12th International Interoperability Test Event

Testing implementations of ISO/IEC 18013-5 and -7

16, 17 & 18 November 2025, Wellington, New Zealand

Version 1.0 – 26 September 2025

Hosted by

NZ TRANSPORT AGENCY WAKA KOTAHI

Te Tari Taiwhenua Internal Affairs

Endorsed by

AAMVA

Austroads

EReg ASSOCIATION OF EUROPEAN VEHICLE AND DRIVER REGISTRATION AUTHORITIES

1 Introduction

ISO/IEC 18013-5:2021 standardizes requirements for mobile driving licenses (mDL) and generic mobile document (mdoc) protocols. The implementation of the standard by Issuing Authorities, Verifiers and their suppliers in various mdoc solutions should result in a secure and interoperable mdoc ecosystem. Where ISO/IEC 18013 part 5 includes protocols for in-person presentation and verification of mdocs, ISO/IEC 18013-7 adds protocols for over-the-internet presentation of mdocs, leveraging the data structures, request-response messages and selective disclosure approach standardised in part 5.

Task Force 14 on mDL within ISO/IEC JTC1/SC17/WG10 has worked towards standardisation of mDL/ mdoc since 2014. Members of Task Force 14 have taken an unconventional approach to assure a high-quality standard: in addition to joint work on the standard, and international review and balloting rounds, a number of "Prototype Interoperability Parties" have been organized. These test events contribute to:

- Confirming the feasibility to implement the standard, leading to interoperable implementations;
- Detailed feedback, disambiguation, clarification and increased quality of the standard;
- Keeping momentum in the market and accelerating the time to market for mDL implementations.

Important milestones so far have been:

- 2014: creation of ISO/IEC JTC1/SC17/WG10/ Task Force 14 on mobile driving licence;
- 2017: formal New Work Item Proposal acceptance and launch of the standardization project;
- April 2018: 1st Committee Draft (CD) of ISO/IEC 18013-5 for international ballot/commenting;
- October 2018: first mDL interoperability party in Okayama, Japan, based on the 1st CD draft;
- December 2018: Austroads, AAMVA and EReg endorse the international standardization of mDL at their Global Summit in Melbourne, Australia;
- March 2019: 2nd CD draft for ballot, incorporating the learnings from the first test event;
- August 2019: America's first mDL test event at the AAMVA AIC, based on the 2nd CD draft.
- November 2019: Australia's first mDL test event in Brisbane, Australia, based on the proposed text for the Draft International Standard (DIS);
- April 2020: approval of the DIS version of ISO/IEC 18013-5;
- August 2021: approval of the Final Draft International Standard version ISO/IEC 18013-5;
- September 2021: publication of the final International Standard ISO/IEC 18013-5:2021
- October 2021: European test event in Rotterdam, The Netherlands;
- November 2021: American test event in Houston, TX, USA;
- May 2022: 6th International test event in Louisville, KY, USA;
- December 2022: 7th International test event in Brisbane, QLD, AU;
- Summer 2023: first online-only event for testing ISO/IEC TS 18013-7;
- December 2023: 9th in-person international test event in Paris, FR;
- October 2024: 10th in-person international test event in Sydney, NSW, AU.
- February/March 2025: 11th in-person international test event in Utrecht, the Netherlands.

The 12th international interoperability test event is planned for 16, 17 and 18 November 2025 in Wellington, New Zealand.

This document provides further details on the upcoming interoperability test event. This includes details on the venue, the terms and conditions for participation, test process and registration process.
The main objectives of the event are testing interoperability of standardised functions between implementations of different solution providers and jurisdictions, keeping momentum in the industry, generating input for further standardisation, and to reach out to the European market. Following up on the test event in Sydney, the 11th interoperability test event will involve the use of Verified Issuer Certification Authority Lists (VICALs).

2 Organization

Organiser & Host:	NZ Transport Authority Waka Kotahi (NZTA) & Department of Internal Affairs (of the government of New Zealand)
Coordinator:	Remco Schaar (in collaboration with Arjan Geluk and Oliver Terbu)
Contact:	mdoctestevent@fime.com
Date:	Sunday 16 till Tuesday 18 November 2025
Location:	NZTA office, ground floor, 44 Bowen Street
	Thorndon, Wellington, New Zealand
Co-located activities:	111th meeting of ISO/IEC JTC1/SC17/WG10 on driving licenses, 18-20 November 2025
	136th meeting of ISO/IEC JTC1/SC17/WG4 on mobile documents, 21 November 2025

3 Eligibility

Eligible for participation in the interoperability test event are organisations who bring an mdoc and/or mdoc reader implementation which implement at least the data structures, transport protocols and verification mechanisms standardized in ISO/IEC 18013-5:2021 and/or ISO/IEC TS 18013-7:2025. However, the primary focus of the event will be on qualitative testing of the new features added in the draft 2nd edition of ISO/IEC 18013-5 (updated request structure, revocation methods, RICAL) and draft 3rd edition of ISO/IEC 18013-7 and proposed items therefore (including annex D).

Reader implementations should be able to rely on a test VICAL conforming to ISO/IEC 18013-5:2021 Annex C for authenticating the issuer of mdocs. Implementations of an mdoc supporting reader authentication are encouraged to leverage a test RICAL confirming to draft ISO/IEC 18013-5 second edition, annex F.

Interested parties do not need to be ISO members or affiliated with any other group or organization to register for the interoperability test event.

The event will be open to selected observers, at the discretion of the organizer and coordinator. Requests to attend the test event as observer may be directed to the coordinator. Conditions for attending as observer may apply.

Due to capacity limitation at the venue, the organization reserves the right to ask participating organizations to limit their number of participants. Note that one participant per implementation is expected to participate.

Refer to Chapter 5, Test scope, for detailed requirements on specific implementations, and Chapter 6, Test Process, for procedural and communication requirements for participants.

Note: if any participant needs a visa to visit New Zealand, the host or coordinator may be able to assist. Please contact them for support. Such request can be indicated during the registration as well.

4 Schedule and dates

Note: all dates and times below are tentative and may be subject to change.

- 2025/10/07: Online introductory webinars (13:00 UTC, 23:00 UTC; note the latter is October 8th for the APAC region)
- 2025/10/24: Registration deadline (23:59:59 UTC)
- 2025/10/31: IACA and reader CA certificates submitted
- 2025/10/31: Remote readers are requested to have public endpoints available and submitted for testing
- 2025/11/03: mdocs supporting 18013-7 can start testing against Reader endpoints.
- 2025/11/13: Final confirmation of supported features, for test scheduling
- 2025/11/16: Interoperability test event (full day)
- 2025/11/17: Interoperability test event (full day)
- 2025/11/17: *[TBC]* Showcase and drinks (end of afternoon / evening)
- 2025/11/18: Interoperability test event evaluation with and feedback to WG10 (morning)
- TBC: Publish general presentation with high-level test results

5 Test scope

5.1 Overview

The interoperability testing is based on ISO/IEC 18013-5:2021 for in-person (proximity) transactions and on ISO/IEC TS 18013-7:2025 for remote transaction, both with the mDL, a Photo ID and other credential types. Participants can bring implementations of other mdocs, e.g. an EU PID, a vehicle registration certificate and/or a health certificate.
All mdocs should be authenticated using the test VICAL (Verified Issuer CA List) which will be provided before, and updated during, the event. mdoc readers can be authenticated using the test RICAL (Reader Identity CA List), which will likewise be provider before, and updated during, the event.

