Digital Identification Methods and Testing for AML Programs

CAMS-Audit Advanced Certification White Paper

Eugenio (Gene) Di Mira

Establishing digitally sourced trusted identities is not only critical to fighting money laundering by reducing risk, it will also improve the customer experience and save companies significant resources.

Table of Contents

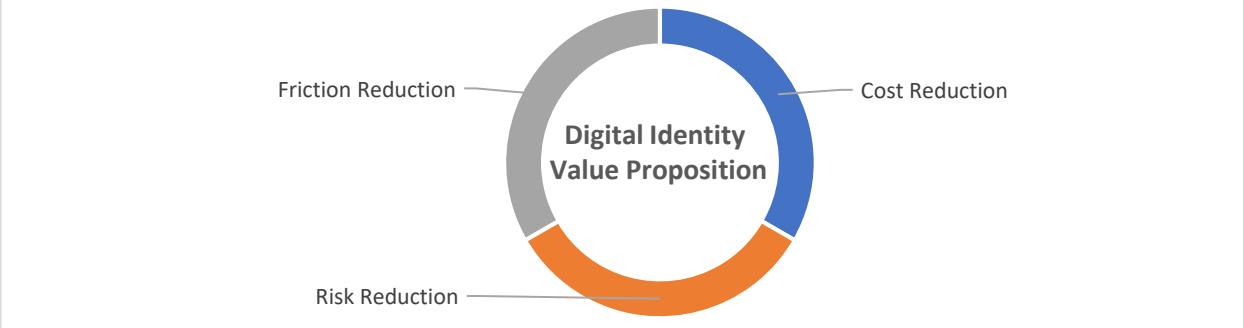
Executive Summary of a Study of Digital Identification Methods and Testing for AML Programs

To study the impact of the modernization of client identification in combating money laundering and terrorist financing, this paper will begin with a definition of identification, and then outline current methods to identify persons using physical and/or electronic records, and consider approaches to testing these processes.

Identification is based on resolution of the identity of a person using trusted, reliable sources of information to achieve confidence that not only the person exists, but also that we are dealing with that person. The strength of the identification process directly contributes to the integrity of information which is relied upon to untangle potential proceeds of crime from legitimate property.

This paper will include in the definition of identification, an approach to assessing the strength of identification, and how to apply reasonable measures to reduce risk. These measures can then be used to monitor and audit the success of programs as new tools are developed to identify persons.

Innovations in identity management, moving from physical to authenticated electronic records, will improve record integrity (reduce risk), be more efficient due to reduction in staff time to review documents (reduce cost), and will be easier for the customer through online access (reduce friction).



Audience and Scope of This Paper

This paper introduces the reader to key concepts behind the acceptance of identity as well as how client information can be collected effectively using online channels to combat the use of proceeds of crime. To help audit and compliance personnel keep pace with the various methods of identification innovations and how to test each one based on their designs, this paper is designed using a case study approach.

The scope will be limited to the identification of living persons and exclude legal entities, which merit their own dedicated discussion. The paper will target a non-technical audience, using footnotes to provide sources for further study. (Example: *A Blueprint for Digital Identity* from the World Economic Forum is a good primer with technical support.[1])

[1] *A Blueprint for Digital Identity* from the World Economic Forum is a good primer with technical support. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

Why Do Financial Institutions and Persons Need Identification?

The focus of identification within financial institutions is to tie the property to be held in custody for a person to their identity. This is accomplished through processes in place that rely on prior trusted relationships between the person and other trusted entities which are reviewed at the beginning (onboarding) of a new account relationship. Subsequent interactions with the same persons are then confirmed based on established records in a process known as authentication. For higher-risk transactions, a repeat of the identification process is used to compare the customer to the records on file with the financial institution.

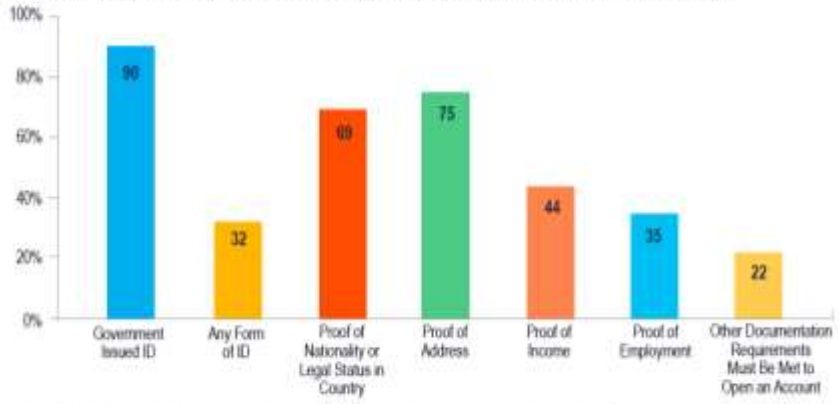
The Role of Identity Within Programs Built to Combat Proceeds of Crime

To combat the proliferation of proceeds of crime and terrorist financing, a primary recommendation of the Financial Action Task Force (FATF)[2] and requirement of corresponding anti-money laundering (AML) legislation is to collect know-your-client information (KYC). The identification of the persons who own or control property held with financial institutions and participating organizations within an AML regime is a core component of KYC collection. Identification also provides the ability of institutions to perform due diligence and to research names that match with high-risk persons.

Government issued identification documents or records have been the primary reliable method to identify a person, however technology has evolved, and rules have adjusted to allow commerce to rely on multiple methods of identification based on other reliable sources.[3]

Figure 2: Document Type Needed for Account Opening

% of responding jurisdictions that require documentation type to open an account at a Commercial Bank



Source: 2017 Global Financial Inclusion & Consumer Protection (FICP) Survey, WBG. 124 jurisdictions participated in the survey

The level of diligence required in the execution of identification varies from the principles-based approach[4] of achieving a "reasonable belief that it knows the true identity of each customer" taken in the United States to more prescribed methods in other countries.

[2] FATF Recommendation 10(a)at http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

[3] *G20 Digital Identity Onboarding*, Figure 2: Document Type Needed for Account Opening, The World Bank Group at https://www.gpfi.org/sites/default/files/documents/G20_Digital_Identity_Onboarding_WBG_OECD.pdf

[4] *BSA/AML Manual*, "Customer Identification Program Overview," FFIEC at https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_011.htm

When Do Organizations Identify or Authenticate Customers?

