagnetic energy that's transmitted to read the RFID tag is also used to power it. Active RFID tags are typically used for inventory control (supply chain) applications and are powered by the energy derived from an internal source, typically a battery. In addition to the tags, a basic RFID system includes readers and antennas used to interrogate the tags.

This description of passive RFID applies to both contactless smart cards and non-smart RFID cards. Non-smart card RFID uses an embedded RFID tag containing a microchip with limited computational ability, limited memory, and an antenna. Passive RFID cards can operate at various distances depending on the technology selected for the specific application. This report focuses on three passive RFID technologies that have seen adoption for authentication:

1. Proximity (ISO 14443, high frequency); nominal read range of 10 centimeters (covered in section 2.2.4)
2. Vicinity (ISO 15693, high frequency); nominal read range of 1 meter
3. Long range (ISO 180006-C, ultra-high frequency); nominal read range of 10 meters

This section of the report focuses on RFID non-smart cards, which have utility in certain applications but have not seen the same level of adoption as RFID smart cards, which are used in electronic machine-readable travel documents (MRTDs). A prime example of a non-smart card application of RFID is the US land border, where long-range RFID is used to identify travelers as they approach the border in vehicles. The ultra-high frequency (UHF) RFID tags are embedded in Trusted Traveler ID cards (SENTRI and NEXUS).[85] Such cards can be used by Americans, lawful permanent residents, and Mexican nationals who have enrolled and who cross the southern border in an enrolled vehicle (SENTRI) or cross the northern border (NEXUS) via vehicle. They can also be used by US citizens in possession of a US passport to travel to Canada, Mexico, Bermuda, and the Caribbean by a mode other than air. The RFID chip stores only a unique identifying number for accessing the cardholder's information in a secure Customs and Border Protection database.[86]

By design, passive RFID tags provide information when interrogated by a reader, and the information is limited to a unique identifier and other tag information (typically no PII). To prevent unintended card access, it is recommended that contactless RFIDs be stored in an RF-blocking sleeve similar to those provided with US passports and NEXUS and SENTRI cards.

What problems can it solve?

- **Performance.** Long-range RFID cards can be read at distances of about 10 meters and can be read in a rapid succession. These qualities make them useful for identifying travelers in vehicles as they approach borders. What's more, non-smart card RFID has an advantage over bar code technology in that it doesn't require the ID document to be in the card reader's line of sight—thus accelerating data capture.
- **Security.** Long-range RFIDs contain a serial number that lets authorized users access the associated information from a secured data repository. There is no PII that requires securing in the card.
- **Affordability.** Implementing baseline RFID-card technology requires relatively little investment, though the technology is more expensive than similar bar code technology.

What problems does it not solve?

- **Security.** When RFID tags are not in their shielded sleeves, authorized and unauthorized individuals can read them. This raises concerns about privacy and possible surreptitious tracking of anyone who has an exposed tag on his or her person.
- **Affordability.** Tags and scanners are more expensive than bar code stickers and bar code readers, a potential concern in developing countries.
- **Scalability.** Passive RFID technology lacks the capacity to store large amounts of data and lacks processing power, two capabilities needed to support advanced identification operations.

What problems could it create?

- **Security.** While RFID tags have advanced in complexity, power, and flexibility, they are still vulnerable to rogue RFID readers, who could read the tag information and use it for nefarious purposes. Additionally, individuals wouldn't even know that their data had been compromised in this way. This is similar to someone associating a vehicle's license plate number with an individual and tracking him or her based on that number. Users should take care when removing the RFID from its protective sleeve, to minimize surreptitious reads.

[85] *Global Entry Card.* U.S. Customs and Border Protection. Retrieved from: https://www.cbp.gov/travel/trusted-traveler-programs/global-entry/card

[86] Nogueira, M. and Greis, N. (December 2009). *Uses of RFID Technology in U.S. Identification Documents. Institute of Homeland Security Solutions.* Retrieved from: https://www.kenan-flagler.unc.edu/~/media/Files/kenaninstitute/CLDS/IHSSResearchBrief_RFID.pdf

4.2.3. Contact Smart Cards

A contact smart card is a physical credential with an embedded microchip and processing unit that's designed to operate when in physical contact with a card reader. The microchip includes a processor, memory, and a cryptographic controller that provides higher processing speeds and better security than memory-based cards designed for storing more data.[87] These cards follow ISO 7816 protocol, and have seen wide adoption in many countries, including Saudi Arabia, Pakistan, Kuwait, and South Africa. Governments use them to let individuals securely access multiple services. In Pakistan, for instance, the Computerized National Identity Card (CNIC) issued by the National Database and Registration Authority (NADRA) has been integrated with as many as 336 services. Individuals must use the card to vote, open a bank account, apply for a passport or driver's license, buy airline or train tickets, and complete many more processes.

Contact smart cards can also act as a payment or credit card. MasterCard and NADRA, for example, are optimizing CNICs for electronic payments.[88,89]

What problems can it solve?

- **Security.** Contact smart cards let individuals securely execute transactions online and offline at their convenience. Users validity can be confirmed offline at a local level, eliminating the need to transfer data over a network and thus avoiding the associated network vulnerabilities. Moreover, communication can be made more secure using the cards' built-in hashing, digital signature and encryption capabilities.
- **Scalability.** The technology can store sufficient identity data and perform cryptographic computations, thus lending itself to usage across many different services. As the technology has evolved, the cards have been able to store and transmit increasingly larger volumes of data with greater speed and computing power.
- **Adoption (integration).** The ability to add other applications to the card is another important advantage. Depending on the amount of memory available, smart cards can serve as multi-application credentials used for many purposes, including giving users physical access to facilities and tracking their time spent and attendance at a facility. Thus, smart cards offer great flexibility.

What problems does it not solve?

- **Scalability.** Contact smart cards require a reader that operators may have to procure and install if their computing device doesn't already have one.
- **Performance.** Smart cards must be in contact with the reader, and information is retrieved at relatively low speed. A photo on a smart card, for example, could take several seconds to read.
- **Affordability.** Although contact smart cards require less upfront investment than contactless smart cards, the overall costs might still be high.
- **Security.** The technology is moderately vulnerable to circumvention. That's because authentication of individuals is PIN-based (and a PIN can be observed or guessed). Alternatively, authentication may be biometric-based. The biometric reference is retrieved from the smart card and compared against a live biometric captured on an external sensor, allowing for presentation or man-in-the-middle

[87] Aarti R. (30 July 2009). *Types of Smart Cards.* Buzzle. Retrieved from: https://www.buzzle.com/articles/types-of-smart-cards.html

[88] Staff Reporter (19 January 2017). *Mastercard, NADRA sign accord on CNIC e-payment facility.* Dawn. Retrieved from: https://www.dawn.com/news/1309369

[89] *Computerized National Identity Card.* Retrieved from: https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Computerised_National_Identity_Card.html

attacks.[90] Certificate revocation lists (CRLs) should be consulted to determine that a contact smart card is still valid. This requires real-time connectivity or connectivity at intervals to download the latest CRL(s) locally.

What problems could it create?

- **Security.** If the card is secured with a four-digit PIN, for example, circumventers could access the protected information relatively easy if the card were not blocked after a number of failed attempts.

4.2.4. Contactless Smart Cards or Documents

A contactless smart card (ISO 14443) is a physical credential with an embedded microchip similar to that of a contact smart card as described above. It provides similar processing capabilities, but with the addition of a radio frequency (RF) transceiver and antenna designed to operate when in proximity to a card reader. The card is powered by the electromagnetic energy emanating from the reader.

Contactless smart cards have the same physical dimensions as contact smart cards and typically share the same processor options. However, contactless data-transmission rates tend to be slower than those of contact data transmission.

These cards can take the form of documents as well, including electronic passport books.[91] The technology is valuable for applications that require protection of personal information and secure communication with the contactless device. The on-chip intelligence enables systems to comply with privacy and security guidelines.

What problems can it solve?

- **Security.** A password for identification of individuals makes the technology moderately resistant to circumvention. And using an integrated circuit chip, cryptography protects information about the cardholder and programs for the multiple applications stored on the card.
- **Adoption (integration).** Tens of millions of contactless smart cards in the form of eMRTDs are in use globally, and these numbers are not expected to diminish in the near future. The technology can store sufficient identity data and perform cryptographic computations, thus lending itself to usage across many different services. As the technology has evolved, the cards have been able to store and transmit increasingly more data with greater speed and computing power.

What problems does it not solve?

- **Performance.** Although read speeds have increased over the years, it is still a gating factor. For example, about one third of the average time traversing an e-Gate is dedicated to reading an e-Passport (about 5 seconds).
- **Scalability.** Network scalability is medium because the technology relies on a network for either real-time CRL checks or intermittent downloads to a local cache, for example.
- **Affordability.** A card typically costs between US$2 to US$10, which may put it out of reach of low-income individuals—often the very people who most need an ID to access services.

[90] "An attack where the attacker keeps himself/herself between two parties, making them believe that they are talking directly to each other over a private connection, when actually the entire conversation is being controlled by the attacker" Tanmay Patange. *How to defend yourself against MITM or Man-in-the-middle attack.* The Windows Club. Retrieved from: http://www.thewindowsclub.com/man-in-the-middle-attack

[91] *International Civil Aviation Organization (2015).* Machine Readable Travel Documents. ICAO, 7th Edition. Retrieved from: https://www.icao.int/publications/Documents/9303_p4_cons_en.pdf

What problems could it create?

- **Security.** Contactless smart cards, similar to contact smart cards, may use PINs that can be observed or guessed. Moreover, just as in the case of non-smart RFID cards, a similar RFID tracking vulnerability and mitigation strategy applies in the case of contactless smart cards.

4.2.5. Biometric System on Card (BSoC)

Biometric system on card (BSoC) technology combines the biometric sensor and matcher on a smart card, typically a credit-card-sized card in conformance with ISO 7810. It thus improves on match-on-card solutions, which contain only the matcher. The sensor captures the biometric sample, and the processor then extracts biometric features from the image, comparing them against the enrolled feature set for verification. BSoC never transfers any sample or data to an external terminal.

Mastercard and VISA have recently unveiled its next-generation biometric card combining chip technology with biometrics. Customers can now establish their identity for in-store purchases easily through their fingerprints in Europay, Mastercard, and VISA (EMV) machines and can pay through mobile.

What problems can it solve?

- **Security.** Biometric authentication is performed when the legitimate cardholder is present, improving security. The technology is also highly resistance to circumvention. Transmission of data is secure because only the authentication result is transmitted, not PII.
- **Scalability.** Because the card performs matching locally, fingerprint information does not need to be transmitted to a central server, enhancing scalability of the technology.
- **Affordability.** Though BSoCs are more expensive than standard smart cards, they eliminate the need for costly external fingerprint readers.
- **Performance.** Authentication accuracy is moderate, owing to the sensor's size, but matching speed is high because the process is performed locally.

What problems does it not solve?

- **Maturity.** The technology offers moderate interoperability because interchange standards haven't been fully developed and defined.
- **Affordability.** Given the cost of these cards, agencies considering using this technology should conduct cost-benefit analyses to assess the trade-offs in adopting this solution.
- **Performance.** The sensor may experience undue wear and tear if mishandled, which could decrease the device's ability to perform accurate biometric authentications.

What problems could it create?

- **Adoption.** The experience of using these cards will be questionable for those with poor fingerprint friction ridges, those who don't use the technology to get familiar enough with it, and those who mishandle the card, especially the sensor.

4.2.6. Key Trends in Cards

Digital ID cards in global circulation are expected to increase from 1.75 billion in 2013 to 3.3 billion in 2021. Of this, a total of 3.2 billion national ID smart cards will be issued by 103 countries.[92]

As of early 2017, 82% of all countries issuing official ID cards have implemented programs that depend on smart cards or plastic cards and biometrics.[93]

Other innovations in cards include NFC—wireless communication that permits the exchange of data between devices that are just a few centimeters apart. NFC-enabled devices, together with mobile eID applications, enable mobile authentication in Germany's ID card system. Bluetooth low-energy beacon technology is innovation in the optional card characteristics domain. The beacon can find the location of a smart device and use transmitters to push pertinent information to Bluetooth-enabled devices.

Many countries are now implementing cards with built-in biometric security for their respective national ID programs. The government of Maldives has recently launched a biometric smart card based national ID called "Passport Card" for its citizens in collaboration with Mastercard. It contains a unique combination of dual-interface chip for contactless and contact card reading. This card functions as the passport, driving license, and national ID of the cardholder, and can be used to provide health and e-services by the government. It also functions as a payment card to make payments.[94] The card contains 10 fingerprints for secure verification.

Contactless smart cards are increasingly being adopted by many national identity programs such as the German Identity card and MyKad—the identity card issued by the Government of Malaysia to its citizens. MyKad is a multipurpose contactless smart card issued by the Government of Malaysia that functions as an identification card, driving license, passport, transit card, and health document. The card stores the cardholder's fingerprint information that can be accessed by a reader to verify the individual.

German identity card is a contactless smart card issued to the citizens of Germany. The contactless smart card is based on RFID technology and can be read from a distance of only 4 centimeters. Moreover, the chip is protected by a PIN which protects the data from being released unless the correct PIN is entered. Communication between the card and reader is also encrypted. This identity card can also be used as a valid travel document between European Union countries.[95]

In the future, biometric cards are likely to have a built-in biometric sensor on them instead of just storing a biometric template. The integrated sensor on a card model will replace the need for PINs and passwords and will work only after the cardholder activates it using his or her biometric information.[96] While fingerprint remains the primary biometric used on such cards, there is potential to use other metrics such as electrocardiography (ECG).[97]

[92] *The Global National eID Industry Report: 2017 Edition* by Acuity Market Intelligence.

[93] *The Global National eID Industry Report: 2017 Edition* by Acuity Market Intelligence,

[94] Mastercard (26 October 2017). *Mastercard and Bank of Maldives Introduce Passport Card in Partnership with Maldives Immigration.* Mastercard. Retrieved from: https://newsroom.mastercard.com/asia-pacific/press-releases/mastercard-and-bank-of-maldives-introduce-passport-card-in-partnership-with-maldives-immigration/

[95] Ryan Kline (01 February 2011). *Germany deploys contactless national ID.* SecureIDNews.com. Retrieved from: https://www.secureidnews.com/news-item/germany-deploys-contactless-national-id/

[96] Alan Goode (15 December 2016). *Biometric Trends for 2017.* Veridiumid.com. Retrieved from: https://www.veridiumid.com/blog/biometric-trends-for-2017/

[97] Tseng, K.-K., Huang, H.-N., Zeng, F., and Tu, S.-Y. (2015). *ECG Sensor Card with Evolving RBP Algorithms for Human Verification.* Sensors (Basel, Switzerland), 15(8), 20730–20751. Retrieved from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4570445/

4.3. Supporting Technologies for Cards

The supporting technologies for cards like the ones described in the previous sections could be augmented with other characteristics described in this section. These characteristics may increase the speed of reading physical cards, provide alternate means of reading the information contained on the cards, or make these cards more secure.

Supporting technologies for cards include bar codes, magnetic stripes, physical security features, and machine-readable text (see Figure 10.) Figure 11 shows the assessments for each of these.

Figure 10: Supporting Technologies for Cards

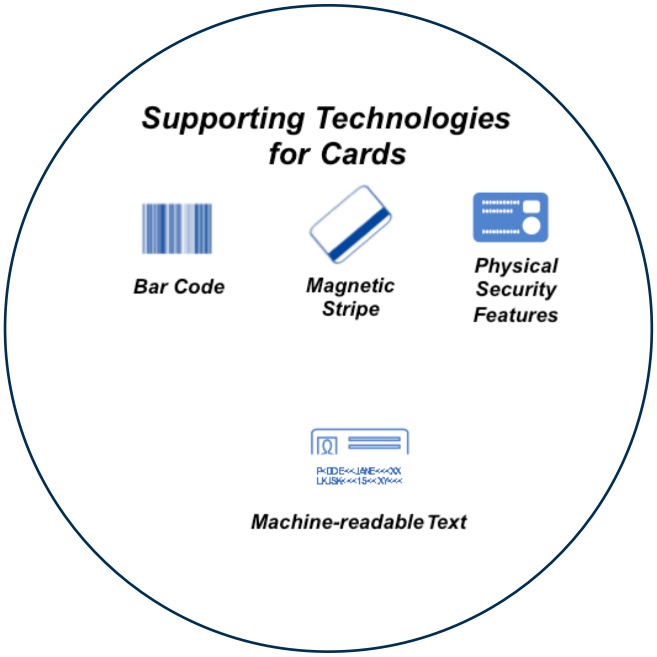
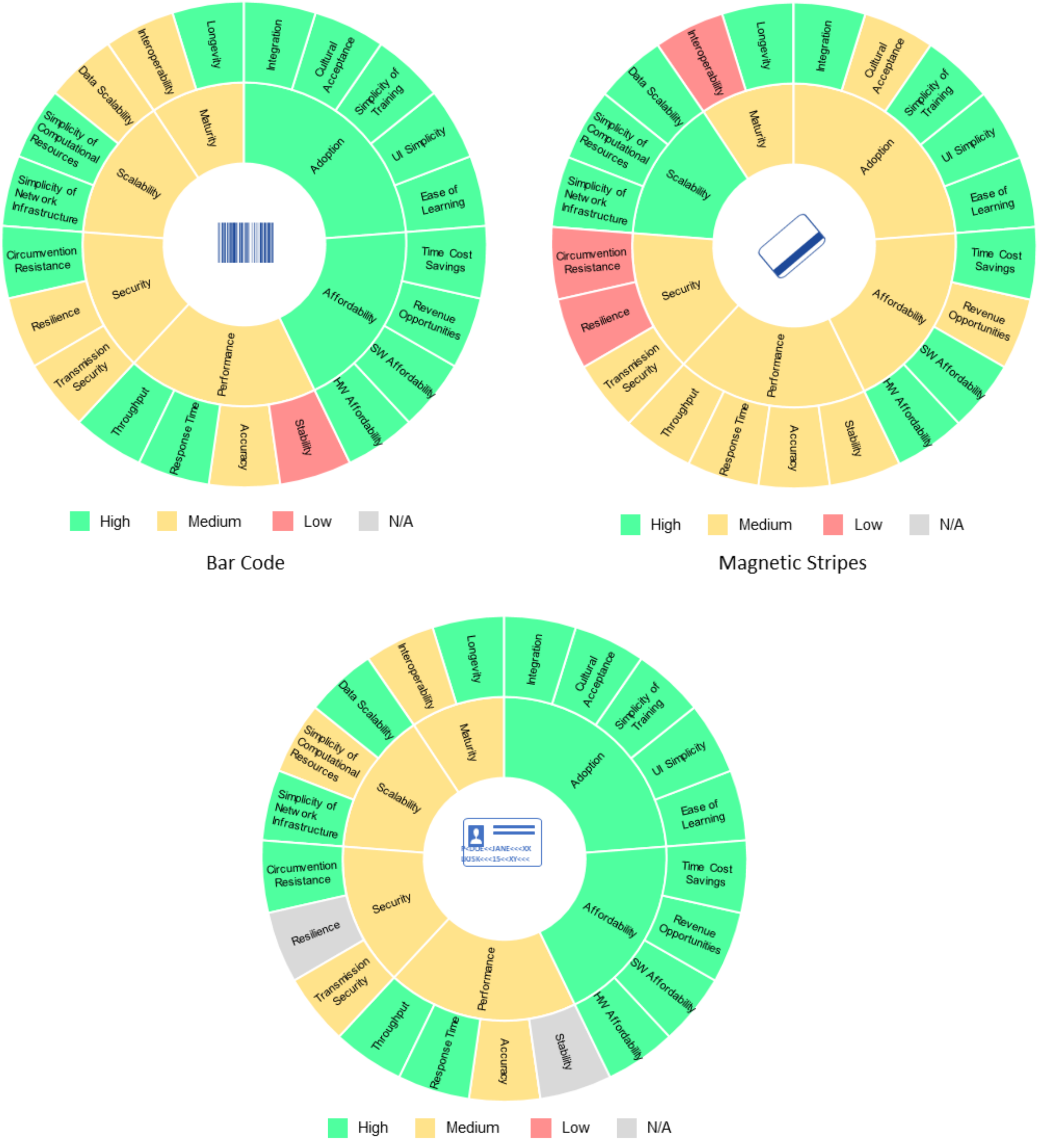


Figure 11: Supporting Technologies for Cards Assessment



Bar Code

Magnetic Stripes

Machine-readable Text

4.3.1. Bar Codes

Bar codes are machine-readable symbols used to encode information about a product. They comprise a pattern of lines with varying widths (1D bar codes) or rectangles, dots, hexagons, and other geometric patterns in two dimensions (2D bar codes). They are read by special optical scanners. People today can use their mobile devices to scan bar codes to find information of interest, such as features and prices of products they're considering buying. The technology is mature and widely used in national ID cards, including in Argentina, Costa Rica, and Bosnia and Herzegovina (to name a few).

Governments are starting to use bar codes that are generated automatically according to information entered by an individual, in the pre-enrollment phase of the Identity Lifecycle. Individuals fill out a form online, which generates a bar code capturing the information on the form.

