Technical Specification

ISO/IEC TS 18013-6

First edition
2024-11

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

Reference number
ISO/IEC TS 18013-6:2024(en)

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

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.

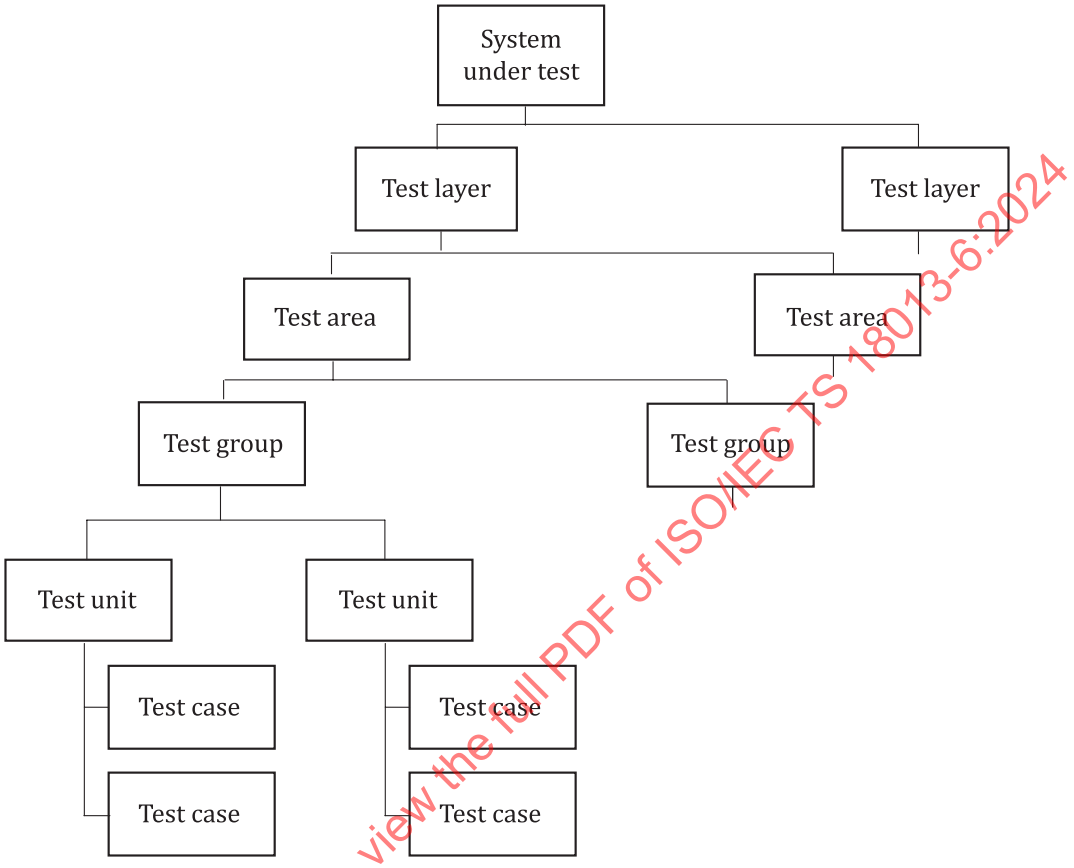

Figure 1 — Test element hierarchy

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	Defines the test steps that shall be taken. 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. Each test step is defined by the following information: — 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.

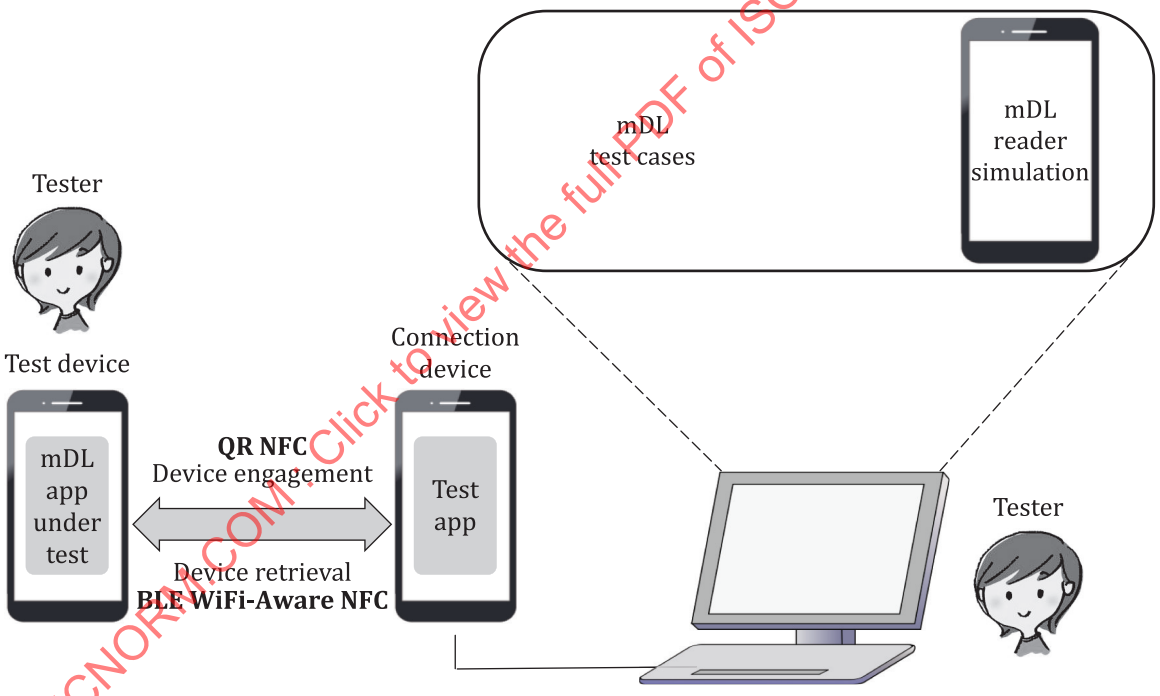

Figure 2 — Test Apparatus for testing an mDL

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 seperate 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:

