



10th International Interoperability Test Event

General Presentation

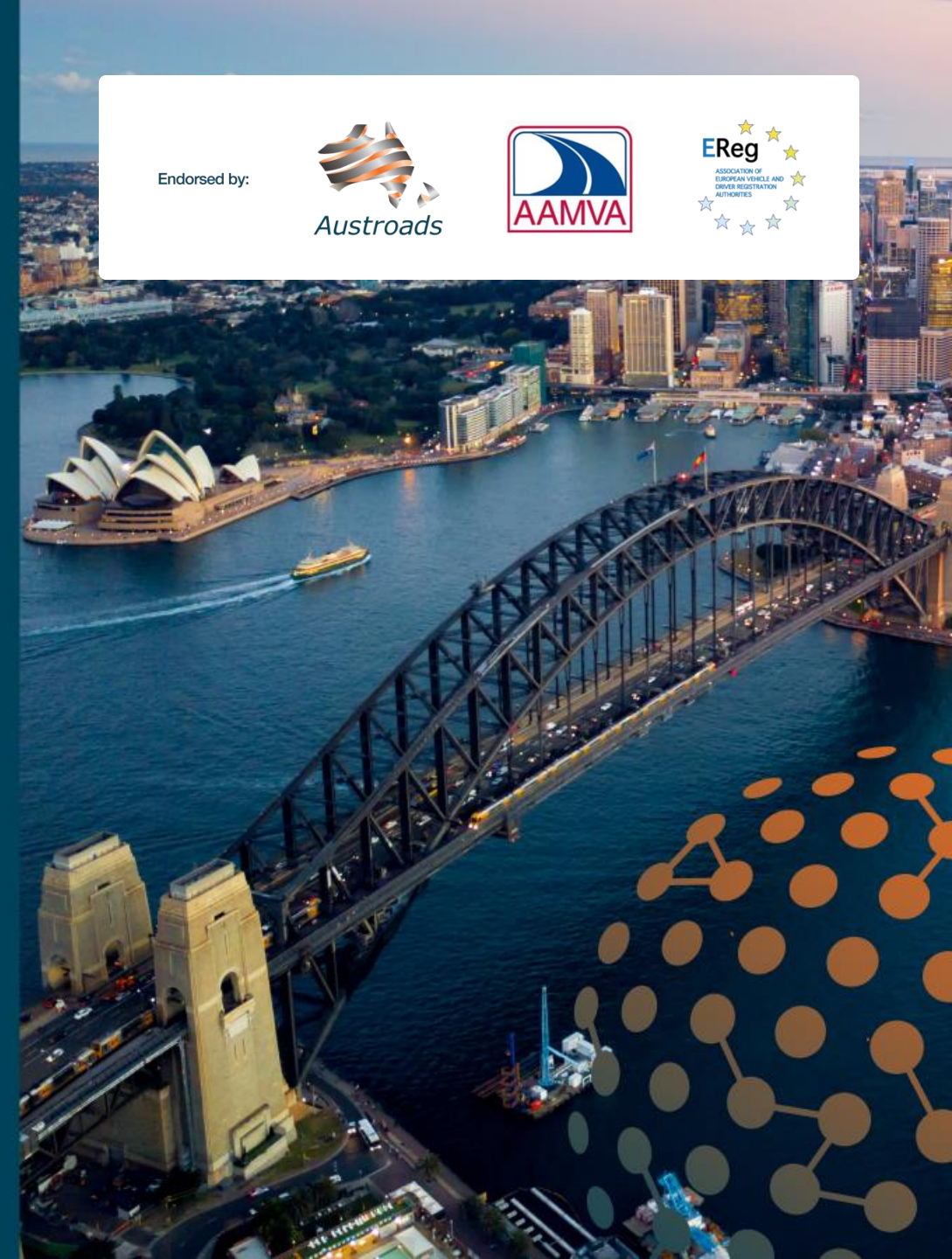
Hosted by:



MATTR

Facilitator: MATTR
Date: 3-5 October 2024
Location: Hilton Sydney

Endorsed by:



Overview

10th International Interoperability Test Event Summary

Introduction

Testing Scope

Test Event Statistics

Test Execution Statistics

Observations

Test Event Summary

Lessons Learned

Next Steps



Introduction



Austroroads

MATR

MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

Goals, Past Events & Key Activities

ISO/IEC 18013-5:2021 alongside adjacent standards and technical specifications define requirements for mobile driving licenses (mDLs) and generic mobile documents (mdocs) to enable a secure and interoperable digital ecosystem.

The mDL/mdoc community hosts interoperability test events regularly to:

Confirm the feasibility of implementing the standards.

Offer feedback, disambiguation, and clarification to increase the standards quality.

Maintain market momentum and accelerate mDL and mdoc implementations time to market.

Past Events & Key Activities:

2017: Formal New Work Item Proposal acceptance and launch of the standardization project.

August 2021: Approval of the Final Draft International Standard version ISO/IEC 18013-5.

April 2018: 1st Committee Draft (CD) of ISO/IEC 18013-5 for international ballot/commenting.

September 2021: Publication of the final International Standard ISO/IEC 18013-5:2021.

October 2018: 1st mDL interoperability event in Okayama, Japan, based on the 1st CD draft.

October 2021: European test event in Rotterdam, The Netherlands.

December 2018: Austroads, AAMVA, and EReg endorse the international standardization of mDLs at their Global Summit in Melbourne, Australia.

November 2021: American test event in Houston, TX, USA.

March 2019: 2nd CD draft for ballot, incorporating the learnings from the first test event.

May 2022: 6th international test event in Louisville, KY, USA.

August 2019: America's first mDL test event at the AAMVA AIC, based on the 2nd CD draft.

December 2022: 7th international test event in Brisbane, QLD, Australia.

November 2019: Australia's first mDL test event in Brisbane, Australia, based on the proposed text for the Draft International Standard (DIS).

August 2023: First online-only event for testing ISO/IEC TS 18013-7.

April 2020: Approval of the DIS version of ISO/IEC 18013-5.

December 2023: 9th in-person international test event in Paris, France.

General Prerequisites

Participation was free but prior registration before the registration deadline was required with limited available seats

Registration for the test event was different from the registration for the introductory webinar

No affiliation with ISO/IEC or any other organisation was required

In-person attendance was required and remote attendance was not possible

Technical Prerequisites

Participation was open for organisations offering mdoc holder and/or reader implementations compliant with ISO/IEC 18013-5:2021

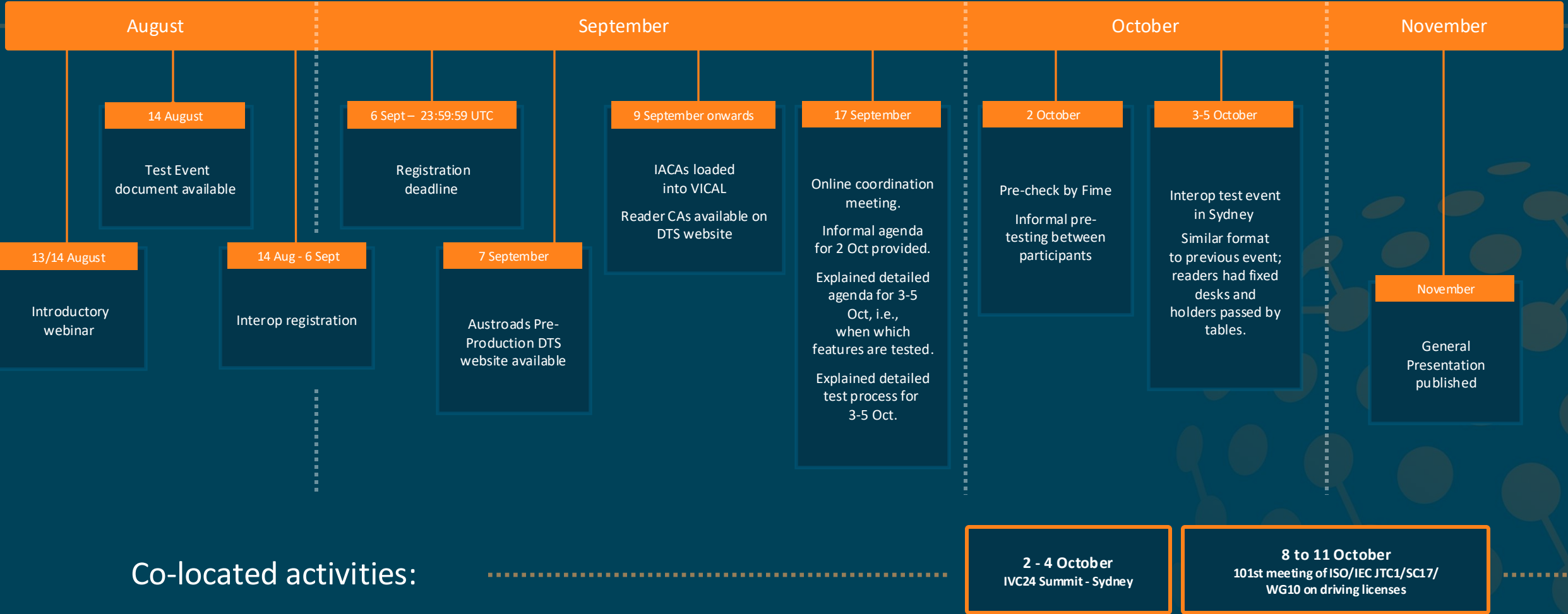
Participants with support for Austroads Pre-Production DTS for obtaining the VICAL, IACA and reader certificates were prioritized

Participants were also invited to optionally test implementations of draft versions of ISO/IEC TS 18013-7 and ISO/IEC 18013-5 Amendment 1, ISO/IEC TS 23220-4, ISO/IEC TS 23220-2, and a profile for the W3C Digital Credentials API (Browser API), as well as other credential types such as photoID, mobile vehicle registration Cards (mVRC) and mobile health certificates (micov)

Event Details and Dates

Organiser & Host: Austroads
Facilitator: MATTR

Endorsed by:



MATTR

MATTR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

Before the Event

Two introductory webinars were hosted by the facilitator (APAC/EU and US/EU-friendly)

Registration website was hosted under a public website

During registration, participants were required to submit a conformance statement and if applicable their IACA as well as reader certificate(s)

Registration period was 13 August – 6 September 23:59:59 UTC

After registering for the test event, the coordinator provided:

Link to Austroads Pre-Production DTS to fetch VICAL and Reader CAs used for the test event

Draft Specifications

Examples

Pseudonymous identifier for each implementation

Participants could raise questions by sending an email to the coordinator to clarify questions on the test process, supporting material and interpretation of standards and draft specifications.

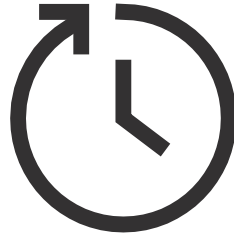
Participants received answers by email and an anonymized answer was provided in the issue log on the event website.

For the test event a coordinator email was created

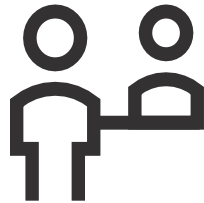
Optional coordination meeting on 17 September where the detailed agenda and test approach was discussed

OPTIONAL

At the 2 October Event



Pre-check by [Fime](#) (formerly known as UL Solutions) with each participant to check conformance with ISO/IEC 18013-5:2021 and ISO/IEC TS 18013-7 Annex A, and provide feedback if submitted conformance statement was still accurate



Unmoderated pre-testing between participants

REQUIRED

At the 3-5 October Event

Interoperability testing organized and moderated by the facilitator

A limited number of observers were present (IVC summit and others)

Facilitator helped with the interpretation of standards and/or draft technical specifications

Facilitator presented the test plan including three test focuses

Facilitator organized **crossover testing**

Participants tested their implementations crossover with other participants

Participants captured their own test results using an online form provided by the facilitator:

To reduce manual errors in reporting

To optimize for testing time



After the Event

Facilitator generated high level General Presentation based on anonymized captured test results submitted by participants using an online form

General Presentation will be provided to ISO/IEC SC17/JTC1 WG10 to inform the standardization process

Facilitator created this General Presentation including a summary of the test event, test approach and test results

Participants indicated approval or disapproval of the use of their organization's name and logo in this General Presentation

Participants will receive the General Presentation and submitted test results pertaining their implementations

Participants were not allowed to use their participation in the test event to promote themselves as ISO-approved, WG10—approved etc.

