Proposed mDL Metadata Framework to support KYC & CIP Compliance for the United States

Author: Juliana Cafik

October 29, 2025

With sincere appreciation, I would like to thank the following individuals for their invaluable expertise throughout the development of this work: Ryan Galluzzo (NIST); Bill Fisher (NIST); Gail Hodges (OIDF); Mark Haine (SelectID, OIDF); Mike Jones (Self-Issued Consulting); George Fletcher (Practical Identity) & Tim Cappalli (Okta).

Note to Reader:

This document presents a proposed metadata framework for mobile driver's license (mDL) adoption for high-assurance identity verification to support KYC and CIP compliance in U.S. financial institutions. It is intended as a draft for discussion and feedback from the identity, financial services, and regulatory communities. The recommendations, technical approaches, and operational flows described herein are not final standards or regulatory guidance. Stakeholder input is actively sought to validate, refine, and improve the framework. Readers are encouraged to review, comment, and contribute to the ongoing development of these requirements to ensure they meet the needs of all parties and align with evolving best practices and regulatory expectations.

Executive Summary

Traditionally, US financial institutions maintain control over the service providers and technologies that underpin the onboarding and account creation for their customers ensuring direct oversight of identity verification processes, risk management and regulatory compliance. Shifting to a decentralized credential model—where Cryptographically Verifiable credentials (VC's) such as mobile driver licenses (mDLs) serve as critical evidence for Customer Identification Program (CIP) and Know Your Customer (KYC) compliance marks a fundamental change for financial institutions. This transition requires extending trust beyond internal systems and trusted service providers, to external entities including credential issuers and digital wallets.

While current guidance and standards—such as the National Institute of

Standards and Technology (NIST) Digital Identity Guidelines Special Publication 800-63-4, the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards 18013-5 and 18013-7 for mobile driver's licenses, and the American Association of Motor Vehicle Administrators (AAMVA) guidelines, establish foundational controls, they lack consistent, machine-readable mechanisms to convey assurance and provenance at the level of fidelity required for Financial Institution high-assurance account onboarding. As a result, institutions face challenges in reliably mapping decentralized credentials to regulatory requirements to achieve the transparency needs for robust CIP and KYC compliance.

A standardized metadata framework helps to bridge these gaps by translating trust signals into structured attributes, such as credential provenance, assurance levels, authentication method, context, and compliance indicators, enabling auditable, interoperable workflows that introduce transparency into third-party processes to establish a shared state of awareness across disparate parties.

1. Context & Scope

1.1 Context

The adoption of Mobile Driver's Licenses (MDLs) for satisfying Know Your Customer (KYC) and Customer Identification Program (CIP) compliance presents significant challenges for Financial Institutions (Fis). Uncertainty remains around how these emerging standards map to existing regulatory requirements, and institutions often lack the necessary context and fidelity to confidently assess and manage third party risk associated with mDL issuers and digital wallets. The legal framework for Know Your Customer (KYC) and Customer Identification Program (CIP) requirements is primarily shaped by regulations designed to prevent financial crimes. These rules mandate that FIs must verify the identity of their customers and assess associated risks prior to opening an account. In practice, identity verification involves several key steps to ensure the authenticity and integrity of customer identities and to comply with KYC & CIP obligations. However, current processes do not yet extend to accepting Verifiable Credentials (VCs) such as mDLs as valid forms of identity verification.

Unlike traditional identity verification systems managed internally by FIs, which allow for direct oversight and rapid threat response, mDLs introduce third-party dependencies. These external processes vary in rigor and transparency, limiting an FI's ability to independently validate identity claims and respond to emerging risks. Despite the potential security, privacy, and usability benefits of mDLs, this lack of operational control has remained a barrier to widespread adoption.

The NIST National Cybersecurity of Excellence Project (NCCoE), through its Digital Identities – Mobile Driver's License project, is playing a pivotal role in advancing the adoption of mDL standards and best practices to support higher-assurance identity verification, while satisfying financial institution KYC processes and CIP requirements. Financial Institutions participating in the NCCoE mDL initiative have identified critical concerns related to the enrollment, issuance, and presentation workflows of mDLs. Their primary focus centers on evaluating assurance levels and managing risk exposure when relying on external entities, such as state-level issuers and wallet providers.

To help address these concerns, NIST NCCoE has published SP 800-63A Profile for mDL Issuance (800-63 Profile) which recommends controls selected from SP 800-63A Digital Identity Guidelines (SP 800-63A) to promote greater consistency in how mDLs are issued into digital wallets.

Primary Gaps Limiting Financial Institution Adoption:

1. Identity Evidence Validation:
   Issuers may apply inconsistent standards for identity proofing—ranging from the type and quality of source documents to the rigor of document authentication and database corroboration against DMV and ancillary records. Practices for evidence binding and retention practices also vary, reducing auditability for financial institutions.
2. Binding and Presentation Context:
   Wallet device binding and revocation signaling may also vary. These variations impact a financial institution's ability to trust credential provenance, evaluate assurance at the point of use, and retain evidence required for CIP compliance.

Without normalizing these variances and conveying them through a standardized, auditable metadata model, financial institutions will be challenged to reliably map mDL presentations to consistent KYC/CIP controls or confidently accept the associated third-party risk.

The Open Identity Foundation (OIDF) has commissioned a significant body of work that underscores its commitment to advancing secure, interoperable, and privacy-preserving identity standards. Through its mission, OIDF fosters collaboration across sectors to build trusted digital identity ecosystems. This vision is actively realized through the efforts of its specialized working groups, including the Digital Credentials Protocols (DCP) and the KYC & Identity Assurance (IDA) Working Groups, which are instrumental in developing frameworks that support robust identity verification and credentialing. As part of this initiative, OIDF is a key contributor to the National Institute of Standards and Technology's (NIST) National Cybersecurity Center of Excellence (NCCoE) Project. By commissioning and contributing to this work, OIDF helps ensure that emerging identity solutions align with rigorous standards for security, privacy, and interoperability— critical components for enabling scalable and trustworthy digital services

1.2 Scope

Building on the foundational work done within the NCCoE and the OIDF KYC, Identity Assurance (IDA) and Digital Credentials Protocols (DCP) Working Groups, this document recommends structured metadata to convey assurance levels in a standardized interpretable format that enables Relying Parties to make informed decisions for new account onboarding. It focuses specifically on a metadata framework for mobile driver's license (mDL) implementations governed by ISO/IEC 18013-5/7, the identity proofing requirements outlined in NIST Special Publications 800-63A/B/C and American Association of Motor Vehicle Administrators (AAMVA) mDL Implementation Guidelines.

