13th International Interoperability Test Event

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

27 – 29 May 2026, La Ciotat, France

Version 1.0 rev.1 – 29 April 2026

Hosted by

France Titres

AGENCE NATIONALE DES TITRES SÉCURISÉS

Endorsed by

AAMVA

Austroads

EReg

ASSOCIATION OF EUROPEAN VEHICLE AND DRIVER REGISTRATION AUTHORITIES

1 Introduction

ISO/IEC 18013-5:2021 standardises 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.
- November 2025: 12th in-person international test event in Wellington, New Zealand.

The 13th international interoperability test event is planned for 27 – 29 May 2026 in La Ciotat, France.

This document provides further details on the upcoming interoperability test event. This includes details on the venue, 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 events in Sydney, Utrecht and Wellington, the 13th interoperability test event will involve the use of Verified Issuer Certification Authority Lists (VICALs) and Reader Identification Certification Authority Lists (RICALs).

2 Organisation

Organiser & Host:	France Titres, Ministry of Interior, France
Coordinator:	Arjan Geluk
Contact:	info@mdoc.online
Date:	Wednesday 27, Thursday 28 and Friday 29 May, 2026
Location:	Wednesday: TBC (close to the ISO meeting at the Best Western); Thursday & Friday: Limone Rooftop, 756 avenue Émile Bodin, 13600, La Ciotat, France
Co-located activities:	114th meeting of ISO/IEC JTC1/SC17/WG10 on driving licenses, 25-27 May Photo ID & mdoc showcase, Friday 29 May 2026

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 optionally 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 (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. mdoc implementations with reader authentication are encouraged to leverage a test RICAL conforming to draft 2nd edition of ISO/IEC 18013-5, annex F.

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

The event will be open to selected observers, at the discretion of the organiser 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 organiser/coordinator reserves the right to ask participating organisations 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 France, 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.

- 2026/04/16: Online introductory webinar (13:00 UTC)
- 2026/05/05: Registration deadline (23:59:59 UTC)
- 2026/05/15: IACA and reader CA certificates submitted
- 2026/05/15: Final confirmation of supported features, for test scheduling
- **2026/05/19: pre-event coordination meeting with registered participants (13:00 UTC)**
- 2026/05/27: individual participant's conformity test with CLR and Fime.
- 2026/05/28: Interoperability test event (full day)
- 2026/05/29: Interoperability test event (morning)
- 2026/05/29: Showcase of Photo ID, mDL, mVC and other mdocs (afternoon)
- Post-event: 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 (ISO/IEC TS 23220-4), mVC (ISO/IEC DTS 7367-2) and other doctypes. Participants can bring implementations of other mdocs, e.g. an EU PID, EU age attestation 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 also be provider before, and updated during, the event.

During the first day of the event (27 May), participants will be invited for an individual time slot to perform a subset of conformity tests specified in ISO/IEC TS 18013-6. This will take place at or close to the meeting location of ISO/IEC JTC1/SC17/WG10 (Best Western, La Ciotat).

On 28 May and the morning of 29 May, 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.

During the 3rd day of the test event (29 May), 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 edition of ISO/IEC 18013-5 and draft 3rd edition of ISO/IEC TS 18013-7 (developer feedback to be provided to the ISO work group).

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 DIS text for the 2nd edition of ISO/IEC 18013-5.
        - Additional information to describe the requested information
        - mDL revocation (status list / identifier list)
        - Support sending the request during NFC handover
        - BLE L2CAP mode improvements
        - RICAL support
        - Document response encryption
        - Zero Knowledge Proof support[1]
        - sd-jwt-vc in device request/response
    - 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/.
    - The following two profiles for Browser API can be tested:
        - ISO/IEC 18013-7:2025 Annex C: According to the profile defined in ISO/IEC TS 18013-7:2025;
        - OIDF HAIP (Annex D of the draft 3rd edition of ISO/IEC 18013-7): 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.html. 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 (Annex E of the draft 3rd edition of ISO/IEC 18013-7)
    - 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.html of the HAIP profile.

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 the Draft International Standard text of the 2nd edition of “ISO/IEC 18013-5 - Mobile driving licence (mDL) application”.

[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.

