Certification Test Report for HID Global

Testing Android-based goID Starter App Version 1.0.2.5 against ISO / IEC 18013-5:2021

Author	UL
Test Report Number	UL_eID_HID_Android_001
Version	1.0
Date of Issue	2023-08-22
Status	Final
Classification	Proprietary

Device/OS	Google Pixel 6a: Android 13
Passed Tests	225
Failed Tests	0
Not Applicable Tests	234
Total	459

Device/OS	Samsung Galaxy S9 : Android 10
Passed Tests	225
Failed Tests	0
Not Applicable Tests	234
Total	459

Document Information

Project Owner	David Bakker/Gerardo Dibildox Ramos /Jerrin Jose Thomas
Customer	HID Global
System Under Test	HID Global Android-based mDL Application goID Starter App Version 1.0.2.5
Project Code	PR-024656
Certification Test Report Number	UL_eID_HID_Android_001
Document Title	Certification Test Report for HID Global – Testing Android-based goID Starter App Version 1.0.2.5 against ISO/IEC 18013-5:2021
File Name	UL eID Technology Certification Test Report UL_eID_HID_Android_001.docx
Classification	Proprietary
Status	Final
Distribution	HID Global

Version History

Version	Date	Status	Author
1.0	2023-08-22	Final	UL VS

Change History

Version	Date	Changes
1.0	2023-08-22	The final version to be sent to the customer

Table of Contents

1 INTRODUCTION

1.1 SCOPE

The scope of this document is to provide a clear understanding of the activities performed for the certification testing of HID Global's Android-based mDL Application and version - goID Starter App Version 1.0.2.5. This Test Report document includes information about the validation results along with observations drawn from the test activities.

UL conducted Functional Certification testing against the ISO/IEC 18013-5:2021 standard, where the System Under Test (SUT) is the mDL application and its interface to the mDL reader (see area 1.1 in Figure 1 below). This Certification Test Report intends to provide HID Global with an overview of the test activities and the resultant outcomes.

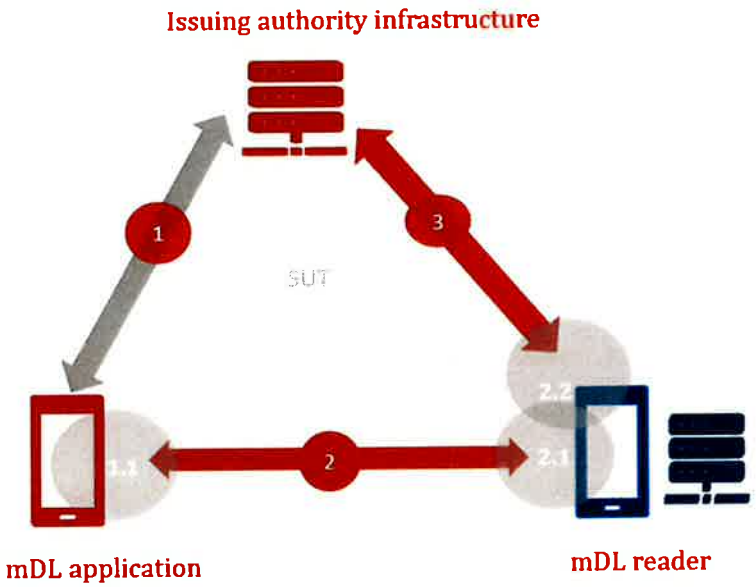

Figure 1: mDL System Under Test

1.2 DOCUMENT STRUCTURE

The certification test report document follows the below structure.

- Section 1 provides details on the scope and system under test, including configuration, samples used, and personalized mDL data set used for the certification.
- Section 2 provides details on the test devices, test tools, test scope, test execution steps and the test time frame followed during the certification.
- Section 3 provides details on the high-level test results and detailed test scope and test results.

