ISO/IEC JTC1/SC17/WG10

mDL prototype interoperability party

October 7th 2018, Okayama, Japan

Version 1.0

08/08/2018

Organized / supported by

 **** 

ISO WG10 UTMS society AAMVA Joint mDL EReg Topic

Members of Japan Working Group Group XIX

# Introduction

ISO/IEC 18013 part 5 standardizes requirements for mobile driving license (mDL). The implementation of the standard by Issuing Authorities and their suppliers in various mDL solutions should result in a secure and interoperable mDL ecosystem.

Task Force 14 on mDL within ISO/IEC JTC1/SC17/WG10 has worked towards mDL standardization since 2014. The first CD draft of Part 5 was issued for ballot in April 2018 and generated useful feedback for improvement of the standard. At the event of the ISO/IEC JTC1/SC17 plenary and work group meetings in Okayama, Japan, a first mDL Prototype Interoperability Party will be hosted. The main objectives of the event are to test interoperability of standardized functions between implementations of different mDL solution providers, to keep momentum in the standardization work, and to generate further feedback on the draft standard.

The event allows Issuing Authorities, mDL solution providers and the standardization community to

* try out prototype implementations
* evaluate the interoperability of their implementation with other prototypes
* confirm their interpretation of the draft standard
* generate further feedback to clarify requirements and to enhance uniform interpretation of provisions in the standard under development

This document provides further details on the mDL Prototype Interoperability Party which will be held on 7 October 2018 in Okayama, Japan. This includes details on the venue, the terms and conditions for participation, test process and registration forms.

# Organization

Date: 7th October 2018

Host: UTMS society of Japan

Location: Okayama City Hotel Kuwatacho

<https://www.japanican.com/en/hotel/detailmap/7103102/>

Meeting room #306 for IOP event #301 for Staff room, available from 9:00-21:00

Organizers: ISO WG10 Task Force 14

Supporters: ISO WG10

UTMS society of Japan

AAMVA Joint mDL Working Group

EReg Topic Group XIX on Virtual Driving Licence

# Participation

## Registration

Participants are required to register in advance of the test event. The registration form, including instructions for registration are available in ‎Annex A in this document.

## Publication of the results

Participants must know that neither the organizers nor the WG10 endorse the results of the party. Passing the tests does not result in an “ISO certification” or “WG10 approval”.

Participants will receive their results. No results will be presented at the end but only a summary of the standard issues will be addressed.

The results of tests shall not be used by the participants for any commercial or marketing purposes. However, participants are encouraged to use the test results to improve their products.

# Test scope

## Base document

The test is based on the most recent version of ISO/IEC 18013-5 which is distributed in April, 2018 (SC17\_N6250).

## Features to be tested

The main features to be tested in this test event are device engagement and offline and online data transfer. Table 1 lists features to be tested during the party. Not all features are mandatory and a combination of a QR code as a device engagement method and BLE as a data transfer method is a main focus for the test event.

For device engagement, the test scope covers both a QR code and NFC, as specified in ISO/IEC 18013-5.

For data transfer to the mDL reader, the test scope includes both offline methods and online methods. By default, data is transferred using an offline method. For the test event, the scope is limited to BLE, NFC and compact encoding using QR code (specified in ‎Annex D in this document). When both mDL and mDL reader have internet connectivity and support online methods, an online mDL transaction will be carried out, using the mDL (Issuing Authority) backend REST or OIDC API available to the mDL reader.

Participants should implement appropriate security measures – Passive Authentication and Active Authentication or Chip Authentication and Secure Messaging in case of offline data transfer; electronic signing, signature verification and certificate chain validation and TLS communication in case of online data transfer.

The mDL data to be available for transfer in scope for the test event are license and holder data (data elements as grouped in DG1 for offline), face image (DG6 for offline) and mDL refresh info (DG10, for offline only). It is desirable that age verification is supported (tag ‘5F A7 XX’ in case of offline) and for this test event it is recommended to use DG32 for this data element.

Table 1 test overview

|  |  |  |
| --- | --- | --- |
|  | Features | |
| Offline | Online |
| Device Engagement | * QR * NFC | * QR * NFC |
| Data transfer | * BLE * NFC * QR (compact encoding) | * REST * OIDC |
| Security | * Passive authentication * Active authentication * Secure messaging | * Signature verification * Certificate chain validation |
| Data | * mDL Data   + License and holder data (DG1)   + Face image (DG6)   + Refresh info (DG10) * Security related data   + Active authentication (DG13)   + Passive authentication (EF.SOD) * Data minimization   + Age verification (tag ‘5F A7 XX’) | * mDL Data   + Licence and holder data (DG1 equivalent)   + Face image   + Age claim |

## Test scenario

Details of test scenarios can be found in ‎Annex C in this document. In test scenario ID, XXOF-XXX means offline tests and XXON-XXX indicates online tests.