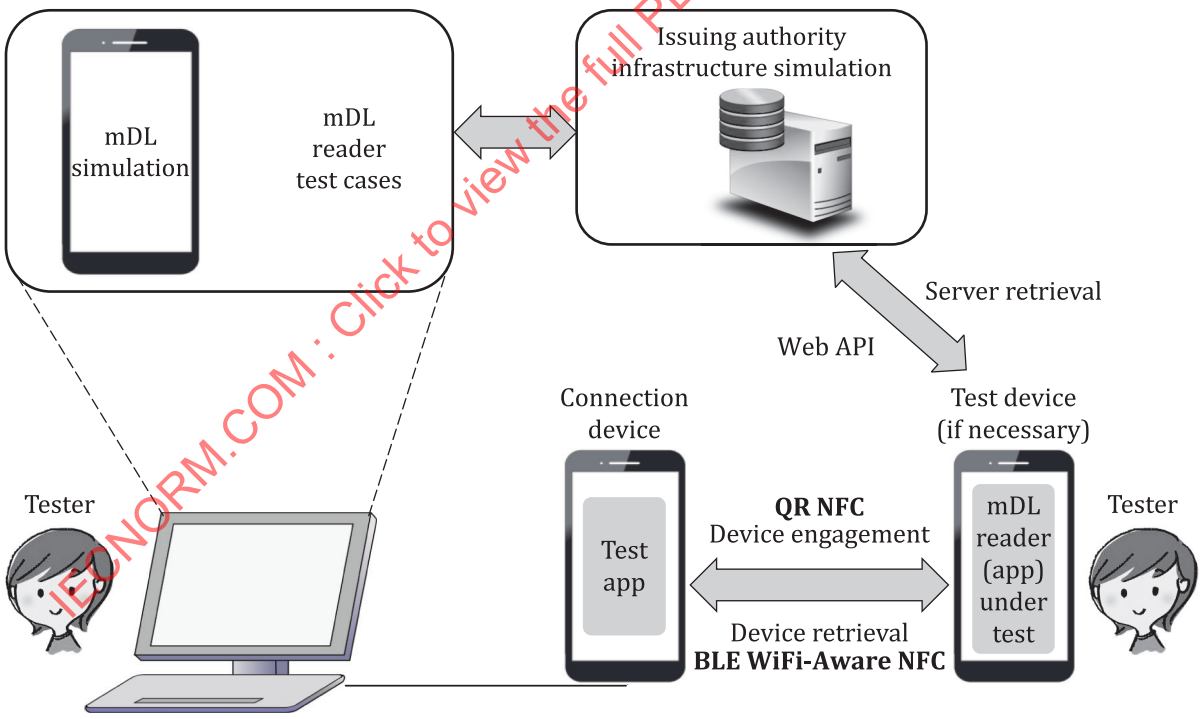

Figure 3 — Test apparatus for testing an mDL reader

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		

Table A.1 *(continued)*

Test layer	Test area	Test group	Test unit
	SignatureUsualMark		
MessageStructure (MS)			
	DeviceEngagement (DE)		
		General (Gen)	
		DataRetrievalNFC (DRNFC)	
		DataRetrievalBLE (DRBLE)	
		DataRetrievalWiFi (DRWiFi)	
	SessionData (SD)		
	DeviceRequest (DReq)		
	DeviceResponse (DR)		
		HappyFlow (HF)	
			Generic (Gen)
			MobileSecurityObject (MSO)
		UnhappyFlow (UF)	
Technologies (Tech)			
	DeviceEngagement (DE)		
		NFC	
		QRCode (QR)	
	DeviceRetrieval (DR)		
		BLE	
		NFC	
		WiFiAware (WiFi)	
SecurityMechanisms (SM)			
	SessionEncryption (SEnc)		
		DeviceEngagement (DE)	
		SessionEstablishment (SEst)	
			HappyFlow (HF)
			UnhappyFlow (UF)
		SessionData (SD)	
		SessionTermination (ST)	
	IssuerDataAuthentication (IDA)		
	mdocAuthentication (mdocAuth)		
		General	
		MAC	
		ECDSA/EdDSA (ECdDSA)	
	mdocReaderAuthentication (mdocRAuth)		
		HappyFlow (HF)	
		UnhappyFlow (UF)	

Table A.1 *(continued)*

Test layer	Test area	Test group	Test unit
Use Cases			

A.2 mDL reader

Table A.2 describes the test unit structure for mDL reader test cases.

Table A.2 — Test unit structure for mDL reader test cases

Test layer	Test area	Test group	Test unit
MessageStructure (MS)			
	SessionEstablishment (SE)		
	DeviceRequest (DR)		
	ServerRequest (SR)		
		WebAPI	
Technologies (Tech)			
	DeviceEngagement (DE)		
		NFC	
		QRCode (QR)	
	DeviceRetrieval (DR)		
		BLE	
		NFC	
		WiFiAware (WiFi)	
	ServerRetrieval (SR)		
		WebAPI	
	SessionData		
SecurityMechanisms (SM)			
	SessionEncryption (SEnc)		
		DeviceEngagement (DE)	
		SessionEstablishment (SEst)	
		SessionData (SD)	
		SessionTermination (ST)	
	IssuerDataAuthentication (IDA)		
		HappyFlow (HF)	
		UnhappyFlow (UF)	
	mdocAuthentication (mdocAuth)		
		Generic	
			HappyFlow
			UnhappyFlow
		MAC	
			HappyFlow
			UnhappyFlow
		ECDSA/EdDSA (ECdDSA)	
			HappyFlow

Table A.2 *(continued)*

Test layer	Test area	Test group	Test unit
			UnhappyFlow
	mdocReaderAuthentication (mdocRAuth)		
	TLS		
		HappyFlow	
		UnhappyFlow	
	JWS		
		HappyFlow	
		UnhappyFlow	
Use Cases			

A.3 Certificates

Table A.3 describes the test unit structure for certificate test cases.

Table A.3 — Test unit structure for certificate test cases

Test layer	Test area	Test Group
Generic (Gen)		
tbsCertificate (TBS)	Generic (Gen)	
	Version (Ver)	
	SerialNumber (SN)	
	Signature (Sig)	
	Issuer (Iss)	
	Validity (Val)	
	Subject (Sub)	
	SubjectPublicKeyInfo (SPKI)	
	Extensions (Ext)	
		Generic (Gen)
		AuthorityKeyI dentifier (AKI)
		SubjectKeyIdentifier (SKI)
		KeyUsage (KU)
		CertificatePolicies (CP)
		SubjectAlternativeName (SAN)
		IssuerAlternativeName (IAN)
		BasicConstraints (BC)
		ExtendedKeyUsage (EKU)
		CRLDistributionPoints (CDP)
		AuthorityInformationAccess (AIA)
		RevocationCheckingOfAnAuthorizedResponder (RCOAAR)
SignatureAlgorithm (SA)		
SignatureValue (SV)		

A.4 Common

Table A.4 describes the test case hierarchy of common test cases.

