PCTF Automotive Identity Profile

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, a Final Recommendation is a deliverable that represents the findings of a DIACC Expert Committee that have been approved by an Expert Committee and have been ratified by a DIACC Sustaining Member Ballot.

This document has been developed by DIACC's Trust Framework Expert Committee PCTF Automotive Identity Profile Design Team. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the Pan-Canadian Trust Framework Work Programme.

Table of Contents

1. Introduction to the PCTF Automotive Identity Profile

The Digital ID and Authentication Council of Canada (DIACC) is developing the PCTF Automotive Identity Profile to standardize and secure digital identity verification practices across the automotive financing and leasing ecosystem.

This specialized profile is driven by both market demand and the growing need for a clear, auditable assurance mechanism that supports its key audience: automotive dealerships and leasing and finance entities which, as entities engaged in the sale, financing, or leasing of vehicles, are Reporting Entities (REs) under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), carry statutory Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance obligations administered by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and require strong identity verification practices to combat identity fraud.

In response to directives from major Canadian banks requiring dealerships to implement robust identity verification during financing, the PCTF Automotive Identity Profile will define transparent, auditable criteria that enable service providers to be certified against trusted standards. This certification, recognized through the DIACC PCTF Certification Program, will give dealerships, lenders, and technology partners confidence in secure, privacy-preserving digital identity tools that protect consumer data and meet regulatory expectations. By establishing a consistent trust layer for digital identity in vehicle purchasing and financing, the profile will reduce fraud, forgery, and document counterfeiting, while strengthening AML compliance assurance across the sector.

2. Applicable vs Interested Parties

2.1 Interested Parties

Private Sector

- Dealers & Dealer Groups (Franchised Dealers; Independent Dealers)
- Lenders / Financial Institutions (Banks, Credit Unions; Captive Finance Arms)

Industry Associations

- Canadian Finance & Leasing Association (CFLA)
- Canadian Lenders Association (CLA)
- Canadian Automobile Dealers Association (CADA)
- Used Car Dealers Association (UCDA)

- Provincial Dealership Associations

2.2 Applicable Parties

Digital ID & Authentication Solution Providers

- Digital ID & Authentication Solution Providers interested in or engaged in DIACC certification, or previously DIACC certified.

2.3 Dealer Operational Guidance and Procedures

This document fulfills two key functions. Sections 1 through 6 explain the background: who this Profile is for, the parties involved, and the terms used. Section 7 sets out the conformance criteria — the auditable technical requirements that an identity verification (IDV) service provider must meet to earn DIACC certification. The conformance criteria apply to the service provider, not to the dealership. Choosing a certified IDV provider gives a dealership confidence that the technical side of identity verification — document checks, biometric matching, data handling — meets a trusted standard. It does not transfer the dealership's responsibilities to the provider. The dealership remains accountable for the governance around the tool: maintaining a written identity verification policy, deciding how mismatches and fraud flags are handled, obtaining customer consent, keeping records, and meeting the legal obligations that apply to its business. The numbered guidance below describes those responsibilities. In short: a certified provider supplies the solution; the dealership remains accountable for how it is used.

As entities engaged in the sale, financing, or leasing of vehicles, dealerships are Reporting Entities under the PCMLTFA and carry direct statutory obligations for client identification, record-keeping, and reporting. The guidance in this section supports those obligations; it does not enumerate or replace them. Where the lender is also a Reporting Entity, the lender retains full statutory accountability for its own client identification and record-keeping obligations under the PCMLTFA and its regulations, regardless of who performs the verification. Neither party's use of a certified IDV service, nor the dealership's accountability under this Profile, displaces the other's independent regulatory obligations. Before relying on a certified identity verification service, a Relying Party should satisfy itself, as part of its own risk-based compliance program, that the verification method and the assurance it provides are appropriate to the risk of the product, customer, and transaction involved; certification attests to the quality of the verification process, not to its sufficiency for every use case.

1. **Governance and Policy Requirements**

- **Establish Rules:** The dealership must maintain a written identity verification policy, either as a standalone document or as a component of broader

compliance documentation. This policy must explain its process for checking identities and define the "risk framework" used to determine whether a customer is who they claim to be.

- **Data Mismatches:** The policy must describe how staff handle discrepancies in a customer's name, address, or date of birth when the digital results do not exactly match the customer's stated information.
- **Industry Alignment:** As a Reporting Entity, the dealership must ensure its internal risk thresholds meet the requirements that apply to its business under the PCMLTFA and its regulations.

2. **Fraud Management and Decision Making**

- **Review Red Flags:** When a service provider or credit bureau returns an "anti-fraud flag," the dealership must have a business process to review it and determine whether the transaction represents an "acceptable risk" according to its policy.
- **Escalation and Human Review:** The dealership's process should identify who reviews flagged or failed verifications, when a transaction is escalated to trained personnel for secondary review, and how verification is handled when systems are unavailable.
- **Ensure Data Independence:** When using the Dual Process Method, the dealership must not use its own internal records (such as a previous service invoice) as a source for verification, and must rely on independent, reliable sources.

3. **Contracting and Third-Party Oversight**

- **Security Certification of Providers:** Before contracting with an IDV service provider, the dealership should determine whether the provider holds a recognized information-security certification (such as SOC 2 Type II, SOC 3, or ISO/IEC 27001). Where a proposed provider does not hold such a certification, the dealership should assess, and be prepared to accept and document, the residual risk of contracting with that provider.
- **Determine the Legal Mechanism:** Before a dealership relies on another party's identity verification — or performs verification that a lender will rely on — it must determine and document which mechanism under the PCMLTFA regulations governs the arrangement: direct verification (s.105), agent or mandatary (s.106), or reliance (s.107). These mechanisms carry materially different liability, contracting, and record-keeping implications. The dealership should seek legal advice where the classification is unclear.
- **Formalize Agreements:** Where a dealership relies on a third party to verify identities, a written contract must be in place before the verification occurs.
- **Contract Essentials:** Such contracts must clearly define the scope of work, how data is shared, who maintains the records, and who is responsible for errors.