Organizations want to balance the risk of not having records with integrity, while managing the operations burden of identification and authentication processes. They look to minimize customer inconvenience of completing forms and repeating information as they improve the customer experience while saving costs. Records are retained and relied upon at every stage of customer interaction.

1) First meeting with a customer involves collecting attributes from trusted sources.
2) Identification/subsequent authentication process is performed; the attributes received from trusted sources or on file are validated with the customer.
3) The "Information Transaction" with the customer is stored, including the source, time, and records.
4) The records are then relied upon (e.g., opening a new relationship, paying a claim, adding a new party to an existing contract).
5) Updated communications and actions are relying on these records.
6) As needed, process can revalidate or improve the information on file.

Onboarding and subsequent processes all rely on identification documents and other records provided by the customer to the financial institution, which can run the risk of being fraudulent. The review of photo identification documents by staff can fail due to inexperience with the type of records, a resistance to challenging a customer for fear of loss of business, or internal compromise of the employees. The masking of identities, using pseudonyms, also-known-as (AKA) names, or synthetic identities, is used by criminals to obscure the connection of proceeds of crime. Due to the proliferation of information compromises, resulting from data breaches and social engineering, there has been a move to rely on refreshing identification methods using other trusted sources (primarily mobile one-time passwords or biometric tokens) to improve security measures.

Privacy and information security principles[5] are equally important for persons in order to reduce the unnecessary sharing of information used for identity confirmation. Requiring persons to confirm the information being used improves its accuracy and supports individuals in taking a strong ownership of their identity to aid in the fight against fraud. Another privacy principle involves the collection of the consent of the consumer, prior to the collection, or sharing of personal information.

[5] Privacy principles are similar in many countries. The Privacy by Design framework encourages incorporating these concepts in the design of processes at the onset to improve the management of information. See https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/.

Information security programs have grown and formalized not only to protect a company from intrusion and require robust controls, but also to protect client data as well. Regulators have taken notice and are setting standards[6], while the private sector is not shy to search for compensation from those who cause a breach.[7]

Testing the Effectiveness of Identity Programs and Customer Identity Access Management

Required Element(s)	Test(s)
When is identification recommended and required?	1) Is Identification required only when needed to meet minimum legal requirements? 2) Is identification, or partial identification, performed on a risk-based approach at onboarding and to strengthen authentication? 3) Is identification also reviewed or confirmed with suspicious activity detection, higher-risk transactions, or enhanced due diligence measures?
How is the identification program monitored?	1) Is monitoring of unusual activity, fraud, and investigations part of dedicated teams who have tools to detect identification compromises? 2) Is identification part of the customer risk-assessment program? 3) Are identification requirements included in quality assurance, compliance testing, and audit testing programs?
How is information protected within the system and in the process?	1) Is personal and identifiable data stored and encrypted at rest? 2) Is personal and identifiable data stored and encrypted in motion? 3) Is the information stored or accessible by a vendor in any part of the process? If so, how is information security maintained?
Privacy and personal information management	1) Is only the minimum information retained or confirmed for the required purpose? a. Personal information can be validated in the process, but only the result stored. A current use case of this includes the smartphone method to store a fingerprint and applications that use a fingerprint match only typically receive a token confirmation that the match was successful, and the fingerprint itself is not provided to the application. b. Personal information may be retrieved from other sources and provided to the customer to confirm (e.g., phone number lookup used to confirm the address of a person). 2) Once the identity has been confirmed, what rights and permissions are provided to this person?

[6] "Cyber Security Self-Assessment Guidance," Office of Superintendent of Financial Institutions, Government of Canada at http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx.
[7] See Wendy's settlement with banks to compensate for data breach at https://www.bankinfosecurity.com/wendys-reaches-50-million-breach-settlement-banks-a-12032.

Why Now? The Pivotal Point in the Evolution of Identification

From an identity perspective, many of the challenges highlighted above, include record integrity, reducing information over collection, and reducing poor customer experience, and the process friction that comes from the manual collection of data. Technology has evolved to allow the customer to provide permission for an existing relationship with a trusted entity (government, financial institution, or utility), which both the customer and a new business relationship would trust, for the transfer of customer's information securely to a new entity.

Technology has evolved significantly in recent years to strengthen identity-access management of systems into robust processes involving cryptography to provide reliable and traceable tools for confirming the legitimacy of information exchange to a source. These new tools have resulted in frameworks that can provide identity solutions for commerce that are comparable or stronger than in-person methods, while adding significant efficiencies for global trade.

Government approaches to embracing technological changes have varied with some methods turning to enhancing national identity-document programs with biometrics and additional data, while others have turned to trust frameworks and digital identity tokens.

Commercial solutions that create digital identity networks managed by the person and using trusted stewards of data, known as self-sovereign identity,[8] also evolved.

In response, the FATF is releasing new guidance related to the reliance on self-sovereign identity (non-government issue using a trusted framework). FATF committees have been reluctant to comment on the need for principles-based guidance to help steer international approaches to digital identity that improve the processes for collecting identity across borders.

Defining Identification – Answering the Question: Who Are You?

Identification is the process of establishing the **resolution** of a unique person (either individual or entity) though the use of **attributes** provided by a **reliable source** (i.e., based on trusted record[s] or organization[s]), and matching them to a person **(identity proofing)**. To comply with anti-money laundering programs, however, the **traceability** of the identification is a critical part of a compliance program. Each of the terms in bold will be clarified in this paper.

Understanding Identity Concepts to Assess Identification

These three key questions will help define key concepts to determine the strength of an identification process. These concepts are more thoroughly explained and defined in international standards, such as NIST Digital Identity Guidelines[9] for the United States which are used by both the public and private

[8] Sovrin is a prominent Self-Sovereign Identity Network: https://sovrin.org/faqs/
[9] NIST Special Publication 800-63-3 Digital Identity Guidelines provide enhanced details on international expectations in systems and process requirements to meet identity assurance levels and proofing.

sector, the European eIDAS regulation, which requires cross-acceptance across the European Union,[10] and for the United Kingdom in gov.verify,[11] which is a public-sector led network with active private-sector participants.