- **Photo ID**, as defined in annex C.2.1 of ISO/IEC TS 23220-4;

- **Mobile vehicle registration certificate (mVC)**, as defined in ISO/IEC TS 7367-2, optionally augmented with the EU namespace, as defined in the APTITUDE Rulebook for EU mVRC: https://github.com/APTITUDE-Consortium/aptitude-eudi-wallet-specs/blob/main/docs/rulebook/mVRC-rulebook.md;

- **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);

- **EU Age Verification**, as defined in https://ageverification.dev/av-doc-technical-specification/docs/architecture-and-technical-specifications/#41-proof-of-age-attestation

- **EU PID**, as defined in the PID Rulebook in the EUDI Wallet Architecture Reference Framework v2.8.0 (available on https://github.com/eu-digital-identity-wallet/eudi-doc-attestation-rulebooks-catalog/blob/main/rulebooks/pid/pid-rulebook.md);

5.2.3 Examples

The coordinator will provide examples of a document for the following mdoc document types on the resource page in the test event management platform:

- PhotoID
- mVC
- micov
- EU Age Verification
- 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.

Participants can also use the test event management platform to:
- issue credentials with sample data (using OID4VCI) under the Credential Issuance menu item
- try remote presentation of their credentials under the Remote Readers menu item
- try their remote readers using the emulation under the Wallet Simulator menu item

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 credential with

- Holder data

- Age verification (age over 18)
- eMRTD data groups (to support use as Digital Travel Credential)

Implementations should support the mVC credential with

- Holder data
- Vehicle data
- Additional data in the EU namespace

Implementations may also support micov, EU Age Verification and EU PID. 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 may be implemented as defined in ISO/IEC 18013-5. The optional mdoc reader authentication (device 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 18013-5 in the second edition. Server retrieval will not be tested during the event.

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
		NFC	NFC static handover
			NFC negotiated handover
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
Security	Device retrieval	Issuer data authentication
		mdoc authentication
		Session encryption
		mdoc reader 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 MRTD data groups for DTC)
		Mobile Vehicle Registration Certificate (mVC)
		Mobile International Certificate of Vaccination (micov)
		EU Age Verification
		EU Person Identification Data (PID)

Table 1: ISO/IEC 18013-5 features to be tested

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, OpenID4VP, or Device Retrieval to a website over an API.

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

ISO/IEC TS 18013-7:2025 features		
Data transfer	Device retrieval	Annex A - device-retrieval-to-a-website (RestAPI)
		Annex B - OpenID4VP
		Annex C - 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 should 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
Device retrieval	New BLE L2CAP PSM profile
	New request structure
Proposed features	sd-jwt-vc in device request / response
	NFCv2

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, mdoc app implementations should allow the selection of which mdoc is included in the response to the mdoc reader or mdoc remote reader.

New request structure

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`

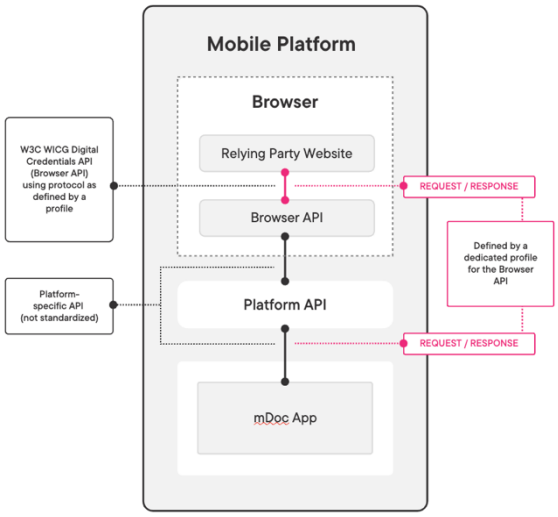
To maximise benefit from testing this functionality, mdoc app providers are requested to be prepared to respond with different data in different transactions (e.g. by forcing selection by the user, or by varying mdoc data sets issued with different combinations of data elements).