Table 2 test scenario list – offline implementation

|  |  |
| --- | --- |
| Test scenario ID | Descriptions |
| DTOF-001a | This test checks data transfer by BLE when device is engaged using QR without secure messaging |
| DTOF-001b | This test checks data transfer by BLE when device is engaged using QR with secure messaging |
| DTOF-002a | This test checks data transfer by BLE when device is engaged using NFC without secure messaging |
| DTOF-002b | This test checks data transfer by BLE when device is engaged using NFC with secure messaging |
| DTOF-003a | This test checks data transfer by NFC when device is engaged using NFC without secure messaging |
| DTOF-003b | This test checks data transfer by NFC when device is engaged using NFC with secure messaging |
| DTOF-004a | This test checks data transfer by NFC when device is engaged using QR without secure messaging |
| DTOF-004b | This test checks data transfer by NFC when device is engaged using QR with secure messaging |
| DAOF-001 | This test checks whether license and holder data (DG1) are correctly transferred |
| DAOF-002 | This test checks whether facial image data (DG6) is correctly transferred |
| DAOF-003 | This test checks whether DG10 data is correctly transferred |
| DAOF-004 | This test checks whether age verification is correctly processed using data minimization |
| SEOF-001 | This test check whether passive authentication is performed successfully |
| SEOF-002 | This test check whether active authentication is performed successfully |

Table 3 test scenario list – online implementation

|  |  |
| --- | --- |
| Test scenario ID | Descriptions |
| DTON-001 | This test checks data transfer by REST API when device is engaged using QR |
| DTON-002 | This test checks data transfer by OIDC API when device is engaged using QR |
| DTON-003 | This test checks data transfer by REST API when device is engaged using NFC |
| DTON-004 | This test checks data transfer by OIDC API when device is engaged using NFC |
| DAON-001 | This test checks whether license and holder data (DG1 equivalent) are correctly transferred |
| DAON-002 | This test checks whether facial image data is correctly transferred (online) |
| DAON-003 | This test checks whether age verification is correctly processed using data minimization (online) |
| SEON-001 | This test check whether the signature of the message in API is correctly signed |
| SEON-002 | This test check whether the certificate chain of the message in API is correct |

# Test process

## Implementation Conformance Statement

Upon registration, participants need to fill in an implementation conformance statement, indicating which standardized functions and/or protocols are supported in the implementation presented for interoperability testing. The Implementation Conformance Statement is available in ‎Annex B in this document.

## Test materials

Participants providing an mDL (holder) implementation are required to provide their test IA CA certificate (made in accordance to A.5 of ISO/IEC 18013-3) two weeks in advance of the test event. The organizers of the test event will distribute the IA CA certificates to the providers of mDL reader implementation at the start of the event.

## Test stations

At the test event, mDL (holder) implementations pass by test stations with mDL reader implementations to check the interoperability between the mDL and mDL reader implementations.

## Facilitation / support

### Pre-check

Before mDL (holder) implementations engage in transactions with mDL reader implementations, a pre-check will be carried out on the device engagement info. The information provided by the mDL in the QR code or over NFC will be parsed to check the structure of the device engagement info.

Before mDL reader implementations engage in transactions with mDL (holder) implementations, a pre-check (happy flow) will be carried out, in which several different instances of compliant device engagement info will be provided.

Depending on the number of participants, an additional smoke test may be performed after the pre-checks.

### Debug support

In advance of the test event, a Logical Data Structure with signature and certificate chain can be provided if requested.

During the test event, the organizers offer support in analyzing causes for any interoperability issues. It is recommended that mDL reader implementations are able to export transaction logs (incl. REST/OIDC messages).

## Test deliverables

A provider with an mDL reader shall complete a spreadsheet with executed test scenarios and test results. Anonymized test results will be presented to ISO/IEC JTC 1/SC 17/WG10.

1. – Registration form

ISO WG10 mDL Prototype Interoperability Party

7th October 2018, Okayama, Japan

To be returned before XX September 2018 to [Arjan.geluk@ul.com](mailto:Arjan.geluk@ul.com) and in CC: [Yaejin.lee@ul.com](mailto:Yaejin.lee@ul.com) and [nakamura.kenken@jp.panasonic.com](mailto:nakamura.kenken@jp.panasonic.com).