- **Verification of Partners:** The dealership must confirm that any third-party verifier complies with the identity laws and regulations of Canada and the jurisdictions in which the dealership operates.
- **Right to Audit:** Contracts should include "audit rights" so the dealership can confirm its partners are adhering to the required standards.

4. **Affiliate and Member Verification**

- **Verify the Group:** The dealership must not rely only on a customer's word. It must use an independent source (such as a corporate registry or government database) to confirm that the organization the customer claims to belong to actually exists.
- **Confirm Status:** The dealership must confirm that the customer's relationship with that group is current and in good standing at the time of the transaction.
- **Gather Evidence:** The dealership should obtain evidence of the relationship (such as a membership card, employee ID, or digital confirmation) to support the verification.

5. **Privacy and Documentation**

- **Secure Consent:** The dealership must obtain "informed consent" (clear permission) from the individual before collecting or using their digital identity data, and ensure a record evidencing that consent, including the date, is retained. This expectation is a conformance requirement for the certified verification process under criterion 102.1.0.10 (General Requirements), which applies across all verification methods.
- **Minimize and Protect Data:** The dealership should collect only the personal information the verification requires, and consider privacy-preserving measures such as tokenization or hashing of stored data, in line with guidance from the Office of the Privacy Commissioner of Canada.
- **Keep Clear Records:** The dealership must maintain its own records of the verification — including the date it happened, the source used, and the specific information obtained — and retain them for the period required by applicable law.
- **Accessibility:** The dealership should ensure, and be able to demonstrate, that its identity verification process is accessible to all customers (referencing WCAG 2.2 level AA standards where applicable).

3. Trusted Processes

The PCTF promotes trust through a set of auditable business and technical requirements for various processes. A process is a business or technical activity (or set of such activities) that transforms an input condition to an output condition – an output on which others typically rely.

In the PCTF context, a process that is designated a Trusted Process is assessed according to well-defined and agreed-upon Conformance Criteria. The integrity of a Trusted Process is paramount because many participants - across jurisdictional, organizational, and sectoral boundaries and over the short-term and long-term - rely on the output of that process.

Note: For more information on Trusted Processes associated with client identification and verification, please review the PCTF Verified Person component.

The PCTF Verified Person component is referenced here as a related body of work only. It does not form part of the PCTF Automotive Identity Profile, and conformance with this Profile is assessed solely against the criteria in Section 7 of this document. Certification under the PCTF Verified Person component is neither required for, nor does it confer, certification under this Profile.

4. Example of Auto Sales Transaction

Note: The following example flow is illustrative only. It is not intended to be a thorough or accurate representation of any real-world process; it is intended to show where different processes may exist in some transaction flows.

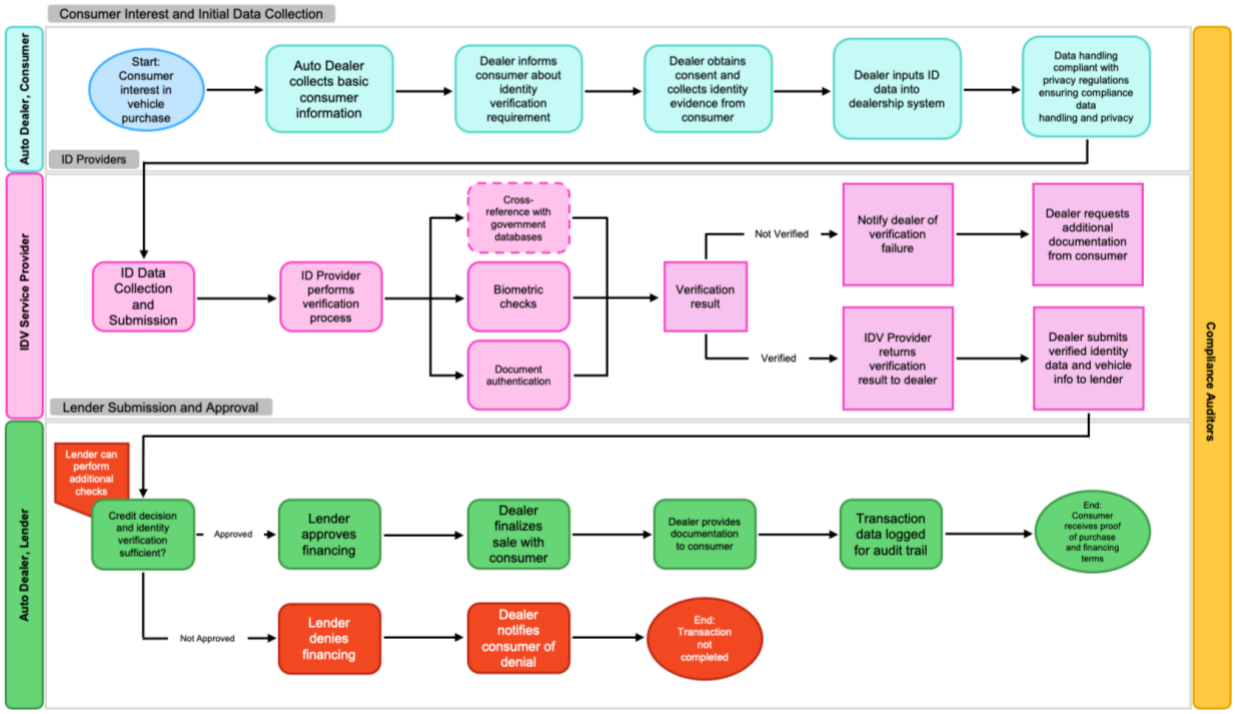

Figure 1. Trusted Process Example (non-normative): Auto Sales Transaction

5. Profile Background

The PCTF Automotive Identity Profile is a specialized framework that establishes clear, auditable criteria for identity verification and compliance within Canada's automotive financing and leasing ecosystem.

