DIRECTORY OF PRODUCTS THAT ASSESS IDENTIFICATION DOCUMENTS AND VERIFY IDENTITY

The Directory of Products that Assess Identification Documents and Verify Identity ("The Directory") is designed to provide industry with information on solutions that provide a service which confirms the authenticity of the government photo identification and matches the result to the image or video of a person.

The Directory is based on service providers who have completed a self-attestation of survey questions designed to gauge the extent to which their solutions are aligned with DIACC's Digital Identity Ecosystem Principles.

Background and why is this important.

In June 2019, Canada's regulatory environment moved to accepting innovative technologies to allow for reporting entities to use identification document capture and comparison tools to meet the requirements of anti-money laundering efforts. Reporting entities include Banks, Insurers, Securities, Realtors, Accountants, Notaries, Dealers in precious metals and money services businesses that are required to identify persons in a business relationship (plus other requirements). Additional tools to perform identification in a digital channel remain available using the credit bureau information and dual records from other reliable sources (e.g., Utility providers or regulated financial services).

Stakeholders and Benefits.

For service providers, this Directory provides awareness of the new Canadian marketplace expectations and new customers. The addition of these markets to start using applications to assess identification documents and verify identity is expected to expand the demand for digital identity solutions in Canada.

For consumers, more choice in how they provide identification. This empowerment of a new wave of sophisticated tools currently in use around the world may empower Canadian commerce to reduce customer friction and provide a secure tool for a person to both provide and access their own information and property.

For reporting entities; a centralized list of service providers and the start of an assessment process. To adopt these tools, reporting entities (for example banks, insurers, and security dealers) will be required to perform a risk assessment and document this exercise prior to use of the technology in their anti-money laundering programs. This survey will include many of the common questions used in the assessment of digital identification tools from an anti-money laundering perspective.

The Directory will be hosted by the DIACC and available free of charge to meet the objectives listed above. The Directory will also be provided to regulatory bodies to raise awareness of innovations in the marketplace available for regulated reporting entities to use. Membership in the DIACC is strongly encouraged for service providers and those interested in supporting the digital identity community in Canada.

DISCLAIMER

The information contained in the Directory is for general information purposes only. While DIACC endeavours to keep the information up to date and correct, DIACC makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, certification or compliance status, suitability or availability with respect to the Directory or the information, products, services, or related graphics contained on the Directory for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

In no event will DIACC, and its members, be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of the Directory.

A. ABOUT THE SERVICE PROVIDER

A1. Please provide a brief description about your company: (250 words) *

Shufti Pro is an AI driven digital KYC/AML/KYB service provider for identity verification that uses a combination of artificial intelligence and human intelligence to enable automated verification solutions that surpass its competitors. Businesses looking for efficient digital identity verification and authentication solutions can benefit from real-time, global services.

Shufti Pro provides a multi-layered risk cover against digital identity fraud, money laundering, and terrorist financing. Verifications are completed within 30-60 seconds, with global coverage to verify the identity documents in 150 languages. Its services are currently utilised in 230+ countries and territories. AML screening is performed against 1700+ watch lists.

Know Your Customer (KYC) Services include face verification, document verification, address verification, 2factor authentication, consent verification. In addition, ongoing AML, AML for business, Know Your Business (KYB) and Biometric Sign-in services through facial recognition are all offered to a global clientele. The new addition to the services is video KYC for the financial industry and touch-less biometric authentication for airport security clearance. A2. Please provide a brief description about your ID Capture technology: (250 words) *

Shufti Pro performs its ID verification through its sophisticated AI algorithms, in which it verifies the liveness of the person and then compares it against the photo on the official document. This process is carried in any of the two ways:

Onsite Verification

On-site verification means that Shufti Pro will be interacting directly with the end-user and will be responsible for data collection in order to perform Identity verification. Shufti Pro customers will only be notified about the verification status via Shufti Pro Back Office.

