Exploration of Remote Identity Proofing Alternatives to Knowledge Based Verification

This paper explores current issues and opportunities in remote identity proofing and alternatives to knowledge based verification. This paper was developed by DIACC members The ID Crowd Limited & Digidentity, Commercial in Confidence under an applied research program of the Digital ID & Authentication Council of Canada (DIACC). This paper has been developed for the purpose of enhancing community based knowledge sharing.

Table of Contents

About the Authors

ID Crowd

David Black, Gillan Ward, Julian White, Alastair Treharne

ID Crowd[1] specialises in mitigating business and technology risks relating to identity, helping clients understand how they can better trust their customers and the businesses they transact with. We understand how the concepts of digital identity and trust work together with the various threat vectors including cyber-attack, identity and eligibility fraud. ID Crowd has real-world expertise and experience having defined and delivered population scale trust ecosystems.

Digidentity

Dick Dekkers, Marcel Wendt

Founded in 2008 and based in The Netherlands, Digidentity[2] provides an identity verification and authentication platform to central and local governments, companies and individuals. Digidentity can issue identities up to the highest level of assurance and is certified to provide qualified digital signatures. Through years of extensive international experience and as founding partners of multiple trust eco systems, Digidentity plays a big role in establishing identity standards and frameworks across the globe.

[1] http://www.idcrowd.co.uk
[2] https://www.digidentity.eu/en/home/

About this paper

Information in this report is based on research funded by the U.S. Department of Homeland Security Science & Technology Directorate (DHS S&T). Any opinions contained herein are those of the performer and do not necessarily reflect those of DHS S&T.

For more information, please contact:

Anil John
Technical Director
Silicon Valley Innovation Program
Science and Technology Directorate
US Department of Homeland Security
Washington, DC, USA
anil.john@hq.dhs.gov

This content of this white paper is developed under the governance of the DIACC International Applied Research program. The International Applied Research program connects innovators that align with the DIACC Digital Identity Ecosystem Principles[3] with international applied research funding opportunities. The content of the paper was submitted by SecureKey and does not necessarily reflect those of the DIACC membership.

For more information regarding this program please contact:

Joni Brennan
President of the DIACC
Info@diacc.ca

[3] https://diacc.ca/principles/

Context

Online Identity related fraud is increasing at an alarming rate. Fraudsters are impersonating genuine customers to steal assets as well as defrauding organizations out of goods and services. At the most extreme end, impersonating others to gain access to their physical personal space.

Digital identity could not only mitigate these risks but also bring benefits to organizations including better compliance, greater customer reach, competitive advantages, streamlined secure onboarding processes, whilst protecting their customers and their assets.

Remote verification is the process where an online user proves they are the owner of a claimed digital identity. This has typically involved asking questions from credit agency files. Such files are prone to breaches and this paper outlines less susceptible alternative strategies for remote verification.

Management Summary

Data breaches are becoming more frequent; these breaches undermine the integrity of confirming the identity of an individual using knowledge based verification as private attributes, held by organisations, relating to an individual inevitably become more widely available. Thus allowing criminals to more easily masquerade as another individual. This research studied five alternatives to traditional knowledge based verification, to determine whether they are both viable verification methods and less susceptible to data breaches than traditional methods:

- Machine Readable Travel Document biometric features comparison and US driving license biometric features comparison verify an individual by the user taking a selfie which is then compared to a biometric image held on a document associated with the claimed identity.
- Mobile subscriber check and Verification against Financial account verify the individual by demonstrating that they are in control of an account or device that is associated with the claimed identity.
- Verification against financial transactions utilises knowledge based verification from a highly dynamic source associated with the claimed identity.

The research analysed the issuance processes, security features, verification steps and availability of validation sources. The study determined that all methods are credible identity verification alternatives to traditional knowledge based verification and warrant further detailed investigation.

Problem research aimed to solve

The technical challenge with knowledge based verification is that it is almost entirely based upon the premise of “what the user knows”, the key objective is to bind the entity to the claimed identity. This relies on some fact both parties know what was exchanged/created during a previous interaction. This information may be held by the authority with whom the user previously transacted or by an authoritative source. For instance, a user may set up an overdraft facility with their bank using knowledge based verification questions from a data aggregator such as a credit reference agency.

Knowledge based verification relies on the integrity of the underlying information; a data breach may result in facts becoming available to unauthorised third parties. Such breaches may be the result of a mass attack on a data source or obtained from the individual via a compromised device, the result of poor data hygiene or a targeted phishing attack. A fraudster may have access to the personal mail of the individual in a shared residence, which may compromise any information sent in the post, such as that on a statement from a financial institution. This can result in a fraudster masquerading as the individual and gaining access to personal data such as healthcare records.

Knowledge based questions may often be too complex for the user; a reliance on data aggregators mean that the questions may be impossible for the subject to answer, for instance the name of a credit card provider may not be recognised due to branding differences, or because the parent company, rather than the contracting entity is referenced.

Issues with current knowledge based verification methods

The technical challenge with knowledge based verification is that it is almost entirely based upon the premise of “what the user knows”, the key objective is to bind the entity to the claimed identity. This relies on some fact both parties know what was exchanged/created during a previous interaction. This information may be held by the authority with whom the user previously transacted or by an authoritative source. For instance although the user may set up an overdraft facility with their bank the questions may come from a data aggregator such as a credit reference agency.

