PCTF Automotive Identity Profile

Document Status: Draft Recommendation V1.0

In accordance with the DIACC Operating Procedures, a Draft Recommendation is a deliverable which is used to share early findings and to gather broad feedback.

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 two key audiences:

1. Automotive dealerships that are generally not Reporting Entities (REs) under the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) but require stronger Know Your Customer (KYC) practices to combat identity fraud; and
2. Leasing and finance entities that are FINTRAC-regulated REs, which must meet statutory Anti-Money Laundering (AML) and KYC compliance obligations.

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

While an Identity Verification (IDV) service provider delivers the technical solution and is bound by the auditable conformance criteria documented further below, the Responsible Authority (the dealership) remains accountable for the governance and manual processes required to maintain a Trusted Process.

1. **Governance and Policy Requirements**

- **Establish Rules:** You must maintain a written identity verification policy, either as a standalone document or as a component of broader compliance documentation. This document must explain your process for checking identities and define the "risk framework" used to determine if a customer is who they claim to be.
- **Address Mismatches:** Your policy must describe how your staff should 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:** You must ensure that your internal risk thresholds meet the standards expected of a regulated financial environment.

2. **Fraud Management and Decision Making**

- **Review Red Flags:** When a service provider or credit bureau returns an "anti-fraud flag," you must have a business process to review it and determine whether the transaction represents an "acceptable risk" according to your policy.

- **Ensure Data Independence:** If using the **Dual Process Method**, you must not use your own internal records (such as a previous service invoice) as a source for verification. You must use independent, reliable sources.

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

- **Formalize Agreements:** If you rely on a third party to verify identities (the **Reliance Method**), you must have a written contract in place before the verification occurs.
- **Contract Essentials:** These 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:** You must confirm that any third-party verifier complies with the identity laws and regulations of Canada and the jurisdictions in which you operate.
- **Right to Audit:** You should include "audit rights" in your contracts to ensure your partners are adhering to the required standards.

4. **Affiliate and Member Verification**

- **Verify the Group:** You must not rely only on a customer's word. You must use an independent source (like a corporate registry or government database) to confirm that the organization they claim to belong to actually exists.
- **Confirm Status:** You must confirm the customer's relationship with that group is current and in good standing at the time of the transaction.
- **Gather Evidence:** You 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:** You must obtain "informed consent" (clear permission) from the individual before collecting or using their digital identity data.
- **Keep Clear Records:** You must maintain your own records of the verification, including the date it happened, the source used, and the specific information obtained.
- **Accessibility:** You should ensure and be able to demonstrate that your identity verification process is accessible to all customers (referencing WCAG 2.0 level AA standards)

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.

4. Example of Auto Sales Transaction

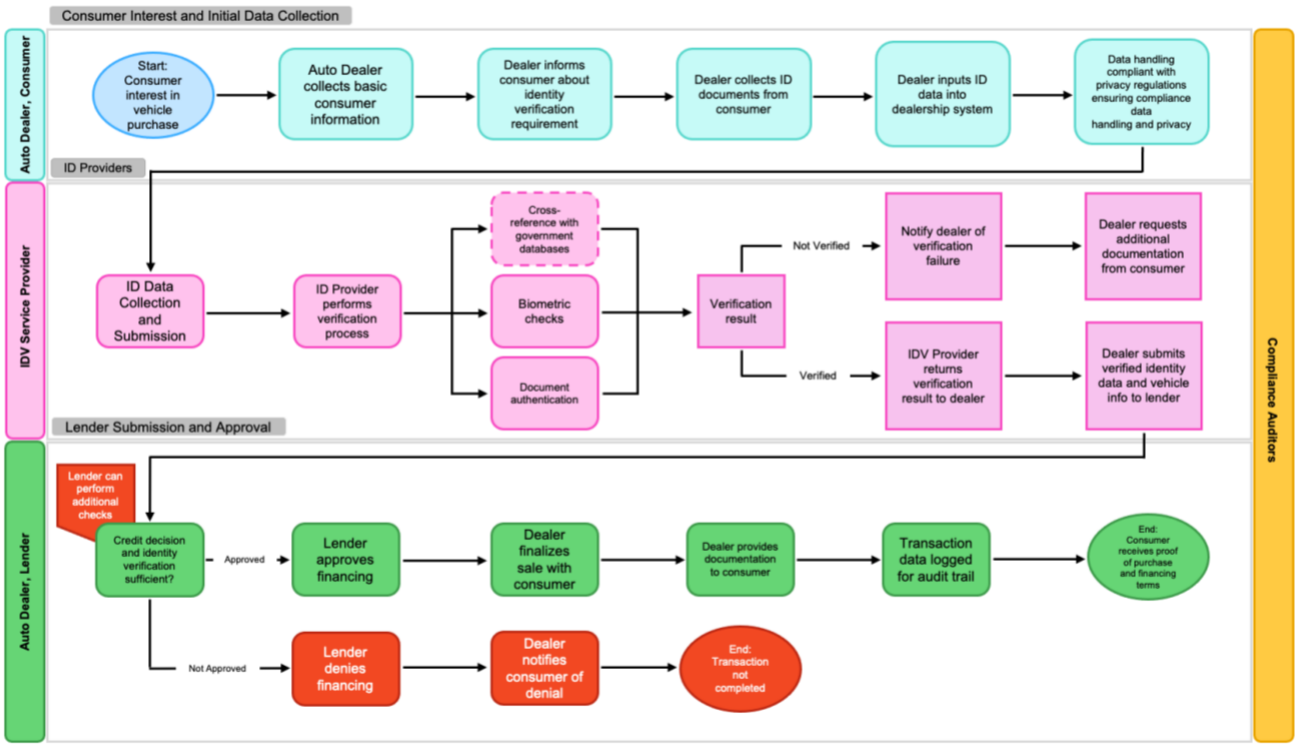

Figure 1. Trusted Process Example (non-normative): Auto Sales Transaction

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 two distinct but interconnected audiences:

1. Automotive Dealerships that are generally not REs under FINTRAC, where the primary need is to strengthen KYC procedures to prevent and detect identity fraud; and
2. Leasing and Finance Entities that are REs under FINTRAC, which have statutory AML and KYC compliance obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

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 and synthetic fraud threats. 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.