To support high-assurance use cases, such as financial account opening, metadata must provide clear, verifiable signals enabling financial institutions to assess risk and confidently comply with regulatory requirements. By defining a baseline set of metadata attributes, both issuers and wallets can actively contribute to a reliable assurance framework. The goal is to deliver assurance data that is consistent, auditable and interoperable across all parties.

The scope of this document deliberately excludes non-US jurisdictions, authentication for recurring account access, biometric verification methods, wallet architecture, and cryptographic protocols except where such components directly impact metadata required for financial compliance, including guidance informed by NIST and ISO/IEC18013 standards.

1.3 Metadata Standardization

Current mDL architectures and standards lack a unified metadata framework for issuance, wallet functions (such as holder binding and authentication), and presentation events, limiting a financial institution's ability to audit and verify mDL transactions reliably. Embedded structured metadata that conveys assurance, allows Relying Parties to make informed decisions without interpreting the technical details of each implementation.

Establishing standardized metadata and clear standards mappings is critical to ensure mDLs, and other verifiable credentials are trustworthy, interoperable, and capable of enahancing financial institutions' agility in threat response, while meeting regulatory compliance obligations for KYC and CIP.

1.4 Establishing a Trust Layer

Metadata allows relying parties (RPs) to evaluate a credential at runtime—without needing direct access to the issuer's systems. It provides structured, machine-readable information such as:

- Credential provenance.
- Level of Assurance indicators.
- Authentication methods.
- Compliance flags.
- Revocation status and.
- Jurisdictional Trust Framework.

1.5 Supporting Interoperability

Mapping metadata to recognized standards reduces fragmentation, enables scalable adoption and ensures:

- Consistency across jurisdictions and platforms.

- Interoperability between wallets, issuers, and relying parties.
- Regulatory alignment with KYC/CIP.
- Security, auditability, and extensibility for evolving identity ecosystems.

1.6 Enabling Risk-Based Decisioning

Embedding metadata aligned to standards supports:

- Bank risk-based access decisions (e.g. step-up identity verification for high value transactions).
- Reducing unnecessary friction (e.g. avoiding extra biometric checks) when metadata indicates high assurance.
- Auditability, non-repudiation and regulatory compliance (CIP/KYC).
- Interoperability and policy enforcement across platforms.

1.7 Supporting Stakeholder Collaboration

A shared metadata schema:

- Creates a common language for issuers, wallet providers and relying parties.
- Enables policy enforcement without centralized control.
- Ensures interoperability and scalability across jurisdictions and platforms.
- Supports auditability, assurance, and privacy-preserving practices.
- Aligns with regulatory frameworks (e.g. NIST SP 800-63-4, FFIEC and CIP) and emerging standards.

1.8 Cryptographic Assurance

Metadata acts as a sharable context layer allowing Relying Parties to interpret and trust the cryptographic properties and the presentation of a credential. It helps demonstrate:

- Origin and authenticity.
- That the credential is held and presented by the rightful holder.
- Tamper-evidence and integrity of the data.
- Revocation status and trust anchor references for validation.

1.9 Holder Consent

Holder consent refers to the explicit, verifiable permission granted by a credential holder to share or use their identity data under defined conditions. Consent is conveyed through authentication metadata, between the wallet and the issuer and subsequently the wallet and the Relying Party. This includes acr (Authentication Context Class Reference) and amr (Authentication Methods References) values, which indicate the Authentication Assurance Level (AAL), per NIST 800-63 B, enumerate applied factors (e.g. knowledge possession, inherence) and specify authentication methods used. Conveying this metadata is ensures enforcement of assurance policies and accurate security context. Combined with OAuth and OpenID Connect, these values bind consent to a verified identity, enable traceability across its lifecycle, and support portability in federated environments. Reliable conveyance of this metadata is critical for CIP and KYC compliance, auditability and privacy preserving practices.

context and supports regulatory compliance for identity proofing and risk-based authentication.

The following key dimensions further illustrate this alignment:

1. Binding Identity to authentication context for Consent
   - NIST: Authenticators prove subscriber identity during authentication. For consent, they ensure the same verified identity is linked to the consent action.
   - KYC: Consent must be attributable to a verified person, not an anonymous actor.
   - OAuth: The authorization server authenticates the user before issuing tokens. Consent is captured during authorization.
   - Acr/amr: The authorization server reports authentication characteristics using acr and amr values, indicating the assurance level and the factors applied.
2. Federated Identity and Consent Assertion:
   - NIST: In federated scenarios (OpenID Connect), acr and amr values must be included in the assertion.
   - KYC: These values enable downstream relying parties to trust consent records, supporting interoperability and compliance requirements.
   - Regualtory readiness: Incorporates lifecycle management (including holder-requested revocation and consent withdrawal), auditability and privacy-preserving practices, and non-repudiation for legal enforceability.

1.10 CIP & KYC

The Customer Identification Program (CIP) mandated under the Bank Secrecy Act (BSA) is the statutory minimum and a foundational step in a FIs broader Know Your Customer (KYC) obligations. CIP requires that financial institutions verify the identity of individuals and entities seeking to open new accounts. Key elements of CIP relevant to mDL are:

1. Identity verification procedures to establish a reasonable belief of customer identity.
2. Minimum information: full name, date of birth, address, and identification number (e.g., SSN for U.S. persons, passport number for non- U.S. persons).
3. Acceptance of government-issued photo ID's that are authentic, verifiable and issued by a trusted authority.
4. Recordkeeping of identity verification data.

KYC expands in CIP and includes:

1. Customer Due Diligence (CDD): Assessing the nature and purpose of customer relationships.
2. Enhanced Due Diligence (EDD): Applying stricter scrutiny to high-risk customers.
3. Ongoing monitoring and AML compliance.

mDl metadata can strengthen CIP/KYC by providing verifiable assurance levels, issuer provenance, and authentication context aligned with NIST SP 800-63-4, AAMVA guidelines and ISO/IEC 18013 standards.

1.11 ISO/IEC 18013-5 Trust Chain Overview

The ISO/IEC 18013-5 trust model establishes a hierarchical public key infrastructure to ensure the authenticity and integrity of mobile driver's licenses. At its foundation, the Issuing Authority Certificate Authority (IACA) acts as the root of trust for each jurisdiction, issuing Document Signer Certificates (DSCs) to authorized entities responsible for creating Mobile Security Objects (MSOs). Each MSO is cryptographically signed, and its authenticity is validated by verifying the signature against the DSC and tracing the certificate chain back to the IACA. This trust chain: MSO to DSC to IACA to Trust List—enables Relying Parties, such as FIs to confidently accept mDLs as Documentary evidence for regulatory compliance.

