



BSI Standards Publication

Personal identification — ISO-compliant driving licence

Part 6: mDL test methods

National foreword

This Published Document is the UK implementation of ISO/IEC TS 18013-6:2024.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and security devices for personal identification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 14025 5

ICS 35.240.15

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2024.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------



Technical Specification

ISO/IEC TS 18013-6

Personal identification — ISO- compliant driving licence —

Part 6: mDL test methods

*Identification des personnes — Permis de conduire conforme
à l'ISO —*

*Partie 6: Méthodes d'essai relatives au permis de conduire sur
téléphone mobile*

**First edition
2024-11**



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents		Page
Foreword.....		iv
Introduction.....		v
1	Scope.....	1
2	Normative references.....	1
3	Terms and definitions.....	2
4	Abbreviated terms.....	3
5	Conformance.....	3
6	Test design.....	3
6.1	General.....	3
6.2	Test case hierarchy.....	4
6.2.1	Structure.....	4
6.2.2	System under test.....	4
6.2.3	Test layers, test areas, test groups and test units.....	5
6.2.4	Test cases.....	5
6.3	Test administration.....	7
6.3.1	Preconditions for testing of an mDL.....	7
6.3.2	Preconditions for testing of an mDL reader.....	9
6.3.3	Implementation conformance statements.....	11
6.3.4	Test report.....	12
7	mDL conformity test methods.....	12
8	mDL reader conformity test methods.....	12
Annex A (normative) Test case hierarchies.....		13
Annex B (informative) Implementation conformance statements.....		18
Annex C (normative) Test certificates.....		26
Bibliography.....		57

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 17, *Cards and security devices for personal identification*.

A list of all parts in the ISO/IEC 18013 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The ISO/IEC 18013 series establishes guidelines for the design format and data content of an ISO-compliant driving licence (IDL) with regard to human-readable features (ISO/IEC 18013-1), ISO machine-readable technologies (ISO/IEC 18013-2), access control, authentication and integrity validation (ISO/IEC 18013-3), associated test methods (ISO/IEC 18013-4) and interface and related requirements to facilitate ISO-compliant driving licence (IDL) functionality on a mobile device (ISO/IEC 18013-5). It creates a common basis for international use and mutual recognition of the IDL without impeding individual countries/states in applying their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs.

ISO/IEC 18013-5 establishes interface specifications for the implementation of a driving licence in association with a mobile device. It specifies the interface between the mobile driving licence (mDL) and mDL reader and the interface between the mDL reader and the issuing authority infrastructure.

This document prescribes requirements for testing of the compliance of the data model, device engagement, data transfer and security mechanisms on a mobile driving application with the requirements of ISO/IEC 18013-5.

Personal identification — ISO-compliant driving licence —

Part 6: mDL test methods

1 Scope

This document specifies test methods for testing conformity of a mobile driving licence (mDL) or an mDL reader to ISO/IEC 18013-5. This document specifies test methods for:

- mDL on its interface to an mDL reader;
- mDL reader on its interface to an mDL;
- mDL reader on its (optional) interface to an issuing authority infrastructure.

Test cases for an issuing authority infrastructure on its interface to an mDL reader are not included in this document.

Test cases for the use of OIDC by an mDL reader on its interface to an issuing authority infrastructure are not included in this document. This document only provides test cases for the use of WebAPI on this interface.

This document only addresses the functional behaviour of an implementation under test (IUT) on its interface(s) in scope. It does not address:

- the internal implementation of an IUT, such as a secure area in an mDL;
- any functional requirements to an IUT not specified in ISO/IEC 18013-5, for example, requirements of a particular issuing authority;
- non-functional aspects of the IUT, nor IUT interfaces not listed above, such as the interface from an issuing authority infrastructure to an mDL, used to provision mDL data.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9646 (all parts), *Information technology — Open Systems Interconnection — Conformance testing methodology and framework*

ISO/IEC 18013-5:2021, *Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application*

Bluetooth, *Bluetooth Core Specification, Version 5.2*

Bluetooth, *Supplement to the Bluetooth Core Specification, Version 9*

NFC Forum, *Connection Handover Technical Specification, Version 1.5, 2020*

Wi-Fi Alliance, *Neighbor Awareness Networking Specification, Version 3.1*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18013-5 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 implementation conformance statement

ICS

statement made by the supplier of an implementation or system claimed to conform to a given specification, stating which capabilities have been implemented

[SOURCE: ISO/IEC 9646-1:1994, 3.3.39, modified — Form specification removed.]

3.2 implementation under test

IUT

implementation of one or more open systems interconnection (OSI) protocols, being that part of a real open system which is to be studied by testing

[SOURCE: ISO/IEC 9646-1:1994, 3.3.43, modified — User/provider information removed.]