Bar code-enabled voter cards containing biometric data were used in Egypt to authenticate individuals during the last elections. The biometric data can be stored on voter cards in the form of a 2D bar code or in an embedded chip. The voter card is scanned, and the voter's fingerprint or iris is captured and matched against the biometric reference data stored on the voter card or in a local database.[98] The data encoded in the 2D bar code on the card includes a cryptographic signature used to validate the bar code's integrity and authenticity.

What problems can it solve?

- **Performance.** Bar code technology has high throughput and accuracy compared to manual entry (with an error rate of just 1 in every 36 million characters scanned). It thus lends itself to high-volume data processing for identification applications.
- **Maturity.** Bar codes have been used for decades and have proven effective for line-of-sight, low-volume data capture.
- **Affordability.** Hardware and software costs for this technology are relatively low, making it worth considering for ID systems.
- **Adoption.** The technology is easy to integrate with existing systems.

What problems does it not solve?

- **Performance.** The bar code must be in the line of sight of the reading device. Bar code scanning accuracy can be compromised by factors like printing inconsistencies, wear and tear on the bar code, improper color contrasts between the light and dark elements of the bar code, and improper positioning of the bar code reader.
- **Scalability.** The amount of data that can be encoded into a bar code is limited even with high-density encoding schemes. For instance, QR encoding in byte mode is limited to 2,953 bytes.

4.3.2. Magnetic Stripes

A magnetic stripe, or Magstripe, consists of minute iron particles spread on a plastic-like film[99] and magnetized into a certain orientation. A magnetic scanner reads the stripe and translates the electronic impulses into data. The technology is very mature and has high market penetration. It is widely used in credit and debit cards and is used on some identity cards for various needs. In the United States, the

[98] *Data protection and confidentiality to ensure reliable processes in the organization of democratic elections.* Zetes. Retrieved from: http://peopleid.zetes.com/en/solution/elections

[99] *How does a magnetic stripe on the back of a credit card work?* (14 April 2008). HowStuffWorks.com. Retrieved from: http://money.howstuffworks.com/personal-finance/debt-management/magnetic-stripe-credit-card.htm

personal identity verification (PIV) card includes an optional ISO 7811-compliant magnetic stripe to encode a Federal Agency Smart Card Credential Number (FASC-N).[100]

What problems can it solve?

- **Adoption.** Magnetic-stripe technology is easy to use and requires little training.
- **Affordability.** The costs associated with magnetic-stripe cards and readers are lower than for smart cards and only slightly higher than for generic plastic cards. For example, it costs less than US$1 to produce one card.[101]

What problems does it not solve?

- **Security.** The data contained in the magnetic stripe can be read and cloned, however it is not a very pressing concern as in a national ID system, these magnetic stripes are used as an index to an ID in a central database. Therefore, just cloning the magnetic stripe alone will not serve any purpose to an attacker as the system will be able to identify an impersonator either based on corresponding fingerprint or photographic data.
- **Performance.** Magnetic stripes rely on contact technology, and both the reader and magnetic stripe are prone to degradation through wear and tear.

4.3.3. Machine-Readable Text

Machine-readable text technology uses algorithms to optimize and recognize characters within images and convert them into text that's readable by human beings. The technology has been widely adopted in a broad array of industries. All ICAO-compliant MRTDs include a machine-readable zone (MRZ) that can be read using OCR technology. In these MRTDs, the font (OCR-B), the ink color (B425 – B680 per ISO 1831) and other elements are specified to optimize OCR performance. However, these characteristics are not necessary to read information from identity documents using OCR technology.

What problems can it solve?

- **Performance.** Data entry of machine-readable text through OCR is faster, more accurate, and more efficient than keystroke data entry. With OCR, data can be read from paper documents with instantaneous character recognition rates in excess of 4,000 characters per second.[102]
- **Scalability.** Machine-readable text and OCR technology help government organizations scale their registration processes while maintaining reliability, accuracy, and speed. The technology can also accommodate a wide variety of input formats. In addition, it uses a modular architecture that's open and scalable.
- **Affordability.** OCR-equipped scanners can cost as little as US$150, versus several thousands of US dollars for high-capacity auto-feed units. Organizations using this technology can reduce their manual labor costs significantly by replacing manual entry and corrections.

[100] National Institute of Standards and Technology (August 2013). *Personal Identity Verification (PIV) of Federal Employees and Contractors. NIST.* Retrieved from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

[101] *DHgate.* Retrieved from: https://www.dhgate.com/wholesale/magnetic+stripe+card.html

[102] Herbert F. Schantz. *Optical Character Recognition—The Mature Technology with The Brilliant Future.* ECM Connection. Retrieved from: https://www.ecmconnection.com/doc/optical-character-recognition-the-mature-tech-0001

What problems does it not solve?

- **Performance.** OCR's speed and accuracy are lower for handwritten text than for typewritten text. Accuracy rates have been in the high 90th percentile. Other factors can erode accuracy, including image quality, font type and size, word spacing, and text-column width.
- **Scalability.** Machine-readable text requires ID cards to be in the line of sight of reader devices.

4.3.4. Physical Security Features

Physical credentials used for identification may incorporate optical and physical security features that make it difficult for forgers and impersonators to create unauthorized cards. Many countries use these security features in their digital identification cards as well as passports[103] to provide anti-forgery capabilities to these credentials. Optical and physical security features commonly in use today include the following:

- **Hologram.** A hologram is a three-dimensional appearing graphic created through laser technology that's placed anywhere on the card surface before lamination.[104] When true holograms are broken, each piece shows the entire original image, but from a different perspective each time the card is viewed from a different angle. Holograms are thus difficult to recreate.
- **Ghost images.** A ghost image is a semi-visible graphic (usually another photo of the cardholder) applied to the card. Holograms or logos with ghost images printed in combination with ID numbers are particularly difficult to fake.[105]
- **Microprinting.** Microprinting looks like an ordinary thin line to the naked eye. But it consists of tiny characters that are less than 0.3 mm in height—usually readable only with a magnifying glass or microscope.
- **Tactile.** An impression of a specific image is created on the card just before lamination.[106] Government agencies and organizations can create their own tactile features that go on each card they print. Some agencies view tactile elements as the safest and most cost-effective way to ensure card security. That's because the tactile image gets badly damaged if anyone tries to tamper with the card for the purposes of impersonation or faking. When tactile is combined with a holographic laminate, security improves even further.
- **Rainbow printing.** Rainbow printing is typically used to discourage counterfeiting. The technique involves printing gradients of multiple colors onto a material's surface through a highly sophisticated lithography process.[107] The combination of technical sophistication and hefty investment required to use this technique makes it very difficult to copy.

The effectiveness of optical and physical security features depends on the document inspector's skills. Even people who have a solid understanding of security features may fail to detect fake cards; for example, if they take insufficient time to inspect a card. Where enhanced security features are required, the electronic security features of smart cards can be implemented. In the context of identity systems, ICAO Document 9303 defines many electronic security options available to protect data and data interchanges.

The choice of security features also affects the material used to produce identification cards—and thus the manufacturing process and costs. For instance, though materials like PVC are inexpensive, features like

[103] Bundesdruckerei GmbH (January 2014). *Security Features of the German Identity Card.* Retrieved from: https://www.bundesdruckerei.de/de/system/files/dokumente/pdf/Flyer-Security-Features-German-ID-Card.pdf.pdf

[104] Woodford, C. (2008/2017). *Holograms*. Retrieved from: http://www.explainthatstuff.com/holograms.html

[105] Chen, W. and Chen, X. (November 2013). *Ghost Imaging for Three-Dimensional Optical Security.* Applied Physics Letters, 103(22), pp. 221106–2211064. Retrieved from: http://aip.scitation.org/doi/full/10.1063/1.4836995

[106] Myers, W. (25 October 2016). *Tactile Impressions for Secure ID Cards: Security & Brand Impact You Can See & Feel.* Raco Industries. Retrieved from: https://racoindustries.com/tactile-impressions-secure-id-cards-security-brand-impact-can-see-feel/

[107] *Counterfeit Detection: A Guide to Spotting Counterfeit Currency—Intaglio.* Indigo Image. Retrieved from: https://www.indigoimage.com/count/feat2.html#intdetail

laser engraving or embossing don't work well with that material. And as more features are added to a card, more expensive underlying materials are required to print the cards—raising production costs.[108]

4.3.5. Key Trends in Card Technologies

As scanner technology continues to evolve, there will be less need and demand for 1D bar codes as they can hold only limited information, a maximum of 85 characters. In contrast, 2D bar codes can store over 7,000 characters, allowing for the transmission of over a page of text.[109] 2D bar codes can encode up to 500 bytes per square inch, making it possible to store biometric data such as fingerprint and signature capture, or compressed versions of cardholder portraits. This feature is not possible with 1D linear bar codes.

Research is under way to add more dimensions to 2D bar codes to encode more data into them. 3D bar codes have been created by using space (protrusive bars/squares)[110] and color (color-coded bars/squares).[111] Protrusive 3D bar codes are likely to be highly resistant to alterations, and will require specialized readers as they will be engraved directly on a product's surface. There is further research into creating 4D bar codes using height, width, color, and time as four dimensions to encode data. These 4D bar codes will use time-multiplexed colored 2D bar codes to transmit large amounts of data. However, these can only be displayed on mobile or spatial devices.[112]

There has been some research into multi-function card technology that allows a single card to be used for banking ATM withdrawals, credit card purchases, or as a loyalty card by simply pressing a button to reprogram how it functions. There is little evidence of testing of this technology in the context of digital identification, but multi-function cards using magnetic stripes could allow a single ID card to serve multiple functions if implemented. Some of the latest cards also have a global system for mobile (GSM) cellular antenna inside that can connect to a mobile network. These cards can be instantly programmed with the required details using the card's cellular connection. If the cardholder's information is compromised, instead of having to wait for a replacement card, these cards could be electronically programmed with new information so that the user could continue to use it almost instantly.[113]

Cards with improved security features make it very difficult for traditional frauds like card skimming (the illegal copying of information from the card, in the magnetic strip or chip.) Some interactive cards do not hold information while it is switched off and is considered safe from skimming and could prevent identity theft.[114] To turn the device ON, a user must enter an unlocking code into the card. If the user enters in the correct unlocking code, the card will then visually display the user's card number and the stripe is then populated with the correct magnetic information. After a period of time, the display turns off and the stripe erases itself, thus removing all critical information from the surface of the card.[115]

[108] Martin, Z. (11 August 2015). *Advanced card materials enable layered security features.* SecureID News. Retrieved from: https://www.secureidnews.com/news-item/advanced-card-materials-enable-layered-security-features/

[109] Brian Sutter (26 May 2015). *Future of Barcodes, RFID, and Image Barcodes; How They Will Impact IOT Wasp Barcode.* Retrieved from: http://www.waspbarcode.com/buzz/future-barcodes/

[110] Gladstein, D., Kakarala, R., and Baharav, Z. *3D Barcodes: Theoretical Aspects and Practical Implementation.* SPIE Digital Libary. Retrieved from: http://www.spiedigitallibrary.org/conference-proceedings-of-spie/9405/1/3D-barcodes-theoretical-aspects-and-practical-implementation/10.1117/12.2082864.short?SSO=1

[111] Koddenbrock et al. (2016). *An innovative 3D color barcode: Intuitive and realistic visualization of digital data.* Proceedings of the 17th International Conference on Computer Systems and Technologies 2016 pp. 175–181. Retrieved from: https://dl.acm.org/citation.cfm?id=2983486&dl=ACM&coll=DL

[112] Langlotz, T. and Bimber, O. *Unsynchronized 4D Barcodes.* ISVC'07 Proceedings of the 3rd international conference on Advances in visual computing—Volume Part I pp. 363–374. Retrieved from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.9056&rep=rep1&type=pdf

[113] Andrew Liszewski (11 January 2018). *This Cellular-Connected Smart Credit Card Can Show You. How Much Money You've Got Left to Spend.* Gizmodo. Retrieved from: https://gizmodo.com/this-cellular-connected-smart-credit-card-can-show-you-1821972060

[114] Vishal Chawla (18 January 2018). *Payment Cards Are Evolving into Mini Computers.* Computer World. Retrieved from: http://www.computerworld.in/feature/how-payment-cards-are-evolving-mini-computers

[115] Michael Kassner (20 September 2010). *Debit/credit card fraud: Can smart payment cards prevent it?* Tech Republic. Retrieved from: https://www.techrepublic.com/blog/it-security/debit-credit-card-fraud-can-smart-payment-cards-prevent-it/

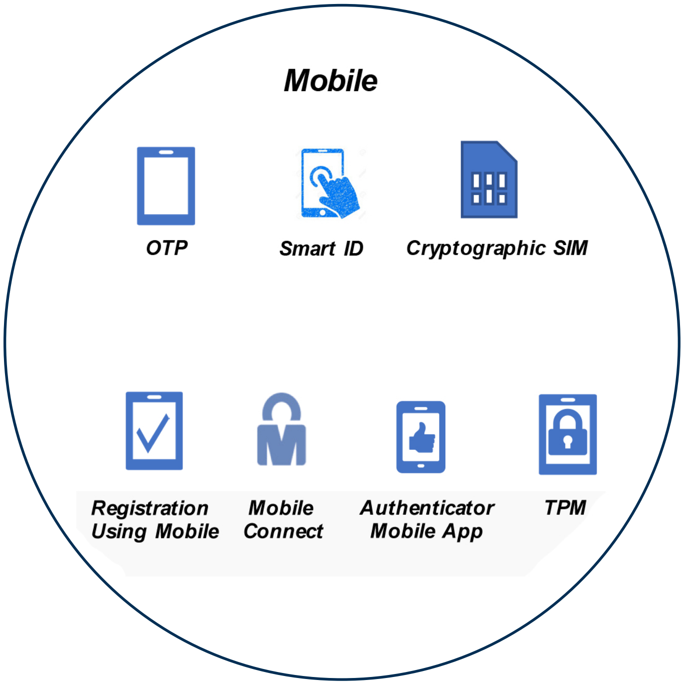
4.4. Mobile

Mobile technologies related to identity consist of phone- and tablet-based hardware and software solutions used to register, authenticate, and verify an individual's identity.

The rapid proliferation of smart mobile devices, fast improving wireless network capabilities, and adoption of cloud technologies has resulted in easy-to-provide and easy-to-use mobile identity solutions. With falling prices of smartphones, more and more people in developing countries are beginning to access the Internet. In India, for example, the number of Internet users is expected to reach 450–465 MN by June 2017.[116] Also, Indians accessed the Internet through their mobiles nearly 80% of the time in 2017,[117] which implies that access to digital services online will most often be through the use of a mobile phone. Clearly, mobile identification and authentication technologies will be important particularly in developing countries.

Mobile technologies take numerous forms, and this report focuses on the forms shown in Figure 12.

Figure 12: Mobile Sub-Technologies



[116] Chopra, A. (02 March 2017). *Number of Internet users in India could cross 450 million by June: Report.* LiveMint. Retrieved from: http://www.livemint.com/Industry/QWzIOYEsfQJknXhC3HiuVI/Number-of-Internet-users-in-India-could-cross-450-million-by.html

[117] Bhattacharya, A. (29 March 2017). *Internet use in India proves desktops are only for Westerners.* Quartz. Retrieved from: https://qz.com/945127/internet-use-in-india-proves-desktops-are-only-for-westerners/

Bridging credential domains from physical to mobile is the derived credential, which is a means to implement a credential on a mobile device where the same authenticator assurance levels (AALs) would apply. For example, *NIST's Guidelines for Derived PIV Credentials*[118] notes that "In response to the growing use of mobile devices within the federal government, FIPS 201 was revised to permit the issuance of an additional credential, a Derived PIV Credential, for which the corresponding private key is stored in a cryptographic module with an alternative form factor to the PIV Card."

The underlying credential technology, derived or not, is defined by the AAL required by the relying party, as described in *NIST's Digital Identity Guidelines.*[119] The three AALs define the subsets of options agencies can select based on their risk profile and the potential harm caused by an attacker taking control of an authenticator and accessing agencies' systems. The AALs are as follows:

AAL1 provides some assurance that the claimant controls an authenticator bound to the subscriber's account. AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.

AAL2 provides high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.

AAL3 provides very high confidence that the claimant controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication uses a hardware-based cryptographic authenticator and an authenticator that provides verifier impersonation resistance. The same device may fulfill both these requirements. To authenticate at AAL3, claimants prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.

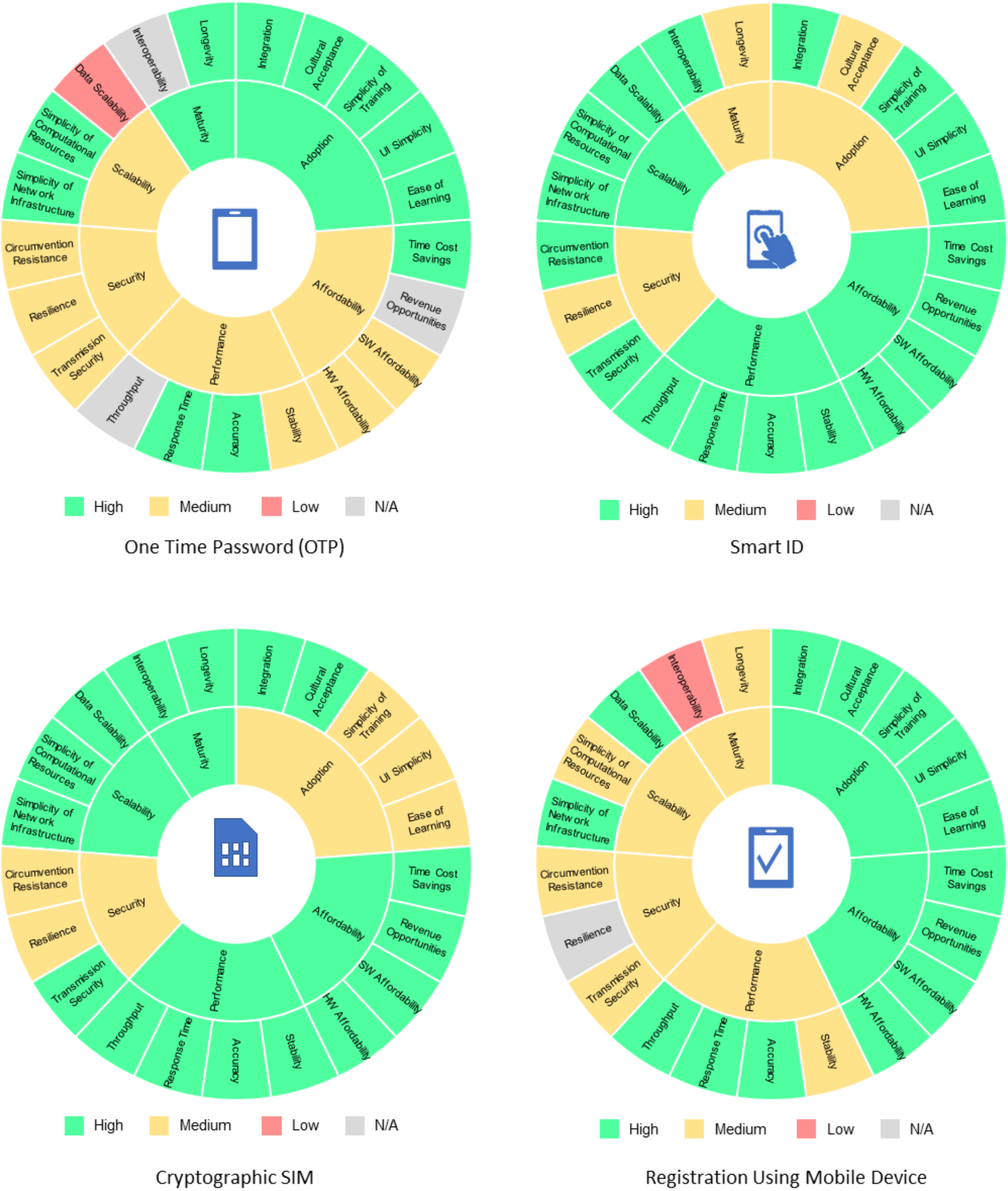
To meet AAL2 or AAL3, a mobile-device-based derived credential would have to support approved cryptographic techniques. Fast identity online (FIDO) Universal Authenticator Framework (UAF)-compliant mobile devices (and corresponding host system(s)) are AAL3 compliant, for example.

The following sections take a closer look at the different categories of mobile solutions, and the assessments of these technologies are shown in Figure 13.