Delegation/participant of country, organization or company

Provider of

mDL prototype

mDL reader prototype

Full name :

Company :

Email :

Participant

The results of tests shall not be used by the participants for any commercial or marketing purposes.

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. – Implementation Conformance Statement

This implementation conformance statement shall be included as a part of registration. In order to set up the tests properly, the table below shall be completed.

NOTE Participants are asked to send a preliminary version of this conformance statement before 17 August 2018 to [Arjan.geluk@ul.com](mailto:Arjan.geluk@ul.com) and in CC: [Yaejin.lee@ul.com](mailto:Yaejin.lee@ul.com). This is only used as an indication for preparation of the event. In September, this form should be submitted as a part of the formal registration.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category | | Profile | Applicable for mDL (holder) | Applicable for mDL reader |
| Device engagement | | QR |  |  |
| NFC |  |  |
| Data transfer | offline | NFC |  |  |
| BLE |  |  |
| QR (Compact encoding ) |  |  |
| Online | REST |  |  |
| OIDC |  |  |
| Security | Offline | Passive authentication (EF.SOD) |  |  |
| Active authentication (DG13) |  |  |
| Secure messaging (PACE) |  |  |
| Online | Signature verification |  |  |
| Certificate chain validation |  |  |
| Data | Offline | Logical Data Structure containing DG1 |  |  |
| Logical Data Structure containing DG6 |  |  |
| Logical Data Structure containing DG10 |  |  |
| Data minimization - Logical Data Structure containing age verification tag ('5F A7 XX') |  |  |
| Online | License and holder data |  |  |
| Facial image |  |  |
| Age claim |  |  |
| Request for Logical Data Structure with signature and certificate chain | | |  |  |

1. – Test scenarios
   1. Test scenarios - offline

|  |  |
| --- | --- |
| Test Case-ID | DTOF\_001a |
| Purpose | This test checks data transfer by BLE when device is engaged using QR without secure messaging |
| References | ISO/IEC 18013-5 |
| Profile | QR, BLE |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR is set as the device engagement method   + BLE is set as the data transfer method, BLE is activated   + mDL application is launched   + mDL does not need to support BAP or PACE |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates QR code encoding device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (EF.SOD, DG1, DG6 and DG10) and one BLE profile 2. mDL reader captures QR code from mDL display 3. mDL reader establishes BLE connection with mDL by using parameters from device engagement structure 4. mDL reader sends SELECT command with AID acc. to ISO/IEC 18013-5 application 5. mDL reader sends sequence of READ BINARY commands to receive data from EF.SOD, DG1, DG6 and DG10   6. mDL reader decodes mDL data |
| Expected Results | 1. QR code is displayed on mDL display 2. QR code is captured and decoded by mDL reader 3. BLE connection between mDL reader and mDL has been established 4. R-APDU from mDL is 0x9000 5. Sequence of R-APDUs encoding with the status word 0x9000 the mDL data 6. mDL data are displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DTOF\_001b |
| Purpose | This test checks data transfer by BLE when device is engaged using QR with secure messaging |
| References | ISO/IEC 18013-5 |
| Profile | QR, BLE, PACE |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR is set as the device engagement method   + BLE is set as the data transfer method, BLE is activated   + mDL application is launched   + mDL supports PACE and provides input string |
| Test Scenario | Perform the following checks for data transfer   1. see Step 1 of DTOF\_001a with device engagement structure encodes "input string (access password)" serving as PACE input string 2. see Step 2 of DTOF\_001a 3. see Step 3 of DTOF\_001a 4. see Step 4 of DTOF\_001a 5. mDL reader sends READ BINARY command on EF.CardAccess 6. mDL reader performs PACE protocol (MSE command and sequence of GENERAL AUTHENTICATE commands) and derives session keys according to parameters given in EF.CardAccess 7. see Step 5 of DTOF\_001a by applying secure messaging   8. see Step 6 of DTOF\_001a |
| Expected Results | 1. see Step 1 of DTOF\_001a 2. see Step 2 of DTOF\_001a 3. see Step 3 of DTOF\_001a 4. see Step 4 of DTOF\_001a 5. R-APDU encoding EF.CardAccess with the status word 0x9000 6. Session keys (shared secret key and MAC) are derived 7. see Step 5 of DTOF\_001a by applying secure messaging 8. see Step 6 of DTOF\_001a |