Table A.4 — Test unit structure of mDL common test cases

Test layer	Test area	Test group	Test unit
CBOR			
Cert_CRL_Time			
COSE_Key			
COSE_Sign1			
COSE_MAC0			
JSON			
JWT_JWS			

Annex B
(informative)

Implementation conformance statements

B.1 ICS for mdocs

B.1.1 Generic information

ICS statements in Table B.1 are based on Clauses 8 and 9 of ISO/IEC 18013-5.

NOTE Hence these statements use "mdoc" rather than "mDL".

Table B.1 — ICS for generic information for mdoc

#	Implementation Conformance Statement	Value
1	How many documents are present on the mdoc under test?	
2	For each document, please specify the applicable DocType.	
3	For each document, please specify all namespaces used by the document.	
4	For each namespace different from the mDL namespace ("org.iso.18013.5.1"), please specify the identifiers of all data elements present on the document.	

B.1.2 For mDL Data Model test cases

All of the data elements in this subclause are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in Table B.2 shall be filled in only for mDLs, i.e. mobile documents having DocType = "org.iso.18013.5.1.mDL".

Table B.2 — ICS for mDL Data Model test cases

#	Implementation Conformance Statement	Value
5	Data element administrative_number is present in the mDL data.	Yes/No
6	Data element sex is present in the mDL data.	Yes/No
7	Data element height is present in the mDL data.	Yes/No
8	Data element weight is present in the mDL data.	Yes/No
9	Data element eye_colour is present in the mDL data.	Yes/No
10	Data element hair_colour is present in the mDL data.	Yes/No
11	Data element birth_place is present in the mDL data.	Yes/No
12	Data element resident_address is present in the mDL data.	Yes/No
13	Data element portrait_capture_date is present in the mDL data.	Yes/No
14	Data element age_in_years is present in the mDL data.	Yes/No
a) EXAMPLE The following set complies with the above rules: age_over_15 = TRUE (NN1 = 15) age_over_18 = TRUE (NN2 = 18) age_over_21 = TRUE (NN3 = 21) age_over_60 = FALSE (NN4 = 60) age_over_65 = FALSE (NN5 = 65) age_over_68 = FALSE (NN6 = 68)		

Table B.2 *(continued)*

<table>
<tr><th>#</th><th>Implementation Conformance Statement</th><th>Value</th></tr>
<tr><td>15</td><td>Data element age_birth_year is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>16</td><td>Data element age_over_NN is present in the mDL data.
In case you select YES, please provide six (6) age_over_NN data elements in the mDL data, of which three (3) lower NN values with the value TRUE and three (3) higher values with the value FALSE. Please make sure the set of age_over_NN data elements is consistent. List the values for NN1 – NN6 present in the mDL data.
<table><tr><th>Value for NN in data element identifier</th><th>Value (TRUE / FALSE)</th></tr><tr><td>age_over_NN1(L)</td><td>TRUE</td></tr><tr><td>age_over_NN2(L)</td><td>TRUE</td></tr><tr><td>age_over_NN3(L)</td><td>TRUE</td></tr><tr><td>age_over_NN4(H)</td><td>FALSE</td></tr><tr><td>age_over_NN5(H)</td><td>FALSE</td></tr><tr><td>age_over_NN6(H)</td><td>FALSE</td></tr></table> a)</td><td>Yes/No
NN1(L):
NN2(L):
NN3(L):
NN4(H):
NN5(H):
NN6(H):</td></tr>
<tr><td>17</td><td>Data element issuing_jurisdiction is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>18</td><td>Data element nationality is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>19</td><td>Data element resident_city is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>20</td><td>Data element resident_state is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>21</td><td>Data element resident_postal_code is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>22</td><td>Data element resident_country is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>23</td><td>Data element biometric_template_face is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>24</td><td>Data element biometric_template_voice is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>25</td><td>Data element biometric_template_finger is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>26</td><td>Data element biometric_template_iris is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>27</td><td>Data element biometric_template_retina is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>28</td><td>Data element biometric_template_hand_geometry is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>29</td><td>Data element biometric_template_signature_sign is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>30</td><td>Data element biometric_template_keystroke is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>31</td><td>Data element biometric_template_lip_movement is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>32</td><td>Data element biometric_template_thermal_face is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>33</td><td>Data element biometric_template_thermal_hand is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>34</td><td>Data element biometric_template_gait is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>35</td><td>Data element biometric_template_body_odor is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>36</td><td>Data element biometric_template_dna is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>37</td><td>Data element biometric_template_ear is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>38</td><td>Data element biometric_template_finger_geometry is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>39</td><td>Data element biometric_template_palm_geometry is present in the mDL data.</td><td>Yes/No</td></tr>
<tr><td>40</td><td>Data element biometric_template_vein_pattern is present in the mDL data.</td><td>Yes/No</td></tr>
</table>

a) EXAMPLE The following set complies with the above rules:

age_over_15 = TRUE (NN1 = 15)
age_over_18 = TRUE (NN2 = 18)
age_over_21 = TRUE (NN3 = 21)
age_over_60 = FALSE (NN4 = 60)
age_over_65 = FALSE (NN5 = 65)
age_over_68 = FALSE (NN6 = 68)

Table B.2 *(continued)*

#	Implementation Conformance Statement	Value
41	Data element biometric_template_foot_print is present in the mDL data.	Yes/No
42	Data element family_name_national_character is present in the mDL data.	Yes/No
43	Data element given_name_national_character is present in the mDL data.	Yes/No
44	Data element signature_usual_mark is present in the mDL data.	Yes/No
a) EXAMPLE The following set complies with the above rules: age_over_15 = TRUE (NN1 = 15) age_over_18 = TRUE (NN2 = 18) age_over_21 = TRUE (NN3 = 21) age_over_60 = FALSE (NN4 = 60) age_over_65 = FALSE (NN5 = 65) age_over_68 = FALSE (NN6 = 68)		

B.1.3 For Technologies test cases

ICS statements described in Table B.3 are based on Clauses 8 and 9 of ISO/IEC 18013-5.

NOTE Hence these statements use "mdoc" rather than "mDL".

