Harmonized mDL Metadata for eKYC & CIP: Comparative Analysis and Implementation Guidance

Author: Juliana Cafik
October 29, 2025

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

This paper supplements the "*Proposed mDL Metadata Framework to support KYC & CIP Compliance for the United States*". It synthesizes how core regulatory and technical frameworks—including the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Kantara Privacy Enhancing Mobile Credentials (PEMC), NIST Digital Identity Guidelines (SP 800-63A/B/C), Federal Financial Institutions Examinations Council (FFIEC) / Bank Secrecy Act-Anti-Money Laundering (BSA-AML), ISO/IEC Mobile Driver's License (mDL) Application Standard 18013-5, and Technical Specification Personal Identification- ISOcompliant driving license-Part 7: Mobile driving license add-on functions 18013-7 align with, and inform, a harmonized metadata field set spanning issuers, wallets, and verifiers. The goal is to reduce fragmentation, improve interoperability, and embed privacy-by-design across cross-jurisdictional identity transactions.

Key takeaways:

- A concise, harmonized metadata schema acts as a trust layer across issuer, wallet, and verifier, enabling consistent assurance, consent, and audit signals.

- A REAL ID compliance indicator materially strengthens documentary evidence for CIP.
- Enforcing revocation freshness and explicit error-handling policies is essential to prevent acceptance of stale or unknown status.
- Propagating authentication assurance (acr/amr) and consent context end-to-end supports AAL evaluation, privacy obligations, and auditability.
- Clear role delineation for issuer, wallet, and verifier aligns with ISO/IEC 18013-5/-7, NIST SP 800-63, FFIEC/BSA-AML, and OIDC Core for operational integrity.

1.0 Objective and Audience

This document provides OIDF eKYC/IDA and DCP working groups with a map of alignments, gaps, and design choices across regulatory and technical frameworks, culminating in a pragmatic, implementable metadata schema for standards editors, solution architects, implementers, and compliance leads.

2.0 Scope and Assumptions

The analysis targets mDL-based identity presentations within OpenID Connect (OIDC) and adjacent protocols, focusing on documentary evidence for CIP, privacy obligations under GDPR and CCPA, assurance evaluation per NIST SP 800-63-4, and interoperability with ISO/IEC 18013-5 and -7, as well as FFIEC examiner expectations. It assumes issuer-conformant MSO structures and wallet capabilities to propagate assurance, consent, and revocation evidence.

In addition to these requirements, the analysis incorporates ISO/IEC 29184 guidelines for online privacy notices and consent, ensuring that consent mechanisms are transparent, granular, and revocable. It also references Kantara Consent Receipt and Privacy Enhancing Mobile Credentials (PEMC) frameworks to align wallet-based identity flows with standardized consent and privacy assurance practice.

3.0 Baseline Proposal

This set of principles outlined in the *"Proposed mDL Metadata Framework to support KYC & CIP Compliance for the United States"* document establishes the foundation for a robust, interoperable, and auditable mDL metadata framework tailored for highassurance financial account opening. By standardizing metadata as a trust layer across issuers, wallets, and verifiers, and embedding cryptographically bound compliance indicators, the framework ensures reliable evidence for CIP and KYC. It further enforces revocation freshness and auditability, propagates authentication

assurance and consent signals throughout the credential lifecycle, and aligns roles and responsibilities with leading standards such as ISO/IEC 18013-5/7, NIST SP 800-63-4, FFIEC/BSA-AML, OIDC Core. Collectively, these measures support secure, privacy-preserving, and standards-based digital identity transactions.

4.0 Identity Assurance (NIST SP 800-63A/B/C)

This table provides a high-level comparative overview of how identity assurance requirements, as defined in NIST SP 800-63A/B/C, align to the OIDC/eKYC mDL framework.

Topic	**Baseline (OIDC/eKYC mDL)**	**NIST Alignment**	**Observation(s)**
Identity proofing (IAL)	Issuer provenance + REAL ID flag via MSO; authoritative attributes with issuance/expiry.	Explicit mapping to SP 800-63A IAL2/IAL3; in-person proofing context.	Intent aligns; use normative section anchors in WG text.
Authentication (AAL, acr, amr)	Propagate acr/amr; bind consent to verified identity context.	Map acr→AAL and amr methods to SP 800-63B including lifecycle/session.	No contradictions; adds specificity for policy evaluation.
Federation & assertions	OIDC Core with session_id, audience, consent_id, wallet_signature for traceability.	Map to SP 800-63C assertion integrity and audit requirements.	Strong alignment; standardize claim names and audit semantics.
Revocation & freshness	credential_status, status_check_timestamp, freshness_threshold.	Reinforce lifecycle controls and freshness policy hooks.	Adopt MUST/SHOULD to avoid stale-status acceptance.

