

Event Results Summary

ISO/IEC 18013-7 Interoperability Event

August 2023

Author:	SpruceID
Date:	October 25, 2023
Status:	Published
Classification:	Public

1. Executive Summary

The August 2023 ISO/IEC 18013-7 Interoperability Event, organized by SpruceID, aimed to test the draft technical specification ISO/IEC 18013-7, focusing on unattended or fully online use cases of Mobile Driver's Licenses (mDL) such as presentation of an mDL over-the-internet to a relying party website. This event marked a significant shift as the first fully remote testing initiative of its kind with participants taking part from their own offices.

Participants from various organizations engaged in testing both Rest API and OpenID4VP protocol implementations. The event's objective was to evaluate the draft specification's global interoperability and ability to be implemented as written. In addition, the committee gathered insights and recommendations for refinement of the technical specification.

Notably, the draft specifications were found to have no major issues requiring normative changes. Interoperability challenges mainly stemmed from variances in which draft specification document a participating implementation chose to implement and the absence of non-critical features in specific implementations. These issues were largely due to updates to the draft documents in advance of the interoperability event that some participants did not have adequate time or resources to address. However, these challenges were successfully addressed, demonstrating the commitment to fostering interoperability.

Feedback from the event, along with preliminary test results and troubleshooting, was presented to ISO/IEC JTC1/SC17 WG10 in Singapore. The findings and resolutions have been documented as N2349 in the ISO Global Directory. These insights have been incorporated into the latest version of ISO/IEC 18013-7, represented by N2356, which is the DTS draft 1 of the specification, enriched to enhance interoperability. The event's success reflects the collective effort to advance standards for mDLs.

2. Introduction

Driver's licenses serve more use cases than just proving one's capability to operate a vehicle—many people globally use their driver's license as their primary form of identification. As society shifts to a digital-first world, people need digital identification credentials to represent various facets of their identity online in a secure way. However, creating a digitally capable credential is not as simple as taking a picture of the plastic credential card. Digital credentials need to be verifiable, tamper-evident, and provably authentic, while simultaneously being usable across various industries and sectors and presentable both online and in-person.

This means that it is critical to build Mobile Driver's License (mDL) solutions using standardized data formats and protocols, so Verifiers across different geographies and industries are able to confirm a person's identity.

ISO/IEC JTC 1/SC 17 works on standards for motor vehicle driver licenses and related documents, with the aim of providing a common technical framework and promoting the safe and secure use of this technology. The ISO/IEC 18013-5 standard specified by ISO/IEC JTC 1/SC 17 defines requirements for the security, data elements, and information exchange of mobile driving licenses (mDL) between the mobile device and authorized parties, while supporting user data protection and protecting driver privacy. ISO/IEC 18013-5 focuses on attended in-person use cases where parties are in close proximity during presentation time. ISO/IEC JTC 1/SC17 published a Committee Draft consultation of ISO/IEC 18013-7, a draft technical specification that focuses on unattended or fully online use cases of mDL where parties are remotely connected at the time of presentation.

Previous interoperability events enabled mDL Verifiers and Issuers to test the interoperability of their respective solutions, most recently in December of 2022 in Brisbane, Australia testing implementations of ISO/IEC 18013-5 and ISO/IEC 18013-7 presentation and verification where participants were in the same room to test their implementations in-person.

This event focused on testing only ISO/IEC 18013-7, and therefore was conducted asynchronously as the first fully remote event of its kind.

2.1 Scope

This document summarizes the results from the ISO/IEC 18013-7 Interoperability Event, hosted in August of 2023. As ISO/IEC 18013-7 focuses primarily on unattended or fully online use cases of mDL, the event was hosted remotely with asynchronous testing over a period of three weeks. This report was prepared by SpruceID, the host of the event.

The goal of this publication is to share insights on:

- statistics related to event participation to inform understanding of industry maturity,
- aggregate outcomes for the testing that took place,
- detailed insights related to specific technology protocols used,
- trends observed related to the technology and adoption,
- and recommendations for clarifications for the draft standard based on testing.