[118] Ferraiolo, et al. (December 2014). *Guidelines for Derived Personal Identity Verification (PIV) Credentials.* National Institute of Standards and Technology. Retrieved from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf

[119] Grassi, P.A., Garcia, M.E., and Fenton, J.L. (June 2017). *Digital Identity Guidelines. National Institute of Standards and Technology.* Retrieved from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Figure 13: Mobile Technologies Assessment

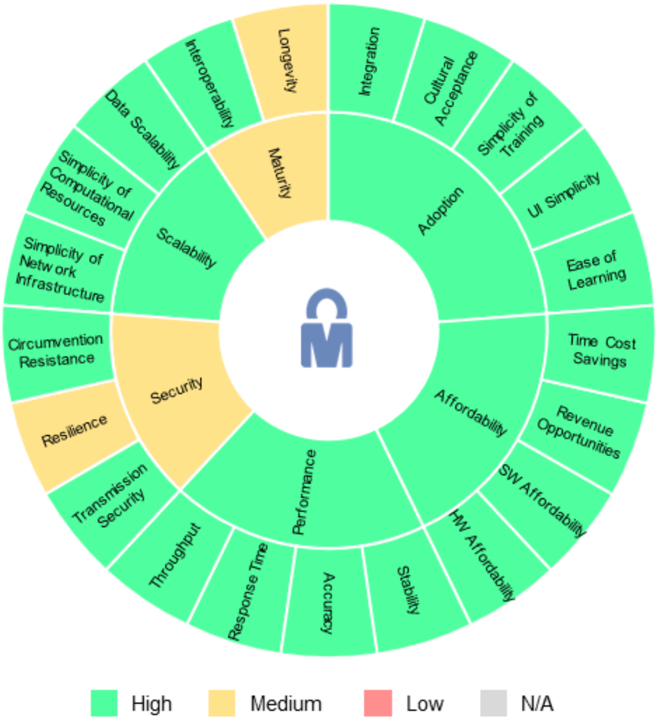


One Time Password (OTP)

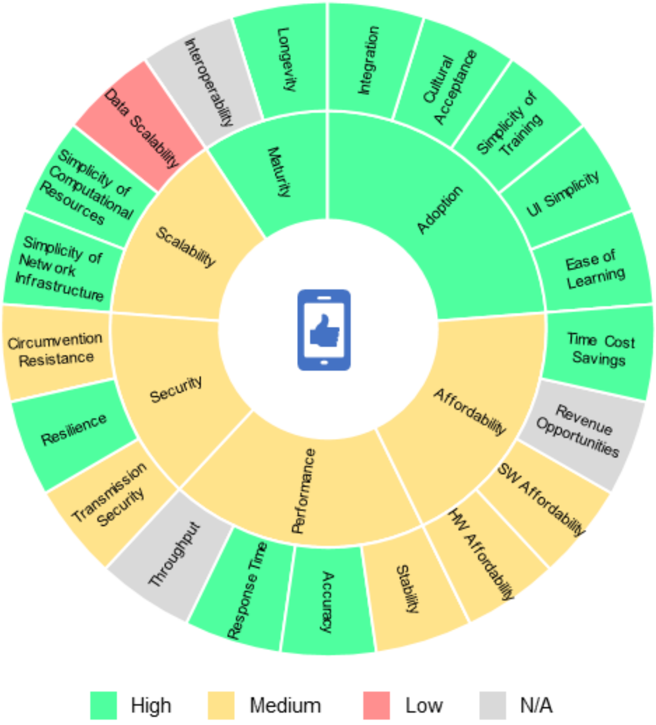
Smart ID

Cryptographic SIM

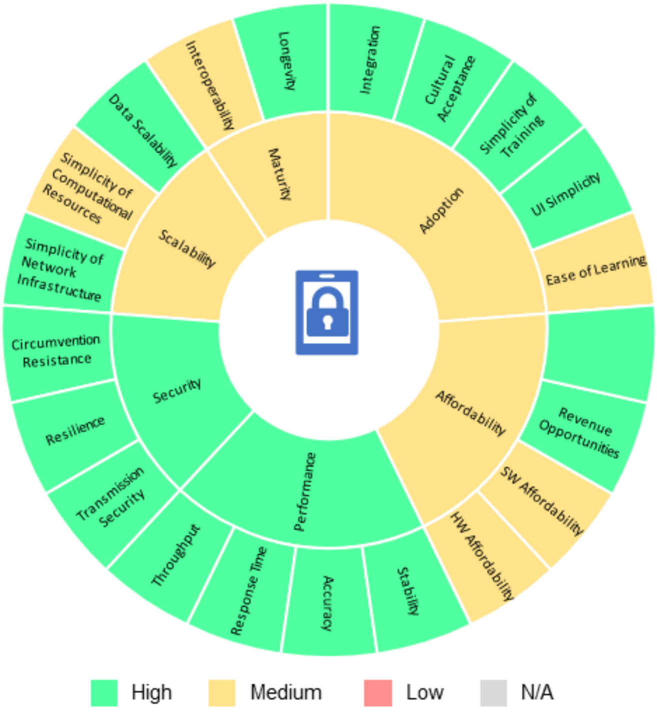
Registration Using Mobile Device



Mobile Connect



Authenticator Mobile App



TPM

4.4.1. One-Time Password (OTP)

One-time password (OTP), or dynamic password technology, is used to authenticate a user for one session only. Every time an individual successfully validates himself or herself or when the countdown timer stops, the password expires. OTP is known for being easy to use. Authentication using OTPs requires access to something a person has (in this case, access to a mobile phone or e-mail address) as well as something a person knows (such as a PIN).[120]

OTP technology is compatible with multiple devices, including computers, mobile phones, and smart tokens. It can be implemented through software tokens like mobile-based short message service (SMS) or PC-based software. OTP technology can also be implemented through use of handheld token devices or smart cards synced with a central authenticating agency. NIST has recently qualified the use of SMS for out-of-band verification. As NIST explains, "The out-of-band device SHOULD be uniquely addressable and communication over the secondary channel SHALL be encrypted unless sent via the public switched telephone network (PSTN). Methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or e-mail, SHALL NOT be used for out-of-band authentication."[121]

OTP technology has been used in multiple applications, including emergency services (when it's necessary to contact a large database of people), secured services (such as financial transactions), the retail industry, and delivery of government services. The technology can be used as a stand-alone authentication mechanism as well as in multi-factor authentication. In a stand-alone or single-factor login, the user keys in only an OTP for validation. For multi-factor authentication, an OTP is combined with other validation methods, such as use of a PIN, biometric data, or contextual network data known by the mobile network. This is much more secure than single-factor authentication.

What problems can it solve?

- **Scalability.** OTP technology's computational and network requirements are minimal, enabling scalability to large populations.
- **Adoption.** It's easy to learn how to use OTP; the user interface shows a simple display of a six-digit token, or the user receives an SMS containing the OTP, which must be entered in the appropriate field for validation. All of this fosters ready adoption of the technology.
- **Maturity.** OTP technology has been in use for over a decade and has been widely accepted. One recent example of use of OTP in a digital ID system is the linking of individuals' mobile SIM cards in India with their Aadhaar number through the use of an OTP.[122]

What problems does it not solve?

- **Security.** The technology requires the sharing of secrets, providing multiple points of attack. Refer to the NIST's update relating to the deprecation of sharing OTPs via SMS.

What problems could it create?

- **Security.** If an active OTP is accessed by a fraudster by cloning a SIM card, identity theft could occur.

[120] Thomas A. Fine. *One-Time Passwords—Roadmap.* Retrieved from: https://hea-www.harvard.edu/~fine/Tech/otp.html

[121] Multiple Authors. *Digital Identity Guidelines Authentication and Lifecycle Management NIST.* Retrieved from: https://pages.nist.gov/800-63-3/sp800-63b.html

[122] Timesofindia.com (04 January 2018). *Link Aadhaar to Existing SIM Cards using OTP.* Times of India. Retrieved from: https://timesofindia.indiatimes.com/business/faqs/aadhar-faqs/otp-based-aadhaar-verification-for-existing-sim-cards/articleshow/62350208.cms

4.4.2. Smart ID

Smart ID is an electronic identification app available on tablets and smartphones. It enables authentication of users seeking to access online services. The solution works across devices, but users must register each device individually for the authentication to work. They can register in the app by using their digital ID cards and valid certificates. Once they've registered, they can use Smart ID to digitally authenticate themselves on various devices.[123]

As a security measure, the first time the PIN is entered incorrectly three times, the user's account is blocked for three hours. After three further wrong attempts, the account is locked for 24 hours. A further attempt to use the incorrect PIN three times, blocks the account permanently.[124]

The technology is being used in a number of countries. For example, in the Baltics, there are more than 300,000 users.[125] All of SEB Bank's customers can use Smart ID for online banking. To apply for a Smart ID, customers visit their local SEB branch, where bank officials establish their identity and guide them through the process of creating their Smart ID account.

Swedbank is another case in point. The bank has introduced online services authenticated via Smart ID for their Latvian and Lithuanian branches.[126] Customers can download and register on the Smart ID app and perform banking transactions by authenticating themselves through their Smart ID PINs. Eesti Gaas, a natural gas company in Estonia, has extended Smart ID services to its customers to enable them to access their accounts online.[127] Indeed, Estonia was the first country to implement Smart ID solutions for initiatives including i-Voting, e-taxation, and e-residency,[128] with the first e-services using Smart ID going online in February 2017. These Smart IDs are expected to replace the chip-based ID cards that Estonians currently use for conducting online transactions. In March 2017, Latvian and Lithuanian e-services started providing access to customers with Smart ID.

What problems can it solve?

- **Security.** Users' electronic identity based on Smart ID is independent of the SIM cards in their mobile device. Once they register with Smart ID, individuals only need an active Internet connection to authenticate themselves on the partnered online services. In addition, data are secure because the Smart ID app uses just the two PINs to validate users for services; it doesn't store any user passwords.
- **Adoption.** Customers can readily understand Smart ID without extensive training. What's more, this technology is not dependent on a SIM card and can be used around the world.
- **Affordability.** As the number of Smart ID transactions soars, the prices per transaction are plummeting for e-service providers. In addition, the app is free for end users.[129]
- **Performance.** The solution boasts excellent processing speed, limited only by the end user's Internet speed, and secure transactions. Smart ID also meets the EU's eIDAS requirements and the European Central Bank's requirements as a strong authenticator tool.

[123] *Smart-ID—The smart way to identify yourself.* Smart-ID.com. Retrieved from: https://www.smart-id.com/about-smart-id/

[124] *Using Smart-ID Is Secure and Safe.* Smart-ID.com. Retrieved from: https://www.smart-id.com/security/

[125] Lukin, L. (28 June 2017). *Smart-ID is used by 300,000 people in the Baltics.* SK ID Solutions AS. Retrieved from: https://sk.ee/en/News/smart-id-is-used-by-300-000-people-in-the-baltics

[126] *Introducing Smart-ID.* Swedbank. Retrieved from: https://www.swedbank.lv/private/campaign/smart-id

[127] *Eesti Gaas Is the First Energy Company to Take to Use Smart-ID.* (25 May 2017). Eesti Gaas Retrieved from: http://www.gaas.ee/en/eesti-gaas-is-the-first-energy-company-to-take-to-use-smart-id/

[128] *e-Estonia at the Mobile World Congress 2016.* (15 February 2016). SK ID Solutions AS. Retrieved from: https://www.sk.ee/en/News/e-estonia-at-the-mobile-world-congress-2016

[129] *Price List of Smart-ID Service.* SK ID Solutions AS. Retrieved from: https://sk.ee/en/services/pricelist/smart-id/

- **Scalability.** The solution can be scaled easily across services in industries ranging from banking to energy and more. Once a customer registers, he or she can use that same registration to access services in multiple industries.

What problems does it not solve?

- **Maturity.** The solution was developed by a private player, has limited geographic reach, and has not yet moved to major markets. It is currently limited to Estonia, Latvia, and Lithuania.
- **Scalability.** The solution needs a reliable connectivity to a stable network to seamlessly perform the validation process.

What problems could it create?

- **Security.** Although the solution blocks a user's account when incorrect PINs are entered, it's still vulnerable to security breaches. Anyone who gets hold of a user's PINs can then access his or her accounts.

4.4.3. Cryptographic SIM

SIM cards use cryptographic algorithms that turn the card into a user identification tool. For example, the A3 (authentication) and A8 (cipher key generation) algorithms are written into the SIM card during the production process and are secured from reading in normal circumstances. The PUK (personal unlocking key) code is held by the operator, and the user can access it by submitting a request to the operator.[130] The cipher key is derived from the subscriber authentication key using encryption.

Such algorithms enable secure communication between the user and the network without exposing information about subscribers or the network that someone could use to gain illegal access to services that subscribers are using.[131]

During authentication, the Authentication Center generates a random number that is sent to the mobile number. This random number is then used in conjunction with the user's encryption key and the A3 algorithm to generate a number that is then sent back to the Authentication Center. If the number sent by the user's mobile matches the number generated by the Authentication Center, the user is verified.[132]

Countries that have adopted cryptographic SIM cards include Estonia, Moldova, and Finland.[133,134] Norwegian mobile operators offer their subscribers secure mobile authentication through a local BankID solution to provide secure online user identification and user digital signature verification.

What problems can it solve?

- **Security.** Cryptographic SIM cards provide secure, reliable identification for subscribers to access online services.

[130] He, S. *SIM Card Security*. Ruhr-University Bochum. Retrieved from: https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/slides_sim_card_security.pdf

[131] Jansen, W.A. and Delaitre, A. (2007). *Reference Material for Assessing Forensic SIM Tools.* 41st Annual IEEE International Carnahan Conference on Security Technology, Ottawa, Ont., pp. 227–234. Retrieved from: https://csrc.nist.gov/csrc/media/projects/mobile-security-and-forensics/documents/mobile_forensics/reference%20mat-final-a.pdf

[132] *SIM Cards.* Gemalto. Retrieved from: https://www.gemalto.com/companyinfo/digital-security/techno/sim

[133] World Bank (2016). *Digital Identity: Towards shared principles for public and private sector cooperation (English).* World Bank Group. Retrieved from: http://documents.worldbank.org/curated/en/600821469220400272/Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation

[134] *When eID becomes Mobile for a whole nation.* Gemalto. Retrieved from: https://www.gemalto.com/brochures-site/download-site/Documents/gov_cs_finland_valimo.pdf

- **Affordability.** Mobile network operators charge end users a per-use fee when they use a digital signature to authenticate themselves for e-Gov and other online services. But the cost is not very steep, as it is also shared with the service providers.
- **Performance.** The solution lets users quickly access online services without having to set up and remember complicated usernames and passwords. Users can log in using a PIN, and because the solution depends only on network connectivity for authentication, it is highly reliable.
- **Scalability.** The solution can authenticate users across multiple online services, needing only authentication by the mobile operator.

What problems does it not solve?

- **Adoption.** Though more and more people have access to mobile connectivity, cryptographic SIM technology hasn't yet been implemented extensively across countries. As more services move online and the need for online user verification increases, this could change.

What problems could it create?

- **Security.** Hackers can trick a mobile user into installing malicious software that gives them complete control of the user's phone, letting them eavesdrop and commit other malicious acts.

4.4.4. Registration Using Mobile Devices

Mobile registration technologies comprise hardware and software solutions that enable enrollment of individuals into an ID system. For example, existing features of smartphones or specialized mobile devices are used by government authorities or by individuals to capture biometric data and photos. The ability to collect biographic data (such as breeder documents) and biometric information (including fingerprints, iris images, and photos) for digital ID registration via mobile technology has recently improved. For example, smartphones can be outfitted with capture devices directly or via Universal Serial Bus (USB), Bluetooth (and Bluetooth Low Energy—BLE) and NFC. These purpose built devices can offer better capture capabilities in terms of ease of use, throughput, and image quality, compared to sensors embedded in a smartphone. It is therefore not uncommon for public officials to use a mobile device to capture data from citizens to facilitate enrollment in a centralized identification system.

Mobile operators have been involved in birth registration systems in several countries, playing a vital role in registering the population into a government identity system. In Tanzania, for instance, the government's Registration and Insolvency Agency (RITA), in partnership with UNICEF and mobile operator Tigo, has developed an Android-based application that lets registrars in local health clinics and government offices collect birth registration data and upload it to a centralized system.[135,136] To date, more than 1.6 MN children have been registered and issued a birth certificate under this initiative. The overall level of registration and certification has jumped from 10% to 79% across the seven regions where this initiative was implemented.[137]

In Pakistan, UNICEF and mobile operator Telenor developed a mobile application that digitizes the birth registration form and provides SIM cards with data connectivity and wi-fi access. Public officials received mobile devices or tablet computers to carry out the registration process. This program resulted in a 300%

[135] Tigo. *Mobile Birth Registration.* Tigo Tanzania. Retrieved from: https://www.tigo.co.tz/mobile-birth-registration

[136] UNICEF Tanzania (24 November 2015). *TIGO teams up with UNICEF, champions innovations for Tanzania's children.* UNICEF. Retrieved from: https://www.unicef.org/tanzania/media_17334.html

[137] SME Input from Marta Ienco—Head of Government and Regulatory Affairs, GSMA Identity Programme at GSMA.

and 126% increase in registration rates of newborns, respectively, in Pakistan's provinces of Punjab and Sindh. The project has resulted in an estimated 705,000 registrations after being scaled to 108 locations.[138]

With fingerprint and iris scanners almost commonplace in smartphones, more users (particularly in developed markets where smartphone adoption is high) are self-registering their biometric data on these devices. The private sector is creating apps that then use the biometric data to authenticate the individual for a transaction, such as the purchase of a product or access to a service. Some companies are working on developing software-only solutions that allow any mobile with a common camera paired with AI and deep-learning algorithms to capture a user's biometrics such as palm, feet, and ear morphology to perform mobile registration.[139]

What problems can it solve?

- **Affordability.** Smartphones with built-in biometric sensors are becoming less expensive, with global smartphone prices decreasing by 27% from 2010 to 2017.[140] Specialized hardware attachments to add biometric capture capability to ordinary phones are affordable too, and can be set up quickly.
- **Adoption.** More than 1 billion (BN) biometric smartphones are in use today, and individuals can quickly use this technology with minimal training and investment. External fingerprint scanners cost around 20% of standard medium-range smartphones, and can be paired with multiple smartphones by installing free mobile applications. The onetime setup process is easy as well.
- **Scalability.** Fingerprint and iris scanners are becoming commonplace on mobile phones, making mobile registration scalable. However, the integrated biometric sensor on mobiles cannot be used to register and authenticate users for large-scale identification programs because the biometrics cannot be stored or transferred to a cloud or database. Instead, the biometrics are saved on a secure enclave on the phone that is separate from the rest of the phone's operating system. Large-scale enrollment and authentication requires stand-alone biometric scanners.
- **Performance.** Because smart devices collect the data, the registration process is quick and accurate. And because the solution depends only on network connectivity for authentication, it's typically reliable. Also, certain mobile solutions can conduct offline authentication without the need to connect to a mobile network. These enrollments can be supervised if necessary (for example, through a bank's agent network).[141]

What problems does it not solve?

- **Security.** If mobile data registration is unsupervised, establishing trust in the data is difficult.
- **Maturity.** Mobile registration solutions offered by different vendors use different data exchange standards, discouraging interoperability.

What problems could it create?

- **Performance.** With rapid technology advancements, existing mobile devices could become incompatible or obsolete. For example, new smartphones are moving to USB-C standards, rendering many of today's biometric devices out of date.

[138] GSMA. *Innovations in Mobile Birth Registration: Insights from Tigo Tanzania and Telenor Pakistan.* GSMA. Retrieved from: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/01/Innovations-in-Mobile-Birth-Registration_Insights-from-Tigo-Tanzania-and-Telenor-Pakistan.pdf

[139] SME Input from Rebecca Distler—Director, Global Health Initiatives—Element Inc.

[140] *Statista Global average selling price of smartphones from 2010 to 2019 (in U.S. dollars).* Retrieved from: https://www.statista.com/statistics/484583/global-average-selling-price-smartphones/

[141] SME Input from Rebecca Distler—Director, Global Health Initiatives—Element Inc.

- **Adoption.** In more than 145 countries, SIM procurement requires users to present a recognized identity credential.[142] Therefore, using mobile-based identification and authentication solutions will prove very difficult for individuals who don't have any other officially recognized forms of identification.
- **Security.** Malicious apps can retrieve biometric data from a mobile device or passively capture biometric data and personal information—raising concerns about security.

4.4.5. Mobile Connect

GSMA Mobile Connect is a portfolio of mobile-based secure identity services driven by mobile network operators globally. It is a multipurpose identity solution that uses the inherent trust, security, and ubiquity of mobile networks. Mobile network operators give users control over their own data and enable end users, businesses, and governments to interact and access online services in a convenient, private, and trusted environment.

By using an individual's mobile phone number as the identifier and the mobile phone as the authentication device, Mobile Connect supports a wide range of practical applications—including registration and login to websites and apps and authorization of transactions online. Mobile Connect is delivered as a federated identity framework through participating mobile operators. Developers can access the ecosystem of operators who've partnered with GSMA for Mobile Connect and their user base,[143] including a separate developer portal and test suite.[144] In 2015, GSMA's Mobile Connect became the first private-sector cross-border public-service authentication solution compatible with eIDAS, and since then, the number of mobile operators testing Mobile Connect against eIDAS keeps increasing.[145]

One of Mobile Connect's popular services, Authenticate/Plus allows a user's mobile number to act as a unique digital identifier leveraging the trusted relationship with the mobile operator. This enables users to easily login without the need for usernames and passwords to any participating online service, just by using the mobile phone number as a means of authentication. Authentication is managed by the existing mobile network operator, and no personal data are shared with the website without the user's consent.[146]

Once registered, users can log into online services whenever the Mobile Connect logo appears, by simply clicking the logo or entering a secure PIN (for services requiring greater security). In using this technology for applications that require a high level of assurance (LOA), it is important to conduct identity proofing and a strong know your customer (KYC) process during mobile number registration with the service provider.