This initiative responds to both growing market demand and the need for a credible assurance mechanism that meets the expectations of its audience: automotive dealerships and leasing and finance entities which, as entities engaged in the sale, financing, or leasing of vehicles, are REs under FINTRAC with statutory AML and KYC compliance obligations under the PCMLTFA, and which need to strengthen KYC procedures to prevent and detect identity fraud.

Please note that the current Identity Profile does not align to specific identification methods or related requirements prescribed under the PCMLTFA and its associated regulations, further described in FINTRAC's guidance.

Several of Canada's major financial institutions have issued directives to their dealer networks, mandating stronger identity verification processes for financing and lease transactions to address:

- Rising identity theft;
- Synthetic fraud threats;
- AI-enabled fraud;
- Deepfake presentation attacks; and,
- Account farming.

This shift has created increasing demand for clear, industry-aligned guidance and reliable, privacy-preserving digital identity verification tools.

The PCTF Automotive Identity Profile directly addresses this need by defining auditable criteria for digital identity verification specific to automotive finance transactions. These criteria will serve as the foundation for an industry certification program, enabling service providers to be assessed and certified against standardized, transparent requirements.

Certified service providers will earn the PCTF Automotive Identity Profile Trustmark, signifying that their solution meets the highest standards of security, privacy, interoperability, and compliance. For dealerships and their staff, this trustmark provides confidence that their chosen service meets both operational and regulatory expectations - ensuring transactions are secure, compliant, and consumer data remains protected.

By establishing this profile, the automotive finance sector gains a consistent, evidence-based method for evaluating digital identity verification services. This, in turn, helps

reduce adoption barriers, enhances fraud resilience, and supports broader trust in Canada's digital identity ecosystem.

Jurisdictional note: In Quebec, the Act respecting the protection of personal information in the private sector (as amended by Law 25) imposes obligations directly relevant to the verification methods in this Profile, including the requirement to declare biometric databases and systems to the Commission d'accès à l'information du Québec (CAI). Participants operating in Quebec remain responsible for compliance with these requirements, which are triggered by the biometric processing in the Photo ID Method.

Note: PCTF Conformance Criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy, and regulations in their jurisdiction.

6. Document Conventions

6.1 Conformance Criteria Keywords

The following keywords indicate the precedence and general rigidity of a given Conformance Criteria, and are to be interpreted as:

- **MUST** means that the requirement is absolute as part of the Conformance Criteria.
- **MUST NOT** means that the requirement is an absolute prohibition of the Conformance Criteria.
- **SHOULD** means that the requirement is expected to be met, except in limited cases where the applicant documents valid reasons or circumstances to ignore the requirement. The full implications of such an exception must be understood and carefully weighed before choosing not to adhere to the Conformance Criteria as described.
- **SHOULD NOT** means that a valid exception reason may exist in particular circumstances when the requirement is acceptable or even useful, however, the full implications should be understood and the case carefully weighed before choosing not to conform to the requirement as described.
- **MAY** means that the requirement is discretionary but recommended.

Keywords appear in bold and ALL CAPS in the Conformance Criteria.

6.2 Terms and Definitions

For a comprehensive list of terms and definitions used in the PCTF, please refer to the PCTF Glossary.

- **Affiliate:** an entity connected to another if one wholly owns the other, both are wholly owned by the same entity, or their financial statements are consolidated
- **Canadian Credit Bureau:** A private company (e.g., Equifax or Transunion) that collects, stores, and sells consumer credit information (e.g., loan payments, credit card history, bankruptcies) to lenders and others, creating a detailed credit report and score to help assess creditworthiness for loans and services, though they don't make lending decisions themselves. They compile data from banks, creditors, and public records, providing insights into a person's borrowing habits for financial institutions to use.
- **Relying Party:** A Role that an Organization or Person performs to consume Digital Identity Information created and managed by Participants to conduct digital transactions with Subjects. In the context of this profile, a Relying Party is a lender.
- **Reporting Entities:** Generally refers to an organization that is required or chooses to prepare financial statements, or one that has specific legal obligations to report certain transactions to a regulatory body. Under the federal PCMLTFA, Reporting Entities are businesses and organizations that are legally required to meet specific obligations, including reporting suspicious and large transactions to FINTRAC.
- **Responsible Authority:** A Role that a Participant performs to provide one or more of the Verified Person or Verified Organization Trusted Processes to establish that a Subject is real, unique, and identifiable, and protects related information against compromise. In the context of this profile, a Responsible Authority is a dealership.
- **Tradeline:** A credit reporting term for a specific account listed on an individual's or business's credit report. Each separate credit account (such as a credit card, mortgage, or car loan) has its own corresponding Tradeline that details the history and status of that account.

7. Conformance Criteria

Scope of These Criteria. The conformance criteria in this section define the trusted process for verifying the identity of a person, and the records that process must produce and make available. They do not address the broader legal obligations of any participant — including record retention and disposal, regulatory reporting, sanctions or PEP screening, beneficial-ownership determination, or ongoing monitoring. Those obligations are governed by the legislation and regulations applicable to each participant and remain that participant's responsibility regardless of certification. These criteria do not replace or supersede existing legislation, policy, or regulation.