2.2 Intended audience

This document is publicly available for any individual or organization that is interested in understanding the maturity of ISO/IEC 18013-7, which is in draft form at the time of the event and at the time of this writing.

3. Event Logistics and Details

3.1 Organization

The event was hosted remotely, with an asynchronous testing window that opened on August 21, 2023, and remained open until September 8, 2023. The SpruceID team hosted the event and coordinated the asynchronous testing with participation by members of ISO/IEC JTC 1/SC17/WG10 and other industry members. The event was supported by AAMVA and Austroads, which are non-profit associations representing state, provincial, and territorial officials in North America and Australia, respectively, who develop model programs and best practices for motor vehicle administration, police traffic services, and highway safety.

Please be aware that participation in this event or successful test demonstrations does not translate to an endorsement by ISO, IEC, Austroads, AAMVA, or SpruceID.

3.2 Goals

The objective of the event was to provide a collaboration forum for implementers of ISO/IEC 18013-7 to test their respective solutions in an effort to drive forward cross-industry interoperability and adoption while accelerating feedback and clarity for implementations of the standards.

In July 2023, WG10 convened to discuss feedback on the recent updates to the draft specification. Based on the outcomes of those meetings, updates were made to Annex A, Annex B, and the main document in the draft of ISO/IEC 18013-7. The testing guidelines were updated to reflect these changes, in order to allow implementers of 18013-7 to demonstrate interoperability while also providing feedback on the clarity and completeness of new drafts of the standard. Collecting feedback on these draft versions to inform the final version of ISO/IEC 18013-7 was an important objective of this testing event.

The three-week testing window allowed for participants to actively test and iteratively make adjustments to their implementations to optimize test results.

3.3 Participation

Any organization (or group, or individual) who 1) registered through the registration form before the registration window closed and 2) provided the required verifier link (if applicable) and/or X.509 certificates for issuer and/or reader authentication was eligible to participate in the Interoperability Event. This event was not restricted to any particular working group membership or organization size.

The test event was facilitated remotely, which allowed organizations of all sizes and based globally to participate without any required travel. There was an open registration window for any interested parties that spanned one month from July 7, 2023, through August 7, 2023. The open invitation to participate was circulated through relevant standards working groups and on professional networking sites, including LinkedIn.

3.4 Test process

The event took place online asynchronously, allowing for participants to test interoperability throughout a fixed three-week period to encourage maximum participation and allow for active development iterations to optimize test results over the three-week window. Participants who brought their verifier and/or mDL app implementations were encouraged to test both OpenID4VP and RestAPI implementations which are the two available protocol options to implement ISO/IEC 18013-7.

At the commencement of the testing period, each respective mDL implementer and mDL reader implementer received a packet of testing instructions, with a testing results spreadsheet.

mDL Reader Implementers were required to:

- Provide the public HTTPS URL for their verifier web application
- (Optional) Provide the X.509 certificate for reader authentication
- Support each of the test scenarios outlined in Section 3.4.1
- Implement the web application requirements outlined in the Testing Guidelines
- Perform the required data and security checks outlined in Section 3.4.2
- Produce, retain, and submit log outputs for all testing

mDL App Implementers were required to:

- Provide their public IACA root x.509 certificate (as per 18013-5) to enable issuer authentication
- Support the test scenarios outlined in Section 3.4.1
- Perform the required data and security checks outlined in Section 3.4.2
- Complete their unique test results spreadsheet provided directly to each participant
- Submit log output files at the end of the testing window

AAMVA provided the Verifier Issuer Certificate Authority List (VICAL) via their Digital Trust Service (DTS) test environment to support dissemination of the IACA root certificates.

3.4.1 Test Scenarios

The following test scenarios were defined for this event:

Table 1: Scenario Identifiers for results tracking

Scenario ID	Scenario Description
SCE_REST_1	Verifier requests for all mandatory license and holder data (including the portrait of mDL holder) using “RestApi”.
SCE_4VP_1	Same as SCE_REST_1 but instead using “OpenID4VP”.
SCE_REST_2	Verifier requests for age verification (over 18), no portrait of mDL holder. Note: This scenario might have limited real-world use since the verifier does not receive an indication of the confidence it can place in the binding between the information received and the person sharing the information.
SCE_4VP_2	Same as SCE_REST_2 but instead using “OpenID4VP”.