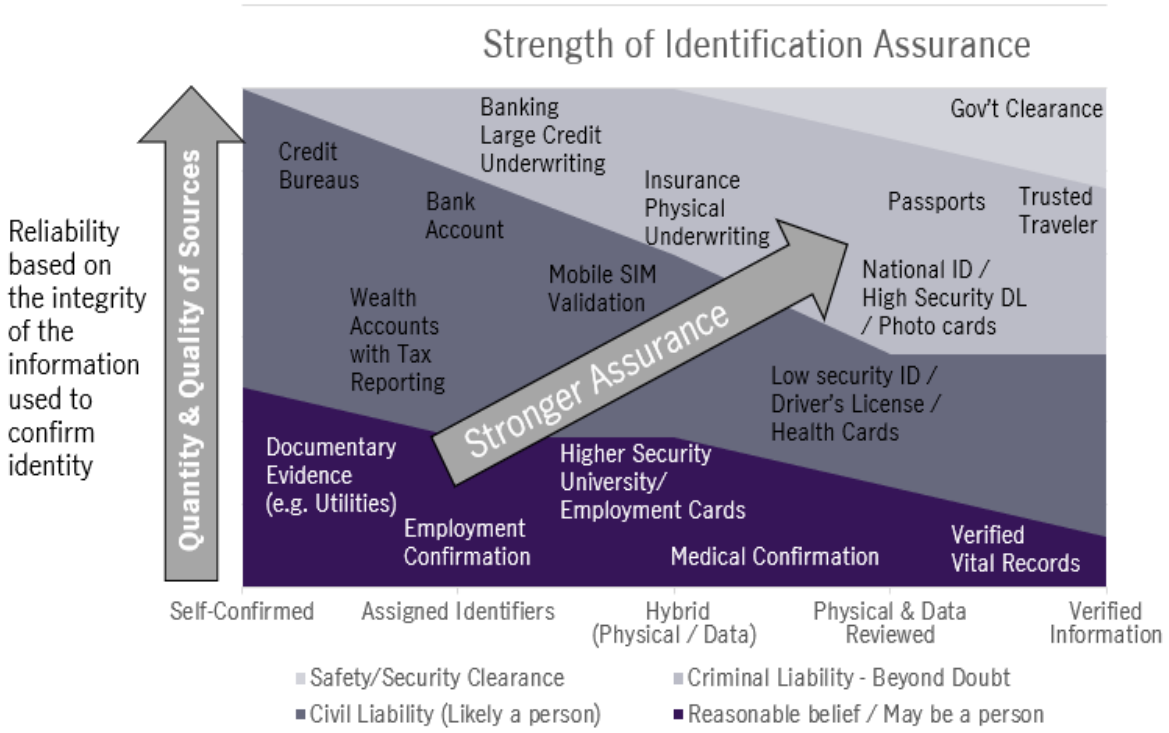
Concept	Question	Answer	Examples
Identity Resolution	How much unique information is needed to resolve a person's existence?	With the growth of population and ability to change names, a combination of name and attributes is required to resolve a unique person.	Name, date of birth, address, and unique ID identifiers are the bare minimum records used. See Appendix B for other fields.
Identity Proofing	How do we establish that a subject is who the subject claims to be?	Both the quantity of sources (attestations) and reliability of records (proof level) contribute to the ability to rely on the identification process.	Trusted sources can attest to a person's identity based on existing relationships and authentication or confirming record integrity to its source or security features.
Identity Assurance	What level of confidence in the identity of the person is needed?	The risk appetite from a false identity or identity takeover would need to be assessed to determine an adequate confidence level. Large case underwriting may be exposed to fraud risk and criminal activity.	As outlined in the following chart, the strength of using combined attestations and proofing provides for higher confidence levels appropriate for the risk level desired.

The following graphic displays the relationship with the attestation of sources compared to the proof level of the attributes used in an identification process to achieve levels of identity assurance and overall reliability.

Example: Government clearance would require both multiple attestations (confirmation of relationships using background checks) as well as a high-proof level (through the validation of records to their sources) for the clearance to be granted.

[10] "Digital Single Market Policy," Trust Services and Electronic Identification (eID), European Commission. https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

[11] Verify allows partner companies to verify the identity of the person for ongoing access to online services. See Guidance Gov.UK Verify at https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.



Source: Author with additional context provided in Appendix A

Authentication – Answering the Question: Is It You?

For existing relationships, to gain the authorization to access an account, a consumer will need to provide attributes to confirm that the consumer is the person who has the relationship with the financial institution.

A "simple" authentication may include providing a card with a PIN number in person, or a username and password with an online session. In both cases, the provider of information will share the attributes of which the provider has control.

These attributes may be items they have (card/token), what they know (personal information), or who they are (biometrics).

Source of Attribute	*Common Attributes Used in Authentication/ID*
Who they are: Physical	Government identification, which includes: age, height, face, eyes, fingers, hair, teeth Used through voice recognition, fingerprint, facial recognition, retina scan
What they have: Acquired, provided, or detected identifiers	Passwords, security questions, taxID, phone #, e-mail, IP#, cell ID #, employee ID, address, and location identifiers
What they know: Relationships and commerce	Name and family, marital status, gender, financial ties, profession, employment, religion, affinity groups, social media

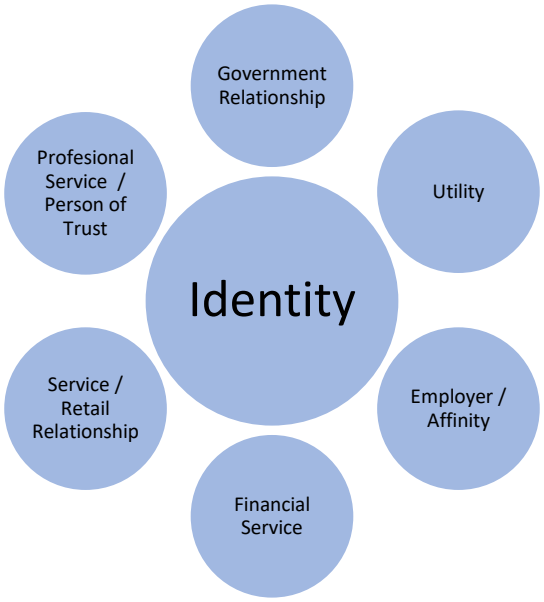
Where enhanced security may be beneficial (e.g., to request a large withdrawal, change an address or phone number), then enhanced authentication or an update of the identification has shown to be critical for managing the added risk of the transaction.