3.3 system under test

SUT

real open system in which the IUT resides

Note 1 to entry: The following systems under test are recognised in this document: mDL, mDL reader, issuing authority infrastructure, certificate and CRL. Apart from these, this document specifies common test cases, that are applicable to several systems under test; see [6.2.2](#).

Note 2 to entry: ISO/IEC 18013-5 defines and uses the terms "mdoc" and "mdoc reader" next to "mDL" and "mDL reader". Clauses 6 and 7 of ISO/IEC 18013-5, as well as Annex B, are applicable only to mdocs that fulfil the same function as an ISO-based driving licence (IDL), and hence use "mDL" and "mDL reader". Clauses 8 and 9 of ISO/IEC 18013-5 are applicable to mdocs in general, and hence use "mdoc" and "mdoc reader". This document follows ISO/IEC 18013-5, and uses "mDL" or "mDL reader" in test cases that are based on Clauses 6 or 7 or Annex B, and "mdoc" or "mdoc reader" for test cases that are based on Clauses 8 or 9 of ISO/IEC 18013-5. Nevertheless, this document uses "mDL" and "mDL reader" to indicate the possible Systems under Test, because ISO/IEC 18013-5 primarily standardises the mobile driving licence.

[SOURCE: ISO/IEC 9646-1:1994, 3.3.103, modified — Notes to entry added.]

3.4 test case

description of test purpose, unique test case identifier, test inputs, test execution conditions, test steps, and the results required to pass the test

[SOURCE: ISO/IEC 18013-4:2019, 3.1]

4 Abbreviated terms

CA	certificate authority
CBOR	concise binary object representation
COSE	cbor object signing and encryption
CRL	certificate revocation list
DS	document signer
ECDSA	elliptic curve digital signature algorithm
IACA	issuing authority certificate authority
JWS	JSON web signature
OCSP	online certificate authority
OID	object identifier
TLS	transport layer security
URI	uniform resource identifier
URL	uniform resource locator

5 Conformance

Test cases are described in the Appendices 1, 2 and 3 to this document, which are published as separate documents and can be found at <https://standards.iso.org/iso-iec/ts/18013/-6/ed-1/en>. Test cases are intended to be performed separately and independently. An IUT is not required to pass through all tests sequentially. In addition, not all tests may be applicable to a given implementation of an mDL or mDL reader. The applicability of a test case is determined by comparing the statements in the profile element of each test case (see 6.2.4.2) to the implementation conformance statement for the IUT provided by the applicant for conformance testing; see 6.3.3.

An IUT is considered conformant to this document and, in extension, to ISO/IEC 18013-5, if it passes all applicable test cases specified in this document.

NOTE Passing all applicable test cases in this document does not guarantee that no failures will occur under operational conditions.

6 Test design

6.1 General

This clause describes mDL and mDL reader test design in accordance with the ISO/IEC 9646 series. Several basic elements referred to in the specification of individual test cases are explained in this clause.

NOTE These elements facilitate the synchronisation of additional specifications written by different organisations with this document.

6.2 Test case hierarchy

6.2.1 Structure

Test cases specified in this document are grouped into a coherent test structure. This clause describes the following elements of the test structure: system under test, test layer, test area, test group, test unit and test case. These elements have a hierarchical relationship, as shown in [Figure 1](#).

