

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)

LexisNexis Risk Solutions leverages its industry-leading Big Data computing platform with vast data assets, proprietary advanced linking technology, and a sophisticated analytics platform to drive decision intelligence for our customers, enabling businesses of all sizes to turn their data into actionable insights and improve time-to-results and decisions. With our solutions, our customers transform their risk decision-making and are empowered to make better decisions easier. We help them with business challenges like fighting fraud, facilitating compliance, streamlining workflows and increasing efficiencies, improving customer experience, and keeping communities safe by providing timely insights for business decisions. For example, our LexisNexis® Risk Solutions fraud and identity and financial crime compliance portfolios offer robust solutions available in the Canadian market.

LexisNexis® Risk Solutions provides solutions across multiple industries, including Insurance, Financial Services, Collections and Recovery, Retail/eCommerce, Health Care, Communications, and more. We have offices throughout the world and are part of RELX, a global provider of information-based analytics and decision tools. Visit www.risk.lexisnexis.com

LexisNexis® Risk Solutions global sample statistics:

- Customers in more than 100 countries
- 7 of the world's top 10 banks
- Majority of the largest Canadian banks
- 88% of the Fortune 100 companies

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

LexisNexis® TrueID® provides fully automated document capture and authentication that uses a patented global ID library. It can be implemented across multiple channels, including online, mobile, and in-person. TrueID captures identity documents and authenticates the document without human intervention against one of the world's largest and robust, patented forensic library to evaluate the authenticity of government issued IDs. TrueID offers effective, rapid, and flexible identity document authentication capabilities for managing risk by validating and verifying documents.

TrueID enables you to:

- Easily capture images of the ID document using scanners, mobile devices, webcams, or most any high resolution, full color imaging device. Our All-in-One scanners are a highly-effective and self-contained option for in-person transactions.
- More accurately and rapidly confirm whether the ID is authentic or potentially fraudulent, using a series of automatic forensic security feature tests.
- Extract biographic data from the ID for use in other business workflows (e.g., name, address, date of birth, and ID #). These elements can be used to easily initiate

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.

additional verification steps, pre-fill credit applications, or begin other processes with minimal data entry or input error.

LexisNexis® TrueID®, can effectively evaluate more than 6,600 different global IDs from more than 200 countries and territories. A few examples of the IDs that TrueID can authenticate include:

- Canadian and other international driver's licenses
- Other kinds of Canadian Identity documents like Indian Status and Health cards
- Passports
- Visas (including international student visas)
- Global National ID Cards
- Travel documents and permits

TrueID features coverage of Canadian federal IDs (like passports) as well as IDs from all 13 Canadian provinces and territories.

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

LexisNexis® ThreatMetrix® detects fraud by analyzing consumer identities and associated devices. Using anomaly and velocity rules to make near real-time decisions, it builds an online profile of each user attempting an online transaction. Each profile accounts for a user's device (cookie-enabled and cookie-less identifiers), true location, persona information for trusted users and behaviors across the LexisNexis® Digital Identity Network®.

LexisNexis® Behavioral Biometrics analyzes anonymized input data including keyboard usage, mouse movement, manipulation of special keys and more, to detect behavior inconsistencies potentially indicating fraud.

LexisNexis® Emailage® helps augment risk assessment protocols by enabling organizations to confidently validate consumers' emails and assess the risk associated with an email address. Emailage leverages near real-time access to more than three billion unique email addresses, proven analytics and machine learning to quickly detect valid and invalid emails.

LexisNexis® Instant Verify International combines robust country coverage with a pass/fail verification response for critical identity elements.

LexisNexis® One Time Password enables multifactor identity authentication and validation by delivering a time-sensitive, unique password via SMS text, email or phone.

LexisNexis® Phone Intelligence provides phone risk assessment coupled with intelligence from our Digital Identity Network®, delivering visibility into real-time behaviors and activities around a phone number.

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.

LexisNexis® InstantID® Q&A Shared Secrets and Custom Questions authenticate consumers via consumer answers to security questions provided during enrolment, or answers to company-specific questions.

LexisNexis® Push Authentication authenticates users by leveraging mobile devices' cryptographically-backed hardware. Users are authenticated after unlocking their device in response to a push notification.

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

Credit Bureau Validation – PII verification through Instant Verify International

Face ID in lieu of Credentials and Country Signer Certificate Authentication are roadmap items. Implementation considered upon customer request.

Other: push authentication via mobile device.

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

This information is considered company confidential.

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

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.

Primary Contact: Alanna Shuh – Director - Market Planning, Fraud & Identity, Canada –
Alanna.Shuh@lexisnexisrisk.com

Secondary Contact: Kate Davis Green – Sr. Director, Fraud & Identity Global Strategy –
Kate.Davisgreen@lexisnexisrisk.com

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

TrueID site: <https://risk.lexisnexis.com/global/en/products/trueid>

LexisNexis Risk Solutions Fraud and Identity site:
<https://risk.lexisnexis.com/global/en/financial-services/fraud-and-identity-management>

N/A for DIACC blog posts.