To strengthen the security of communications with customers, financial institutions started to request more information from customers to build makeshift supplementary passwords. This took the form of having customers answer historical, personal questions as a tool when enhanced authentication was needed to authorize higher-risk transactions or account changes. By requesting out-of-wallet information (in case of an identity theft using lost-wallet details), organizations would be able to use familiar information set up by the customer, such as the name of their first dog, first date with a spouse location, or education history. Due to social media, however, many of these private details have entered the public domain, and the strength of this information has had a dramatic reduction in its effectiveness.

Enhanced authentication is also performed in a method called multi-factor authentication, as it relies on multiple communication methods (e.g., phone call, text, mail, conversation), which are used to confirm the person has control of more than one communication channel, as provided during the identification stage.

Reliable Sources of Identification

To be a reliable source of identification information, whether it be a government body, an organization, or a person, it should have the following features:



1) Supports an ongoing relationship and not a one-time service
2) Be in a sector or one which requires strong record-keeping practices and controls for all stages of a customer's lifecycle
3) Only provides identification that has an active and sustained relationship with the person being identified (or list expiry date)
4) Provides traceability to demonstrate the identification is in place and can be relied upon
5) Provides security features to support the authenticity of the record

An alternate form of identification is through non-government trusted sources by leveraging established relationships of the person to resolve the identity and confirm the authenticity of a person. These records may be attestations, financial statements, utility bills, or other sources which, in combination, meet a reasonable person's expectation that the person both exists and the party is that person.

By relying on physical records, a common challenge is to address the risk of fraud by confirming a record is valid when it has been provided by the client. Within digital networks, this is solved with the client's authorization to share a record from one network provider can be passed to another network participant, and delivers a timely and authentic record.

For this paper, *digital identification* will follow the same definition as identification, however, it will have the added requirement that the exchange of information is performed within an electronic session. The traceability of records and information to the reliable source is critical for a process to have a high level of integrity, and it is used to meet regulatory and risk requirements.

How Is a Person Identified Today? Methods and Testing Using Case Studies

Case Studies: Reviewing Identification Records

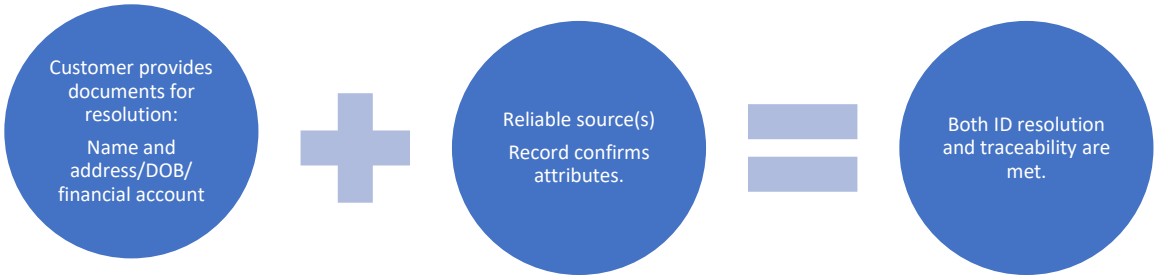
Example 1: To get a birth certificate – Parents present a child in a hospital and request a birth registration.

The recipient performing the identification (hospital) trusts their employees (reliable source) who hosted the birth and has parents (reliable source) to grant a birth registration to the baby. Attributes include the date of birth, parent names, place of birth, and possibly other elements or physical characteristics.

Example 2: To get a driver's license – Person presents birth certificate and other records.

The reliable source (record from the hospital) is provided with attributes (name and date of birth), which are reviewed alongside other records (perhaps citizenship document or parent identification).

Putting It All Together: In-Person Method of Confirming Identity by an Employee or Agent



Testing the Effectiveness of the Collection of Identification and Audit Measures

Required Element(s)	Test(s)
Are procedures and training up to date for employees and agents on identification processes?	Confirm if procedures and training include: i) acceptable forms of identification, ii) how to review identification documents, iii) comparing the identification to the client, iv) documenting the review, and v) escalating any unusual activity.
Are identification records complete when required?	Validate if the records are complete and sample test for accuracy if available: i) identification type, ii) identification number, iii) jurisdiction or source of issue, iv) date of collection, and v) expiry date (confirm if it is after the date of collection).
Does the AML program risk assessment of customers include the quality of identity and risk factors on file?	How many of these sources of identity are on file? i) Government identity records ii) Verified bank account numbers belonging to the client iii) Verified communication channels iv) Confirmation with credit bureau of address and phone number v) Verified employment information vi) Reports to taxation authorities over a taxation cycle
Does the AML program note if communication methods have been verified and are up to date with the customer?	Positive indicators of strong ties to customer attributes: i) Mail delivery without return mail ii) E-mail delivery without return e-mail iii) Phone contact to a number confirmed to belong to the client/employer iv) Text and response to a number confirmed to belong to the client/employer v) Successful website login that resulted in a communication type listed above
Are risk indicators or tools present to detect potential targets of identity theft or account takeovers?	Client identity theft by redirection of communications or funds: i) Multiple contact information sources ii) Common contact information across multiple customers without direct relationships (accountant/lawyer/financial advisor) iii) Common banking information across multiple customers without direct relationships (accountant/lawyer/broker-dealer)
Opportunities for automated controls/tools built to monitor identity resolution	Client profiles not consolidated: Example: Multiple client profiles with the same name, date of birth, and common unique identifiers, such as tax identification numbers/Social Security numbers, to reduce the risk of “shadow accounts” used for identity takeovers or to mask multiple accounts for the same person beyond their financial means

Digital Use Cases: Sovereign Identity

Government Provides an Identity Record or Online Identity Authentication

The use of government-issued physical documentation (e.g., driver's licenses, identification cards, and passports) is the mainstream standard for both the attributes for a unique person with clear identifiers (e.g., document numbers) and the security features to validate their authenticity.

Governments are starting to extend the use of their citizens' and residents' identity records to online equivalent to access government services.[12] These processes are also are beginning to extend into commercial applications, and countries have been assessing the issuing a public key/private key method of Web authentication aligned with new Web standards.[13] The government issue of digital versions of identity documents through mobile applications is a variant of this approach (e.g., U.S. Department of Homeland Security e-Passport).