3.4.2 Data and Security Checks

For each test scenario from the table in **3.4.1 Test Scenarios**, verifiers were expected to perform, log and display the following data and security checks:

Table 2: Verifier Log Identifiers for statistical gathering

Check ID	Check Description	Reference	Required/Optional
V_DATA_1	Provide “RestApi” or “OpenID4VP” request. When the verifier provided the actual encrypted “RestApi” or “OpenIDVP” request to the mDL app.	ISO/IEC 18013-7 Annex A and Annex B	REQUIRED.
V_DATA_2	Receive “RestApi” or “OpenID4VP” response.	ISO/IEC 18013-7 Annex A and Annex B	REQUIRED.
V_DATA_3	Receive expected data set. After the verifier decrypted the response, the verifier needs to check if the	ISO/IEC 18013-7 Annex A and Annex B, ISO/IEC 18013-5	REQUIRED.

	response includes all requested namespaces and data elements in the correct format, and no extraneous namespaces or elements.		
V_SEC_1	Decrypt response.	ISO/IEC 18013-7, Clause A.7 for “RestApi”, Clause B.4.3.2.2 for “OpenID4VP”	REQUIRED.
V_SEC_2	Perform issuer data authentication. Verifies the signature of the MSO based on the distributed X.509 IACA certificate.	ISO/IEC 18013-5	REQUIRED.
V_SEC_3	Verify mdoc authentication.	ISO/IEC 18013-5	REQUIRED.

For each test scenario from the table in **3.4.1 Test Scenarios**, mDL implementers were expected to perform, log and record the following data and security checks:

Table 3: mdoc application identifiers for statistical log gathering

Check ID	Check Description	Reference	Required/Optional
M_DATA_1	Receive “RestApi” or “OpenID4VP” request.	ISO/IEC 18013-7 Annex A and Annex B	REQUIRED.
M_DATA_2	Decode expected request. Check whether the request was a valid test scenario. This could be done by displaying the requested data elements to the end-user.	ISO/IEC 18013-7 Annex A and Annex B	REQUIRED.
M_DATA_3	Provide “RestApi” or “OpenID4VP” response.	ISO/IEC 18013-7 Annex A and Annex B, ISO/IEC 18013-5	REQUIRED.
M_SEC_1	Reader authentication.		

	“RestApi”	ISO/IEC 18013-5 Clause 9.1.3	OPTIONAL.
	“OpenID4VP”	ISO/IEC 18013-7 Clause B.4.2.3.3 using the Client Identifier scheme x509_san_uri	

3.5 Participants and Implementations

3.5.1 Overview

There were 41 unique registrations for the Interoperability Event, including organizations intending to actively test in the event and those interested in observing the event to understand the maturity and adoption of the standard. Of the 41 unique registrations, 16 organizations provided mDL reader applications for testing, and 13 organizations provided mDL implementations.

The participating mDL reader implementers included: Bundesdruckerei GmbH, Credence ID, Google, HID Global, ImproveID, MyNextID, the National Institute of Standards and Technology (NIST), Okta, OneProof, Panasonic, Ping Identity, Samsung, Scytales, SpruceID, and Thales.

The participating mDL implementers included: Bundesdruckerei GmbH, Google, HID Global, ImproveID, MyNextID, NEC, OneProof, Panasonic, Samsung, Scytales, SpruceID (jointly with the State of California Department of Motor Vehicles), and Thales.

Participants in the event were encouraged to test both Rest API and OpenID4VP implementations. The distribution of implementations across roles, protocols, and platforms is given in *Table 1*. For each participant, an implementation is recognized individually per role, platform, and protocol.