Knowledge based verification relies on the integrity of the underlying information; a data breach may result in facts becoming available to unauthorised third parties. Such breaches may be the result of a mass attack on a data source or obtained from the individual via a compromised device or targeted phishing attack. A fraudster may have access to the personal mail of the individual in a shared residence, this may compromise any information sent in the post such as that on a statement from a financial institution. This can result in a fraudster masquerading as the individual and gaining accessing to personal data such as healthcare records.

Knowledge based questions may often be too complex for the user; a reliance on data aggregators mean that the questions may be impossible for the subject to answer, for instance the name of a credit card provider may not be recognised due to branding differences.

Knowledge based questions should ideally rely on a diverse pool of information across the individual’s lifestyle events; the use of data aggregators results in a focus on financial products, this data was originally not developed for identity but for financial risk assessment, so there are limitations to breadth and depth of data. However the individual has many other interactions, often at either a Federal or Local Government level. Large scale, complex integration is often required In order to ensure data diversity across these datasets in order to present a diverse set of knowledge based questions.

Mitigating known issues

In order to bring the proposed innovation to Identity verification one needs to simplify the verification question to "is the entity asserting the evidence the true owner of the asserted identity". This can be achieved by matching attributes and features from valid and genuine evidence to the entity asserting the evidence. This is done millions of times each day when a user is asked to present ID; the features on their ID are compared with those belonging to the individual, be that by a Police office, Border control officer or liquor store owner.

The proposed innovation will remove the risk of data breach by using secure methods that will not only ask for "what you know" but may also check "what you own". Solutions include checking biometric or photographic information on government issued documents including passports or driving licenses and utilising challenge and response methods using Chip and PIN technology.

These innovations are relevant and significant to the need to find alternatives to knowledge based verification as they will remove the risk of a data breach compromising an Identity verification process by establishing a strong link between the asserting entity and the claimed identity. This is accomplished by relying on strong evidence issuance processes and robust controls. The risk of fraudulent evidence being asserted is mitigated through innovative controls that ensure the evidence is both genuine and valid.

The proposed innovation is relative to the state of the art developments since the continual development of secure methods of identity is essential to border security and counter terrorism given both the Government and its adversaries are increasingly reliant on technology. These developments ensure:

- Identity evidence has strong issuance processes
- The Identity evidence is strongly bound to the individual through the comparison of elements from the evidence to the individual
- The physical evidence is tamper proof
- The evidence has strong methods to avoid counterfeits through watermarks, fonts etc.
- The evidence can be checked as valid and genuine in the field using low cost accessible technology

The proposed methods for remote verification for online government services can leverage these features as well as the trust established by these controls to ensure the integrity and security of the transaction. This will make sure that personal information is only disclosed to the correct individual and that US citizens, the US Government and its employees are protected from fraud.

This proposed work is of major importance as the provision of any online service brings threats; the assumed assurance that comes with a face to face transaction is replaced by risks: The risk of fraud, the risk of deception and the risk of personal or organisational data loss.

Bulk data breaches are becoming more common and reported more often; the increased awareness of these breaches should bring about better controls and behavioural changes. However the arms race with the fraudsters is ongoing, both parties adapt and evolve to gain the upper hand. Therefore one must accept that total trust and assurance is not going to be possible; threat and risk assessments together with the resulting level of assurance must accept that a certain degree of residual risk will always remain.

A study of the “Dark Web” will reveal that there is a marketplace within the criminal community, not only for credentials and financial assets such as credit card details, but also information that may undermine knowledge based verification. There is also a market for identity assets such as passport and driving licence details. Therefore there is a constant need to strengthen the controls to determine the real identity owner is the person asserting their identity.

The methods proposed by this exercise had to be resilient to threats such as data loss, masquerading and counterfeiting, they must also be extensible to cope with the ongoing arms race. Yet they need to strike a careful balance with usability and affordability so that they can be implemented successfully at population scale.

Research methodology

The Phase I R/R&D proposes five or more methods of verification that provide proof that the person asserting the identity is the rightful owner of the identity. The candidates will be drawn from a number of areas:

- Methods and datasets that exist in practice, these will be closely aligned to the methods and datasets that exist in other international trust ecosystems.
- The analysis of methods and datasets utilised a qualitative assurance processes. This structure allowed them to determine the technical feasibility of an approach and determine whether it can mitigate known threats, for example:
- Identity evidence had to have properties that enabled it to be remotely checked to determine whether it is valid. These might include unique reference numbers and attributes linked to the claimed identity than can be checked against an issuing or authoritative source. This mitigates the risk of invalid evidence being asserted, e.g. lost, stolen or revoked documents. This also binds the evidence to the claimed identity.
- Identity evidence may have a photograph/image/biometric of the subject allowing remote comparison of the person asserting the evidence in real time. This mitigates the risk of a third party impersonation of the claimed identity.
- Identity evidence may contain counter fraud features that enable a remote application to determine whether it is genuine, e.g. fonts and watermarks. This mitigates the risk of counterfeit evidence being asserted.
- Identity evidence may contain cryptographically protected information on a physical document (e.g. RFID in passports, EMV Smart Cards) which can be checked using appropriate readers which are accessible to the general public.