Digitized Government Identity Method Bottom Line

Pros	Cons
1) Equivalent identity assurance and identity proofing approach as physical identification 2) Uses more security features than a living person can 3) Consumer confidence higher as it is tied to government services	1) Varies by country and functionality 2) Limited interoperability or common standards for international identity 3) Cost to integrate into systems, processes and, people (training)

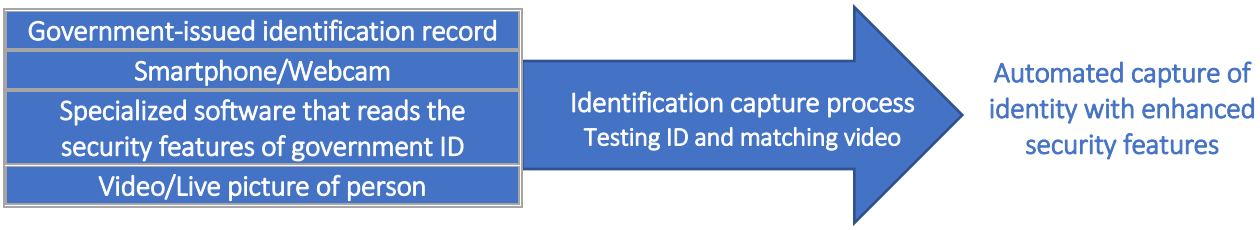
[12] Estonia E-Identity: https://e-estonia.com/solutions/e-identity/id-card/

[13] Web Authentication API (WebAuthn) is a specification with the participation of Google, Mozilla, Microsoft, and others, which allows servers to integrate securely with a public key and private key combination using cryptography for security. See https://webauthn.guide/#looking-ahead. Countries can issue a private key to their citizens and validate the public key combination for any party for which the private key holder would like to have confirmed.

Digital Use Cases: Digitized Identification

Identity Record Capture of Passports, National Identity Cards, or Recognized Identity Cards

Many regulatory technology solutions have been established that have software tools which are able to use mobile camera functionality or webcams to perform a review of the security features of government-issued identity documents and match them to a live person.



Program/Audit Testing for Identity Record Capture Processes

Required Element	Test(s)
Government-issued identification record	1) Validate which government ID is allowed based on risk profile of the customer (Passport and National ID only, or regional and others). 2) Validate if only domestic ID is allowed, or if high-risk countries are excluded, or other factors.
Smartphone/ Webcam	1) Validate that the device has features which connect it to the client with a common device identifier, such as placing a token/tracking code for traceability to identify the hardware for future authentications. 2) Use supplemental tools, such as the ability to review a smartphone's SIM card to confirm the location, telecommunications carrier, and phone number match the client.
Specialized software	1) Confirm the identity security features are utilized in the model. Examples include but are not limited to: • design features of the identification, such as the font type on the identification document, positioning, graphics; • identifier algorithms and length; and • confirmation identity has not expired. 2) Test and ongoing monitoring of the software to confirm it remains current. 3) Has software testing been performed by independent testers to confirm that malicious code has not been implanted?
Video/Live picture of person matching photo	1) Does the software require live video, or can it be compromised with a photo or prerecorded video? 2) Has testing been performed to confirm if videos can beat the test?

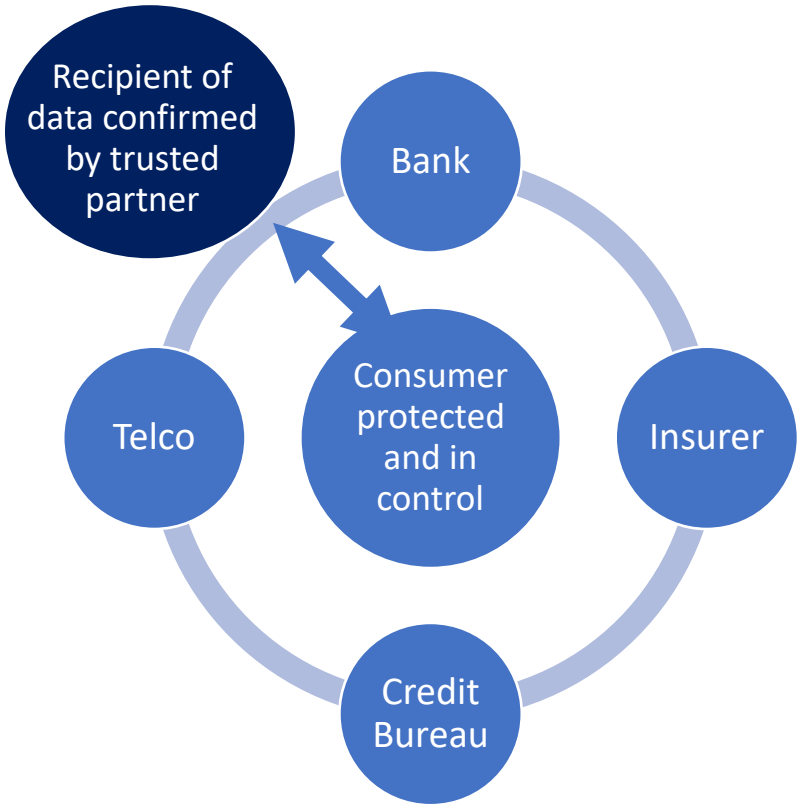
Digitized Identification Method Bottom Line

Pros	Cons
1) Leverages existing physical identification 2) Uses more security features than a living person can	1) May not meet local AML requirements 2) Cost to integrate into systems, processes, and people (training)

Digital Use Case: Federated/Trusted Steward Network Method

Within some technology solutions, a client can authenticate themselves with a trusted source, and then relay this information to another reporting entity (with the client's permission).[14] For example, a person can authenticate themselves through an existing relationship with a telecommunications provider or financial institution, and then authorize their information to be passed onto a secure, federated network of multiple established and trusted recipients. Then through matching a combination of name, address, date of birth, together with other unique identifiers, the person can be verified using other reliable sources, such as government services, credit bureau data, telecommunications, utilities, and financial services accounts in a secure network.