Table B.3 — ICS for mdoc Technologies test cases

#	Implementation Conformance Statement	Value
45	mdoc supports device engagement using NFC Static Handover.	Yes/No
46	mdoc supports device engagement using NFC Negotiated Handover.	Yes/No
47	mdoc supports device engagement using QR code.	Yes/No
48	mdoc supports device retrieval using NFC.	Yes/No
49	mdoc supports extended-length APDUs for device retrieval using NFC.	Yes/No
50	mdoc supports BLE version 4.2 (or above) and LE Data Packet Length Extension.	Yes/No
51	mdoc supports device retrieval using BLE in mdoc central client mode.	Yes/No
52	If BLE in mdoc central client mode is used for device retrieval, mdoc verifies the value of the Ident characteristic.	Yes/No
53	mdoc supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE.	Yes/No
54	mdoc supports device retrieval using BLE in mdoc peripheral server mode.	Yes/No
55	mdoc supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE.	Yes/No
56	mdoc supports device retrieval using Wi-Fi Aware.	Yes/No
57	mdoc supports the NCS-PK-2WDH-128 cipher suite for Wi-Fi Aware.[a)]	Yes/No
58	mdoc supports server retrieval using OIDC.	Yes/No
59	mdoc supports server retrieval using WebAPI.	Yes/No
60	mdoc supports transferring server retrieval information in the device engagement structure.	Yes/No
61	mdoc implements a time-out for the time between sending device engagement data and receiving the session establishment message	Yes/No
62	If yes, how many seconds is the time-out period for session termination implemented by the mdoc?	
a) Only applicable in case the mdoc supports Wi-Fi Aware for device retrieval and supports NFC Negotiated Handover for device engagement.		

B.1.4 For Security Mechanisms test cases

ICS statements described in Table B.4 are based on Clauses 8 and 9 of ISO/IEC 18013-5.

NOTE Hence these statements use "mdoc" rather than "mDL".

Table B.4 — ICS for mdoc security mechanisms test cases

#	Implementation Conformance Statement	Value
63	Which curves does the mdoc support for session establishment? Select all that are supported.	Curve P-256 Curve P-384 Curve P-521 X25519 X448 brainpoolP256r1 brainpoolP320r1 brainpoolP384r1 brainpoolP512r1
64	mdoc supports exchanging more than one device retrieval mdoc request and response with the mdoc reader in a single session.	Yes/No
65	If yes, how many seconds is the time-out period for session termination implemented by the mdoc?	
66	Which curves does the issuing authority support for issuer data authentication on this mdoc? Select all that are supported.	Curve P-256 Curve P-384 Curve P-521 Ed25519 Ed448 brainpoolP256r1 brainpoolP320r1 brainpoolP384r1 brainpoolP512r1
67	The mdoc supports mdoc MAC authentication.	Yes/No
68	If yes, which curves does the mdoc support for mdoc MAC authentication? Select all that are supported.	Curve P-256 Curve P-384 Curve P-521 Ed25519 Ed448 brainpoolP256r1 brainpoolP320r1 brainpoolP384r1 brainpoolP512r1
69	The mdoc supports mdoc ECDSA/EdDSA authentication.	Yes/No
70	If yes, which curves does the mdoc support for mdoc ECDSA/EdDSA authentication? Select all that are supported.	Curve P-256 Curve P-384 Curve P-521 X25519 X448 brainpoolP256r1 brainpoolP320r1 brainpoolP384r1 brainpoolP512r1
71	mdoc supports mdoc reader authentication.	Yes/No

a) At least one of ICS #73 and ICS #74 should be answered with Yes. Otherwise, failing reader authentication would not have any consequences.

Table B.4 *(continued)*

#	Implementation Conformance Statement	Value
72	If yes, which curves does the mdoc support for mdoc reader authentication? Select all that are supported.	Curve P-256 Curve P-384 Curve P-521 X25519 X448 brainpoolP256r1 brainpoolP320r1 brainpoolP384r1 brainpoolP512r1
73	If yes, if mdoc reader authentication fails, does the mdoc notify the mdoc holder that the mdoc verifier's identity could not be verified? [a)]	Yes / No
74	If yes, if mdoc reader authentication fails, are there any data elements that the mdoc will not release? If so, please list them all by namespace and identifier.	Yes / No
75	If yes, mdoc supports retrieving OCSP information, if available, when verifying a mdoc reader authentication certificate.	Yes / No
75	A test CRL for all IACA root certificate provided by applicant is available during testing.	Yes / No
76	A test CRL for all Document Signer certificate provided by applicant is available during testing.	Yes / No
a) At least one of ICS #73 and ICS #74 should be answered with Yes. Otherwise, failing reader authentication would not have any consequences.		

B.1.5 For Use Case test cases

The mDL enables the mDL holder to refuse consent for sharing the portrait, but give consent for sharing other data elements requested in the same request. Table B.5 describes ICS for For Use Case test cases.

NOTE The requirement for test case is specified in ISO/IEC 18013-5:2021, E,13,

Table B.5 — ICS for Use Case test cases

#	Implementation Conformance Statement	Value
77	The mDL allows the mDL holder to refuse consent for sharing the portrait data element but give consent for sharing other requested data elements.	Yes / No

B.2 ICS for mdoc readers

B.2.1 Generic information

ICS statements in Table B.6 are based on Clauses 8 and 9 of ISO/IEC 18013-5.

NOTE Hence use "mdoc reader" rather than "mDL reader".

Table B.6 — ICS Generic information for mdoc readers

#	Implementation Conformance Statement	Value
1	Specify which DocType(s) the mdoc reader supports.	
2	For each DocType, specify with namespace(s) the mdoc reader supports.	
3	For each namespace, specify the identifiers of all data elements that can be requested by the mdoc reader.	
4	mdoc reader is able to request multiple documents in a single DeviceRequest message.[a)]	Yes / No
5	mdoc reader is able to request multiple documents in a single ServerRequest message.[b),c)]	Yes / No

a) If this is set to YES, the mDL reader should support at least two different DocTypes.

b) This statement is only applicable if the mDL reader supports server retrieval using WebAPI.

c) If this statement is set to YES, the mDL reader should support at least two different DocTypes.

B.2.2 For Technologies test cases

ICS statements described in Table B.7 are based on Clauses 8 and 9 of ISO/IEC 18013-5.

NOTE hence use "mdoc reader" rather than "mDL reader".

