DIRECTORY OF IDENTITY MANAGEMENT AND PROOFING PRODUCTS

Time to complete: Approximately 15-20 minutes

The Directory of Identity Management and Proofing Products ("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. a

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)

iProov is the world leader in passive face biometric verification and authentication technology.

iProov verifies the genuine presence of people asserting their identity online. Using patented face biometric technology which is inclusive, trusted and secure.
Tested to national security standards and trusted by the UK Home Office, Singapore Government, Australian Government and the US Department of Homeland Security.
iProov's enterprise solution with SaaS infrastructure has been designed for scalability and resilience, with proven ability in real-world environments where high levels of uptime and capacity are required to handle millions of verifications.
Government organizations, Financial Institutions, Healthcare and Digital Service Identity Providers rely on iProov to securely and effortlessly authenticate their citizens and users. iProov is proud to have been awarded many industry awards.

Our Science and Innovation team, which includes over 10 Ph.D.s, use the latest in AI and machine learning for biometric assurance alongside cutting-edge academic research and techniques to solve real-world problems. Their work includes; Advanced Machine Learning, Behavioral Science, Optics, Computer Vision, and Cryptography. External academic researchers are regularly involved in assessments and enhancements of our systems.

An intellectually rich company, iProov regularly assesses and protects its assets. We strive to deliver the most advanced technology available to safeguard organizations. Patent protection upholds the value and credibility of our products and technologies, ensuring they cannot be copied by other providers who cannot deliver the platform, infrastructure, compliance, and governance vital to underpinning advanced threat mitigation technology.

A2. Please provide a brief description about your ID Capture technology: (250 words)

Organizations must offer a fully digital customer experience. One of the areas of highest risk for a digital service is onboarding. The risk of enrolling, and subsequently granting access to the wrong person can incur significant financial loss, impact regulatory compliance, or lead to social disruption.

iProov authenticates the genuine presence of a remote user online, replacing the need for in-person identity checks, making the process more secure and convenient.

iProov Genuine Presence Assurance® (GPA) Technology for onboarding provides the highest level of assurance for remote onboarding and integrates with best-of-breed document capture partners to scan documentation to offer an end-to-end remote identity verification capability. The face image sourced either optically (OCR) or electronically (NFC), from biometric photo ID documents (typically passports), non-

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.

biometric photo ID documents, or centralized databases (e.g. government) is securely passed to iProov to ensure that the image matches the face of the person asserting their identity remotely. In addition, liveness detection and assurance of genuine presence checks are completed. This series of activities ensure that the person asserting their identity is the right person and not an impostor, a real person and not a presented spoof such as a mask or video recording and is authenticating right now and not a synthetic or digitally injected attack.

GPA uses patented Flashmark™ technology, which creates a one-time biometric with controlled illumination to verify that the user is a real person and authenticating right now, and critically, that they are not an injected replay or synthetic video attack.

A3. Please provide a brief description about complementary products or services: (250 words)
In addition, to GPA for onboarding, iProov offers a suite of secure biometric authentication solutions:

iProov Genuine Presence Assurance Technology for authentication
Patented multi-dimensional solution verifies a person's face against a pre-enrolled biometric template, and assures that an online customer is the right person, a real person, and is authenticating right now using a reassuring ceremony that delivers secure, effortless, and passive authentication.

iProov Liveness Assurance™ (LA) Technology for authentication
Patented 3D solution combines camera imagery and contextual data to verify a person’s face against a pre-enrolled biometric template, and assures the online customer authenticating is a real person and confirms that they are the right person using a simple, low ceremony, passive biometric authentication experience.

iProov Flexible Authentication
Unique Flexible Authentication capability enables organizations to invoke a simple back-end flag to select the iProov technology of choice to meet the organization's risk appetite or perceived threat level. Transaction-based assurance selection enables flexible business rules, to suit varying risk appetites with a consistent interface, single compact SDK integration, simple procurement, and cloud-based security.

iProov Palm Verifier
Provides secure, discrete, and contactless authentication without the need for specific hardware. Accurately enrolls and verifies the person's palm. Users simply hover their palm above their device and Palm Verifier will authenticate them in seconds.

iProov for Kiosks
Provides secure authentication in low security, unsupervised or semi-supervised locations such as shopping centers or travel hubs. Ensures maximum accessibility and inclusion, as citizens and customers without a smartphone or a computer can access services.

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.

A4. What other solutions does your organization offer to help with identity verification and authentication?
Note: what is the list of complimentary products and services.