Blockchain Technology Among Trusted Partners to Protect Privacy and Enable Digital ID

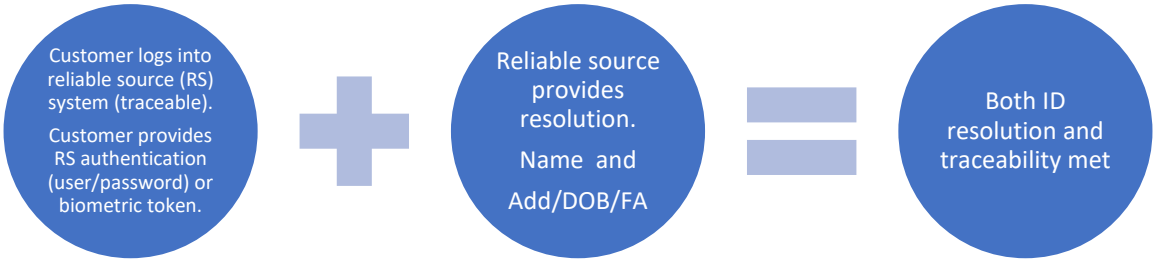


- New tools can provide customers the ability to turn to a trusted partner to confirm their ID with another trusted partner.
- Consumer private information stays within encrypted messages and never at rest outside of a host or participant organization.
- Each information exchange is logged and stored in blockchain tables. The consumer data does not need to be stored as it is traceable within the blockchain for law enforcement as needed.
- Real-time validation with hosts, which can be government or large trusted partners

[14] Examples include Alastria in Spain (https://alastria.io/index_en.html) and SecureKey in Canada (www.securekey.com).

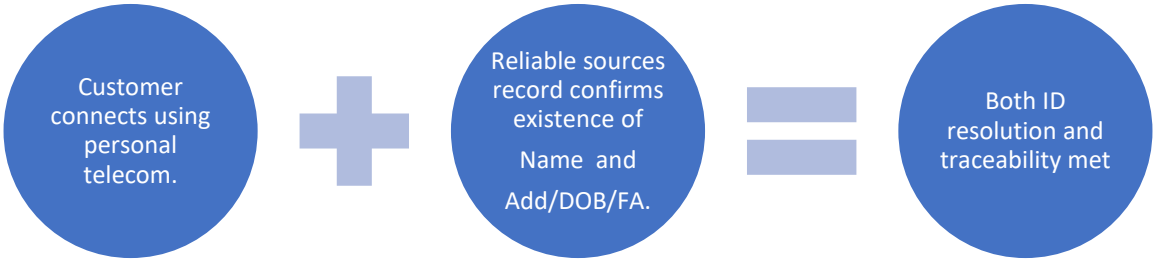
In these cases, the integrity is provided up front, which may raise a concern about the reliance on a trusted source's authentication practices. This can be mitigated by using multiple sources for higher-risk transactions, which would be more challenging for criminals to master.

Aggregator method using open banking as an added tool within a trusted network:



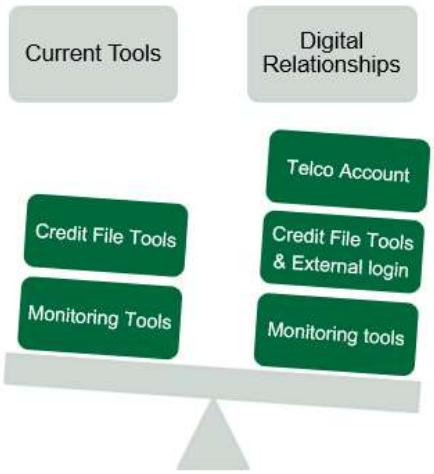
- Customer provides records for traceability and integrity of records (authentication).
- Reliable source provides records for identity resolution.

Aggregator method using cellular or Internet tracing as an added tool within a trusted network:



- Customer provides device, which provides telecom records for traceability (authentication).
- Reliable source provides records for identity resolution and integrity of records.

Beyond identity, these additional tools also reduce fraud risk:



Verified bank accounts: The redirection of funds by providing a new account number can be mitigated by confirming the ownership of the destination account.

Verified mobile device: With an ability to validate the mobile device to enhance authentication capabilities, these new networks will provide added tools to strengthen internal controls.

The addition of the telecommunication validation as well as an easier method to validate the owner of a destination bank account will contribute to a reduction in both account takeover and fraud risk.

Source: Author based on the modern ability of records to be authenticated to sources electronically instead of relying on a review of paper documents

Multiple relationships to reduce synthetic identities:

With the addition of multiple authenticated sources, it will become more challenging for synthetic identities to be maintained and controlled. The integration of government databases and identities with greater physical attributes will provide significant tools to fight the establishment and continuation of synthetic identities.

Program/Audit Testing for Federated/Trusted Steward Network Method

Required Element	Test(s)
What trusted sources are available to be used?	1) Can the source be used to meet local AML identity requirements? 2) Will all of the information required be provided to meet local AML identity requirements?
Quality of identity resolution	1) What attributes will be shared? 2) What is the quality of the attributes to be shared (address standardization, completeness of date of birth, refresh rate of data)? 3) What are the methods of identity resolution matching within the organization and tied to the network?
Traceability of records provided	1) Is a process in place to meet law enforcement requests for traceability of records? 2) Will records meet all requirements needed for customer due diligence assessments and filing suspicious activity reports?

	3) Will detected fraud events be shared across the network without a law enforcement request?
Business continuity	1) Does the business have multiple methods to perform identification? 2) Are there SLAs for availability or uptime, or scheduled down periods of the network?

Digital Use Case: Federated/Trusted Steward Network Method Bottom Line

Pros	Cons
1) Records contemporaneously validated directly with the source(s) 2) Facilitates instant confirmations of relationships with integrity 3) Low customer friction encourages high adoption rate. 4) Low cost encourages integration into steady state processes.	1) Initial establishment of networks needs buy-in from major players. 2) Consumer education and fear of privacy and security breaches 3) Criminal phishing attacks or internal security compromises with trusted stewards may result in loss in consumer confidence.

Conclusions and Recommendations

By studying the impact of the modernization of client identification in combating money laundering and terrorist financing, this paper provided a definition of identification, and outlined the current methods to identify persons using physical and/or electronic records and the approaches to testing these processes.

Innovations in identity management moving from physical to authenticated electronic records will improve record integrity (reduce risk), be more efficient due to reduction in staff time to review documents (reduce cost), and will be easier for the customer through online access (reduce friction).

Through the review of how to assess the strength of identification, a risk-based approach can be used within digital identity tools to apply the right level of risk mitigation by reaching out to newly available, trusted sources of identification (e.g., utilities, banks, etc) to meet the needs of the relationships that financial institutions have with clients.

The ability to test and audit the success of these programs is getting more complex, based on the number of attributes increasing; however, this is offset by improved reliability and completeness of the data, simplifying the building of monitoring tools.

This paper is designed using a case study approach to help the audit and compliance personnel keep pace with the various methods of identification innovations and how to test each one based on their designs.