Participants are only allowed to use the General Presentation for promotion and marketing

Interoperability Testing



Austrorads

MATR

MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

Scope and Base Documents

Required

- mobile Driving License (mDL) as per ISO/IEC 18013-5:2021
- Attended (proximity) Device Retrieval as per ISO/IEC 18013-5:2021, e.g., QR/NFC/BLE/WiFi-Aware

Preferred

- Verified Issuing Certificate Authority List (VICAL) as per ISO/IEC 18013-5:2021
- Austroads pre-production Digital Trust Service (DTS) to load VICAL, IACA and Reader CA certificates

Optional

- PhotoID as defined in ISO/IEC TS 23220-4 Annex C (WG4/N4583)
- Mobile health credential certificates (micov) as defined in Guidelines for developing ISO-compliant mdoc for eHealth (RC3.1)
- Mobile vehicle registration certificates (mVRC) as defined in ISO/IEC 7367 (WD2.2)
- Common namespace in ISO/IEC 23220-2 (Final DTS)
- Attended Server Retrieval as per ISO/IEC 18013-5
- Remote (unattended) transactions
 - ISO/IEC TS 18013-7 RestAPI and OpenID4VP (Final DTS)
 - W3C WICG Digital Credentials API (Browser API) using Austroads Request Forwarding Profile (WG10/N2489)
- Newly provisioned features of ISO/IEC 18013-5 Amendment 1 (WD8)
 - MSO revocation
 - New request structure
 - New BLE L2CAP

Crossover Testing

Facilitator assigned pseudonymous identifiers to each holder and reader implementation: PRx for proximity readers, RRx for remote readers, Hx for holders

Readers were assigned fixed tables, holders passed by tables

Implementations used the Austroads pre-production DTS to get the latest VICAL, IACA and reader certificates

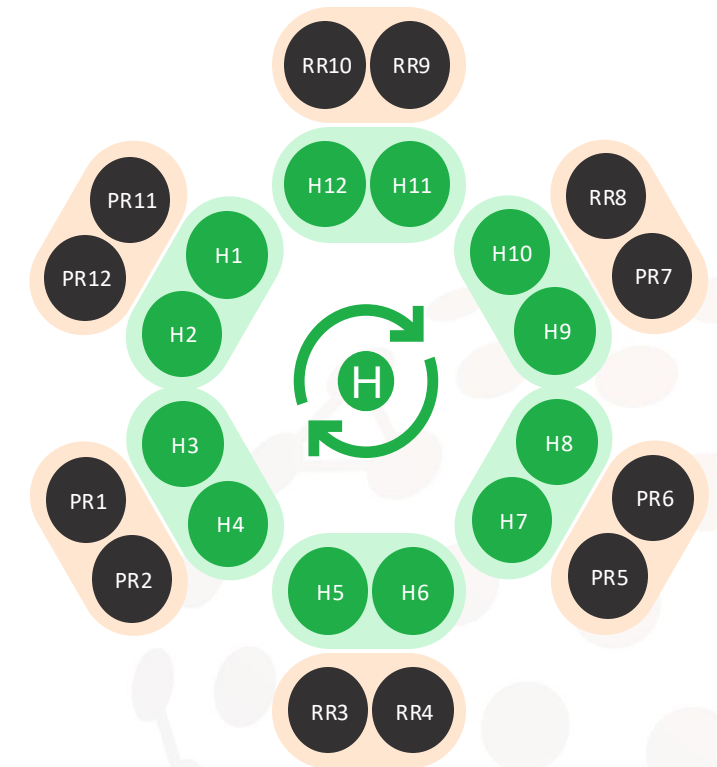
Three days test event was divided into 15 minutes testing rotations with three focus areas

Every 15 minutes, facilitator presented the current testing rotation:

- Assigned combinations of reader and holder implementations for crossover testing based on their submitted conformance statements
- Provided focus area for each combination using colour codes
- Reminder to test also less common features

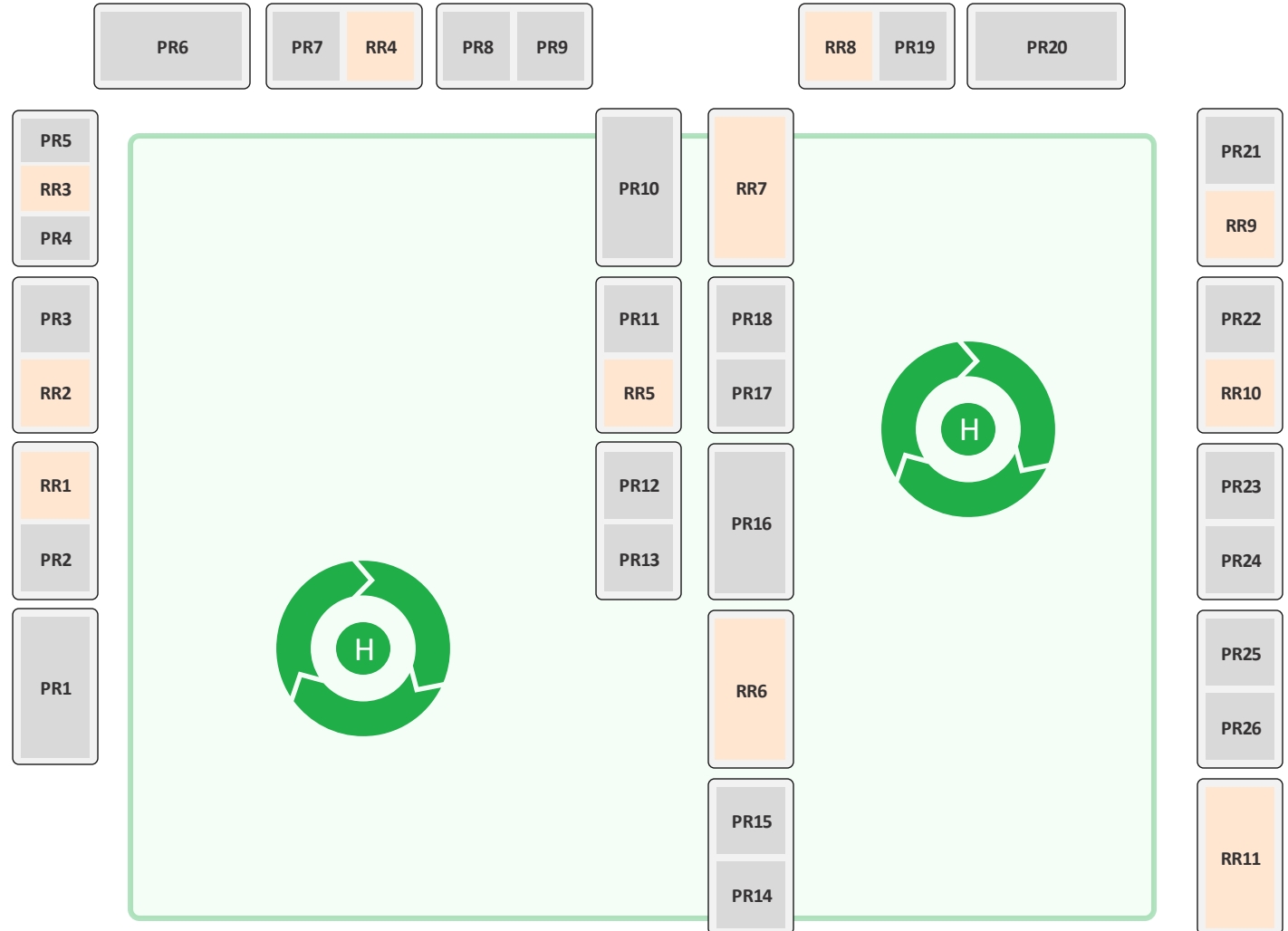
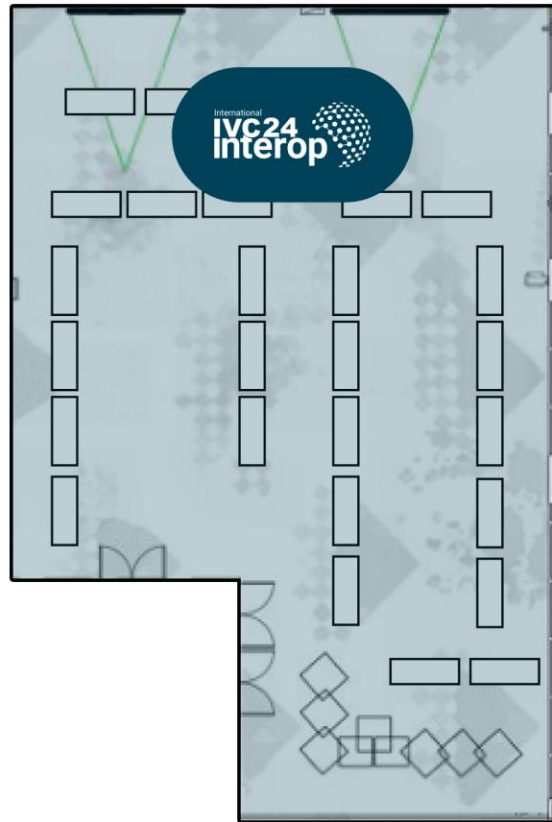
At the end of each rotation, reader participants were asked to submit results of all recorded transactions (possibly multiple) using an online form

Facilitator monitored submitted results to check if participants had issues submitting their forms and check if participants kept the right focus and also tested less common features



Rotations every 15 minutes

Final Floor Plan



Test Focus 1

Proximity Readers (PR):

Primary focus:

- ISO 18013-5 implementation's default config, e.g., QR + BLE, NFC + BLE, NFC + NFC, with mDL credentials.

Secondary focus:

- if supported, other configs, e.g. Wifi Aware
- if supported, photo ID

Tertiary focus:

- if supported, other credential types, i.e., mVRC, micov

Remote Readers (RR):

Primary focus:

- OID4VP / Rest API (ISO 18013-7) with mDL credentials

Secondary focus:

- if supported, photo ID

Tertiary focus:

- if supported, other credential types, i.e., mVRC, micov

Test Focus 2

Proximity Readers (PR):

Primary focus:

- ISO 18013-5 regressions, or
- if supported, ISO 18013-5 server retrieval
- if supported, ISO 18013-5 amendment 1 features (new request structure, new L2CAP, *MSO revocation*)

Remote Readers (RR):

Primary focus:

- ISO 18013-7 regressions
- if supported, Browser API

Secondary focus:

- if supported, ISO 18013-5 amendment 1 features (new request structure, *MSO revocation*)

Test Focus 3

Proximity Readers (PR):

Primary focus:

- ISO 18013-5 regressions, or
- if supported, ISO 18013-5 amendment 1 features (MSO revocation, *new request structure*, *new L2CAP*)

Remote Readers (RR):

Primary focus:

- if supported, ISO 18013-7 regressions
- if supported, ISO 18013-5 amendment 1 features (MSO revocation, *new request structure*)
- if supported, Browser API

Example Rotation Slide

Day 2: 11-11:15am (15 mins)

Focus 1

Focus 2

Focus 3

Unassigned slots were introduced to facilitate regression testing and to give participants more flexibility

Readers	Apps
PR1	H14
PR2	H29
PR3	H8
PR4	H13
PR5	H6, H7
PR6	
PR7	H20
PR8	H22
PR9	H19
PR10	H26
PR11	H17