|  |  |
| --- | --- |
| Test Case-ID | DTOF\_002a |
| Purpose | This test checks data transfer by BLE when device is engaged using NFC without secure messaging |
| References | ISO/IEC 18013-5 |
| Profile | NFC, BLE |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + NFC is set as the device engagement method   + BLE is set as the data transfer method, BLE is activated   + mDL application is launched   + mDL does not need to support BAP or PACE |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (EF.SOD, DG1, DG6 and DG10) and one BLE profile and makes available through NFC 2. mDL reader establishes NFC connection and read encoded device engagement structure from mDL holder 3. mDL reader establishes BLE connection with mDL by using parameters from device engagement structure 4. mDL reader sends SELECT command with AID acc. to ISO/IEC 18013-5 application 5. mDL reader sends sequence of READ BINARY commands to receive data from EF.SOD, DG1, DG6 and DG10.   6. mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through NFC 2. NFC is captured and decoded by mDL reader 3. BLE connection between mDL reader and mDL has been established 4. R-APDU from mDL is 0x9000 5. Sequence of R-APDUs encoding the mDL data with the status word 0x9000. 6. mDL data are displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DTOF\_002b |
| Purpose | This test checks data transfer by BLE when device is engaged using NFC with secure messaging |
| References | ISO/IEC 18013-5 |
| Profile | NFC, BLE, PACE |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + NFC is set as the device engagement method   + BLE is set as the data transfer method, BLE is activated   + mDL application is launched   + mDL supports PACE and provides input string |
| Test Scenario | Perform the following checks for data transfer   1. see Step 1 of DTOF\_001a with device engagement structure encodes "input string (access password)" serving as PACE input string 2. see Step 2 of DTOF\_001a 3. see Step 3 of DTOF\_001a 4. see Step 4 of DTOF\_001a 5. mDL reader sends READ BINARY command on EF.CardAccess 6. mDL reader performs PACE protocol (MSE command and sequence of GENERAL AUTHENTICATE commands) and derives session keys according to parameters given in EF.CardAccess 7. see Step 5 of DTOF\_001a by applying secure messaging   8. see Step 6 of DTOF\_001a |
| Expected Results | 1. see Step 1 of DTOF\_001a 2. see Step 2 of DTOF\_001a 3. see Step 3 of DTOF\_001a 4. see Step 4 of DTOF\_001a 5. R-APDU encoding EF.CardAccess with the status word 0x9000 6. Shared secret key and MAC key between mDL and mDL reader established 7. see Step 5 of DTOF\_001a by applying secure messaging 8. see Step 6 of DTOF\_001a |

|  |  |
| --- | --- |
| Test Case-ID | DTOF\_003a |
| Purpose | This test checks data transfer by NFC when device is engaged using NFC without session security |
| References | ISO/IEC 18013-5 |
| Profile | NFC, NFC |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + NFC is set as the device engagement method   + NFC is set as the data transfer method   + mDL application is launched   + mDL does not need to support BAP or PACE |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (EF.SOD, DG1, DG6 and DG10) and one NFC profile 2. mDL reader establishes an NFC connection and read encoded device engagement structure from mDL holder 3. mDL reader establishes an NFC connection with mDL by using parameters from device engagement structure 4. mDL reader sends SELECT command with AID acc. to ISO/IEC 18013-5 application 5. mDL reader sends sequence of READ BINARY commands to receive data from EF.SOD, DG1, DG6 and DG10   6. mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through NFC 2. Received device engagement structure decoded by mDL reader 3. NFC connection between mDL reader and mDL has been established 4. R-APDU from mDL is 0x9000 5. Sequence of R-APDUs encoding the mDL data with the status word 0x9000 6. mDL data are displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DTOF\_003b |
| Purpose | This test checks data transfer by NFC when device is engaged using NFC with secure messaging |
| References | ISO/IEC 18013-5 |
| Profile | NFC, NFC, PACE |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + NFC is set as the device engagement method   + NFC is set as the data transfer method, BLE is activated   + mDL application is launched   + mDL supports PACE and provides input string |
| Test Scenario | Perform the following checks for data transfer   1. see Step 1 of DTOF\_001a with device engagement structure encodes "input string (access password)" serving as PACE input string 2. see Step 2 of DTOF\_001a 3. see Step 3 of DTOF\_001a 4. see Step 4 of DTOF\_001a 5. mDL reader sends READ BINARY command on EF.CardAccess 6. mDL reader performs PACE protocol (MSE command and sequence of GENERAL AUTHENTICATE commands) and derives session keys according to parameters given in EF.CardAccess 7. see Step 5 of DTOF\_001a by applying secure messaging   8. see Step 6 of DTOF\_001a |
| Expected Results | 1. see Step 1 of DTOF\_001a 2. see Step 2 of DTOF\_001a 3. see Step 3 of DTOF\_001a 4. see Step 4 of DTOF\_001a 5. R-APDU encoding EF.CardAccess 6. Shared secret key and MAC key between mDL and mDL reader established 7. see Step 5 of DTOF\_001a by applying secure messaging 8. see Step 6 of DTOF\_001a |