For example: If a company brings a Rest API mDL implementation on Android and a Rest API mDL Verifier, that would add one to the tally for Rest API mDL Unique vendors, Rest API mDL Android, and Rest API mDL verifier Unique vendors.

Table 4: Unique implementations tested by protocol

	Unique vendors	Android	iOS	Other (e.g. CLI)
Rest API mDL	10	8	5	0

Rest API mDL Reader	11	-	-	-
OpenID4VP mDL App	7	4	3	3
OpenID4VP mDL Verifier	8	-	-	-

3.5.2 Geographical Participation

The event had participation from organizations headquartered globally, including in France, Germany, Japan, Slovenia, South Korea, Sweden, and the United States.



Figure 1: Event participation based on company headquarters.

4. Results

4.1 Data Collection and Processing

Data was collected through a combination of mDL implementers filling in result submission sheets for outcomes with the verifiers that they had tested with, and verifiers submitting a log output of their respective verifier pages for the duration of the testing period. Submitted mDL result sheets could then be cross-referenced with the submitted verifier logs.

While this approach allowed for real-time updates and feedback during the three-week testing window, the asynchronous nature of the event led to variations in the completeness and structure of the submitted results. As a result, programmatically processing the verifier logs became unfeasible.

To address this challenge, a manual cross-referencing process was undertaken. This involved comparing the mDL result submission sheets with the submitted verifier logs, leading to the compilation of outcomes categorized by protocol and platform.

This resulted in a grid of outcomes separated by protocol and platform as represented in *Table 2* and *Table 3*. For the reporting of errors, a distinction was made between Transport type errors and Validation type errors. Transport type errors are errors that a Verifier logged under checks *V_DATA_1*, *V_DATA_2* and *V_SEC_1*. Validation type errors are errors that a Verifier logged under checks *V_DATA_3*, *V_SEC_2* and *V_SEC_3*. As Reader Authentication was an optional feature during this Interoperability Event, a failure to pass Reader Authentication has not been counted as an error. With variability in the submitted verifier logs, skipped/unimplemented issuer and/or device authentication on the verifier's part are not counted as errors.

4.2 Data

This section shows aggregate outcomes per platform for the Rest API protocol and the OpenID4VP protocol in *Sections 4.2.1* and *4.2.2*, respectively. In *Figures 2 and 3*, anonymized success rates per implementation are given for the Rest API mDL implementations and Rest API Verifier implementations. Success rates are shown as a fraction. *Figures 4 and 5* contain parallel data for the OpenID4VP mDL implementations and OpenID4VP Verifier implementations. For success rate calculations, skipped outcomes are counted as unsuccessful outcomes.

4.2.1 Rest API Implementations

Table 5: Distribution of test scenario outcomes per category for the 'Rest API' protocol. Any missing results are counted in the "Skipped" category.

Result per check	Android		iOS		Other
	Count	Percentage	Count	Percentage	
OK	142	80.6%	80	72.7%	N.A.
Transport error	19	10.8%	14	12.7%	N.A.
Validation error	7	4.0%	0	0%	N.A.
Skipped	8	4.5%	16	14.6%	N.A.
Total	176		110		N.A.