Table B.7 — ICS for mdoc reader Technologies test cases

#	Implementation Conformance Statement	Value
6	mdoc reader supports device engagement using NFC Static Handover.	Yes / No
7	mdoc reader supports device engagement using NFC Negotiated Handover.	Yes / No
8	mdoc reader supports device engagement using QR code.	Yes / No
9	mdoc reader supports device retrieval using NFC.	Yes / No
10	mdoc reader supports device retrieval using BLE in mdoc central client mode.	Yes / No
11	mdoc reader supports device retrieval using BLE in mdoc peripheral server mode.	Yes / No
12	mdoc reader supports device retrieval using BLE version 5.0 (or above) LE 2M PHY.	Yes / No
13	mdoc reader supports device retrieval using Wi-Fi Aware.	Yes / No
14	mdoc reader supports server retrieval using OIDC.	Yes / No
15	mdoc reader supports server retrieval using WebAPI.	Yes / No
16	mdoc reader supports extended length APDUs for device retrieval using NFC.	Yes / No
17	mdoc reader supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE.	Yes / No
18	mdoc reader supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE.	Yes / No
19	mdoc reader sends a ReaderEngagement structure as part of the Handover Request Message during device engagement using NFC Negotiated Handover	Yes / No
20	mdoc reader implements a time-out for the time between the transaction initialisation and receiving device engagement data.	Yes / No
21	If yes, indicate how long is the time-out (in seconds).	
22	mdoc reader implements a time-out for the time between receiving device engagement data and the successful set-up of a device retrieval connection.	Yes / No
23	If yes, indicate how long is the time-out (in seconds).	

B.2.3 For Security Mechanisms test cases

ICS statements described in Table B.8 are based on Clauses 8 and 9 of ISO/IEC 18013-5.

NOTE Hence these statements use "mdoc reader" rather than "mDL reader".

Table B.8 — ICS for mdoc reader security mechanisms test cases

#	Implementation Conformance Statement	Value
24	mdoc reader supports mdoc reader authentication	Yes / No
25	If yes, a test CRL for all mdoc reader authentication certificates used by the mdoc reader is available during testing.	Yes / No
26	If yes, the CA that signed all mdoc reader authentication certificates used by the mdoc reader has an OCSP service.	Yes / No
27	If yes, a test OCSP Responder for all mdoc reader authentication certificates used by the mdoc reader is available during testing.	Yes / No
28	If yes, which curve does the mdoc reader use for mdoc reader authentication? Select one.	Curve P-256 Curve P-384 Curve P-521 Ed25519 Ed448 brainpoolP256r1 brainpoolP320r1 brainpoolP384r1 brainpoolP512r1
29	mdoc reader supports exchanging more than one device retrieval mdoc request and response with the mdoc in a single session.	Yes / No
30	mdoc reader supports exchanging more than one server retrieval request and response with the issuing authority infrastructure in a single session.	Yes / No
31	mdoc reader supports retrieving OCSP information, if available, when verifying a TLS server certificate.[a)]	Yes / No
32	mdoc reader requests OCSP status information for the server certificate in the TLS handshake.[a)]	Yes / No
33	mdoc reader supports TLS v1.3.[a)]	Yes / No
34	mdoc reader supports TLS Client Authentication.[b)]	Yes / No
35	If yes, a test CRL for all TLS Client certificates used by the mdoc reader is available during testing.	Yes / No
36	If yes, the CA that signed all TLS Client certificates used by the mdoc reader has an OCSP service.	Yes / No
37	If yes, a test OCSP Responder for all TLS Client certificates used by the mdoc reader is available during testing.	Yes / No
38	How many seconds is the time-out period for session termination implemented by the mdoc reader?	

a) This statement is only applicable if the mdoc reader supports server retrieval using WebAPI.

b) This statement is only applicable if the mdoc reader supports mdoc reader authentication.

B.3 ICS for Certificates

Table B.9 describes ICS for certificates.

Table B.9 — ICS for certificates

#	Implementation Conformance Statement	Value
1	What is the certificate type? Select one.	IACA root IACA link Document Signer (DS) JWS Signer TLS Server TLS Client mdoc reader authentication OCSP Signer VICAL Signer
2	The CA that signed this certificate has an OCSP service.	Yes / No
3	If yes, a test OCSP Responder for this certificate is available during testing.	Yes / No
4	A test CRL for this certificate is available during testing.	Yes / No

Annex C
(normative)

Test certificates

C.1 General

All certificates specified in this Annex are X.509 certificates in accordance with Annex B in ISO/IEC 18013-5:2021. The tables below give only the value of the certificate fields whose values are not determined fully by ISO/IEC 18013-5. Values between double angle brackets (<< >>) shall be specified by the tester prior to testing.

C.2 Certificates necessary for testing an mDL

C.2.1 CA root certificates

C.2.1.1 Certificate origin and usage

The root CA certificates defined in this clause, as well as the associated key pairs, shall be generated by the tester prior to testing. During testing, these CA certificates shall be present in an mDL under test as trust points for mdoc reader authentication, if this security mechanism is supported by the mDL under test. Please refer to 6.3.1.2 for more information.

The private keys associated with the public keys in these certificates shall only be used by the tester to sign mdoc reader authentication certificates as defined in C.2.2.

C.2.1.2 CA_01

Table C.1 describes the profile of IACA root certificate using curve Curve P-521. Used for signing the following certificates:

— mdocReaderAuth_01

— mdocReaderAuth_02

— mdocReaderAuth_03

— mdocReaderAuth_04

— mdocReaderAuth_05

Table C.1 — CA_01 certificate profile

Issuer	CN = “Test Root CA cert 1 for mDL”, O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation’s country>>, ST = <<code for issuing organisation’s state or province>>
Subject	Identical to issuer field
Subject public key info parameters (OID)	1.3.132.0.35 (Curve P-521)
IssuerAltName (URI)	“https://www.iso.org”
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

NOTE ISO/IEC 18013-5 specifies that the CA certificate that signs an mdoc reader authentication certificate does not have to be an IACA certificate as specified in B.1.1. However, this document uses the IACA certificate profile for all CA certificates, for lack of any other suitable pre-defined profile.