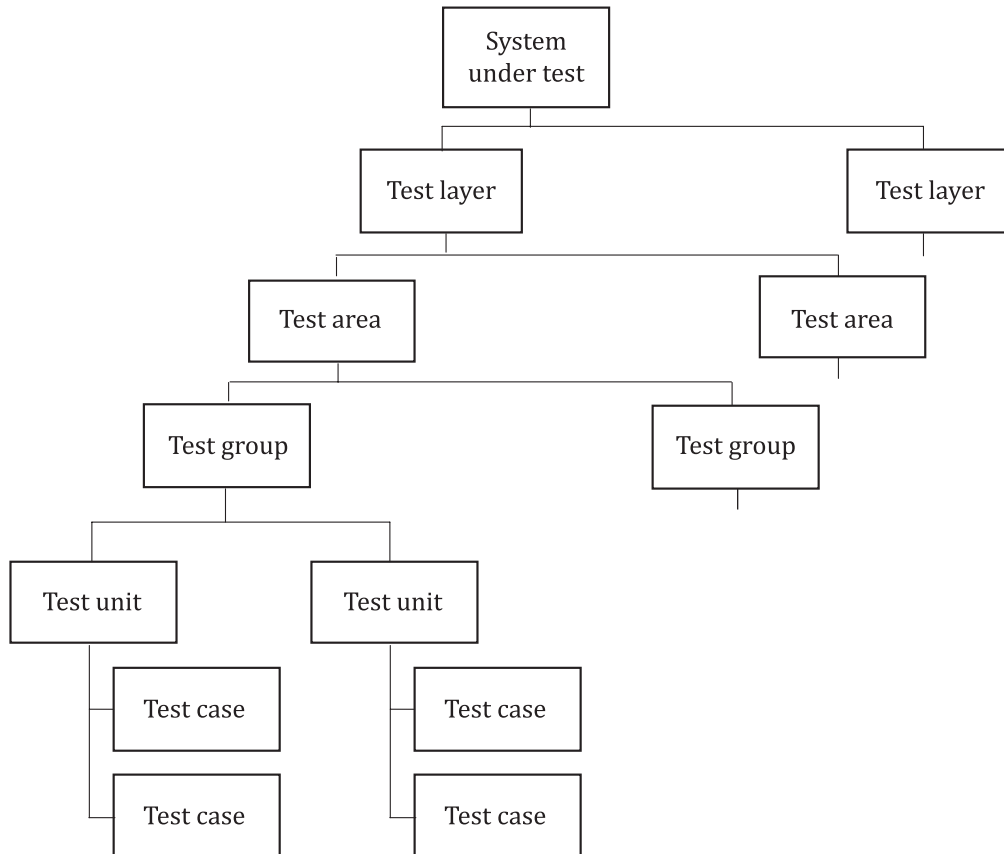


Figure 1 — Test element hierarchy

[Subclauses 6.2.2](#), [6.2.3](#) and [6.2.4](#) provide more information about the elements of the test case structure.

6.2.2 System under test

An IUT can be one of following main systems under test (see ISO/IEC 18013-5):

- an mDL;
- an mDL reader;
- an issuing authority infrastructure.

This document specifies test cases for mDLs and mDL readers. Apart from these, this document also specifies:

- Test cases for certificates specified in ISO/IEC 18013-5: These test cases will typically not be executed independently. They are primarily invoked when executing test cases for an mDL or mDL reader. For example, when testing the implementation of issuer data authentication by an mDL under test, the certificate test cases applicable to a document signer certificate will be executed on the DS certificate provided by the mDL. Next to that, certificate test cases may optionally be executed independently, for example to verify the format of a certificate stored as a file.

- Common test cases: These test cases are applicable to more than one system under test. Common test cases will not be executed independently. Rather, they are invoked when executing test cases for an mDL or mDL reader. For example, when testing whether a device retrieval mdoc request received from an mDL reader under test is correctly formatted, the Common_CBOR test cases will be executed together with other Common_CBOR test cases. The same test cases will also be executed when testing the device retrieval mdoc response received from an mDL under test.

NOTE Test cases for certificate revocation lists, as specified in ISO/IEC 18013-5, are not included in this edition of this document.

6.2.3 Test layers, test areas, test groups and test units

The test case structures for each of the systems under test distinguished in 6.2.2 are provided in Annex A in this document. These test case structures are derived from the structure of ISO/IEC 18013-5:2021, clauses 7, 8, 9 and Annex B. For each SUT, a number of test layers are defined. When needed, a test layer is divided into test areas, a test area into test groups and a test group into test units, to further clarify the intent of the test cases within them, or to prevent the number of test cases in a single area, group or unit from growing inconveniently large.

6.2.4 Test cases

6.2.4.1 General

Each test case is defined by the following information:

Test case-ID	Uniquely identifies the test case. See 6.2.4.2.
Purpose	Specifies the requirement(s) addressed in this test case.
References	Identifies specific references to the requirement(s) addressed by this test case.
Profile	Defines the profile(s) for which the test case is applicable. See 6.2.4.3.
Preconditions	Define the state in which the IUT needs to be before the test case can be executed, See 6.2.4.4.
Test scenario	<p>Defines the test steps that shall be taken.</p> <p>Each step covers a simple, exactly defined operation with a measurable result that can be included in the test report. The steps shall be performed in the order listed.</p> <p>Each test step is defined by the following information:</p> <ul style="list-style-type: none"> — Test step ID: a consecutive number, uniquely identifying each test step and the execution order in the test case. — Description: defining the operation that has to be executed for this step. — Configuration data: optionally specifying input data required to perform this test step.
Expected result	The expected result defines pass criteria for each test step in the test scenario. The analysis of the observed result in comparison with the expected result leads to a verdict, e.g. "Pass" or "Fail". The results of the individual test steps or the overall result, or both, of the test case are transferred to the test report.

6.2.4.2 Test case ID

Test case IDs are formed as follows:

SUT_TestLayer_Test_Area_TestGroup_TestUnit_##, where:

- SUT is the name of the system under test (see 6.2.2) for which the test case is applicable, e.g. mDL (mDL), mDL reader (mDLR), certificate (Cert), or common (Common);

- TestLayer, TestArea, TestGroup and TestUnit are the names of the test layer, test area, test group and test unit to which the test cases belong, as shown in the tables in [Annex A](#). To prevent names from becoming too long, the name abbreviation given between brackets is used, if provided. If no abbreviation is given, the full name is used;
- ## is a two-digit decimal number.