- **Document response encryption**: mdoc reader or mdoc remote reader implementations should test this feature by asking the mdoc app to provide a PhotoID document including eMRTD data groups, by sending a Device request with:
    - 1 docRequest requesting `family_name`, `given_name`, `portrait` and `travel_document_number`, and
    - 1 docRequest requesting `dg1`, `dg2` and `sod` with document response encryption
- **sd-jwt-vc in device request/response**: mdoc reader or mdoc remote reader implementations should test this feature by asking the mdoc app to provide documents in mdoc and sd-jwt format, by sending a Device request with:
    - 1 docRequest requesting an mDL
    - 1 docRequest requesting an EU PID in mdoc format
    - 1 docRequest requesting an EU PID in sd-jwt-vc format (optionally as alternative to EU PID in mdoc format)

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 OIDF OpenID4VC High Assurance Interoperability Profile (HAIP), proposed Annex D of the draft 3rd edition of ISO/IEC 18013-7 (WG10N2792).

5.3.5.4 HAIP – discussed new Annex, for OID4VP using haip-vp:// URI scheme

OpenID Foundation defines a profile that works *without* the DC API. mdoc remote readers and mdoc applications can engage using the haip-vp:// URI scheme, using the profile defined in the provisions of OIDF OpenID4VC High Assurance Interoperability Profile (HAIP), proposed Annex E of the draft 3rd edition of ISO/IEC 18013-7 (WG10N2792).

5.4 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

haip-vp:// scheme	OpenID4VP, using proposal being discussed (OID4VP + HAIP)

Table 4: list of test scenarios

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 that sd-jwt-vc data was correctly transferred

Table 5: list of mdoc data checks

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.

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 webinar will be held on **Thursday 16 April 2026 13:00 UTC**. Registration is open to the public and invitations are

sent to ISO/IEC and members of the EU Large Scale Pilot APTITUDE. Attendees are able to ask questions during the webinar.

6.1.2 Registration

Participants are required to register in advance of the interoperability test event. The registration deadline is **5 May 2026 23:59:59 UTC**.

The registration portal enables registration of participants, their organisation and implementations. It includes functionality for registration and adding test objects, declaring the supported features of implementations to be tested (the implementation conformance statement) and is available on https://france2026.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.

  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 without the certificates. Certificates can be updated afterwards in the system used for registration once they become available**. All certificates shall be submitted by 15 May 2026 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 without the endpoint(s). Endpoints can be updated afterwards in the system used for registration once they become available**.

  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, and requests for a letter of invitation for visa.

6.1.3 Distribution of IACA and reader CA certificates

The coordinator will make the IACA and reader CA certificates available to the test event participants after the submission deadline in the resource page of the test event management platform.

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 30 April.

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 in the resource page of the test event management platform.

6.1.5 Pre-event coordination meeting

The host and coordinator invite registered parties to join the pre-event coordination meeting in which we present more details on the logistics and test schedule. The coordination meeting will be held on **Tuesday 19 May 2026 13:00 UTC**. Invitations are sent to registered participants to the event. Attendees are able to ask questions during the coordination meeting.

6.1.6 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. Remote reader implementations and a wallet simulator are available in the test event management platform to support such pre-event testing.

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 amongst yourselves. 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.

6.2 At the test event

The following sections cover a preliminary agenda for the interoperability test event, during 27, 28 and 29 May.

6.2.1 Optional conformity testing (individual time slot)

On 27 May a subset of conformity tests specified in ISO/IEC TS 18013-6 will be performed. Participants will be invited for an individual time slot to perform conformity testing with CLR and Fime. Conformity tests will be performed at or very near the venue of the ISO/IEC WG10 meeting.

6.2.2 Test stations / mdoc cross-over testing

On 28 May (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 them.

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 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).

6.2.3 Showcase of implementations

The organiser of the event will arrange for a showcase event for implementations. This event is scheduled for Friday afternoon. More information on this will be shared separately.

6.3 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 meetings.

- 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 review the results pertaining to their provided implementation in the test event management platform. 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 anonymised 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 standardisation.

7 Changelog

Version	Date	Changes
0.4	10/04/2026	First complete draft.
1.0	20/04/2026	Final version for publication.
1.0 rev1	29/04/2026	Registration deadline set to 5/5/2026 23:59:59 UTC Added reference to EU mVRC rulebook (EU namespace for mVC)