During the first two days of the test event (16 & 17 November), all participants can perform cross-over interoperability testing. The coordinator will prepare a schedule for pairing peers for testing with matching features. Combinations of peers can together test interoperability of their implementations and are requested to report on test execution and possible findings.

Furthermore, the test event will facilitate interested parties to have a “hackathon”. In these mini-hackathon(s), participants can collaboratively do explorative testing on topics of interest. See section 5.4 for more information.

During the 3rd day of the test event (18 November), the participants and WG10 together will evaluate the findings of the test event. This will provide the opportunity for implementors and members of the work group to discuss the standards and share feedback.

During the test event, the focus will be on qualitative assessment of provisions of the standard implemented by the participants (implementation feedback for the participants), as well as

qualitative assessment of the standard itself, especially the new provisions in the draft 2nd editions of ISO/IEC 18013-5 and ISO/IEC 18013-7 (developer feedback to be provided to the ISO work group, who will meet the days following the test event).

5.2 Base documents

The following is a list of base documents used for the test event.

5.2.1 Protocol and technical specifications

The following specifications are in scope for protocols and technical specifications for the test event.

- ISO mdoc (mDL) in-person presentation
    - As defined in ISO/IEC 18013-5:2021;
- ISO mdoc (mDL) remote presentation
    - as defined in ISO/IEC TS 18013-7:2025;
- New mdoc (mDL) features
    - As defined in the draft text for DTS ballot for the 2nd edition of ISO/IEC 18013-5 (available in ISO Global Directory, WG10/N2718).
        - Additional information to describe the requested information
        - mDL revocation (status list / identifier list)
        - Zero Knowledge Proof support[1]
        - Support sending the request during NFC handover
        - BLE L2CAP mode improvements
        - RICAL support
        - third party recipient encryption feature (f.k.a. WG10/N2672)
    - A copy of the draft specification will be provided by the coordinator upon request.
- mdoc specific features
    - As defined in "ISO-IEC DTS 23220-4 - Proposed updated text for second DTS" (available in ISO Global Directory, WG4/N4770).
        - Reverse QR engagement
    - A copy of the draft specification will be provided by the coordinator upon request.
- The Browser API
    - The Browser API is defined in W3C WICG as the Digital Credentials API and the specification can be access from https://www.w3.org/TR/digital-credentials/[2].
    - The following two profiles for Browser API can be tested:

[1] Note: ZKP support in the draft of 18013-5 second edition does not specify specific ZKP schemes. Full interoperability testing depends on a ZKP scheme. Therefore, ZKP testing is a topic for the hackathon part of the event.

[2] At the time of writing, the latest draft is the working draft of 23 September 2025, which can be found on https://www.w3.org/TR/2025/WD-digital-credentials-20250923/. Changes may happen, as the Browser API is under development, and supporting browsers may follow updates if applicable.

        - ISO/IEC 18013-7:2025 Annex C: According to the profile defined in ISO/IEC TS 18013-7:2025;
        - OIDF HAIP (candidate Annex D of future ISO/IEC 18013-7 revisions): According to the profile defined in the OpenID4VC High Assurance Interoperability Profile (HAIP) and can be accessed from https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0-04.html (draft 04). This references version 1.0 of OpenID4VP which can be accessed from here https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.

- Using OID4VP 1.0 with the HAIP profile, without Browser URI

    - Work is ongoing on a proposal for 18013-7 to use OID4VP 1.0 for remote presentation of an mdoc, without using the Browser API but URI-scheme engagement instead.
    - For engagement, the haip-vp:// URI scheme should be used, see section 5.1 of https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0-04.html (draft 04) of the HAIP profile.
    - More information may follow in an update to this document.

5.2.2 Document specifications

The following specifications are in scope for document format specifications for the test event.

- Driver License (mDL)

    - As defined in section 7 of " ISO-IEC 18013-5:2021 - Mobile driving licence (mDL) application" (available through regular ISO channels), and section 13 of draft “ISO/IEC 18013-5 - Mobile driving licence (mDL) application” second edition (available in ISO Global Directory, WG10/N2718).

    - A copy of the draft specification (2nd edition) will be provided by the coordinator upon request.

- Photo ID

    - As defined in annex C.2.1 of "ISO-IEC DTS 23220-4 - Proposed updated text for second DTS" (available in ISO Global Directory, WG4/N4770);

    - Doctype, namespaces and data elements are listed in Annex A for convenience.

    - A copy of the draft specification will be provided by the coordinator upon request.

- Mobile international certificate of vaccination (micov)

    - As defined in "Guidelines for developing an ISO-compliant mdoc for eHealth" RC3.1 (available in ISO Global Directory, WG10/N2477);

    - Doctype, namespaces and data elements are listed in Annex B for convenience.

    - A copy of the specification will be provided by the coordinator upon request.

- Mobile vehicle registration certificate (mVC)
    - As defined in ISO/IEC 7367 PDTS (available in ISO Global Directory, SC17/N7603);
    - Doctype, namespaces and data elements are listed in Annex C for convenience.
    - A copy of the draft specification will be provided by the coordinator upon request.
- EU PID
    - As defined in "Commission Implementing Regulation (EU) 2024/2977" (available on https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402977) and the PID Rulebook in the EUDI Wallet Architecture Reference Framework v2.4.0 (available on https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.4.0/annexes/annex-3/annex-3.01-pid-rulebook/#3-isoiec-18013-5-compliant-encoding-of-pid);

5.2.3 Examples

The coordinator will provide examples of a document for the following mdoc document types:

- mVC
- PhotoID
- micov
- EU PID

These may be used as documents during the test event. The examples will include the details and device keys needed for using them.

5.3 Tested features

5.3.1 Credential types

The mDL credential type as defined in ISO/IEC 18013-5 shall be supported with the following data sets at minimum:

- License and holder data. The mandatory data elements are defined in Table 5 of ISO/IEC 18013-5.
- Age verification (age over 18)

Implementations should support the Photo ID and may support micov, mVC and EU PID. Note that Photo ID requires a portrait and age over 18, like mDL. Support for multiple document types is a pre-requisite for testing all new request structure features of draft 18013-5 second edition.

See Section 5.2 for a list of base documents defining these credential types.

5.3.2 ISO/IEC 18013-5 features to be tested (in-person transactions)

Participants shall bring at least one implementation (mdoc app or mdoc reader) supporting at least one device engagement and one device retrieval option from ISO/IEC 18013-5:2021. This includes security and data checks.

Other device engagement and data transfer mechanisms (device and server retrieval) may be implemented as defined in ISO/IEC 18013-5. The optional mdoc reader authentication (device retrieval) and TLS client authentication (server retrieval) may be implemented and can be tested at the event as well. Note that server retrieval will no longer be part of ISO/IEC 18031-5 in the second edition, as it will be moved into a separate specification.

Additionally, mdoc readers should support VICAL to authenticate IACA certificates of mdocs provided by mdoc applications. During the test event participants can expect the VICAL to be updated between days for certain test scenarios. For this reason, mdoc readers and mdoc remote readers are encouraged to have the ability to update their VICAL dynamically during the test event.

Multiple mdocs per request may be tested as well. Note that this is even a conceptual pre-requisite for testing some of the capabilities in the new request structure feature of (draft) 18013-5 2nd edition, see section 5.3.4.

Table 1 provides an overview of all features that may be tested from ISO/IEC 18013-5:2021.