1.12 Selective Disclosure Integrity

Selective disclosure in mDLs is cryptographically protected by the MSO. Each disclosed attribute's hash is verified against the MSO, ensuring authenticity event when only partial data, such as and age over value, is shared. This mechanism allows the FI to validate individual attributes without exposing the entire credential, supporting privacy and data minimization.

1.13 Compliance Alignment

The ISO/IEC 18013-5 trust model provides a foundation for using mobile drivers licenses as documentary evidence for Customer Identification Program and Know Your Customer compliance. For FIs to accept mDLs as verified government-issued identity documents the credential must be cryptographically verifiable as an authentic photo ID issued by a trusted authority and there must be a 'reasonable belief' that it is the identity of the holder. To strengthen the reliability of mDL verification, US FIs should validate issuer certificates against the AAMVA Digital Trust Service. By referencing a recognized trust list, FIs can confirm that presented credentials originate from authorized and trusted sources, regardless of jurisdiction or wallet provider. This approach was taken in the NIST NCCoE Project to support interoperability, reduce third party risk and align with best practices for secure and compliant digital identity verification.

2. REAL ID

REAL ID establishes requirements for issuing physical identity cards but does not address the creation or provisioning of a digital mDL to a wallet. For FIs to accept mDLs as valid evidence under CIP, they must have assurance that robust identity proofing was performed during issuance, and that the credential is authentic, cryptographically bound to the holder, and accurately represents their identity. Metadata indicating REAL ID compliance, issuer provenance, and lifecycle status further supports auditability and regulatory readiness.

2.1 REAL ID Identity Proofing

To ensure mobile drivers licenses meet financial institution compliance requirements it is essential to understand the identity proofing prerequisites established by REAL ID. These requirements verify authenticity and legitimacy before issuing a REAL-ID compliant physical or digital credential. The process involves multiple layers of verification and documentation, providing assurance for CIP acceptance of mDLs as reliable identity evidence.

Mandatory checks include:

1. Verification of a photo identity document (or non-photo with full legal name and date of birth).
2. Confirmation of date of birth.
3. Validation of Social Security Number or confirmation of ineligibility
4. Confirmation of principal residence address.
5. Evidence of lawful status (e.g. citizenship, visa, asylum. Refugee status).

Supporting procedures include:

1. Document verification with issuing agencies.
2. Use of Systematic Alien Verification for Entitlements (SAVE) system for non-citizens.
3. Retention of source documents for auditability (7-10 years).
4. Mandatory facial image capture.
5. Fraudulent document recognition training for staff.

For mDL acceptance, these checks should align with NIST IAL standards, incorporate cryptographic binding to the holder, and support auditability, privacy preserving practices, and lifecycle management.

2.2 REAL ID FLAG

The REAL ID flag is a designation on a physical ID card, or mobile driver's license, that indicates compliance with the US Federal REAL ID Act requirements, confirming that the holder has undergone enhanced identity proofing. In an mDL this flag is implemented as an attribute within the data structure, and its integrity is protected by the Mobile Security Object (MSO).

The REAL ID compliance status, "F" for fully compliant and "N" for non-compliant, is included as a data element in the mDL payload. The MSO contains hashes of all data elements, including the REAL ID flag and is cryptographically signed by the issuer. This process binds the REAL ID flag, and all other attributes, to the credential. During verification, the FI, or Relying Party, validates the MSO signature, checks the certificate chain, and recomputes hashes to confirm the REAL ID flag matches what the issuer signed consistent with IOS/IEC 18013-5 and AAMVA mDL implementation guidelines.

To improve interoperability and compliance signalling the REAL ID status can also be conveyed as a metadata field, such as DHS_compliance, using values "F" and " N". This approach leverages ISO/IEC 18013-5 standards and aligns with the NIST SP 800-63 mDL Assurance Profile, which maps mDL issuance processes to assurance requirements and enables relying parties to assess trustworthiness.

The MSO is defined in ISO/IEC 18013-5, Section 8.2.2 as a cryptographically signed container that encapsulates: core identity attributes, document metadata, hashes of each data element and issuer metadata, validity and digital signature. This structure supports:

- Integrity and Provenance: Cryptographic signatures and hashes ensure every attribute presented originates from the issuer, providing tamper-evident provenance.
- Verification Events: Each mDL transaction involves validating the MSO signature, recomputing hashed and confirming values match the issuer's signed data. These verification events can be logged for auditability.
- Recordkeeping: The MSO's includes issuance and expiration dates, document numbers, and issuer identifiers supporting compliance with 31 CFR 1020.220 and FFIEC recordkeeping requirements.
- Auditability and Lifecycle Management: Standardized, machine-readable MSO data enables automated logging, revocation checks and verification history for internal audits and external regulatory reviews.

.

2.3 REAL ID Flag NIST Alignment

In the NIST 800-63A profile for mDL issuance, control EV-1 refers to a single piece of strong evidence issued by the DMV where the applicant interacts directly with the issuing authority and identity proofing occurs during the physical credential issuance process.

The REAL ID compliant flag adds an additional layer of trust to EV-1 by confirming that the credential was issued under federally mandated proofing standards including:

- In-person identity verification.
- Validation with the issuing authority.
- Meeting or exceeding the strength required for IAL2 identity assurance.

Inclusion of the REAL ID is not required for KYC/CIP; however, it significantly enhances assurance across key dimensions:

- Upstream Issuance Assurance: Demonstrates issuance under DHS standards, including in-person identity proofing, source document verification, lawful status checks, proof of residence, and enhanced security controls.
- Greater Confidence in Attribute Authenticity: Confirms that core identity attributes, such as name, date of birth, and address, were verified by a trusted authority prior to issuance, reinforcing the cryptographic integrity provided by the MSO.
- Risk-Based Decisioning: Serves as a positive risk indicator, potentially reducing reliance on weaker non-documentary methods (e.g., knowledge-based authentication) when other controls are satisfactory.
- Audit and Examiner Justification: Provides clear rationale for treating the ID as high assurance, supporting compliance during FFIEC or internal reviews.
- Standards-based Interoperability: Embedding the REAL ID flag within ISO/IEC 18013-5 and AAMVA compliant metadata ensures consistent interpretation across wallets, issuers, and relying parties, enabling scalable adoption and reducing fragmentation.

2.4 MSO Data Elements

The MSO is critical for verifying that data provided by the mDL holder has not been altered and originates from a trusted issuer. Defined in ISO/IEC 18013-5 as part of the security framework supporting both offline and online verification, the MSO structure and its metadata fields are defined and governed by: ISO/IEC 18013-5, for mDL data format and presentation and ISO/IEC 18013-7 for trust and interoperability profiles.

