IDENTITY & ACCESS FORUM

Powered by SECURE TECHNOLOGY ALLIANCE

Mobile Driver's License (mDL) and mDL Reader Interoperability Testing Guidance

Version 1.5
January 2026

Identity & Access Forum
544 Hillside Road
Redwood City, CA 94062

www.securetechalliance.org

About the Identity and Access Forum

The Identity and Access Forum is a cooperative, cross-industry body dedicated to developing, advancing, and adopting secure identity technologies, including physical and logical access. Through the collaborative efforts of a diverse group of stakeholders, the Forum advocates for market adoption of trusted, user-centric, and interoperable digital identities to ensure safe and seamless access to services across all interactions. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies.

Table of Contents

1. Introduction

With accelerating momentum in the U.S. Mobile Driver's License (mDL) market to promote the issuance, adoption and use of mDLs, the Secure Technology Alliance Identity Access Forum (STA IAF) has established a framework to assess that technologies, which read and verify mDLs ("mDL Readers"), comply with the ISO/IEC 18013-5 and ISO/IEC 18013-7 mDL standards. Interoperability testing against mDL standards and related implementation guidelines will ensure that mDL Readers and mDLs will successfully interoperate across a wide range of use cases.

The STA IAF publishes and maintains current and comprehensive guidance for mDL ecosystem stakeholders on mDLConnection.com and Identity and Access Forum - Secure Technology Alliance. STA IAF Interoperability Test events will be promoted, and subsequent test-event results will be published on these STA IAF websites.

1.1 References

This document draws from the mDL ISO Standards, similar national and international ISO-compliant mDL/mdoc Interoperability Test events, and US mDL-Issuing Authority sources:

1. **ISO Standards**
   - ISO/IEC 18013-5:2021 – "Mobile driving licence (mDL) application"
   - ISO/IEC 18013-7:2025 – "Mobile driving licence (mDL) add-on functions"
   - ISO/IEC TS 18013-6:2025 – "mDL test methods"
2. **mDL Implementation Guidelines**
   - AAMVA mDL Implementation Guidelines
3. **mDL State Issuer IACA Public Keys/Certificates**
   - Mobile Driver License Digital Trust Service - American Association of Motor Vehicle Administrators - AAMVA
   - Secure Technology Alliance, U.S. Payments Forum & Identity & Access Forum - IACA Public Keys
4. **National and International mDL/mdoc Interoperability Testing**
   - New Zealand Interoperability Test Event
   - Austroads IVC24 Interop Test Event
   - Tests Confirm Austroads' Digital Trust Service Now Positioned for Scalable Nationwide Expansion - Tech Business News
   - ISO/IEC 18013-7 Interoperability Event Results (SpruceID)

2. Overview

This document provides an mDL Interoperability Testing framework targeted to objectively and qualitatively assess mDL Reader solutions and their ISO-compliant engagement and

interoperability with US State-Issued mDLs – in accordance with the ISO/IEC 18013-5:2021[1] (for in-person mDL transactions) and ISO/IEC 18013-7:2025 (for remote mDL transactions) standards, and their specific Optional/Conditional/Mandatory requirements for mDL-to-Reader device engagement and data retrieval scenarios.

The following subsections touch on related contextual topics (e.g., Participants, Goals and Benefits, and Confidentiality).

Section 3 describes how Interoperability Testing will be set up and conducted at each Interoperability Test event.

Section 4 provides the baseline ISO 18013-5 and ISO 18013-7 Interoperability Testing checklists that will be used during test events to evaluate mDL Reader solutions.

> *NOTE: This document is intended to be adaptive and reusable for multiple US mDL Interoperability Test events that the STA IAF may conduct, and is not specific to any one event. The STA IAF will update this document following relevant feedback from each Interoperability Test event, and will also welcome any supportive changes and recommendations from reviewers.*

2.1 Test Event Participants and Roles

mDL Interoperability Testing relies on the direct, peripheral, and/or conditional engagement of supporting participants and test-execution roles, as follows:

1. **mDL Reader Solution Technology Providers**
   Those Organizations that have solutions that support reading and verifying one or more State-issued mDLs, and/or Test mDLs. These Tech Providers may demonstrate their solutions in conjunction with State mDL Issuer and Relying Party "partners".
2. **Relying Parties**
   Those public and private sector entities (e.g., retailers, merchants, banks, government agencies, and healthcare providers) that have integrated, or will be integrating, mDL reader solutions to support their specific use cases, and wish to have their integrated mDL Reader solutions assessed within Interoperability Test events.