- Section 4 provides detailed test results.
- Appendix A.1 lists the Implementation Conformance Statement that is filled by the customer and was used to generate the applicable test cases for the certification.
- Appendix A.2 provides an overview of the samples used during the certification testing.

1.3 REFERENCE DOCUMENTS

The following documents have been referenced for the Functional Certification testing of the product:

Ref	Title	Author	Status	Version	Receipt Date
[1]	ISO/IEC 18013-5: 2021	ISO/IEC	Final	First edition	September 2021
[2]	UL mDL Test Case Specification	UL	Draft	-	-

Table 1: Reference Documents

1.4 SYSTEM UNDER TEST

1.4.1 IDENTIFICATION

The mDL application under test is identified as follows:

Application owner	HID Global
Operating System	Android
Application name and version	goID Starter App Version 1.0.2.5
Date of receipt of application	2023-08-17

Table 2 Identification of mDL Application under test

HID Global developed this mDL Application using a Software Development Kit (SDK) provided by HID Global. This SDK is identified as follows:

SDK Owner	HID Global
Operating System	Android
SDK Name and Version	goid-core-sdk-android-release-PI_3.23_R_2.2.1
SHA-256 hash over SDK	682b566b9bb7eaaf674074b13be98231e856142e39f05db8e3492236f812a00b

Table 3 Identification of mDL Application under test

Please refer to section 3.2 for more information.

1.4.2 CONFIGURATION

The mDL Application under test was configured to support the ISO/IEC 18013-5:2021 features as declared by HID Global in the Implementation Conformance Statement (ICS) in Appendix A.1.

1.4.3 NUMBER OF SAMPLES

HID Global provided UL with 1 test sample. The sample used for testing is identified in Appendix A.2.

1.4.4 MATERIALS RECEIVED FROM THE CLIENT

UL has referenced the following materials received from HID Global for testing activities.

Reference	Materials	Purpose	Receipt Date
1	IACA root certificate	To test Security Mechanism test cases	2023-07-07

Table 4: Materials received from the client.

1.5 UL eID TECHNOLOGY CERTIFICATION BODY LOCATION

The UL Certification Body (CB) operating under the eID Technology scheme is located at the address below.

UL VS INC.
1945 The Exchange, Suite 200 SE,
Atlanta, GA 30339
United States

1.6 UL CERTIFICATION TESTING LOCATION

UL certification testing activities were performed at the following location by the UL CB staff operating under the eID Technology certification scheme:

UL VS INC.
1945 The Exchange, Suite 200 SE,
Atlanta, GA 30339
United States

1.7 CUSTOMER CONTACT DETAILS

This document is the official test report for the following customer:

Customer Name	HID Global
Customer Contact	Fabrice Jogand-Coulomb
Customer Contact Email	Fabrice.jogandcoulomb@hidglobal.com
Customer Address	31 Rue de Verdun, Suresnes, Iles de France, 92150

Table 5: Customer contact details

1.8 UL CONTACT DETAILS

Test Analyst Name	Jerrin Thomas
Test Analyst Email	Jerrin.Thomas@ul.com
Lab Lead Name	Same as above
Lab Lead Email	Same as above

Table 6: UL contact details

1.9 DISCLAIMER

The test results in this report are valid for the mDL application name and version mentioned in section 1.4.1 when configured as described in section 1.4.2. HID Global provided all of the application software for testing by UL and is responsible for the configuration of all samples provided, as well as for the correctness of the data listed in Appendices A.1 and A.2.

The correct functioning of an mDL application is dependent on several factors in its operational environment, including but not limited to the availability and proper function of the supported technologies by the mobile device on which the application is installed, network connectivity, ISO/IEC 18013-5:2021 conformant behaviour of the mDL reader it interacts with, and availability of a correctly structured, ISO / IEC 18013-5:2021 conformant mDL data set provisioned by the Issuing Authority or its agent.

HID Global is solely and fully responsible for the conformity of all products to all applicable standards, specifications, and requirements.