For each proposed method a series of detailed questions was posed. This resulted in the analysis of the underlying controls, features and use cases. This assessment determined what level of assurance can be achieved by the method, how technically feasible the solution is and an outline view on effort required to commercialise the method at population scale.

For example, a method may include the assertion of the physical document such as a passport and how this is remotely checked as valid, genuine and belonging to the individual. To answer this question one needs not only to look at the features and controls associated with the evidence but also its issuance process, the supporting systems, the integration challenges, the risks associated with the method and threat being mitigated by the method.

The following questions were used during the analysis; other technical questions may emerge as further detailed analysis is undertaken:

- What is the issuance process associated with any evidence used in the proposed method? Was an identity check performed as part of the issuance process? Can it be assumed that the evidence was delivered into the possession of the individual? Does the issuance process fulfil the requirements of other regulations such as anti-money laundering legislation? Does the issuing source maintain an accessible dataset that can be interrogated during the identity verification process to check for revoked, lost or stolen documents?
- Does the method use physical evidence or cryptographic methods that demonstrate that the person to whom the evidence relates, is in possession of the evidence at the time that the evidence is being asserted?
- Does the method rely on information known only to the person asserting their identity? What are the risks of this information being compromised? Is the method vulnerable to attack from social engineering or phishing? The use of physical evidence that may contain a digital, biometric or photographic link to the person should mitigate the risk of a user being a victim of such attack. For instance a challenge/response dialog using a chip and PIN (EMV) bank card will require the user to have in their possession the card, a suitable reader and knowledge of the PIN. In theory this PIN is only known to the cardholder, however it could have been compromised through phishing or skimming techniques or be known to the subject’s spouse or partner.
- Can the evidence be checked as valid? Does the evidence have a unique reference number that relates solely to the evidence or the person to whom it was issued? Can this reference number be checked against an issuing or authoritative source? Can this check be made in real time? Can the source corroborate biographic information asserted by the person such as name, date of birth and address?
- Can the evidence be checked as genuine? Does the evidence have physical or cryptographic features that can be remotely checked? Are these controls documented in the public domain to allow commercial development of these checks?
- What national and international counter fraud sources are available to determine whether the claimed identity and/or the asserted evidence has not been subject to Identity fraud?
- Does the method use non Federal, individual State issued assets such driving licenses? What are the risks, issues and constraints when attempting to integrate to multiple issuing sources across numerous jurisdictions? Are Federal initiatives required to coordinate or possibly implement infrastructure to enable remote validation of these evidence types?
- Does the method rely on integration with non-governmental third party commercial providers to access their methods and/or datasets? These might include but is not limited to payment provider networks, mobile network operators and credit reference agencies.
- Does the evidence contain biographic and/or biometric information protected by cryptographic means that can be checked remotely? For instance a passport may hold a photo and biographic information on a RFID chip that can be interrogated using a NFC reader on a mobile device. This information can be compared to the information and photo being asserted by the person claiming the identity. There is scope for innovation to mitigate the low ownership of suitable NFC capable mobile devices.

- If the method includes a physical object, then is there a requirement for proprietary knowledge or equipment to reproduce it?
- Are the underlying processes that support the method scalable? Do they involve human interaction that might result in scale issue at times of peak demand, for instance approaching tax filing deadlines?
- Does the method assume that only the subject has access to a device used during the verification process? For instance an SMS message meant for the subject could be intercepted by a work colleague or a family member with access to the physical mobile device, or an SMS is shared across platforms (such as Apple).
- Can the integrity of a channel used in the method be guaranteed? These might include compromised browsers, intermediate platforms and networks (including non 3G/4G mobile phone networks).
- How adaptable is the method in the event of a breach or if an underlying system and/or process is compromised?

Should a piece of evidence, method and/or dataset meet the above criteria then it becomes a suitable candidate for further research. The evaluation was structured to eliminate non-viable approaches early in the process. Each approach must be eligible to stand as both a technical and commercial offering.

Key Deliverables

For each of the five methods of verification the following was delivered:

- A description of the technical solution in terms of use cases, information flows, validation checks, genuine checks, cryptographic checks and contra-indicator checks.
- A description of the methods by which the evidence can be assessed as valid. This may include checks against an issuing or authoritative source.
- A description of the methods by which the evidence can be assessed as genuine, this may include cryptographic checks using suitable readers.
- A description of the evidence properties including the required features to mitigate specific threats. This will include unique identifiers, identity attributes, biometric features, cryptographic features and counter fraud features.
- A description of the issuance process for the specific evidence whether:
- An identity check was performed as part of the issuance process and It can be assumed that the evidence was delivered into the possession of the individual.
- An initial assessment of the relative strength of the evidence and associated methods based upon the technical process, evidence features and issuance processes.
- A description of any offline verification processes including utilisation of a face to face channel.
- Any knowledge gained during the evaluation and productization of this method for use within other Government schemes.
- A commercialisation strategy based upon scalability, sustainability, deliverability, affordability and constraints such as data protection and privacy. Commercial applications may include the potential for not only government services but also commercial services. The re-use of identity will become one of the key elements for the digitisation of services. It is therefore important to be cognisant of these forthcoming demands and ensure they are addressed in the eventual commercial strategy.