In case no test area, test group, or test unit is defined in [Annex A](#) for the test case, the respective name is omitted from the test case ID.

6.2.4.3 Technology

Functions are defined for identifying which technology (i.e. device engagement and data transfer) in the IUT is to be tested in each scenario. If a test case is applied to only optional functions (e.g. L2CAP), the IUT which does not support such optional functions, the test shall be skipped for IUT.

a. Engagement and Data Transfer Technologies

[mDL]	mdoc supporting doctype org.iso.18013.5.1.mDL
[QR-NFC]	Device engagement with QR code/Data Transfer with NFC
[QR-BLE]	Device engagement with QR code/Data Transfer with BLE Peripheral Server mode
[QR-WiFiAware]	Device engagement with QR code/Data Transfer with WiFi Aware
[QR-WebAPI]	Device engagement with QR code/Server retrieval Token with WebAPI
[QR-OIDC]	Device engagement with QR code/Server retrieval Token with OIDC
[NFC-NFC]	Device engagement with NFC/Data Transfer with NFC
[NFC-BLE]	Device engagement with NFC/Data Transfer with BLE
[NFC-WiFiAware]	Device engagement with NFC/Data Transfer with WiFi Aware
[NFC-WebAPI]	Device engagement with NVC/Server retrieval Token with WebAPI
[NFC-OIDC]	Device engagement with QR NFC/Server retrieval Token with OIDC

b. Security mechanisms

[SEC-MSO]	Issuer data authentication
[SEC-DSA]	mdoc ECDSA/EdDSA authentication
[SEC-MAC]	mdoc MAC authentication
[SEC-RA]	Reader authentication

6.2.4.4 Profile

Profiles are defined for identifying optional functionality in the IUT. If a profile is present in a test case, this impacts the applicability of that test case. This enables the tester or the automated test apparatus to select which tests should be executed to the IUT. This selection is based upon comparing the profile of the test case to the IUT information in the ICS filled out by the applicant or tester (also see [6.3.3](#)).

If no profile is listed in a test case, the test case shall be executed on all implementations under test. If one or more profiles are specified and the IUT does not match with all of the specified profiles, the test shall be skipped for that IUT and shall be marked as Not Applicable in the test report.

6.2.4.5 Preconditions

Preconditions define the state in which the IUT needs to be before the test case can be executed. Preconditions can apply, among others, to:

- any action that must have taken place, such as successful device engagement;
- conditions that must be fulfilled, for example correct CBOR encoding of a tested device retrieval request or response;
- the presence of a certain CA certificate as a trust point in the IUT;
- the availability, in the test apparatus, of certain end-entity certificates and associated private keys.

If the preconditions listed in the test case cannot be fulfilled during test execution, test execution shall be skipped, and the test case shall be marked as Inconclusive in the test report.

6.3 Test administration

6.3.1 Preconditions for testing of an mDL

6.3.1.1 Preparation, personalisation, and configuration of the mDL

Before testing can begin, the mDL under test shall be prepared. It is very likely that the mDL under test takes the form of an application intended to be installed on a generic-purpose mobile device. If so, the mDL application under test is installed on a suitable test device, whose hardware and software supports all technology options that must be tested for the mDL application under test according to the ICS. Any action needed to install the mDL application under test is proprietary.

NOTE The term "mDL application" is not used in ISO/IEC 18013-5. The standard does not make a distinction between the different elements that make up an mDL, such as the mobile device, the application residing on that device, the document(s) within that application and the data associated with each document. Many requirements in the standard can only be complied with by several of these elements in combination. However, for the purposes of testing a distinction is made between the mDL application, the data within that application, and the mobile device on which it resides. This is because the mDL application and the data within it form the implementation under test, whereas the mobile device is part of test apparatus.

After installation, the new mDL application instance needs to be configured and personalised:

- Configuration means setting the functional properties of the mDL instance under test. Configuration of an mDL application instance is proprietary. It is up to the tester, possibly in cooperation with the applicant, to perform this correctly for the given mDL application.

EXAMPLE 1 If the mDL application supports multiple curves for session encryption, the curve to be used by this application instance under test must be configured. It is not possible to use multiple curves simultaneously.

EXAMPLE 2 If the mDL application supports both QR code and NFC for device engagement, the mDL application instance must be configured to use either QR code or NFC, unless the application allows the tester to change this during testing. Similarly, if NFC is used, the application instance must be configured to use either Static Handover or Negotiated Handover, since these options cannot be supported simultaneously.