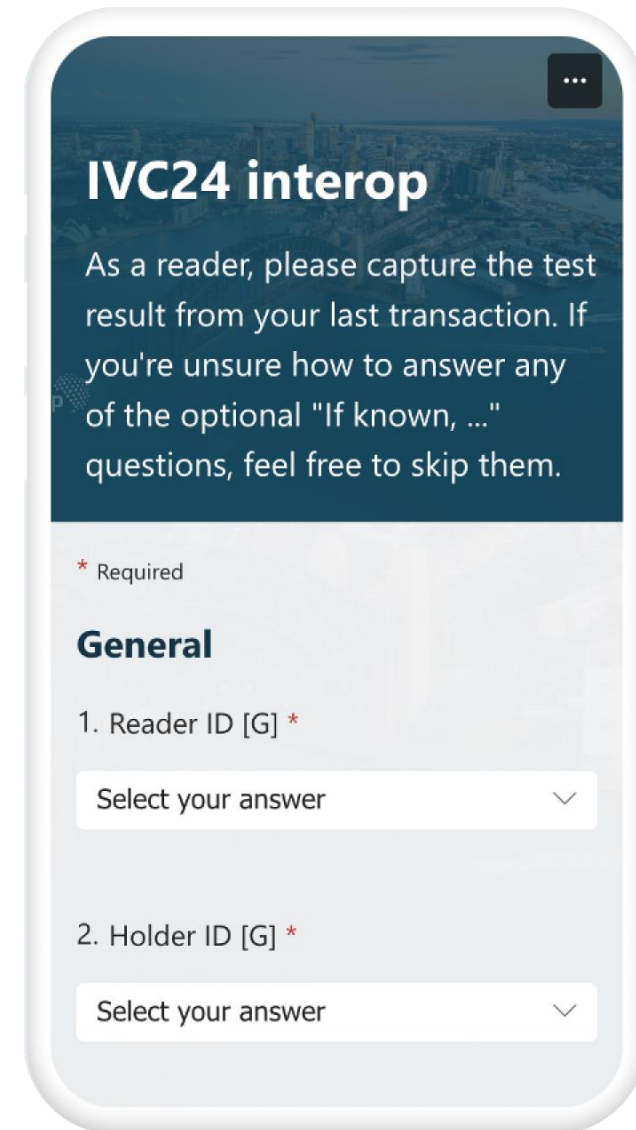
Readers	Apps
PR12	H21
PR13	H16
PR14	H23
PR15	H4, H5
PR16	H15
PR17	H11
PR18	H24
PR19	H2
PR20	H28
PR21	H18
PR22	H9

Readers	Apps
PR23	H1
PR24	H3
PR25	H27
PR26	H25
RR1	H30
RR2	
RR3	
RR4	
RR5	
RR6	
RR7	

Readers	Apps
RR8	
RR9	
RR10	
RR11	

Test Result Capture

- Readers were asked to submit the results of each transaction using an online form after testing a transaction with a holder.
- The form was available online.
- Amongst other metrics, the form asked for
 - Reader and holder ID
 - Main test scenario
 - VICAL usage
 - Credential types (multiple possible)
 - Transaction type
 - Performed security and data checks
 - Applicable ISO/IEC 18013-5 Amendment 1 features
 - Overall test result
 - Failure phase, issue and cause
 - Feedback



The screenshot shows a mobile application interface for capturing test results. At the top, there is a dark blue header with the title "IVC24 interop" and a three-dot menu icon. Below the header, a white text box contains the instruction: "As a reader, please capture the test result from your last transaction. If you're unsure how to answer any of the optional 'If known, ...' questions, feel free to skip them." Below this, a red asterisk indicates a required section titled "General". The form contains two numbered questions, each with a dropdown menu:

- 1. Reader ID [G] *
Select your answer
- 2. Holder ID [G] *
Select your answer

Test Event Statistics



Austroroads

MATR

MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT



FeliCa Networks



RDW

THALES

SAMSUNG



MATR



MATR

MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT



MATTR

MATTR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

Conformance Statements Received¹⁾

Number of organisations:

22

Number of participants:

74

Number of Mdoc apps:

30

All support Device Retrieval

All IACAs loaded into VICAL

Server Retrieval: 8

New request structure: 7

MSO revocation

- Identifier list: 7
- Status list: 8

New L2CAP: 12

Online Retrieval

- Rest API: 15
- OID4VP: 15
- Browser API: 8

Mdoc reader apps:

26

All support Device Retrieval

VICAL: 17

Server Retrieval: 10

New request structure: 10

MSO revocation

- Identifier list: 8
- Status list: 11

New L2CAP: 14

Mdoc remote reader websites:

11

VICAL: 6

Server Retrieval: 2

New request structure: 2

MSO revocation

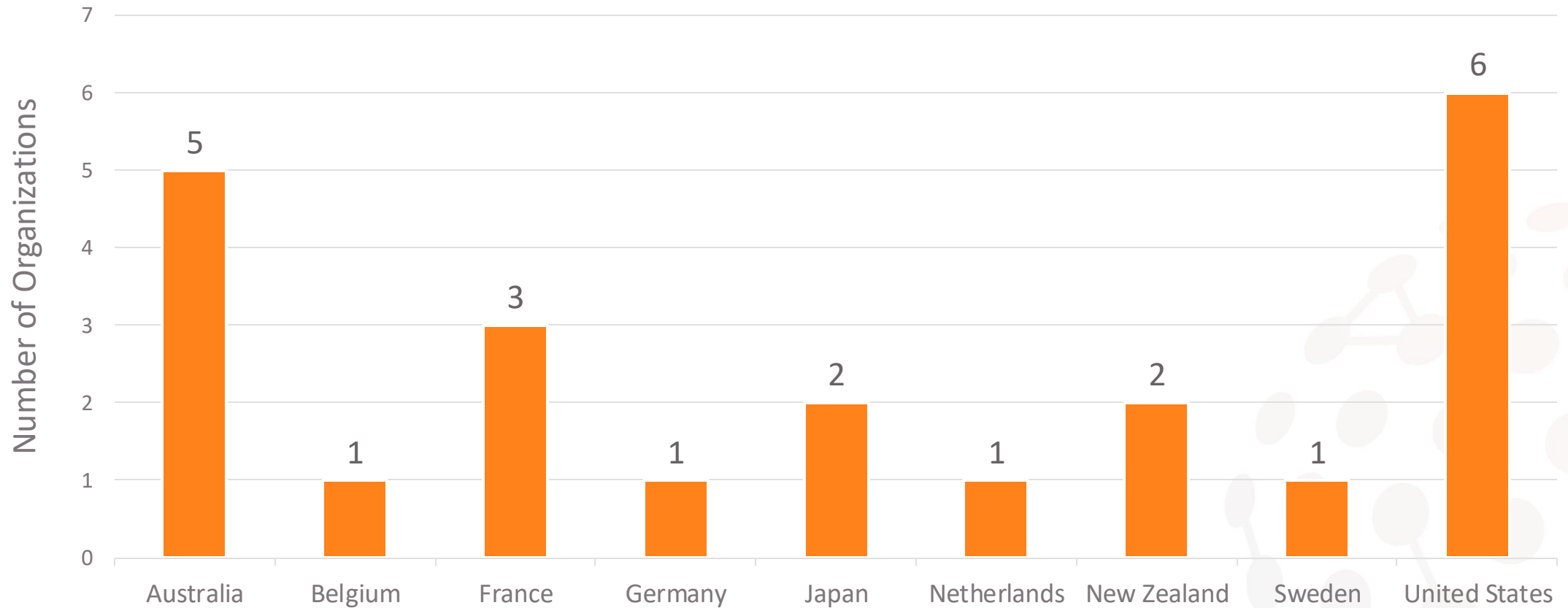
- Identifier list: 3
- Status list: 5

Online Retrieval

- Rest API: 8
- OID4VP: 9
- Browser API: 7

¹⁾ Number of implementations per feature varied in the test event, e.g., new request structure

Participating Organizations by Country¹⁾



¹⁾ As provided in the registration form by the representative of the participating organization

Test Execution Statistics



Austroroads

MATR

MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

Disclaimer

- Reported test results are based on submitted test results by the provider of reader implementations
- All figures in the following sections may not cover all test executions and may contain minor inaccuracies



Total Transactions



Austrroads

MATR

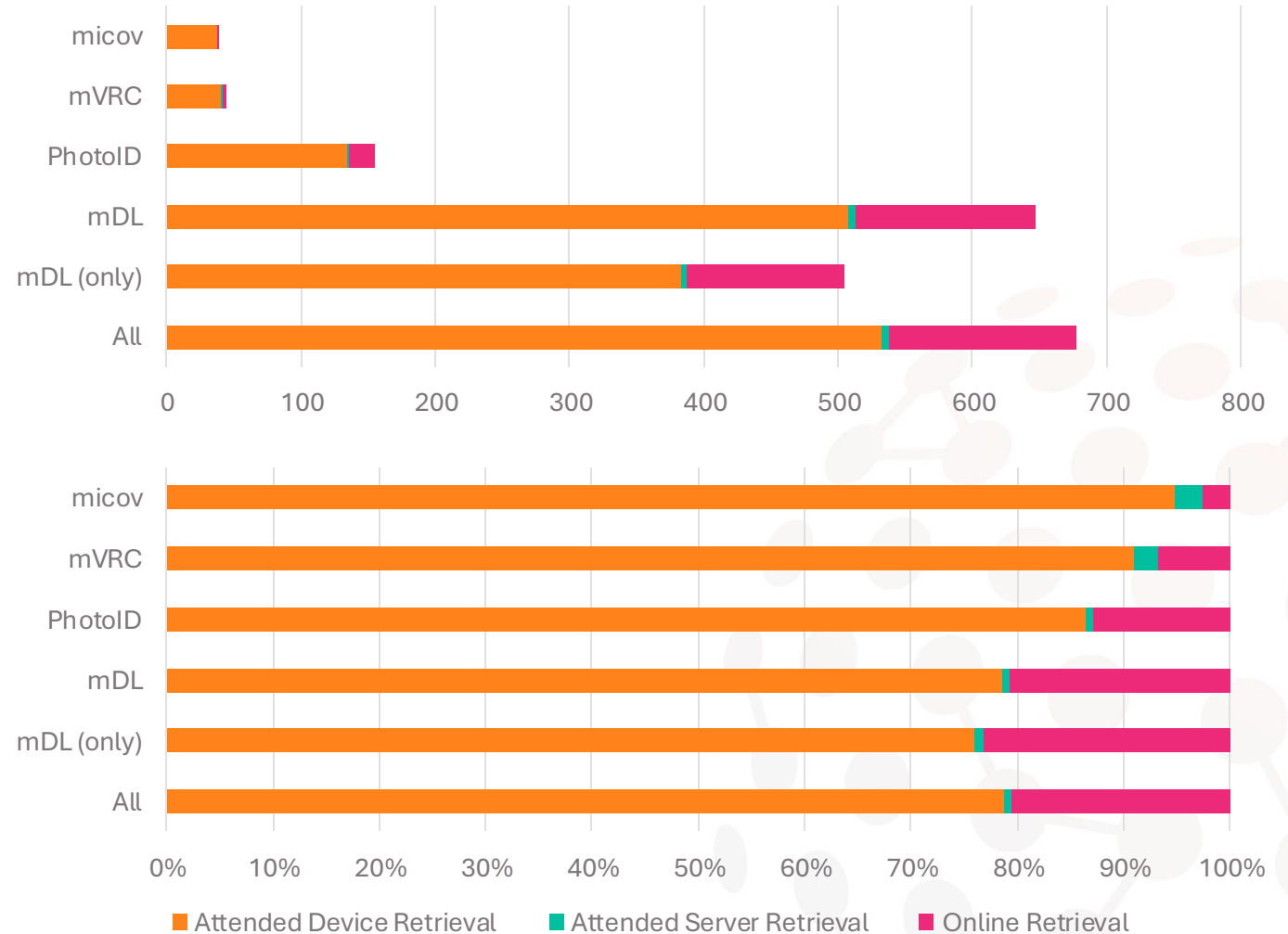
MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

Terminology

- **Main scenarios**
 - Attended Device Retrieval (ISO/IEC 18013-5:2021 without Amendment 1 features)
 - Attended Server Retrieval (as per ISO/IEC 18013-5:2021 without Amendment 1 features)
 - Online Retrieval (ISO/IEC 18013-7:2024 or Browser API)
- **Credential types**
 - Unless stated otherwise, e.g., “mDL (only)”, transactions were attributed to a specific credential type even if other credential types were used in the same transaction
 - Possible values: all, mDL, mDL (only), PhotoID, mVRC, micov
- **Configuration:** a combination of device engagement and data retrieval (for Attended Device Retrieval), or server retrieval method and during which phase the server token is transmitted (for Attended Server Retrieval), or online retrieval protocol (for Online Retrieval)
- **All configurations:** the complete set of configurations for a specific holder/reader combination
- **Default configuration:** the first configuration that was tested for a specific holder/reader combination
- **Round:** the 1-N transaction for a specific combination of holder/reader and configuration
- **All rounds:** the complete set of 1-N regressions
- **Best/worst round:** the round with the best/worst overall transaction result
- **Last round:** the Nth round
- **Top-10-10:** best rounds of the top 10 holder and reader implementations, based on their overall test results across all configurations. This metric is useful for showing statistics that exclude the impact of less mature implementations, which may affect the overall success rate.