2 TEST METHODOLOGY

2.1 TEST DEVICES

The mDL application under test was installed on the following mobile devices for testing. All test cases were executed with the application running on both devices.

Device	OS and version
Google Pixel 6a	Android 13
Samsung Galaxy S9	Android 10

Table 7 Test devices and OS versions used for certification testing.

2.2 TEST TOOLS

This mDL application certification testing was conducted using the following version of the UL mDL Test Tool, which consists of the UL mDL Test Suite and the UL mDL Test App.

Test Tool	Version
UL mDL Test Suite	UL mDL Application Test Suite v1.2.3
UL mDL Test App	mdltestapp-1.2.1.apk
Test Case Specification	UL mDL Test Case Specification[1]

Table 8 Tools used for testing.

2.3 TEST SCOPE

The test scope for certification includes all test cases in the UL mDL Test Case Specification. However, many of these test cases are conditional and must only be executed if the mDL Application under test supports one of the optional features of ISO/IEC 18013-5:2021. To determine which test cases to execute, UL used the Implementation Conformance Statement provided by HID Global, which is reproduced in Appendix A.1.

Section 4 contains an overview of all test cases, specifying the test result (Pass / Fail / Not Applicable / Inconclusive) for each.

[1] In the absence of a published version of ISO/IEC 18013-6, the official test standard for ISO/IEC 18013-5, UL is keeping the mDL Test Case Specification identical to the latest draft of ISO/IEC 18013-6 available within the responsible ISO Working Group.

2.4 TEST EXECUTION

During test execution, qualified UL Test Analysts:

1) Installed the mDL application under test on each of the test devices specified in section 2.1.
2) In collaboration with HID Global, ensured that the mDL Application was correctly configured.
3) Entered the configuration of the mDL application under test in the UL mDL Application Test Suite, according to the Implementation Conformance Statement (ICS) provided by HID Global.
4) Loaded the root certificate(s) and all applicable end-entity certificate(s) for relevant security mechanisms in the UL mDL Application Test Suite.
5) Executed all applicable test cases in the UL mDL Application Test Suite, using the associated UL mDL Test App to interact with the mDL application under test, as installed on each of the test devices, while also performing the required user interaction with the mDL application under test.
6) Analyzed the test results of each test case.
7) Reported the final test results in the UL mDL Application Certification Test Report.

2.5 TEST TIMEFRAME

The mDL application goID Starter App Version 1.0.2.5 was received from HID Global on 2023-08-17. Testing this version took place from 2023-08-17 to 2023-08-22 using the test devices identified in 2.1.

3 HIGH-LEVEL TEST RESULTS

3.1 OVERVIEW

Table 9 shows a summary of test results for the goID Starter App Version 1.0.2.5 mDL Application on all devices used for testing.

Device	OS Version	Pass	Fail	Not Applicable	Total
Google Pixel 6a	Android 13	225	0	234	459
Samsung Galaxy S9	Android 9	225	0	234	459

Table 9: High-level test results

For the goID Starter App Version 1.0.2.5 application as installed on the specified test devices, all applicable test cases were performed successfully and passed. The functional behaviour of the goID Starter App Version 1.0.2.5 application, as observed in the test environment, is conformant to ISO / IEC 18013-5:2021.

Section 4 contains a full overview of the test result of all test cases.

3.2 ONLINE AUDIT ON HID MDL APPLICATION SDK BUILD PROCESS

Before the certification, HID and UL participated in an online meeting on July 7th, 2023. The goal of this meeting was for HID to demonstrate to UL how the HID SDK is developed and integrated into an mDL application, and for UL to evaluate if all functions of the resulting application related to ISO/IEC 18013-5 are implemented within HID's SDK. Moreover, UL wanted to evaluate whether HID uses a managed and well-defined process for updating, releasing and versioning the SDK.