The conformance criteria in this section specify the outcomes a certified solution must achieve and the evidence by which those outcomes are verified. They do not mandate, favour, or exclude any particular product, vendor, technique, or system architecture. Where a specific technology is named in a criterion or its accompanying guidance, it is

cited as an illustrative and acceptable means of meeting the requirement, not as a required method; a solution that achieves the required outcome by other means, supported by equivalent evidence, conforms equally. This keeps the criteria technology-neutral, auditable against results rather than implementations, and open to new entrants and emerging methods.

Conformance Criteria are organized according to the following methods to verify an individual's identity.

Credit File Method:

- A method to verify an individual's identity by relying on information in a Canadian credit file if it has been in existence for at least three (3) years. The name, address, and date of birth in the credit file must match that provided by the individual.

Dual Process Method:

- A method for verifying an individual's identity by relying on any two of the following:
    - information from a Reliable Source that contains the individual's name and address;
    - information from a Reliable Source that contains the individual's name and date of birth; and
    - information containing the individual's name that confirms they have a deposit account or credit card or other loan account with a financial institution.

Photo ID Method:

A method for verifying an individual's identity using a valid, authentic, and current (not expired) government-issued identification document containing the individual's name and photograph (e.g., driver's licence, passport, Secure Certificate of Indian Status, Permanent Resident Card, or certain provincial or territorial health insurance cards). Only identification documents issued by the Canadian federal government or a Canadian provincial or territorial government may be used, or a foreign-issued identification document that is equivalent to a Canadian-issued identification document. A foreign-issued document is equivalent only if it is issued by a national government or by a state, provincial, or territorial-level authority of a foreign government; bears the individual's name, photograph, and a unique identifying number; and contains security features whose authenticity can be verified. Identification documents issued by municipal governments (Canadian or foreign) **MUST NOT** be used.

Note: The equivalency determination is made by the Responsible Authority's identity verification solution against the criteria above and is assessed as part of certification.

This does not displace the accountability of the dealership or lender for its own client identification obligations under applicable law. To support that accountability, this Profile requires that every verification result returned to the Relying Party identify the document used, its type, unique identifying number, and jurisdiction and country of issue — so that document-acceptance decisions can be reviewed.

Affiliate or Member Method

This method allows the Responsible Authority to verify a person's identity by confirming that it was previously verified by a qualifying entity with which the person has an Affiliate or member relationship — for example, a bank verifying that an individual was already identified by its regulated Affiliate. The method depends on three confirmations: that the qualifying entity exists, that the person's relationship with it is current, and that the entity previously verified the person's identity using an acceptable method. The categories of entity that qualify are defined in 102.1.4

Affiliate or Member Method (see CC 102.1.4.10.1, which carries the PCMLTFA s.5(a)–5(g) restriction).

Reliance Method
This method addresses arrangements under Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR s.107 (reliance)) only. An Agent/Mandatary method (PCMLTFR s.106) is not included in this version of the Profile and is deferred to a future version. The inclusion of the Reliance Method does not imply that s.107 is the correct classification for any given dealer-lender arrangement; see Section 2.3 for guidance on determining and documenting the applicable mechanism.

The identity of a person may be verified by relying on measures that were previously taken by:

- Another Reporting Entity referred to in any of paragraphs 5(a) to (5g) of the PCMLTFA as listed below:

  (5a) authorized foreign banks within the meaning of section 2 of the Bank Act in respect of their business in Canada, or banks to which that Act applies;

  (5b) cooperative credit societies, savings and credit unions and caisses populaires regulated by a provincial Act and associations regulated by the Cooperative Credit Associations Act;

  (5c) life companies or foreign life companies to which the Insurance Companies Act applies or life insurance companies regulated by a provincial Act;

  (5d) companies to which the Trust and Loan Companies Act applies;

(5e) trust companies regulated by a provincial Act;

(5e.1) trust companies incorporated or formed by or under a provincial Act that are not regulated by a provincial Act;

(5f) loan companies regulated by a provincial Act;

(5g) persons and entities authorized under provincial legislation to engage in the business of dealing in securities or any other financial instruments or to provide portfolio management or investment advising services, other than persons who act exclusively on behalf of such an authorized person or entity;

- An entity that is affiliated with you or with another Reporting Entity and carries out activities outside of Canada that are similar to those of a person or entity referred to in any of paragraphs 5(a) to (g) of the Act (an Affiliated foreign entity).

Digital Credentials Method

FINTRAC has updated its guidance to permit digital identity verification, facilitating the use of advanced digital technologies. However, there is currently no explicit definition for this method in their official documentation. The modernization of FINTRAC's identity verification guidance includes the acknowledgment and authorization of remote identity verification technologies for client identification. Reporting entities are required to comply with FINTRAC's regulations when implementing any identity verification method. For the most accurate and up-to-date information on approved identity verification methods, Reporting Entities should refer to FINTRAC's official guidance.

Reference Conformance Criteria

Reference	Conformance Criteria
102	**PCTF Automotive Identity Profile**
102.1	**Client Identification and Verification**
102.1.0	**General Requirements**
102.1.0.10	The Responsible Authority **MUST** obtain the individual's informed consent to the identity verification before collecting or using their identity information, and **MUST** retain a record sufficient to evidence that consent was obtained, including the date. This requirement applies to all verification methods in 102.1.1 through 102.1.6.
102.1.0.20	The Responsible Authority **MUST** have documented procedures to re-verify a person's identity in accordance with the applicable Conformance Criteria where there are doubts about the validity, currency, or accuracy of previously-collected identity information, consistent with PCMLTFR s.155(1). Triggers for re-verification **MUST** be documented in the Responsible Authority's identity verification policy.
102.1.0.30	The Responsible Authority and any IDV service provider acting on its behalf **MUST** disclose to the Relying Party: • The jurisdictions in which identity data (including biometric templates, document images, and audit logs) is processed, stored, and accessed; and, • Any sub-processor relationships, with the same disclosure. (This criterion is disclosure-only; it does not mandate where data resides.)
102.1.1	**Credit File Method**
102.1.1.10	The full name, home address and date of birth provided by the individual whose identity is being verified **MUST** be matched with the name, address and date of birth contained in the records of a Canadian Credit Bureau (as examples, Equifax and Transunion).
102.1.1.20	Any credit file information used to conduct an identity verification process **MUST** have been in existence for at least three (3) years from the date of verification.