2.2 mDL Interoperability Test Team

For each Interoperability test event, a "Test Team" will be formed to formally manage and execute the test scenarios outlined in this document. The Test Team will be comprised of the following roles:

1. **Test-Team Coordinator**
   The "Coordinator" manages the Test Team, and coordinates the tests with each mDL Reader Solution Provider.

[1] At present, US mDL implementations and relying-party mDL readers have been focused on the 2021 1st edition of ISO 18013-5. As such, this document does not address any new features or modifications in draft versions of ISO 18013-5 2nd edition that are currently in the standards development pipeline.

2. **Test Recorder**
   The Test Recorder records the test scenarios executed during individual mDL Reader testing slots, along with the test results, in the Interoperability Test Checklists (in Section 4).
3. **Test mDL Holders**
   The Test Team will be provisioned with Test mDLs, and will present them to mDL Readers during testing.
4. **State-Issued mDL Holders**
   Test Team members may present their State-Issued mDLs to mDL Readers during testing. The Test Team may also be accompanied by a set of volunteers who may participate in mDL Reader testing, and present their State-Issued mDLs. The goal is to have as many representative State-Issued mDLs as possible, without duplication.

NOTE: Depending on the number of mDL Reader Solution Providers participating in any given Interoperability Test event and the test timeframe allocated for a given event:

- A single individual may hold more than one Test Team role, or all Test Team roles
- Multiple Test Teams may be required

2.3 Interoperability Testing Goals and Benefits

The key goal for mDL Interoperability Testing is to promote the adoption and use of mDLs, and to provide a tangible assessment of how available mDLs and mDL reader verification solutions comply with the ISO/IEC 18013-5 and ISO/IEC 18013-7 standards, and how those solutions support the identified and intended mDL use cases. An assessed baseline of mDL verification solutions will benefit mDL ecosystem stakeholders as follows:

1. **mDL Issuer Benefits**
   AAMVA and US State DMVs can leverage and exploit their investments in the development of mDL apps and the issuance of mDLs to valid driver's license holders within their jurisdictions by assessing mDL Reader solution offerings that have been evaluated during Interoperability Test events.
2. **mDL Reader Solution Technology Provider Benefits**
   While mDL Reader Solution Technology Providers may have tested their mDL reader solutions independently with various State-Issued mDLs, testing within the STA IAF's Interoperability Test event framework will provide independent and objective confirmation that their solutions comply with the standards within the scope of the mDLs used during test events. In addition, any subsequent publishing of the test results (with the Technology Provider's organizational approval) may benefit in promoting their compliant solutions to interested Relying Parties and other mDL ecosystem stakeholders.
3. **Relying Party Benefits**
   Similar to mDL Reader Solution Tech Provider benefits, Relying Parties implementing mDL readers within their specific use cases will benefit from their integrated solutions

being assessed as compliant with the ISO standards, and can leverage the visibility and results of interoperability testing to further promote their offerings.

2.4 Types of mDL Interoperability Test Events

The level and detail of Interoperability Testing for specific test events may vary, depending on the number of participants, the amount of time allocated for testing, and the test event venue.

1. **Informal Interoperability Testing**
   Informal Interoperability Testing is targeted for assessing the test scenarios and test execution procedures addressed in this document. It may entail a small group of participants who volunteer to have their mDL reader solutions evaluated by STA IAF Interoperability Test Team.
2. **Comprehensive Interoperability Testing**
   Thorough Interoperability Testing entails a thorough execution of the test procedures presented in this document, along with publishing the subsequent test results on an online forum approved by the STA IAF.
3. **Certification (Out of Scope)**
   While mDL interoperability certification is not offered through this STA IAF Interoperability Testing initiative currently, mDL Reader certification is available from external international organizations who perform comprehensive testing of mDL Readers to ensure conformance with the ISO 18013-5 and 18013-7 standards, and the "mDL test methods" defined ISO 18013-6. However, STA-IAF mDL Interoperability Testing offers a leverageable benefit to those mDL Reader Solution Providers seeking such certification, as this STA IAF Interoperability Testing focus is targeted to assess that the mDL Readers tested implement all device engagement and data retrieval mechanisms specified in the standards.

2.5 Targeted mDL Readers

Interoperability Testing is intended to target and assess the various form factors and capabilities of mDL Readers for both in-person (ISO 18013-5) and remote (ISO 18013-7) mDL use cases, and how the participating mDL Readers perform when reading and verifying mDL data from presented State-Issued mDLs and Test mDLs used during Interoperability Test events.