C.2.1.3 CA_02

Table C.2 describes the profile of IACA root certificate using curveBrainpoolP512r1. Used for signing the following certificates:

— mdocReaderAuth_06

— mdocReaderAuth_07

— mdocReaderAuth_08

— mdocReaderAuth_09

Table C.2 — CA_02 certificate profile

Issuer	CN = "Test Root CA cert 2 for mDL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject	Identical to Issuer field
Subject public key info. parameters (OID)	1.3.36.3.3.2.8.1.1.13 (BrainpoolP512r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.1.4 CA_ revoked_CRL_01

Table C.3 describes the profile of CA root certificate using Curve P-521 that is revoked by putting it on the CRL. Used for signing the following certificates:

— mdocReaderAuth_revoked_CA_01

— mdocReaderAuth_revoked_CA_02

— mdocReaderAuth_revoked_CA_03

— mdocReaderAuth_revoked_CA_04

— mdocReaderAuth_revoked_CA_05

Table C.3 — CA_revoked_CRL_01 certificate profile

Issuer	CN = "Test Root CA cert 1 for mDL revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject	Identical to Issuer field
Subject public key info parameters (OID)	1.3.132.0.35 (Curve P-521)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.1.5 CA_ revoked_CRL_02

Table C.4 describes the profile of CA root certificate using Curve P-521 that is revoked by putting it on the CRL. Used for signing the following certificates:

— mdocReaderAuth_revoked_CA_06

— mdocReaderAuth_revoked_CA_07

— mdocReaderAuth_revoked_CA_08

— mdocReaderAuth_revoked_CA_09

Table C.4 — CA_revoked02 certificate profile

Issuer	CN = "Test Root CA cert 2 for mDL revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject	Identical to Issuer field
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.13 (BrainpoolP512r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2 mdoc reader authentication certificates

C.2.2.1 Certificate origin and usage

The mdoc reader authentication certificates defined in this clause, as well as the associated key pairs, shall be generated by the tester. These certificates shall be exclusively used to test the correctness of the mdoc reader authentication implementation of the mDL under test, as specified in the test cases in Appendix 2 of this document, which has been published as a seperate document.

The corresponding private keys shall be present in the test apparatus during testing. The test apparatus shall use them to perform mdoc reader authentication by signing the ReaderAuthentication structure in the mdoc requests sent to the mDL under test.

C.2.2.2 mdocReaderAuth_01

Table C.5 describes the profile of mdoc reader authentication certificate using Curve P-256.

Table C.5 — mdocReaderAuth_01 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 1", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.7 (Curve P-256)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "good". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.3 mdocReaderAuth_02

Table C.6 describes the profile of mdoc reader authentication certificate using Curve P-384.

Table C.6 — mdocReaderAuth_02 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 2", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.34 (Curve P-384)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "good". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.4 mdocReaderAuth_03

Table C.7 describes the profile of mdoc reader authentication certificate using Curve P-521.

Table C.7 — mdocReaderAuth_03 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 3", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.35 (Curve P-521)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "good". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.5 mdocReaderAuth_04

Table C.8 describes the profile of mdoc reader authentication certificate using curve Ed25519.

Table C.8 — mdocReaderAuth_04 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 4", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.101.112 (Ed25519)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "good". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.6 mdocReaderAuth_05

Table C.9 describes the profile of mdoc reader authentication certificate using curve Ed448.

Table C.9 — mdocReaderAuth_05 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 5", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.101.113 (Ed448)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "good". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.7 mdocReaderAuth_06

Table C.10 describes the profile of mdoc reader authentication certificate using curve BrainpoolP256r1.

Table C.10 — mdocReaderAuth_06 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 6", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.7 (BrainpoolP256r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "good". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.8 mdocReaderAuth_07

Table C.11 describes the profile of mdoc reader authentication certificate using curve BrainpoolP320r1.

Table C.11 — mdocReaderAuth_07 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 7", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.9 (BrainpoolP320r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "good". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.9 mdocReaderAuth_08

Table C.12 describes the profile of mdoc reader authentication certificate using curve BrainpoolP384r1.

Table C.12 — mdocReaderAuth_08 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 8", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.11 (BrainpoolP384r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "good". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.10 mdocReaderAuth_09

Table C.13 describes the profile of mdoc reader authentication certificate using curve BrainpoolP512r1.

Table C.13 — mdocReaderAuth_09 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 9", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.13 (BrainpoolP512r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "good". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.11 mdocReaderAuth_revoked_CRL_01

Table C.14 describes the profile of mdoc reader authentication certificate using Curve P-256 that is revoked by putting it on the CRL

Table C.14 — mdocReaderAuth_revoked_CRL_01 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 1 revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.2.840.10045.3.1.7 (Curve P-256)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.12 mdocReaderAuth_revoked_CRL_02

Table C.15 describes the profile of mdoc reader authentication certificate using Curve P-384 that is revoked by putting it on the CRL

Table C.15 — mdocReaderAuth_revoked_CRL_02 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 2 revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
https://www.iso.org parameters (OID)	1.3.132.0.34 (Curve P-384)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.13 mdocReaderAuth_revoked_CRL_03

Table C.16 describes the profile of mdoc reader authentication certificate using Curve P-521 that is revoked by putting it on the CRL

Table C.16 — mdocReaderAuth_revoked_CRL_03 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 3 revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.35 (Curve P-521)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.14 mdocReaderAuth_revoked_CRL_04

Table C.17 describes the profile of mdoc reader authentication certificate using curve Ed25519 that is revoked by putting it on the CRL

Table C.17 — mdocReaderAuth_revoked_CRL_04 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 4 revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.101.112 (Ed25519)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.15 mdocReaderAuth_revoked_CRL_05

Table C.18 describes the profile of mdoc reader authentication certificate using curve Ed448 that is revoked by putting it on the CRL

Table C.18 — mdocReaderAuth_revoked_CRL_05 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 5 revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.101.113 (Ed448)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.16 mdocReaderAuth_revoked_CRL_06

Table C.19 describes the profile of mdoc reader authentication certificate using curve BrainpoolP256r1 that is revoked by putting it on the CRL

Table C.19 — mdocReaderAuth_revoked_CRL_06 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 6 revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.7 (BrainpoolP256r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.17 mdocReaderAuth_revoked_CRL_07

Table C.20 describes the profile of mdoc reader authentication certificate using curve BrainpoolP320r1 that is revoked by putting it on the CRL

Table C.20 — mdocReaderAuth_revoked_CRL_07 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 7 revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.9 (BrainpoolP320r1)
IssuerAltName (URI)	"https://www.iso.org/standard/79805.htm"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.18 mdocReaderAuth_revoked_CRL_08

Table C.21 describes the profile of mdoc reader authentication certificate using curve BrainpoolP384r1 that is revoked by putting it on the CRL

Table C.21 — mdocReaderAuth_revoked_CRL_08 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 8 revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.11 (BrainpoolP384r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.19 mdocReaderAuth_revoked_CRL_09

Table C.22 describes the profile of mdoc reader authentication certificate using curve BrainpoolP512r1 that is revoked by putting it on the CRL

Table C.22 — mdocReaderAuth_revoked_CRL_09 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 8 revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.13 (BrainpoolP512r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.20 mdocReaderAuth_revoked_OCSP_01

Table C.23 describes the profile of mdoc reader authentication certificate using Curve P-256 that results in a "revoked" response from the OCSP service.