1) Financial Institutions should assess their identification strategy to determine which method(s) meet their needs and those of their customers. Factors to consider include:
    a. identification at onboarding and potential repetition, based on the activity of interactions with the customer and their risk level; and
    b. privacy and information security risk factors in collecting and managing the information.

2) Having a higher level of identity assurance, reducing fraud risk, and improving our knowledge of our customer can be attained by:
    a. increasing the number and reliability of sources of information,
    b. verifying the attributes to the sources of information (match), and
    c. including identity attributes in monitoring and analytics programs by maintaining traceable records. (These records are also needed for CDD and SAR reporting for AML compliance regimes to be effective and efficient in the execution of programs.)
3) Innovations in technology continue to move rapidly and are responding with rapid adjustments to counteract cybercrime, data breaches, corruption, and organized crime.
    a. The assessment of digital identification tools will continue to change with technology innovations and will need to be revisited periodically with the pace of change.
        i. Attestations from reliable sources (more are better).
        ii. Proof of data (verified are better).
        iii. Traceable records and completeness of attributes are critical.
    b. All identification methods have pros/cons to be considered, monitored, and tested.

In conclusion, leveraging the strength of digital identification methods to improve the integrity of information is a powerful tool to untangle proceeds of crime from legitimate property.

References

Alastria. (2017–2019). Retrieved from https://alastria.io/en/

Cavoukian, A. (n.d.). The seven foundational principles. Privacy by Design Centre of Excellence, Ryerson University. Retrieved from https://www.ryerson.ca/pbdce/certification/seven-foundational-principles-of-privacy-by-design/

Duo Security. (n.d.). WebAuthn: Looking ahead. Retrieved from https://webauthn.guide/#looking-ahead

e-estonia. (n.d.). e-identity. Retrieved from https://e-estonia.com/solutions/e-identity/id-card/

eGoverment and Trust (Unit H.4). (2018, December 12). Trust services and electronic identification (eID). Digital Single Market Policy, European Commission. Retrieved from https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

FATF. (2012–2018). *International standards on combating money laundering and the financing of terrorism and proliferation: The FATF recommendations,* 10(a), 12. Retrieved from http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

FFIEC BSA/AML Infobase. (n.d.). Customer identification program—Overview. *BSA/AML Examination Manual*. Retrieved from https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_011.htm

Government Digital Service. (2019, March 14). Guidance gov.UK verify. Gov.UK. Retrieved from https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2018, June). *Digital identity guidelines*. NIST Special Publication 800-63-3. U.S. Department of Commerce. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

McWaters, R. J. & Robson, C. (lead authors). (2016, August). *A Blueprint for Digital Identity*. World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

Office of Superintendent of Financial Institutions. (2013, October 28). Cyber security self-assessment guidance. Government of Canada. Retrieved from http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx

Schwartz, M. J. (2019, February 19). Wendy's reaches $50 million breach settlement with banks. Bank Info Security. Retrieved from https://www.bankinfosecurity.com/wendys-reaches-50-million-breach-settlement-banks-a-12032

SecureKey. (2019). Retrieved from www.securekey.com

Sovrin. (2019). FAQs. The Sovrin Foundation. Retrieved from https://sovrin.org/faqs/

The World Bank Group. (2018). Figure 2: Document type needed for account opening. *G20 Digital Identity Onboarding*, 2. Retrieved from https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

Appendices

Assessment of Current and Evolving Records of Identification

Identification can be considered the process of establishing the **resolution** of a unique person (either individual or entity) though the use of **attributes** provided by a **reliable source** (i.e., based on trusted record[s] or organization[s]). This table provides some insights on how common forms of identification can be evaluated based on this model.

	Attestation Quantity and Quality of Sources	Identity Proofing: Attribute strength / Physical verifications
Government Clearance	High – multiple sources	High – Validated to attain clearance
Trusted Traveler / Nexus	High – multiple sources	High – Validated to attain status and collect fingerprint/retina
Passport / National ID card	High – multiple forms of supporting documents required	Moderate/High – attributes include facial recognition, height, eye colour, etc.
Underwriting - Bank large case - Insurance large case	Moderate-High – multiple sources commercial validation (limited access to gov't databases)	Moderate-High – financial historical review, limited need to go back >10 yrs
Government functional identification (driver's licenses, health cards, etc.)	Moderate – typically based on two sources	Moderate – dependent on region and security features
Telecommunications SIM validation for mobile	Moderate – gov't ID Low – pay as you go–if no ID	Moderate – gov't ID, traceability to physical address / software relationships
Account with a financial institution (credit, debit)	Moderate – gov't ID and credit bureau typical Low – secured or low-value credit as typically fewer relationships	Moderate – main banking relationships as it includes geolocating of transactions and relationships Low – low-frequency accounts
Wealth management with tax reporting	Moderate – tax reporting plus source of funds from other relationships	Moderate – if in-person relationships Low – if non-face-to-face without compensating controls
University photo Identification or smartcards	Dependent on institution, expected to be moderate due to government taxation reporting and/or validation of international Visa; stronger if tied to verified bank account	Dependent on the jurisdiction to assess if the card acquisition process is tied to a government standard
Documentary evidence (utilities)	Low	Low – tied to a physical residence; can be validated with other sources real time (property registries)
Employee card with photo	Low – single source typically	Moderate – govt ID with photo and security features Low – other ID with photo

Risk Ranking Attributes Used for Identity Resolution and Assurance

To perform enhanced analytics of the identification attributes which financial institutions collect for their clients, the following factors should be taken into consideration:

1) If data is common and likely to have been compromised in large data breaches:
    a. Credit bureau data (outside of Equifax breach, these reports may be on file with multiple financial institutions and subject to internal compromises)
2) If data is in the public domain or can be extrapolated:
    a. Address information or professional directories
3) If data is subject to minor variations:
    a. Naming conventions (space in surname)
    b. Name variants and nicknames
    c. Address non-standardization (suite vs. apartment and town name vs. city name)
4) If data is subject to change:
    a. Address, phone, e-mail, employer updates
    b. Name changes due to life events (marriage, divorce, death of spouse)
    c. Tax ID change due to identity theft