Rest API mDL outcome success rate

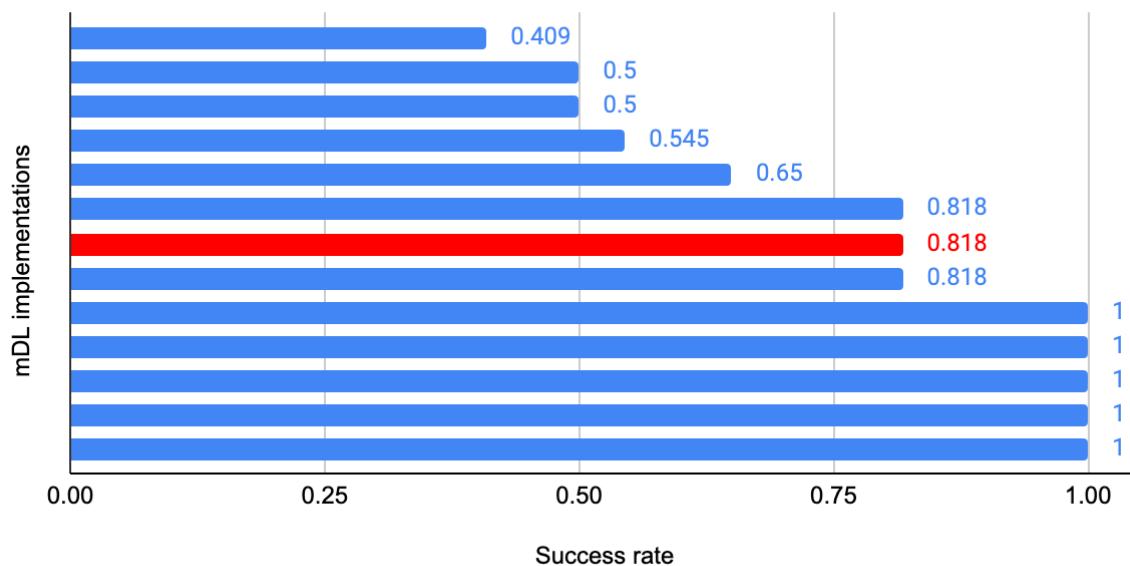


Figure 2: Anonymized aggregate outcome success rate for individual Rest API mDL implementations with Rest API mDL Verifiers. The red bar indicates the median success rate for all Rest API mDL implementations.

Rest API verifier outcome success rate

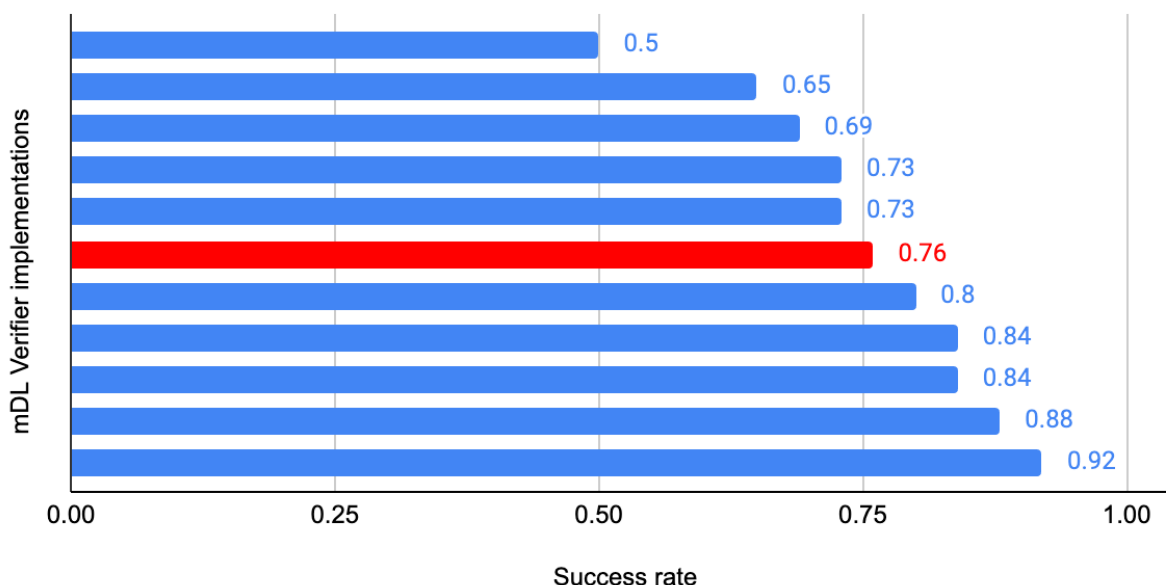


Figure 3: Anonymized aggregate outcome success rate for individual Rest API mDL Verifiers with Rest API mDL implementations. The red bar indicates the median success rate for all Rest API mDL Verifier implementations.

4.3.2 OpenID4VP Implementations

Table 6: Distribution of test scenario outcomes per category for the 'OpenID4VP' protocol. Any missing results are counted in the "Skipped" category.