|  |  |
| --- | --- |
| Test Case-ID | DTOF\_004a |
| Purpose | This test checks data transfer by NFC when device is engaged using QR without secure messaging |
| References | ISO/IEC 18013-5 |
| Profile | QR, NFC |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR is set as the device engagement method   + NFC is set as the data transfer method   + mDL application is launched   + mDL does not need to support BAP or PACE |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates QR code encoding device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (EF.SOD, DG1, DG6 and DG10) and one NFC profile 2. mDL reader captures QR code from mDL display 3. mDL reader establishes NFC connection with mDL by using parameters from device engagement structure 4. mDL reader sends SELECT command with AID acc. to ISO/IEC 18013-5 application 5. mDL reader sends sequence of READ BINARY commands to receive data from EF.SOD, DG1, DG6 and DG10   6. mDL reader decodes mDL data |
| Expected Results | 1. QR code is displayed on mDL display 2. QR code is captured and decoded by mDL reader 3. NFC connection between mDL reader and mDL has been established 4. R-APDU from mDL is 0x9000 5. Sequence of R-APDUs encoding the mDL data with the status word 0x9000 6. mDL data are displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DTOF\_004b |
| Purpose | This test checks data transfer by NFC when device is engaged using QR with secure messaging |
| References | ISO/IEC 18013-5 |
| Profile | QR, NFC, PACE |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR is set as the device engagement method   + NFC is set as the data transfer method   + mDL application is launched   + mDL supports PACE and provides input string |
| Test Scenario | Perform the following checks for data transfer   1. see Step 1 of DTOF\_001a with device engagement structure encodes "input string (access password)" serving as PACE input string 2. see Step 2 of DTOF\_001a 3. see Step 3 of DTOF\_001a 4. see Step 4 of DTOF\_001a 5. mDL reader sends READ BINARY command on EF.CardAccess 6. mDL reader performs PACE protocol (MSE command and sequence of GENERAL AUTHENTICATE commands) and derives session keys according to parameters given in EF.CardAccess 7. see Step 5 of DTOF\_001a by applying secure messaging   8. see Step 6 of DTOF\_001a |
| Expected Results | 1. see Step 1 of DTOF\_001a 2. see Step 2 of DTOF\_001a 3. see Step 3 of DTOF\_001a 4. see Step 4 of DTOF\_001a by applying secure messaging 5. R-APDU encoding EF.CardAccess with the status word 0x9000 6. Shared secret key and MAC key between mDL and mDL reader established 7. see Step 5 of DTOF\_001a by applying secure messaging 8. see Step 6 of DTOF\_001a |