Table C.23 — mdocReaderAuth_revoked_OCSP_01 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 1 revoked OCSP", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.2.840.10045.3.1.7 (Curve P-256)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "revoked". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.21 mdocReaderAuth_revoked_OCSP_02

Table C.24 describes the profile of mdoc reader authentication certificate using Curve P-384 that results in a "revoked" response from the OCSP service.

Table C.24 — mdocReaderAuth_revoked_OCSP_02 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 2 revoked OCSP", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.34 (Curve P-384)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "revoked". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.22 mdocReaderAuth_revoked_OCSP_03

Table C.25 describes the profile of mdoc reader authentication certificate using curve P-521 that results in a "revoked" response from the OCSP service.

Table C.25 — mdocReaderAuth_revoked_OCSP_03 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 3 revoked OCSP", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.35 (Curve P-521)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "revoked". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.23 mdocReaderAuth_revoked_OCSP_04

Table C.26 describes the profile of mdoc reader authentication certificate using curve Ed25519 that results in a "revoked" response from the OCSP service.

Table C.26 — mdocReaderAuth_revoked_OCSP_04 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 4 revoked OCSP", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.101.112 (Ed25519)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "revoked". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.24 mdocReaderAuth_revoked_OCSP_05

Table C.27 describes the profile of mdoc reader authentication certificate using curve Ed448 that results in a "revoked" response from the OCSP service.

Table C.27 — mdocReaderAuth_revoked_OCSP_05 certificate profile

Issuer	Identical to Subject field of CA_01
Subject	CN = "Test mdoc reader authentication cert 5 revoked OCSP", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.101.113 (Ed448)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "revoked". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.25 mdocReaderAuth_revoked_OCSP_06

Table C.28 describes the profile of mdoc reader authentication certificate using curve BrainpoolP256r1 that results in a "revoked" response from the OCSP service.

Table C.28 — mdocReaderAuth_revoked_OCSP_06 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 6 revoked OCSP", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.7 (BrainpoolP256r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "revoked". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.26 mdocReaderAuth_revoked_OCSP_07

Table C.29 describes the profile of mdoc reader authentication certificate using curve BrainpoolP320r1 that results in a "revoked" response from the OCSP service.

Table C.29 — mdocReaderAuth_revoked_OCSP_07 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 7 revoked OCSP", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.9 (BrainpoolP320r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "revoked". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.27 mdocReaderAuth_revoked_OCSP_08

Table C.30 describes the profile of mdoc reader authentication certificate using curve BrainpoolP384r1 that results in a "revoked" response from the OCSP service.

Table C.30 — mdocReaderAuth_revoked_OCSP_08 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 8 revoked OCSP", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.11 (BrainpoolP384r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "revoked". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.28 mdocReaderAuth_revoked_OCSP_09

Table C.31 describes the profile of mdoc reader authentication certificate using curve BrainpoolP512r1 that results in a "revoked" response from the OCSP service.

Table C.31 — mdocReaderAuth_revoked_OCSP_09 certificate profile

Issuer	Identical to Subject field of CA_02
Subject	CN = "Test mdoc reader authentication cert 9 revoked OCSP", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.13 (BrainpoolP512r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
Authority Information Access – Access Description OCSP	Present. OCSP service response is "revoked". accessMethod = 1.3.6.1.5.5.7.48.1 (OCSP) accessLocation = <<accessLocation>>
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.29 mdocReaderAuth_revoked_CA_01

Table C.32 describes the profile of mdoc reader authentication certificate using Curve P-256 that results in a "revoked" response from the OCSP service.

Table C.32 — mdocReaderAuth_revoked_CA_01 certificate profile

Issuer	Identical to Subject field of CA_revoked_CRL_01
Subject	CN = "Test mdoc reader authentication cert 1 revoked CA", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.7 (Curve P-256)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.30 mdocReaderAuth_revoked_CA_02

Table C.33 describes the profile of mdoc reader authentication certificate using Curve P-384 that results in a "revoked" response from the OCSP service.

Table C.33 — mdocReaderAuth_revoked_CA_02 certificate profile

Issuer	Identical to Subject field of CA_revoked_CRL_01
Subject	CN = "Test mdoc reader authentication cert 2 revoked CA", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.34 (Curve P-384)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.31 mdocReaderAuth_revoked_CA_03

Table C.34 describes the profile of mdoc reader authentication certificate using Curve P-521 that results in a "revoked" response from the OCSP service.

Table C.34 — mdocReaderAuth_revoked_CA_03 certificate profile

Issuer	Identical to Subject field of CA_revoked_CRL_01
Subject	CN = "Test mdoc reader authentication cert 3 revoked CA", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.35 (Curve P-521)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.32 mdocReaderAuth_revoked_CA_04

Table C.35 describes the profile of mdoc reader authentication certificate using curve Ed25519 that results in a "revoked" response from the OCSP service.

Table C.35 — mdocReaderAuth_revoked_CA_04 certificate profile

Issuer	Identical to Subject field of CA_revoked_CRL_01
Subject	CN = "Test mdoc reader authentication cert 4 revoked CA", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.101.112 (Ed25519)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.33 mdocReaderAuth_revoked_CA_05

Table C.36 describes the profile of mdoc reader authentication certificate using curve Ed448 that results in a "revoked" response from the OCSP service.