The following figure depicts the various offline and online mDL Reader form factors that may be encountered and evaluated during Interoperability Testing:

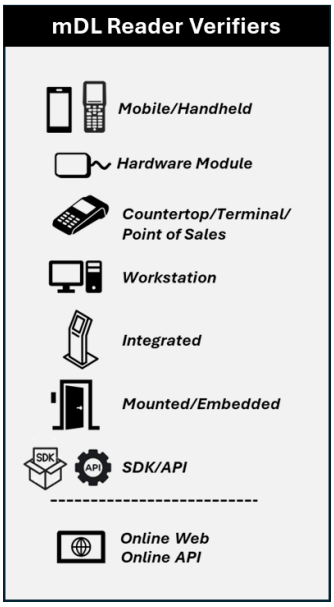

Figure 1 – mDL Reader Form Factors

Further details on mDL Reader form factors and capabilities are provided in Appendix A -

2.6 Test Results Confidentiality and Anonymity Considerations

Test checklists, test metrics, and overall evaluation of each mDL Reader's performance during testing shall remain confidential and anonymous, until which time the STA IAF decides when and how individual and statistical testing results are to be published. All mDL Reader Solution Provider organizational and product identifiers shall remain confidential and will only be released with the mDL Reader Solution Provider's organizational approval.

The venues (e.g., websites, webinars and/or briefings) for the disclosure of subsequent post-test results and assessments are out of scope of this document.

2.7 Privacy Requirements

As "real" State-Issued mDLs may be used during Interoperability Test events for engagement with mDL Readers, mDL Readers should be configured to retrieve the minimum of mDL data elements (e.g., mDL Holder Portrait and Age Verification data) needed to support specific test scenarios and demonstrated use cases.

State-Issued mDL Holders may or may not consent to the retrieval of any Personally Identifiable Information (PII) from their mDL during testing.

mDL Reader Solution Providers SHALL NOT persist, save or export any PII retrieved during Interoperability Testing. All mDL Holder PII that may be retrieved MUST be purged from mDL Readers and any associated datastores immediately following the test event.

For those mDL Holders voluntarily participating in test events, only the mDL Issuing State will be recorded in resulting test artifacts (e.g., Test Checklists), and not their names or any other PII.

3. Interoperability Test Execution

The following subsections describe the mDL Reader and mDL interoperability testing prerequisites, objectives and processes.

3.1 Interoperability Testing Support Kit

The Interoperability Testing Test Team will be supported by, and provisioned, with the following baseline tools, items and artifacts during Interoperability Testing execution:

1. **State-Issued mDLs**
   a. To the extent possible, a collection of US State-issued mDLs will be used during Interoperability Testing, as these mDLs are key to the overall mDL ecosystem -- inclusive of, and independent of -- Interoperability Testing. It is paramount that these real-life mDL's be a part of mDL Reader testing.
   b. The Interoperability Testing Test Team will utilize their own State-Issued mDLs, along with other State-Issued mDL holders who agree to accompany and support the Test Team with their State-Issued mDLs during Interoperability Test events.
   c. At a minimum, the State-Issued mDLs used for testing will include Android Wallet and iOS Wallet mDLs, and custom/commercial mDL mobile applications not based on mobile platform OS wallets.
   d. Note, per ISO 18013-5:2021, mDL methods of interaction with mDL Readers for Device Engagement (i.e., NFC and/or QR Code) and Data Retrieval (i.e., NFC, BLE, and Wi-Fi Aware) are either Optional or Conditional. That is, any given State-Issued mDL application/wallet may, or may not, necessarily implement all the methods for mDL reading and authentication that the Standard specifies.

2. **Test mDLs**
   a. Interoperability Testing will leverage available mobile phone "Test mDLs" issued by those organizations/stakeholders who have Test mDL implementations, and who will voluntarily offer such test mDLs for Interoperability Test events.
   b. Test mDLs used for Interoperability Testing will -- either independently or collectively -- support all methods for offline and online mDL device engagement and data retrieval as specified in ISO 18013-5:2021 and ISO 18013-7:2025.