Shufti Pro offers following services in On-site verification: (Face, Document, Address, Consent, Phone and Background Checks)

Off Site Verification

Offsite Verification means that Shufti Pro will not be interacting with the end-user and Shufti Pro customers will be responsible to collect and provide verification data. Shufti Pro Customer will provide us with the proofs (images/videos) to complete user verification.

Shufti Pro offers following services in Off-site verification: (Face, Document, Address, Consent and Background Checks)

The Verification is performed through the following steps:

Capture: End-user uploads or takes photo of of ID document in real-time

Extract: Shufti Pro extracts pre-defined information from the ID document with OCR

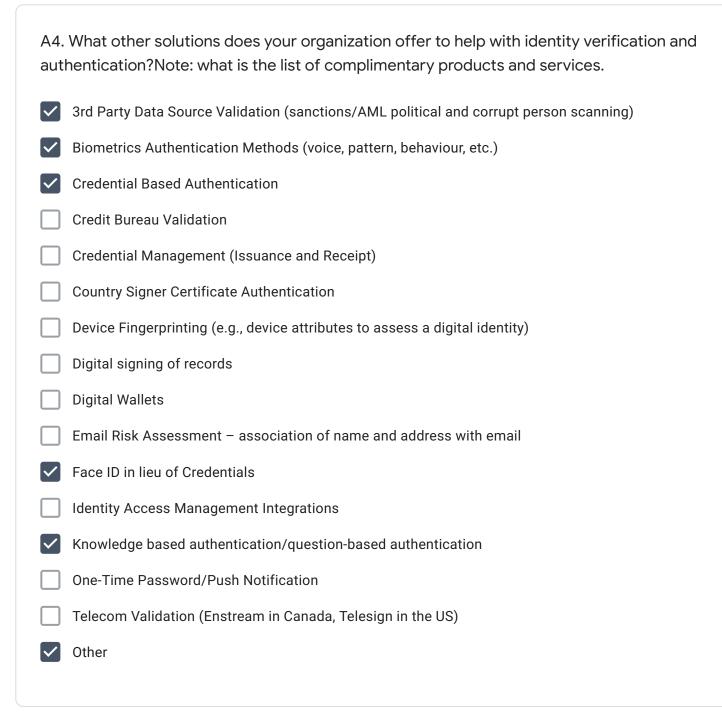
Screen: ID document format and information is verified and results are sent via API or back office Shufti Pro uses AI-based OCR engines that combine both artificial intelligence and OCR technology to transform a document into a machine-readable and editable digital format. Traditional OCR engines aim to analyse a document in the form of an image by detecting based on patterns if the image contains text and then extracts the text into a machine-readable format. This helps convert scanned documents into a digitally editable format while comparing the images of the available characters to the ones stored on its database for traditional OCR engines. A3. Please provide a brief description about complementary products or services: (250 words)

Shufti Pro provides multiple fraud prevention solutions for KYC purpose including SP's face verification service, in which Shufti Pro's AI systems check for Micro Expressions, 3D Depth Analysis, Liveness Detection, Anti-spoofing Checks, Fake Image Detection, Human Face Attributes analysis, and AI mapping techniques. Through the assistance of AI, the whole procedure takes just under 10 seconds and results are delivered with an accuracy rate of over 98%.

Furthermore, Shufti Pro's AI-backed Optical-Character-Recognition (OCR) technology can extract information from any structured or unstructured document. This service is customizable and clients can even specify which information to extract. OCR is an extremely accurate and fast way of extracting information and can reduce our client's operational costs.

For Address Verification, Shufti Pro uses at least two ID documents, which can be Bills, Bank Statements, ID cards, passports, etc, to verify the address. The data is obtained from pictured documents through our OCR technology.

Moreover, Shufti Pro's Video-KYC service enables our clients to perform remote on-boarding of their clients and this would aid the FinTech sector in particular.