|  |  |
| --- | --- |
| Test Case-ID | DAOF\_001 |
| Purpose | This test checks whether license and holder data (DG1) are correctly transferred |
| References | ISO/IEC 18013-5 |
| Profile | Any |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR or NFC is set as the device engagement method   + BLE or NFC is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (DG1) and one BLE/NFC profile and makes available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes BLE/NFC connection with mDL by using parameters from device engagement structure 4. mDL reader sends SELECT command with AID acc. to ISO/IEC 18013-5 application 5. mDL reader sends sequence of READ BINARY commands to receive DG1 data 6. mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through NFC/QR code 2. QR code is captured/device engagement structure is received via NFC connection and decoded by mDL reader 3. BLE/NFC connection between mDL reader and mDL has been established 4. R-APDU from mDL is 0x9000 5. (Sequence of) R-APDUs encoding the Licence and holder data (DG1) 6. License and holder data (DG1) is displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DAOF\_002 |
| Purpose | This test checks whether face image (DG6) are correctly transferred |
| References | ISO/IEC 18013-5 |
| Profile | Any |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR or NFC is set as the device engagement method   + BLE or NFC is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (DG6) and one BLE/NFC profile and makes available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes BLE/NFC connection with mDL by using parameters from device engagement structure 4. mDL reader sends SELECT command with AID acc. to ISO/IEC 18013-5 application 5. mDL reader sends sequence of READ BINARY commands to receive DG6 data   6. mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through NFC/QR code 2. QR code is captured or device engagement data is received via NFC connection and decoded by mDL reader 3. BLE/NFC connection between mDL reader and mDL has been established 4. R-APDU from mDL is 0x9000 5. Sequence of R-APDUs encoding the DG6 data with the status word 0x9000 6. Face image (DG6) is displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DAOF\_003 |
| Purpose | This test checks whether Refresh info (DG10) are correctly transferred |
| References | ISO/IEC 18013-5 |
| Profile | Any |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR or NFC is set as the device engagement method   + BLE or NFC is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (DG10) and one BLE/NFC profile and makes available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes BLE/NFC connection with mDL by using parameters from device engagement structure 4. mDL reader sends SELECT command with AID acc. to ISO/IEC 18013-5 application 5. mDL reader sends sequence of READ BINARY commands to receive DG10 data   6. mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through NFC/QR code 2. QR code is captured or device engagement structure is received via NFC connection and decoded by mDL reader 3. BLE/NFC connection between mDL reader and mDL has been established 4. R-APDU from mDL is 0x9000 5. (Sequence of) R-APDUs encoding the DG10 data 6. Refresh info (DG10) is displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DAOF\_004 |
| Purpose | This test checks whether age verification is correctly processed using data minimization |
| References | ISO/IEC 18013-5 |
| Profile | Any |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR or NFC is set as the device engagement method   + BLE or NFC is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with mandatory data accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and one BLE/NFC profile and makes available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes BLE/NFC connection with mDL by using parameters from device engagement structure 4. mDL reader sends SELECT command with AID acc. to ISO/IEC 18013-5 application 5. mDL reader chooses age verification and sends sequence of READ BINARY commands to receive data according to accessible data groups acc. to EF.GroupAccess 6. mDL holder gives consent and mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through NFC/QR code 2. QR code is captured or device engagement structure is received via NFC connection and decoded by mDL reader 3. BLE/NFC connection between mDL reader and mDL has been established 4. R-APDU from mDL is 0x9000 5. Sequence of R-APDUs encoding the Age verification data with the status word 0x9000 6. Age verification is displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | SEOF\_001 |
| Purpose | This test check whether passive authentication is performed successfully |
| References | ISO/IEC 18013-5 |
| Profile | PA |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR or NFC is set as the device engagement method   + BLE or NFC is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (EF.SOD, DG1, DG6 and DG10) and one BLE/NFC profile and makes available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes BLE/NFC connection with mDL by using parameters from device engagement structure 4. mDL reader sends SELECT command with AID acc. to ISO/IEC 18013-5 application 5. mDL reader sends sequence of READ BINARY commands to receive data from EF.SOD, DG1, DG6 and DG10   6. mDL reader decodes mDL data and performs passive authentication |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through NFC/QR code 2. QR code is captured or device engagement structure is received via NFC connection and decoded by mDL reader 3. BLE/NFC connection between mDL reader and mDL has been established 4. R-APDU from mDL is 0x9000 5. Sequence of R-APDUs encoding the mDL data with the status word 0x9000 6. the result of passive authentication is indicated |

|  |  |
| --- | --- |
| Test Case-ID | SEOF\_002 |
| Purpose | This test check whether active authentication is performed successfully |
| References | ISO/IEC 18013-5 |
| Profile | AA |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR or NFC is set as the device engagement method   + BLE or NFC is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (EF.SOD, DG13, DG1, DG6 and DG10) and one BLE/NFC profile and makes available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes BLE/NFC connection with mDL by using parameters from device engagement structure 4. mDL reader sends SELECT command with AID acc. to ISO/IEC 18013-5 application 5. mDL reader sends sequence of READ BINARY commands to receive data from EF.SOD, DG13, DG1, DG6 and DG10   6. mDL reader decodes mDL data and performs active authentication with INTERNAL AUTHENTICATE command |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through NFC/QR code 2. QR code is captured or device engagement structure is received via NFC connection and decoded by mDL reader 3. BLE/NFC connection between mDL reader and mDL has been established 4. R-APDU from mDL is 0x9000 5. (Sequence of) R-APDUs encoding the mDL data 6. the result of active authentication is displayed |