Mobile penetration has been increasing over the years, and the Mobile Connect solution provides a fast, reliable, secure, and efficient method to provide users with digital identities. As many as 62 mobile network operators in 30 countries have launched Mobile Connect. Most operators have launched Mobile Connect Authenticate, which enables a secure, password-less log-in service on a global scale. Some others are also supporting more than one Mobile Connect service (such as Mobile Connect phone number or Mobile Connect KYC match).

[142] GSMA (April 2006). *Mandatory registration of prepaid SIM cards.* GSMA. Retrieved from: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

[143] *Introducing Mobile Connect—the new standard in digital authentication.* GSMA. Retrieved from: https://www.gsma.com/identity/mobile-connect

[144] *Mobile Connect Developer Portal*. Developers. Retrieved from: https://developer.mobileconnect.io/faq

[145] Marta Ienco (06 July 2017). *Mobile Connect-eIDAS Pilot Prepares for Secure Cross-Border Trade.* GSMA. Retrieved from: https://www.gsma.com/identity/eidas-pilot-prepares-secure-cross-border-trade

[146] *Introducing Mobile Connect—the new standard in digital authentication.* GSMA. Retrieved from: https://www.gsma.com/identity/mobile-connect

Mobile Connect user authentication is available with telecom operators around the globe including Airtel, Idea, and Vodafone in India; Orange Telecom in Morocco and Egypt; and Turkcell in Turkey.[147] Mobile Connect uses the principle of a "pluggable authenticator," where the mobile authentication mechanism (authenticator) can be plugged in based on the mobile operator's choice. Some of the popular authenticators used in Mobile Connect around the world are Authenticator Mobile Apps, the SIM Applet, SMS+URL, USSD, network-based seamless authenticator, and trusted platform module (TPM).[148] Some of these technologies are discussed in detail in the following sections.

What problems can it solve?

- **Security.** Once users are registered to Mobile Connect, they do not need any username or password to log into websites. A simple swipe on a notification or a PIN is all that is needed to log in. Mobile Connect authenticates the user via the mobile operator, and the website receives only confirmation of user identity. Because no user data are shared with the website without the user's consent, the user's data are safe. Mobile Connect is also secure by design in that a mobile network can disable a device's SIM card over-the-air and flag the device as lost or stolen in a global database if a user reports either situation.[149]
- **Adoption.** Adoption is easy because many mobile network operators, particularly in developing countries, have already signed up for the services. The solution is also easy for individuals to understand and use.
- **Affordability.** The solution is highly affordable, with initial monetary investment required from the online services willing to provide Mobile Connect as a log-in option.
- **Scalability.** Once operators make the service available, developers can build apps for the online services to allow the user log-in option using Mobile Connect. Once this option is available, the solution can then be made available across the user base without any further scalability issues.

What problems does it not solve?

- **Performance.** Mobile Connect relies on mobile operators to validate users' authenticity. This might limit the solution's performance at locations where operators do not have proper coverage.
- **Scalability.** Network scalability is low, as the solution depends on connectivity with a stable network operator for user authentication. If a user's location does not have a stable network connection, as may be common in developing countries, the solution will be unavailable.

What problems could it create?

- **Adoption.** The solution is very operator dependent and first needs registration with a mobile device. Moreover, only some mobile operators have signed up for Mobile Connect. So, particularly in developing countries where mobile connectivity is not substantial, registering numerous users can be challenging. In addition, any time a user switches to a different mobile network operator, he or she must repeat the registration process.

[147] *Secure digital identity is now in your hands.* Mobile Connect. Retrieved from: https://mobileconnect.io/

[148] SME Input from Gautam Hazari—Technical Director—Personal Data at GSMA.

[149] GSMA (September 2016). *Mobile Connect: Mobile high-security authentication.* Retrieved from: https://www.gsma.com/identity/wp-content/uploads/2016/10/MC_high-security-authentication_Sep-16.pdf

4.4.6. Authenticator Mobile App

While a simple OTP technology alleviates security concerns with a static password, it does not completely eliminate the risk of circumvention. Two approaches have been widely accepted by the industry today to make OTP technology more secure, both of which use pseudorandom algorithms:

HMAC-based OTP. Hash message authentication code (HMAC) OTP (or HOTP) relies on a secret key and a counter. This approach is commonly used with token-based authentication. Every time the user tries to authenticate or increments the counter on the token by pushing a button on a hardware token or refreshing (in case of a software token), the generator creates a new OTP. These OTPs do not have a time-bound expiry.

Time-based OTP. Time-based one-time password (TOTP) is a temporary passcode, generated depending on the time of the day. Unlike with HOTP, there is no counter. The time must be synchronized on the user's end and the resource's end. The time stamps are usually synchronized using a network time protocol (NTP). The time stamps could be incremented every 30 seconds or 1 minute, so when a user wants to log in, he or she would put in his or her username, password, and the latest TOTP code.

Mobile authenticator apps like Authy and Google Authenticator are TOTP enabling two-factor authentication. This approach is gradually seeing increased adoption and is much more secure compared to traditional SMS-based OTP or even HOTP. Google Authenticator has added support for multiple apps like LastPass, WordPress, Facebook, Evernote, Microsoft, IFTTT, Dropbox, Amazon, and Slack.

What problems can it solve?

- **Scalability.** Data scalability in hardware tokens has not yet been implemented, and no identity management use cases have been identified. However, computational and network requirements are minimal.
- **Adoption.** Adoption of the technology is easy, thanks to cultural acceptance and simplicity of learning and training. The user interface is generally simple, using prominent display of a six-digit token for validation. Additionally, with TOTP, the password expires frequently, which gives end users practice in using the technology, further fostering adoption.
- **Maturity.** As an extension to mature OTP technology, HOTP and TOTP technology should see wide adoption because end users' experience would remain almost the same as traditional SMS-based OTP technology.
- **Security.** TOTP technology makes OTP technology less vulnerable to circumvention. As the dynamic password refreshes frequently, any fraudster who has possession of a token would find it difficult to be validated as the correct owner of the token.

What problems does it not solve?

- **Affordability.** Implementing OTP would involve additional hardware, software, and administrative costs that could translate into substantial up-front and operational expenses.

What problems could it create?

- **Security.** TOTP comes with enhanced security measures. The password generated gets refreshed frequently, presenting challenges for would-be hackers. However, if a token is stolen, the above-mentioned additional benefit is nullified. A two-factor combination of biometric validation with OTP solves this problem.

4.4.7. Trusted Platform Module (TPM)

A TPM is a hardware-based cryptographic tool, usually a chip on a computing device's motherboard. The technology enables strong disk encryption to provide secure user authentication without the need for complex passwords. Any computer or device, like a smartphone or tablet, equipped with a TPM can be used to store a credential. The solution is based on public key encryption on the user's device to mitigate security risks.[150]

TPM provides users with a unique digital identity represented by a Rivest-Shamir-Adleman (RSA) secure key pair called the endorsement key. An attestation identity key uses a hashing algorithm to provide security against illegal firmware and software. The endorsement key can be validated by the privacy certification authority to determine an individual's digital identity.

TPM can be combined with other security features such as firewalls and passwords to enhance device security. As a device boots up, TPM can determine whether it has been tampered with (since the last stable state) and can then block access to sensitive applications.

Many laptop manufacturers, such as IBM and Lenovo, already have TPM preconfigured in their hardware, but the module remains dormant until activated through the firmware in the laptop's processor. This feature can be activated for many users to provide identity and access management, protecting sensitive information from potential hacks.

TPMs are also present on mobile devices. On Apple devices, for example, a Secure Enclave protects a user's passcode and fingerprint data. Apple's biometric sensor, called Touch ID, doesn't store any images of the device owner's fingerprint. Instead, it saves only a mathematical representation or a template. This makes it impossible for someone to reverse engineer the actual fingerprint image from this stored template. The secure enclave is walled off from the rest of the chips and the device's operating system.

TPM is used as one of the authentication mechanisms in Mobile Connect.[151]

What problems can it solve?

- **Adoption.** Any TPM-enabled machine can be used to store the virtual user identity in what is called virtual smart cards at no additional cost, and distribution of these cards is easy over the Internet.
- **Affordability.** Maintenance costs for virtual smart cards are lower than for physical smart cards, which are easily lost, stolen, or broken from normal wear. TPM virtual smart cards are lost only if a user's device is lost or broken.
- **Scalability.** Because many devices now come preconfigured with TPM, the solution can be easily scaled up.
- **Security.** All confidential information on the virtual smart card is encrypted through use of the TPM on the host computer and thus cannot be used on any other computer. In addition, TPMs provide the same properties of isolated cryptography offered by physical smart cards. Finally, if a user enters a PIN incorrectly, the virtual smart card responds by using the TPM's anti-hammering logic, which rejects further attempts for a while instead of blocking the card (also known as lockout).

[150] *How to Use the TPM: A Guide to Hardware-Based Endpoint Security.* (01 March 2009). Trusted Computing Group. Retrieved from: https://trustedcomputinggroup.org/use-tpm-guide-hardware-based-endpoint-security/

[151] SME Input from Gautam Hazari—Technical Director—Personal Data at GSMA.

What problems does it not solve?

- **Adoption.** Because there is no physical representation of this identity document, users and governments cannot conduct transactions that traditionally require presentation of a physical identity document, such as at immigration checkpoints.
- **Scalability.** In Sub-Saharan Africa and Southeast Asia, the number of TPM-enabled computers might not be sufficient to scale this technology, and adding a TPM module to an existing computer is difficult, further limiting scalability.

What problems could it create?

- **Security.** TPM virtual smart cards reside on individuals' computers, which may frequently be left unattended. Such a situation opens the door for malicious individuals to use a brute-force attack or hammering (trying multiple PINs) to circumvent the system. The anti-hammering behavior of a virtual smart card differs in that it only presents a time delay in response to repeated PIN failures, as opposed to fully blocking the user.
- **Adoption.** The technology cannot be used in situations where an individual must present a physical identity proof, such as at a border crossing or a hospital. This slightly limits the technology's applications.

4.4.8. Key Trends in Mobile Solutions

Biometric smartphones have proliferated, with more than 500 models introduced since early 2013 and 1 BN of these devices in use today.[152] Projections show that by 2020, there will be 4.8 BN biometrically enabled smart mobile devices.[153] As the technology gets more portable and less expensive, portable registration of remote populations in developing countries may increase. Voter registration in several African countries[154] and population registration in Tanzania[155] are examples of how mobile technologies can help governments bring mobile registration to the people, versus the other way around.

Mobile ID is also increasingly emerging as a preferred choice for implementing digital ID systems. Consider these examples:

- Estonia's Mobile ID, launched in 2007, lets individuals access personal data and information on their mobile devices and authenticate online transactions using secure public key infrastructure (PKI) technology. SIM-based mobile ID can be used exactly like a regular physical credential with 300-plus organizations in Estonia's private and public sectors. The electronic signature function of mobile devices enables all of this and holds legal equivalence to a "wet" signature.
- Mobile ID is also available in Austria, Azerbaijan, Belgium, Finland, Germany, Iceland, Japan, Lithuania, Moldova, Norway, and Sweden.

[152] *Acuity Market Intelligence (2017).* PR Newswire. Retrieved from: https://www.prnewswire.com/news-releases/biometrics-on-smart-mobile-devices-to-redefine-digital-identity-with-129-billion-biometric-app-downloads-between-2014-and-2020-300115442.html

[153] *Acuity Market Intelligence (2017).* PR Newswire. Retrieved from: https://www.prnewswire.com/news-releases/biometrics-on-smart-mobile-devices-to-redefine-digital-identity-with-129-billion-biometric-app-downloads-between-2014-and-2020-300115442.html

[154] *Biometrics for elections to support the "One person, One vote" principle.* (04 November 2017). Gemalto. Retrieved from: http://www.gemalto.com/govt/coesys/enrolment/biometric-voter-registration

[155] Matthew Wilson (14 September 2017). *Mapping Access to Birth Registration and Updates from Tanzania.* GSMA. Retrieved from: https://www.gsma.com/mobilefordevelopment/programme/digital-identity/mapping-access-birth-registration-updates-tanzania

- In 2014, Oman became the first country in the Middle East to complement its electronic ID card with a mobile-ID scheme. Qatar and UAE later followed suit.

Mobile registration, where a registration authority uses mobile technology in the enrollment process, is becoming easier, more accurate, and more cost effective as specialized mobile devices are integrated with existing smartphones. For example, the BioID facial-recognition mobile app lets people pre-enroll in BioID with just a few clicks and captured facial images. Tascent's M6 is a mobile accessory that integrates with the iPhone and adds dual-iris capture along with dual-fingerprint-capture capability; along with the mobile app, it also provides capabilities for enrolling, de-duplicating, and authenticating subjects.[156] Other emerging technologies are using software-only solutions for mobile registration. For example, Element Inc. uses the existing cameras on mobile devices for biometric data capture, powered by deep-learning algorithms. Element's software can enroll multiple modalities (face, palm) without requiring connectivity or specialized hardware. The software is also accessible through software development kits (SDKs) or stand-alone applications, allowing common smartphones and tablets to become biometrically enabled.

Other advancements (such as SIM-based mobile ID, derived mobile ID, and NFC-based mobile ID) will enable users to identify themselves seamlessly to gain access to government services. Mobile apps are also adopting dynamic authentication techniques based on geolocation and users' transaction histories. Innovative applications are enabling multimodal biometric data capture, and some governments are combining such capture with deep-learning algorithms to create maternal and child heath registries.

Meanwhile, the Mobile ID SIM applet now allows individuals to confirm their identity and sign documents directly from their mobile phone, by entering a unique user-selectable PIN. Unified, personalized, multi-channel and multi-platform solutions are expected to emerge, using existing technologies like AI, voice recognition, and geolocation. These technologies will be easy to use, making tasks like authentication seamless and efficient.

Governments are also increasingly exploring a variety of public-private partnerships (PPPs) and revenue-sharing models to generate funds for the additional investments in hardware and network strength that mobile authentication systems require. In some of these models, mobile operators charge end users a fee for using mobile signatures and pass on part of the income to the government, as was done in Moldova.[157]

[156] *Tascent M6.* Tascent, Inc. Retrieved from: https://tascent.com/products-services/tascent-m6/

[157] World Bank (2016). *Digital Identity: towards shared principles for public and private sector cooperation (English).* World Bank Group. Retrieved from: http://documents.worldbank.org/curated/en/600821469220400272/Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation

SPOTLIGHT: CROSS-BORDER SYSTEMS

Advances in technology are enabling digital identification systems to operate across borders. Individuals holding a valid ID from one country can use their credential to conduct a transaction in another country (such as filing their taxes) or to identify and authenticate themselves at checkpoints or border crossings in other countries. The section discusses an example of cross-border identification systems that illustrate the above-mentioned use cases.

In the European Union, eIDAS (electronic Identification, Authentication and Trust Services) is a regulation on electronic identification and trust services for electronic transactions in the European Single Market. Under eIDAS, individuals can carry out secure cross-border electronic transactions that require them to authenticate their identity, such as enrolling in a university, opening a bank account and authorizing access to their electronic medical records.

There are three major stakeholders in the eIDAS network:[158] individuals seeking access to a service or establishing their identity in another country, the server providing access to a secure application or service, and the provider of the services an individual is looking for.

Once data to be authenticated are collected at the immigration point, depending on the IT architecture in use, the data are validated through a central database maintained on site or remotely validated if the database is located in a separate geography. A secure information exchange channel is achieved using SAML (Security Assertion Markup Language) for single sign on, error handling, and communication. End-point security is ensured using TLS (Transport Layer Security—a cryptographic protocol that provides communication security over a computer network).

The eIDAS regulation also includes rules for trust services providers—companies that handle electronic signatures, time stamps, electronic seals, and other methods for verifying documents—and it governs the use of trust services by consumers, businesses, and agencies to manage electronic transactions or access online services.[159]

[158] European Commission (06 November 2015). *eIDAS—Interoperability Architecture.* European Commission. Retrieved from: https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf

[159] Koo, J.H. (29 November 2017). *Please E-Sign Here: EU Cybersecurity Agency Finds Online Document Verification Services Secure.* The Bureau of National Affairs, Inc. Retrieved from: https://www.bna.com/please-esign-eu-b73014472575/

5. Authentication and Trust Frameworks: Technologies and Protocols

Federated authentication provides a standards-based solution to the issue of trusting identities across diverse organizations which may even be across countries. This requires the establishment of a trust framework between the identity provider and the relying party (service providers). A trust framework is a set of business, legal, and technical rules that members of a community agree to follow to achieve trust online.

Individuals typically require access to services hosted by different providers both within their national borders and beyond. A federated authentication framework comprised of governance, standards, and supporting technologies will enable Identity Providers and Relying Parties a means to provision trusted credentials and authenticate individuals with known assurance levels across a diverse range of service providers. The major advantage of the federated identity management approach is that the management of identity and credentials remains the responsibility of the original Identity Provider, and Relying Parties can define, and redefine, authorizations—what access is granted to the individual for voting, health records, financial transactions, etc., as they wish. This increases inclusion, interoperability, scalability, and security as it prevents the creation of credentials required to access many different applications, and it also “hides” identity attributes from all but the original Identity Provider.

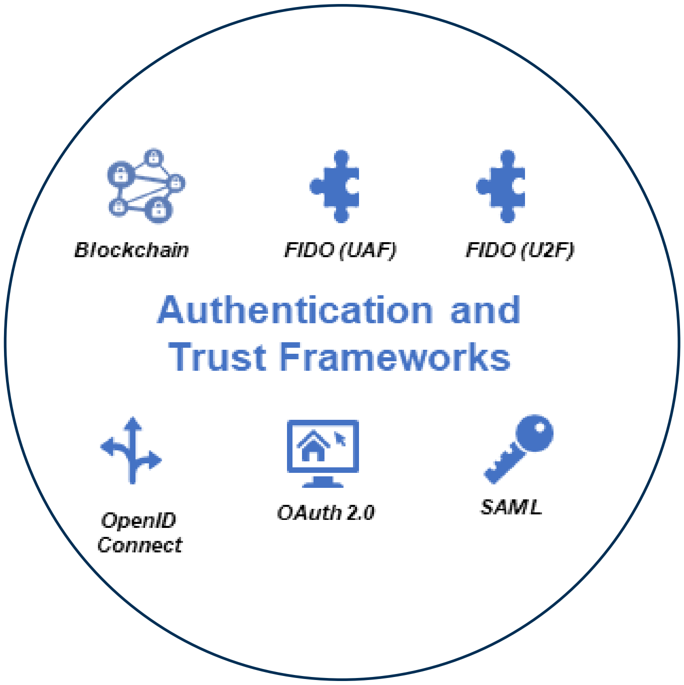
Open Authorization (OAuth) 2.0, is a framework, specified by the Internet Engineering Task Force (IETF) in remote function calls (RFCs) 6749 and 6750 (published in 2012) designed to support the development of authentication and authorization protocols. OpenID Connect (OIDC) is an interoperable authentication protocol based on the OAuth 2.0 family of specifications. It allows various applications to authenticate users without taking on the responsibility of storing and managing passwords. OpenID Connect was designed to also support native apps and mobile applications, whereas SAML was designed only for web-based applications.

FIDO defines both the Universal Authentication Framework (UAF) and the Universal Second factor (U2F) specifications. Together, they define a powerful model of user authentication—one that leverages established public key cryptography at the server, but also normalizes a pluggable architecture for local authentication. In FIDO, the user logically authenticates to the local device (phone, PC, etc.) via a variety of methods. This authentication method unlocks a private key (previously registered at the server) for signing an authentication challenge string. The server is insulated from the messy details of the actual user authentication and need only support a much simpler crypto protocol.