102.1.1.30.2	Any credit file information used to conduct an identity verification process **MUST** contain information from two (2) independent Tradelines, where each Tradeline confirms one of the two (2) categories of information required to verify the identity of a person under this method. In this instance, each Tradeline is a distinct source; the credit bureau is not the source.
102.1.1.40.1	Any credit file information used to conduct an identity verification process **MUST** be obtained directly from a Canadian Credit Bureau or through a Responsible Authority (third-party vendor) authorized by a Canadian Credit Bureau.
102.1.1.60	Any credit file information used to conduct an identity verification process **MUST**: • Be obtained at the time the verification process is conducted; and, • Be valid and current at the time the verification process is conducted. (i.e., an individual cannot provide you with an imagery of their credit file, nor can a previously obtained credit file be used).
102.1.1.70.1	The Responsible Authority **MUST** collect and return all the following data points to the Relying Party: • The individual's name; • The name of the credit bureau holding the credit file; • The individual's credit file number; • The date the credit file was consulted; and, • The outcome of the verification check, including whether the individual's identity was verified or unverified, the reliability of the results and all other data points that might affect the lender's decision to interact with, or represent, the individual.
102.1.1.80	The Responsible Authority **MUST** develop and document an identity verification policy that describes the risk assessment framework used to evaluate discrepancies between current credit file information and the claimed identity.
102.1.1.90	An identity verification policy **MUST** describe the approach used to evaluate differences in name, address, and date of birth between the credit file and the claimed identity, either individually or as part of a larger data set.

102.1.1.100.1	When a credit bureau returns anti-fraud flags of any kind in response to an identity verification event, the Responsible Authority **MUST** have business processes in place to evaluate these flags for acceptable risk according to documented policy.
102.1.1.120.1	The Responsible Authority using the Credit File Method **MUST** collect the legal name, date of birth, and home address information for the individual being verified and provide this data to a Canadian Credit Bureau for processing, including: • At least two (2) home addresses if the party has moved within the past three (3) years; and, • At most six (6) home addresses.
102.1.2	**Dual Process Method**
102.1.2.10	When verifying the name, address, and date of birth provided by the individual claiming an identity, the Responsible Authority **MUST** ensure the information it receives is valid and current, comes from two (2) different Reliable Sources, and contains at least two (2) of the following: • Information from a reliable source that contains the individual's name and address; • Information from a reliable source that contains the individual's name and date of birth; and, • Information that contains the individual's name and confirms that they have a deposit account, a prepaid payment product account, or a credit card or other loan amount with a financial institution. (For example, a reliable source could be the federal, provincial, territorial or municipal levels of government, Crown corporations, federally regulated financial institutions, or utility providers.)
102.1.2.20	Information sourced by the Responsible Authority or agent of the Responsible Authority from within their own line of business **MUST NOT** be used to verify identity, even if it would otherwise be considered a reliable source for this purpose.
102.1.2.30	Information from the individual claiming the identity **MUST NOT** be used to also verify the identity. (Information collected from an individual is used to resolve the claimed identity to a single legal person which is then subsequently verified against reliable sources to ensure that the resolved identity exists and is valid.)

102.1.2.40	If credit file data is used as one of the sources used to satisfy the requirements of the Dual Process Method, the Responsible Authority **MUST** confirm the credit file from which the data is extracted has been in existence for at least six months.
102.1.2.50.2	If credit file data is used as one of the sources used to satisfy the requirements of the Dual Process Method, the Responsible Authority **MUST** verify that the credit file has been established and is active at the time of verification.
102.1.2.51.1	If the Responsible Authority is relying on two Tradelines, it **MUST** contain information from two independent Tradelines within the same credit file, where each Tradeline confirms one of the two categories of information required to verify the identity of a person under this method. In this instance, each Tradeline is a distinct source; the credit bureau is not the source.
102.1.2.60.2	The Responsible Authority **MUST** ensure documents used to satisfy the requirements of the Dual Process Method (e.g., a bill from a utility company) are evaluated using a solution that is capable of detecting evidence of alteration, tampering, forgery, or other indicators that would reasonably call the authenticity or integrity of a document into question and identify documents that do not satisfy the applicable validity and currency requirements.
102.1.2.80	The acceptable level of risk resulting from differences between the information provided by the reliable source and the claimed identity information **MUST** conform to the requirements of regulated industry services, if applicable.
102.1.2.90.1	The Responsible Authority **MUST** develop and document policies that outline the process and approach used to evaluate discrepancies in the identity data presented within different Reliable Sources.

102.1.2.110.1	The Responsible Authority **MUST** collect and return all the following data points to the Relying Party (e.g., lender): • The individual's name; • The date the information was verified; • The names of the two different Reliable Sources that were used to verify the identity of the individual; • The type of information referred to; • The number associated with the information collected (for example, account number or if there is no account number, a number that is associated with the information, which could be a reference number or certificate number, etc.); and, • The outcome of the verification check, including whether the individual's identity was verified or unverified, the reliability of the results and all other data points that might affect the lender's decision to interact with, or represent, the individual.
102.1.3	**Photo ID Method**
102.1.3.10.1	The Responsible Authority **MUST** collect and return all the following data points from government-issued photo identification to the Relying Party (e.g., lender): • Imagery of the document(s) that were used for verification; • The individual's name; • The date on which the individual's identity was verified; • The type of document used for verification (e.g., driver's license, passport, etc.); • A unique identifying number of the document used; • The jurisdiction (province or state) and country of issue of the document; • The expiry date of the document, if available. (i.e., if this information appears on the identification document, it must be collected and returned); and, • The outcome of the verification check, including whether the identity was verified or unverified, the reliability of the results and all other data points that might affect the lender's decision to interact with, or represent, the individual.