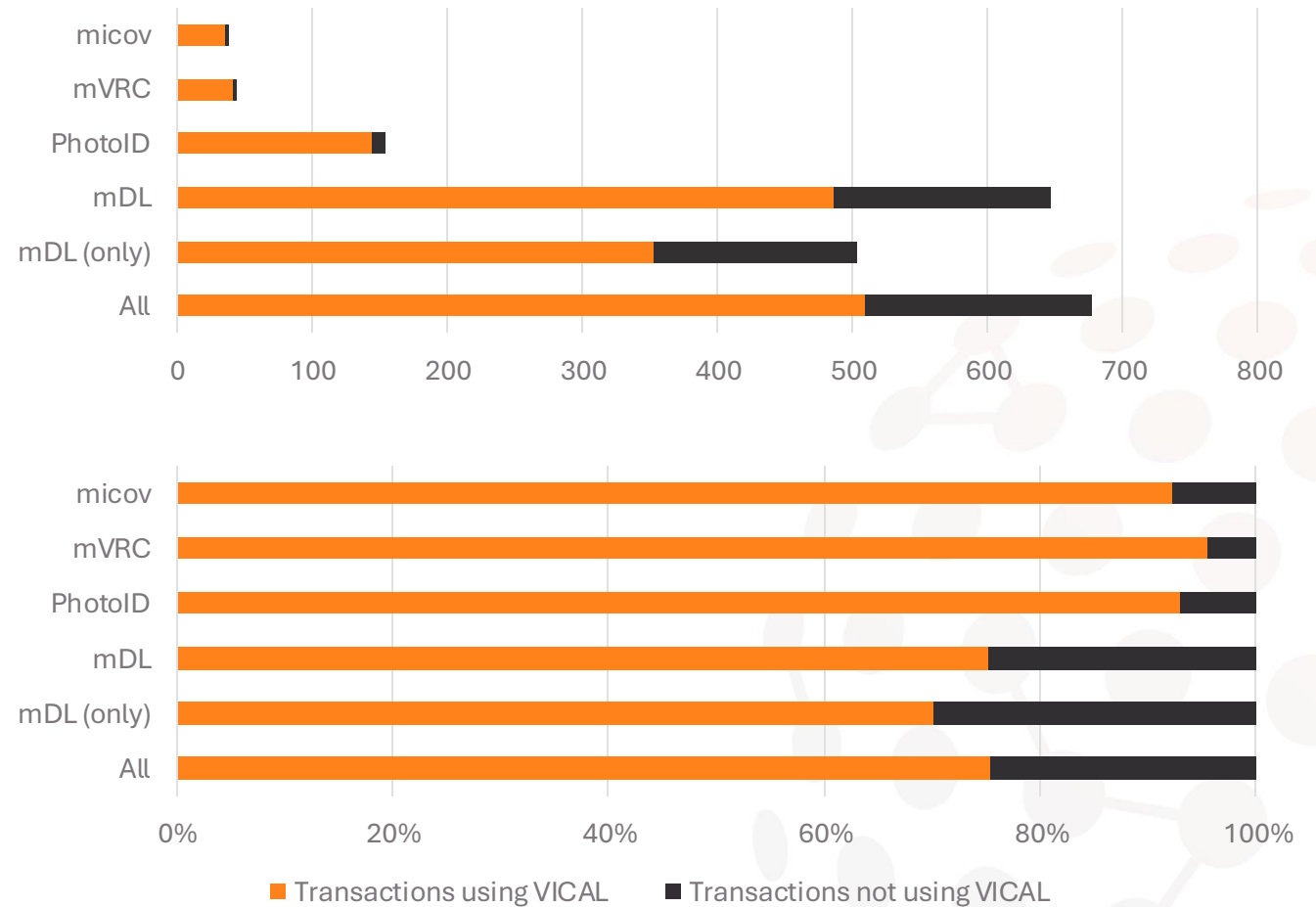
Number of Transactions by Main Scenario

- Shows the total number of transactions by main scenario and credential type
- Includes all rounds for comprehensive analysis
- Percentages per transactions type for all credential types
 - **Attended Device Retrieval: 78.73%**
 - **Attended Server Retrieval: 0.74%**
 - **Online Retrieval: 20.53%**
- Attended Server Retrieval was the least popular option with only 5 transactions
- mDL was the most popular credential type across all transaction types due to its mandatory status
- mDL and PhotoID were the most commonly used credential types in optional transaction types
- micov and mVRC were primarily tested in the mandatory transaction type
- Optional credential types were mostly tested in combination with the mDL, in particular, or with other credential types



Number of Transactions by VICAL Usage

- Displays the total number of transactions by VICAL usage and credential type
- Includes all rounds to ensure comprehensive analysis
- Approximately 75% of all transactions used the VICAL provided by the Austroads Pre-Production Digital Trust Service (DTS) for issuer data authentication
 - Using VICAL: 510 transactions
 - Without VICAL: 167 transactions
- VICAL usage percentage increases when optional credential types are included
- Numbers show that the VICAL provided by the Austroads Pre-Production DTS was well accepted by most implementers
- No failures directly related to VICAL were reported



Attended Device Retrieval Transactions



Austrade

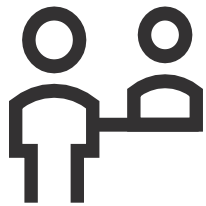
MATR

MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

VICAL Update Transactions



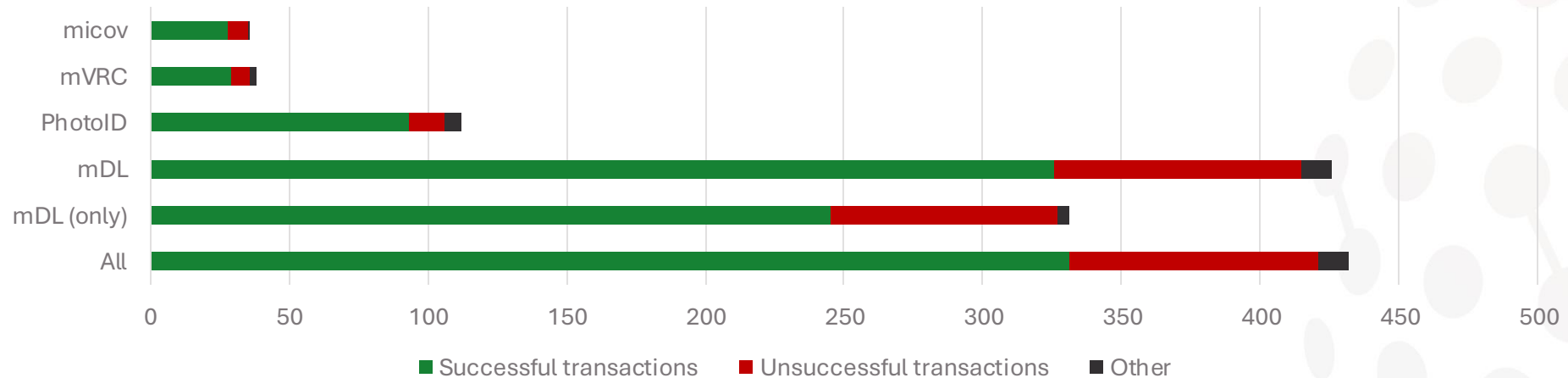
- Austroads successfully demonstrated a live update of its Pre-Production Digital Trust Service (DTS). Using the self-service portal, the IACA of an mDL holder implementation was removed, with 11 readers then verifying the change.



- 10 readers confirmed the mDL was no longer trusted, showcasing the effectiveness of the DTS, while one reader encountered an unrelated issue.

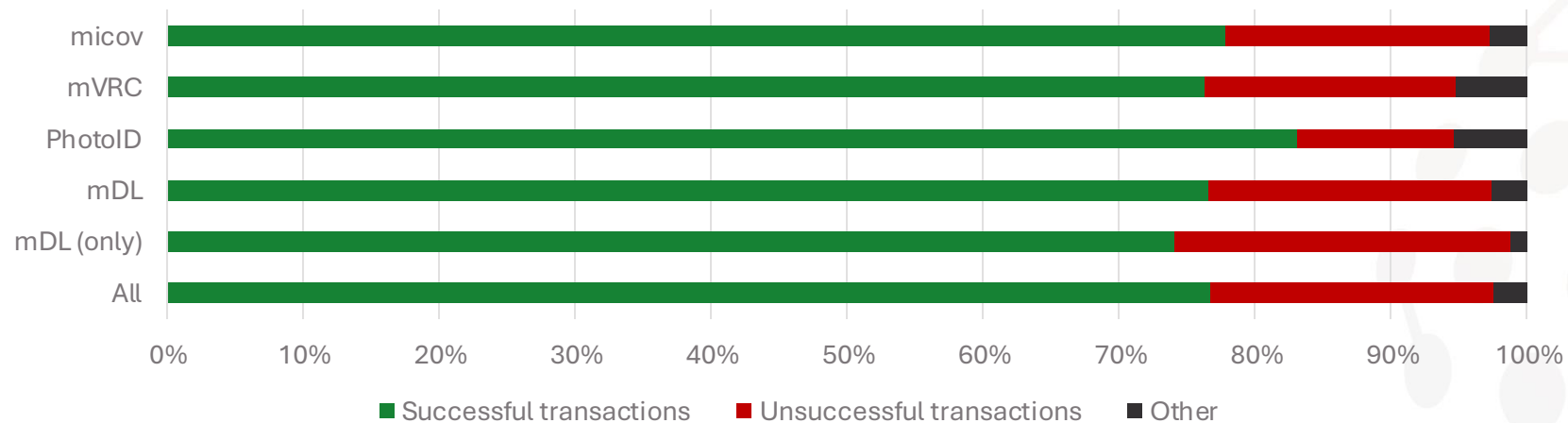
Number of Transactions by Success Rate (all configurations)

- Displays the total number of Attended Device Retrieval transactions by success rate and credential type
- Includes **all configurations** and best rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- 432 total transactions in all configurations and best rounds
- 325 transactions used the VICAL
- 426 transactions included mDL
- 331 transactions included mDL only
- 112 transactions included PhotoID
- 38 transactions included mVRC
- 36 transactions included micov



Number of Transactions by Success Rate (all configurations)