Result per check	Android		iOS		Other	
	Count	Percentage	Count	Percentage	Count	Percentage
OK	40	62.5%	30	62.5%	32	66.7%
Transport error	9	14.0%	4	8.3%	4	8.3%
Validation error	4	6.3%	0	0%	4	8.3%
Skipped	11	17.2%	14	29.2%	8	16.7%

Total	64		48		48	
-------	----	--	----	--	----	--

OpenID4VP mDL outcome success rate

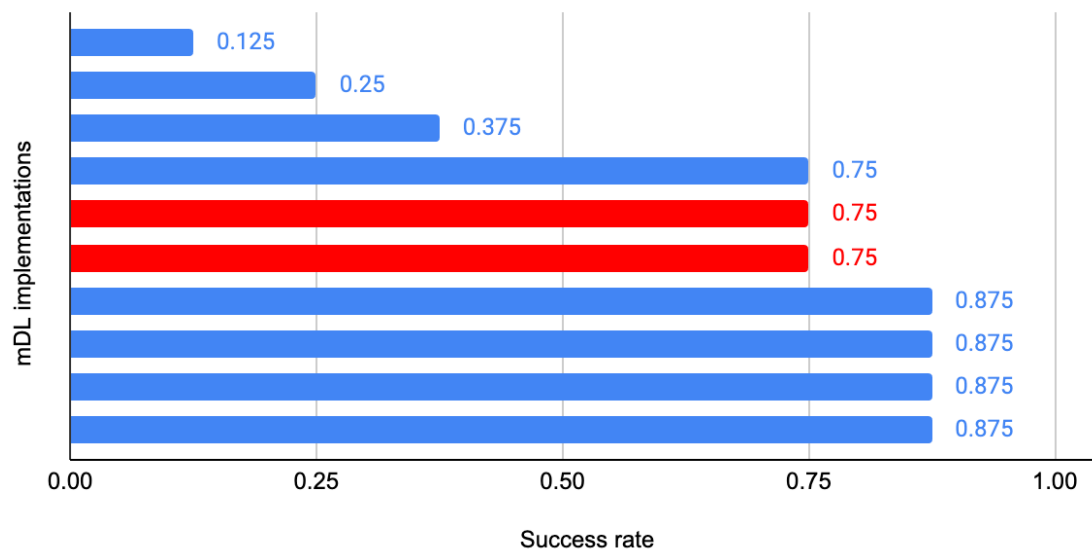


Figure 4: Anonymized aggregate outcome success rate for individual OpenID4VP mDL implementations with OpenID4VP verifiers. The red bars indicate the two components of the median value for all OpenID4VP mDL implementations.