102.1.3.20.1	The Responsible Authority **MUST** verify that the government-issued photo identification document is authentic and validly issued by the Authoritative Source (e.g., a federal, provincial, territorial, or foreign government) by: a) using technology capable of evaluating the document's security features when the verification is conducted remotely (the individual is not physically present); or, b) when the verification is conducted in person, by either physically inspecting the document's security features in the presence of the individual or using technology that provides an equivalent level of assurance. (Guidance: Forensic validation of the document, including barcode and MRZ cross-checks, NFC chip reading, and issuer-certificate validation, is encouraged where the document and capture device support it. OCR-only capture that performs no authenticity verification does not satisfy this criterion. NFC chip reading remains a SHOULD; see 102.1.3.110.)
102.1.3.30.1	For documents with MRZs and/or barcodes, the Responsible Authority **MUST**, in accordance with accepted best practice, compare the contents of the MRZ/barcode with data printed on the document and highlight mismatches. (An MRZ code is a string of characters that appears on the bottom of the personal data page of a passport. It is a combination of letters, numbers, and symbols that are arranged in three (3) lines.)
102.1.3.40.1	The Responsible Authority **MUST** enforce the capture of government-issued photo identification documents in real time and prevent the uploading of an image file. This requirement applies only to the Photo ID Method described in 102.1.3 and does not preclude the use of scanned or imaged documents as reliable-source information under the Dual Process Method (102.1.2), consistent with FINTRAC Methods Guidance Annex 5.

102.1.3.50.4	The Responsible Authority **MUST** support, at minimum, presentation of any government-issued photo ID document types that include a full name, unique identification number and photo if: • It is issued by a provincial, territorial or federal government in Canada or an equivalent foreign government; • It is valid (not expired); • It bears a unique identifier number (such as a driver's license number); • It bears the name of the individual being identified; and • It bears a photo of the individual being identified.
102.1.3.60.1	The Responsible Authority **MUST** document their conformity claims to WCAG 2.2 level AA at minimum, noting any jurisdictional regulatory floors that reference an earlier version (e.g., accessibility legislation that references WCAG 2.0 level AA). (Web Content Accessibility Guidelines (WCAG) are developed through the W3C process in cooperation with individuals and organizations around the world, with a goal of providing a single shared standard for web content accessibility that meets the needs of individuals, organizations, and governments internationally.)
102.1.3.70.1	The Responsible Authority **MUST** use reliable technology as determined acceptable and based on industry standards, to compare the features of the real-time selfie to the photo on the authentic government-issued photo identification document.
102.1.3.71	The Responsible Authority completing the government-issued photo Identification Method **MUST** perform an active or passive liveness check on the selfie.

102.1.3.72	For remote (unattended) verification, the Responsible Authority's solution **MUST** resist the injection of synthetic or pre-recorded media into the verification data stream, evaluated against CEN/TS 18099:2025 (Biometric data injection attack detection), or its successor ISO/IEC 25456 once published, by a competent independent laboratory, achieving at least Level 2. (Injection Attack Detection addresses synthetic or pre-recorded media, such as deepfakes, virtual-camera substitution, and data-stream injection, fed directly into the verification pipeline, bypassing the camera. Specific techniques such as endpoint or sensor attestation, virtual-camera detection, and analysis of captured media for AI-generated content are illustrative means of meeting this requirement, not mandatory methods.)
102.1.3.73	Evidence of the Injection Attack Detection evaluation result achieved under 102.1.3.72 **MUST** be available to be verified by an external auditor.
102.1.3.80.1	Face-matching solutions employed by a Responsible Authority **MUST** undergo testing by a qualified and independent third-party to evaluate the performance of the face recognition algorithm in a one-to-one matching scenario. (The existence, but not the content, of these test results must be available to be verified by an external auditor.)
102.1.3.100.1	The Responsible Authority's liveness check **MUST** be evaluated for Presentation Attack Detection in accordance with ISO/IEC 30107-3 by a laboratory accredited to ISO/IEC 17025 for that testing, and achieve at least ISO/IEC 30107-3 Level 2. (Presentation Attack Detection is automated detection of an attempt to subvert a liveness check through measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture.)
102.1.3.101	Evidence of the Presentation Attack Detection evaluation result achieved under 102.1.3.100.1 **MUST** be available to be verified by an external auditor.

102.1.3.110	When using a mobile application to scan NFC-readable Photo ID documents, an NFC chip reading **SHOULD** be used for a higher level of assurance to cryptographically verify authenticity and issuer certificate origin. (Near-field communication (NFC) is a set of communication protocols that enables communication between two electronic devices over very short distances)
102.1.4	**Affiliate or Member Method**
102.1.4.10.1	The Responsible Authority **MUST** verify that the individual is an Affiliate or member of an entity that: (a) is a Reporting Entity referred to in any of paragraphs 5(a) to 5(g) of the PCMLTFA; (b) is a foreign Affiliate that carries out activities outside Canada similar to those of an entity referred to in paragraphs 5(a) to 5(g); or (c) is a financial entity subject to the Act that is a member of the Responsible Authority's financial services cooperative or credit union central, and whose existence the Responsible Authority has confirmed through independent verification.
102.1.4.20	The Responsible Authority **MUST** confirm the existence of the Affiliate or member entity by referring to an independent and reliable source, such as corporate registries, professional licensing bodies, or government databases.
102.1.4.30	The Responsible Authority **MUST** collect the following minimum information from the individual: • Full legal name; • Individual's address; • Name of the Affiliate or member entity; and, • Nature of the individual's relationship to the entity.
102.1.4.31	The Responsible Authority **MUST** confirm that the individual's information (the person's name, address, and date of birth) matches information found in the Affiliate's or member's records.
102.1.4.40	The Responsible Authority **MUST** verify the existence of the Affiliate or member entity before or at the time of confirming the individual's identity through this method.
102.1.4.50.1	The Responsible Authority **MUST** verify that the individual's Affiliate or member status is current and in good standing at the time of identity verification.