- Personalisation means providing the new application instance with the correct mDL data, including cryptographic keys and certificates. The mDL tests in this document require a fully personalized mDL. This means that all mandatory data elements shall be present as a minimum. In addition, the mDL shall be personalised with all data, cryptographic keys and certificates required to test the mandatory features specified in ISO/IEC 18013-5, as well as all optional features declared in the ICS according to [6.3.3](#). Personalisation of an mDL application is not standardized in ISO/IEC 18013-5. It is up to the tester, possibly in cooperation with the applicant, to perform this correctly.

6.3.1.2 Installing the CA root certificates for mdoc reader authentication in the mDL under test

If the mdoc reader authentication security mechanism must be tested, the mDL under test needs to verify a mdoc reader authentication certificate presented by the test apparatus. To be able to do this, the mDL needs the public key in the CA root certificate that was used to sign this mdoc reader authentication certificate.

Annex C gives an overview of all CA root certificates that are used in the test cases for mdoc reader authentication. The applicant, possibly in cooperation with the tester, shall make sure that all of the certificates (or at least the relevant information extracted from these certificates) from [Annex C](#) are present in the mDL under test as trust points. How this can be done is proprietary for each mDL under test.

6.3.1.3 Installing the IACA root certificates for issuer data authentication in the test apparatus

As part of testing the issuer data authentication security mechanism, the test apparatus (see [6.3.1.4](#)) needs to verify one or more DS certificates presented by the mDL under test. To be able to do this, the test apparatus needs the public key(s) in the IACA root certificate(s) that were used to sign these DS certificates.

The applicant shall provide the necessary IACA root certificate(s) to the tester. The tester shall ensure that all of these IACA root certificate(s) are present in the test apparatus as trust points. How this can be done is proprietary for each test apparatus.

6.3.1.4 Test apparatus

[Figure 2](#) gives an overview of the test apparatus that is assumed to be present for testing an mDL.

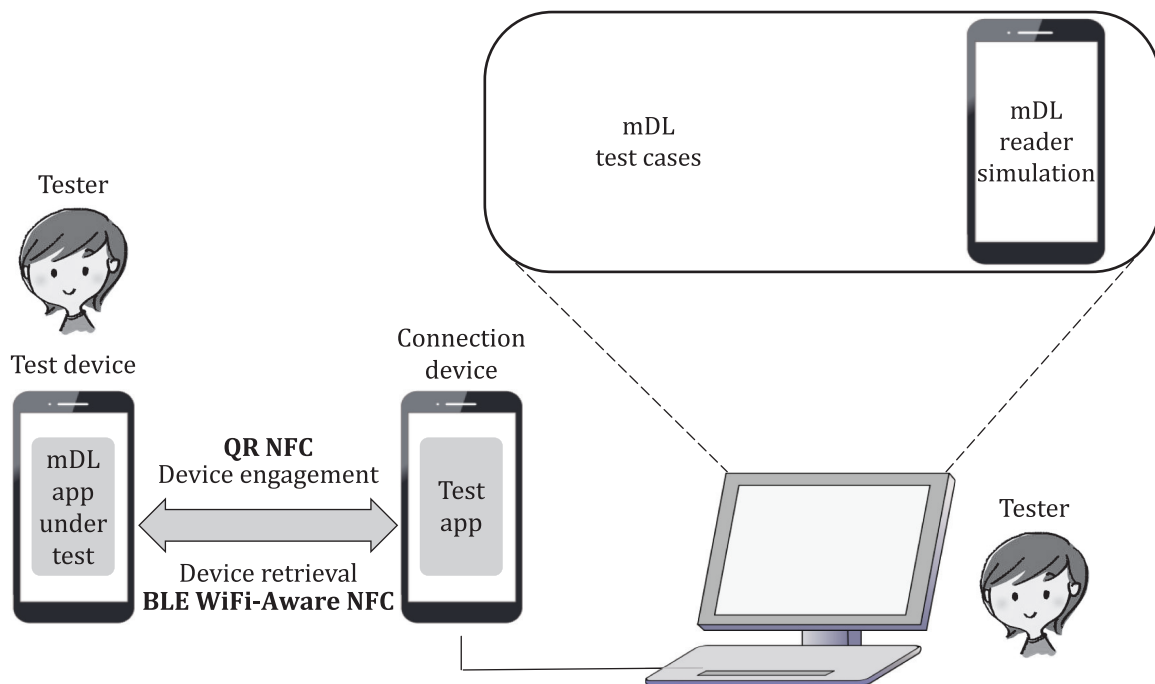


Figure 2 — Test Apparatus for testing an mDL

In order to allow testing, the mDL application under test is installed on a suitable test device. This test device shall comply with the (minimum) requirements set by the applicant for the mDL application under test. In particular, it shall support all communication technologies for device engagement (either QR code or NFC, or both) and device retrieval (BLE, Wi-Fi Aware, NFC, or all) that must be tested for the mDL application under test.