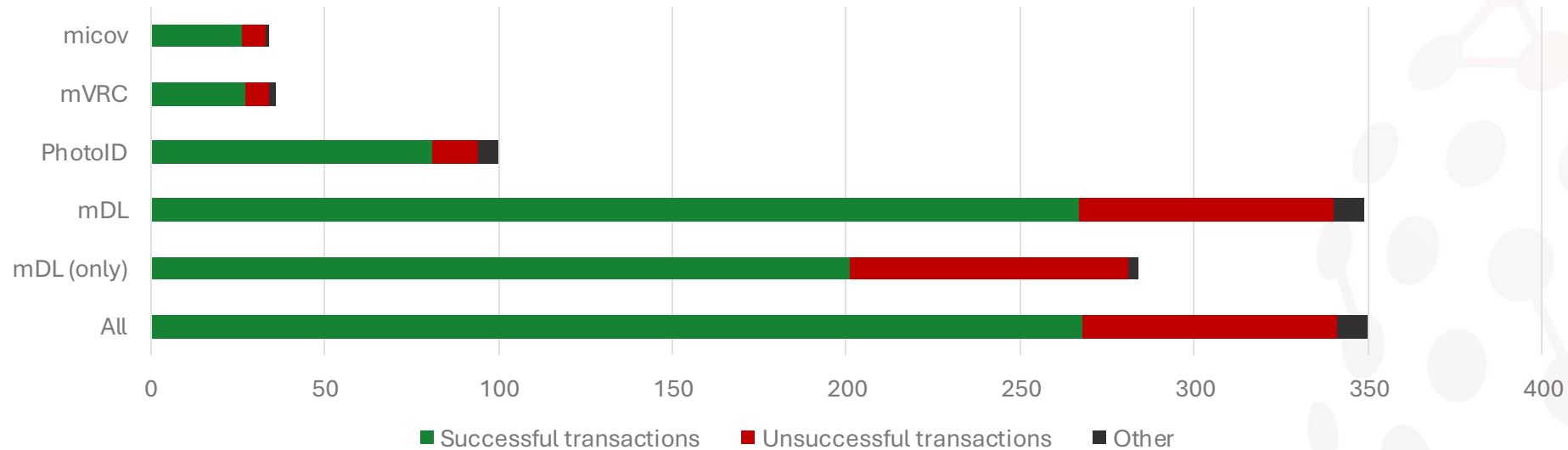
- Displays the percentage of Attended Device Retrieval transactions by success rate and credential type
- Includes **all configurations** and best rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- 75.23% of transactions used the VICAL
- 98.61% of transactions included mDL
- 76.62% of transactions included mDL only
- Overall success rate is 76.62% across credential types
- mDL (only) have a slightly lower success rate because they are overrepresented in less mature configuration implementations



Number of Transactions by Success Rate (default configurations)

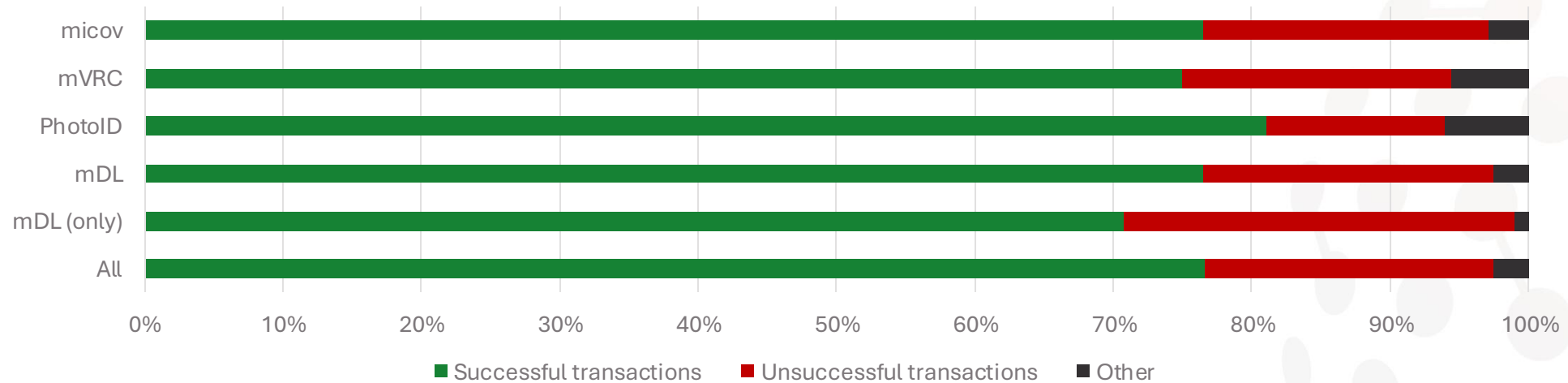
- Displays the total number of Attended Device Retrieval transactions by success rate and credential type
- Includes **default configurations** and best rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures

- 350 total transactions in default configurations and best rounds
- 261 transactions used the VICAL
- 349 transactions included mDL
- 284 transactions included mDL only
- 100 transactions included PhotoID
- 36 transactions included mVRC
- 34 transactions included micov



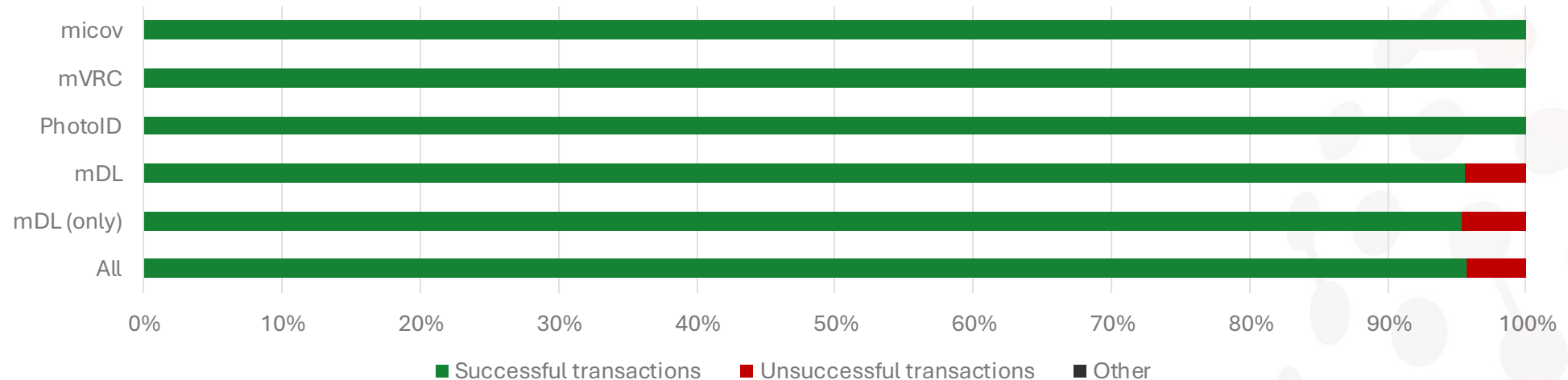
Number of Transactions by Success Rate (default configurations)

- Displays the percentage of Attended Device Retrieval transactions by success rate and credential type
- Includes **default configurations** and best rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- 99.71% of all transactions included mDL
- 81.14% of all transactions included mDL only
- 74.57% of all transactions used the VICAL
- Overall success rate is 76.57% across credential types
- Same observations as for **all configurations** and no improvement of success rate between all configurations and default configurations



Number of Transactions by Success Rate (top-10-10)

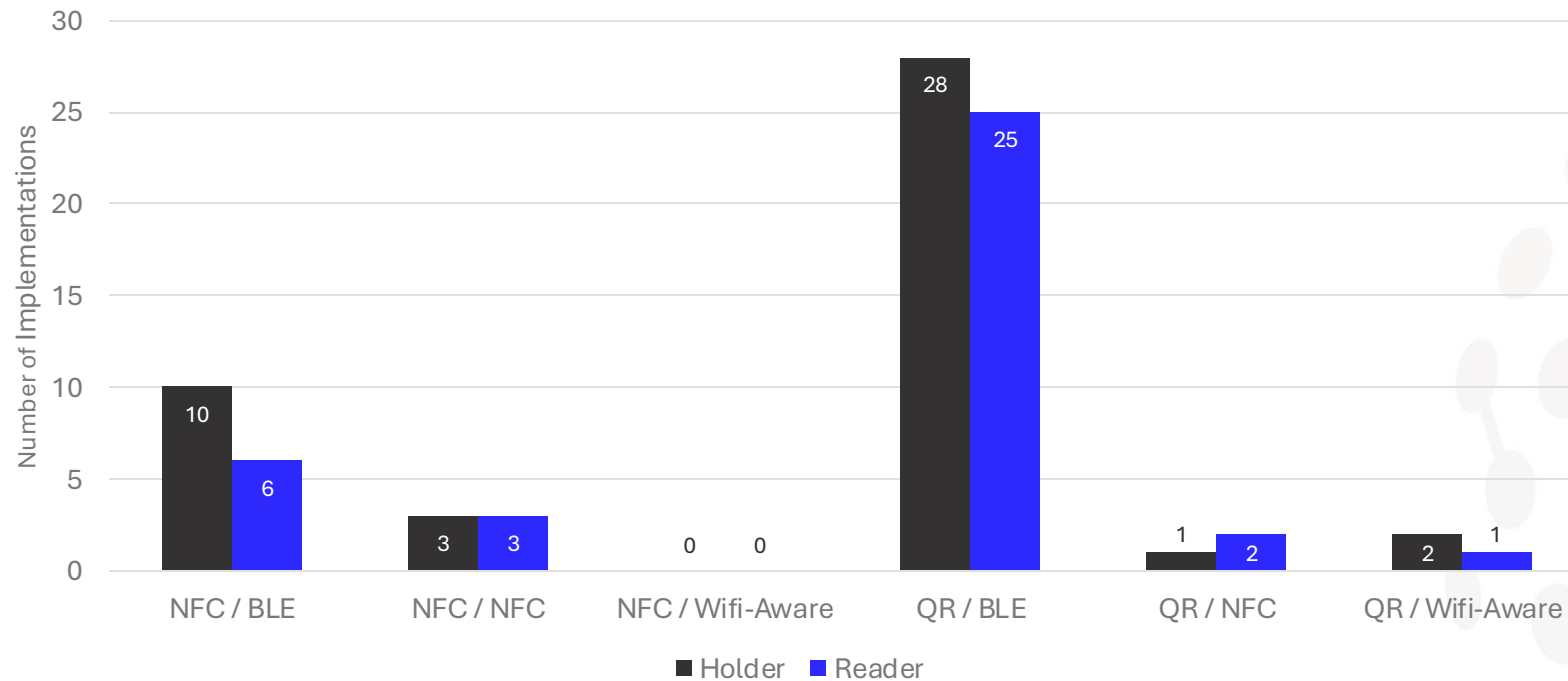
- Displays the percentage of Attended Device Retrieval transactions by success rate and credential type
- Includes all configurations and best rounds of the **top-10-10** excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- 93.48% of all transactions included mDL
- 97.83% of all transactions included mDL only
- 93.48% of all transactions used the VICAL
- Overall success rate is 95.65% which shows a very high degree of interoperability between the more mature implementations
- Since outliers are filtered out, also the mDL credential type has a naturally very high success rate compared to all implementers.