3. **mDL Issuer Data Authentication Public Keys/Certificates**
   a. Interoperability Testing will assess and verify that tested mDL Readers are authenticating the mDL-Issuer signed Mobile Security Object (MSO), i.e. "Issuer Data Authentication"
   b. mDL Reader Solution Providers must have processes for incorporating current US State-Issued mDL public keys/certificates (provided online by the AAMVA DTS VICAL, and by individual State mDL IACA download sites) into their mDL Readers to authenticate State-Issued mDLs used during Interoperability Testing.

c. How mDL Readers install and configure AAMVA DTS VICAL and State IACA root certificates as a trust point for mDL Issuer data authentication may be proprietary and is outside the scope of this document.
d. For Test mDLs used during Interoperability Testing, the STA IAF will provide mDL Reader Solution Providers with Test mDL-Issuer public keys/certificates prior to the test event, in order for these public keys/certificates to be pre-installed/configured in the mDL Readers to be tested.
e. NOTE: To support the assessment that mDL Readers are authenticating mDLs, Test Team will also present Test mDLs with Issuer public keys/certificates that ARE NOT provided prior to the test event.

4. **Interoperability Testing Checklists**
   The resulting output for each Interoperability Test event will be the documented execution of the checklists presented and described in Section 4, along with an overall summary assessment of the test results.

3.2 Test Objectives and Test Procedures

3.2.1 Test Objectives

The test objectives for both offline and online mDL data retrieval and verification are to evaluate mDL Reader ISO-conformance when presented with the State-Issued and Test mDLs by the Test Team. As indicated by the checklists in Section 4, mDL Readers will be assessed on:

- Functional interoperability with State-Issued and Test mDLs
- Employing mDL-Issuer public keys/certificates to authenticate mDLs and retrieved mDL data elements
- mDL engagement methods (QR Code and NFC)
- Data retrieval protocol compatibility (NFC, BLE, WiFi Aware, OID4VP, REST API, DC API)
- Selective mDL data element retrieval (e.g., license and holder data, portrait and age verification) requests by mDL Readers with the consent of mDL Holders

3.2.2 Test Procedures

Interoperability Testing will be divided into specific testing time slots for each mDL Reader Solution Provider for the designated test scenarios. Prior to a test event, mDL Reader Solution Providers will be provided with a current version of this mDL Interoperability Test Plan, Test mDL public keys/certificates, and any other artifacts deemed necessary to perform the testing.

The Test Team will move between mDL Reader test stations, or Tech Provider tables, equipped with State-Issued and Test mDLs and present them to mDL Readers – following the individual test indicated in the checklists related to the mDL Reader form factors for either offline ISO/IEC 18013-5 engagement or online ISO/IEC 18013-7 engagement, or both.

In each testing slot:

1. The Test Team presents the relevant test scenario(s) and checklists.
2. The mDL Reader Solution Provider sets ups/configures the mDL Reader for the specific test scenario.
3. The Test Team presents mDLs to the mDL Reader, i.e.:
    a. State-Issued mDLs that implement the device engagement and device/data retrieval modes that the mDL Reader accommodates.
    b. Test mDLs with test mDL Issuer public keys/certificates provisioned prior to the test event.
    c. Test mDLs with test mDL Issuer public keys/certificates NOT provisioned to mDL Reader Solution Providers prior to the test event.
4. mDL Reader Solution Provider executes the test scenario for the mDL Reader.
5. The Test Team observes the stepwise test results, and records them in the test scenario checklist specific to the mDL Reader for the test scenario, noting pass/fail results, error handling, and adding any relevant comments.
6. The Test Team aggregates the test results.

3.3 Testing Metrics and Evaluation

The resulting test checklists (per Section 4) will be used to evaluate individual mDL Reader test performance, based on the following metrics:

1. Pass/fail results per each test scenario
2. Error handling, comments and failure points analysis
3. mDL Data Element validation (e.g., photo, age verification
4. Signature verification
5. Data element correctness
6. Overall subjective usability feedback

3.4 Test Result Distribution and Review Process

Following interoperability testing, mDL Reader Solution Providers will be provided with the resulting checklist(s) for each mDL Reader tested, along with a summary assessment.

All test results will be held confidentially by the Test Team and a select group supporting the Interoperability Test event, in accordance with Section 2.6 – “Test Results Confidentiality and Anonymity Considerations”.

mDL Reader Solution Providers will have an opportunity to review and dispute any test scenario result(s), if need be, – and will be given an opportunity to discuss the test results with the Test Team to resolve any disputes or discrepancies.

The venues (e.g., websites, webinars and/or briefings) and format(s) for the disclosure of subsequent post-test results and assessments are out of scope of this document.

4. Interoperability Test Checklists

This section provides the mDL Interoperability Testing checklists for mDL Reader features and capabilities to be tested for both ISO/IEC 18013-5:2021 and ISO/IEC 18013-7:2025 test scenarios.