Blockchain is an emerging technology with use cases identified in the domain of digital identification for providing self-sovereign identity. “Public blockchains can provide decentralized registration and discovery of the public keys needed to provide digital signatures. These two steps pave the way for establishing a global public utility for self-sovereign identity—lifetime portable digital identity that does not depend on any central authority and can never be taken away.”[160]

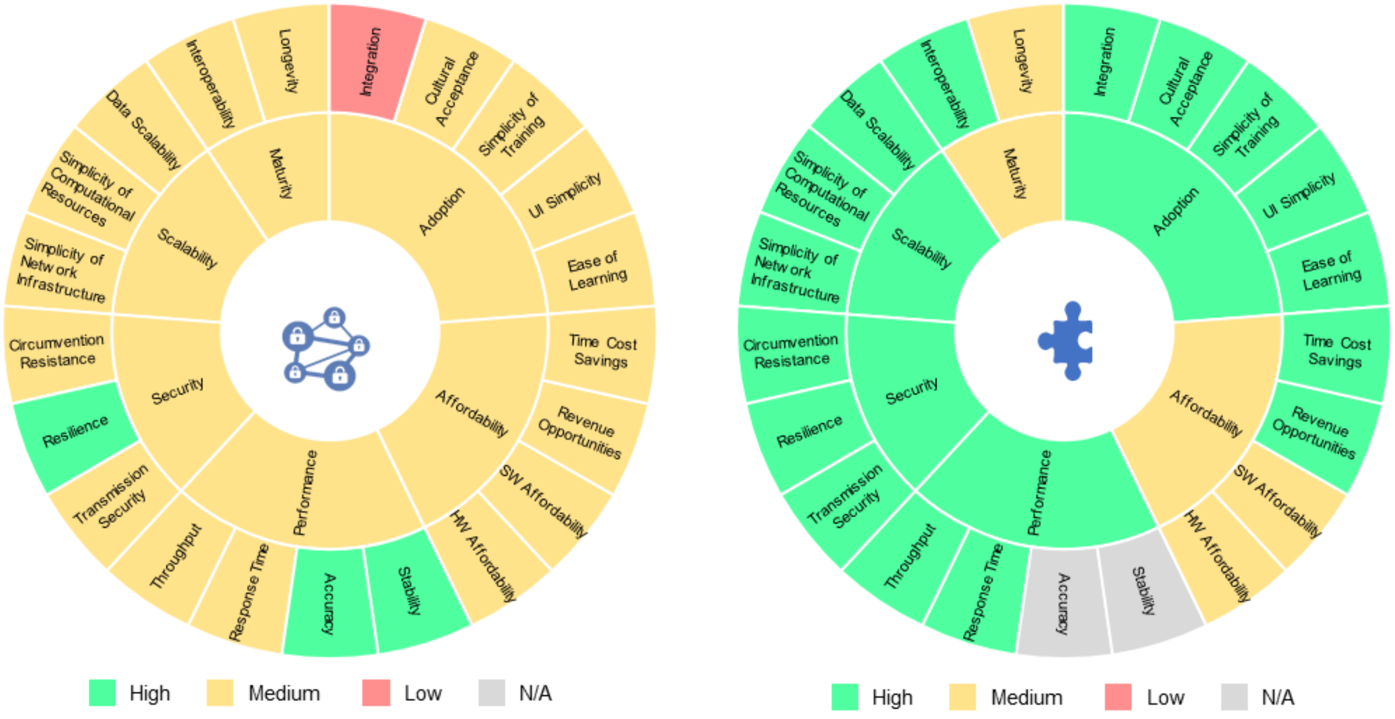
[160] *Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust.* A white paper from the Sovrin Foundation, Version 1.0, January 2018. https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

Figure 14: Authentication and Trust Frameworks: Technologies and Protocols



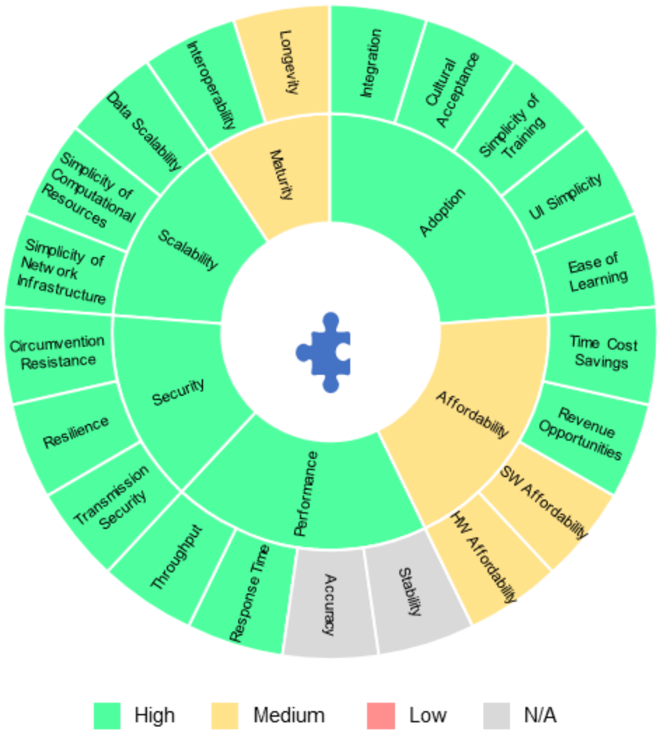
The following technologies are evaluated: blockchain (a type of distributed ledger technology, or DLT), protocols like OpenID connect and OAuth 2.0, FIDO (UAF), FIDO (U2F) and SAML. Figure 15 shows the results from the Technology Assessment Framework for each of these.

Figure 15: Assessment of Authentication and Trust Frameworks, Technologies, and Protocols

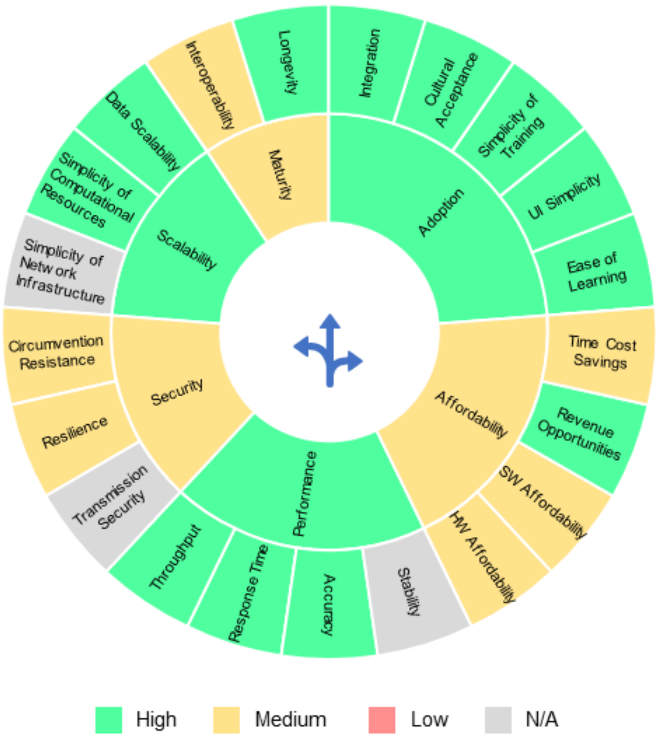


Blockchain

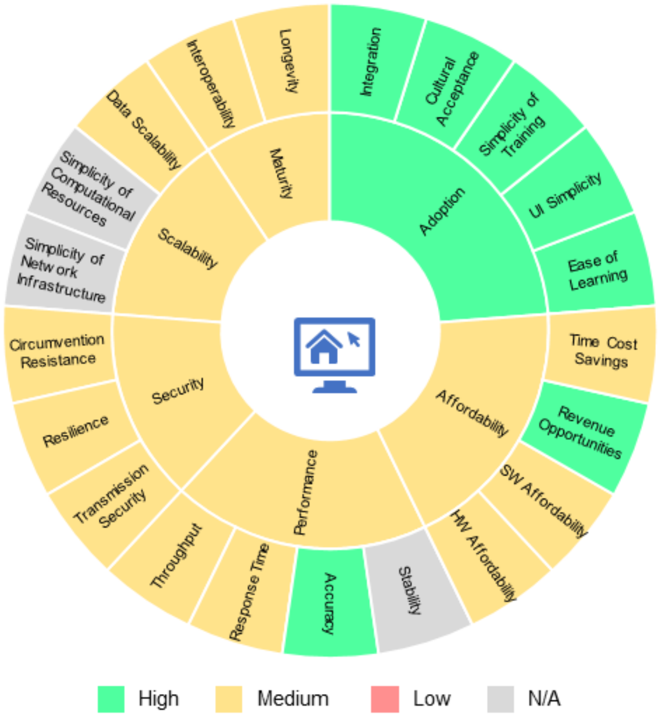
FIDO (UAF)



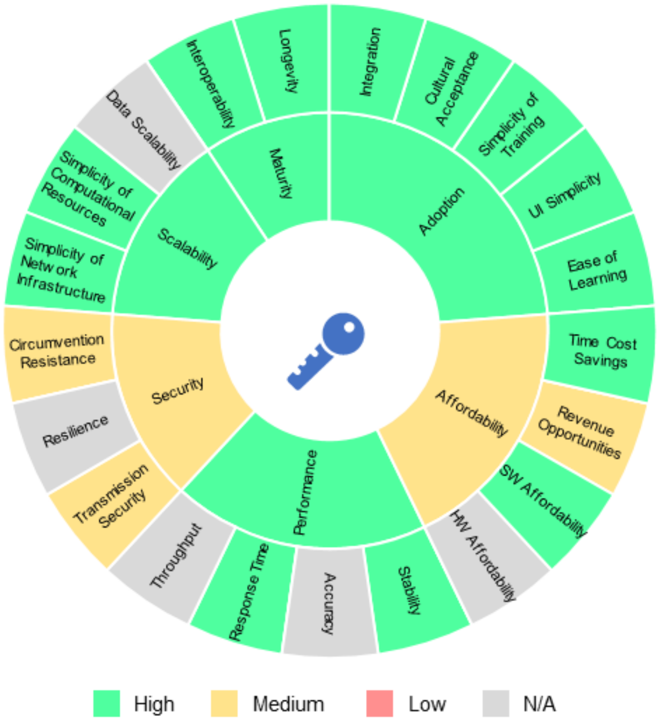
FIDO (U2F)



OpenID Connect



OAuth 2.0



SAML

5.1. Blockchain

Blockchain, sometimes referred to as "distributed ledger technologies" (DLT), is an emerging technology that records in chronological order transactions in a decentralized ledger that is hosted on "nodes" or servers across a peer-to-peer infrastructure. As one observer put it, "Picture a spreadsheet that is duplicated thousands of times across a network of computers and then the network is designed to regularly update this spreadsheet."[161]

Blockchains are immutable—someone can't edit a record that already exists, instead a new record needs to be created to show any corrections or changes to an existing record. That record is then verified for authenticity through a consensus mechanism and a new block is added to the chain. The type of consensus mechanism used depends on the architecture and usage of the blockchain. Common consensus mechanisms are "proof of work," "proof of stake," and "proof of authority." "Proof of Work" involves many nodes of the network racing to solve a complex math problem first, in turn earning a reward and the responsibility to close the block of transactions. "Proof of Stake" involves holders of large amounts of tokens in the system being randomly selected to agree to close the block of transactions. "Proof of Authority" involves the issuance of authority to members of the network who then close the block of transactions. Consensus mechanisms govern the speed of adding transactions to a blockchain as well as the resources required to add them.

Although in its early stages, blockchain technologies are being explored as an identity trust fabric enabling individuals to control their decentralized identity, including where and when they share identity attribute information. The advantage to utilizing a distributed system for identity verification is that there is no dependency solely on a single authority, and a person's identity attributes cannot be arbitrarily or abruptly taken away. Such an identity is usually termed a self-sovereign digital identity (SSID).

At this time, blockchains can be classified into three types, depending on how users are granted access to view, read, and write data on the chain.

- **Public and permissionless blockchains** are distributed ledgers open to the public to read and write or verify valid transactions using the blockchain platform. The most well-known example of a public and permissionless blockchain is Bitcoin. Public blockchains are secured through a consensus mechanism based on economic incentives and cryptographic verification, such as proof of work or proof of stake. The main drawback of proof of work is the amount of computing power needed and the energy costs required.
- **Public and permissioned blockchains** are distributed ledgers where the consensus process is controlled by a preselected set of nodes, usually a consortium of participants who have established a legally binding trust framework. The actual transactions on the network are publicly viewable and therefore verifiable.
- **Private and permissioned blockchains** utilize the same consensus process as a public and permissioned blockchain, however the transactions are only viewable by those participating in the network. For example, imagine a consortium of 15 financial institutions. Each operates a node, and ten of them must sign every block in order for the block to be valid. The right to read the distributed ledger is restricted to the participants.

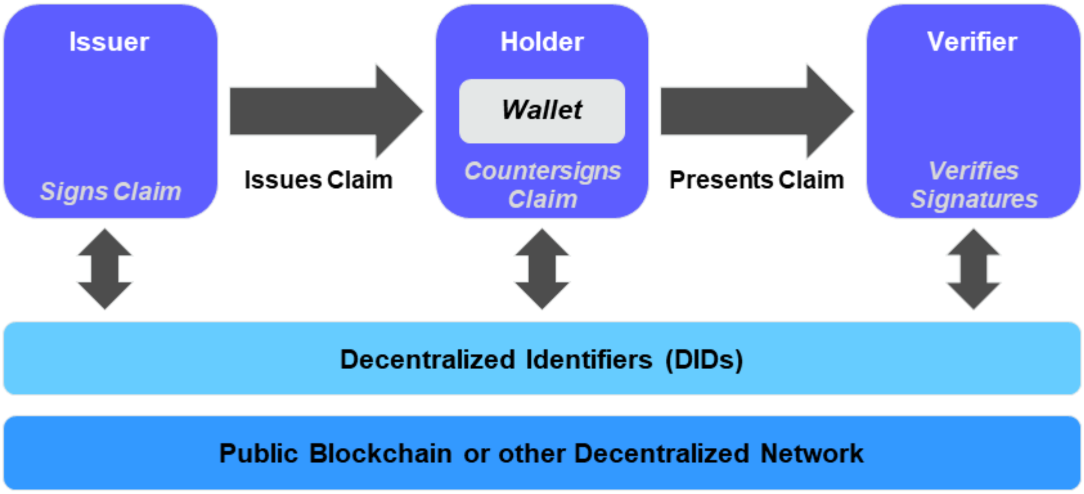
For digital identity applications, there is greater use of permissioned ledgers among trusted parties, as this approach provides increased transaction speeds and improved data privacy. Many proposed blockchain-backed ID systems are examples of accumulated IDs, whereby blockchain technology can be used to record

[161] BlockGeeks (19 September 2016). *What Is Blockchain Technology? A Step-by-Step Guide for Beginners.* Retrieved from: https://blockgeeks.com/guides/what-is-blockchain-technology/

transactions between an individual (potentially with no other formal ID document) and a peer, service provider, or authority. The history of transactions and identity attestations, sometimes called verifiable claims, are built up over time to form the accumulated ID.

Figure 16 provides a simple overview of an architecture of a decentralized identity ecosystem. A digital wallet stores verifiable claims, or accumulated ID information. The issuer is the organization or peer that provides a claim with identity attributes about the wallet holder. The verifier is an entity that the wallet holder would like to establish trust with, to transact. The wallet holder shares a decentralized identifier (DID) associated with the claim with the verifier, who can verify its legitimacy on the blockchain. Trust is maintained in the whole process by using public- and private-key encryption, whereby the individual's private keys are stored in the wallet. The wallet can be identified through a more convenient user ID (such as the user's Mobile Station International Subscriber Directory Number or MSISDN) and can be unlocked using conventional multifactor authentication mechanisms.[162]

Figure 16: Trust Framework[163]



What problems can it solve?

- **Privacy.** Blockchain identity systems, architected with privacy by design principles,[164] can provide individuals with the means to control and share identity information with third parties, without sharing information that is not needed to transact.
- **Security.** Any tampering with transactions in a blockchain is easily visible. This property fosters trust in the data, minimizing the need for central institutions to verify the data. The cryptography and consensus mechanisms built into blockchain technology make it very difficult for malicious users to attack.
- **Adoption (Cross-border verification).** Blockchain-based decentralized identity solutions could potentially support cross-border verification of identity. The technology enables individuals access

[162] Gautam Hazari (1 November 2016). *The Relationship Between Blockchain and Digital Identity.* GSMA. Retrieved from: https://www.gsma.com/identity/the-relationship-between-blockchain-and-digital-identity

[163] Sovrin Foundation (20 November 2017). *The Reality of Blockchain Identity* (presentation).

[164] Cavoukian, A. *Privacy by Design The 7 Foundatonal Principles.* Internet Architecture Board. Retrieved from: https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

and control over their personal identification anywhere in the world. However, interoperability between different platforms is challenging, and there is a need for standards to be developed to address this.

What problems does it not solve?

- **Complexity.** Fundamentally, blockchain technology does not by itself solve the challenge of registration and identity proofing. The integrity of IDs based on a blockchain depend on the integrity of documents or data used to onboard an individual onto a blockchain (i.e., the verifiable claims) or a volume of transactions to create an accumulated ID. Likewise, uniqueness cannot be ensured. There is nothing within blockchain architecture that would prevent a person from owning multiple private-key pairs.[165] Private keys can be linked to multiple public keys, which can be a positive or negative, depending on the use case.
- **Usability.** Much work is needed to make blockchain technology easy for most people to use. For example, when an individual forgets their password for a centralized identity system, there is a reset password option governed by the system providers. There is no central ownership for a decentralized system, and currently, no easy way for an individual to retrieve their private keys if they forget or lose them. Moving to decentralized identity systems means that the administrative burden for identity information is transferred from an experienced organization to an individual.
- **Adoption.** Blockchain solutions become more effective with more participants, however scaling requires up-front legal, policy and trust negotiations between partners and a greater understanding of the technology's capabilities.[166] An internet connection is needed to access a wallet and the ideal place to store identity information including private keys is a smartphone, a technology that is not available to much of the developing world.
- **Security.** Blockchain requires a large network of nodes to be resistant to attacks. With a smaller network, the chances increase that an attacker could manipulate a majority of a node into recording incorrect data. This is referred to as a 51% attack. Blockchain solutions consist of other complimentary components that can be more easily compromised than the chain itself, such as wallets.

What problems could it create?

- **Privacy.** The data on a blockchain are immutable, which has ramifications on privacy, including, for example, the "right to be forgotten." Cryptographic security also has a limited shelf life before new technologies are able to break it. With this in mind, most industry experts believe that personally identifiable information (PII) and biometric information should never be stored on a blockchain.

5.2. FIDO Universal Authentication Framework (UAF)

The Fast Identity Online (FIDO) alliance was 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 usernames and passwords.[167] The FIDO Alliance currently has two sets of specifications for simpler, stronger authentication: Universal Authentication Framework (UAF) and Universal Second Factor (U2F). This section focuses on the FIDO UAF protocol, whereby users register their device and then perform local

[165] Yaga, Mell, Roby and Scarfone (January 2018). *Blockchain Technology Overview.* NIST Retrieved from: https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf

[166] Nolan Bauerle (16 March 2017). *What Are Blockchain's Issues and Limitations?* Retrieved from: https://www.coindesk.com/information/blockchains-issues-limitations/

[167] FIDO Alliance (13 November 2013). *About the FIDO Alliance.* Retrieved from: https://fidoalliance.org/about/overview/

authentication on that device. FIDO UAF works on the principle of public-key cryptography and comprises the following steps:

- **Enrollment.** A public and a private-key pair are created that the protocol uses to authenticate users. The private key is retained by the user's device, while the public key is shared with the digital service.
- **Authentication.** The user can authenticate on the local device using biometric or non-biometric methods. During login, the online service challenges the user's authenticity. The user then authenticates himself or herself using biometrics or any other authentication method on the local device. Once the user is authenticated on the local device, the device responds to the online service's challenge by sending a signed challenge to the online service. The online service then verifies the device reply with the stored public key and lets the user log in.

What problems can it solve?

- **Scalability.** FIDO can be integrated with a variety of online services across industries. The protocols allow for universal standards, and with the increase in the number of biometrics-enabled smartphones, a large number of devices can implement the technology. Once provisioned, the same device can be used for multiple accounts and services without any additional cost and effort, allowing reuse for varied services across industries.
- **Performance.** Because the physical device remains with the user and the biometric data is stored in it, response time is very fast. What's more, the server stores only an encrypted public key for the user; biometric data is stored in the user's physical device. Authentication happens in the physical device, and only a private key is sent to the server to match with the public key to complete the authentication. Result? The process requires little data storage on the server, and computation is simple and easy.
- **Adoption.** Thanks to the technology's simple functionality and automated software prompts, individuals need little training to learn how to use it. And because a PIN or biometric data is stored in a local physical device in possession of the user, user acceptance of the technology is high.
- **Security.** Because authentication happens locally, and only private-/public-key pair matching happens on a server, the solution is very secure. Storing the private key in the user's device provides easier and stronger authentication while protecting user privacy. The protocols don't generate information that enables online service providers to track users. Biometric information for authentication never leaves the user's device, making chances of a security breach extremely low.

What problems does it not solve?

- **Maturity.** Some security and authentication protocols related to this technology are not yet approved. Only the FIDO certification protocol is complete.
- **Security.** As an authentication framework, FIDO was designed for decentralized enrollment (registration) and authentication. The framework does not support unique identification; this would need to be handled separately.

What problems could it create?

- **Performance.** Organizations seeking to implement FIDO also need a FIDO-less plan, because users might lose their registered device or forget to carry it with them.
- **Security.** For organizations planning to make online services accessible to all bring-your-own devices (BYODs), the diversity of such devices presents significant security and usability challenges. That's because individuals will use the same device for both private and professional use. It's therefore

imperative for organizations to ensure security of these devices and the credential information contained in them. Additional checks will be required to ensure compliance with organizations' security policies.