* 1. Test scenarios – online

|  |  |
| --- | --- |
| Test Case-ID | DTON\_001 |
| Purpose | This test checks data transfer by REST API when device is engaged using QR |
| References | ISO/IEC 18013-5 |
| Profile | QR, REST |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR is set as the device engagement method   + Online (REST) is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates QR code encoding device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and one online (rest) profile 2. mDL reader captures QR code from mDL display 3. mDL reader establishes online (rest) connection with mDL by using parameters from device engagement structure 4. mDL reader sends get command to the server to retrieve the data   5. mDL reader decodes mDL data |
| Expected Results | 1. QR code is displayed on mDL display 2. QR code is captured and decoded by mDL reader 3. Online connection between mDL reader and mDL has been established 4. The server responds with mDL data 5. mDL data are displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DTON\_002 |
| Purpose | This test checks data transfer by OIDC API when device is engaged using QR |
| References | ISO/IEC 18013-5 |
| Profile | QR, OIDC |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR is set as the device engagement method   + Online (OIDC) is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates QR code encoding device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and one online (OIDC) profile 2. mDL reader captures QR code from mDL display 3. mDL reader establishes online (OIDC) connection with mDL by using parameters from device engagement structure 4. mDL reader sends get command to the server to retrieve the data   5. mDL reader decodes mDL data |
| Expected Results | 1. QR code is displayed on mDL display 2. QR code is captured and decoded by mDL reader 3. Online connection between mDL reader and mDL has been established 4. The server responds with mDL data 5. mDL data are displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DTON\_003 |
| Purpose | This test checks data transfer by REST API when device is engaged using NFC |
| References | ISO/IEC 18013-5 |
| Profile | NFC, REST |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + NFC is set as the device engagement method   + Online (REST) is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and one online (rest) profile and make available through NFC 2. mDL reader receives device engagement structure via NFC connection from mDL reader 3. mDL reader establishes online (rest) connection with mDL by using parameters from device engagement structure 4. mDL reader sends get command to the server to retrieve the data   5. mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through NFC 2. Device engagement structure is received via NFC connection and decoded by mDL reader 3. Online connection between mDL reader and mDL has been established 4. The server responds with mDL data 5. mDL data are displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DTON\_004 |
| Purpose | This test checks data transfer by OIDC API when device is engaged using NFC |
| References | ISO/IEC 18013-5 |
| Profile | NFC, OIDC |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + NFC is set as the device engagement method   + Online (OIDC) is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with mandatory data elements, accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and one online (OIDC) profile and make available through NFC 2. mDL reader receives device engagement structure via NFC connection from mDL reader 3. mDL reader establishes online (OIDC) connection with mDL by using parameters from device engagement structure 4. mDL reader sends get command to the server to retrieve the data   5. mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through NFC 2. Device engagement structure is received via NFC connection and decoded by mDL reader 3. Online connection between mDL reader and mDL has been established 4. The server responds with mDL data 5. mDL data are displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DAON\_001 |
| Purpose | This test checks whether license and holder data (DG1 equivalent) are correctly transferred |
| References | ISO/IEC 18013-5 |
| Profile | QR/NFC, REST/OIDC |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR/NFC is set as the device engagement method   + Online (REST/OIDC) is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with license and holder data, accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and one online (REST/OIDC) profile and make available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes online (REST/OIDC) connection with mDL by using parameters from device engagement structure 4. mDL reader sends get command to the server to retrieve the data   5. mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through QR code/NFC 2. QR code is captured or device engagement structure is received via NFC connection and decoded by mDL reader 3. Online connection between mDL reader and mDL has been established 4. The server responds with mDL data 5. License and holder data are displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DAON\_002 |
| Purpose | This test checks whether facial image data is correctly transferred (online) |
| References | ISO/IEC 18013-5 |
| Profile | QR/NFC, REST/OIDC |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR/NFC is set as the device engagement method   + Online (REST/OIDC) is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with facial image data, accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and one online (REST/OIDC) profile and make available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes online (REST/OIDC) connection with mDL by using parameters from device engagement structure 4. mDL reader sends get command to the server to retrieve the data   5. mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through QR code/NFC 2. QR code is captured or device engagement structure is received via NFC connection and decoded by mDL reader 3. Online connection between mDL reader and mDL has been established 4. The server responds with mDL data 5. Facial image data is displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | DAON\_003 |
| Purpose | This test checks whether age verification is correctly processed using data minimization (online) |
| References | ISO/IEC 18013-5 |
| Profile | QR/NFC, REST/OIDC |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR/NFC is set as the device engagement method   + Online (REST/OIDC) is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with no element data, accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and one online (REST/OIDC) profile and make available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes online (REST/OIDC) connection with mDL by using parameters from device engagement structure 4. mDL reader chooses age verification and sends get command to the server to retrieve the data   5. mDL holder gives consent and mDL reader decodes mDL data |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through QR code/NFC 2. QR code is captured or device engagement structure is received via NFC connection and decoded by mDL reader 3. Online connection between mDL reader and mDL has been established 4. The server responds with mDL data 5. Age verification is displayed on display of mDL reader |