The MSO is generated and signed by the issuing authority. Key data elements include:

- Document type: e.g. mDL.
- Certificated references for signature validation.
- Issuers digital signature over the MSO.
- Device Key Information (optional): device binding, key ID, binding level.

- Core identity attributes: e.g., family name, given name, birth date, place of birth, nationality, sex, portrait, portrait capture date, signature (usual mark), age attestation.
- Residence address.
- Document metadata: document number, issue date, expiry date, issuing country, issuing authority, issuing jurisdiction.
- Hash algorithm identifiers and MSO version.
- Revocation status (Optional).
- REAL ID Compliance Flag: Fully (F), Non (N).

2.5 Standards-Based Party Roles in an mDL Metadata Framework

An mDL metadata framework relies on the coordinated among multiple ecosystem participants, fulfilling distinct responsibilities across the credential lifecycle. This collaborative, standards-driven approach ensures transparency, interoperability, and regulatory alignment for identity verification and financial compliance.

2.6 NIST-based Architecture Party Roles in an mDL Metadata Framework

In the NIST NCCoE reference architecture, notice and consent to release mDL data is primarily presented by the wallet (holder-controlled app) during the presentation step. However, a financial institution app can play an alternate, or complimentary, role for consent, particularly for FI policy-based use-of-data specific consent and federated sharing.

Financial Institution policy-based notice & consent:

- Relying Party App UX – Use of Data Consent Before/After Verification: In the NCCoE flows, the FI app initiates identity proofing and orchestrates the verifier call. Data-use, retention and revocation notices can be presented and captured per FI policy prior to invoking the mDL presentation request. *Note*: ISO/IEC 18013 requires the holder to control selective disclosure, FI consent cannot replace wallet consent for attribute release but can cover how the FI processes, stores and shares received data.
- Authorization Server (idP) Consent Screens for Federation: If the FI uses OpenID Connect (OIDC) for sign-in/federation, consent prompts typically occur at the Authorization Server (AS), which may be operated by the FI. The AS collects consent for scopes/claims requested, and the FI app can record granular consent to release claims when requested. This can be used to record granular consent in addition to the wallet's consent for attribute release. NCCoE interaction diagrams highlight OIDC as a key component for federated flows.
- Verifier Orchestration Policy Screen – Prior to Wallet Redirect: The FI app can present a purpose-specific notice and capture consent prior to redirecting the mDL holder to the wallet's selective disclosure screen, making the user journey is explicit and auditable for compliance.
- Align Consent Flows with Standards: Implement consent signaling consistent with ISO/IEC 29184, which specifies controls for the content and structure of online privacy notices, and NIST SP 800-63C for federation assurance.
- Log Consent Events with Assurance Context: Record acr/amr values and verifier outcomes alongside current events to support FFIEC audits and regulatory reviews.

2.7 Ecosystem Party Roles and Consent Placement Summary

The following table provides a comprehensive view of the roles and responsibilities of key ecosystem participants within an mDL metadata framework. It highlights how each party contributes to Mobile Security Object (MSO) management, REAL ID compliance, and financial institutions obligations under CIP/KYC. In addition to operational roles, the table integrates lifecycle management, privacy and consent considerations, and consent placement touchpoints based on the NIST NCCoE reference architecture. This structured approach ensures transparency, interoperability, and regulatory alignment across the credential lifecycle, supporting both technical assurance and compliance requirements.

Party / Provisioning Role	Primary Role in MSO	Primary Role in REAL ID Flag	Supporting Guidance & Standards	KYC/CIP Compliance	Lifecycle & Revocation	Privacy & Consent	Consent Placement Summary
Issuing Authority (State DMV)	Issues MSO, generates/signs MSO, manages PKI, defines data elements	Assigns REAL ID flag per DHS standards	ISO/IEC 18013-5, ISO/IEC 18013-7, AAMVA Guidelines, REAL ID Act	Provides identity documents for CIP	Handles credential issuance, updates, and revocation	Ensures lawful collection and retention of source documents	N/A – Consent handled at wallet level
Digital Wallet	Stores/presents mDL, conveys MSO and issuer chain	Displays REAL ID status if provided by issuer	ISO/IEC 18013-5, AAMVA Guidelines	Provides wallet attestation and integrity evidence	Manages credential lifecycle within wallet	Implements consent signaling per ISO/IEC 29184	Primary consent point for selective disclosure during presentation
Wallet Holder (Individual)	Authenticates to wallet, consents to share attributes	Obtains REAL ID credential via in-person proofing	ISO/IEC 18013-5, REAL ID Act	Subject of CIP verification	Requests updates or revocation through issuer	Provides explicit consent for data sharing	Provides consent for attribute release in wallet
Verifier / Reader (FI device)	Requests attributes, validates MSO and issuer cert chain	Checks REAL ID flag as risk signal	ISO/IEC 18013-5, ISO/IEC 18013-7	Validates identity attributes and document authenticity	Logs verification events for audit	Ensures consent metadata is honored	Displays purpose-specific notice before redirect to wallet
Relying Party (Financial Institution)	Defines requested attributes, logs MSO validation outcomes	Treats REAL ID flag as positive risk indicator	31 CFR 1020.220, FFIEC BSA/AML Manual	Performs identity verification and recordkeeping	Maintains audit logs and revocation checks	Enforces consent policies in federated flows	Use-of-data consent before/after verification in FI app UX
Identity Provider (Federation)	Optionally conveys verified claims referencing mDL	No role in REAL ID issuance	OpenID Connect for Identity Assurance, NIST SP 800-63	Supports CIP by conveying verified identity attributes	Updates federated trust relationships	Provides consent granularity and portability	OIDC consent screens for scopes/claims at AS
Trust Service / PKI	Publishes issuer certificates and trust anchors	No role for REAL ID flag	AAMVA Guidelines, ISO/IEC 18013-7	Supports CIP indirectly by enabling trust in identity checks	Maintains certificate lifecycle and revocation lists	No direct consent role	N/A
DHS / TSA (REAL ID oversight)	N/A	Sets/enforces REAL ID requirements	REAL ID Act, 6 CFR Part 37	No direct role in CIP compliance	Oversees compliance audits	No direct consent role	N/A

3.0 Proposed Metadata Framework

This document proposes a layered metadata framework to support Know Your Customer (KYC) and Customer Identification Program (CIP) compliance for mobile driver's license (mDL) adoption in the United States. The framework defines specific metadata elements as trust anchors for regulatory requirements with the REAL ID compliance flag serving as a machine-verifiable attribute that confirms a credential meets federally mandated identity proofing standards. The inclusion of the REAL ID compliance flag as an attribute in US mDL issuance is specified in the AAMVA Mobile Driver's License Implementation Guideline. Section 3.2 of the guidelines details the mDL data element set including the REAL ID regulatory compliance indicator, which is presented alongside the other standardized attributes.