ISO/IEC 18013-5 features			
Device engagement		QR	QR code
			QR code with WebAPI token
			QR code with OIDC token
		NFC	NFC static handover
			NFC negotiated handover
			NFC with WebAPI token
			NFC with OIDC token
Data transfer	Device retrieval	NFC	
		BLE	BLE mdoc central client mode
			• Without BLE L2CAP profile • With BLE L2CAP profile
			BLE mdoc peripheral server mode
			• Without BLE L2CAP profile • With BLE L2CAP profile
		Wi-Fi Aware	
	Device / server retrieval	Token transfer using device retrieval	
	Server retrieval	WebAPI	
		OIDC	
Security	Device retrieval	Issuer data authentication	
		mdoc authentication	
		Session encryption	
		mdoc reader authentication	
		VICAL processing to authenticate the IACA certificate	
	Server retrieval	JSON Web Token	
		TLS server authentication	
		TLS client authentication	
		VICAL processing to authenticate the IACA certificate	

Data	Device / server retrieval	License and holder data
		Portrait image
		Age verification (age_over_18)
Multiple mdocs		Globally interoperable ISO-compliant mobile Driving License (mDL)
		Photo ID (+ optional DTC)
		Mobile International Certificate of Vaccination (micov)
		Mobile Vehicle Registration Certificate (mVC)
		EU Person Identification Data (PID)

Table 1: ISO/IEC 18013-5 features to be tested (grey is low priority)

5.3.3 ISO/IEC 18013-7 features to be tested (remote transactions)

Participants may test mdoc app and mdoc reader implementations of ISO/IEC 18013-5 that are augmented with add-on functions defined in ISO/IEC 18013-7. The test scope covers engagement for unattended transactions, as well as data retrieval.

Regarding engagement for unattended transactions, the flow of reader engagement, establishment of a communication channel, followed by device engagement may be tested.

For data retrieval, the device retrieval can be tested over RestAPI (ISO/IEC TS 18013-7 Annex A), OpenID4VP (ISO/IEC TS 18013-7 Annex B), or Device Retrieval to a website over an API (ISO/IEC TS 18013-7:2025 Annex C).

Whether server retrieval in combination with ISO/IEC TS 18013-7 is within the scope of the test event depends on the number of parties that declared support in their conformance statement and the time available in the test event schedule.

Table 2 provides an overview of all features to be tested from ISO/IEC TS 18013-7.

ISO/IEC TS 18013-7:2025 features		
Engagement		Reader engagement transmitted using the mdoc:// scheme, communication channel establishment, device engagement (only for device retrieval to a website).
		Reader engagement transmitted using the mdl-openid4vp:// scheme (only for OpenID4VP).
		Reader engagement transmitted using the W3C Digital Credential API (digital credential api retrieval).
Data transfer	Device retrieval	RestAPI (device-retrieval-to-a-website).
		OpenID4VP
		Digital Credential API retrieval.

Table 2: ISO/IEC TS 18013-7 features to be tested

5.3.4 Draft 2nd edition of ISO/IEC 18013-5 features to be tested

Participants should test implementations of ISO/IEC 18013-5 that implemented the new features defined in the draft 2nd edition of ISO/IEC 18013-5. **Table 3** provides an overview of all features that may be tested in the test event.

ISO/IEC 18013-5 draft 2nd edition features	
Revocation methods	Identifier list

		Status list
RICAL support		RICAL processing to authenticate the mdoc Reader
Security / privacy		ZKP framework
Data transfer	Device retrieval	New BLE L2CAP PSM profile
		Sending request during NFC handover
		New request structure

Table 3: Draft 2nd edition of ISO/IEC 18013-5 features to be tested

Participants supporting one of the revocation methods and providing an mdoc app implementation should prepare both revoked and non-revoked mdocs of the same credential type. Alternatively, participants could revoke documents overnight and test before and after revocation presentation.

Mdoc app implementations should support authentication Readers using the RICAL to validate certificates against CAs listed. During the test event participants can expect the RICAL to be updated between days for certain test scenarios. For this reason, mdoc app implementations are encouraged to have the ability to update their RICAL dynamically during the test event.

Based on the test scenario, they should allow the selection of which mdoc is included in the response to the mdoc reader or mdoc remote reader.

The following features of the new request structure should be tested:

- **Issuer selection based on issuer identifier:** mdoc reader or mdoc remote reader implementations should load the public keys from the IACA certificates for possible issuer selection in preparation for the test event.

  To maximise benefit from testing this functionality, reader providers are requested to make the issuer selection configurable. This enables performing both a positive test (i.e. a test in which the holder's mDL issuer is included) and a negative test (i.e. a test in which the holder's mDL issuer is excluded).

- **Alternative data elements:** mdoc reader or mdoc remote reader implementations should test this feature by asking the mdoc app to provide an mDL with either `age_in_years` and `portrait`, or `age_birth_year` and `portrait` or `age_over_18` and `portrait` as alternative data sets.

  To maximise benefit from testing this functionality, mdoc app providers are requested to be prepared to respond with different data in different transactions (e.g. by forcing selection by the user, or by varying mDL data sets issued with different combinations of data elements).

- **Use cases (age verification):** mdoc reader or mdoc remote reader implementations should test this feature by asking the mdoc app to provide

  - an mDL with `portrait` and `age_birth_year` OR
  - an EU PID with `portrait` and `birth_date` OR
  - a PhotoID with `portrait` and `age_over_18` OR

  To maximise benefit from testing this functionality, mdoc app providers are requested to be prepared to respond with different data in different transactions (e.g. by forcing selection by the user, or by varying mdoc data sets issued with different combinations of data elements).

- **Use cases (hypothetical "land border random check"):** mdoc reader or mdoc remote reader implementations should test this feature by asking the mdoc app to provide

    - an mDL with `portrait` and `driving_privileges` AND an mVC with `registration_number` OR

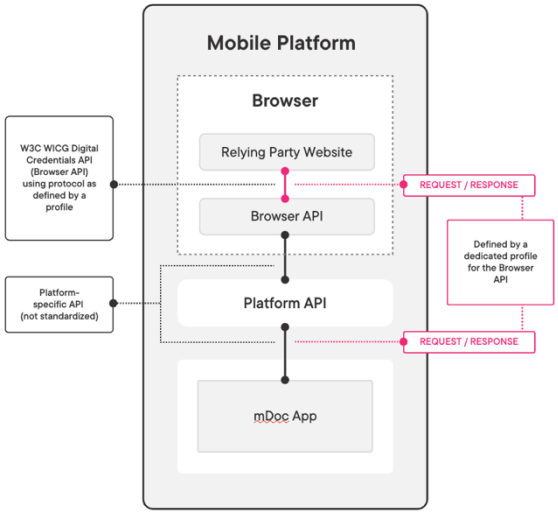
    - an EU PID with `given_name` AND a PhotoID with `dg1` from the "org.iso.23220.datagroups.1" namespace

  To maximise benefit from testing this functionality, mdoc app providers are requested to be prepared to respond with different data in different transactions (e.g. by forcing selection by the user, or by varying mdoc data sets).

5.3.5 Proposed 3rd edition of ISO/IEC 18013-7 features to be tested (Browser API)

5.3.5.1 Browser API (W3C WICG Digital Credential API)

This mechanism can be tested using the https://www.w3.org/TR/digital-credentials/ (referred to as Browser API) which defines a Web Platform API allowing web sites acting as mdoc readers using a Browser API (JavaScript) to send requests and receive responses from mdoc implementations. The API itself does not define an exchange protocol while acting as a pipe between the mdoc reader and the mdoc app supporting multiple protocols defined by profiles. The Web Platform (i.e. browser), working in conjunction with other layers, such as the app platform/operating system, and based on the permission of the end-user, will send the request data along with the web origin of the mdoc reader to the end-user's chosen mdoc implementation.



The Browser API offers several advantages for implementers of both mdoc remote readers and mdoc implementations.