Attribute	Lower Strength	Moderate Strength	Higher Strength
Name – Prefix / Designations	Professional designations which are traceable without image (doctor/ politician / judge)	n/a	Professional designations which are traceable with image (doctor/ politician / judge)
Name – Title	If title matches gender	n/a	n/a
Name – First name (s)	Common name with variety of spelling or slight variance of match	Name with exact match	Unique name with exact match
Name - Middle name (s)	Common name with variety of spelling or slight variance of match	Name with exact match	Unique name with exact match
Name – Last name (s)	Common name with variety of spelling or slight variance of match	Name with exact match	Unique name with exact match
AKA / Maiden name(s)	Common name with variety of spelling or slight variance of match	Name with exact match	Unique name with exact match
Gender / Sex	Exact match	n/a	n/a
Signature (Artwork)	Exact match	n/a	n/a

Attribute	Lower Strength	Moderate Strength	Higher Strength
Age	Year of Birth	Date of Birth (unverified)	Date of Birth (Verified)
Facial recognition	n/a	Match to government ID by person / software tool	Match to government database
Fingerprint match	n/a	Match to pre-authenticated fingerprint on device in control of person	Match to government database
Retina match	n/a	n/a	Match to government database
Domestic tax ID	n/a	Exact match	n/a
Foreign tax ID	n/a	Exact match	n/a
Foreign tax jurisdiction	Exact match	n/a	n/a
Net income amount reported on prior-year tax return as reported to tax authority	n/a	Exact match	n/a
Date of death	Year of death	Date of death (unverified)	Date of death (verified)

Attribute	Lower Strength	Moderate Strength	Higher Strength
Address	General address or subject to care-of or nominee holding	Clear address tied to person using trusted sources	Specific location with address standardization and geolocation
Address validation date	Returned mail, caution	Mail confirmed receipt and not returned to sender over 30 days	Mail confirmed receipt and actioned within last 30 days
Phone number	Mobile carrier match for registered line (not pay as you go)	SIM card validation	SIM card validation combined with mobile location to customer residence
Phone number type	Unknown (note: pay-as-you-go lines may be cautioned if not common in region)	Provided by client and traced to client	Can be confirmed to the client using trusted sources
Phone number validation date	Never verified	Verified more than 5 days ago	Verified within last 5 days
E-mail address	Large free domains, some may not be permissible for secure communication	Utility provided domain verified using one-time password	Large employer or government domain verified using one-time password
E-mail address validation date	Never verified	Verified more than 5 days ago	Verified within last 5 days
Website authentication	n/a	n/a	n/a
Mobile location detection	Same country	Same city as customer	n/a
Internet protocol address	If consistent and not matching employer/large organizations	n/a	n/a
OpenAuth ID (Facebook / Google+)	n/a – TBD	n/a – TBD	n/a – TBD

Attribute	Lower Strength	Moderate Strength	Higher Strength
Government-issued passport identifier collected by a person	Foreign passport, other language	Foreign passport in a domestic language	Domestic passport
Government-issued passport identifier collected by software tools	n/a	Foreign passport	Domestic passport
National ID cards	Foreign national ID card in same language as reviewer	Photo ID without high-security features and issued to all persons	Photo ID with high-security features
Regional ID cards (including, health, driver's, other services functional cards)	No photo or limited security features	Limited security features, however includes photo	High-security features (e.g., photo, hologram, machine encoding)

Attribute	Lower Strength	Moderate Strength	Higher Strength
Spousal name match	Exact match	Exact match and spouse is customer as well	n/a
Spouse tax ID	Exact match	Exact match and spouse is customer as well	n/a
Spouse employer	Exact match	Exact match and spouse is customer as well	n/a
Marital status	Exact match of status (likely public domain)	n/a	n/a
Marital status date	Exact match of date (likely public domain)	n/a	n/a

Attribute	Lower Strength	Moderate Strength	Higher Strength
Bank account number	Handwritten or verbally provided	Pre-printed void check or bank statement	Verified ownership of account (cleared check or direct from bank)
Credit card number(s)	Handwritten or verbally provided	n/a	Verified ownership w/ cleared transaction or authorized transaction
Life underwriting	Identity collected by health professional	Health only underwriting smaller cases	Full financial and health underwriting
Health plans	Health relationship – Therapy services	Health relationship – Pharma	Health relationship – Dental services
Other relationships (Affinity / Loyalty programs / Partner_	Dependent on relationships and program		

Attribute	Lower Strength	Moderate Strength	Higher Strength
Employer Name	Employer not confirmed, provided by client	Confirmed, large employer or executive (likely background search)	Confirmed, Regulated / Government employer
Employer payment of Health Benefits	Not participating	Confirmed, large employer or executive (likely background search)	Confirmed, Regulated / Government employer
Employer savings plan or pension	New employee prior to taxation reporting cycle	Confirmed, large employer or executive (likely background search)	Confirmed, Regulated / Government employer
Employer life underwriting	Built into standard health plan	Confirmed, large employer or executive (likely background search)	Confirmed, Regulated / Government employer

Reference – International Approaches to Digital Identification

Countries are recognizing the benefits of digital identification for enhancing the delivery of government service and economic benefits to commerce while protecting consumers. These references may help your future study in this area.

Trends include:

- technology identification tools that can enhance privacy,
- biometrics joining national ID programs to reduce lost passwords and improve security, and
- ID empowering developing economies and consumers.

Organization / Region	Links
World Bank – ID for development 1) ID4D program 2) Identification for development global dataset	1) ID4D reference 2) ID4D global dataset (2017 inventory of ID worldwide) 3) ID4D technical specification
United Nations: ID-2020 Alliance For digital identity to meet the needs of governments, international organizations, businesses, and individuals alike, it must be:	1) http://id2020.org/ Personal: unique to you and only you Persistent: lives with you from life to death Portable: accessible anywhere you happen to be Private: only you can give permission to use or view data
Asia / Australia / New Zealand: 1) China digital ID pilots: WeChat – Guangzhou region; Alipay – Wuhan region 2) Singapore 3) Australia 4) New Zealand 5) India	1) South China Morning Post overview and PC Mag Overview 2) Singapore National Digital ID framework And myinfo details 3) Australia Framework and Australian Identity Security and Engage Digital Australia 4) New Zealand "RealMe" 5) UIDAI - AAdhaar

Americas 1) U.S. 2) U.S. Aid – International assessment 3) Canada – DIACC	1) National Strategy for Trusted Identities in Cyberspace (NSTIC) and NIST Digital ID 2) Identity in a Digital Age World report and US Blueprint report 3) The Pan-Canadian Trust Framework, a Digital ID and Authentication Council of Canada
Europe 1) Digital single market 2) UK	1) Digital Single Market Strategy 2) Gov.UK.Verify