3.1 Metadata - REAL ID Compliance Flag for CIP Compliance

The REAL ID compliance flag is a machine-verifiable attribute that indicates a credential was issued under federally mandated identity proofing standards. When cryptographically bound to the mobile driver's license (mDL) and included within the Mobile Security Object (MSO) alongside essential provenance and validity attributes, this flag enables financial institutions (FIs) to confidently rely on the credential as authentic, government-issued, and sufficient for meeting Customer Identification Program (CIP) statutory requirements. This supports automated, auditable, and interoperable compliance checks for high-assurance identity verification.

Under 31 CFR 1020.220, financial institutions must implement risk-based procedures to form a reasonable belief that they know a customer's identity before opening an account. The MSO provides cryptographic integrity and tamper-evident verification of mDL data, supporting a verifiable audit trail. Inclusion of the REAL ID compliance flag adds upstream provenance and signals that the credential was issued under Department of Homeland Security (DHS) standards. This assurance strengthens risk-based decisioning and enhances Know Your Customer (KYC) workflows, allowing FIs to meet regulatory obligations without replacing statutory minimums.

The AAMVA Mobile Driver's License Implementation Guidelines (Section 3.2) specify the inclusion of the REAL ID compliance flag as an attribute in US mDL issuance. ISO/IEC 18013-5 ensures key metadata fields and core identity attributes are part of its standardized structure. However, jurisdiction-specific regulatory indicators such as the REAL ID flag are defined by AAMVA and US regulatory requirements. Inclusion of the REAL ID flag would enable FIs to quickly and reliably determine whether a presented mDL meets federally mandated identity verification proofing requirements.

To ensure minimum compliance for CIP when adding the REAL ID flag several key conditions must be met:

- The REAL ID flag must be cryptographically bound to the credential.
- The issuer must be a recognized authority (e.g., DMV).
- The credential type must be "mDL".
- The validity period must be current (not expired).

From a privacy perspective, selective disclosure enables financial institutions to request only the metadata necessary for CIP compliance, minimizing the exposure of personal information. Standardized metadata fields, including a trust framework indicator, lay a future foundation for supporting the acceptance of mDLs from multiple jurisdictions.

The following table defines a trust framework specific metadata field to indicate REAL ID compliance for mDLs:

Trust Framework	Metadata Field	Description	Value	Source/Standard	Responsible Party
NIST	DHS_compliance	Indicates if the mDL is REAL ID compliant ("F" = Fully, "N" = Non-compliant)	F or N	ISO/IEC 18013-5, REAL ID Act, AAMVA Guidelines	Credential Issuer (DMV/Agency)

3.2 Expanded Metadata Framework for KYC Compliance

The proposed metadata framework enhances KYC capabilities by delivering standardized, machine-readable data that financial institutions can use to verify identity, assess risk, and maintain auditability throughout the credential lifecycle. While CIP compliance remains foundational, ensuring institutions can establish a reasonable belief in a customer's identity, the expanded schema addresses broader KYC requirements by incorporating:

- Wallet and device binding strength
- Presentation context
- Revocation status
- Audit trail information

These additional metadata elements enable institutions to evaluate assurance at the point of use, detect fraud, and meet regulatory obligations beyond CIP, such as Customer Due Diligence (CDD) and enhanced risk management for KYC compliance. The framework supports selective disclosure, allowing only the necessary attributes to be presented for compliance, minimizing exposure of personal information. Standardized, machine-readable metadata fields facilitate interoperability and acceptance of digital credentials across jurisdictions, resulting in a comprehensive solution for digital identity verification. The structured approach ensures credential provenance is trusted, assurance can be evaluated dynamically, and audit trail information is maintained using cryptographically protected, tamper-evident records. This guarantees that evidence is retained for CIP and broader KYC compliance requirements.

The table below maps key metadata fields to their responsible parties and aligns to the referenced standards and guidelines: NIST SP 800-63A/B, ISO/IEC 18013-5/7, OpenID Connect, W3C, and AAMVA:

Category	**Proposed Metadata Field(s)**	**Purpose**	**Responsible Party**
Identity Proofing	DHS_compliance	Identity Assurance	Issuer
Authentication	acr, amr	Conveys authentication context & method	Wallet / Relying Party
Holder Binding *(*noting placeholder further standards work to be completed (FIDO/WebAuthn))*	**proof_of_possession* **device_attestation* acr/amr	Cryptographic proof of possession	Wallet / Relying Party
Holder Consent	acr, amr	Verifiable consent record	Wallet
Verification	session_id	Links the presented credential to the original request	Verifier/Relying Party
Credential Status	credentialStatus, StatusList2021	Indicates current credential validity	Issuer
Revocation Freshness	status_check_timestamp	Implementation-level timestamp of last credential check	Wallet
Freshness Threshold	freshness_threshold	FI Implementation Policy driven freshness parameter	Relying Party
Verifier	audience	Unique Identifier of the Verifying Entity	Verifier/Relying Party
Validity Period	validFrom, validTo issuanceDate, expirationDate	Credential validity window	Issuer/ Verifier

4.0 mDL FI CIP & KYC Operational Flows for New Account Opening

4.1 Overview

This document details the operational steps for financial account onboarding using the recommended metadata framework for mobile driver's licenses. While it references the architectural approach outlined in the NIST NCCoE Mobile Driver's License Project, its primary focus is on highlighting the operational processes spanning all parties, aligned with FI regulatory requirements.

When an mDL holder requests credential issuance to their wallet, both credential status and authentication assurance metadata must be conveyed during issuance and authentication. This ensures trust, regulatory compliance, and addresses primary gaps limiting FI adoption, as outlined in Section 1.1.