- The Browser API serves as a privacy-preserving alternative to invoking mdoc apps via URLs, particularly custom URL schemes. The underlying app platform will only invoke a mdoc app if the user confirms the request based on contextual information about the request and the requestor (mdoc reader).

- The session with the user will always continue in the initial context, typically a browser tab, when the request has been fulfilled (or aborted), which results in an improved user experience.

- Cross-device requests benefit from the use of secure transports with proximity checks, which are handled by the OS platform, e.g., using FIDO CTAP 2.2 with hybrid transports.

- As part of the request, the mdoc app is provided with information about the mdoc reader's origin as authenticated by the user agent, which is important for phishing resistance.

5.3.5.2 Annex C of the 2nd edition of ISO/IEC 18013-7

The 2nd edition of ISO/IEC 18013-7 (ISO/IEC TS 18013-7:2025) defines a profile that works with the https://www.w3.org/TR/digital-credentials/. mdoc remote readers and mdoc app implementations may test the Browser API using the profile defined in the 2nd edition of ISO/IEC 18013-7 Annex C to test requests conforming to ISO/IEC 18013-5:2021 as well as in combination with features of the draft 2nd edition of ISO/IEC 18013-5.

5.3.5.3 HAIP – Proposed Annex D of a future edition of ISO/IEC 18013-7

OpenID Foundation defines a profile that works with the https://www.w3.org/TR/digital-credentials/. mdoc remote readers and mdoc app implementations may test the Browser API using the profile defined in the provisions of draft 04 of OIDF OpenID4VC High Assurance Interoperability Profile (HAIP), proposed Annex D of future ISO/IEC 18013-7 revisions.

5.3.5.4 HAIP – Ongoing work for OID4VP 1.0 using haip-vp:// URI scheme

OpenID Foundation defines a profile that works *without* the Browser API. mdoc remote readers and mdoc applications can engage using the haip-vp:// URI scheme, using the OID4VP version 1.0 protocol. Work is ongoing on a proposal for 18013-7 to use OID4VP 1.0 for remote presentation of an mdoc using URI-scheme engagement. More detailed specifications may follow.

5.4 Exploratory testing / prototyping hackathon

Part(s) of the test event will facilitate interested parties to have a "hackathon". In the hackathon, the participants can collaboratively do explorative testing on topics of interest. Currently we anticipate participant may be interested in the following topics:

- NFC optimizations (WG10/2708)
- Issuance and provisioning (draft ISO/IEC 23220-3)
- Exploring support for SD-JWT over 18013 protocols
- Testing with specific ZPK schemes

Other topics may be suggested by participants during registration. The coordinator will align with interested parties on topics and matching for the test event.

5.5 mdoc transaction scenarios

Table 4 provides an overview of the transaction scenarios that will be tested during the event. Practically, all combinations are possible. After each test run, participants will be able to use an automatic form with dropdown lists to enter the results of the transaction and the applied data/security checks listed in **Table 5** and **Table 6**.

Invocation	Data Transfer
	Device Retrieval
QR NFC (static handover) NFC (negotiated handover)	BLE (mdoc central client mode) BLE (mdoc peripheral server mode) BLE (mdoc central client mode) with L2CAP BLE (mdoc peripheral server mode) with L2CAP NFC

	Wi-Fi Aware
	Device retrieval to a website
mdoc:// scheme	RestAPI
mdoc-openid4vp:// scheme	OpenID4VP (18013-7, Annex B)
W3C DC API, using the “org-iso-mdoc” string	W3C DC API, using annex C as protocol
W3C DC API, using the “openid4vp-v1-signed” string	W3C DC API, using proposed annex D (OID4VP 1.0 + HAIP) as protocol
[TBC] haip-vp:// scheme	OpenID4VP, using proposal being discussed (OID4VP + HAIP)
	Server Retrieval
QR NFC (static handover) NFC (negotiated handover) mdoc:// scheme	WebAPI (token transferred after device engagement during device retrieval) WebAPI (token transferred during device engagement) OIDC (token transferred after device engagement during device retrieval) OIDC (token transferred during device engagement)

Table 4: list of test scenarios (grey is low priority)

For each transaction scenario, the applicable data checks and security checks listed in **Table 5** and **Table 6** shall be performed.

Data checks
(mDL) Check whether license and holder data are correctly transferred
(mDL and photo ID) Check whether facial image data is correctly transferred
(mDL and photo ID) Check whether age verification is correctly transferred
Check whether all other mandatory doctype-specific namespaces and data elements were correctly transferred
If applicable, check whether transferred credentials match the selected issuer identifiers.
If applicable, check whether alternative data elements were correctly transferred.
If applicable, check whether the Use case specific data elements were correctly transferred (use case age verification)
If applicable, check whether the Use case specific data elements were correctly transferred (use case land border random check)

Table 5: list of mdoc data checks

Security checks
Device retrieval security checks
Check whether issuer data authentication is performed successfully – step 1: validation of the mDL data using the Mobile Security Object (MSO).
Check whether issuer data authentication is performed successfully – step 2: validation of the MSO using the Document Signer Certificate.
Check whether issuer data authentication is performed successfully – step 3: validation of the Document Signer Certificate using the IACA root public key.

Check whether issuer data authentication is performed successfully – step 4: validation of the IACA certificate using the provided VICAL.
Check whether issuer data authentication is performed successfully – step 5: validation of the doctype listed with the IACA certificate in the provided VICAL.
Check whether the MSO was revoked.
Check whether mdoc authentication is performed successfully.
Check whether session encryption is performed successfully.
If performed, check whether mdoc reader authentication was successful.
In case the RICAL is supported, check whether mdoc reader authentication was successful based on a CA listed on the provided RICAL.
Server retrieval security checks
Check whether TLS server authentication is performed successfully. This includes the validation of the TLS server certificate.
Validate trust in the server retrieval mdoc response – step 1: validation of the JSON Web Signature of the message (JWT) using the JWS certificate.
Validate trust in the server retrieval mdoc response– step 2: validation of the JWS certificate using the IACA root public key.
Validate trust in the server retrieval mdoc response– step 3: validation of the IACA certificate using the provided VICAL.
If performed, check whether TLS client authentication was successful. This includes the validation of the TLS client certificate.

Table 6: list of mdoc security checks

6 Test process

6.1 Before the test event

6.1.1 Introductory webinar

The coordinator invites interested parties to join an introductory webinar that provides an overview of general logistics, background, history, test scope, and test process. The introductory webinars will be held on **Tuesday 7 October 2025 13:00 UTC and 23:00 UTC**. Registration is open to the public and invitations are sent to ISO/IEC, OIDF, and members of Austroads, Digital Identity New Zealand (NZ identity community) and IDPro (Australian identity community) as well as those of AAMVA and EReg. Attendees are able to ask questions during the webinar.

The webinars can be joined at the following URLs and will be hosted on MS Teams:

Tuesday 7 October 2025, 13:00 UTC	**Join the meeting now**
Tuesday 7 October 2025, 23:00 UTC (Wednesday 8 October, 12:00 NZ time)	**Join the meeting now**

6.1.2 Registration

Participants are required to register in advance of the interoperability test event. The registration deadline is **Friday 24 October 2025 23:59:59 UTC**.

The registration form, including instructions for registration and declaring the supported features (the implementation conformance statement) are available on https://nzta.mdoc.online/. For this test

event the registration system will allow participants to update the technical details of their registration, until final scheduling will happen.

Upon registration, specifically the following information is needed:

- A completed implementation conformance statement shall be submitted for each implementation.

