

DIRECTORY OF IDENTITY MANAGEMENT AND PROOFING PRODUCTS

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.

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) *

WorldReach uses innovative processes and technology to verify you are who you say you are to enable digital services delivery, through its systems for:

- government travel services (borders, immigration, passport, consular) and digital citizen services;
- safe and seamless traveller journey with the travel sector;
- highly trusted digital Identity verification and corroboration.

WorldReach improves international travel safety and security through the modernization of immigration and border management programs and the seamless traveller journey. We are recognized as innovators in consular and passport services globally. We provide the highly trusted remote digital ID verification for the UK's EU Settlement Scheme's digital channel, setting an exemplar for ID Verification.

We believe the key to interoperability and user adoption of any Identity Verification solution lies in strict adherence to international standards. Our focus is on chipped, standards-compliant identity documents which can be authenticated using the built-in digital security and cryptography without the need to depend on third party databases or manual reviews.

In addition to representation on DIACC's TFEC/OEC, WorldReach are proud members of: the Biometrics Institute; the International Border Management & Technologies Association (IBMATA); the FIDO Alliance; the World Travel & Tourism Council (WTTC) focusing on Safe & Seamless Traveller Journey; the International Air Transport Association (IATA) contributing to the IATA One ID initiative and the Document Security Alliance (DSA). WorldReach have active representation on ICAO's Implementation and Capacity Building Working Group (ICBWG) supporting the New Technologies Working Group (NTWG) focusing on Doc 9309 Standards and the new Digital Travel Credential (DTC).

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

WorldReach's remote Identity and Document Verification service is based on WorldReach's IdentityReach™ and Know Your Traveller™ platform. It allows an eligible applicant to read and authenticate their ePassport (or eMRTD card) remotely, using a smartphone app to read the passport chip, validating the cryptographic security controls embedded in the chip, and avoiding reliance solely on OCR and scanned pictures. Biometric facial matching and genuine presence (also known as liveness detection) are used to verify that the applicant is the rightful holder of the validated ID document. This is similar to the functionality of border kiosks.

This high level of identity assurance service is coupled with an automated back-end process suite that verifies the claimed identity, authenticates and checks the validity of documentation, determines eligibility, checks for watchlist alerts and processes that application through to issue, rejection or referral.

It should be considered in any situation where there is a requirement to verify the identity of large numbers of individuals, typically as a step in a registration, on-boarding or application process. IdentityReach works 24/7 from anywhere there is network coverage and typically takes minutes to complete an application, with no prior coaching or experience. It was developed adhering to both Privacy-by Design principles and GDPR mandates.

The service is designed to integrate and scale easily within planned or existing application processing and identity management ecosystems. It is highly configurable and comes with a suite of management, workflow and monitoring tools that can be tailored to the needs of the Customer.

A3. Please provide a brief description about complementary products or services: (250 words)

Our IdentityReach service provides digital service delivery organizations with a set of capabilities for securely on-boarding individuals by assessing their electronic identification documents and verifying their identity. We accomplish this while meeting our clients' strict requirements for service reliability, data security and privacy such as GDPR.

Once the IdentityReach service has completed the vetting and communicated the results to downstream client systems, all personally identifiable information is deleted from the IdentityReach system and is not retained either on the server or the applicant's smartphone. IdentityReach is not a digital ID. It can be used as a self-service remote enrollment platform for any government digital service delivery requiring enrolment to a high identity assurance level:

- Immigration permissions, such as for the UK Home Office EUSS.
 - ETA, eVisa, visa applications without the need to visit a Visa Application Centre.
 - Passport renewals.
 - A no-touch alternative passport control channel by replicating all of the functions currently performed by border crossing kiosks.
 - The front door to traveller facilitation schemes such as IATA's OneID, WTTC's SSTJ and similar programs.
-

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

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

N/A

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

Randy Wong
National Accounts Manager
+1 613 742 6482 office
+1 613 292 8847 mobile
randy.wong@worldreach.com
WorldReach Software, 2650 Queensview Drive, Suite 250,
Ottawa, ON Canada K2B 8H6
Website: www.worldreach.com
Twitter: @worldreach_WRS
LinkedIn: www.linkedin.com/company/worldreach

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://worldreach.com/worldreach-2020-the-year-of-rapid-digital-change/>

<https://worldreach.com/worldreach-profiled-in-juniper-research-digital-identity-report-2020-2025/>

<https://www.thinkdigitalpartners.com/news/2020/05/26/has-the-uk-just-quietly-seen-one-of-the-most-successful-government-it-projects-ever/>

DIACC Video: https://www.youtube.com/watch?v=DDtuvM3S_ug&t=23s

DIACC Video: <https://diacc.ca/resources/videos/>

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? *

- 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 *

- 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

Additional comments

C. IMPLEMENT, PROTECT, AND ENCHANCE 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

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

Supporting Global Government and public sector programs, WorldReach solutions and services are multi-lingual and must comply with all accessibility guidelines.

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)

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)

N/A

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

N/A

Additional comments

WorldReach high identity assurance IDV services and solutions focus on Government-issued, chipped foundational ID trust anchor documents and cards.

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

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

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

WorldReach has a multitude of flexible cost-model options.

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

WorldReach supports all sizes of Government and public sector departments with remote identity and document verification services supporting programs from the 1,000s to the 1,000,000s.

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

11. 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

12. 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

13. 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
- No

14. 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

15. Does the application verify that the chipped ID document has been authenticated? (e.g., Country signer, Active Authentication, etc.)? *

- Yes
- No

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

- Yes
- No

17. 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

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

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). *

Yes

No

110. 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

WorldReach IDV solutions and services depend on chip authentication checks and biometric matching to the quality photo on the chip over physical security features checks.

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)
- 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