To overcome these operational barriers this proposal emphasizes three critical elements:

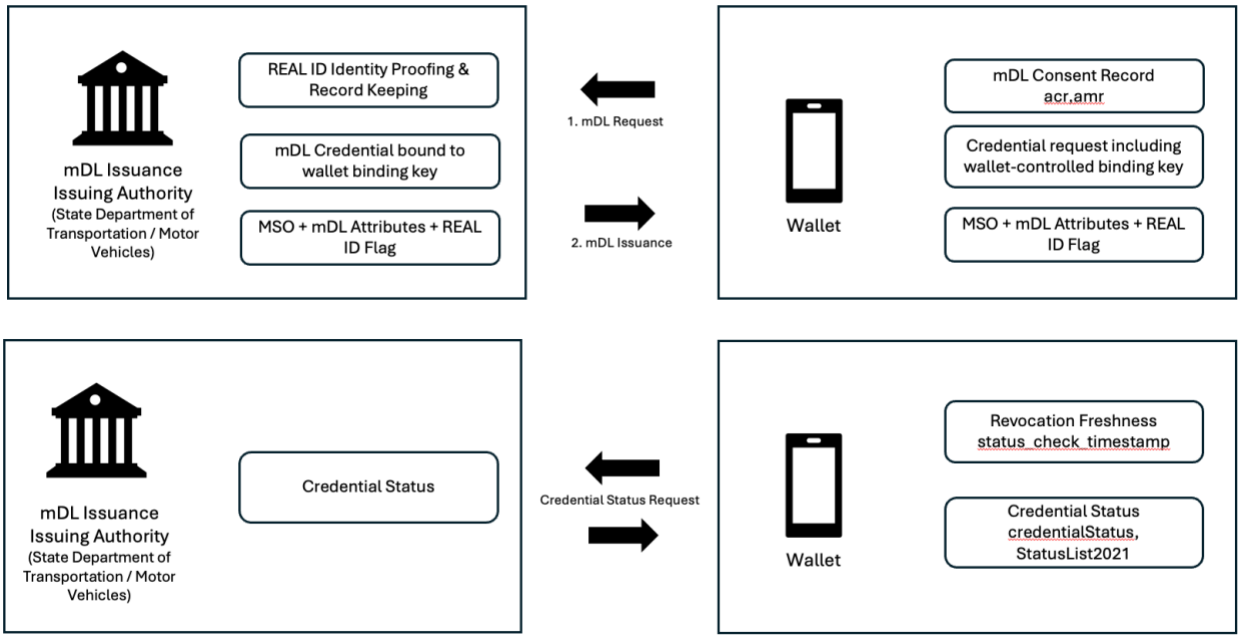
1. Propagation of authentication assurance metadata during issuance and presentation
2. Enforcement of revocation freshness,
3. Contextual binding of identity evidence

During issuance, assurance metadata should indicate the authentication strength under which the credential is provisioned. In OpenID Connect-based implementations, this may include acr (Authentication Context Class Reference), amr (Authentication Methods Reference), and a mapped NIST Authentication Assurance Level (AAL). While ISO/IEC 18013-5 does not mandate these elements, they are essential for informed consent and for verifiers to meet CIP and KYC requirements. In parallel, ISO/IEC 18013-5 requires mechanisms to verify revocation status and evaluate freshness to prevent reliance on stale or missing data. For FIs, credential validity cannot be inferred from the absence of revocation information; missing or outdated status may be treated as "unknown", and a policy-driven freshness threshold ensures revocation checks for compliance. Standardizing metadata exchange from issuer to wallet to verifier, combining assurance propagation, revocation freshness, and contextual binding of identity evidence is critical to preserve consent, prevent silent failures, and maintain regulatory compliance. Maintaining a tamper-evident audit trail for all credential lifecycle events further strengthens operational transparency and regulatory assurance.

4.2 mDL Holder Request and Issuance to the Wallet

The illustrated architecture addresses the critical operational barriers identified by the FIs for identity evidence validation, binding, and presentation context by adhering to ISO/IEC 18013-5 standards and guidance from AAMVA and NIST. It incorporates REAL ID proofing, wallet binding, and the propagation of authentication assurance metadata. This integrated approach supports regulatory compliance, interoperability, and high-assurance identity verification.

Identity evidence validation and binding are achieved through REAL ID identity proofing, demonstrated by the DHS-compliant REAL ID flag, and cryptographic binding of an mDL credential to the wallet's binding key. These steps ensure that the credential originates from a trusted issuer and is securely linked to the holder's wallet. Presentation Context is supported by the inclusion of authentication assurance metadata acr and amr values within the consent record during issuer authentication, enabling verifiers to evaluate the assurance level under which the credential was provisioned. Together, these mechanisms, aligned with ISO/IEC 18013-5. AAMVA, NIST and OpenID Connect, strengthen trust and compliance during issuance and presentation, forming a foundational first step for high- assurance onboarding workflows per the following diagram:



4.3 mDL Credential Status and Revocation Freshness

mDL credential status and revocation freshness are critical components of trust and compliance with both ISO/IEC 18013-5 and KYC requirements. ISO/IEC 18013-5 specifies mechanisms for verifying whether an mDL has been revoked and mandates that revocation information must be evaluated for freshness to prevent reliance on stale or missing data. A credential's validity cannot be inferred solely from the absence of revocation data; instead, missing or outdated status data should be treated

as “unknown” and handled according to the financial institution’s policy, particularly in high-assurance use cases such as CIP and KYC.

The diagram above illustrates how this requirement is operationalized through the following fields:

- status_check_timestamp: Indicates the last date & time of the last revocation check performed by the wallet.
- freshness_threshold: A FI policy-driven parameter that defines the maximum allowable age of revocation data before it is considered stale. Note the wallet adheres to this policy but does not establish it.

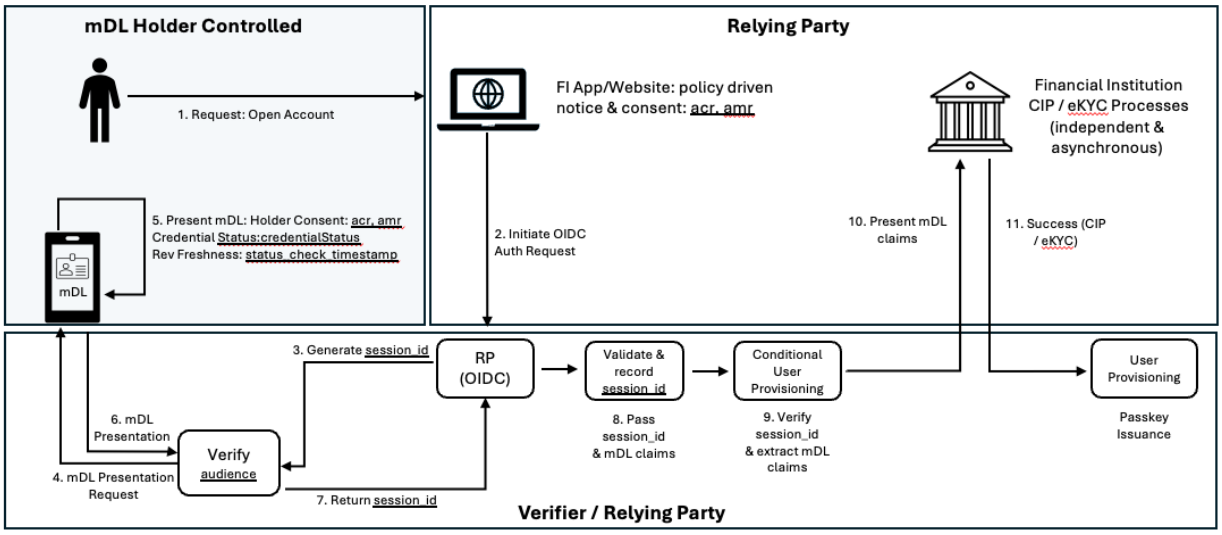
The wallet is responsible for maintaining and transmitting these metadata elements during credential presentation, ensuring that verifiers can assess both the status and freshness of revocation information in real time. This approach aligns with ISO/IEC 18013-5, NIST SP 800-63B, and financial compliance frameworks, enabling institutions to dynamically evaluate assurance, mitigate fraud risk, uphold regulatory obligations, and maintain a tamper-evident audit trail for operational transparency.