During the meeting, HID provided an overview of the system architecture and explained what functions are provided by the different components of the system. HID then went on explain how these components are managed, updated, and released. Next, HID discussed how to use SDK to create an mDL application, including demonstrating the API that the SDK provides. HID also showed how a developer can use this API to control the functions provided by the SDK. Finally, HID demonstrated the source code interface which sits between the SDK and any mDL Application which would be developed using the SDK.

After seeing parts of the source code, witnessing the build process, and discussing with the HID developers and experts, UL is confident that the SDK indeed provides all Android ISO/IEC 18013-5-related functions of an mDL application that is based on the SDK. Moreover, UL determined that HID indeed uses a managed and well-defined process for updating, releasing and versioning the SDK.

4 DETAILED TEST RESULTS

4.1 DATA MODEL TEST CASES

4.1.1 DATA MODEL

Test	Verdict	Paragraph
mDL_DM_FamilyName_01	Pass	
mDL_DM_FamilyName_02	Pass	
mDL_DM_FamilyName_03	Pass	
mDL_DM_GivenName_01	Pass	
mDL_DM_GivenName_02	Pass	
mDL_DM_GivenName_03	Pass	
mDL_DM_BirthDate_01	Pass	
mDL_DM_BirthDate_02	Pass	
mDL_DM_BirthDate_03	Pass	
mDL_DM_BirthDate_04	Pass	
mDL_DM_IssueDate_01	Pass	
mDL_DM_IssueDate_02	Pass	
mDL_DM_IssueDate_03	Pass	
mDL_DM_IssueDate_04	Pass	
mDL_DM_IssueDate_05	Pass	
mDL_DM_ExpiryDate_01	Pass	
mDL_DM_ExpiryDate_02	Pass	
mDL_DM_ExpiryDate_03	Pass	
mDL_DM_ExpiryDate_04	Pass	
mDL_DM_IssuingCountry_01	Pass	
mDL_DM_IssuingCountry_02	Pass	
mDL_DM_IssuingCountry_03	Pass	
mDL_DM_IssuingAuthority_01	Pass	
mDL_DM_IssuingAuthority_02	Pass	
mDL_DM_IssuingAuthority_03	Pass	
mDL_DM_DocumentNumber_01	Pass	
mDL_DM_DocumentNumber_02	Pass	
mDL_DM_DocumentNumber_03	Pass	
mDL_DM_Portrait_01	Pass	
mDL_DM_Portrait_02	Pass	
mDL_DM_Portrait_03	Pass	
mDL_DM_DrivingPrivileges_01	Pass	

mDL_DM_DrivingPrivileges_02	Pass	
mDL_DM_DrivingPrivileges_03	Pass	
mDL_DM_DrivingPrivileges_04	Pass	
mDL_DM_DrivingPrivileges_05	Pass	
mDL_DM_DrivingPrivileges_06	Pass	
mDL_DM_DrivingPrivileges_07	Pass	
mDL_DM_DrivingPrivileges_08	Pass	
mDL_DM_DrivingPrivileges_09	Pass	
mDL_DM_DrivingPrivileges_10	Pass	
mDL_DM_DrivingPrivileges_11	Pass	
mDL_DM_DrivingPrivileges_12	Pass	
mDL_DM_DrivingPrivileges_13	Pass	
mDL_DM_DrivingPrivileges_14	Pass	
mDL_DM_DrivingPrivileges_15	Pass	
mDL_DM_DrivingPrivileges_16	Pass	
mDL_DM_DrivingPrivileges_17	Pass	
mDL_DM_DrivingPrivileges_18	Pass	
mDL_DM_DrivingPrivileges_19	Pass	
mDL_DM_DrivingPrivileges_20	Pass	
mDL_DM_DrivingPrivileges_21	Pass	
mDL_DM_DrivingPrivileges_22	Pass	
mDL_DM_DrivingPrivileges_23	Pass	
mDL_DM_DrivingPrivileges_24	Pass	
mDL_DM_UNDistinguishingSign_01	Pass	
mDL_DM_UNDistinguishingSign_02	Pass	
mDL_DM_UNDistinguishingSign_03	Pass	
mDL_DM_AdministrativeNumber_01	Not Applicable	
mDL_DM_AdministrativeNumber_02	Not Applicable	
mDL_DM_AdministrativeNumber_03	Not Applicable	
mDL_DM_Sex_01	Pass	
mDL_DM_Sex_02	Pass	
mDL_DM_Sex_03	Pass	
mDL_DM_Height_01	Not Applicable	
mDL_DM_Height_02	Not Applicable	
mDL_DM_Weight_01	Not Applicable	
mDL_DM_Weight_02	Not Applicable	
mDL_DM_EyeColour_01	Not Applicable	
mDL_DM_EyeColour_02	Not Applicable	
mDL_DM_EyeColour_03	Not Applicable	