The test device should preferably be provisioned by the tester. To ensure that test results are representative for all possible mobile devices on which the mDL application will be used in practice, the tester should carefully choose the test device. To increase representativeness, the tester may consider installing the mDL

application under test on multiple test devices, each having different characteristics regarding, for example, hardware and OS version, and running all test cases on all of these.

NOTE 1 In the above, it is assumed that the mDL under test is implemented as an application intended to be installed on a generic mobile device. It is theoretically possible that the applicant implemented the mDL as one device, including both hardware and software. In such a case, no test device is necessary.

Communication to the mDL application is performed by means of a connection device, which is often a mobile device supporting the necessary communication technologies. A dedicated test app on the connection device connects to a computer, which runs an mDL reader simulation. The mDL reader simulation shall be capable of executing the mDL test cases specified in Appendix 2 to this document, which has been published as a separate document, and of reporting on the results of each test case towards a human tester.

NOTE 2 The mDL reader simulation can also be implemented in the test app running on the connection device. In that case, no separate computer is needed.

The human tester shall be responsible for determining which test cases are run, based on the ICS provided by the mDL application manufacturer and by the profile information in each test case; see [6.3.3](#). The tester shall also be responsible for interpreting the results of each test case to arrive at a verdict, see [6.3.4](#).

NOTE 3 Both of these tasks can be automated in the mDL reader simulation. However, even if this is the case, the tester bears the end responsibility for ensuring that these tasks are performed correctly.

Finally, the human tester also interacts directly with the mDL application under test, for example when performing device engagement and when giving consent to share mDL data.

6.3.2 Preconditions for testing of an mDL reader

6.3.2.1 Preparation, personalisation and configuration

Before testing can begin, the mDL reader under test shall be prepared. The mDL reader may take the form of an application intended to be installed on a generic-purpose mobile device. In that case, the application is installed on a suitable test device, whose hardware and software support all technology options that are tested for the mDL reader under test. If the mDL reader under test integrates both hardware and software, this step is not needed. In any case, any action to install the mDL reader under test is proprietary.

After installation, the mDL reader needs to be configured and personalised:

- Configuration means setting the functional properties of the mDL reader. The way in which an mDL reader can be configured is proprietary. It is up to the tester, possibly in cooperation with the applicant, to perform this correctly for the given mDL reader.

EXAMPLE If the mDL reader under test supports multiple curves for mdoc reader authentication, the curve to be used by this mDL reader instance must be configured. It is not possible to support multiple curves simultaneously.

- Personalisation means providing the reader with the correct cryptographic keys and certificates. The mDL reader under test shall be equipped with all data, cryptographic keys and certificates required to test the mandatory features specified in ISO/IEC 18013-5, as well as all optional features declared in the ICS according to [6.3.3](#). Personalisation of an mDL reader is not standardized in ISO/IEC 18013-5. It is up to the tester, possibly in cooperation with the applicant, to perform this correctly.

6.3.2.2 Installing the IACA root certificates for issuer data authentication, TLS server authentication and JWS in the mDL reader

For testing the issuer data authentication security mechanism, the mDL reader under test needs to verify a DS certificate presented by the test apparatus. To be able to do this, the mDL reader needs the public key in the IACA root certificate that was used to sign this DS certificate.

Similarly, for testing the TLS server authentication and JWS security mechanisms, the mDL reader needs the IACA root certificate that was used to sign the TLS server authentication and JWS signer certificates presented by the test apparatus.

[C.3.1](#) gives an overview of all IACA root certificates that are used in the test cases for issuer data authentication, TLS and JWS. The applicant or the tester shall make sure that all of these certificates (or at least the relevant information extracted from these certificates) are present in the mDL reader under test as trust points. How this can be done is proprietary for each mDL reader under test.

6.3.2.3 Installing the CA root certificates for mdoc reader authentication and TLS client authentication in the test apparatus

If the mdoc reader authentication security mechanism must be tested, the test apparatus needs to verify one or more mdoc reader authentication certificates presented by the mDL reader under test. To be able to do this, the test apparatus needs the public key(s) in the CA root certificate(s) that were used to sign these certificates.

Similarly, if the TLS client authentication security mechanism must be tested, the test apparatus needs to verify one or more TLS client authentication certificates presented by the mDL reader under test using the public key in the associated CA root certificate.

The applicant shall provide the necessary IACA root certificate(s) to tester. The test shall ensure that all of these IACA root certificate(s) are present in the test apparatus as trust points. How this can be done is proprietary for each test apparatus.