Method 1: Machine Readable Travel Document biometric features comparison

Biometric feature comparison between a user and their US or non-US travel document	
Use Case	Machine Readable Travel Document (MRTD) compliant with ICAO 9303[4]
Use Case ID	IDC-DIGI-001
Use Case Level	Function
Description	The method enables the comparison between the biometric features on an ICAO compliant travel document (the MRTD) and a captured real time image (the selfie) of the person (the user) asserting their identity. This covers US and non-US passports, passport cards and identity cards. This will verify to a level of certainty[5] that the user is the rightful owner of the identity stated by the biographic details on the MRTD. The method involves the use of technology in a mobile device or kiosk to capture the biometric image of the user either as a photograph or, if the phone or kiosk is equipped with Near Field Communications (NFC), reading the image from the document's RFID chip (if available and functioning correctly). The user then takes photographs of themselves which are compared with the image from the MRTD and a liveness check will be executed.
Pre-condition(s)	The MRTD must be an ICAO 9303 machine readable travel document (MRTD) that contains a photograph/image of the person to whom it relates. The MRTD should have a chip that contains the biographic and biometric details of the person to whom it relates. The MRTD must be issued by an authority that is recognised and trusted within the jurisdiction of the organisation that is proofing the user. The MRTD must have security features that can be checked to determine whether the document is genuine and has not been tampered with.
Success Post-condition(s)	Various controls have determined that: – The document is genuine and has not been tampered with – Details from the MRTD have been confirmed as valid by comparison with information held/published by the Issuing Source/Authoritative Source – The biometric traits on the selfie are from a living person rather than an artificial or lifeless person (e.g. a photo or mask) – There is a strong likeness between the biometric image on the MRTD and the selfie taken by the user.

[4] https://www.icao.int/publications/pages/publication.aspx?docnum=9303

[5] Highly likely, but not certain. Twins, siblings or just lucky doppelgangers are still a risk.

Failure Post-condition(s)	MRTD is not genuine: on inspection of the physical MRTD it was determined it did not appear to be genuine. MRTD may be lost, stolen or revoked: The MRTD matched a record that implies it may be lost, stolen or revoked. MRTD matched a known fraudulent document: The identifiers and biographic details from the MRTD have been matched to a record for the same document type that is known and/or suspected to be involved with document fraud. Identity fraudster: The biographic from the MRTD has been matched to a record of a person that is known, or suspected, to be involved with identity fraud.
Primary Actors	User making the application.
Secondary Actors	User browser, agent (kiosk), human document inspector, human biometric features comparator, automated document inspector, automated biometric features comparator.
Non Functional	Transparent functionality, performance, minimal delays to user, security.

MAIN SCENARIO	
Trigger	Service requires the user to verify their identity.
Step 1. The user obtains an app on a suitable device to undertake the verification process. This maybe in response to a prompt from an online desktop session, from an existing mobile session or out of band prompt (phone, in person, email, post etc.). The user links the app with existing service. There is also an option to capture the evidence details in an in-person environment (kiosk). Step 2. The user enters or captures the attributes from the MRTD required e.g. document number, given names, date of birth, document expiry date etc. Step 3. The system determines that the physical evidence is genuine. Step 4. The system checks that the MRTD is valid. Step 5. The user captures an image of themselves using the camera feature on the mobile device through the app (Selfie) or in a kiosk environment. Step 6. The system makes a remote comparison between the captured image of the user and the biometric image held on the MRTD. Step 7. If all checks are successful the identity verification system confirms the asserted identity to the relying party.	

Method 2: US driving license biometric features comparison

Checking attributes and biometric information held on a driving license	
Use Case	Using a US driving license as identity evidence
Use Case ID	IDC-DIGI-002
Use Case Level	Function
Description	This method enables the comparison between the user asserted identity attributes and those held on a driving license in addition to a comparison between the biometric image of the user and the image held on the driving license. This will verify to a level of certainty[6] that the user is the rightful owner of the identity stated by the biographic details on the driving license. The method has variances depending on upon the issuing state; the variable elements are dependent on a number of factors: – The issuance process – The security features on the license – The ability to validate the attributes on the license with an authoritative or issuing source. Some licenses may not be suitable due to exceptions to any of the these factors.
Pre-condition(s)	The issuance process for the license complies with the REAL ID requirement set out in the REAL ID act. The document must have physical multi-layered security features compliant with REAL ID; the templates for these features must be available for implementation within the solution. The photo on the license must comply with ISO/IEC 19794-5:2005(e) [7]requirements. The issuing state must have made available a real time interface to check the validity of the document (is the license reference number valid and/or has it been revoked, lost or stolen?).

[6] Highly likely, but not certain. Twins, siblings or just lucky doppelgangers are still a risk.

[7] https://www.iso.org/standard/38749.html

Success Post-condition(s)	Various controls have determined that: – The document is genuine and has not been tampered with – Details from the license have been confirmed as valid by comparison with information held/published by the Issuing Source/Authoritative Source – The biometric traits on the user’s photographic image are from a living person rather than an artificial or lifeless person (e.g. a photo or mask) – There is a strong likeness between the biometric image on the license and the image of the user (e.g. a selfie taken by the user).
Failure Post-condition(s)	The license cannot be used as identity evidence due to the aforementioned constraints. The license is not genuine: On inspection of the physical license it was determined it did not appear to be genuine. The license may be lost, stolen or revoked: The license matched a record that implies it may be lost, stolen or revoked. The license matched a known fraudulent document: The identifiers and biographic details from the license have been matched to a record for the same document type that is known and/or suspected to be involved with document fraud. Identity fraudster: The biographic from the license has been matched to a record of a person that is known, or suspected, to be involved with identity fraud.
Primary Actors	User making the application.
Secondary Actors	User browser, agent (kiosk), human document inspector, human biometric features comparator, automated document inspector, automated biometric features comparator.
Non Functional	Transparent functionality, performance, minimal delays to user, security.