5.3. FIDO Universal Second Factor (U2F)

FIDO U2F is a new authentication standard published by the FIDO Alliance. The goal of this protocol is to simplify the two-factor authentication process with an open, secure, and easy-to-use standard. U2F enables phishing-resistant authentication using dedicated end-user hardware that could be Bluetooth devices, USB devices, or biometric devices. These devices do not require any special drivers; they just need a supported web browser. Once the website verifies the user's password, U2F authentication comes in. Using a public- and private-key pair, the website sends a "challenge" to the browser, which the U2F device plugged into the machine signs and returns. These devices integrate directly with the browser and mitigate many credential theft techniques like key-logging, phishing, and other attacks.[168] The strong second factor allows the service to simplify its passwords (for example, it may require only a four-digit PIN) without compromising security.[169]

What problems can it solve?

- **Security.** With U2F, one key can support access to many online services, without the need to share user information or create any encryption keys. Thus, the user is never tracked.
- **Performance.** Because the physical device remains with the user and uses a PIN for validation, response time is very fast. And because the server stores only an encrypted public key for the user, the data storage requirements for a user are very low. Biometric data are stored in the physical device, not in the server. Authentication happens entirely in the user's physical device, and only a private key is sent to the server to match with the public key to complete the authentication. Hence, computation is simple and easy.
- **Adoption.** Thanks to the technology's simple functionality and automated software prompts, individuals need little training to learn how to use it. And because a PIN or biometric data is stored in users' physical devices granting better security, user acceptance of the protocol is high.
- **Scalability.** Once provisioned, the same device can be used for multiple accounts and services without any additional cost and effort, enabling reuse for numerous services across industries. Time required to set up the device is fairly low.

What problems does it not solve?

- **Security.** The technology does not eliminate the need for passwords, because the relaying parties still need to authenticate individuals by using passwords before registering to FIDO U2F.
- **Adoption.** Users must always carry a physical device for authentication. Devices can be costly and prone to theft or loss.

What problems could it create?

- **Affordability.** The technology is expensive, requiring investments in FIDO infrastructure components such as security tokens and FIDO authenticators. In addition, operating expenses can be hefty, owing to costs required for implementation, support, and logistics of new token distribution.

[168] Duo Security (21 October 2014). *FIDO U2F—Universal Second Factor.* Retrieved from: https://youtu.be/v-GvJJEG9sw
[169] FIDO Alliance (13 November 2013). *Approach & Vision.* Retrieved from: https://fidoalliance.org/approach-vision/

- **Adoption.** If individuals lose their device or switch devices, they must register new devices using passwords. This cancels out the technology's primary benefit of access through a password-less mode.

5.4. OAuth 2.0

OAuth 2.0 is a token-based open-standard protocol for delegated authorization over the Internet. It provides client applications with secure delegated access. OAuth works over hyper text transfer protocol (HTTP) and authorizes devices, APIs, servers, and applications with access tokens rather than credentials. The technology enables users to authorize their identity to third-party services, without having to share their credentials. OAuth 2.0 assumes that the user is authenticated (by the service that hosts the user account), and does not define how authentication should be performed. When a user accesses services with an OAuth token, the services don't need to know who the user is, as long as he or she has a valid token. The identity provider makes this possible by issuing a token to the third-party application with the user's approval.

User-managed access (UMA) is an OAuth 2.0 extension that defines how owners of resources can control a resource's access to requesting parties, where the resources reside in a number of different servers and a centralized authorization server governs access policies. With UMA, the included authorization manager (AM) lets users delegate access control from host applications to the AM. As a result, administrators can compose access-control policies in a uniform way and in a single policy language of their choice. The benefit of this in digital ID systems is that UMA as a digital gatekeeper allows a user to manage, define, and monitor detailed sharing preferences for her or her data from multiple sources. Users can choose who gets to see their data, what type of data gets sent and how long the data can be accessed. This makes it easy to add a consent layer to API and applications through standards.[170]

What problems can it solve?

- **Maturity.** OAuth 2.0 tokens enable easier integration of web services through Application Programming Interfaces (APIs) without the need to share clients' credential data. The mechanism thus lets users share their account information with third-party applications or websites.
- **Performance.** This technology doesn't store clients' credential data and provides only an authorization flow through which a third-party source can authorize a user. Therefore, very few errors and defects in authorization occur as users log in.
- **Adoption.** OAuth 2.0 is vendor agnostic, user friendly, and easy to learn, fostering adoption. Moreover, it doesn't compromise clients' privacy, further enhancing acceptance.
- **Affordability.** The technology is highly reusable. Once the flow is defined and implemented, many applications can use it without incurring additional cost.
- **Security.** Implementing apps with OAuth 2.0 ensures that they're vendor agnostic and can withstand changes in server-side environments and policies.

What problems does it not solve?

- **Performance.** The number of requests that OAuth 2.0 can handle depends on server configuration. The technology also depends on how many requests a third-party server can process at any moment and how long it takes to process them.

[170] Amber Osborne (November 2016). *Sharing Is Caring: The Benefits of User Managed Access.* Retrieved from: http://www.think-progress.com/wp-content/uploads/2016/11/Content_Sharing-Caring-r4.pdf

- **Scalability.** OAuth 2.0 has not yet been used in any digital ID program. Therefore, its scalability has yet to be ascertained.
- **Security.** Because OAuth 2.0 only validates the token's origin and integrity, a stolen token can be used by anyone.
- **Affordability.** Setting up OAuth 2.0 requires deployment of a dedicated server, which can be costly. However, use of cloud infrastructure services can decrease hardware costs.

5.5. OpenID Connect

OpenID Connect provides developers with a framework for building functional and secure authentication systems for mobile use. It's an open standard for authentication designed to work in conjunction with the authorization capabilities of OAuth 2.0. An identity security layer built on top of OAuth 2.0, it allows verification of an end user's identity as well as the obtaining of basic profile information about the user. It achieves this by adding an identity token to OAuth 2.0 authorization.

OpenID Connect allows control over how much information about a user will be shared with third-party websites he or she visits. User credentials are never transmitted to those sites. OpenID Connect confirms the user's identity and shares only those details that the user has authorized it to share. In the near future, more software as a service (SaaS) offerings will accept ID tokens, which will greatly simplify development of applications that can authenticate users for API-driven applications.

The difference between OAuth 2.0 and OpenID Connect is that OAuth 2.0 is primarily an access-delegation protocol, through which resource owners grant permission or access rights to the requesting client with the help of access tokens. The OpenID Connect protocol is built on OAuth 2.0 specifications, with an additional ID token that provides information about the user (such as how and when the user was authenticated). OpenID Connect authentication services can be used by mobile devices through APIs. Mobile network operators are gradually adopting this enabling protocol to meet soaring market demand for mobile identity services.

As users seek more secure and efficient ways of authentication, standards are constantly changing. As this technology matures, adoption by large government agencies may pick up.

What problems can it solve?

- **Maturity.** OpenID Connect lets developers authenticate individuals across websites and apps without the need for the developers and apps to own and manage password files. The technology thus enables easy use of digital identities across websites and applications via any computing or mobile device. This capability creates a secure, flexible, and interoperable ecosystem for digital identity. Moreover, the technology can be easily integrated with multiple systems and platforms.
- **Performance.** Because OpenID Connect has a built-in security layer over the OAuth 2.0 token, it negates dependency on third-party authorizations—boosting the number of requests that the technology can handle.
- **Scalability.** OpenID Connect stores clients' credential data on their own server for self-authentication. Because it stores only usernames and passwords, it's not data intensive, fostering high scalability.
- **Security.** Because OpenID Connect builds on top of OAuth 2.0 and is self-authenticating, it's more secure than OAuth 2.0. And because third-party servers aren't involved, the standard is less prone to defects in data and less vulnerable to exceptional conditions.
- **Affordability.** With OpenID Connect, individuals can use the same credentials to access multiple services without incurring any additional cost or effort.

What problems does it not solve?

- **Security.** If clients' credentials are stolen, their security is at risk.
- **Affordability.** Setting up infrastructure for OpenID Connect requires an on-premise data server and a robust system for ensuring that data are stored securely on the server. Software and hardware costs are therefore significant. However, use of cloud-based storage services can mitigate hardware costs.

5.6. SAML

SAML stands for Security Assertion Markup Language, an XML-based open standard. This protocol supports the exchange of authorization and authentication information among business partners through web services. End users can access exclusive content across multiple sites or applications with a single sign-on.[171] A user's ID is said to have been federated among a set of providers when the providers have agreed on a set of identifiers or identity attributes by which the sites will refer to the user.

The SAML ecosystem consists of two parties, the SAML asserting party and the SAML relying party. At the heart of most SAML assertions is a subject (a principal—an entity that can be authenticated—within the context of a security domain) about which something is being asserted. The subject could be a human being or some other kind of entity, such as a company or a computer.[172]

SAML technology comprises the following components:

- **Assertion.** The asserting party asserts security information in the form of statements about a subject. An assertion contains some basic required and optional information that applies to all of the statements, and usually contains the subject and conditions used to validate the assertion.
- **Protocols.** These include request/response rules for performing tasks, such as authentication, single logout, assertion query, requesting, and artifact resolution.
- **Bindings.** These spell out how SAML protocol messages can be carried over underlying transport protocols (such as HTTP redirecting and HTTP posting).

What problems can it solve?

- **Maturity.** The technology has been in use for a while and has been implemented successfully across many government and corporate functions, proving widespread acceptance of this protocol. The XML-based guidelines support integration of authentication requirements across multiple platforms in different technologies, independently of the overarching technology stack.
- **Scalability.** SAML federation guidelines can be easily adopted in any end-user ecosystem of service providers.
- **Adoption.** The simple, user friendly system fosters easy adoption, though adoption by secured transaction systems hasn't yet been proven.

[171] Onelogin Developers (21 May 2015). *Dev Overview of SAML.* Retrieved from: https://developers.onelogin.com/saml

[172] Oasis (25 March 2008). *Security Assertion Markup Language (SAML) V2.0 Technical Overview.* Retrieved from: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

What problems does it not solve?

- **Security.** The technology is vulnerable to a number of different threats.[173] For example, in replay attacks, hackers hijack a SAML token and replay it to gain illicit access to services. In Domain Name System (DNS) spoofing, hackers intercept a SAML token and send a false DNS address. And in HTTP referrer attacks, hackers reuse an HTTP referrer tag.
- **Scalability.** Nonelectronic cards provide little opportunity to scale SAML technology. And with no data storage possible, the technology can't provide many built-in functions.

5.7. Key Trends in Authentication and Trust Frameworks: Technologies and Protocols

Developers around the globe are working on an open source, self-sovereign, blockchain-based identity system that will enable people, products, apps, and services to interact across blockchains, cloud providers, and government organizations. Organizations are also striving to establish standards and best practices supporting interoperability and fostering trust among different kinds of blockchain technology.

For example, the Government of Dubai recently announced a plan to use blockchain technology to verify all information on an Emirates ID card. Details related to a resident would be stored on the card, including insurance documents, passport information, and health data, and by 2020 will be stored in blockchains, secured, and encrypted.[174] Meanwhile, the Illinois Blockchain Initiative, in partnership with self-sovereign identity solution provider Evernym, will use the Sovrin Foundation's distributed identity ledger to create a secure, self-sovereign identity for Illinois residents during the birth-registration process.[175]

However, effective change management needs to be conducted at country locations to ensure that people's attitudes toward blockchain and the technology involved are understood fully before migration to this technology.

By contrast, OpenID Connect is rapidly gaining adoption on the web, with more than 1 BN OpenID Connect-enabled user accounts and 50,000 plus websites accepting OpenID Connect for logins. A number of large organizations issue or accept OpenID, including Google, Facebook, Yahoo!, Microsoft, AOL, Myspace, Sears, Universal Music Group, France Telecom, Novell, Sun, and Telecom Italia.

At the same time, the OAuth 2.0 working group—whose focus is on increasing interoperability of OAuth deployments and to improve security—is seeking to add an OAuth 2.0 device flow (which is typically used by applications on devices with limited input or display capabilities, such as TVs or other appliances). The goal is to let devices like mobile phones drive popularization of IoT devices.[176]

[173] Jem Jensen (07 March 2017). *Attacking SSO: Common SAML Vulnerabilities and Ways to Find Them.* NETSPI. Retrieved from: https://blog.netspi.com/attacking-sso-common-saml-vulnerabilities-ways-find/

[174] Tobias Young (14 March 2017). *Blockchain technology cuts through the hurdles to simplify everyone's lives.* The National. Retrieved from: https://www.thenational.ae/business/blockchain-technology-cuts-through-the-hurdles-to-simplify-everyone-s-lives-1.85148

[175] IL Blockchain Initiative (31 August 2017). *Illinois Partners with Evernym to Launch Birth Registration Pilot.* The Illinois Blockchain Initiative. Retrieved from: https://illinoisblockchain.tech/illinois-partners-with-evernym-to-launch-birth-registration-pilot-f2668664f67c

[176] Gartner (2017). *2017 Hype Cycles Highlight Enterprise and Ecosystem Digital Disruptions.* Gartner, Inc. Retrieved from: https://www.gartner.com/technology/research/hype-cycles/

Meanwhile, FIDO authentication protocols show promise, and a large group of vendors support FIDO specifications. However, FIDO's potential as a completely interoperable platform has yet to be fulfilled.[177] Gartner predicts that by 2019, 20% of organizations will support FIDO 2.0 for B2E (business-to-employee) online services.[178] Microsoft is also championing a Windows Hello Companion Device Framework. This is an open API that uses external devices, such as wearables or other Bluetooth-equipped devices with biometric sensors, to enable biometric security for devices that don't have it, and to extend verification to any sites or services that support FIDO 2.0 standards.[179] Regional government initiatives such as Australia's Digital Transformation Agency, UK government services, and the US Department of Commerce have implemented FIDO UAF for user authentication. Some large corporations, including Bank of America, Microsoft, PayPal, MasterCard, and Google, have also adopted it.

Additionally, software applications are being built to support a variety of federated protocols to authenticate, manage, and audit user identity through intranet and extranet sites. Several trust frameworks and interoperability guidelines have also been developed in the federated identity space. Organizations have established trust frameworks such as open-identity exchange and federal government identity, credential, and access management. Through this trust framework, identity providers and relying parties agree to trust and exchange credentials among themselves according to defined guidance and policies.

Federation and federated single sign-on (SSO) are fast becoming the standard mechanism to provide SSO across applications, and is becoming the preferred authentication mechanism with companies and across applications. This is due to native support for SAML in many software packages and adoption of SaaS applications.[180] The eIDAS interoperability framework to support cross-border identification and authentication processes uses SAML 2.0 for exchange of messages, as agreed in the eIDAS technical subgroup, and is spelled out in the eIDAS Interoperability Architecture.[181]

[177] Gartner (2017). *2017 Hype Cycles Highlight Enterprise and Ecosystem Digital Disruptions.* Gartner, Inc. Retrieved from: https://www.gartner.com/technology/research/hype-cycles/

[178] Bhat, M. and Singh, A. (13 December 2016). *Innovation Insight for Fast Identity Online Protocols.* Gartner, Inc. Retrieved from: https://www.gartner.com/doc/3540023/innovation-insight-fast-identity-online

[179] Bhat, M. and Singh, A. (13 December 2016). *Innovation Insight for Fast Identity Online Protocols.* Gartner, Inc. Retrieved from: https://www.gartner.com/doc/3540023/innovation-insight-fast-identity-online

[180] Brett Valentine (05 July 2017). *Current Trends in Identity and Access Management: July 2017.* SecurityIntelligence by IBM. Retrieved from: https://securityintelligence.com/current-trends-in-identity-and-access-management-july-2017/

[181] Joinup by European Commission. *eIDAS SAML Message Format.* European Commission. Retrieved from: https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_message_format_v1.0.pdf

6. Analytics Technologies

Analytics technologies use mathematical, statistical, and predictive modeling techniques that leverage a variety of data sources to find meaningful insights and patterns in data.

In digital ID systems, analytics can be used to build a comprehensive identity for an individual by combining data from multiple sources. Use of such analytics adds a layer of intelligence to an individual's identity profile. In this report, the following (see Figure 17) are examined: risk analytics, predictive analytics, business activity and operational analytics, and biographic matching (fuzzy search). Figure 18 shows the details of the Technology Assessment Framework for each analytics sub-technology.

Figure 17: Analytics Sub-Technologies

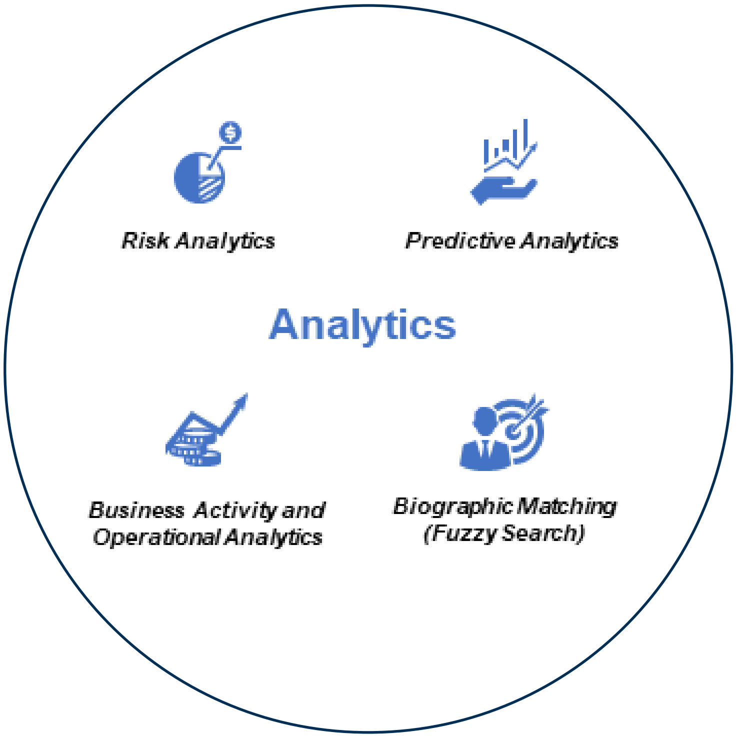
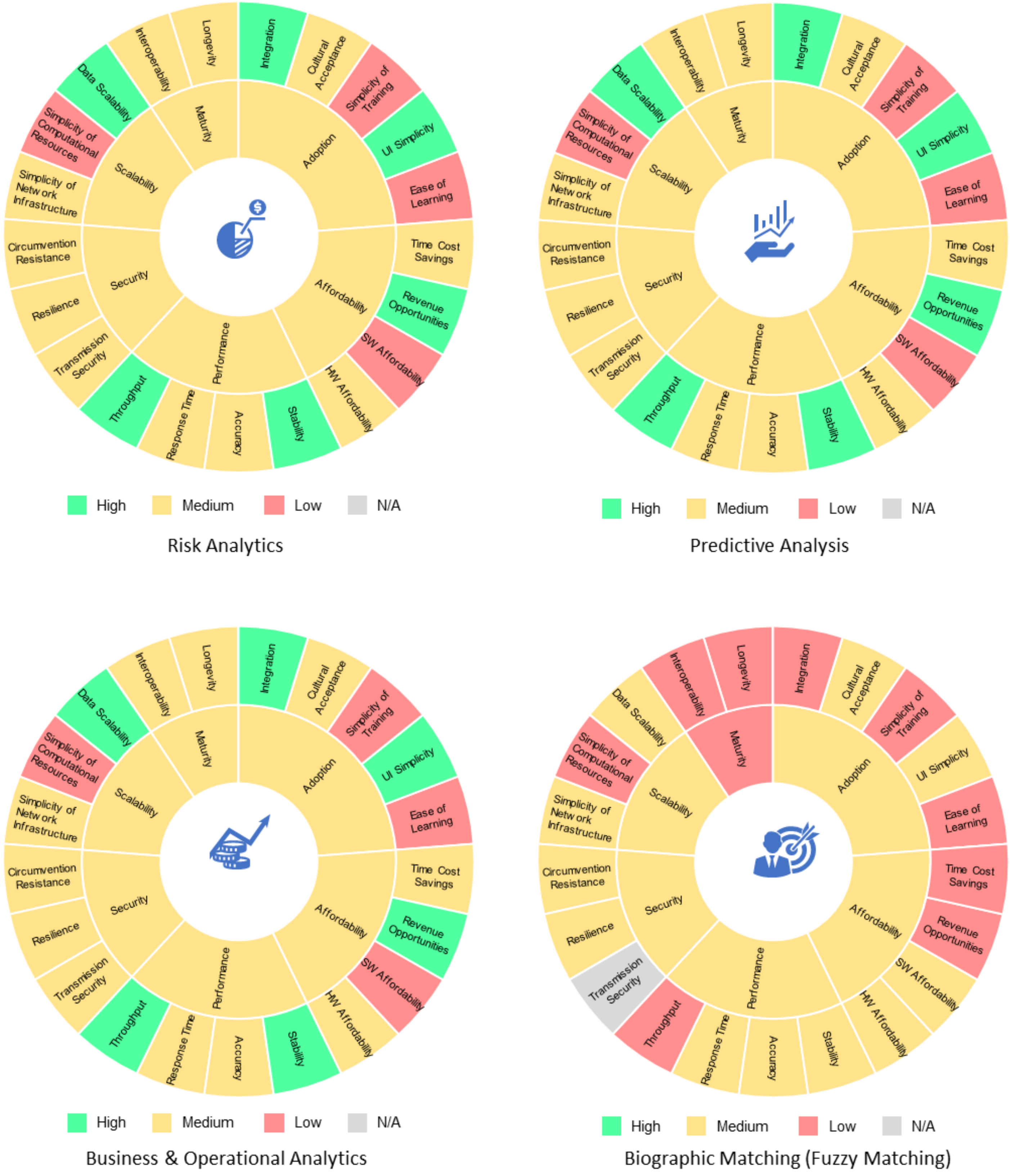

Risk Analytics
Predictive Analytics
Analytics
Business Activity and Operational Analytics
Biographic Matching (Fuzzy Search)

Figure 18: Analytics Sub-Technologies Assessment



Risk Analytics

Predictive Analysis

Business & Operational Analytics

Biographic Matching (Fuzzy Matching)

6.1. Risk Analytics

Governments and organizations can use risk analytics primarily to predict fraudulent and delinquent behavior in an individual and to assign a risk score based on information such as his or her financial or social history, criminal records, and instances of defaulting on loans. Today, risk analytics is more widely used in the private sector than in digital ID and authentication systems. Risk or threat analytics are being bundled with emerging identity systems like Enterprise Mobility + Security (EMS) from Microsoft and by Google in gmail to analyze and flag risk during user authentication. These algorithms check for suspicious log-in activity; for example, when a user logs in from a new device or location. The algorithm also analyzes log-in patterns to flag suspicious activity. For instance, if a user logs in from somewhere in the United States at 9:00 A.M. and then attempts to log in from India at 9:00 P.M., the system will flag this as an anomaly, as there is no realistic way for the user to travel that distance in 12 hours.