Table C.36 — mdocReaderAuth_revoked_CA_05 certificate profile

Issuer	Identical to Subject field of CA_revoked_CRL_01
Subject	CN = "Test mdoc reader authentication cert 5 revoked CA", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.101.113 (Ed448)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.34 mdocReaderAuth_revoked_CA_06

Table C.37 describes the profile of mdoc reader authentication certificate using curve BrainpoolP256r1 that results in a "revoked" response from the OCSP service.

Table C.37 — mdocReaderAuth_revoked_CA_06 certificate profile

Issuer	Identical to Subject field of CA_revoked_CRL_02
Subject	CN = "Test mdoc reader authentication cert 6 revoked CA", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.7 (BrainpoolP256r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.35 mdocReaderAuth_revoked_CA_07

Table C.38 describes the profile of mdoc reader authentication certificate using curve BrainpoolP320r1 that results in a "revoked" response from the OCSP service.

Table C.38 — mdocReaderAuth_revoked_CA_07 certificate profile

Issuer	Identical to Subject field of CA_revoked_CRL_02
Subject	CN = "Test mdoc reader authentication cert 7 revoked CA", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.9 (BrainpoolP320r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.36 mdocReaderAuth_revoked_CA_08

Table C.39 describes the profile of mdoc reader authentication certificate using curve BrainpoolP384r1 that results in a "revoked" response from the OCSP service.

Table C.39 — mdocReaderAuth_revoked_CA_08 certificate profile

Issuer	Identical to Subject field of CA_revoked_CRL_02
Subject	CN = "Test mdoc reader authentication cert 8 revoked CA", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.11 (BrainpoolP384r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.2.2.37 mdocReaderAuth_revoked_CA_09

Table C.40 describes the profile of mdoc reader authentication certificate using curve BrainpoolP512r1 that results in a "revoked" response from the OCSP service.

Table C.40 — mdocReaderAuth_revoked_CA_09 certificate profile

Issuer	Identical to Subject field of CA_revoked_CRL_02
Subject	CN = "Test mdoc reader authentication cert 9 revoked CA", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.13 (BrainpoolP512r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.3 Certificates necessary for testing an mDL reader

C.3.1 IACA root certificates

C.3.1.1 Certificate origin and usage

The IACA root certificates defined in this clause, as well as the associated key pairs, shall be generated by the tester prior to testing. During testing, these IACA certificates shall be present in an mDL reader under test as trust points for issuer data authentication, TLS server authentication, and JWS, if these security mechanisms are supported by the mDL reader under test. See 6.3.2.2 for more information.

The private keys associated with the public keys in these certificates shall only be used by the tester to sign document signer certificates as defined in C.3.2, TLS server certificates as defined in C.3.3 and JWS certificates as defined in C.3.4.

C.3.1.2 IACA_01

Table C.41 describes the profile of IACA root certificate using Curve P-521.

Used for signing the following certificates:

— DocumentSigner_01

— DocumentSigner_02

— DocumentSigner_03

— DocumentSigner_04

— DocumentSigner_05

— TLSServer_01

— TLSServer_02

— TLSServer_03

— JWS_01

— JWS_02

— JWS_03

Table C.41 — IACA_01 certificate profile

Issuer	CN = "Test Root CA cert 1 for mDL reader", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject	Identical to Issuer field
Subject public key info parameters (OID)	1.3.132.0.35 (Curve P-521)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.3.1.3 IACA_02

Table C.42 describes the profile of IACA root certificate using curve BrainpoolP512r1.

Used for signing the following certificates:

— DocumentSigner_06

— DocumentSigner_07

— DocumentSigner_08

— DocumentSigner_09

— TLSServer_04

— TLSServer_05

— TLSServer_06

Table C.42 — IACA_02 certificate profile

Issuer	CN = "Test Root CA cert 2 for mDL reader", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject	Identical to Issuer field
Subject public key info parameters (OID)	1.3.36.3.3.2.8.1.1.13 (BrainpoolP512r1)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.3.1.4 IACA _revoked_CRL_01

Table C.43 describes the profile of IACA root certificate using curve Curve P-521 that is revoked by putting it on the CRL.

Used for signing the following certificates:

— DocumentSigner_revoked_CA_01

— TLSServer_revoked_CA_01

— JWS_revoked_CA_01

Table C.43 — IACA_revoked_CRL_01 certificate profile

Issuer	CN = "Test IACA Root cert 1 for mDL reader revoked CRL", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject	Identical to Issuer field
Subject public key info parameters (OID)	1.3.132.0.35 (Curve P-521)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.3.2 DocumentSigner certificates

C.3.2.1 Certificate origin and usage

The document signer certificates defined in this clause, as well as the associated key pairs, shall be generated by the tester. These certificates shall be exclusively used to test the correctness of the issuer data authentication implementation of the mDL reader under test, as specified in the test cases in Appendix 3 of this document.

The corresponding private keys shall be present in the test apparatus during testing. The test apparatus shall use them to perform issuer data authentication by signing the MSO in the device retrieval mdoc responses sent to the mDL reader under test.

C.3.2.2 DocumentSigner_01

Table C.44 describes the profile of DocumentSigner certificate using Curve P-256.

Table C.44 — DocumentSigner_01 certificate profile

Issuer	Identical to Subject field of IACA_01
Subject	CN = "Test DocumentSigner cert 1", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.2.840.10045.3.1.7 (Curve P-256)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.3.2.3 DocumentSigner_02

Table C.45 describes the profile of DocumentSigner certificate using Curve P-384.

Table C.45 — DocumentSigner_02 certificate profile

Issuer	Identical to Subject field of IACA_01
Subject	CN = "Test DocumentSigner cert 2", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.34 (Curve P-384)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.3.2.4 DocumentSigner_03

Table C.46 describes the profile of DocumentSigner certificate using Curve P-521.

Table C.46 — DocumentSigner_03 certificate profile

Issuer	Identical to Subject field of IACA_01
Subject	CN = "Test DocumentSigner cert 3", O = <<organisation issuing the test certificate>>, C = <<code for issuing organisation's country>>, ST = <<code for issuing organisation's state or province>>
Subject public key info parameters (OID)	1.3.132.0.35 (Curve P-521)
IssuerAltName (URI)	"https://www.iso.org"
CRLDistributionPoint (URL)	<<URL>> This certificate will not be included in the CRL.
SignatureAlgorithm (OID)	1.2.840.10045.4.3.4 (ECDSA with SHA512)

C.3.2.5 DocumentSigner_04

Table C.47 describes the profile of DocumentSigner certificate using curve Ed25519.