Additional Comments

A5. Please list any other service providers which include your technology which are available in Canada (indirectly able to use your service).

https://shuftipro.com/customers

A6. Please provide your contact information for inquiries related to this survey including websites, emails, social media or other methods. *

https://shuftipro.com/ sales@shuftipro.com https://www.facebook.com/TheShuftiPro/ https://linkedin.com/company/shufti-pro https://twitter.com/Shufti_Pro https://twitter.com/Shufti_Pro https://github.com/shuftipro https://github.com/shuftipro

A7. Please provide a link to any blog posts which may be available about your company (please include DIACC Spotlights or blog posts as well).

https://shuftipro.com/blog/why-shufti-pro-is-perfect-for-digital-verification

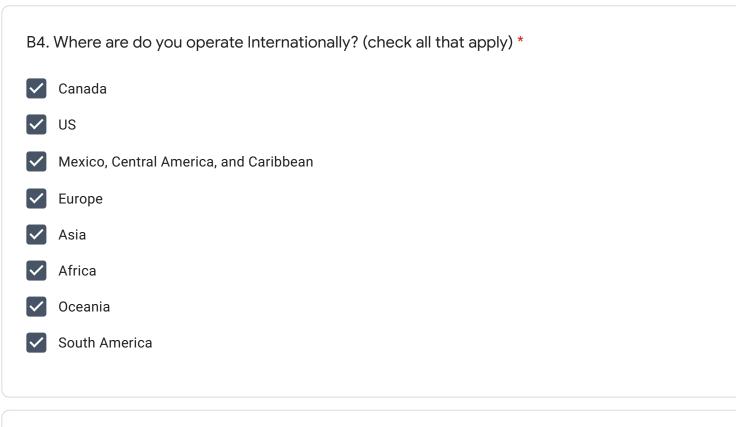
B. ROBUST, SECURE, SCALEABLE

Digital identity solutions must be robust enough to ensure it is secure, available, and accessible at all times. Full time services access also requires redundancy and disaster recovery tools.

Yes

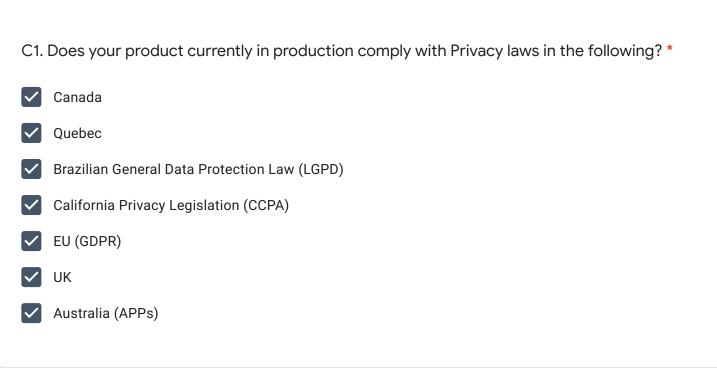
No No

B1. Is the organization a member of the DIACC? *
Not a member
O Considering Membership
O Board Level
Sustaining
O Adopting
B2. Is your model self-attested to be compliant with the Pan-Canadian Trust Framework [™] (PCTF)? To learn more about the PCTF, please contact <u>info@diacc.ca</u> *
O Yes
In progress
O Undecided
Not planning on it
B3. Does the organization participate in IdentityNORTH Conferences?



Additional comments

C. IMPLEMENT, PROTECT, AND ENCHANCE PRIVACY BY DESIGN



Additional comments		
D. INCLUSIVE, OPEN, AND MEETS BROAD STAKEHOLDER NEEDS		
D1. Which languages does your application support? (check all that apply) *		
English		
Canadian French		
✓ Other		
D2. Which languages do you provide technical support in? (check all that apply) *		
English		
Canadian French		
Other		
D3. Does your application design address web content accessibility guidelines and is certified to: *		
WCAG (Web Content Accessibility Guidelines)		
WCAG 2.0 (ISO/IEC40500)		
WCAG 2.1		
Been tested to Ontario's AODA compliance		
Not Yet		
✓ Other		

Additional comments
E. PROVIDES CANADIANS CHOICE, CONTROL, AND CONVENIENCE
E1. In addition to Canadian passports and driver's licenses issued by provinces, territories and the Canadian department of defence, does your application currently support. (Note: Canadian citizenship card not added to the list as there are limited security features (e.g., no barcode and not reissued since 2012). The laminated (certificate Indian Status card) does not have a barcode or security features and accordingly, is not recommended for this process). *
Ontario Health card (only to be used for health purposes)