But governments are increasingly using data-driven insights to measure, quantify, and predict risk. The accuracy of risk models can be continuously improved by validating the results of the models through statistical feedback. They can also enhance confidence in a risk model's output by using highly trusted information, such as passport databases, as inputs for the model.

Thanks to the dramatic increase in computing power in recent years, along with maturing of analytical algorithms, organizations can now deploy advanced analytical techniques on a large scale.

What problems can it solve?

- **Performance.** Risk analytics integrates a high volume of structured and unstructured data into a single, unified view, from which operators can gather valuable information and actionable insights. Immigration services, for example, use these analytical models to evaluate risk profiles of foreign visitors based on their travel patterns. Also, as results are validated through statistical feedback, the models' accuracy continually improves.
- **Affordability.** Risk analytics models present considerable opportunities for organizations and departments to generate revenues that offset costs, because results and insights from these models can be used to make more informed decisions in a wide range of contexts, including identification.

What problems does it not solve?

- **Affordability.** To derive value from risk analytics, organizations must invest in powerful hardware and advanced software. Those are expensive, as is training practitioners and data models.
- **Security.** The data in a risk analytics model is subject to theft and manipulation during storage and transmission, unless data and process controls are applied at each stage of the analytics process to enhance security.
- **Adoption.** Training requirements are high, and building a risk model requires skills in both business and technology.

What problems could it create?

- **Adoption.** Collection of data by government agencies to profile individuals could raise concerns about online surveillance. That could catalyze strong opposition from the public.
- **Performance.** Poor data quality could lead the model to deliver false recommendations.

6.2. Predictive Analytics

Predictive analytics uses data, statistical algorithms, and machine learning techniques to predict the likelihood of potential future outcomes based on historical data. It hasn't yet found much applicability in digital ID systems. However, some research is under way on how such analytics might be used to predict how a person's fingerprint might change with age.

What problems can it solve?

- **Performance.** Predictive analytics models' overall response time is high when they use the right data processing framework, location of data, and appropriate output formats—even when data from various sources are combined and analyzed to derive insights. In addition, these models can be used to predict how an individual's biometric template might change with age. This could be useful for matching biometrics with an older test sample.
- **Scalability.** Predictive analytics models use transactional and behavioral data from multiple sources and can be scaled up to accommodate increasing data volumes. Emergence of cloud computing services has made predictive analytics models even more scalable.
- **Affordability.** Cloud-based technologies have considerably reduced the costs required to implement a predictive analytics solution.

What problems does it not solve?

- **Security.** Predictive analytics solutions are similar to risk analytics solutions in that they are vulnerable to data theft.
- **Affordability.** These solutions require extensive training of models and data scientists.

What problems could it create?

- **Adoption.** Collection of data such as an individual's online footprint could raise concerns about privacy and ethical violations.

6.3. Business Activity and Operations Analytics

Service providers can use business activity and operations analytics to analyze operational data in real time, with the goal of improving business process efficiency through continuous monitoring.

What problems can it solve?

- **Performance.** Business activity and operations analytics models can analyze large volumes of structured and unstructured data to find the root causes of service delivery problems.
- **Scalability.** Cloud-based computing has reduced complexity of and time required for implementation of these analytics models, improving scalability.
- **Security.** Identity and access management solutions can ensure strong compliance and enhance security by protecting and monitoring individuals' access to the models.

What problems does it not solve?

- **Affordability.** These models require significant investments in high-speed data exchange channels, computing power and network infrastructure to facilitate parallel processing and to run large-scale data algorithms. Data transfer infrastructure must be upgraded and integrated to handle all types of data, further raising expenses.
- **Adoption.** These models require a thorough understanding of niche technical topics. There are few expert data scientists, data architects, and analytical modelers working in this area.
- **Performance.** Poor quality of input data and improper data management can lead to inaccuracies in the models' output.

6.4. Biographic Matching (Fuzzy Search)

Biographic matching uses so-called fuzzy search to perform less than 100% matches on identity data. Fuzzy matching enables extraction of data from disparate biographical data sources, along with normalization and de-duplication of the data. It also enables semantic matching to extract meaning from unstructured text. For example, the software can match the word "big" to "large" or "car" to "automobile" because they are semantically related.

Multicultural name matching is a case in point. Fuzzy matching resolves situations where different versions of a person's name that reside in multiple sources must be identified as related. A person can have multiple versions of his or her name for several reasons. For instance, the individual has a nickname, gets married and adopts the spouse's name, or receives an advanced degree or a title. Transliteration, translation, or even simple data input errors can also lead to variations of a person's name. These variations can be problematic for officials seeking to search, merge, or de-duplicate records in an identity database. In such situations, and many others, fuzzy search can help officials find a person's name records that would otherwise not be located. For example, the names Dan Thomas and Daniel Thomas may be the same person, and R.S Singh and Ram Sewak Singh could be the same person. Fuzzy-search algorithms can be trained or programmed to make these associations.

What problems can it solve?

- **Performance.** Fuzzy algorithms are helpful for managing multicultural name matching and improving OCR search capabilities. They can also be used for partial text searching and support multiple languages.

What problems does it not solve?

- **Maturity.** Biographic data matching technology is still evolving, and the technology has not been standardized. Lack of interoperability standards and protocols for biographic data matching makes integration of unstructured and nonstandardized biographic data from multiple sources challenging.
- **Scalability.** Complex algorithms, high data storage requirements, and long computational time all make scaling this technology difficult.
- **Security.** Because the databases mostly contain unstructured data, checking database integrity after an attack isn't easy.
- **Affordability.** Unstructured data require more storage space, and developing fuzzy-search algorithms are costly. What's more, the algorithms can't be reused for other projects.
- **Performance.** These systems can't accommodate large numbers of queries at any one time, and fuzzy queries take longer to run than regular queries.

6.5. Key Trends in Analytics Technologies

Analytics technologies are enjoying a brisk market growth. Predictive analytics has seen a particularly rapid surge in popularity, with many organizations adopting innovative techniques, such as neural networks and machine learning. Predictive analytics could help reduce error rates due to template aging. Biometric template aging is defined as an increase in recognition error rate with increased time since enrollment.[182] A user's biometrics change with age, medical conditions, or normal wear and tear. Predictive analytics could simulate the effects of aging on the stored biometric template used for matching against the test sample—reducing false matches and rejections.

Along with predictive analytics, AI is seeing use in such forms as virtual assistants and chatbots to improve individuals' experience in using government digital services. New Zealand plans to use AI for real-time verification of individuals' digital identity. Dubai has built its first AI assistant to respond to individuals' queries about electricity and water services. Singapore's tourism board plans to use AI to predict and customize visitors' experiences.[183]

For countries seeking to build digital ID systems, use of analytics to support continuous authentication will help create a better user experience and enhance security and data resilience. Tools can unobtrusively gather information from several sources, including individuals' use of mobile devices, to create a profile that is unique to the account owner and that can't be stolen or replicated by fraudulent users.[184]

Identification and authentication platforms are being bundled with embedded analytics, which add reporting and analytic capabilities. The integration of a business intelligence (BI) platform with the ID architecture will enable real-time decision making, generate insights, and reveal patterns in data that help government agencies improve delivery of public services. New information and communication technologies (ICTs) like social media are also being used to facilitate crowdsourced identity vetting. Digitally enabled collective action initiatives by non-state actors (such as not-for-profit organizations) will prove invaluable, especially in places lacking democratic governance. For instance, the Ushahidi platform was used to monitor the 2011 Nigerian elections. In the meantime, to improve KYC processes, many organizations are applying identity analytics or identity intelligence to social media, unstructured, public or unreliable data gathered through open searches on the Internet.

In the meantime, user behavior analytics is a promising new area focusing on users' digital behavior, such as apps launched, network activity, and files accessed. This technology connects data from such disparate sources to glean insight into potential threats, suggested by unusual behaviors such as multiple log-in failures and access from an unknown location.

Business activity and operations analytics models are used to present information related to key performance indicators (KPIs). These, in turn, are used to provide information on an identification system's activity and performance. Technical and business operations professionals can use such information to detect impending problems, such as data processing bottlenecks. For instance, India's Aadhaar system analyzes performance on important metrics for operators, machines, and devices—such as the time spent on certain processes and task error rates, error rates at particular enrollment centers, and time spent on a

[182] Fenker, S.P., Ortiz, E., and Bowyer, K.W. (2013). *Template Aging Phenomenon in Iris Recognition.* IEEE Access, vol. 1, pp. 266–274. Retrieved from: http://ieeexplore.ieee.org/document/6516567/

[183] Basu, M. and Rohaidi, N. (29 June 2017). *The Briefing: How global governments are using AI right now.* GovInsider. Retrieved from: https://govinsider.asia/innovation/the-briefing-global-governments-ai-artificial-intelligence/

[184] Gartner (2017). *2017 Hype Cycles Highlight Enterprise and Ecosystem Digital Disruptions.* Gartner, Inc. Retrieved from: https://www.gartner.com/technology/research/hype-cycles/

particular screen during the enrollment and other processes.[185] Alerts on events of concern are processed in real time and pushed to the dashboards.

Business activity and operations analytics can also generate automated notifications that can be sent to groups of people or to a particular individual or department, depending on the issue at hand. Automated problem solving, where feasible, can correct or restart any failed processes related to identification and authentication.

With increasing use of digital identification programs, there emerges a pressing need to detect anomalies in the system arising from identity theft, and to take corrective action. Newer technologies, like neural networks,[186] are now being explored to find relevant factors in users' behavior, such as commute times, the user's location, and services requested—with the aim of detecting anomalies.

[185] Based on SME discussion with Sanjay Jain, former Chief Product Manager of UIDAI.

[186] Tanprasert, T., Saiprasert, C., and Thajchayapong, S. (2017). *Combining Unsupervised Anomaly Detection and Neural Networks for Driver Identification.* Journal of Advanced Transportation, vol. 2017, Article ID 6057830, 13 pages. Retrieved from: https://www.hindawi.com/journals/jat/2017/6057830/

7. Other Considerations

This report has provided a robust review and assessment of digital ID technologies across six parameters. In the context of digital ID implementation planning, it is important to evaluate these technologies through the lens of additional factors, such as privacy and data protection, open standards and vendor neutrality, demographics, culture, required service levels, economic feasibility, and infrastructure constraints, to further support effective decisions.

7.1. Privacy and Data Protection

Aside from the considerations listed above, governments must also take measures to implement a proper governance framework and to define policies for what personal data is captured, where it is captured, how the captured data is protected from attacks and intrusions, and how citizens' privacy and data confidentiality are preserved. Governments must also clearly specify what purposes the data will be used for and who will have access to the data, and set up mechanisms to ensure that consent from individuals is obtained before data are accessed and used. Individuals must also have appropriate legal recourse in case their data are misused or deployed with malicious intent.

Privacy and data protection regimes need to establish predictable rights and obligations regarding the treatment of individual data and personally identifiable information (PII) that are an important part of establishing trust in digital systems—trust that then encourages use.[187] Among other things, these regimes ensure that individuals should be aware of who has access to personal data, and grants individuals control over sharing personal data, as well as rights to access and correct such data. The harm caused by a data breach, theft, or compromise can result in identity theft, physical harm, discrimination, and emotional distress, causing individuals to lose faith (trust) in the system. And organizations may also suffer financial loss, erosion of reputation and confidence, and legal liability in cases of data breach.[188] In addition to legal and regulatory requirements of general application that protect data and ensure privacy, this report also highlights examples of industry-developed principles as applied to certain technologies.

7.2. Open Standards and Vendor Neutrality

As per the Principles for Identification referenced before, "Open design principles enable market-based competition and innovation. They are essential for greater efficiency and improved functionality of identification systems, both within country and also across borders. In addition, robust ICT procurement guidelines must be in place to facilitate competition and innovation and prevent possible technology and vendor "lock-in" which can increase costs and reduce flexibility to accommodate changes over time. Technology neutrality and diversity should be fostered to increase flexibility and avoid system design that is not fit for purpose or suitable to meet policy and development objectives."

[187] See *Digital Dividends,* The World Development Report 2016, at page 222 et seq., The World Bank; available at: http://www.worldbank.org/en/publication/wdr2016

[188] National Institute of Standards and Technology, U.S. Department of Commerce (April 2010). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

7.3. Demographics

Conditions such as size, distribution, composition, and movements of population are important when choosing technologies for digital identification programs. For example, the maturity of fingerprint and iris matching technologies has enabled them to be used with large populations. Contactless fingerprint capture and at-a-distance iris capture on the other hand, are emerging, supporting faster processing of more individuals than traditional capture devices can support.

With mobile technology becoming ubiquitous, mobile registration provides an opportunity to expand the reach of identification systems to people even in remote areas. This is especially useful in populations that are sparsely distributed across vast and remote terrains. Mobile registration can be used to capture individuals' credentials even in remote areas as long as a mobile connection is available. While most mobile solutions have been tested in limited pilots, their applicability in digital ID systems are still being studied.

7.4. Culture

Choice of technology must also align with the cultural practices of the society in which the identification program is being implemented. In cultures where people may perceive physical contact with biometric scanners as unhygienic or undesirable, innovations such as contactless fingerprint capture and at-a distance iris capture have become important. In some cultures, for example, it is unacceptable for a male agent at a digital ID enrollment site to touch a woman's hands to position them correctly on the fingerprint-capture device. Contactless technologies can ease such concerns.

Facial recognition is fast becoming popular as well. With its seamless authentication experience and improving accuracy, it may even replace fingerprinting in the near future. It does not depend on physical contact with individuals for authentication and therefore can be used in cultures where physical contact is undesirable. It can also be used in scenarios such as cross-border travel when large numbers of authentications must be done rapidly. While facial-recognition technology is still susceptible to morphing, it is rapidly improving, especially with the advent of 3D facial recognition. However, in cultures where women cover their faces with a niqab or veil, face recognition may be difficult to use. For this reason, many Middle Eastern countries have adopted iris capture and matching technologies in immigration control.

Rapid DNA technology has reduced the time and cost to process DNA samples. Use of Rapid DNA profiling and DNA matching technology is highly accurate and stable. Yet it is also controversial in digital ID programs, because of its potential to reveal highly sensitive and confidential information such as genetic, health, and familial information about individuals' private lives without their consent. Thus, cultural acceptance for any DNA-based solution is still low.

7.5. Service-Level Requirements

Service levels related to identification and authentication can be evaluated on criteria such as throughput (how many transactions per hour does the system need to support?), response time (how fast does the system have to provide a response?), and accuracy (how many FARs are allowed given a particular FRR?).

Machine-readable text and contactless smart card technologies have been widely deployed to secure and facilitate the reading of information from e-Passports. This is increasing the number of travelers that can be processed per unit of time in both automated and manual inspection lanes.

Enforcing biometric sample quality at capture and/or matching can help enhance accuracy, as can the use of biometric fusion technologies within a modality or across multiple modalities.

7.6. Economic Feasibility

While certain technologies might enable countries to implement an efficient identification program, they may not be economically feasible. For example, contactless smart cards may be useful in some cultural contexts. But they are more expensive than traditional ID cards, putting them out of reach for governments with comparatively less financial resources, such as those in emerging economies.

Similarly, blockchain may have limited applicability in developing countries. Its transaction costs are high compared to other database technologies, as each transaction must be verified at multiple nodes.

FIDO, SAML, and OpenID technologies are useful in identity federation, as described earlier in this report. This is especially relevant for emerging economies, because the technologies reduce the need for different functional registries to maintain their own database of individuals or users. These technologies offer not only lower costs but also enhance security.

7.7. Infrastructure Constraints

Infrastructure constraints in areas with no mobile network coverage and low Internet and mobile penetration can influence the choice of technologies to use for identification systems. Biometric system on card (BSoC) technology, for instance, reduces network dependency in regions with poor network connectivity because it combines the biometric sensor and matcher on a smart card, thereby eliminating the need for the biometric information to be sent to a central server or database for matching. BSoC also increases security, because the biometric information never leaves the card. However, no large-scale pilots or tests have been conducted for this technology, and interoperability standards haven't been fully developed.

Mobile-based identification and authentication solutions, such as Mobile Connect can be useful in emerging economies with high mobile penetration such as Nigeria,[189] where most Internet users access it using their mobile phones. However, the solution assumes that individuals have smartphones and that network connectivity is sound, conditions that may be less prevalent in developing countries.

7.8. Conclusion

The technologies and trends covered in this report are evolving rapidly, and their associated challenges and limitations highlighted here may not be applicable in the future. Therefore, readers are encouraged to regard this report as a snapshot in time. However, the Technology Assessment Framework introduced in this report—with its evaluation parameters of adoption, affordability, performance, security, scalability, and maturity—will prove useful for evaluating technologies even in the future and thus help readers make more informed technology choices.

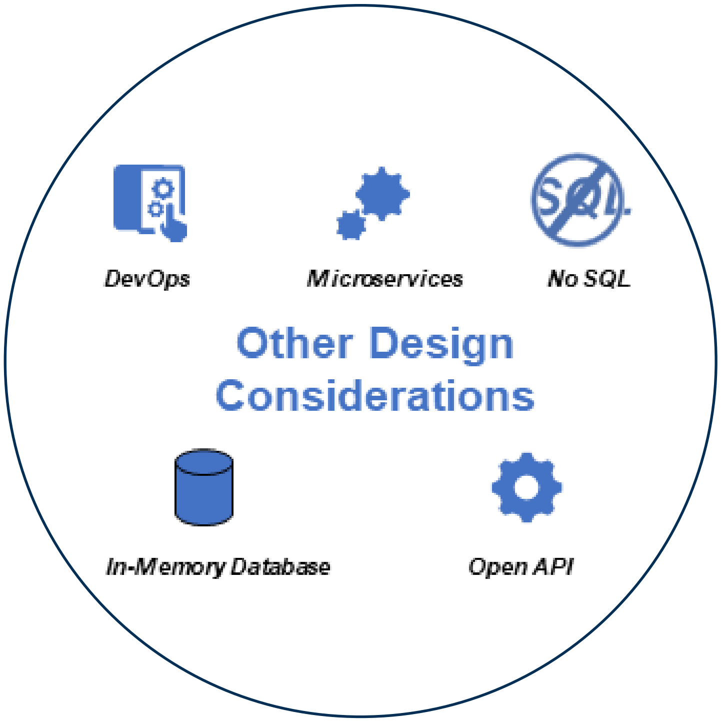
Many countries have made significant progress in the implementation of their respective digital identification programs. As more countries adopt and expand these programs, developing countries will benefit by learning from the experiences of those who are further ahead on the implementation curve. Understanding the challenges and benefits of various technologies, their associated costs and adoption across different socioeconomic and cultural groups will enable governments to develop identification programs best suited to their unique characteristics, challenges, and opportunities.

[189] Statista (January 2017). Mobile internet traffic as percentage of total web traffic as of January 2017, by country. Statista. Retrieved from: https://www.statista.com/statistics/430830/share-of-mobile-internet-traffic-countries/

Appendix 1. Other Design Considerations

The emerging technologies and design concepts covered in this section, while not core to identification and authentications systems, are still important to highlight for countries looking to setup nationwide identification systems.

Figure 19: Other Design Considerations as Spotlights



Application Programming Interfaces (APIs)

An API decouples a software application from its underlying functionality implementation. Decoupling or loosely coupling is a software term used to imply that one component is not heavily dependent on the other component, and therefore one can safely change one part without affecting the other. Here, such terms imply that for APIs, features of the software app can be changed without affecting the functionality too much.