6.3.2.4 Test apparatus

[Figure 3](#) gives an overview of the test apparatus that is assumed to be present for testing an mDL reader:

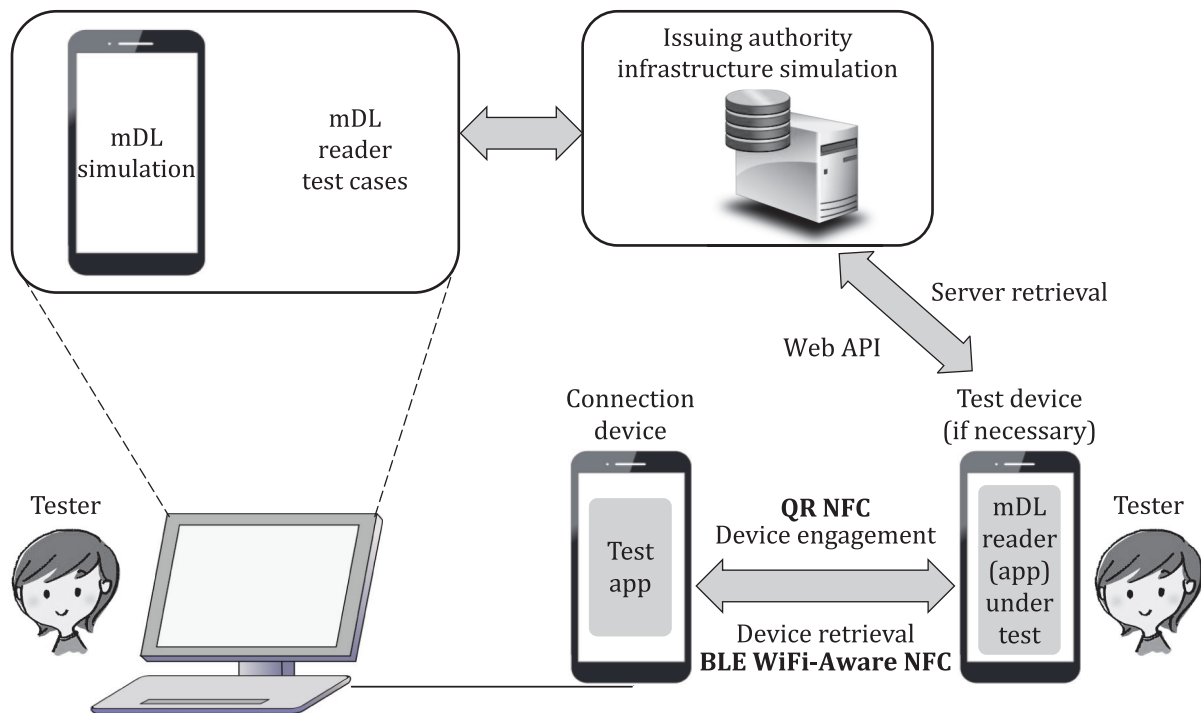


Figure 3 — Test apparatus for testing an mDL reader

If the mDL reader is implemented as an application intended to be installed on a generic mobile device, the mDL reader application under test is installed on a suitable test device. This test device shall comply with the (minimum) requirements set by the applicant for the mDL reader application under test. In particular, it shall support all communication technologies for device engagement (QR code, NFC, or both) and device retrieval (BLE, Wi-Fi Aware, NFC, or any of them) that must be tested for the mDL reader application under test.

The test device should preferably be provisioned by the tester. To ensure that test results are representative for all possible mobile devices on which the mDL reader application will be used in practice, the tester should carefully choose the test device. To increase representativeness, the tester may consider installing the mDL reader application under test on multiple test devices, each having different characteristics regarding, for example, hardware and OS version, and running all test cases on all of these.

NOTE 1 In the above, it is assumed that the mDL reader under test is implemented as an application intended to be installed on a generic mobile device. It is possible that the applicant implemented the mDL reader as one device, including both hardware and software. In such a case, no test device is necessary.

For testing device retrieval, communication to the mDL reader is performed by means of a connection device, which is a (mobile) device supporting the necessary communication technologies. A dedicated test app on the connection device connects to a computer, which runs an mDL simulation. The mDL simulation shall be capable of executing the mDL reader test cases for device retrieval specified in Appendix 3 to this document, and of reporting on the results of each test case towards a human tester.

NOTE 2 The mDL simulation may also be implemented in the test app running on the connection device. In that case, no separate computer is needed.

For testing server retrieval, communication to the mDL reader under test is performed by means of a web server connected to a computer running an issuing authority infrastructure simulation. The issuing authority infrastructure simulation shall be capable of executing the mDL reader test cases for server retrieval specified in Appendix 3 of this document, and of reporting on the results of each test case towards a human tester.

NOTE 3 A server retrieval transaction involves both an mDL and an issuing authority infrastructure. A single computer will typically run both simulations.