Quebec Health card

Provincial Photo ID cards (Alberta, Manitoba, New Brunswick, Newfoundland, Labrador, Nova Scotia, Ontario, Prince Edward Island, British Columbia, and Saskatchewan)

Canada/US Nexus (Trusted Traveller)

Canadian Permanent Resident card

Secure Indian Status card

In Process

E2. Globally, how many countries or regions can your service assess Passports (for example: 150)

195

E3. Globally, how many countries or regions can your service assess National ID cards (for example: 100)

230

E4. Globally, how many total identification records* can your service assess? (Example: *includes above and other records, 1000)

3000

E5. Globally, how many countries or regions can your service assess Driver's Licenses (for example, 500) Note: if a jurisdiction has 3 versions of the same Driver's License, please only count it as 1 jurisdiction for this question

230+

Additional comments

F. BUILT ON OPEN STANDARDS-BASED PROTOCOL

Digital identity solutions must be robust enough to ensure it is secure, available, and accessible at all times. Full time services access also requires redundancy and disaster recovery tools.

F1. On which platforms are your solutions available? (check all that apply) *

- Apple App store
- Google app store
- Windows/Microsoft application
- Embedded within client's application
- In-person scanner hardware
- Not at this time
- Other

F2. Please list all Accreditations, Certifications, and Standards that your organization complies with (check all that apply) *		
FIDO® Certified		
HIPAA - Self-attestation to meet the requirements of Health Insurance Portability and Accountability Act (USA)		
ISO/IEC 27001 - an international standard for information security management		
ISO/IEC 27018:2019 - Code of practice for protection of personally identifiable information (PII) in public clouds		
ISO 30107-3 - Biometric Presentation Attack Detection		
NIST 800-63 series - Self-attestation to meet the requirements of NIST Digital Identity guidelines		
SOC 2 Type 1 (at point of time) - Service Organization Control		
SOC 2 Type 2 (over a 6-month period) - Service Organization Control		
Not at this time		
✓ Other		
F3. Does the solution utilize open standard protocols such as: *		
OAUTH2		
OPENID CONNECT 1.0		
SAML		

Not at this time

Additional comments

G1. Confirm if you have an imaging standard for photos and facial capture (check all that apply) \star
Passport Image Standard (ISO IEC19794-5)
PNG
JPEG
GIF
TIFF
Proprietary standards
✓ Other, please describe
Additional Comments
PDF, JPG
H. COST EFFECTIVE AND OPEN TO COMPETITIVE MARKET FORCES
H1. What is the cost-model? (check all that apply) *

Flat fee for time period

Pay per use model

- Mixed model of flat fee and usage
 - Other

Additional comments

H2. What size of organizations have adopted your vendor's solution(s)? (check all that apply) *

- Government and public sector
- ✓ Large organizations (Over 500 employees)
- Small organizations (Under 500 employees)
 - Consumer direct
 - Other

Additional Comments

I. ABLE TO BE INDEPENDENTLY ASSESSED, AUDITED, AND SUBJECT TO ENFORCEMENT

I1. How does the application capture the image of a live person? (check all that apply) *

- Via computer webcam picture
- ✓ Via computer webcam video
- ✓ Via computer webcam interactive video
- ✓ Via mobile device picture
- ✓ Via mobile device video
- ✓ Via mobile device interactive video
- Other

I2. Does the application perform a liveness detection or genuine presence test and how? (check all that apply) *			
Yes, actions to be performed by person (active liveness check)			
Yes, live video capture and/or motion detection (passive liveness check)			
Yes, session can be reviewed by a live human checker			
Not at this time			
Other			
I3. Does the application read the machine-readable portion of the photo identification documents as applicable? *			
• Yes, recorded and used for validation (the information read from the machine-readable portion is compared to the text on the identity document)			
Yes, recorded only without validation			
O No			
I4. Does the application read the facial biometric (ICAO 9303) NFC chip of machine-readable passports? (check all that apply) *			
Android ready now			
Android within next 3 months			
Apple ready now			
Apple ready within 3 months			
Not at this time			
Other			