Open APIs let owners of a network-accessible service give universal access to consumers of that service. They also let outside developers access back-end data that developers can then use to build new applications or enhance their existing applications. Thus, countries could look to publish datasets and APIs online for developers to build rich and useful applications for users. National ID platforms such as Aadhaar in India and Smart Nations in Singapore have adopted open API specifications to integrate their national ID databases with external applications.

Open APIs allow content or data that's created in one place to be dynamically shared and updated through multiple channels like the web, mobile devices, and TV. They also automate the generation of content and data across channels. This fosters efficient sharing and distribution of data, and better accuracy of the content and data. These APIs also reduce the need for governments of unique ID providers to invest directly in application development efforts. That's because freelancing developers can create innovative applications that add value to how consumers use unique ID data. In addition, Open APIs help drive innovation of new products and services through public-private collaborations.

Examples include the LTA DataMall, which provides travel-related APIs; Monetary Authority of Singapore (MAS) APIs, which help financial institutions and application service providers serve their customers better; and OneMap APIs, which let users embed an interactive map of Singapore on websites for providing location-based services.[190]

Security is critical when it comes to APIs. If an API service is breached or compromised, an organization's underlying internal data may be vulnerable to hackers. In addition, if the system lacks effective load-balancing tools, a spike in the number of API calls from other apps and services may lead to system overload.

Microservices

Microservices enable developers to build large applications as a collection of loosely coupled modular services—as opposed to traditional monolithic architecture. These services implement business capabilities such as responding to identification or authentication requests, and are independent and individually scalable. Put another way, instead of building one big application to achieve a specific outcome, developers build the application as a set of interconnected smaller services. This approach makes it easier for developers to understand, develop, test, and scale the application and fosters agile application development. Multiple vendors in the private sectors are using service-oriented-architecture (SOA)-based microservice platforms to provide enrollment, de-duplication, and authentication services.

In digital ID systems, which use complex processes, modularity is vital for testing, integrating, deploying, scaling, and upgrading these systems. And if demand for a specific service spikes—for example, the number of API calls increases—system operators can scale the corresponding microservices as needed to meet that demand, without needing to scale the whole system. This ability to scale the different component applications independently as needed creates efficiency, because not every part of an application experiences the same amount of load.

Perhaps not surprisingly, microservices have seen wide adoption, as many private-sector companies and even government services like the UK's Government Digital Service have moved from monolithic to microservice architecture.

However, this increased modularity comes with some compromise in performance. For instance, an application's throughput may be reduced if high volumes of service calls and network traffic occur over the distributed network. A modular system may also be vulnerable to network latency (which is the amount of time a message takes to traverse a system) and packet loss (which occurs when one or more packets of data travelling across a computer network fail to reach their destination). Microservices have traditionally been inefficient for information transmission, because the presence of an independent security barrier for each service to authenticate identity slows down the process. However, some innovations are under way to help create a distributed authentication mechanism for microservices.

[190] Smart Nation Singapore. Open Data. Government of Singapore. Retrieved from: https://www.smartnation.sg/resources/open-data

Going forward, microservices, along with APIs, will enable government agencies to build more individual-centric ID platforms.

In-Memory Databases

In-memory databases (IMDBs) store all or part of the data in random-access memory (RAM) instead of secondary disk storage. Most modern biometric-recognition systems use in-memory data storage mechanisms to maximize identification and matching speeds. In such systems, templates are stored and matched in-memory and persisted (for Restore operations) in traditional data repositories.

Working with data in-memory is much faster than writing to and reading from a file system or disk drive, magnetic, or solid-state technology. For this reason, in-memory databases can significantly speed up identification or de-duplication and authentication in identity management by greatly reducing the time required to access data. Storing data in-memory can also enable real-time analytics on identity data, which includes model-based risk assessment and biographic matching (for example, multicultural name matching).

In-memory data storage costs much more than traditional disk storage, however. Moreover, operators must understand data-access rules across different server nodes and mechanisms for loading data into the memory. All this entails a steep learning curve. Further, in IMDBs, the in-memory information is typically unencrypted to allow for faster processing. This creates vulnerability to attack and data theft. Research is under way to evaluate the effectiveness of encrypted template matching, but there are no such algorithms in production today. Other risk-mitigation ideas include anonymizing or separating PII to minimize storage of all data in one location—which prevents creation of a “honey pot” that attracts hackers or data thieves.

NoSQL Databases

NoSQL databases facilitate data management through a non-relational or schema-less, mostly open source and scalable database design. They thus differ from traditional databases, which use a relational model or schema to order existing data or any new incoming data into rows and columns.

Because NoSQL databases don’t rely on tabular relations to store and retrieve data, they boast fast processing speeds, especially when dealing with unstructured or semi-structured data. They also work well in a distributed architecture (a setup where components located on networked computers communicate and coordinate in order to achieve a common goal). And they scale well by readily enabling addition of nodes. They are used primarily to handle large volumes of data in diverse formats.

With traditional databases, considerable time and resources are often needed to align identity-related data into fixed schemas or to create new ones to meet operational needs. This may require creation of complex flows that call for considerable effort to design and update. Sometimes, useful data may have to get dropped because it does not fit in the schema. NoSQL databases mitigate these constraints by allowing unstructured data to be saved along with structured data and to apply a schema as required.

NoSQL databases are particularly useful for digital ID programs with a large population that generates a high volume of data and that require agile data storage design. Government agencies can use NoSQL databases to manage the ongoing flow of user data, some of which could help agencies improve individual services. In fact, NoSQL databases are expected to see more adoption in the future, owing to their flexible schema, high-volume data-management capabilities, and supporting multiple data format features.

Implementation of NoSQL databases may also present some challenges such as integration with traditional relational databases, especially if their data formats are not compatible. Moreover, NoSQL databases, just like the traditional databases, may also be susceptible to injection attacks—whereby an outsider gains access to and manipulates resident data because it requires relatively few relational constraints and consistency checks.

Distributed Systems

A distributed computer system consists of multiple software components that are on multiple computers, but run as a single system.[191] For national ID systems, these computers are geographically distant and connected by a wide area network. Distributed systems typically have a load balancing algorithm or system that assigns tasks to each note to minimize overall execution time of a request. Such systems have traditionally been used to manage large, complex volumes of data. The physical data in a distributed system can be organized in three ways:

- **Partitioned.** No data is duplicated.
- **Fully duplicated.** All data is duplicated in every computer in the network.
- **Partially duplicated.** Some data is duplicated in some computers in the network.

Distributed systems are built on the concept of parallel processing, so they deliver higher throughput and response rates compared to an equivalent centralized system. Also, owing to the architecture's modularity, these systems can be easily scaled horizontally (adding more nodes) and vertically (increasing processing power of each node) to handle ever larger volumes of data. Moreover, distributed systems have high redundancy, so a failure in one part of the network won't bring down the entire system. This increases the resilience of the overall system.

However, such systems also come with challenges. These include high hardware costs, because the system calls for different nodes or centers to be set up. What's more, these systems depend on complex software to manage various data handling and recovery functions, and such software is expensive. Setting up a distributed system requires highly trained practitioners who thoroughly understand key data architecture concepts like site autonomy, system transparency, data replication, and partitioning. Such practitioners are in short supply. Finally, distributed systems perform numerous data-communication transactions within the computing and data nodes. An increase in the number of nodes in the system thus makes it vulnerable to potential network attacks.

DevOps

DevOps is a software engineering practice that aims to unify software development and software operations. It is used to support fast, continuous development and deployment of applications. It enables an agile approach to accelerating software application releases and driving technology platform innovations. As a practice, DevOps requires software developers and operations teams to work together to build, test, deploy, and improve new application features.

A key element in DevOps focuses on application development, testing, and rapid deployment. Organizations using DevOps can perform these activities by automating the software-release process, from build to deploy. Another key element in DevOps focuses on operation and monitoring of applications, whereby teams capture, categorize, and analyze data and logs generated by the application. Through this process, they learn how updates in the application are affecting end users and system performance—and can make

[191] IBM Knowledge Center. What Is Distributed Computing. IBM. Retrieved from: https://www.ibm.com/support/knowledgecenter/en/SSAL2T_8.2.0/com.ibm.cics.tx.doc/concepts/c_wht_is_distd_comptg.html

improvements if needed. The system also generates alerts on the analyzed data, providing further feedback to development and operations teams.

In the future, DevOps could help government agencies modernize their large legacy identification systems by breaking them into small, independent components that can each be improved through agile development and delivery. Such use of DevOps could mitigate the time, costs, and risks that come with major modernization initiatives in big, complex organizations. However, to get the most from this use of DevOps, government organizations will need to use the right technologies and establish a collaborative culture that fosters the sharing of development responsibility across IT teams. Public-sector agencies that master DevOps could build identity proofing and authentication platforms using an agile approach that supports incremental improvement. They could more speedily address such platforms' technical shortcomings and roll out new capabilities (such as authentication using multiple modalities) essential for identification and authentication.

DevOps improves on existing approaches by establishing streamlined processes to deliver predictable, agile, efficient, and high-quality outcomes at every stage of the application-development lifecycle. Moreover, developers and operators work together, supporting early detection and faster correction of defects through the use of automated testing. The most valuable result is improved speed to market with a quality product that meets or exceeds expectations.

Appendix 2.

Table 1: Rating Comparison for Biometric Sub-Technologies

Technology Parameters	Fingerprint		Facial		Iris		Voice		Vascular		DNA		Behavioral	
	Capture	Matching	Capture	Matching	Capture	Matching	Capture	Matching	Capture	Matching	DNA Profiling	Biometric Matching	Capture	Matching
Maturity	**High**	**High**	**High**	**High**	**High**	**High**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**High**	**Low**	**Low**
Longevity	High	High	High	High	High	High	High	High	Medium	Medium	Medium	High	Low	Low
Interoperability	High	High	High	High	High	High	Medium	Medium	Medium	Medium	Medium	High	Low	Low
Performance	**High**	**High**	**Medium**	**High**	**Medium**	**High**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**High**	**Medium**	**Medium**
Throughput	High	High	High	High	High	High	Medium	High	High	High	Low	High	Medium	Medium
Response Time	High	High	High	High	High	High	Low	Medium	High	High	Medium	High	Medium	Medium
Accuracy	High	High	Medium	High	Medium	High	Medium	Low	Medium	Medium	High	High	Medium	Low
Stability	High	High	Medium	High	High	High	Medium	Medium	High	High	High	High	Medium	Medium
Scalability	Medium	**High**	**High**	Medium	**High**	**High**	**Medium**	**Medium**	**High**	**Medium**	**High**	**High**	**Medium**	**Medium**
Data Scalability	N/A	High	N/A	Medium	N/A	High	N/A	Low	N/A	Medium	N/A	High	N/A	Low
Simplicity of Computational Resources	High	High	High	High	High	High	High	High	High	High	High	High	Medium	Medium
Simplicity of Network Infrastructure	Medium	High	High	High	High	High	Medium	High	High	High	High	High	Low	Medium
Adoption	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**
Integration	High	High	High	High	High	High	High	Medium	High	High	Medium	High	High	Medium
Ease of Learning	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	High	Medium	Medium
UI (User Interface) Simplicity	High	High	High	High	High	High	High	Medium	High	High	Medium	High	Medium	Medium
Simplicity of Training	High	Medium	High	Medium	High	Medium	High	Medium	High	Medium	High	Medium	High	Medium
Cultural Acceptance	High	High	High	High	Medium	Medium	High	High	High	High	Low	Low	Medium	Medium
Security	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**
Circumvention Resistance	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	High	Medium	Low	Low
Resilience	Medium	Medium	Medium	Medium	High	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Transmission Security	High	Medium	High	Medium	Medium	Medium	High	Medium	High	Medium	High	Medium	High	High
Affordability	**Medium**	**Medium**	**High**	**Medium**	**Medium**	**Medium**	**High**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**
Hardware Affordability	Medium	High	High	High	Medium	High	High	Medium	Medium	High	Low	High	High	High
Software Affordability	High	Medium	High	Medium	High	Medium	High	Medium	High	Medium	Medium	High	Medium	High
Revenue Opportunities	High	High	High	High	High	High	High	High	High	High	Medium	Medium	High	High
Time Cost Savings	High	High	High	High	High	High	High	High	High	High	Medium	Medium	Medium	Medium

Table 2: Rating Comparison for Cards

Technology Parameters	Nonelectronic Card	RFID Non-Smart Card (ISO 180006-C, ISO 15693)	Contact Smart Card (ISO 7816)	Contactless Smart Card or Document (ISO 14443)	BSoC
Maturity	**High**	**Medium**	**Medium**	**Medium**	**Medium**
Longevity	High	Medium	Medium	Medium	Low
Interoperability	High	High	High	High	Medium
Performance	**High**	**Medium**	**Medium**	**Medium**	**Medium**
Throughput	N/A	N/A	Medium	Medium	Medium
Response Time	N/A	Medium	Medium	Medium	Medium
Accuracy	N/A	N/A	N/A	N/A	Medium
Stability	High	Medium	High	Medium	Medium
Scalability	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**
Data Scalability	Low	Low	Medium	Medium	Medium
Simplicity of Computational Resources	High	High	High	High	High
Simplicity of Network Infrastructure	N/A	High	Medium	Medium	High
Adoption	**High**	**Medium**	**High**	**Medium**	**Medium**
Integration	High	High	High	High	Medium
Ease of Learning	High	High	High	High	High
UI (User Interface) Simplicity	N/A	High	High	High	High
Simplicity of Training	High	High	High	High	Medium
Cultural Acceptance	High	Medium	High	Medium	Medium
Security	**Medium**	**Medium**	**Medium**	**Medium**	**High**
Circumvention Resistance	Medium	High	Low	Low	High
Resilience	N/A	N/A	N/A	N/A	N/A
Transmission Security	N/A	Medium	High	High	High
Affordability	**High**	**Medium**	**Medium**	**Medium**	**Medium**
Hardware Affordability	High	Medium	Medium	Medium	Low
Software Affordability	N/A	High	High	High	Medium
Revenue Opportunities	High	High	High	High	High
Time Cost Savings	High	High	High	High	High

Table 3: Rating Comparison for Supporting Technologies for Cards

Technology Parameters	Barcode	Magnetic Stripe	Machine-Readable Text
Maturity	**Medium**	**Medium**	**Medium**
Longevity	High	High	High
Interoperability	Medium	Low	Medium
Performance	**Medium**	**Medium**	**Medium**
Throughput	High	Medium	High
Response Time	High	Medium	High
Accuracy	Medium	Medium	Medium
Stability	Low	Medium	N/A
Scalability	**Medium**	**High**	**Medium**
Data Scalability	Medium	High	High
Simplicity of Computational Resources	High	High	Medium
Simplicity of Network Infrastructure	High	High	High
Adoption	**High**	**Medium**	**High**
Integration	High	High	High
Ease of Learning	High	High	High
UI (User Interface) Simplicity	High	High	High
Simplicity of Training	High	High	High
Cultural Acceptance	High	Medium	High
Security	**Medium**	**Medium**	**Medium**
Circumvention Resistance	High	Low	High
Resilience	Medium	Low	N/A
Transmission Security	Medium	Medium	Medium
Affordability	**High**	**Medium**	**High**
Hardware Affordability	High	High	High
Software Affordability	High	High	High
Revenue Opportunities	High	Medium	High
Time Cost Savings	High	High	High

Table 4: Rating Comparison for Mobile Sub-Technologies

Technology Parameters	OTP	Smart ID	Cryptographic SIM	Registration Using Mobile Device	Mobile Connect	Authenticator Mobile App (TOTP, HOTP based)	TPM
Maturity	**High**	**Medium**	**High**	**Medium**	**Medium**	**High**	**Medium**
Longevity	High	Medium	High	Medium	Medium	High	High
Interoperability	N/A	High	High	Low	High	N/A	Medium
Performance	**Medium**	**High**	**High**	**Medium**	**High**	**Medium**	**High**
Throughput	N/A	High	High	High	High	N/A	High
Response Time	High	High	High	High	High	High	High
Accuracy	High	High	High	High	High	High	High
Stability	Medium	High	High	Medium	High	Medium	High
Scalability	**Medium**	**High**	**High**	**Medium**	**High**	**Medium**	**Medium**
Data Scalability	Low	High	High	High	High	Low	High
Simplicity of Computational Resources	High	High	High	Medium	High	High	Medium
Simplicity of Network Infrastructure	High	High	High	High	High	High	High
Adoption	**High**	**Medium**	**Medium**	**High**	**High**	**High**	**Medium**
Integration	High	High	High	High	High	High	High
Ease of Learning	High	High	Medium	High	High	High	Medium
UI (User Interface) Simplicity	High	High	Medium	High	High	High	High
Simplicity of Training	High	High	Medium	High	High	High	High
Cultural Acceptance	High	Medium	High	High	High	High	High
Security	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**High**
Circumvention Resistance	Medium	High	Medium	Medium	High	Medium	High
Resilience	Medium	Medium	Medium	N/A	Medium	High	High
Transmission Security	Medium	High	High	Medium	High	Medium	High
Affordability	**Medium**	**High**	**High**	**High**	**High**	**Medium**	**Medium**
Hardware Affordability	Medium	High	High	High	High	Medium	Medium
Software Affordability	Medium	High	High	High	High	Medium	Medium
Revenue Opportunities	N/A	High	High	High	High	N/A	High
Time Cost Savings	High	High	High	High	High	High	High

Table 5: Rating Comparison for Authentication and Trust Frameworks: Technologies and Protocols

Technology Parameters	Blockchain	FIDO (UAF)	FIDO (U2F)	OpenID Connect	OAuth 2.0	SAML
Maturity	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**High**
Longevity	Medium	Medium	Medium	High	Medium	High
Interoperability	Medium	High	High	Medium	Medium	High
Performance	**Medium**	**High**	**High**	**High**	**Medium**	**High**
Throughput	Medium	High	High	High	Medium	N/A
Response Time	Medium	High	High	High	Medium	High
Accuracy	High	N/A	N/A	High	High	N/A
Stability	High	N/A	N/A	N/A	N/A	High
Scalability	**Medium**	**High**	**High**	**High**	**Medium**	**High**
Data Scalability	Medium	High	High	High	Medium	N/A
Simplicity of Computational Resources	Medium	High	High	High	N/A	High
Simplicity of Network Infrastructure	Medium	High	High	N/A	N/A	High
Adoption	**Medium**	**High**	**High**	**High**	**High**	**High**
Integration	Low	High	High	High	High	High
Ease of Learning	Medium	High	High	High	High	High
UI (User Interface) Simplicity	Medium	High	High	High	High	High
Simplicity of Training	Medium	High	High	High	High	High
Cultural Acceptance	Medium	High	High	High	High	High
Security	**Medium**	**High**	**High**	**Medium**	**Medium**	**Medium**
Circumvention Resistance	Medium	High	High	Medium	Medium	Medium
Resilience	High	High	High	Medium	Medium	N/A
Transmission Security	Medium	High	High	N/A	Medium	Medium
Affordability	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**	**Medium**
Hardware Affordability	Medium	Medium	Medium	Medium	Medium	N/A
Software Affordability	Medium	Medium	Medium	Medium	Medium	High
Revenue Opportunities	Medium	High	High	High	High	Medium
Time Cost Savings	Medium	High	High	Medium	Medium	High

Table 6: Rating Comparison for Analytics Technologies

Technology Parameters	Risk Analytics	Predictive Analytics	Business Activity and Operational Analytics	Biographic Matching (Fuzzy Search)
Maturity	**Medium**	**Medium**	**Medium**	**Low**
Longevity	Medium	Medium	Medium	Low
Interoperability	Medium	Medium	Medium	Low
Performance	**Medium**	**Medium**	**Medium**	**Medium**
Throughput	High	High	High	Low
Response Time	Medium	Medium	Medium	Medium
Accuracy	Medium	Medium	Medium	Medium
Stability	High	High	High	Medium
Scalability	**Medium**	**Medium**	**Medium**	**Medium**
Data Scalability	High	High	High	Medium
Simplicity of Computational Resources	Low	Low	Low	Low
Simplicity of Network Infrastructure	Medium	Medium	Medium	Medium
Adoption	**Medium**	**Medium**	**Medium**	**Medium**
Integration	High	High	High	Low
Ease of Learning	Low	Low	Low	Low
UI (User Interface) Simplicity	High	High	High	Medium
Simplicity of Training	Low	Low	Low	Low
Cultural Acceptance	Medium	Medium	Medium	Medium
Security	**Medium**	**Medium**	**Medium**	**Medium**
Circumvention Resistance	Medium	Medium	Medium	Medium
Resilience	Medium	Medium	Medium	Medium
Transmission Security	Medium	Medium	Medium	N/A
Affordability	**Medium**	**Medium**	**Medium**	**Medium**
Hardware Affordability	Medium	Medium	Medium	Medium
Software Affordability	Low	Low	Low	Medium
Revenue Opportunities	High	High	High	Low
Time Cost Savings	Medium	Medium	Medium	Low

worldbank.org/id4d

ID4D
IDENTIFICATION FOR DEVELOPMENT

WORLD BANK GROUP