<table>
<tr><td colspan="2"><b>MAIN SCENARIO</b></td></tr>
<tr><td><b>Trigger</b></td><td>Service requires the user to verify their identity.</td></tr>
<tr><td colspan="2">Step 1. The user obtains an app on a suitable device to undertake the verification process. This may be in response to a prompt from an online desktop session, from an existing mobile session or out of band prompt (phone, in person, email, post etc.). The user links the app with the existing service. There is also an option to capture the evidence details in an in-person environment (kiosk).
Step 2. The user asserts the issuing authority (state) and the issuance date of the license.
Step 3. The system checks that driving licenses from this issuing authority issued on and after the issuance date:
– Have been issued in accordance with the requirements of the REAL ID act
– Have security features in accordance with the requirements of the REAL ID act
– Can be checked against known document templates to determine the license is genuine
– Can be checked as valid against a authoritative or issuing source.
If any of these are negative then the user is advised that the license cannot be used as evidence and an alternative method is proposed.
Step 4. The user captures an image of the front and (if required) rear of the license.
Step 5. The system extracts the required document and biographic attributes either through optical character recognition, from a barcode or Machine readable zone (if present on rear of document).
Step 6. The system determines that the physical evidence is genuine.
Step 7. The system checks that the license is valid.
Step 8. The user captures an image of themselves using the camera feature on the mobile device through the app (Selfie) or in a kiosk environment.
Step 9. The system makes a remote comparison between the captured image of the user and the biometric image held on the license.
Step 10. If all checks are successful the identity verification system confirms the asserted identity to the relying party.</td></tr>
</table>

Method 3: Mobile subscriber check

Verifying claimed identity against mobile subscriber attributes	
Use Case	Checking the claimed biographic attributes against the subscriber details of a mobile device in the possession of a claimant.
Use Case ID	IDC-DIGI-003
Use Case Level	Function
Description	This use case verifies a user's asserted identity attributes by comparing them with those associated with their mobile phone contract. A mobile phone containing a sim card associated with the user's account is confirmed to be in the possession of the user through the issuance of a one time passcode in an SMS message across the mobile network The mobile operator matches the user's phone number and asserted identity attributes against their own internal records. A number of contra-indicator checks are also undertaken to ensure that the mobile device and/or contract have not been compromised.
Pre-condition(s)	The claimant has a mobile phone contract with a participating mobile network operator (MNO). The issuing authority (MNO or representative sales agent) confirmed the applicant's identity through an identity checking process. It can be reasonably assumed that the SIM card related to the mobile phone contract has been delivered into possession of the person to whom it relates. The mobile contract is linked to the same biographic attributes as those asserted by the entity claiming the identity. The mobile contract is solely associated with the entity claiming the identity. A mobile device containing a SIM card linked to the mobile contract is in the possession of the entity claiming the identity.
Success Post-condition(s)	Various controls have determined that: The asserted biographic attributes match the biographic attributes associated with the mobile device that is in possession of entity claiming the identity. No significant contra-indicators exist that may indicate that the mobile channel, device or account has been compromised.

Failure Post-condition(s)	The mobile device and account cannot be used as identity evidence due to the following constraints: The user's mobile operator does not participate The mobile contract issuance process does not have sufficient strength The user is unable to enter the correct one time password sent to their mobile device The identity attributes asserted by the user do not match those held by the mobile network operator A contra-indicator indicates that the mobile channel, device or contract may have been compromised.
Primary Actors	User claiming the identity, the mobile device, the SMS gateway, the mobile network operator data sets, the mobile network, the identity verification system.
Secondary Actors	User browser, issuing or authoritative sources of data.
Non Functional	Transparent functionality, performance, minimal delays to user, security.

MAIN SCENARIO	
Trigger	The relying party service requires the user to verify their identity.
Step 1. The user selects their mobile operator from a constrained list on the identity verification system. Step 2. The user inputs their mobile number and biographic attributes to the identity verification system. Step 3. The identity verification system generates a one-time passcode and sends it to the user’s mobile device via an SMS aggregator. Step 4. The user enters the one time passcode into the identity verification system which is confirmed as correct. Step 5. The identity verification system sends the asserted mobile number and identity attributes to the relevant the mobile network operator. Step 6. The MNO operator confirms a match to the identity verification system and confirms that the mobile network contract and issuance process is of sufficient strength. Step 7. The asserted mobile number is checked against fraud and risk services to ensure no issues exist. Step 8. If all checks are successful the identity verification system confirms the asserted identity to the relying party.	