  Note that an mdoc reader on iOS and an mdoc reader on Android would count as two distinct implementations and requires two conformance statements to be submitted. This helps the coordinator to manage the test slots more efficiently and optimize for testing time to avoid allocating time for incompatible implementations.

  If a participant wants to bring more than five implementations to the test event, please reach out to the coordinator.

  The number of persons of an organization that will attend the event shall be equal or higher to the number of implementations.

  Please find more details on conformance statement requirements of your implementations in Chapter 5.

- If possible, the IACA and Reader CA certificates for implementations should be submitted at the time of registration. If it is not possible to provide (all) certificates upon registration, participants are asked **to proceed and submit the registration form without the certificates. Certificates can be updated afterwards in the system used for registration once they become available**, or alternatively can be sent to the coordinator email address. All certificates shall be submitted by Friday 31st of October 2025 latest.

  The coordinator will check the submitted IACA certificates and provide feedback by email in case re-submission is required.

- If possible, mdoc remote readers public endpoints should be provided at time of registration. If it is not possible to provide (all) endpoints upon registration, participants are asked **to proceed and submit the registration form without the endpoint(s). Endpoints can be updated afterwards in the system used for registration once they become available**, or alternatively can be sent to the coordinator email address. If public testing prior the test event is supported, the endpoint shall be shared with the coordinator by Friday 31st of October 2025 latest.

  Note that a public endpoint for testing a mdoc remote reader implementation is expected to be an endpoint where engagement with an mdoc app can be initiated. In other words, the endpoint should be where a user can trigger an engagement and request for the mdoc app.

- Participants shall indicate the approval or disapproval of the use of their organization's name/ logo in publications regarding the test event including in the report with anonymized test results.

Apart from technical information about an implementation, participants are asked to share some logistical information through the registration as well. This includes, among others: dietary restrictions, requests for a letter of invitation for visa and interest in the showcase event.

6.1.3 Distribution of IACA and reader CA certificates

The coordinator will distribute the IACA certificates and reader CA certificates to the test event participants after the submission deadline of October 31st.

IACA certificates will be provided using VICAL as defined in Annex C of ISO/IEC 18013-5:2021.

Reader CA certificates will be provided using RICAL as defined in Annex F of draft second edition of ISO/IEC 18013-5.

6.1.4 Support and questions before the event

The coordinator will provide base documents of draft specifications (remote transactions, credential types etc.) upon request, after registration. Sample data sets will be provided to all registered participants by 31 October, latest.

In case any clarification is required, participants are encouraged to promptly report any issue with the test scope, test process, or interpretation/ implementation of the base documents and other supporting technical material listed in Chapter 5 with the coordinator by email.

With respect to the interpretation/ implementation of the base documents, the coordinator will provide initial clarification to the reporting participant, maintain an issue log, provide clarifications to registered participants as soon as possible after the registration deadline, and, as needed, organize a conference call to discuss reported issues with registered participants. The coordinator strives to respond to any queries within a week of reporting.

The coordinator will distribute anonymized issues and answers to the registered participants by email.

6.2 Pre-event testing for remote presentation

Participants willing to test prior to the test event itself, are encouraged to do so for online (remote) presentment of mDL and other documents. Public endpoints of mdoc remote readers for online testing will be shared by the coordinator on November 3rd latest. mdoc app implementations supporting any of the remote presentation protocols can test using these endpoints unattended until the test event.

Testing prior to the event is optional. mdoc app implementations are asked to test with available endpoints. Reporting any findings should be done during the test event itself, as testing collaboratively with the participants providing the mdoc remote reader implementation will result in higher quality feedback.

There will be no coordination for having interactive sessions between peers of mdoc and mdoc reader participants prior to the test event. Of course, you are free to informally align among yourself. Questions raised during pre-testing can be shared with the coordinator. In case of suspected findings during pre-testing, peers can ask the coordinator to be scheduled to check and confirm possible findings.

6.3 At the test event

The following sections cover a preliminary agenda for the interoperability test event, during 16, 17 and 18 November.

6.3.1 Test stations / mdoc cross-over testing

On 16 November (full day), cross-over testing begins, moderated and facilitated by the coordinator. Cross-over testing is divided into specific testing slots (e.g., 15 minutes each) for designated test

scenarios. mdoc app implementations move between test stations equipped with mdoc (proximity/ remote) reader implementations to check interoperability between the mdoc and mdoc (proximity/ remote) reader implementations.

In each testing slot:

- The coordinator presents the relevant test scenario(s).
- The coordinator assigns mdoc app to mdoc readers implementations using their pseudonymous identifier and based on the submitted conformance statement.
- Participants execute the test scenario and observe the results.
- Participants capture the test result using a results form.

The coordinator will aggregate and anonymize the test results. High level anonymized test results will be reflected in the test deliverables.

During the first day of the test event (16 Nov), the focus of testing will be on

- Proximity transactions with mDL based on ISO/IEC 18013-5:2021
- Proximity transactions with multiple mdocs
- Authentication of mdocs using the VICAL
- Reader authentication, using the RICAL
- Revocation methods defined in the draft 2nd edition of ISO/IEC 18013-5
- Remote transactions using the mdoc or mdoc-openid4vp URI schemes:
    - RestAPI defined in ISO/IEC TS 18013-7:2025 (Annex A)
    - OpenID4VP defined in ISO/IEC TS 18013-7:2025 (Annex B)

During the 2nd day of the test event (17 Nov), the focus of testing will be on

- Proximity and remote transactions with the new deviceRequest structure according to the draft 2nd edition of ISO/IEC 18013-5 (and its backward compatibility with ISO/IEC 18013-5:2021)
- Document request during NFC handover
- Proximity transactions with the new L2CAP PSM profile (enabling reduced transaction time)
- 3rd party recipient encryption of document responses
- Remote transactions using the W3C DC API (Brower API):
    - Digital Credentials API profile defined in ISO/IEC TS 18013-7:2025 (Annex C)
    - HAIP mdoc profile for the Digital Credentials API (proposed ISO/IEC TS 18013-7 Annex D)

During both days, the focus will be on qualitative assessment of provisions of the standard implemented by the participants (implementation feedback for the participants), as well as qualitative assessment of the standard itself, especially the new provisions in the draft 2nd edition of ISO/IEC 18013-5 and the proposed/draft 3rd edition of ISO/IEC 18013-7 (developer feedback to be provided to the ISO work group, who will meet during the week following the test event).

6.3.2 Mini-hackathon(s)

Time will be reserved in the schedule for those participants that want to participate in the mini-hackathon(s). For participants not interested, more cross-over interoperability will be scheduled.

6.3.3 Showcase of implementations

The organizer of the event will arrange for a showcase event for implementations. This event is scheduled for Monday afternoon and early evening, along with a social activity (drinks/dinner). More information on this will be shared separately with interested parties. More details will be shared with participants of the test event after registration.

6.3.4 Reflection together with members WG10

During the third day ((morning of) 18 November), participants of the test event are invited to share and discuss feedback with the experts of the ISO working groups (ISO/IEC JTC1 SC17 working group 10 and working group 4). Here we can collaboratively reflect upon findings and share insights.

6.4 After the test event

Participants should be aware that neither the organizers nor the coordinator, nor WG10 endorse the results of the interoperability test event. Passing tests in the event does not result in an "ISO certification" or "WG10 approval".

- High level, anonymized test results will be provided to ISO WG10 meeting for discussion during their meeting following the event.

- A general presentation with a summary of the interoperability test event, the test approach and high-level anonymized test results will be prepared for use by participants in their organization and/or other industry events.