For each checklist and its utilization during Interoperability events, the Test Team will observe and record the mDL Reader testing results in the checklist. Checklists are organized as follows:

1. **Test Point Information**
    a. **Test Team** – The Test Team will record their name and organizational affiliation, along with any other testers and/or test observers active in any given mDL Reader test scenario.
    b. **Test Location –** The name of the Interoperability Test event or venue where interoperability testing took place.
    c. **Start and End Data/Time** – The start and end date and time of the specific test scenario.
2. **Device Engagement**
    a. **ISO 18013-5 –** For Device Engagement, either QR Code-only, NFC-only, or both may be tested within the same checklist. QR Code and NFC are to be asserted by the mDL application.
    b. **ISO 18013-7 –** For Device Engagement, QR Code is the only mode, where the mDL application scans a QR Code asserted by the online mDL Reader solution.
3. **Data Retrieval**
    a. **ISO 18013-5 –** To the extent possible, the Test Team determines and notes which Data Retrieval mode(s) (e.g., BLE, NFC and Wi-Fi Aware) the mDL supports, and whether the mDL Reader successfully implements the Data Retrieval modes accommodated by the mDL.
    b. **ISO 18013-7 -** To the extent possible, the Test Team determines and notes which Data Retrieval mode(s) (e.g., REST API, OID4VP and DC API) the mDL supports, and whether the mDL Reader successfully implements the Data Retrieval modes accommodated by the mDL.
4. **Security**
    To the extent possible, the Test Team determines and notes whether the following Security Mechanisms are successfully implemented and demonstrated:
    a. Issuer Data Authentication
    b. mdoc Authentication
    c. Session Encryption
    d. mdoc Reader Authentication (Optional)
5. **Selective Data Retrieval Verification**
    Depending on the mDL Reader and the tested Use Case(s), the Test Team notes (if any) which mDL data elements were retrieved from the mDL, in the context of mDL Use Consent.

6. **General Checklist Items**
    a. **Checkmarks –** The checklists include “checkmarks” for the Test Team to indicate which test scenario item(s) were executed during Interoperability Testing for a specific mDL Reader.
    b. **Test Result Dropdown List –** The Test Team shall indicate the result (Successful/Unsuccessful), where applicable, for each test scenario item executed.
    c. **Comments –** The Test Team may enter explanatory comments related to test scenario instances executed, such as - why a test was unsuccessful, extraneous circumstances which hampered the test, or why the outcome of a test was undetermined.

4.1.1 ISO/IEC 18013-5 mDL Reader Interoperability Test Checklist (In-Person/Proximity Presentation Transactions)

Table 1 – ISO/IEC 18013-5 mDL Reader Interoperability Test Checklist for In-Person mDL Data Retrieval & Verification

ISO/IEC 18013-5 mDL Reader Interoperability Test Checklist for In-Person mDL Data Retrieval & Verification			
Test Point Information			
Test Team Name(s)	**Test Location**	**Start Date/Time**	**End Date/Time**
mDL Reader Organization			
Organization Name	**Product Name**	**mDL Reader Type**	**Use Case(s) Tested**
		Select Reader Type	
mDLs Used for Testing (State Issued mDLs, Test mDLs, etc.)			
General Comments			
Device Engagement			
Engagement Mode	**Test Result**	**Comments**	
☐ QR Code	Select Result		
☐ NFC Static Handover	Select Result		
☐ NFC Negotiated Handover	Select Result		
Data Retrieval			
Transmission Technology	**Test Result**	**Comments**	
☐ NFC	Select Result		
☐ BLE Central	Select Result		
☐ BLE Peripheral	Select Result		
☐ BLE L2CAP	Select Result		
☐ WiFi-Aware	Select Result		
Security			
Security Mechanism	**Test Result**	**Comments**	
☐ Issuer Data Authentication	Select Result		
☐ mdoc Authentication	Select Result		
☐ Session Encryption	Select Result		

☐ Reader Authentication (Optional)	Select Result	
Selective Data Disclosure Verification		
Data	**Test Result**	**Comments**
☐ License and Holder Data	Select Result	
☐ Portrait	Select Result	
☐ Age Verification	Select Result	
☐ Other Data	Select Result	

4.1.2 ISO/IEC 18013-7 mDL Reader Interoperability Test Checklist (Remote/Remote Presentation Transactions)

Table 2 - ISO/IEC 18013-7 mDL Reader Interoperability Test Checklist for Online mDL Data Retrieval & Verification