|  |  |
| --- | --- |
| Test Case-ID | SEON\_001 |
| Purpose | This test check whether the signature of the message in API is correctly signed |
| References | ISO/IEC 18013-5 |
| Profile | QR/NFC, REST/OIDC |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR/NFC is set as the device engagement method   + Online (REST/OIDC) is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with license and holder data, accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and one online (REST/OIDC) profile and make available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes online (REST/OIDC) connection with mDL by using parameters from device engagement structure 4. mDL reader sends get command to the server to retrieve the data   5. mDL reader decodes mDL data and performs a check for the signature chain of the message |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through QR code/NFC 2. QR code is captured or device engagement structure is received via NFC connection and decoded by mDL reader 3. Online connection between mDL reader and mDL has been established 4. The server responds with mDL data 5. mDL data is displayed on display of mDL reader and whether the signature check is done by the holder in the device of verifier |

|  |  |
| --- | --- |
| Test Case-ID | SEON\_002 |
| Purpose | This test check whether the certificate chain of the message in API is correct |
| References | ISO/IEC 18013-5 |
| Profile | QR/NFC, REST/OIDC |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder with mDL data   + QR/NFC is set as the device engagement method   + Online (REST/OIDC) is set as the data transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates encoded device engagement structure with license and holder data, accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and one online (REST/OIDC) profile and make available through QR code/NFC 2. mDL reader captures QR code or receives encoded device engagement structure via NFC connection from mDL holder 3. mDL reader establishes online (REST/OIDC) connection with mDL by using parameters from device engagement structure 4. mDL reader sends get command to the server to retrieve the data   5. mDL reader decodes mDL data and performs a check for the certificate chain of the message |
| Expected Results | 1. Device engagement structure is generated from mDL holder and available through QR code/NFC 2. QR code is captured or device engagement structure is received via NFC connection and decoded by mDL reader 3. Online connection between mDL reader and mDL has been established 4. The server responds with mDL data 5. mDL data is displayed on display of mDL reader whether the certificate chain is checked by the holder in the device of verifier |

1. – Specification and test scenario for compact encoding
   1. Specification

The current version of ISO/IEC 18013-5 does not specify all aspects required to use compact encoding. Therefore this annex describes how to do compact encoding.

One QR code is used for both device engagement and data transfer. The single QR code is encoded with a device engagement structure and concatenated with mDL data encoded in compact format. The device engagement structure has mandatory data elements (where DO'80' is empty), accessible tags according to chosen mDL data (i.e. EF.GroupAccess) and no transfer profile. The concatenated mDL data shall include a face image according to Annex E ISO/IEC 18013-2.

Note1: Absence of DO'A3' to DO'A6' indicates data transfer via QR code.

Note2: Future versions of ISO/IEC 18013-5 may specify a dedicated object (e.g. DO'A7') for optical data transfer specifying 2D barcode format and data encoding.

* 1. Test scenario

|  |  |
| --- | --- |
| Test Case-ID | CE\_001 |
| Purpose | This test checks data transfer by QR code and compact encoding |
| References | ISO/IEC 18013-5 |
| Profile | QR |
| Preconditions | * mDL reader is ready, e.g. mDL reader application is launched * A device of mDL holder is ready with mDL data and   + QR is set as transfer method   + mDL application is launched |
| Test Scenario | Perform the following checks for data transfer   1. mDL holder selects mDL data to be released and mDL generates one QR code 2. mDL reader captures QR code from mDL display 3. mDL reader decodes mDL data and optionally performs passive authentication |
| Expected Results | 1. QR code is displayed on mDL display 2. QR code is captured and decoded by mDL reader 3. mDL data is displayed on display of mDL reader and optionally result of passive authentication is displayed |