5.0 Privacy: GDPR, CCPA, ISO/IEC 29184 & Kantara PEMC

The analysis targets mDL-based identity presentations within OpenID Connect, focusing on documentary evidence for CIP, privacy obligations under GDPR and CCPA, assurance evaluation per NIST SP 800-63-4, and interoperability with ISO/IEC 18013-5 and -7, as well as FFIEC examiner expectations. It assumes issuerconformant MSO structures and wallet and/or FI application capabilities to propagate assurance, consent, and revocation evidence.

In addition to these requirements, the analysis incorporates ISO/IEC 29184 guidelines for online privacy notices and consent, ensuring that consent

mechanisms are transparent, granular, and revocable. It also references Kantara Consent Receipt and Privacy Enhancing Mobile Credentials (PEMC) frameworks to align wallet-based identity flows with standardized consent and privacy assurance practices.

Principle / Right	**Baseline (OIDC/eKYC mDL)**	**GDPR Alignment**	**CCPA Mapping**	**Kantara Alignment**
Lawfulness / Consent / Transparency	Consent tied to acr/amr; audit_log_reference & session_id for traceability	Art. 5, 6, 12–14 supported via acr, amr auditable flows	Right to know; expose session_id, acr, amr	Consent & choice supported via Holder consent
Purpose limitation & minimization	Selective disclosure via claims/scopes; audience scoping	Art. 5(1)(b),(c) via selective claims and scopes	Right to limit sensitive PI via selective disclosure.	Collection limits and minimization reinforced.
Accuracy / Correction	Revocation freshness + authoritative attributes	Art. 16 alignment via credentialStatus / StatusList2021 and updatable attributes such as status_check_timestamp	Right to correct mapped to status and attribute updates.	Accuracy & quality supported by status timestamps.
Accountability & auditability	session_id, verifier roles	Arts. 5(2), 24, 30 mapped to records and logs	Records, logs	Openness & accountability via audience and audit references.

6.0 Comparison Matrix

This "Comparison Matrix" provides a bridge for digital identity requirements to operational and compliance controls to relevant standards, frameworks, and regulatory obligations. It covers baseline practices for OpenID Connect (OIDC) and eKYC mobile driver's license (mDL) implementations, alongside mappings to NIST SP 800-63 (IAL, AAL, Federation), GDPR, CCPA, Kantara, ISO/IEC 18013-5/7, ISO

29184, and FFIEC/CIP. The matrix is designed to help stakeholders understand how each requirement is addressed across different domains, ensuring robust interoperability, privacy, and auditability in digital identity ecosystems. How to Use:

- Reference Requirements: Use the leftmost column to identify key operational, and privacy requirements for digital identity and mDL implementations. • Standards Mapping: Review the corresponding columns to see how each requirement aligns with specific standards and regulations, supporting compliance and best practices.
- Fields and Claims: Consult the "Fields / Claims" column for the concrete data elements or protocol claims that may be required to implement each requirement.
- Implementation Notes: Operational notes to inform design decisions, policy language, and acceptance criteria.
- Citations: Use the "Page/Section Citations" for traceability and to support audits, working group discussions, and conformity assessments.

This matrix is as a first attempt and intended to serve as a practical tool for architects, implementers, and auditors to harmonize requirements, validate coverage, and ensure consistent interpretation across issuer, wallet, and verifier roles.

7.0 Expanded Metadata Field Set (Issuer / Wallet / Verifier)

This harmonized metadata field set defines the core data elements required for interoperability, assurance, and compliance across issuer, wallet, and verifier roles in digital identity and mobile driver's license (mDL) ecosystems. The metadata elements in this table are directly aligned with and expand upon the *"Proposed mDL Metadata Framework to support KYC & CIP Compliance for the United States"* to support regulatory and technical requirements for identity verification, authentication, and auditability. The only exception is the audit log reference element, which is included specifically to address auditability and data subject rights under privacy regulations such as GDPR and CCPA.

The following table presents the expanded metadata field set, detailing data elements that may be required for cross-jurisdictional interoperability, assurance, and compliance across issuer, wallet, and verifier roles in digital identity and mobile driver's license (mDL) ecosystems.