ISO/IEC 18013-7 mDL Reader Interoperability Test Checklist for Online mDL Data Retrieval & Verification			
Test Point Information			
Test Team Name(s)	**Test Location**	**Start Date/Time**	**End Date/Time**
mDL Reader Organization			
Organization Name	**Product Name**	**mDL Reader Type**	**Use Case(s) Tested**
		Select Reader Type	
mDLs Used for Testing (State Issued mDLs, Test mDLs, etc.)			
General Comments			
Device Engagement			
Engagement Mode	**Test Result**	**Comments**	
☐ QR Code	Select Result		
Data Retrieval			
Transmission Technology	**Test Result**	**Comments**	
☐ REST API (Annex A)	Select Result		
☐ OID4VP (Annex B)	Select Result		
☐ DC API (Annex C)	Select Result		
Security			
Security Mechanism	**Test Result**	**Comments**	
☐ Issuer Data Authentication	Select Result		
☐ mdoc Authentication	Select Result		
☐ Session Encryption	Select Result		
☐ mdoc Reader Authentication	Select Result		
Selective Data Disclosure Verification			
Data	**Test Result**	**Comments**	

☐ License and Holder Data	Select Result	
☐ Portrait	Select Result	
☐ Age Verification	Select Result	
☐ Other Data	Select Result	

Appendix A - mDL Reader Classifications

mDL Interoperability Testing is based on the classification and manifestation of mDL Reader solution offerings supporting ISO 18013-5 and ISO 18013-7 for in-person and online mDL verification. The following table represents a questionnaire for surveying and categorizing the different types of mDL Reader solution offerings that may be encountered during Interoperability Test events. This questionnaire is being used by the STA IAF to compile a list mDL readers and their capabilities, which various mDL Reader Solution Providers have voluntarily shared on the STA IAF's website (mdlconnection.com) at [mDL Reader Solutions - mDL Connection].

Table 3 – mDL Reader Capability Survey Questionnaire

1. Company Overview **Company Name:** (company name) **Website:** (company website) **Any Additional Details:** (additional details) **Contact:** • **Name:** (contact name) • **Email:** (contact email) **2. Supported Form Factors** What is the form factor of your mDL reader/verifier product? (you may select more than one answer)? • Mobile Device • Handheld Device • Countertop / Terminal • Workstation • Integrated (e.g., in kiosk or other multifunction formfactor) • Mounted (e.g., in proximity to physical access entry point) • SDK • API • Online Service **3. Supported Use Cases** Which of the following Relying-Party Use Cases does your product support? (you may select more than one answer)? • Age Verification • Transportation Security Administration (TSA) or other Travel • Identity Proofing for Onboarding & Registration • Banking and Financial Services • Access to Secure Area (e.g., Federal Building/Room) • Other: _____	**4. Supported Operating Systems** Which platforms does your mDL reader/verifier product support (you may select more than one answer)? • iOS • Android • Windows • macOS • Linux • Apple watchOS • Android wearOS **5. In-Person Device Engagement** Which of the following initial Device Engagement methods (per ISO 18013-5) does your product support for In Person presentation (you may select more than one answer)? • QR Code • NFC **6. In-Person Data Retrieval** Which of the following Data Retrieval technologies (i.e., Connection Handover following Device Engagement per ISO 18013-5) does your product support for in-person presentation (you may select more than one answer)? • NFC • Bluetooth Low Energy (BLE) • Wi-Fi Aware	**7. Remote Data Retrieval** With the recent publication of ISO 18013-7 standard and its focus on online mDL verification, if your organization has a solution/product or is planning on such, which of the following Data Retrieval methods does it support? • OID4VP • REST API • DC API **8. Standards Compliance** Has your mDL reader product solution been tested and verified for ISO 18013-5 and ISO 18013-7 compliance by an independent organization – Yes/No? *If Yes - please provide the name of the organization who accredited/certified your solution:* _____ **9. Additional Information** Provide any accompanying additional information that you would like to share. _____

Appendix B - Legal Notice

The Identity & Access Forum endeavors to ensure, but cannot guarantee, that the information described in this document is accurate as of the publication date. This document is intended solely for the convenience of its readers, does not constitute legal advice, and should not be relied on for any purpose, whether legal, statutory, regulatory, contractual, or otherwise. All warranties of any kind are disclaimed, including but not limited to implied warranties of merchantability or fitness for a particular purpose, and warranties of title, noninfringement or regarding the accuracy, completeness, or adequacy of information herein.