Method 4: Verification against Financial account

Verifying the ownership of a financial account under the control of the user	
Use Case	Checking the claimed biographic attributes against a financial account under the control of a claimant.
Use Case ID	IDC-DIGI-004
Use Case Level	Function
Description	This verification method demonstrates that the claimed identity attributes are associated with a financial account over which the claimant has control. The control is demonstrated by the claimant being able to log onto their online system for the financial account and retrieving a one-time passcode.
Pre-condition(s)	The claimant has a financial account that has been issued in accordance with anti-money laundering regulations. The issuing authority has confirmed the applicant's identity through an identity checking process.
Success Post-condition(s)	Various controls have determined that: The asserted biographic attributes match the biographic attributes associated with the financial account under the control of the entity claiming the identity. No significant contra-indicators exist that may indicate that the bank account has been compromised.
Failure Post-condition(s)	The financial account cannot be used as identity evidence due to the following constraints: – The financial account issuance process does not have sufficient strength – The user is unable to enter the correct one time password associated with a transaction in their financial account – The identity attributes asserted by the user do not match the attributes associated with the asserted account details – A contra-indicator indicates that the bank account may have been compromised
Primary Actors	User asserting the claimed identity, the financial payments network, the financial institution holding the financial account, the institution's online system to check their account, issuing or authoritative sources of data. The identity verification system.
Secondary Actors	User browser
Non Functional	Transparent functionality, performance, minimal delays to user, security.

MAIN SCENARIO	
Trigger	The relying party service requires the user to verify their identity.
Step 1. The user asserts their biographic details to the identity verification system (name, address, date of birth, historical name; and address values if less than 3 years). Step 2. The user asserts their financial details to the identity verification system (account number, routing details for a bank/checking account or credit card details). Step 3. The identity verification system checks against threat intelligence sources to determine whether the account is known to be associated with fraud or the card is reported lost or stolen. If there is a risk then the process is halted and the identity verification system informs the relying party. Step 4a. The identity verification system validates against an authoritative or issuing source that the account details are associated solely to the biographic details of the user. Step 4b. If DOB or full name cannot be validated in the previous step then the identity verification system should validate the biographic details of the user against an authoritative source. Step 5. The identity verification system makes a small payment into the asserted financial account across the payments network using an electronic funds transfer facility. A one time passcode (OTP) is assigned as the transaction reference details. Step 6, The identity verification system maintains some form of user persistence in order to allow the user to return and enter the OTP at a later date. Step 7. The user checks the online system for the designated bank or credit card account for the payment and OTP. Step 8. The user enters the OTP into the identity verification system. Step 9. If all checks are successful the identity verification system confirms the asserted identity to the relying party.	

Method 5: Verification against financial transactions

Verification utilising recent transactions on a credit card	
Use Case	Verification of individual using credit card transaction data, checking the user is the owner of a specific credit card through a challenge response sequence of questions based upon the transactions recorded for a credit card known to be linked to the Claimed Identity.
Use Case ID	IDC-DIGI-005
Use Case Level	Function
Description	Checking the user is the owner of a specific credit card through a challenge response sequence of questions based upon the transactions recorded for a credit card known to be linked to the Claimed Identity.
Pre-condition(s)	The organisation that has issued the credit card has confirmed the Claimed Identity through an identity proofing process that is compliant with the relevant anti money laundering requirements.[8] The issuing process for the credit card means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates. The credit card contains a PAN that uniquely identifies the person to whom it relates. A series of credit card transactions exist that allow a solution to undertake a series of challenge/response questions with the credit card owner. These transactions have been graded as high, medium and low strength.
Success Post-condition(s)	Various controls have determined that: The credit card is confirmed as valid and linked to the biographic attributes asserted by the user by comparison with information held by the Issuing Source/Authoritative Source The person asserting the credit card attributes can be assumed to be the owner of the identity associated with the credit card as they have answered sufficient questions relating to transactions on the card correctly.

[8] https://www.protiviti.com/sites/default/files/united_states/insights/guide-to-us-aml-requirements-6thedition-protiviti_0.pdf

Failure Post-condition(s)	The credit card cannot be used as identity evidence due to the following constraints: – Wrong type of card: The issuance processes for the card are insufficient (prepaid etc.) – Non participating issuer or authoritative source: The card type denotes that either the issuing or authoritative source does not provide a method to check transactional data – The credit card attributes are not valid: failed LUHN check – The credit card has expired, card has been revoked, card has been reported lost or stolen – The authoritative or issuing source cannot match the asserted attributes (primary account number) and user asserted biographic details (name, address, date of birth) in their records – The credit card matched a known fraudulent document: The identifiers and biographic details from the card have been matched to a record for the same document type that is known and/or suspected to be involved with fraud – The user failed to answer the questions relating to the transactions on the card and there is a risk they are not the Claimed Identity.
Primary Actors	User making the application
Secondary Actors	User browser, issuing or authoritative sources of data.
Non Functional	Transparent functionality, performance, minimal delays to user, security.