Participants can collect results pertaining to their provided implementation. These results are solely intended for use by participants towards improving their mDL/ mdoc (reader) implementation(s). The test results shall not be used by any party for any commercial or (competitive) marketing purposes.

Only the general presentation with a summary of the event, the test approach and high-level anonymized test results may be used by participants to inform relevant stakeholders and for promotion and marketing of the concepts of mDL/ mdoc, interoperability and international standardization.

7 Changelog

Version	Date	Changes
1.0	26/09/2025	Final document for distribution.

Annex A – PhotoID - DocType and NameSpace for an ISO-compliant verifiable photo ID credential

This Annex is for convenience only. Refer to annex C.2.1 of "ISO-IEC TS 23220-4 - Proposed updated text for second DTS " (available in ISO Global Directory, WG4/N4770) for normative definitions.

A.1 Doctype

The document type for Photo ID credentials is "org.iso.23220.photoID.1".

A.2 23220-2 data elements

Photo ID credentials use the following data elements defined in the namespace "org.iso.23220.1".

Presence can be either of mandatory (M), conditional (C), optional (O) or recommended (R).

Data element identifier	Definition	Presence	Encoding format
family_name_unicode	Lastname, surname, or primary identifier, of the holder.	M	tstr
given_name_unicode	First name(s), other name(s), or secondary identifier, of the holder.	M	tstr
birth_date	Day, month and year on which the holder was born. Unknown parts (i.e., year, month, day) are masked with 1.	M	{ "birth_date": full-date, ? "approximate_mask": tstr }
portrait	Portrait data as specified in ISO/IEC 18013-2 C.4.5.	M	bstr
issue_date	Date (and possibly time) when the Photo ID was issued.	M	full-date
expiry_date	Date (and possibly time) when the Photo ID will expire.	M	full-date
issuing_authority_unicode	Name of issuing authority	M	tstr
issuing_country	Country code as alpha 2 and alpha 3 code, defined in ISO 3166-1, which issued the mobile eID document or within which the issuing authority is located.	M	tstr
age_over_18	Attesting whether the Photo ID holder is currently older than 18 (true) or not (false).	M	bool

Data element identifier	Definition	Presence	Encoding format
age_in_years	The age of the holder.	R	uint
age_over_NN	Additional current age attestations, NN <> 18.	R	bool
age_birth_year	The year when the holder was born.	R	uint
portrait_capture_date	Date when the portrait was taken.	O	tdate
birthplace	Country and municipality or state/province where the holder was born	O	tstr
name_at_birth	The name(s) which holder was born.	O	tstr
resident_address_unicode	The place where the holder resides and/or may be contacted (street/house number, municipality etc.).	O	tstr
resident_city_unicode	The city/municipality (or equivalent) where the holder lives.	O	tstr
resident_postal_code	The postal code of the holder.	O	tstr
resident_country	The country where the holder lives as a two letter country code (alpha-2 code) defined in ISO 3166-1.	O	tstr
resident_city_latin1	The city/municipality (or equivalent) where the holder lives, Latin1 characters.	O	tstr
sex	Holder's sex using values as defined in ISO/IEC 5218. (0 = Not known, 1 = Male, 2 = Female, 9 = non-applicable)	O	uint
nationality	Nationality of the holder as two letter country code (alpha-2 code) or three letter code alpha-3 code) defined in ISO 3166-1.	O	tstr
document_number	The number assigned or calculated by the issuing authority.	O	tstr
issuing_subdivision	Subdivision code as defined in ISO 3166-2, which issued the mobile eID document or within which the issuing authority is located.	O	tstr
family_name_latin1	Lastname, surname, or primary identifier, of the holder, Latin1 characters.	O	tstr
given_name_latin1	First name(s), other name(s), or secondary identifier, of	O	tstr

Data element identifier	Definition	Presence	Encoding format
	the holder. Latin1 characters.		

Table 7: Photo ID data elements - Mandatory (M), Conditional (C), Optional (O), Recommended (R)

A.3 Photo ID data elements

Photo ID credentials use the following data elements defined in the namespace "org.iso.23220.photoID.1".

Presence can be either of mandatory (M), conditional (C), optional (O) or recommended (R).

Data element identifier	Definition	Presence	Encoding format
`person_id`	Person identifier of the Photo ID holder.	O	`tstr`
`birth_country`	The country where the Photo ID holder was born, as an Alpha-2 country code as specified in ISO 3166-1.	O	`tstr`
`birth_state`	The state, province, district, or local area where the Photo ID holder was born.	O	`tstr`
`birth_city`	The municipality, city, town, or village where the Photo ID holder was born.	O	`tstr`
`administrative_number`	A number assigned by the Photo ID issuer for audit control or other purposes.	O	`tstr`
`resident_street`	The name of the street where the Photo ID holder currently resides.	O	`tstr`
`resident_house_number`	The house number where the Photo ID holder currently resides, including any affix or suffix.	O	`tstr`
`travel_document_number`	The number of the travel document to which the Photo ID is associated (if associated to or derived from a travel document).	O	`tstr`
`resident_state`	The state/province/district where the mDL holder lives. The value shall only use latin1b characters and shall have a maximum length of 150 characters.	O	`tstr`

Table 8: Photo ID data elements

A.4 Digital Travel Credential data elements

Photo ID credentials use the following data elements defined in the namespace "org.iso.23220.datagroups.1". The data element value shall be identical to the byte value of eMTRD as defined by ICAO 9303 part 10.

Presence can be either of mandatory (M), conditional (C), optional (O) or recommended (R).

Data element identifier	Definition	Presence	Encoding format
version	version	O	tstr
dg1	Data Group 1: biographic data (data recorded in MRZ)	C[a]	bstr
dg2	Data Group 2: reference portrait (encoded face)	C[a]	bstr
dg3	Data Group 3: encoded fingers	O	bstr
dg4	Data Group 4: encoded eye(s)	O	bstr
dg5	Data Group 5: displayed portrait	O	bstr
dg6	Data Group 6: Reserved for future use	O	bstr
dg7	Data Group 7: Displayed signature or usual mark	O	bstr
dg8	Data Group 8: data feature(s)	O	bstr
dg9	Data Group 9: Structure feature(s)	O	bstr
dg10	Data Group 10: Substance feature(s)	O	bstr
dg11	Data Group 11: additional personal detail(s)	O	bstr
dg12	Data Group 12: additional document detail(s)	O	bstr
dg13	Data Group 13: optional detail(s)	O	bstr
dg14	Data Group 14: security options	O	bstr
dg15	Data Group 15: active authentication public key info	O	bstr
dg16	Data Group 16: person(s) to notify	O	bstr
sod	Security Object Data	C[a]	bstr

Table 9: Data elements defined by ICAO Doc 9303 part 10- [a)] If the org.iso.23220.datagroups.1 namespace is present, these elements are to be present.

Annex B – Health certificate – DocType, NameSpace and data element identifiers

This Annex is for convenience only. Refer to "Guidelines for Developing ISO-Compliant mdoc for eHealth" RC3.1 for normative definitions (WG10/N2477).

B.1 Doctype

The document type for mobile international certificate of vaccination is "org.micov.1".

B.2 Vaccination, test, or recovery certificate data elements

The following data elements are defined in the namespace “org.micov.vtr.1”.

Presence can be either of mandatory (M), conditional (C), optional (O) or recommended (R).