102.1.4.60	The Responsible Authority **MUST** obtain documentary evidence that confirms the individual's relationship to the verified entity, such as membership cards, employee identification, or official correspondence.
102.1.4.70	The Responsible Authority **MUST NOT** rely solely on information provided by the individual to confirm the existence of the Affiliate or member entity.
102.1.4.90.2	The Responsible Authority **MUST** produce and make available records of the entity verification, including: • The source consulted; • The date of verification; • Information obtained; • Person's name; • Date the information was verified using this method; • Name of the Affiliate/member; • Method that was used to verify identity; and, • All information that was recorded at the time of verification.
102.1.4.100	The Responsible Authority **SHOULD** supplement this method with additional verification of the individual's address through independent means when the Affiliate or member information does not include confirmation of the individual's residential address.
102.1.4.110	The Responsible Authority **MAY** implement periodic re-verification of the individual's Affiliate or member status as part of ongoing customer due diligence procedures.
102.1.4.120	The Responsible Authority **MUST** confirm that the Affiliate or member has previously verified an individual's identity having recorded the specific method they used.
102.1.5	**Reliance Method**
102.1.5.10	The Responsible Authority **MUST** have a written agreement with any agent or mandatary (third-party verifier) on whom it relies for identity verification activities.
102.1.5.20	The Responsible Authority **MUST** confirm that the third-party verifier relied upon has verified the individual's identity using one of the acceptable methods prescribed by applicable regulations.

102.1.5.30	The Responsible Authority **MUST** obtain from the third-party verifier all information that was used to verify the individual's identity, including: • The method used for verification; • The date verification was completed; • The identity information collected; and, • Copies of any documents examined.
102.1.5.40	The Responsible Authority **MUST** verify that the third-party verifier relied upon is subject to obligations under the same or substantially similar regulatory framework for identity verification.
102.1.5.50	The Responsible Authority **MUST** establish reliance on the third-party verifier's verification before or at the time the Responsible Authority is required to verify the individual's identity, not retroactively.
102.1.5.60	The Responsible Authority **SHOULD** conduct appropriate due diligence on the third-party verifier to confirm their capability, reliability, and compliance with applicable identity verification requirements.
102.1.5.70	A written agreement with the third-party verifier **MUST** specify: • The scope of verification activities; • Information sharing obligations; • Record retention responsibilities; and, • Liability and indemnification provisions.
102.1.5.80.1	The Responsible Authority **MUST NOT** rely on a third-party verifier for identity verification if that third party itself relied on another entity for the verification.
102.1.5.90	The Responsible Authority **SHOULD** include provisions in the written agreement that grant audit rights to verify the third-party verifier's compliance with identity verification requirements.
102.1.5.100.1	The Responsible Authority **MUST** produce and make available documentation of the reliance relationship, including the agreement, evidence of the third-party verifier's regulatory status, and records of information transfers.
102.1.6	**Digital Credentials Method**
102.1.6.10	The Responsible Authority **MUST** verify the authenticity of the digital credential by confirming it was issued by a trusted and verifiable source using cryptographic or other secure validation methods.

102.1.6.20.1	The Responsible Authority **MUST** confirm that the digital credential issuer operates within a recognized trust framework or has been assessed against established standards for digital identity credentialing. (Footnote: see the Pan-Canadian Trust Framework and its trust-framework recognition criteria: https://diacc.ca/trust-framework/)
102.1.6.30	The digital credential **MUST** contain at a minimum the following verified identity attributes: • Full legal name; • Date of birth; • Address or other location information; and, • A unique identifying number of the credential used.
102.1.6.31	The Responsible Authority **SHOULD** ensure that only the information necessary to fulfil the purpose of the transaction is disclosed during credential verification.
102.1.6.40.1	The Responsible Authority **MUST** verify that the digital credential is current and has not expired at the time of identity verification, and confirm the credential's current validity status where possible, including any condition that affects validity or authorized use (expiry, revocation, suspension, restriction, reinstatement), using a mechanism appropriate to the credential's trust model. Acceptable mechanisms include an issuer-published status service, a cryptographic status mechanism (e.g., status lists, revocation registries, accumulator or short-lived-credential schemes), or a holder-presented status proof.
102.1.6.60.1	The Responsible Authority **SHOULD** verify that the digital credential and its validation processes comply with recognized technical standards for digital identity (e.g., ISO/IEC 18013-5 for mobile driving licences (mDLs), the W3C Verifiable Credentials Data Model, other standards, specifications, and national digital identity frameworks).
102.1.6.61	Where a government-issued mobile credential (e.g., a Canadian provincial mDL) is presented, the Responsible Authority **MUST** validate it in accordance with the recognized technical standard under which it is issued, including issuer data authentication and device binding (e.g., ISO/IEC 18013-5), rather than accepting a visual rendering.