<table>
<tr><th colspan="2">MAIN SCENARIO</th></tr>
<tr><td><b>Trigger</b></td><td>Service requires the user to verify their identity.</td></tr>
<tr><td colspan="2">Step 1: The user selects the type of card from a constrained list of cards where the issuing or authoritative source provides a service to allow the user to confirm the details of a recent transaction through a challenge response session. A negative response terminates the use case with a “unable to continue” outcome to the relying party.
Step 2: The user asserts their biographic attributes (name, address, date of birth).
Step 3: The user asserts the Primary account number (PAN[9]), security code and expiry date of a credit card that has been issued in their name and to the address they previously asserted.
Step 4: The solution checks issuer identification number (IIN) on the credit card to determine that the card is the correct type (not prepaid, joint account); A negative response terminates the use case with a “unable to continue” outcome to the relying party.
Step 5: The solution checks that the PAN passes a LUHN[10] check; a negative response terminates the use case with a “failure” outcome to the relying party.
Step 6: The solution checks with an issuing or authoritative source to determine whether a record exists that matches all the credit card and the card holder’s biographic attributes. The solution checks that the card is only linked to that individual. A negative response terminates the use case with a “failure” outcome to the relying party.
Step 7: The solution checks the issuing or authoritative source to determine that the credit card has not been previously associated with credit card fraud, revoked, reported lost or stolen. A negative response terminates the use case with a “failure” outcome to the relying party.
Step 8: The solution checks an authoritative source to determine whether asserted identity has been associated with identity fraud; if a positive response is returned then the level of risk is raised which will impact the amount of challenge/response questions raised.
Step 9: The solution determines the amount of questions based on the level of assurance in the user’s identity required by the relying party and the mitigation of any conditions resulting from the previous checks.
Step 10: The solution establishes a session with the authoritative or issuing source and submits the card attributes.
Step 11: The authoritative or issuing source validates the details and returns the number of questions available and their grading. If insufficient questions are available, the solution terminates the use case with a “unable to continue” outcome to the relying party.
Step 12: The solution requests a specific grade question from the authoritative or issuing source based upon its knowledge based questions strategy.
Step 13: The user is presented with the question and submits their answer.
Step 14: The solution submits the user’s answer to the authoritative or issuing source which checks it and returns a fail or pass based upon specific criteria (for example tolerances)
Step 15: The solution determines whether further questions are required based upon a predetermined strategy.</td></tr>
</table>

[9] https://en.wikipedia.org/wiki/Payment_card_number

[10] https://en.wikipedia.org/wiki/Luhn_algorithm

Comparison of Features

Method	Verification Method	Issuance Process	In person identity check undertaken at issuance?	Evidence issued to owner of identity?	Physical or Cryptographic features	Evidence contains security features to determine evidence is genuine	Validation source available	Proprietary knowledge or equipment required to reproduce physical evidence
Method 1: Machine Readable Travel Document biometric features comparison	Remote comparison of biometric features against asserted reference image (selfie)	Document issued in accordance to international standards (ICAO)	Yes	Yes	Physical photo and subject image on NFC chip on document	Physical checks - templates available Cryptographic checks against NFC chip	Country by country interfaces available to check valid, lost and stolen - not available in US to commercial entities	Yes
Method 2: US driving license biometric features comparison	Remote comparison of biometric features against asserted reference image (selfie)		Yes	Yes	Physical photo on document	Yes - AAMVA best practice guidance for physical security features, however No central repository for templates to allow physical checks	AMVA Driver's License Data Verification (DLDV) does not check lost and stolen	Dependent on security features implemented at an individual State level
Method 3: Mobile Subscriber Check	One time passcode verified against device known to be associated with asserted identity	Contract issued using industry counter fraud best practice	Yes	Yes for new contracts	SIM card associated with contract in mobile device	Yes - ability to send SMS to mobile device across mobile network	GSMA Mobile ID Gateway available but currently not implemented by US MNO's	N/A
Method 4: Financial account check	One time passcode verified against account known to be associated with asserted identity	Account issued in accordance with AML regulations	Optional depending on risk profile and state regulations	N/A - check made against account held at issuing source	N/A - check made against account held at issuing source	N/A - check made against account held at issuing source	Limited commercial availability to validate bank details	N/A
Method 5: Financial transactions	Knowledge based questions from transactions from account known to be associated with asserted identity	Card issued in accordance with AML regulations and counter fraud best practice	No	N/A - check made against account held at issuing source	N/A - check made against account held at issuing source	N/A - check made against account held at issuing source	Commercial checks available against credit files for credit card numbers	N/A

Method	Binding of individual to evidence	Counter Fraud sources available	Requirements for Federal, State or International assets	Adaptable in the event of a breach	NIST 800-63A Evidence Strength	NIST 800-63A Validation	NIST 800-63A Verification	Domestic demographic considerations	Key risks
Method 1: Machine Readable Travel Document biometric features comparison	Strong biometric comparison against image protected by cryptographic controls.	Non available commercial in the US. some international countries have online or phone based checking services	State International	Certificate revocation lists issued by ICAO for in country breaches Lost, stolen revoked checking services available for certain countries	Superior	Crypto: Superior VIZ: Strong	Crypto: Superior VIZ: Strong	40% of US Citizen have passports Ability to read NFC chip currently limited to Android devices	Risk of fraudulently obtained documents from countries with compromised issuance processes.
Method 2: US driving license biometric features comparison	Medium biometric comparison as there is a risk of photo substitution on document	No	State		Strong	Strong	Strong	65% of US population have a drivers license Only 23% of states apply REAL ID standards to issuance process	Risk of counterfeit documents
Method 3: Mobile Subscriber Check	Medium as device or channel could be under control of 3rd party	No	N/A	SIM cards can be re-issued to individual	Strong	Fair	Fair	95% of US population own a mobile phone. 93% of these are not prepaid	Risk of account take over via sim swap or SS7 vulnerability.
Method 4: Financial account check	Medium as account credentials could be in possession of 3rd party	Yes	N/A		Fair	Fair	Fair	93% of US population have a checking account	Risk of masquerading due to weak issuance process. Risk of account takeover via weak help desk processes Risk of phishing for credentials to access online statement
Method 5: Financial transactions	Medium as account credentials could be in possession of 3rd party	Yes	N/A	Source data renewed on regular basis - monthly statements	Fair	Fair	Fair	55% of US population have at least one credit card	Risk of masquerading due to weak issuance process. Risk of account takeover via weak help desk processes Risk of phishing for credentials to access online statement