Data element identifier	Definition	Presence	Encoding format
nam	Legal name – Family name, Given name. See clause A.2.3.1.	C [1)]	Name
fn	Family name	C [1)]	tstr
gn	Given name	C [1)]	tstr
dob	Date of birth	M	full-date
pid_[pty]	Person ID	O	Pid
sex	Sex, encoded per ISO/IEC 5218	O	uint
v_[ICD11DC]_[N]	Vaccination entry	O	Vac
t_[ICD11DC]_[N]	Test entry	O	Test
r_[ICD11DC]	Recovery entry	O	Rec
[1)] at least either nam or fn and gn shall be present. The fn and gn elements may be issued instead of, or in addition to the nam element, to enable selective disclosure, i.e. sharing of partial name info.			

Table 10: Vaccination, test, or recovery certificate data elements

The following tables show how to encode the data structures referenced in the vaccination, test, or recovery certificate data elements above.

Key	Definition	Presence	Encoding format
fn	Family name	O	tstr
fnt	Transliterated family name	O	tstr
gn	Given name	O	tstr
gnt	Transliterated given name	O	tstr

Table 11: Name structure

Key	Definition	Presence	Encoding format
pty	type of person identifier (value per HL7 FHIR https://www.hl7.org/fhir/valueset-identifier-type.html)	M	tstr
pnr	unique number for the pty/pic or pty/pic/pia combination	M	tstr
pic	Issuing country of the pty.	M	tstr
pia	Transliterated Issuing authority of the pty (conditional; shall be present if pnr is not unique for the combination of pty and pic)	O	tstr

Table 12: Pid structure

Key	Definition	Presence	Encoding format
tg	Disease or agent targeted	M	tstr
vp	Vaccine or prophylaxis	O	tstr
mp	Vaccine medicinal product	O	tstr
br	Vaccine brand	O	tstr
ma	Marketing authorization holder / Manufacturer	O	tstr
bn	Batch number or lot number of the vaccine	O	tstr
dn	Dose number	O	tstr
sd	Total series of doses	O	tstr
dt	Date of vaccination	O	full-date
co	Country of vaccination	O	tstr
ao	Administering organization	O	tstr
ap	Administering professional	O	tstr
nx	Due date of next dose, if required	O	full-date
is	Certificate issuer	O	tstr
ci	Unique certificate identifier (UVCI)	O	tstr
pd	Protection duration	O	tstr
vf	Valid from	O	full-date
vu	Valid until	O	full-date

Table 13: Vac structure

Key	Definition	Presence	Encoding format
tg	Disease or agent targeted	M	tstr
tt	Type of test	O	tstr
nm	Test name	O	tstr

Key	Definition	Presence	Encoding format
ma	Test manufacturer	O	tstr
dr	Date/time of test result	O	tdate
sc	Date/time of sample collection	O	tdate
tr	Test result (coding per SNOMED CT)	M	tstr
tc	Testing centre	O	tstr
co	Country where testing was performed	O	tstr
is	Certificate issuer	O	tstr
ci	Unique certificate identifier (UVCI)	O	tstr

Table 14: Test structure

Key	Definition	Presence	Encoding format
tg	Disease or agent recovered from	M	tstr
fr	Date of first positive test result	M	full-date
co	Country of test	O	tstr
is	Certificate issuer	O	tstr
df	Certificate valid from	O	full-date
du	Certificate valid until	O	full-date
ci	Unique certificate identifier	O	tstr

Table 15: Rec structure

B.3 Attestation data elements

The following data elements are defined in the namespace “org.micov.attestation.1”.

Presence can be either of mandatory (M), conditional (C), optional (O) or recommended (R).

Data element identifier	Definition	Presence	Encoding format
[ICD11DC]_vaccinated	Attest that the holder has been fully vaccinated. Replace “[ICD11DC]” in the data element identifier with the ICD-11 Disease Code of the disease or agent targeted, e.g. “1D47_vaccinated” to reflect a yellow fever vaccination.	O	bool
[ICD11DC]_recovered	Attest that the holder has recovered (and is considered immune) from the disease identified in the data element identifier, e.g. “RA01_recovered” to reflect recovery from COVID-19.	O	Recovered
[ICD11DC]_test	Attest that the holder obtained a negative test result.	O	Test
safeEntry_Leisure	Attest that the holder fulfils certain set requirements for safe entry in a leisure context (without disclosing whether that is based on vaccination, recovery, or negative test).	O	SafeEntry

Data element identifier	Definition	Presence	Encoding format
	See below.		
safeEntry_Travel	Attest that the holder fulfils certain set requirements for safe entry in a travel context (without disclosing whether that is based on vaccination, recovery, or negative test). See below.	O	SafeEntry
fac	Face image of the holder, to confirm binding of the attestation to the holder. Encoding: JPEG or JPEG2000.	O	bstr
fni	Family name initial character – supports attestation using partial ID information	O	tstr
gni	Given name initial character – supports attestation using partial ID information	O	tstr
by	Birth year according to RFC3339 – supports attestation using partial ID information	O	date-fullyear
bm	Birth month according to RFC3339 – supports attestation using partial ID information	O	date-month
bd	Birthday according to RFC3339 – supports attestation using partial ID information	O	date-mday

Table 16: Attestation data elements

The following tables show how to encode the data structures referenced in the attestation data elements above.

Key	Definition	Presence	Encoding format
RecovDiseaseAgent	Disease or agent the citizen has recovered from	M	tstr
FirstPosTest	Date when the sample for the test was collected that led to positive test	M	full-date

Table 17: Recovered structure

Key	Definition	Presence	Encoding format
Result	Test result – coding per SNOMED CT	M	tstr
TypeOfTest	Type of test, e.g., PCR test	O	tstr
TimeOfTest	Time of test. Consider rounding to the hour in the interest of privacy preservation	M	tdate

Table 18: Test structure

Key	Definition	Presence	Encoding format
SeCondFulfilled	Safe entry fulfilled, i.e., true/false.	M	bool
SeCondType	Safe entry type. “leisure” or “travel”. Other condition types may be added in the future. The exact scope and (legal) meaning is out of scope of this document.	M	tstr
SeCondExpiry	Safe entry expiry. Consider rounding to the hour in the interest of privacy preservation; recommended to provide	M	tdate

Key	Definition	Presence	Encoding format
	a short validity and refresh regularly, to not leak how the conditions for safe entry are fulfilled (e.g. expiry in a far future suggesting vaccination or recovery)		

Table 19: SafeEntry structure

Annex C – Mobile vehicle certificate – DocType, NameSpace and data element identifiers

This Annex is for convenience only. Refer to ISO/IEC 7367 PDTS for normative definitions (SC17/N7603).

C.1 Doctype

The document type for mobile vehicle registration cards (mVC) is "org.iso.7367.1.mVC".

C.2 mVC data elements

mVC credentials use the following data elements defined in the namespace "org.iso.7367.1".

Presence can be either of mandatory (M), conditional (C), optional (O) or recommended (R).

Data element identifier	Definition	Presence
issue_date	according to ISO/IEC 23220-2 Date when the mVC was issued.	M
expiry_date	according to ISO/IEC 23220-2 Date given by the issuing authority, when the mVC expires. Example: UN element H	O
issuing_authority_unicode	according to ISO/IEC 23220-2 Name of the issuing authority of the vehicle registration certificate. The authority belongs to the issuing signing key and must recognized by the mdoc-reader. The issuing authority also refers to the competent authority.	M
issuing_country	according to ISO/IEC 23220-2 Alpha-2 country code, as defined in ISO 3166-1, of the issuing authority's country or territory of the mVC, or the country or territory which the issuing jurisdiction belongs to.	M
document_number	according to ISO/IEC 23220-2 Unique number of the issued document	O

Table 20: Mobile vehicle registration card data elements

C.3 mVC data elements

mVC credentials use the following data elements defined in the namespace "org.iso.7367.1".