☐ 3rd Party Data Source Validation (sanctions/AML political and corrupt person scanning)
☒ Biometrics Authentication Methods (voice, pattern, behaviour, etc.)
☐ Credential Based Authentication
☐ Credit Bureau Validation
☐ Credential Management (Issuance and Receipt)
☐ Country Signer Certificate Authentication
☐ Device Fingerprinting (e.g., device attributes to assess a digital identity)
☐ Digital signing of records
☐ Digital Wallets
☐ Email Risk Assessment – association of name and address with email
☒ Face ID in lieu of Credentials
☐ Identity Access Management Integrations
☐ Knowledge based authentication/question-based authentication
☐ One-Time Password/Push Notification
☐ Telecom Validation (Enstream in Canada, Telesign in the US)
☒ Other

Additional comments
Other - iProov can be used for the remote identity verification for many of these use cases

A5. Please list any other service providers which include your technology which are available in Canada (indirectly able to use your service)
WorldReach
Acuant
Microblink
InnoValor
Jumio
Treefort

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

Website: www.iproov.com
Email address: leigh.day@iproov.com or contact@iproov.com
Social media: https://www.linkedin.com/company/iproov/, https://twitter.com/iProov #iProov #GenuinePresence
Phone: +1 (231) 201 6944
Other method: https://vimeo.com/user110608533
Contact Person: Leigh Day

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.

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://www.iproov.com/resource-hub
https://diacc.ca/2020/07/15/spotlight-on-iproov/

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.

B1. Is the organization a member of the DIACC? (multiple choice)

- ☐ Not a member
- ☐ Considering membership
- ☐ Board level
- ☒ Sustaining
- ☐ 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 info@diacc.ca (multiple choice).

- ☒ Yes
- ☐ In progress
- ☐ Undecided
- ☐ Not planning on it

B3. Does the organization participate in IdentityNorth Conferences?

- ☒ Yes
- ☐ No

B4. Where are do you operate Internationally? (check all that apply)

- ☒ Canada
- ☒ US
- ☒ Mexico, Central America, and Caribbean
- ☒ Europe
- ☒ Asia
- ☒ Africa
- ☒ Oceania
- ☒ South America

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.

C. IMPLEMENT, PROTECT, AND ENHANCE PRIVACY BY DESIGN

C1. Does your product currently in production comply with Privacy laws in the following?

☐ Canada
☐ Quebec
☐ Brazilian General Data Protection Law (LGPD)
☐ California Privacy Legislation (CCPA)
☒ EU (GDPR)
☒ UK
☐ Australia (APPs)

Additional comments
iProov acts as a Data Processor and complies with the EU GDPR and UK GDPR. Our customers, the Controller, who are based in other jurisdictions comply with applicable data protection regulations specific to that region.

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

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:

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.

☒ 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

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.

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

Approx 200

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

100+

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

6000+

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

180+

Additional comments
iProov works with best-of-breed partners to deliver services globally

F. Built on open standards-based protocol

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

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.

☐ 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 (check all that apply)

☒ OAUTH2
☒ OPENID CONNECT 1.0
☒ SAML
☐ Not at this time

G. Interoperable with international standards

G1. Confirm if you have an imaging standard for photos and facial capture (check all that apply)

☐ Passport Image Standard (ISO IEC19794-5)
☒ PNG
☒ JPEG
☐ GIF
☐ TIFF
☐ Proprietary Standards
☒ Other, please describe

Additional comments
Imagery is streamed to our servers in video format

H. Cost effective and open to competitive market forces

H1. What is the cost-model? (check all that apply)

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.

☐ 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?

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.

☒ 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
☐ 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
☐ No

I6. Does the application connect with any government sources to confirm the legitimacy of the record?

☒ Yes
☐ 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
☐ No

I8. 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

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.

I9. 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? *

☒ Yes
☐ No

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.

I10. What physical identification security features does your solution test against a database of expected results? (check all that apply)

☒ Character spacing
☒ Document 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
Capabilities are delivered through our best-of-breed document capture partners.

J. Minimizes data transfer between authoritative sources and will not create new identity databases

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)
☒ By the entity receiving the identification information (e.g., financial institution)

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.

☐ Any of the above
☒ Other

J2. Does the information stay within Canada for the entire session for Canadian issued identification (e.g., in transit not related to storage)?

☐ Yes
☒ No

J3. Does the ID network encrypt all information in the mobile application in transit?

☒ Yes
☐ No

J4. What option do they have for the storage information? (check all that apply)

☒ Major cloud providers with Canadian server locations
☒ Major cloud providers with International server locations
☒ Private clouds
☐ Other

J5. What option do they have for the delivery of service? (check all that apply)

☒ Major cloud providers (SaaS) with Canadian server locations
☒ Major cloud providers with International server locations
☒ Private clouds
☐ On premise with customer's data center
☒ Mobile Integrations (Customer within their own app via SDK)
☐ Mobile Integrations (Vendor application)
☒ Web Integrations (Customer within their own app via SDK)
☐ Web Integrations (Vendor application)
☐ Other

Additional comments

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.