Appendix A: NIST 800-63A[11] - Strengths of Identity Evidence

Strength	Qualities of Identity Evidence
Unacceptable	– No acceptable identity evidence provided.
Weak	– The issuing source of the evidence did not perform identity proofing. – The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the applicant. – The evidence contains: – At least one reference number that uniquely identifies itself or the person to whom it relates. **OR** – The issued identity evidence contains a photograph or biometric template (of any modality) of the person to whom it relates.
Fair	– The issuing source of the evidence confirmed the claimed identity through an identity proofing process. – The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates. – The evidence: – contains at least one reference number that uniquely identifies the person to whom it relates. **OR** – contains a photograph or biometric template (any modality) of the person to whom it relates. **OR** – can have ownership confirmed through KBV. – Where the evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. – Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it. – The issued evidence is unexpired.

[11] https://pages.nist.gov/800-63-3/sp800-63a.html#sec5

Strength	Qualities of Identity Evidence
Strong	– The issuing source of the evidence confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. Such procedures are subject to recurring oversight by regulatory or publicly-accountable institutions. For example, the Customer Identification Program guidelines established in response to the USA PATRIOT Act of 2001 or the Red Flags Rule, under Section 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act). – The issuing process for the evidence ensured that it was delivered into the possession of the subject to whom it relates. – The issued evidence contains at least one reference number that uniquely identifies the person to whom it relates. – The full name on the issued evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names The: – Issued evidence contains a photograph or biometric template (of any modality) of the person to whom it relates. **OR** – Applicant proves possession of an AAL2 authenticator, or equivalent, bound to an IAL2 identity, at a minimum. – Where the issued evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. – Where the issued evidence contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it. – The evidence is unexpired.

Strength	Qualities of Identity Evidence
Superior	– The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Such procedures are subject to recurring oversight by regulatory or publicly accountable institutions. – The issuing source visually identified the applicant and performed further checks to confirm the existence of that person. – The issuing process for the evidence ensured that it was delivered into the possession of the person to whom it relates. – The evidence contains at least one reference number that uniquely identifies the person to whom it relates. – The full name on the evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. – The evidence contains a photograph of the person to whom it relates. – The evidence contains a biometric template (of any modality) of the person to whom it relates. – The evidence includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed. – The evidence includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it. – The evidence is unexpired.

Appendix B: NIST 800-63A - Validating Identity Evidence

Strength	Method(s) performed by the CSP
Unacceptable	– Evidence validation was not performed, or validation of the evidence failed.
Weak	– All personal details from the evidence have been confirmed as valid by comparison with information held or published by an authoritative source.
Fair	– The evidence: – details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s). **OR** – has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified. **OR** – The evidence has been confirmed as genuine by trained personnel. **OR** – The issued evidence has been confirmed as genuine by confirmation of the integrity of cryptographic security features.
Strong	– The evidence has been confirmed as genuine: – using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified. **OR** – by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified. **OR** – by confirmation of the integrity of cryptographic security features. – All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
Superior	– The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features. – All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

Appendix C: NIST 800-63A - Verifying Identity Evidence

Strength	Identity Verification Methods
Unacceptable	– Evidence verification was not performed or verification of the evidence failed. Unable to confirm that the applicant is the owner of the claimed identity.
Weak	– The applicant has been confirmed as having access to the evidence provided to support the claimed identity.
Fair	– The applicant’s ownership of the claimed identity has been confirmed by: – KBV. **OR** – a physical comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in [SP 800-63B, Section 5.2.3.]. **OR** – biometric comparison of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to all requirements as specified in [SP 800-63B, Section 5.2.3.].
Strong	– The applicant’s ownership of the claimed identity has been confirmed by: – physical comparison, using appropriate technologies, to a photograph, to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in [SP 800-63B, Section 5.2.3.]. **OR** – biometric comparison, using appropriate technologies, of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Biometric comparison performed remotely SHALL adhere to all requirements as specified in [SP 800-63B, Section 5.2.3.].
Superior	– The applicant’s ownership of the claimed identity has been confirmed by biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity, using appropriate technologies. Biometric comparison performed remotely SHALL adhere to all requirements as specified in [SP 800-63B, Section 5.2.3.].

Conclusions

The paper identifies five viable methods of remote verification. Each can mitigate the risks of data breaches, have strengths in the issuance processes and security features of the underlying evidence. The verification methods range from fair to superior when mapped against NIST 800-63A Digital Identity Guidelines for Enrolment and Identity Proofing.

Further research will need to be undertaken to determine the viability of these from a usability, demographic, commercial, privacy and technical perspective.

Contact Us

For further information about the topics discussed in this paper, or to join the DIACC community, visit https://diacc.ca or contact: info@diacc.ca