The human tester shall be responsible for determining which test cases are run, based on the ICS provided by the mDL reader manufacturer and by the profile information in each test case; see [6.3.3](#). The tester shall also be responsible for interpreting the results of each test case to arrive at a verdict, see [6.3.4](#).

NOTE 4 Both of these tasks can be automated in the mDL simulation or issuing authority infrastructure simulation. However, even if this is the case, the tester bears the end responsibility for ensuring that these tasks are performed correctly.

Finally, the human tester also interacts directly with the mDL reader under test, for example when performing device engagement, to instruct the mDL reader to request data elements from the simulated mDL or issuing authority, or to verify (via the mDL reader's user interface) that the reader performed some actions correctly.

6.3.3 Implementation conformance statements

ISO/IEC 18013-5 specifies a large number of options that an IUT may or may not support, or for which a choice needs to be made. An ICS is used to specify if the IUT supports these options and which choices are made. For each IUT, the applicant for conformity testing shall complete the relevant ICS:

- The ICS for mDLs is specified in [B.1](#).
- The ICS for mDL readers is specified in [B.2](#).
- The ICS for certificates is specified in [B.3](#).

NOTE The ICS for certificates is only used when independently testing a certificate stored in a file.

The applicant shall complete the ICS for each implementation under test separately. The tester (or the automated test apparatus) shall use the information in the completed ICS to determine which test cases are applicable for the IUT; see [6.2.4](#).

It can be necessary for the applicant to prepare several IUTs in order to fully test an mDL or mDL reader. For example, an mDL application can support multiple elliptic curves for the session encryption mechanism. However, when that application is installed on a mobile device, one particular curve must be chosen, since it

is not possible to include multiple public keys in the device engagement structure sent to the mDL reader. In such a case, the session encryption mechanism shall be tested using multiple IUTs. For each IUT, a different curve shall be configured during installation, and the tester shall set the ICS correspondingly. All test cases for session encryption shall then be executed on each of the IUTs. Similar considerations apply to testing most of the security mechanisms. They can also apply to other ICS options; for example, see NOTE in [6.3.1.1](#).

6.3.4 Test report

Detailed test results and ICS information shall be recorded for reference in a test report. The test report shall contain the test result of each test case and test step.

If one of the profiles in the test case is not matched by the IUT, the result of the test case is Not Applicable. The tester and the applicant shall perform a plausibility check on all test cases with a Not Applicable result, to verify that no error has been made during completion of the ICS and application of the ICS to the test case.

If one of the preconditions in the test case cannot be fulfilled, the result of the test case is inconclusive. The applicant and the tester shall determine which actions need to be taken to ensure that the preconditions are fulfilled in a next test run for the IUT.

The test result for an executed test case can be:

- Pass: if all obtained results from the IUT match the expected results declared for each test step in the test case; or
- Fail: if one or more of the obtained results from the IUT do not match the expected results declared in a test step; or
- Not Applicable: if the test case is not applicable for the IUT, based on the Profile in the test case and the ICS information for the IUT.

7 mDL conformity test methods

Conformity testing of mDL implementations to ISO/IEC 18013-5 is performed by executing the applicable mDL test cases specified in Appendix 2 to this document, which is published as a separate document.

NOTE When executing the applicable test cases in Appendix 2, also applicable common test cases and certificate test cases from Appendix 1 will be executed by reference.

8 mDL reader conformity test methods

Conformity testing of mDL reader implementations to ISO/IEC 18013-5 is performed by executing the applicable mDL reader test cases specified in Appendix 3 to this document, which is published as a separate document.

NOTE When executing the applicable test cases in Appendix 3, also applicable common test cases and certificate test cases from Appendix 1 are executed by reference.

Annex A
(normative)

Test case hierarchies

A.1 mDL

[Table A.1](#) describes the test unit structure for mDL tests cases.

Table A.1 — Test unit structure for mDL test cases

Test layer	Test area	Test group	Test unit
Data Model (DM)			
	FamilyName		
	GivenName		
	BirthDate		
	IssueDate		
	ExpiryDate		
	IssuingCountry		
	IssuingAuthority		
	DocumentNumber		
	Portrait		
	DrivingPrivileges		
	UNDistinguishingSign		
	AdministrativeNumber		
	Sex		
	Height		
	Weight		
	EyeColour		
	HairColour		
	BirthPlace		
	ResidentAddress		
	PortraitCaptureDate		
	AgeInYears		
	AgeBirthYear		
	AgeOverNN		
	IssuingJurisdiction		
	Nationality		
	ResidentCity		
	ResidentState		
	ResidentPostalCode		
	ResidentCountry		
	BiometricTemplateXX		
	FamilyNameNationalCharacter		
	GivenNameNationalCharacter		