OpenID4VP Verifier outcome success rate

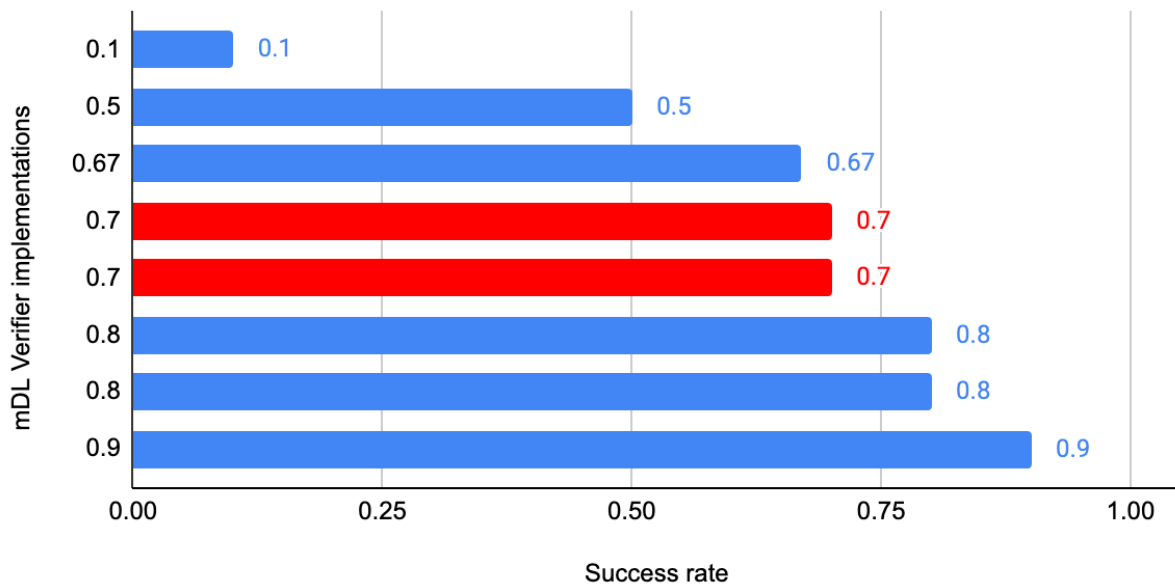


Figure 5: Anonymized aggregate outcome success rate for individual OpenID4VP mDL Verifier implementations with OpenID4VP mDLs. The red bars indicate the two components of the median value for all OpenID4VP mDL Verifier implementations.

4.3 Key metrics

Combining the results from the figures and tables in Section 4.2:

Table 7: Aggregate outcome success rate by protocol and role.

Implementation	Mean Success Rate	Median Success Rate
Rest API mDL	0.78	0.82
Rest API mDL Verifier	0.78	0.76
OpenID4VP mDL	0.64	0.75
OpenID4VP mDL Verifier	0.64	0.70

Furthermore, we observe:

- For both protocols, Transport errors (Rest API: 11.5%, OpenID4VP: 10.6%) were more common than Validation errors (Rest API: 2.4%, OpenID4VP: 5%)
- There were relatively many skipped results for the OpenID4VP protocol (20.6%) as compared to the Rest API protocol (8.4%).
- Validation errors for both protocols only occur on Android. We believe that this is coincidental and reflects a difference in implementation quality rather than any differences between the Android and iOS platforms

5. Conclusions and Findings

We want to thank everyone who participated in this event, and were excited to have participants implementing mDL readers and mDL apps using both Rest API and OID4VP protocol options defined in ISO/IEC 18013-7. Their contributions were crucial in thoroughly evaluating the specification. The good news is that the draft specifications we used for testing turned out to be quite robust. We did not find any major issues that needed fixing using normative changes to the specification.

Our event was designed to encourage cooperation between mDL readers and mDL app makers during interoperability testing. This helped us spot and address any problems that might have arisen when different systems needed to work together. Whenever participants noticed issues, they got in touch with the event organizers. They played a vital role in resolving these problems through email discussions, making sure we recorded feedback during the testing phase.

Most of the challenges we encountered were due to differences in the base documents of the ISO/IEC 18013-7 specification used for the event or the absence of some less critical features in the implementations. These issues were largely due to updates to the draft documents in advance of the interoperability event that some participants did not have adequate time or resources to address. This occasionally led to variations in how well the reader and mDL app systems followed the specifications. Fortunately, these differences were usually resolved by the participants, leading to successful interoperability testing.

After the testing period, we reached out to mDL reader and mDL app vendors to get their thoughts on the testing process and the specifications.

We are confident that the specifications provided clear enough guidance, as we did not discover any major issues that strictly required normative changes. However, the interoperability testing did reveal areas where the specification should improve in certain areas.

We gathered these insights from troubleshooting during the event, feedback forms, and the submitted test results, including the standardized log files. We presented a compiled list of findings without revealing the raw material during the ISO/IEC JTC1/SC17 WG10 in Singapore right after the interoperability event.

The working group reviewed, discussed, and found resolutions to these findings. The final test event findings and resolutions were published as N2349 in the ISO Global Directory.

The feedback from N2349 has been integrated into the latest version of ISO/IEC 18013-7, which we submitted as N2356. N2356 is the first draft of a Technical Specification, and it includes all the improvements and insights we've gathered to enhance the specification for better interoperability.