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.

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.

A. ABOUT THE SERVICE PROVIDER

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

Thales is a world leader in the sphere of biometric verification, secure identification and travel documents and related systems. Thales delivers identity and biometric solutions to governments and private identities in the fields of civil identity, travel and public security. We provide cutting-edge, customized, real-time and cloud-based identification verification and authentication solutions for major governments and private organizations worldwide. Our solutions are fully integrated, meaning that we do not depend on subcontractors for solution elements.

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

Thales's Identity Verification Suite (IDV) solution enables to check the authenticity of an identity document (passport, national identity card, residence permit, etc.). This technology is based on a proprietary identity verification document template database. It includes more than 2200 identity documents (ID, eID, passport, driver's licenses, residency permits, etc). This interactive, on-line library is continually updated as new ID documents are issued and as new fraud threats are identified. Our solution verifies the most comprehensive array of security and visual elements available. It also performs verification of data extracted via NFC (contactless) from the chip of electronic document. In addition, in order to fight identity theft, the IDV service integrates facial biometrics and liveness detection.

.

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

We provide digital wallets and the foundational framework required to issue credentials and verify them in real-time circumstances, both in accordance with DIACC Verifiable credentials standards, as well as AAMVA standards. We have fully implemented such solutions in the US, Europe and Australia.

Our facial recognition engine is based on deep learning algorithms and is ranked among the top of European vendors (for Visa shots) and among the highest ranking against NIST FRVT 1-to-1 and 1-to-many benchmark tests. We offer a mobile SDK that can be integrated into any mobile application to capture a user's facial image. Our solutions can be either accessed through customer on-premise SaaS models or through our own dedicated SaaS.

It is to note that our Identification Verification solution enables the detection of the following attack types during enrollment or authentication:

- Victim impersonation.
- Identity concealment

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

Thales provides all end-to-end solution components for all ranges of customized identity verification and authentication solutions. This includes our advanced, comprehensive Know-Your-Customer solutions that we provide to leading banks and trusts in Canada and beyond. It further includes all solution components for a complete digital wallet issuance, proportioning and verification cloud-based infrastructure, such as the SaaS Gateway system that we have already delivered to the state of Florida.

Thales is also the world's leading supplier of airport and land crossing border management systems and related hardware components used to identify cross-border travelers. Thales Document authentication readers and software are also used around the world and are incorporated into CBSA's border management solution at all Canadian land and air crossing points. We are the world's leading supplier of such hardware and software solutions. We also offer SKDs for a wide range of related functionalities.

Thales is the world's leading supplier of turnkey ID enrollment and issuance systems, that include applicants' data capture, enrollment, biometric authentication, QA verification, secure personalization and issuance to citizens and travelers around the world.

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

Our Know-your-Customer and IDV platforms are used for customer authentication and onboarding by the Bank of Nova Scotia, the National Bank of Canada, Rogers Bank, Tangerine, and Thirdstream, a Western Canadian Trust.

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

javier.montesinos@thalesgroup.com_IDV L3 Support & Presales

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://dis-blog.thalesgroup.com/supercategory/identity-biometric-solutions/

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

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
[JM] as far as I know we are compliant as well with the laws in Singapore. The unic required by the law is not to take the documents out of Singapore

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:

- ☒ 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)

205

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

152

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

1350

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

151

Additional comments

We can provide a whole list of documents supported

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
- ☐ 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
PDF

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
☐ 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

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

Thales IDV solution offers a comprehensive set of visual verification actions that are performed over the captured document image in white-ambient light.
First, the document is identified with exact type, issuing country and document version. Second, MRZ data field and VIZ data (OCR) are extracted. Then, from the document template database, a wide variety of predefined checks will be applied given the document's type. This consists of:
> Data format validation in accordance with ICAO standard
> Data integrity checks of the document's MRZ
> VIZ versus MRZ consistency checks
> Document validity
> Security features and graphical patterns verification in white light only
Thales IDV solution supports different front end channels for image capture: mobile or tablet devices through application integrating the mobile SDK, flatbed based office scanners, and uploads through web channels.

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