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

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, a Canadian provincial or territorial government (or a foreign government if the identification document is equivalent to a Canadian-issued identification document) may be used. Identification documents issued by Canadian or foreign municipal governments **MUST NOT** be used.

Affiliate or Member Method

The identity of a person may be verified by confirming that one of the following entities previously verified the person's identity:

- An affiliate that is a reporting entity referred to in any of paragraphs 5(a) to (5g) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act 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;

- A foreign affiliate of that carries out activities outside of Canada that are similar to the activities of a reporting entity referred to in any of paragraphs 5(a) to (g) of the Act; or,
- A financial entity that is subject to the Act and is a member of your financial services cooperative or credit union central.

Reliance Method

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 Proceeds of Crime (Money Laundering) and Terrorist Financing Act 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.

345

	Reference	Conformance Criteria
345a	**Reference**	**Conformance Criteria**
345b	**102**	**PCTF Automotive Identity Profile**
345c	**102.1**	**Client Identification and Verification**
345d	**102.1.1**	**Credit File Method**
345e	**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).
345f	**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.
345g	**102.1.1.30.1**	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.
345h	**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.
345i	**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).

345j	**102.1.1.70.1**	The Responsible Authority **MUST** collect and return all the following data points to the Relying Party (e.g., TBD based on introduction details): • 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.
345k	**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.
345l	**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.
345m	**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.
345n	**102.1.1.120**	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, • Up to six (6) home addresses maximum.
345o	**102.1.2**	**Dual Process Method**

345p	**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.)
345q	**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.
345r	**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.)
345s	**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.
345t	**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.
345u	**102.1.2.51**	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.

345v	**102.1.2.60.1**	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 authentic, valid and current; and, • Originate from, or are issued by, the Reliable Source or, alternatively, are obtained directly from the Reliable Source.
345w	**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.
345x	**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.
345y	**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.
345z	**102.1.3**	**Photo ID Method**

345aa	**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 licence, 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.
345ab	**102.1.3.20**	The Responsible Authority **MUST** use technology capable of verifying the authenticity of an identity document to evaluate the security features of the government-issued photo identification document and verify that it is a valid document issued by the Authoritative Source (e.g., federal, provincial, territorial, or foreign government).
345ac	**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.)
345ad	**102.1.3.40**	The Responsible Authority **MUST** enforce the capture of government-issued photo identification documents in real time and prevent the uploading of an image file.

345ae	**102.1.3.50.3**	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 that we are identifying.
345af	**102.1.3.60**	The Responsible Authority **MUST** document their conformity claims to WCAG 2.0 level AA or better, as specified in the standard. (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.)
345ag	**102.1.3.70.1**	The Responsible Authority **MUST** use reliable technology to compare the features of the real-time selfie to the photo on the authentic government-issued photo identification document.
345ah	**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.
345ai	**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.)

345aj	**102.1.3.100**	The Responsible Authority completing the government-issued photo Identification Method **SHOULD** have the Liveness check certified for Presentation Attack Detection according to the following criteria: ISO 30107-3 (certified by a third-party). (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.)
345ak	**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)
345al	**102.1.4**	**Affiliate or Member Method**
345am	**102.1.4.10**	The Responsible Authority **MUST** verify that the individual is an affiliate or member of an entity that the Responsible Authority has confirmed exists through independent verification.
345an	**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.
345ao	**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.
345ap	**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.
345aq	**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.

345ar	**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.
345as	**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.
345at	**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.
345au	**102.1.4.90.1**	The Responsible Authority **MUST** retain records of the entity verification in accordance with applicable regulatory requirements, 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.
345av	**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.
345aw	**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.
345ax	**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.
345ay	**102.1.5**	**Reliance Method**
345az	**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.
345ba	**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.

345bb	**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.
345bc	**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.
345bd	**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.
345be	**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.
345bf	**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.
345bg	**102.1.5.80**	The Responsible Authority **MUST NOT** rely on a third-party verifier for identity verification if the third-party itself relied on another entity for the verification, unless that chain of reliance is explicitly permitted by regulation.
345bh	**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.
345bi	**102.1.5.100**	The Responsible Authority **MUST** maintain documentation of the reliance relationship, including the agreement, evidence of the third-party verifier's regulatory status, and records of information transfers.
345bj	**102.1.6**	**Digital Credentials Method**
345bk	**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.

345bl	**102.1.6.20**	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.
345bm	**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.
345bn	**102.1.6.40**	The Responsible Authority **MUST** verify that the digital credential is current, has not expired, and has not been revoked by the issuer at the time of identity verification.
345bo	**102.1.6.60**	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 standards, W3C specifications, national digital identity frameworks).
345bp	**102.1.6.70.1**	The Responsible Authority **MUST** obtain informed consent from the individual for the collection and use of digital credential information.
345bq	**102.1.6.80.1**	The Responsible Authority **MUST** implement mechanisms to check the published revocation status of digital credentials during the verification process.

346

347

348

349

350

351

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.