102.1.6.80.2	The Responsible Authority **MUST** implement mechanisms to confirm the current validity status of digital credentials during the verification process, using a mechanism appropriate to the credential's trust model as described in 102.1.6.40.1.
102.1.6.90	Where a digital credential is used for remote identity verification, the verification **SHOULD** apply cryptographic validation of the credential together with the biometric comparison, liveness, and anti-spoofing protections required under 102.1.3.
102.1.6.100	Digital-credential verification processes **SHOULD** minimize unnecessary disclosure, to the issuer or unrelated parties, of where, when, or to whom a credential is presented, except where required by law or legitimate operational need.
102.1.6.110	Verification processes **SHOULD** minimize the ability of participating entities to correlate separate transactions involving the same individual, unless such correlation is required by law or legitimate business purpose.
102.1.6.120	The Responsible Authority **SHOULD** ensure that requests for identity attributes are limited to those for which the requesting party has a legitimate business, regulatory, or operational purpose.
102.1.6.130	The Responsible Authority **SHOULD** support selective-disclosure presentation where the underlying credential supports it.

8. Revision History

Version	Date of Issue	Author(s)	Change Description
0.01	2025-09-23	PCTF Automotive Identity Profile Design Team	Initial draft developed by the PCTF Automotive Identity Profile Design Team to include background context, terms and definitions, conformance criteria, etc.
0.02	2026-04-07	PCTF Automotive Identity Profile Design Team	Prepared draft for TFEC review and public Call for Comments and IPR review approvals.
1.0	2026-04-22	PCTF Automotive Identity Profile Design Team	Approved by TFEC as Draft Recommendation V1.0 to prepare for public Call for Comments and IPR Review.
1.1	2026-07-16	PCTF Automotive Identity Profile Design Team	Disposition of public review comments applied in redline (123 comments; see Disposition of Comments register and Editor's Note below).
1.0	2026-08-12	PCTF Automotive Identity Profile Design Team	Approved by TFEC as Candidate for Final Recommendation V1.0.
1.0	2026-09-11	PCTF Automotive Identity Profile Design Team	Approved as Final Recommendation V1.0 through a DIACC Sustaining Member Ballot

9. Editor's Note on the Disposition of Public Review Comments

The public review ran May 5 to June 4, 2026 and drew 123 comments. Instead of ruling on each comment in isolation, the editor grouped the recurring questions into decision briefs and brought each brief to the Design Team for discussion. Agreement was reached on each brief before any disposition was finalized, so related comments received one consistent answer and every disposition in the comment register traces back to a decision the team made together.

Those discussions produced the decisions that shape this revision:

- **Scope boundary.** The Profile is a process specification, not a compliance manual. It certifies the trusted process for producing a verified identity and the records that process must produce and make available. Legal obligations that bind participants regardless of certification (record retention and disposal, sanctions and PEP screening, beneficial ownership, ongoing monitoring, regulatory reporting) stay out of the criteria. A scope statement now opens Section 7, and the "retain/maintain" wording became "produce and make available" (102.1.4.90.2, 102.1.5.100.1).
- **Outcomes, not architecture.** Criteria specify the outcomes a solution must achieve and the evidence that proves them. No product, vendor, technique, or system architecture is mandated. Named technologies are illustrative. This principle now also opens Section 7 and drove the technology-neutral rewrites of the credential status criteria (102.1.6.40.1, 102.1.6.80.2).
- **Biometric integrity.** Presentation Attack Detection was elevated from SHOULD to MUST at Level 2 under ISO/IEC 30107-3, tested by an ISO/IEC 17025-accredited laboratory (102.1.3.100.1). A new Injection Attack Detection criterion (102.1.3.72) is a MUST at Level 2 against CEN/TS 18099:2025 for remote verification. Both are written to outcomes, with techniques as examples only, and each carries a separate auditor-evidence criterion (102.1.3.101, 102.1.3.73).
- **Consent.** A single horizontal consent criterion (102.1.0.10) now applies across all methods: obtain informed consent before collection and keep a record with the date. It replaces the Digital Credentials-only consent criterion (102.1.6.70.1, removed). The substance of consent stays governed by privacy law.
- **Section 2.3 rewrite.** The dealer guidance was rewritten once to answer a cluster of comments together: a plain-language foreword on how to use the document, the accountability boundary between certified provider and dealership, the reporting-entity correction (dealers selling or leasing vehicles are now REs under

the PCMLTFA), the s.105/106/107 mechanism-determination guidance, and updated privacy, escalation, and accessibility items.

- **Security certification of providers.** The design team decided against a MUST criterion requiring SOC 2 Type II, SOC 3, or ISO/IEC 27001. Section 2.3 instead advises dealerships to check whether a proposed IDV vendor holds such a certification and to weigh the residual risk that they accept by contracting with one that does not.
- **New horizontal criteria.** Re-verification on doubt (102.1.0.20, consistent with PCMLTFR s.155(1)) and data-residency and sub-processor disclosure (102.1.0.30, disclosure-only) were added under a new General Requirements section (102.1.0).

Risk-based verification is deferred. The most consequential structural request in the review asked the Profile to map verification rigour to transaction risk (value, customer type, fraud signals, commercial vs. retail). The Design Team was unable to reach agreement on this approach in early discussions, despite noting that NIST SP 800-63-4, FATF guidance, and Australia's Digital ID Act have adopted it. Designing auditable tiers, thresholds, and step-up triggers is design work that cannot be done responsibly at final revision, so risk-tiered verification is deferred to the next version of the Profile. In the interim, the Responsible Authority's documented risk-assessment policy (102.1.1.80) remains the mechanism for evaluating elevated-risk indicators, and Section 2.3 directs each Relying Party to make its own risk-based determination that a certified verification suits the use case. Related deferrals on the same basis: the Agent/Mandatary (s.106) method, structured assurance scoring of verification results, and the eIDAS/ETSI crosswalk.

Comment totals: 76 accepted, 35 rejected, 12 deferred. The full record, including every disposition and the decision briefs, is in the Disposition of Comments register for this Profile.