4.4 FI Account Opening Registration Flow

This diagram illustrates the end-to-end flow of mDL presentation in a high-assurance context, based on the NIST NCCoE architecture, beginning with the holder’s request to open an account and culminating in CIP/KYC compliance by the Financial Institution. The process integrates OpenID Connect for authentication and session management, where the relying party generates, and records, a session_id to correlate the mDL presentation with the initial authentication request. During issuance and presentation, authentication assurance metadata for acr and amr, and the mapped NIST AAL (Authentication Assurance Level), is propagated to inform holder consent and strengthen FI trust. The verifier/relying party validates the mDL claims, or attributes along with the REAL ID compliance flag, before passing them to the FI for conditional user provisioning pending completion of the out of band CIP/KYC processes. This flow assumes the FI maintains its existing compliance processes and checks and adds a high assurance identity verification process and associated elements to it. This architecture ensures that assurance context, credential integrity, and regulatory requirements are consistently enforced across issuer, wallet and verifier interactions.

Additionally, the asynchronous account provisioning model allows FIs to decouple identity verification from real-time onboarding enabling:

- Operational Efficiency: FIs can process CIP/KYC checks independently without impacting the user experience.
- Scalability: High-volume account requests can be queued and processed without synchronous bottlenecks.
- Risk management: Compliance checks occur in a controlled back-end workflow, reducing exposure to fraud during live sessions.
- Improved UX: Users can initiate account creation and consent to mDL presentation without waiting for full CIP/KYC completion.



This architecture may facilitate financial institutions adoption of mobile driver's licenses by leveraging standardized, interoperable metadata, modular integration points, real-time assurance, and clear operational roles. Financial institutions can confidently consume, and dynamically act on, identity metadata, streamline onboarding and compliance, and maintain robust audit trails, based on existing standards and protocols.

The architecture further enhances these capabilities by utilizing the proposed standardized metadata fields to address the core operational and regulatory needs of financial institutions. These metadata elements enable seamless integration, dynamic risk management, and regulatory alignment. As a result, financial institutions may benefit from improved interoperability, efficient compliance processes, and strengthened trust in digital identity transactions across the ecosystem.

Streamlined Integration and Interoperability:

- Standardized metadata fields ensure that all parties speak a common language, making it easier for FIs to integrate mDLs into existing onboarding, authentication, and compliance workflows.
- OIDC-based session management (session_id) and assurance claims (acr, amr) are natively supported by most platforms, reducing implementation complexity and accelerating adoption.

Real-Time, Policy-Driven Assurance:

- Credential status and compliance flags (e.g., DHS_compliance) are presented in real time, enabling FIs to dynamically assess the validity and regulatory compliance of credentials at the point of use.
- Freshness and auditability are maintained through session tracking and metadata recording, allowing FIs to meet regulatory requirements for CIP, KYC, and audit trails.

Clear Roles and Responsibilities:

- The wallet acts as the steward of key metadata, ensuring that the latest credential state, assurance level, and consent are transmitted during each transaction. This reduces operational burden for FIs and ensures reliable, up-to-date information.
- Verifiers and relying parties validate and record session and credential metadata, supporting seamless handoff and reducing friction in multi-party environments.

Regulatory and Standards Alignment:

- Metadata fields are mapped to global standards (NIST SP 800-63A/B, ISO/IEC 18013-5, OpenID Connect), making it easier for FIs to demonstrate compliance and interoperability during audits or regulatory reviews.
- Compliance flags and assurance metadata provide clear evidence for regulatory reporting and risk management.

Enhanced Fraud Detection and Risk Management:

- Session tracking and assurance metadata enable FIs to detect anomalies, flag suspicious activity, and trigger step-up verification.
- Audit trails support rapid investigation and resolution of disputes or incidents.

4.5 NIST NCCoE Architecture 18013-5 mDL Metadata Mapping to NIST Assurance

The following table illustrates the alignment between ISO 18013-5 mDL attributes, their corresponding OIDC Claims and NIST 800-63-4 Assurance Levels. By establishing these relationships, financial institutions can integrate mobile driver's licenses (mDLs) into identity verification and compliance workflows using globally recognized standards.

ISO 18013-5 Attribute	OIDC Claim	NIST Assurance	Proposed Metadata Field(s)	Purpose	Responsible Party
family_name	family_name	IAL2+	—	Identity attribute	Issuer
given_name	given_name	IAL2+	—	Identity attribute	Issuer
birth_date	birthdate	IAL2+	—	Identity attribute	Issuer
document_number	document_number	AAL2+	—	Credential binding	Issuer
issue_date	document_issue_date	Lifecycle evidence	issuanceDate	Credential validity window	Issuer
expiry_date	document_expiry_date	Lifecycle evidence	expirationDate	Credential validity window	Issuer
issuing_authority	issuing_authority	Trust alignment	—	Credential issuer info	Issuer
portrait	picture	Optional biometric	—	Holder verification	Issuer

address	address	IAL2+	—	Identity attribute	Issuer
Identity Proofing	—	IAL2+	DHS_compliance	Identity assurance	Issuer
Authentication	acr, amr	AAL2/AAL3	acr, amr	Authentication context & method	Wallet / RP
Holder Binding	—	AAL3 (future)	*proof_of_possession*, *device_attestation*	Cryptographic proof of possession	Wallet / RP
Holder Consent	—	FAL2+	acr, amr	Verifiable consent record	Wallet
Verification	—	FAL2+	session_id	Links credential to request	Verifier / RP
Credential Status	—	Lifecycle evidence	credentialStatus, StatusList2021	Indicates current validity	Issuer
Revocation Freshness	—	Lifecycle evidence	status_check_timestamp	Timestamp of last check	Wallet
Freshness Threshold	—	FI Policy-driven	freshness_threshold	FI freshness parameter	RP
Verifier	—	FAL2+	audience	Unique verifier ID	Verifier / RP
Validity Period	—	Lifecycle evidence	validFrom, validTo	Credential validity window	Issuer / Verifier

4.6 Summary

The use of standardized metadata within this architecture may empower financial institutions to confidently adopt decentralized identity solutions, streamline operational processes, meet regulatory requirements, and enhance fraud detection and risk management. By aligning with globally recognized standards such as ISO/IEC 18013-5, NIST SP 800-63, and OpenID Connect, the architecture ensures interoperability, real-time assurance, and clear auditability. This comprehensive approach supports credential lifecycle management, privacy-preserving consent, and robust audit trails, delivering a solution tailored to the evolving needs of the financial sector.