Number of Implementations by Configuration

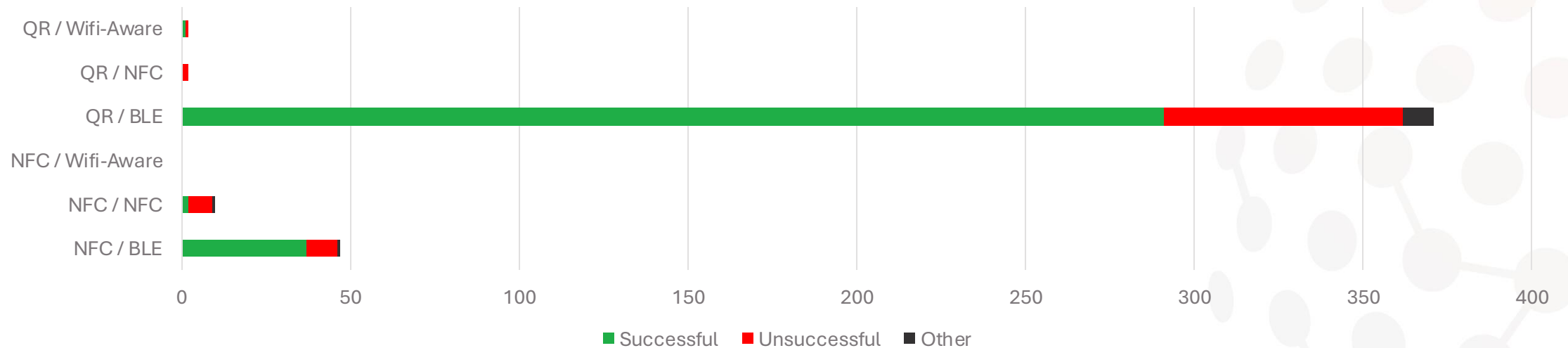
- Displays the number of implementations by per configuration that submitted test results of Attended Device Retrieval transactions

- NFC/BLE: 10 holder, 6 reader
- NFC/NFC: 3 holder, 3 reader
- NFC/Wifi-Aware: 0 holder/reader
- QR/BLE: 28 holder, 25 reader
- QR/NFC: 1 holder, 2 reader
- QR/Wifi-Aware: 2 holder, 1 reader



Number of Transactions by Success Rate and Configuration

- Displays the total number of Attended Device Retrieval transactions per configuration by success rate across all credential types
- Includes best rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- Includes failures across all phases of an Attended Device Retrieval transaction, including those not related to the actual transmission technology, such as security checks, data validation, etc.
- Details about the type of failure can be found in the following slides
- Best rounds
 - NFC/BLE: 47 (total), 37 (success), 9 (fail), 1 (other)
 - NFC/NFC: 10 (total), 2 (success), 7 (fail), 1 (other)
 - NFC/Wifi-Aware: 0 (total)
 - QR/BLE: 371 (total), 291 (success), 71 (fail), 9 (other)
 - QR/NFC: 2 (total), 2 (fail)
 - QR/Wifi-Aware: 2 (total), 1 (success), 1 (fail)

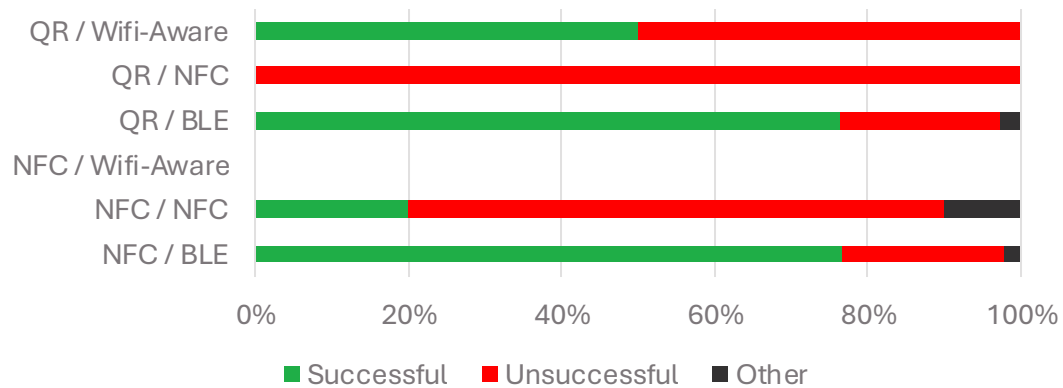


Number of Transactions by Success Rate and Configuration

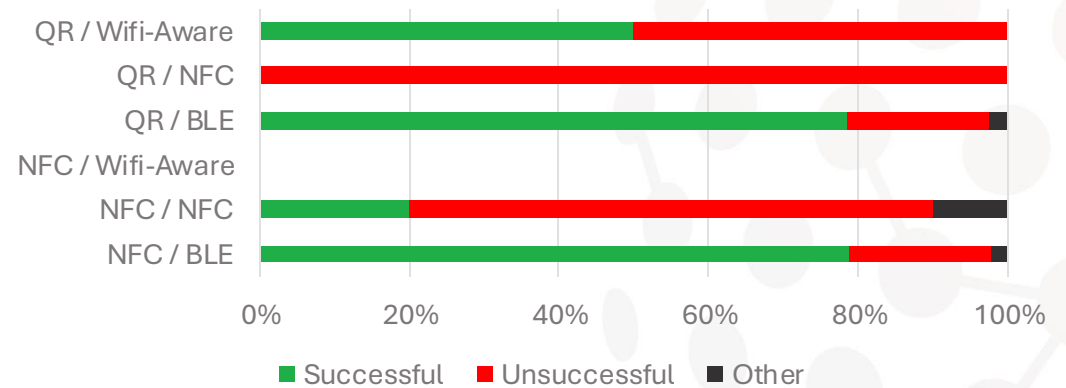
- Displays the percentage of Attended Device Retrieval transactions per configuration by success rate across all credential types
- Distinct charts for best rounds and worst rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- Includes failures across all phases of an Attended Device Retrieval transaction, including those not related to the actual transmission technology, such as security checks, data validation, etc.

- Details about the type of failure can be found in the following slides
- Changes between rounds
 - NFC/BLE: 76.60% → 78.72% success rate
 - NFC/NFC: 20% → 20% success rate
 - NFC/Wifi-Aware: NA (not tested)
 - QR/BLE: 76.28% → 78.44% success rate
 - QR/NFC: 0% → 0% success rate
 - QR/Wifi-Aware: 50% → 50% success rate

Worst round

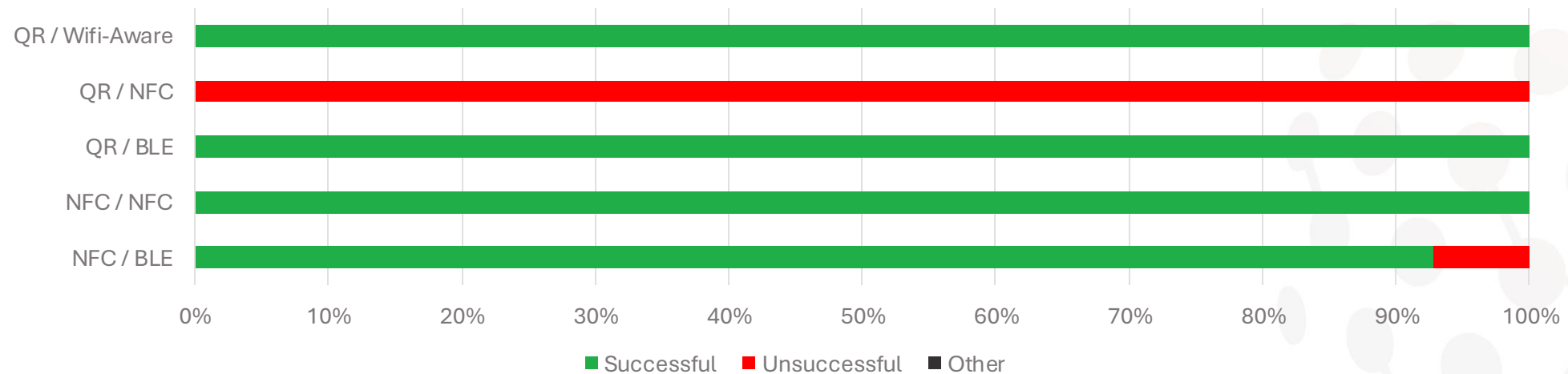


Best round



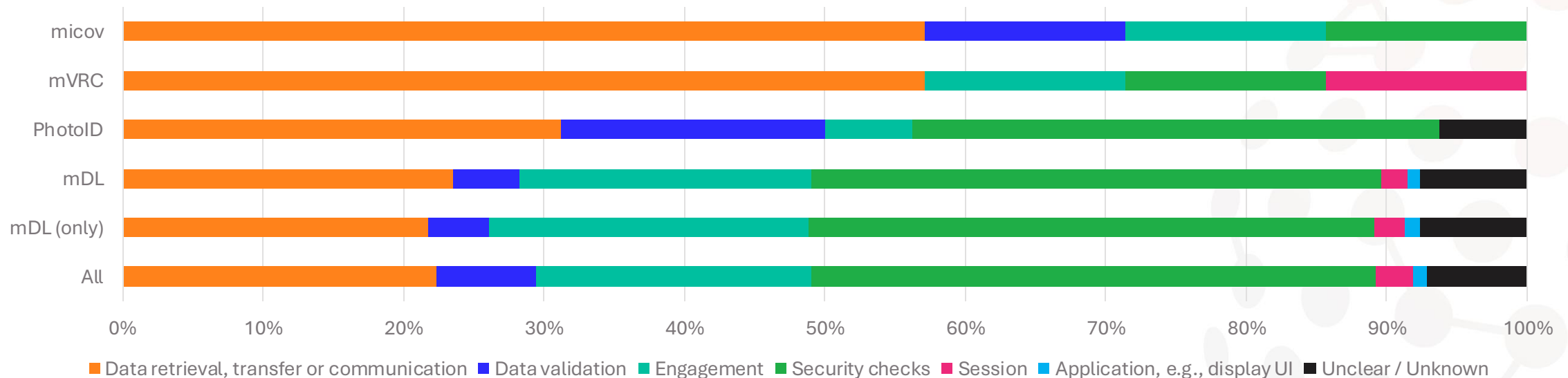
Number of Transactions by Success Rate and Configuration (top-10-10)

- Displays the percentage of Attended Device Retrieval transactions per configuration by success rate across all credential types
- Includes best rounds of the **top-10-10** excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- Best rounds
 - NFC/BLE: 92.68% success rate
 - NFC/NFC: 100% success rate
 - NFC/Wifi-Aware: NA (not tested)
 - QR/BLE: 100% success rate
 - QR/NFC: 0% success rate
 - QR/Wifi-Aware: 100% success rate
- Overall success rates are very high except for QR/NFC where only a very low number of transactions was recorded.



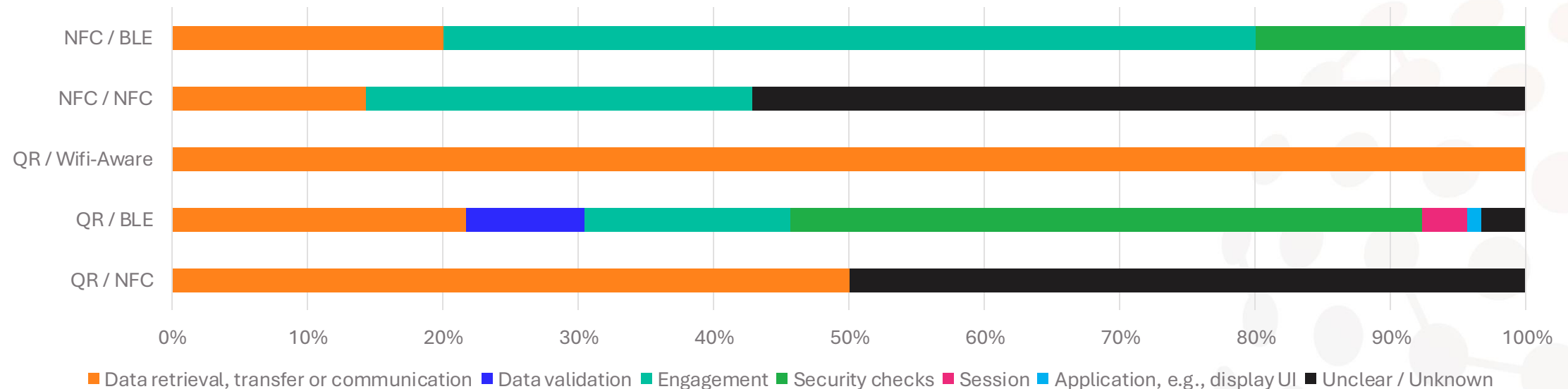
Number of Transactions by Failure Phase

- Displays the percentage of failures per phase of Attended Device Retrieval transactions per credential type
- Includes all configurations and all rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- Most failures occurred during security checks (40.18%), followed by data retrieval (22.32%), engagement (19.64%), data validation (7.14%), unknown/unclear reasons (7.14%), session issues (2.68%), and application errors (0.89%)
- mDL only experienced fewer failures during data validation (4.35%) due to the maturity of its data model; mVRC appears to be an outlier, possibly because it was used less frequently in transactions