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

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.

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

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

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

LexisNexis Risk Solutions maintains regulatory and privacy compliance policies and procedures (including a General Data Protection Regulation (GDPR) compliance program). LexisNexis Risk Solutions carries out Data Protection Impact Assessments to ensure that LexisNexis Risk Solutions scoring models and services comply with applicable Privacy laws as well as to identify and mitigate any risks. We incorporate Privacy by Design robust practices throughout the development of our products/services.

LexisNexis Risk Solutions has a global privacy framework to account for the privacy regulations of all applicable jurisdictions. More information is available at:

<https://risk.lexisnexis.com/privacy-policy>

D. Inclusive, open, and meets broad stakeholder needs

D1. Which languages does your application support? (check all that apply)

- English
- Canadian French

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.

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:

- 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)

200+ countries and territories

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

200+ countries and territories

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.

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

TrueID automatically recognizes ID types, captures and decodes their constituent data, and authenticates more than 6,600 different government-issued ID types. It uses worldwide identity document data for more than 200 countries, all of the U.S., and most global provinces and territories.

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

175

Additional comments

Because space was not provided in the previous section, the following includes comments elaborating on sections D1, D2 & D3, in addition to providing comments on E1 & E5.

D.1 Other:

TrueID web service can OCR the following native languages (special characters) from the ID document during the Document Authentication process:

- Latin
- Arabic
- Cyrillic
- Chinese
- Hebrew
- Japanese
- Korean
- Thai
- Vietnamese

TrueID web service direct API response could pass through overall and individual alert responses in the following native languages:

- Arabic (ar)
- French (fr)
- Portuguese (pt)
- Czech (cs)
- German (de)
- Russian (ru)
- Dutch (nl)
- Greek (el)
- Spanish (es)
- English (en)
- Italian (it)
- Turkish (tr)

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.

However, display of this information for web browser (iframe), print or use in some User Interfaces requires special font support that is custom (e.g. Adobe pdf Chinese font).

D.2 Other: We support French for Canadian customers. We have local language support for France, China, Hong Kong, Brazil, Columbia, Mexico, and Germany.

D.3 Other: LexisNexis Risk Solutions provides several avenues to support the education of staff on current accessibility standards and best practices. The User Experience design team works to provide accessibility consultation services to engineering and business stakeholders. Consultation tasks include manual review of product compliance to WCAG 2.0 AA standards, screen-reader testing, completion of VPAT documents and review of accessibility findings and best practices with business and technical staff.

A11yCAT is an in-house code review tool developed for the express purpose of providing automated code scans, error/warning monitoring and reporting on accessibility compliance of code under review. The tool supports automated code scanning along with local, real-time code checking and recommended resolutions for use by developers. As A11yCAT is developed in-house, it is actively maintained and enhanced to support the programmatic review of code against current WCAG 2.0 guidelines.

The RELX accessibility leadership advisory board provides a forum for the sharing of accessibility best practices, the communication of accessibility news and trends and the general communication of the benefits of accessibility across all RELX businesses including LexisNexis Risk Solutions. LexisNexis Risk Solutions design, engineering and business stakeholders are active participants on the board.

E1: In Process: Ongoing bi-weekly updates. Generally, most outstanding document types can be added to our service by the time of implementation.

E5: Any specific ID document not presently supported can be requested to be added to the applicable document library.

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
- Not at this time

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.

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

Because space was not provided in the previous section, the following includes comments elaborating on sections F1 & F2:

F1: Other - GitHub (Mobile SDK)

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.

F2: Other – LexisNexis Risk Solutions promotes the responsible use of information by employing a risk-management framework for privacy, information and physical security, and compliance. The framework is based on ISO 27002 and includes administrative, physical and technical safeguards designed to reasonably protect the privacy, confidentiality and security of personal information collected from or about consumers. Proprietary customer credentialing criteria and continuous security controls are also key components of the LexisNexis Risk Solutions privacy, security and compliance framework.

To deliver a consistently high standard for data security, LexisNexis Risk Solutions utilizes controls across its systems. In addition to utilizing more than 150 internal controls designed to prevent unauthorized access, LexisNexis Risk Solutions conducts back-end suspicious activity monitoring to detect and respond to anomalous account activity. We also work proactively to identify and resolve potential vulnerabilities in our systems.

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

Cost model depends on deployment type.

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

Other - Resellers and integrators.

I. Able to be independently assessed, audited, and subject to enforcement

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.

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

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.

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?

- 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.

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

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.

- 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

I6: Checks digital certificate revocation status.

I7: RFID chip reading capability on the roadmap.

I8: "Surname Crosscheck" test checks the Ontario DL.

I10: For Holograms, ultraviolet, infrared do not work with mobile phones.

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

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.

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

J4: Other - Custom storage options for self-storage in Canada, or vendor's US data centers. Custom data storage options available.

J5: Other - Web Service API is the primary and preferred delivery method. In addition to web service delivery methods, we also have All-in-One scanners.

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.