5.0 Appendices

5.1 Key Terms and Definitions

1. **Auditability and Regulatory Traceability**: Identifies audit-relevant metadata including verification_time, transaction_id, and audit_log_reference to ensure traceability and facilitate financial institution audit requirements in support of the Customer Identification Program (CIP).
2. **Bank Secrecy Act**: Formally known as the Currency and Foreign Transactions Reporting Act of 1970—is a United States law that requires financial institutions to assist government agencies in detecting and preventing money laundering, tax evasion, and other financial crimes.
3. **Claims Packaging and Transmission**: Specifies packaging of identity claims, including the structure, integrity, and transport protocols required to maintain trust and regulatory compliance.
4. **Credential Lifecycle Management**: Outlines metadata supporting credential issuance, maintenance, expiration, and revocation, e.g., document_binding_method and document_revoked.
5. **Customer Identification Program (CIP)**: A regulatory requirement under Section 326 of the USA PATRIOT Act, codified in 31 CFR 1020.220. It mandates that financial institutions must establish procedures to verify the identity of individuals opening accounts, as part of broader Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) compliance framework.
6. **electronic Know Your Customer (KYC)**: It is a digital process used to verify the identity of individuals remotely, replacing traditional paper-based KYC procedures.
7. **KYC Metadata**: KYC metadata provides information about the context, provenance, lifecycle, and verification of identity attributes and credentials.
8. **Federal Financial Institutions Examination Council (FFIEC):** An interagency body established by the United States Congress in 1979. Its mission is to promote consistency and uniformity in the supervision and examination of financial institutions. The FFIEC develops uniform principles, standards, and report forms to ensure effective oversight across federal regulatory agencies
9. **Identity Assurance**: Defines levels of identity proofing, referencing fields such as IAL (Identity Assurance Level) to indicate the strength of identity verification based on NIST SP 800-63-4.
10. **mDL**: mobile Driver's License.
11. **Mobile Security Object (MSO)**: A cryptographically signed container issued by a trusted authority (e.g. a DMV) that encapsulates core identity attributes and

document metadata for a mobile credential. It ensures the integrity and authenticity of the mDL data presented to Relying Parties. The MSO is defined in ISO/IEC 18013-5 as part of the security framework supporting both offline and online verification.

12. **NIST (National** Institute of Science and Technology): Promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.
13. **NIST NCCoE (National Cybersecurity Center of Excellence):** brings together experts from industry, government, and academia to address the real-world needs of securing complex IT systems and protecting critical infrastructure in the United States.
14. **OAuth:** OAuth 2.0 is the industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, and mobile phones.
15. **REAL ID**: Set standards for the issuance of sources of identification, such as driver's licenses and identification cards. The Act and implementing regulations establish minimum security standards for license issuance and production.
16. **Statement of Record (SOR)**: The State Issuer System of Record (SOR) is the authoritative database maintained by the issuing authority—typically the Department of Motor Vehicles (DMV)—that contains validated identity information collected during prior in-person identity proofing events.
17. **Taxpayer Identification Number (TIN)**: A generic term used by the U.S. Internal Revenue Service (IRS) for numbers used to identify individuals and entities for tax purposes. Common types of TINs include:
    - **SSN (Social Security Number)** – for U.S. citizens and permanent residents.
    - **ITIN (Individual Taxpayer Identification Number)** – for certain non-resident aliens and others who cannot get an SSN.
    - **EIN (Employer Identification Number)** – for businesses and some trusts/estates
18. **Verification Provenance**: Refers to the metadata and contextual evidence that documents how, when, and by whom an identity was verified. It establishes a traceable and auditable chain of trust that supports regulatory compliance, risk management, and non-repudiation in digital identity systems.

5.2 Referenced Standards, Guidance and Documentation

19. NIST SP 800-63A: https://csrc.nist.gov/pubs/sp/800/63/A/4/final
20. NIST SP 800-63B: https://csrc.nist.gov/pubs/sp/800/63/B/4/final
21. NIST SP 800-53 r5: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
22. NIST NCCoE Mobile Driver License Project: https://pages.nist.gov/nccoe-mdl-project-static-website/index.html
23. AAMVA Mobile Driver's License (mDL) implementation Guidelines:
    - Data Element Set and Operational Guidance: https://aamva.org/getmedia/261ed16b-3f5c-4678-a2db-cc3016934234/MobileDLImplementationGuidelines-Version1-3.pdf
    - Technical Overview: data model and MSO digest method: https://pomcor.com/documents/Chapter13.pdf
24. CDD rule (beneficial ownership) — 31 CFR 1010.230 https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010/subpart-B/section-1010.230
25. ISO/IEC 18013-5: https://www.iso.org/standard/69084.html
26. ISO/IEC 23220-4: https://www.iso.org/standard/86785.html
27. ISO/IEC 27001: https://www.iso.org/isoiec-27001-information-security.html
28. ISO/IEC 29184:2020: https://www.iso.org/standard/70331.html
29. OAuth 2.0: https://oauth.net/2/
30. OpenID Connect Core: https://openid.net/specs/openid-connect-core-1_0.html
31. OpenID Connect for Identity Assurance: https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html
32. Bank Secrecy ACT: FFIEC BSA/AML:
    - https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/01
    - https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act
33. CIP: https://www.fdic.gov/news/financial-institution-letters/2021/fil21012b.pdf
34. CIP rule (banks) — 31 CFR 1020.220: minimum identity info, risk-based verification, record keeping: https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1020/subpart-B/section-1020.220
35. ETSI TS 119 461 V2.1.1 (2025-02): https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/02.01.01_60/ts_119461v020101p.pdf
36. FFIEC BSA/AML Manual CIP & OFAC exam procedures:
    CIP: https://www.fdic.gov/news/financial-institution-letters/2021/fil21012b.pdf
37. OFAC: https://bsaaml.ffiec.gov/manual/OfficeOfForeignAssetsControl/01
38. GDPR: https://gdpr-info.eu/