DataElementIDentifier	**Description**	**Entity**	**Required**	**Standards Mapping**

credential_type	Type of credential	Issuer	Yes	ISO 18013-5

	(mDL).			
issuer_id / issuer_name	Issuing authority identifiers	Issuer	Yes	ISO 18013-5; OIDC
issuance_date / expiration_date	Validity window	Issuer	Yes	ISO 18013-5
document_number	Issuer document identifier	Issuer	Yes	ISO 18013-5
core_identity_attributes	Authoritative attributes (name, DOB, address,…)	Issuer	Yes	ISO 18013-5
credentialStatus, StatusList2021	Credential revocation or validity status	Issuer	Yes	ISO 18013-5; NIST SP 800-63B
Trust Framework: e.g. NIST, eIDAS /ARF	Jurisdictional Identifier	Issuer/ Regulatory Body	Yes	
e.g. DHS_compliance	Identity Proofing Regulatory compliance flag (F/N).	Issuer	Yes	REAL ID; AAMVA. NIST 63A profile
status_check_timestamp	Last revocation check time.	Wallet	Yes	ISO 18013-5; NIST SP 800-63B
freshness_threshold	FI Policy for max allowed age of status evidence.	Wallet	Policy	NIST SP 800-63B; FI policy
device_key_info binding_method, acr, amr, proof_ofpossession, device_attestation	Holder Binding	Wallet	Yes	ISO 18013-5/-7

acr	Authentication context (AAL).	Wallet	Yes	OIDC; NIST SP 800-63B
amr	Authentication methods used	Wallet	Yes	OIDC; NIST SP 800-63B
	(AAL).			
consent_id	Verifiable consent record reference.	Wallet	Yes	OIDC; GDPR/CCPA
wallet_signature	Holder/wallet signature over consent/assertion.	Wallet	Yes	OIDC; NIST SP 800-63C
session_id	Correlation of request → presentation.	Verifier/RP	Yes	OIDC; NIST SP 800-63C
audience	Intended relying party identifier.	Verifier/RP	Yes	OIDC; NIST SP 800-63C
audit_log_reference	Pointer to immutable audit record.	Verifier/RP	Yes	GDPR/CCPA

8.0 Operational Gaps, Risks, and Implementation Design Decisions

The following list summarizes key operational gaps, risks, and design decisions identified with harmonization of metadata and implementation requirements for digital identity and mobile driver's license (mDL) solutions. These points highlight areas where further alignment, policy definition, or technical clarification is needed to ensure robust interoperability, regulatory compliance, privacy protection, and consistent user experience across jurisdictions and standards frameworks:

- Trust Framework Identifier and Identity Verification Assurance Flag: assign name, standards& regulatory mappings to derive requirements
- Define normative MUST/SHOULD for revocation freshness and unknown-status handling.
- Harmonize claim names for consent/audit fields across OIDC profiles to avoid divergence.
- Specify device-binding evidence levels (attestation, key strength) with privacy safeguards.

- Create a cross-jurisdictional privacy profile that unifies consent and audit requirements.
- Align language with AAMVA mDL Implementation Guidelines where wallet responsibilities differ.

9.0. Recommendations and Next Steps for the DCP and eKYC& IDA Working Groups

The following recommendations and next steps outline a practical roadmap for advancing the implementation and governance of mDL metadata for the highassurance use case financial account opening with for KYC and CIP compliance requirements. These actions are intended to guide working groups and stakeholders in operationalizing the proposed framework, strengthening interoperability, privacy, and compliance, and ensuring alignment with regulatory and industry best practices:

1. Evaluate and endorse a harmonized metadata set and corresponding values as WG drafts and assign owners (Issuer/Wallet/Verifier).
2. Establish a revocation freshness profile (policy defaults, error handling, RP behavior).
3. Map artifacts to FFIEC examiner expectations for CIP/KYC (evidence templates).
4. Establish Trust Framework Identifiers, standards references and regulatory mappings

Appendix A

1. *AAMVA Mobile Driver's License Implementation Guidelines*
   Operational and technical guidance for mobile driver's license (mDL) implementations, including data elements and interoperability.
2. *CCPA*
   California Consumer Privacy Act: privacy rights and obligations for organizations handling personal data of California residents.
3. *CIP Rule (31 CFR 1020.220)*
   Federal regulation outlining minimum identity information, risk-based verification, and recordkeeping for financial institutions.
4. *FFIEC BSA/AML Manual*
   Manual for financial institutions on Bank Secrecy Act and Anti-Money Laundering compliance, including examiner expectations.
5. *GDPR*
   General Data Protection Regulation: European Union privacy law governing data protection and individual rights.
6. *ISO/IEC 18013-5*
   International standard for mobile driver's license (mDL) data format, security, and presentation.
7. *Kantara Privacy Enhancing Mobile Credentials (PEMC)*
   Kantara Initiative's specification for privacy-enhancing mobile credentials and identity assurance.
8. *NIST NCCoE Mobile Driver License Project*
   National Cybersecurity Center of Excellence project on mDL standards, best practices, and assurance.
9. *NIST SP 800-63A*
   Guidelines for identity proofing and enrollment assurance levels (IAL) in digital identity systems.
10. *NIST SP 800-63B*
    Guidelines for authentication assurance levels (AAL) and technical requirements for authenticators.
11. *NIST SP 800-63C*
    Guidelines for federation and assertion integrity in digital identity ecosystems.
12. *OpenID Connect Core*
    OpenID Foundation specification for federated authentication and identity claims exchange.