I5. Does the application verify that the chipped ID document has been authenticated? (e.g., Country signer, Active Authentication, etc.)? *	
• Yes	
O No	
I6. Does the application connect with any government sources to confirm the legitimacy of the record? *	
Yes	
No No	
I7. Does the application check to confirm the expiry date of the document is not prior to the date of the validation? (As applicable; a requirement from Canadian Anti-Money Laundering regulations) *	
• Yes	
O No	
18. Does the application test the algorithm (if applicable) for the unique identifiers against the ones used by the identification document provider? *	
Yes, when applicable (e.g., Ontario Driver's License has the first letter of the identification number	

matching the first letter of the surname)

No No

19. Is the application able to parse the following data fields needed for relying parties to use the process for Anti-Money Laundering requirements in Canada? (Note: The fields for AML requirements in Canada as follows: name, address (if on document), date of birth, reference number of identification document, expiry date, date and time of identification validation, type of identification, jurisdiction of identification document, and country of identification document). *

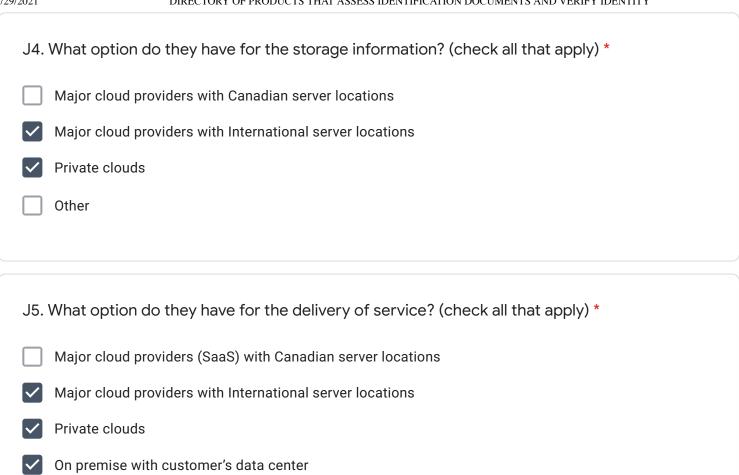
$oldsymbol{O}$	Yes
0	No

I10. What physical identification security features does your solution test against a database of expected results? (check all that apply) *
Character spacing
Ocument size
Document modifications (e.g., cut corner)
Document shape
Font position
Font size
Font type
Holograms
Image frequency
Image positioning
Image size
Markers (logos, symbols or watermarks) positioning
Markers (logos, symbols or watermarks) size
Position and size of magnetic stripe
Raised lettering
Ultraviolet images
Other
Additional Comments

J. MINIMIZES DATA TRANSFER BETWEEN AUTHORITATIVE SOURCES AND WILL NOT CREATE NEW IDENTITY DATABASES

1/29/2021	DIRECTORY OF PRODUCTS THAT ASSESS IDENTIFICATION DOCUMENTS AND VERIFY IDENTITY
J1. '	Where is the identification information ultimately stored? (check all that apply) *
	By the person being identified (e.g., stored digital identity on their device)
	By the vendor on behalf of the subject (e.g., Identity network stores the encrypted access of the digital identity for the person being identified)
	By the vendor as directed by the entity receiving the identification information (e.g., financial institution)
\checkmark	By the entity receiving the identification information (e.g., financial institution)
	Any of the above
	Other
	Does the information stay within Canada for the entire session for Canadian issued ntification (e.g., in transit not related to storage)? *
0	Yes
	Νο
J3.	Does the ID network encrypt all information in the mobile application in transit? *

$oldsymbol{O}$	Yes	
0	No	



- Mobile Integrations (Customer within their own app via SDK)
- Mobile Integrations (Vendor application) \checkmark
- Web Integrations (Customer within their own app via SDK)
- Web Integrations (Vendor application)
 - Other

Additional comments