Presence can be either of mandatory (M), conditional (C), optional (O) or recommended (R).

Data element identifier	Meaning	Definition	Presence	Encoding format
registration_number	Registration Number	a serial number, to be known as the registration number, composed in the manner indicated in Annex 2 to Vienna Convention on Roadtraffic (1968) Example: UN element A	M	tstr
registration_number_type	Registration Number Type	type of registration number when using the same number but for different	O	tstr

Data element identifier	Meaning	Definition	Presence	Encoding format
		classes/types of vehicles (like f.e. registered farming vehicle, motorised scooter, Heavy Vehicles)		
date_of_registration	Date of Registration	date/time of the registration to which this certificate refers	M	tdate or full-date
date_of_first_registration	Date of first registration	date/time of the first registration of the vehicle Example: UN element B	O	tdate or full-date
approval_date_technical_inspection	Date of approval technical inspection	date of the approval of the technical inspection	O	tdate or full-date
expiry_date_technical_inspection	Date of expiration of the approval for the technical inspection	expiry date of the approval of the technical inspection	O	tdate or full-date
vehicle_identification_number	Vehicle Identification Number	Vehicle Identification Number defined by the vehicle manufacture. It is also known as the serial number of the chassis or as the maker's production or serial number. The data element shall/should have a valid value, as defined in ISO 3779. Example: UN element E	M	tstr
vehicle_holder	Registered holder(s) of the vehicle	one or more registered holders of the vehicle by the authority Example: UN element C the mVC shall always include at least one vehicle holder or vehicle owner	C	VehicleHolders
vehicle_owner	Registered owner(s) of the vehicle	one or more registered owners of the vehicle by the authority the mVC shall always include at least one vehicle holder or vehicle owner	C	VehicleOwners
basic_vehicle_info	Basic vehicle info	the basic information of the vehicle	M	BasicVehicleInfo
mass_info	Mass info	the mass information of a vehicle	M	MassInfo
trailer_mass_info	Trailer mass info	the mass information of a trailer only present if applicable	O	TrailerMassInfo
engine_info	Engine info	the info of the engine of a vehicle	O	EngineInfo

Data element identifier	Meaning	Definition	Presence	Encoding format
seating_info	Seating info	the info of the number of seating and standing places in a vehicle	O	SeatingInfo
un_distinguishing_sign	UN distinguishing sign	Distinguishing sign of the issuing country according to ISO/IEC 18013-1:2018, Annex F. If no applicable distinguishing sign is available in ISO/IEC 18013-1, an IA may use an empty identifier or another identifier by which it is internationally recognized. In this case the IA should ensure there is no collision with other IA's.	M	tstr
issuing_jurisdiction	Issuing jurisdiction	Distinguishing sign of the issuing country according to ISO/IEC 18013-1:2018, Annex F. If no applicable distinguishing sign is available in ISO/IEC 18013-1, an IA may use an empty identifier or another identifier by which it is internationally recognized. In this case the IA should ensure there is no collision with other IA's.	O	tstr

Table 21: Mobile vehicle registration card data elements (org.iso.7367.1)

The following tables show how to encode the data structures referenced in the mobile vehicle registration card data elements above.

Key	Description	Presence
organization_name_unicode	according to ISO/IEC 23220-2; empty in case of a natural person; either organization name or the combination of family name and given name must be present	C
organization_name_latin1	according to ISO/IEC 23220-2; empty in case of a natural person; either organization name or the combination of family name and given name must be present	C
family_name_unicode	according to ISO/IEC 23220-2; empty in case of a organization; either Organization name or the combination of family name and given name must be present	C
family_name_latin1	according to ISO/IEC 23220-2 empty in case of a organization; either organization name or the combination of family name and given name must be present	C
given_name_unicode	according to ISO/IEC 23220-2; empty in case of a organization; either organization name or the combination of family name and given name must be present	C

Key	Description	Presence
given_name_latin1	according to ISO/IEC 23220-2 empty in case of a organization; either organization name or the combination of family name and given name must be present	C
resident_address	according to ISO/IEC 23220-2	M
resident_city	according to ISO/IEC 23220-2	M
resident_state	according to ISO/IEC 23220-2	O
resident_postal_code	according to ISO/IEC 23220-2	O
resident_country	according to ISO/IEC 23220-2	M

Table 22: PersonalData (VehicleOwner/VehicleHolder) structure contained in VehicleOwners/VehicleHolders structures as array elements

Key	Description	Presence
vehicle_category_code	vehicle category code as per [3](unece.org)	O
vehicle_category_nat	national vehicle category Vehicle category when vehicle category code is not available	O
type_approval_number	the number of the type approval of the vehicle	O
make	brand of the vehicle Example: UN element D	M
commercial_name	the commercial name of the vehicle	O
colours	the primary colour(s) of the vehicle: 1 (White) 2 (Yellow) 3 (Orange) 4 (red) 5 (violet) 6 (blue) 7 (green) 8 (grey) 9 (brown) 10 (Black)	O
automation_level	level of automation of the vehicle referring to industry-standard scale from zero to five developed by the Society of Automotive Engineers (SAE). The value shall be one of the following: 0, 1, 2, 3, 4, 5.	O
status_vehicle	status of the vehicle like 'Stolen, Written off Vehicle (WOVR), impounded'	O

Table 23: BasicVehicleInfo structure

Key	Description	Presence
unit	the unit in which the mass is expressed. The value shall be one of the following: kg, lb	M

Key	Description	Presence
techn_perm_max_laden_mass	Technical permissible maximum laden mass I	O
vehicle_max_mass	the maximum permissible laden mass of the vehicle in service Example: UN element F	O
whole_vehicle_max_mass	The maximum permissible laden mass of the whole vehicle in service	O
mass_in_running_order	the mass of the vehicle in service Example: UN element G	O

Table 24: MassInfo structure

Key	Description	Presence
unit	the unit in which the mass is expressed. The value shall be one of the following: kg, lb	M
tech_perm_max_tow_mass_braked_trail	the technically permissible maximum towable mass of a braked trailer	O
tech_perm_max_tow_mass_unbr_trailer	the technically permissible maximum towable mass of a unbraked trailer	O

Table 25: TrailerMassInfo structure

Key	Description	Presence
engine_number	The number of the engine of the vehicle	O
engine_capacity	Engine capacity (not applicable for electric vehicles) in cm3	O
engine_power	Maximum net power of a vehicle in kW	O
class_off_hybrid_vehicle_code	the indication that a vehicle is powered - by electricity or fuel cell - as well as another fuel. The value shall be one of the following: OVC-HEV (Off vehicle-charging hybrid electric vehicle) NOVC-HEV (Not off-vehicle charging hybrid electric vehicle) OVC-FCHV (Off-vehicle charging fuel cell hybrid vehicle) NOVC-FCHV (Not off-vehicle charging fuel cell hybrid vehicle)	O
energy_source	The energy source(s) of a vehicle: 10 (Petrol) 11 (Petrol E5) 12 (Petrol E10) 15 (Ethanol) 16 (Ethanol E85) 19 (Mixture) 20 (Diesel) 21 (Biodiesel) 22 (ED95) 30 (LPG) 40 (CNG) 44 (Biomethane) 50 (Hydrogen) 55 (H2NG)	O

Key	Description	Presence
	60 (LNG) 90 (Other) 91 (Compressed air) 95 (Electricity)	

Table 26: EngineInfo structure

Key	Description	Presence
`nr_of_seating_positions`	Number of seating positions (including the driver)	O
`number_of_standing_places`	Number of standing places	O

Table 27: SeatingInfo structure