Number of Transactions by Failure Phase and Configuration

- Displays the percentage of failures per phase of Attended Device Retrieval transactions per configuration for all credential types
- Includes all rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- Most failures in QR/BLE transactions occurred in security checks (46.74%), followed by data retrieval (21.74%), engagement (15.22%), data validation (8.70%), session issues (3.26%), unclear/unknown reasons (3.26%), and application errors (1.09%)
- Most failures in NFC/BLE transactions occurred in engagement (60%), followed by data retrieval (20%), and security checks (20%)



Observations

- QR/BLE was used in 85.88% of all transactions and was by far the most commonly used configuration, followed by NFC/BLE with 10.88%, NFC/NFC with 2.31%, QR/Wifi-Aware and QR/NFC with 0.46% each.
- NFC/Wifi-Aware was not used in any transaction.
- BLE mode details
 - 70.32% used BLE central mode
 - 28.34% used BLE peripheral server mode
 - 1.34% used BLE L2CAP
- NFC mode details
 - 50.88% used NFC negotiated handover
 - 49.12% used NFC static handover
- BLE was consistently the best performing data retrieval method with a success rate of 78.72% (NFC/BLE) and 78.44% (QR/BLE) across all implementers demonstrating its maturity given that new implementers also participated in the event. Note that success/failure rates include failures across all phases of an Attended Device Retrieval transaction, including those not related to data retrieval and engagement, e.g., security checks, data validation, etc.
- Among the top-10-10, the success rates improved (95-100%) drastically, showing there are mature implementations that achieve great interoperability.
- Some NFC/BLE and QR/BLE implementations were improved between rounds.
- Most failures in QR/BLE occurred during security checks, specifically related to document signer certificate (DSC) validation, such as issues with validity periods, extensions or additional fields, and mismatched fields between the DSC and mdoc (e.g., `StateOrProvince`). Other failures included reader certificate/authentication errors and MSO validation. It's important to note that these failures are unrelated to the transmission technology itself. Since QR/BLE is most commonly used as the default configuration, failures are often detected first in this configuration. Consequently, specific tests targeting other features may have also been attributed to QR/BLE, and failures related to these specific tests are surfaced through this configuration as well.
- For NFC/BLE, the engagement phase had the highest number of failures, followed by security checks with similar issues as noted for QR/BLE.
- Wifi-Aware and NFC as a data retrieval method was only sparsely tested which may indicate it is less supported or less used by readers and holders.

Observations

- None of the unsuccessful transactions using the VICAL indicated a failure directly related to the VICAL, and the success ratio of transactions using VICAL is not statistically disproportional to the success rate of transactions not using VICAL.
- In the lead-up to the event, several issues were identified with mVRC and photoID and were reported to the respective ISO Working Groups.
- During the test event, no specification issues were reported, including those related to the newly provisioned features. However, it was suggested to extend issuer data authentication to include validation of the credential type declared in the VICAL. Additionally, guidance was recommended regarding the validity of VICALS in scenarios where a previous VICAL remains valid, but a new VICAL is issued that conflicts with the information in the previous one.
- Some newly provisioned features were not extensively tested, with only a small number of transactions recorded for features such as the new BLE L2CAP and the new request structure. Since the draft specification of ISO/IEC 18013-5 Amendment 1 was distributed only a few weeks before the event, this likely contributed to the limited testing. Further testing is recommended. More details can be found later in this presentation in the slides dedicated to the newly provisioned features transactions.
- MSO revocation had good test coverage, with the identifier list being used more than twice as often as the status list, but both showed a similar success rate and effective validation rate.

Attended Server Retrieval Transactions



Australia

MATR

MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

Observations

- No significant number of Attended Server Retrieval were recorded, so there is no leaderboard.
- A total of 5 transactions were recorded for all configurations and best rounds whereas :
 - WebAPI (token in engagement): 1 (success)
 - WebAPI (token in device request): 2 (success), 1 (fail)
 - Failure occurred due during data retrieval where OIDC was requested instead of WebAPI
 - OIDC (token in engagement): 1 (success) where user authentication was performed on the mdoc device, and the Server Retrieval Token was used as an id_token_hint in OIDC.
- 4 reader and 4 holder implementations tested Attended Server Retrieval

Online or Unattended (Remote) Transactions



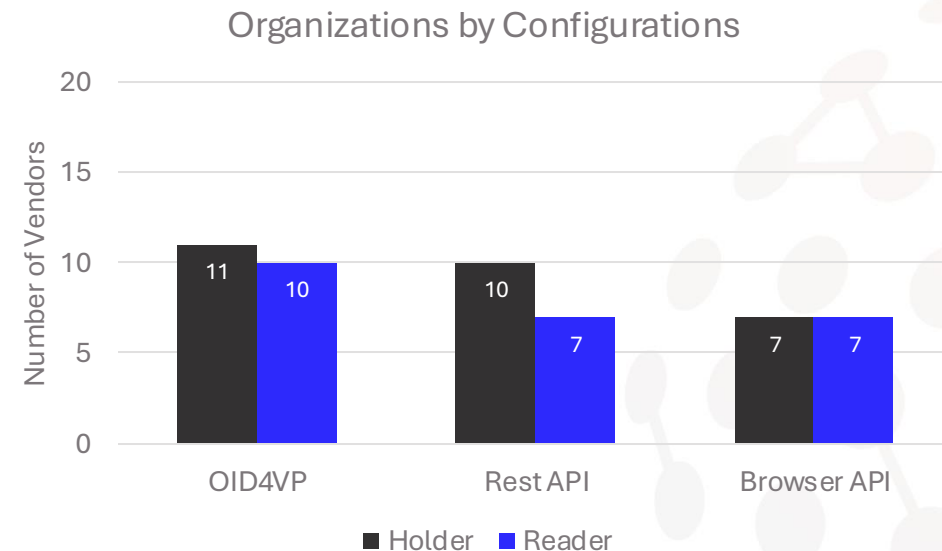
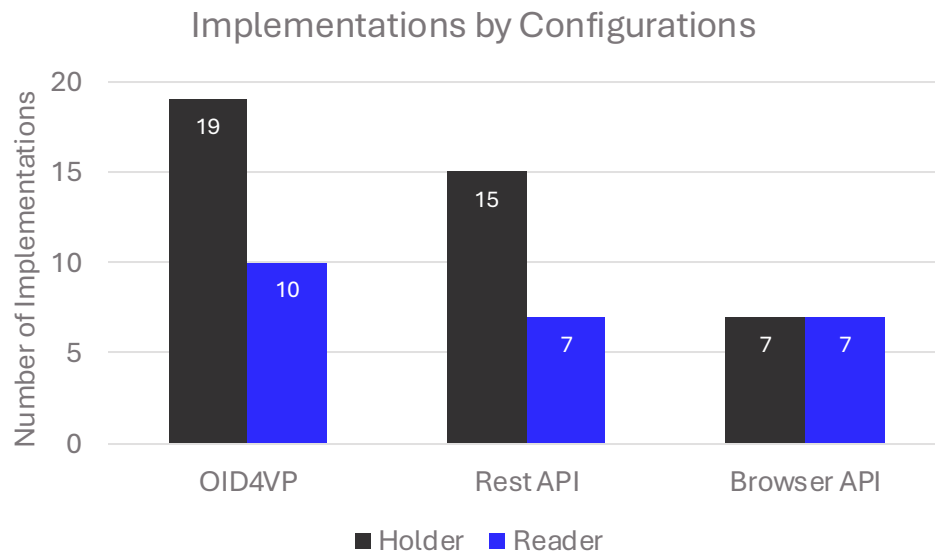
Austrade

MATR

MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

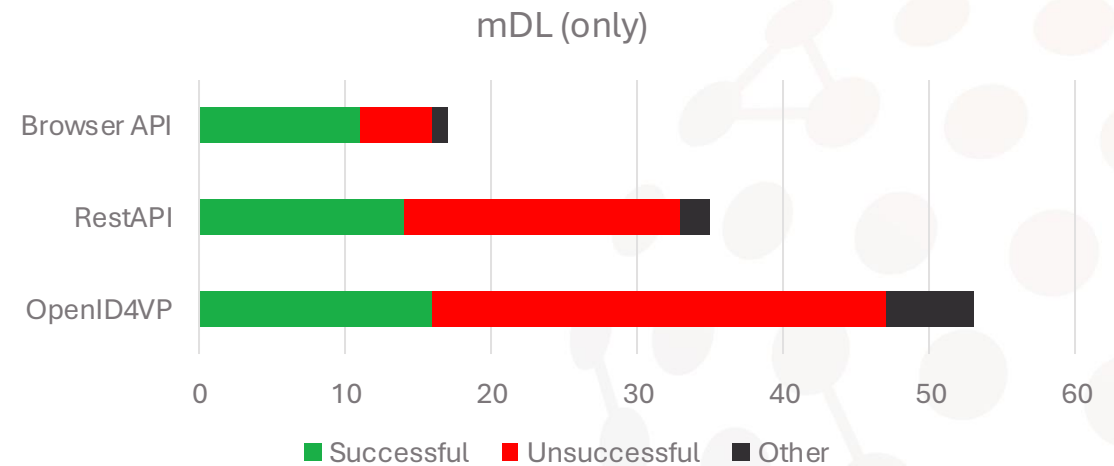
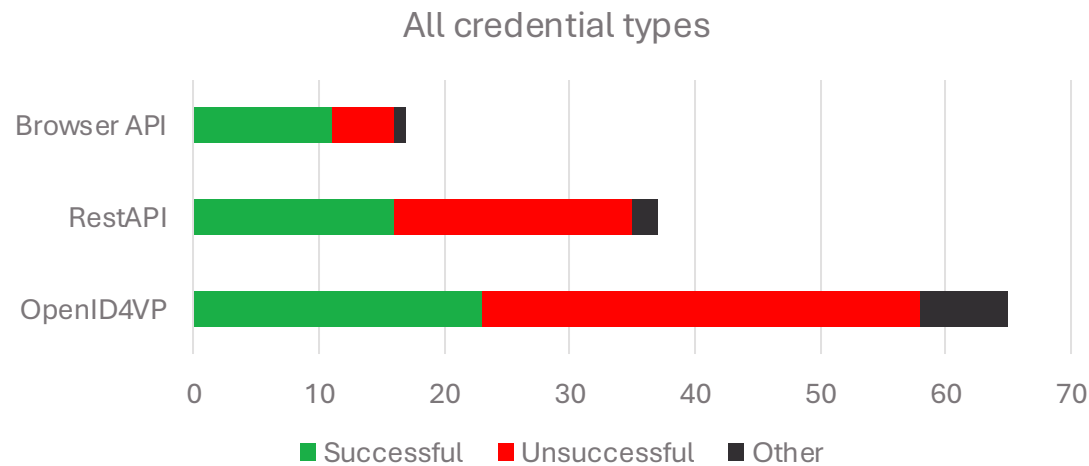
Number of Implementations by Configuration

- Displays the number of implementations and organizations that submitted test results of Online Retrieval transactions by configuration
- Numbers may differ from the received conformance statements, for example, if certain transactions were not reported or if some participants expanded the scope of their implementations at the last minute.



Number of Transactions by Success Rate and Configuration¹⁾

- Displays the total number of Online Retrieval transactions per configuration by success rate across all credential types and for mDL (only)
- Includes best rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- For all credential types
 - **OID4VP: 65 (total), 23 (success), 35 (fail), 7 (other)**
 - **RestAPI: 37 (total), 16 (success), 19 (fail), 2 (other)**
 - **Browser API: 17 (total), 11 (success), 5 (fail), 1 (other)**

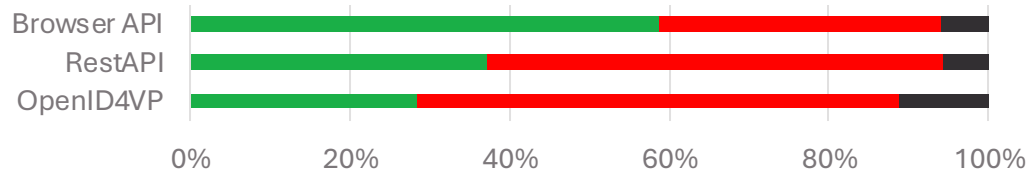


¹⁾ Caution is advised when interpreting the number of succeeded/failed transactions, as participants were found to underreport transactions for certain protocols relative to the number of implementations and recorded transactions.

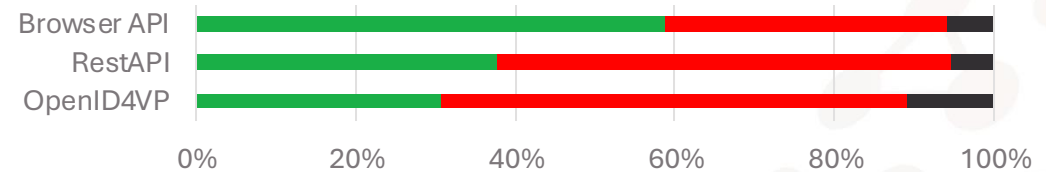
Number of Transactions by Success Rate and Configuration¹⁾

- Displays the percentage of Online Retrieval transactions per configuration by success rate across all credential types and for mDL only
- Distinct charts for best rounds and worst rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- Change between worst and best rounds across all credential types
 - OID4VP: 30.77% / 58.46% → 35.38% / 53.85% (success/fail rate)
 - Rest API: 37.84% / 56.76% → 43.24% / 51.35% (success/fail rate)
 - Browser API: 58.82% / 35.29% → 64.71% / 29.41% (success/fail rate)
- Some implementations across all configurations were improved between rounds which increased the overall success rate

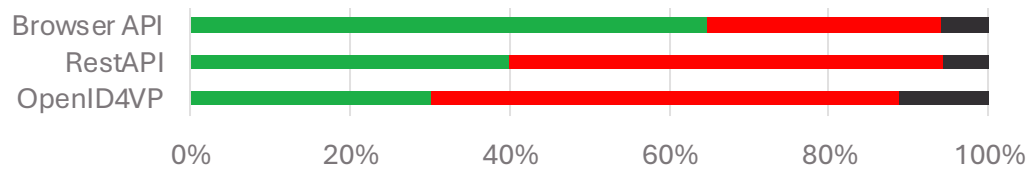
mDL (only) / worst round



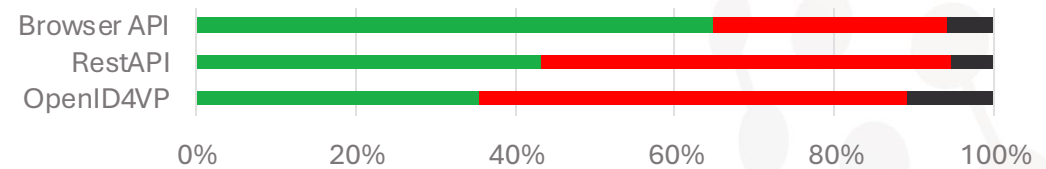
All credential types / worst round



mDL (only) / best round



All credential types / best round



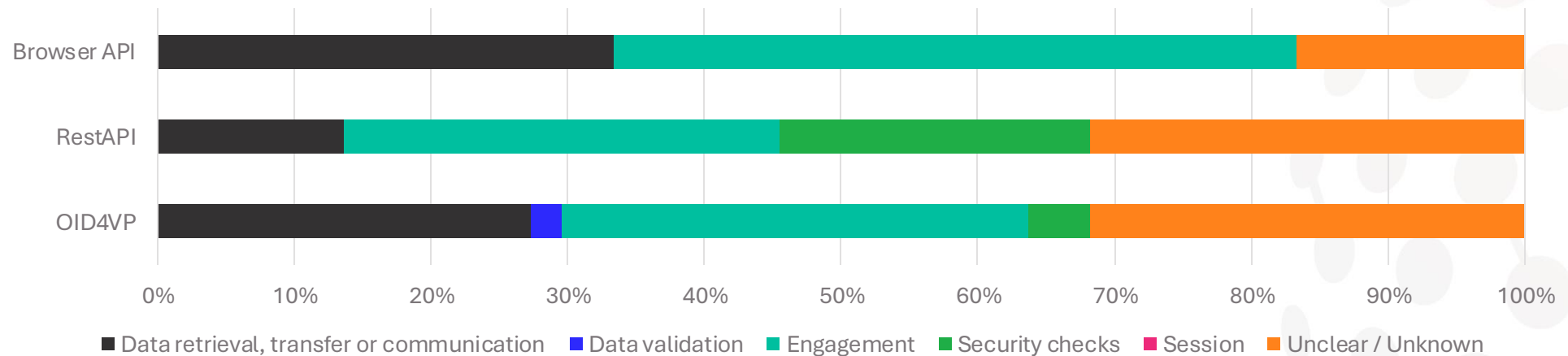
■ Successful ■ Unsuccessful ■ Other

■ Successful ■ Unsuccessful ■ Other

¹⁾ Caution is advised when interpreting the success/failure rates, as participants were found to underreport transactions for certain protocols relative to the number of implementations and recorded transactions.

Number of Transactions by Failure Phase and Configuration

- Displays the percentage of failures per phase of Online Retrieval transactions per configuration for all credential types
- Includes all rounds excluding transactions resulting from ISO/IEC 18013-5 Amendment 1 features failures
- Most failures in OID4VP transactions occurred in engagement (34.09%), followed by data retrieval (27.27%), unclear/unknown reasons (31.82%), data validation (2.27%), and security checks (4.55%)
- Most failures in Rest API transactions occurred in engagement (31.82%), and unclear/unknown reasons (31.82%), followed by security checks (22.73%), and data retrieval (13.64%)
- Most failures in Browser API occurred in engagement (50.00%), data retrieval (33.33%) and for unclear/unknown reasons (16.67%)



Observations

- Optional credential types were generally less tested in Online Retrieval, which is why dedicated charts per credential type (except for mDL) were not generated.
- Some Online Retrieval implementers improved their implementations across all configurations (i.e., Rest API, OID4VP, Browser API) between rounds, as evidenced by increased success rates in subsequent rounds.
- Caution is advised when interpreting the number of transactions, implementations, and success/failure rates, as participants were found to underreport transactions for certain protocols relative to the number of implementations and recorded transactions.
- Initial results still had room for improvement, but participants used the opportunity to collaborate, fix their implementations, and retest. This led to underreporting of transactions but, on the positive side, resulted in an increased success rate during the event. Within just two days, significant improvements were made to implementations, resulting in six additional interoperable implementations, which is a notable achievement. Additionally, this prompted participants to actively engage with the specifications, and no specification-related issues were reported with them.

Observations

OID4VP

- There was a discrepancy between initial conformance statements and actual test results. 4 additional holder and 1 additional reader implementations recorded OID4VP transactions.
- Engagement phase caused the most issues for OID4VP, including:
 - Custom URIs failing to invoke the app or using incorrect URI schemes.
 - ECDH-ES parameter missing in encryption key algorithms.
 - Holder app unable to fetch the request URI.
 - Reader certificate issues.
- No specification-related issues were reported.

Rest API

- Rest API showed a similar success and failure rate to OID4VP but had fewer implementations and recorded transactions.
- It also shows some discrepancy between received conformance statements and reported transactions by having one less reader implementation that submitted test results.
- Engagement phase issues were the most common, such as:
 - Custom URIs not invoking the app or using incorrect URI schemes, resulting in no engagement.
 - Decryption issues.
 - Referrer URL mismatches.
 - Reader certificate issues.
- No specification-related issues were reported.

Observations

Browser API

- Due to the smaller data sample, conclusions should be drawn cautiously.
 - One fewer reader implementation submitted test results than was listed in the conformance statement.
 - Browser API achieved a success rate of 64.71%, which is promising given the relative newness of the specification.
- Engagement phase was the primary cause of failures for Browser API as well, including:
 - Wallet selection or invocation issues.
 - Parsing errors.
 - No specification-related issues were reported.

Observations

- A common issue across protocols was the engagement phase. For RestAPI and OID4VP, custom URI schemes and reader certificates were recurring challenges, while for the Browser API, wallet invocation issues were also reported.

Newly Provisioned Features Transactions across all Scenarios



Australia

MATR

MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

Newly Provisioned Features Transactions

MSO Revocation

- A total of 85 transactions were recorded, with 70 distinct combinations of holders/readers using MSO revocation. However, in most cases, the MSO revocation status was not validated by the reader, suggesting that while the MSO had a revocation status, readers either ignored it, did not implement it, or omitted documentation of the MSO revocation validation.
- During the test event, implementers chose to support both methods; however, in real-world scenarios, it is expected that issuers will decide on the revocation method that best fits their requirements.

Newly Provisioned Features Transactions

MSO Revocation

- Identifier List
 - Used in 84 total transactions across 67 distinct holder/reader combinations.
 - 51 transactions (60.71%) passed, 28 (33.33%) failed, and 4 (4.76%) were inconclusive.
 - 43 (64.18%) of the distinct holder/reader combinations passed transactions that included the identifier list; of these, 17 (25.37%) indicated validation of the identifier list.
 - Reported issues
 - Implementation of different drafts
 - Unexpected certificates

- Status List
 - Used in 22 total transactions across 15 distinct holder/reader combinations.
 - 12 transactions (54.55%) passed, 8 (36.36%) failed, and 1 (4.55%) was inconclusive.
 - 9 (60%) of the distinct holder/reader combinations passed transactions that included the status list; of these, 5 (33.33%) indicated validation of the status list.
 - Reported issues
 - Implementation of different drafts
 - Encoding issues, such as the status_list key

Newly Provisioned Features Transactions

- New BLE L2CAP
 - A total of 3 transactions were reported across distinct holder/reader combinations. Of these, 1 transaction was successful, and 2 failed.
 - New request structure
 - Issuer selection: 5 transactions were reported between distinct holder/reader combinations, with 4 successes and 1 inconclusive result. No data validation failures were reported.
 - Conditional and alternative data elements: 6 distinct transactions were reported, with 5 successes and 1 inconclusive result. No data validation failures were observed.
- It was noted that none of the transactions actively tested the specific new features of the request structure. Instead, forward compatibility with 1.0 implementations was observed, as these implementations successfully ignored the new elements of the request structure.

Lessons Learned



Austrroads

MATR

MATR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT

Lessons Learned

Rotations:

- On days 1-2, the prepared regime with assigned test focuses and specific combinations of mdoc readers and mdoc apps was followed well. However, on the afternoon of day 2 and throughout day 3, participants began deviating to test all combinations or conduct regression testing out of personal interest.

Organization:

- For those with limited conformance to the wider testing group implementations, a different way to involve them in the event is needed to make use of their time. Alternatively, being able to communicate with them up-front that their involvement may be limited to a smaller segment of the wider event would help them avoid excessive downtime.

Test capture form:

- An online form was generally preferred over the spreadsheet used in previous events.
- The online form was too lengthy.
- It would be beneficial to fill out the form only once per mdoc holder/reader combination and use a checklist approach while still allowing for the recording of individual transactions and failures per transaction and feature.
- As the specifications mature and more new implementers join, not all participants are fully familiar with the details of their own implementations or the third-party products they use. Consequently, more detailed questions were made optional, making it harder to categorize failures, understand which security and data checks were performed, and compare results across individual rounds. While it's encouraging to see increased participation in testing events, capturing granular test results will become increasingly challenging as the number of participants grows.

Certificate validation/distribution:

- During validation of the interop participant IACAs provided for the VICAL used in the event, a significant variance in conformance to the IACA standard was observed. Many certificates required multiple round trips to reduce errors enough for them to be deemed suitable.



MATTR

Thank you!



MATTR

MATTR PUBLIC – 10TH INTERNATIONAL INTEROPERABILITY TEST EVENT