mDL_DM_HairColour_01	Not Applicable	
mDL_DM_HairColour_02	Not Applicable	
mDL_DM_HairColour_03	Not Applicable	
mDL_DM_BirthPlace_01	Not Applicable	
mDL_DM_BirthPlace_02	Not Applicable	
mDL_DM_BirthPlace_03	Not Applicable	
mDL_DM_ResidentAddress_01	Pass	
mDL_DM_ResidentAddress_02	Pass	
mDL_DM_ResidentAddress_03	Pass	
mDL_DM_PortraitCaptureDate_01	Not Applicable	
mDL_DM_PortraitCaptureDate_02	Not Applicable	
mDL_DM_PortraitCaptureDate_03	Not Applicable	
mDL_DM_PortraitCaptureDate_04	Not Applicable	
mDL_DM_AgeInYears_01	Not Applicable	
mDL_DM_AgeInYears_02	Not Applicable	
mDL_DM_AgeBirthYear_01	Not Applicable	
mDL_DM_AgeBirthYear_02	Not Applicable	
mDL_DM_AgeOverNN_01	Not Applicable	
mDL_DM_AgeOverNN_02	Not Applicable	
mDL_DM_AgeOverNN_03	Not Applicable	
mDL_DM_AgeOverNN_04	Not Applicable	
mDL_DM_AgeOverNN_05	Not Applicable	
mDL_DM_AgeOverNN_06	Not Applicable	
mDL_DM_AgeOverNN_07	Not Applicable	
mDL_DM_AgeOverNN_08	Not Applicable	
mDL_DM_AgeOverNN_09	Not Applicable	
mDL_DM_IssuingJurisdiction_01	Not Applicable	
mDL_DM_IssuingJurisdiction_02	Not Applicable	
mDL_DM_IssuingJurisdiction_03	Not Applicable	
mDL_DM_Nationality_01	Not Applicable	
mDL_DM_Nationality_02	Not Applicable	
mDL_DM_Nationality_03	Not Applicable	
mDL_DM_ResidentCity_01	Pass	
mDL_DM_ResidentCity_02	Pass	
mDL_DM_ResidentCity_03	Pass	
mDL_DM_ResidentState_01	Pass	
mDL_DM_ResidentState_02	Pass	
mDL_DM_ResidentState_03	Pass	
mDL_DM_ResidentPostalCode_01	Pass	

mDL_DM_ResidentPostalCode_02	Pass	
mDL_DM_ResidentPostalCode_03	Pass	
mDL_DM_ResidentCountry_01	Pass	
mDL_DM_ResidentCountry_02	Pass	
mDL_DM_ResidentCountry_03	Pass	
mDL_DM_BiometricTemplateXX_01	Not Applicable	
mDL_DM_BiometricTemplateXX_02	Not Applicable	
mDL_DM_BiometricTemplateXX_03	Not Applicable	
mDL_DM_BiometricTemplateXX_04	Not Applicable	
mDL_DM_BiometricTemplateXX_05	Not Applicable	
mDL_DM_BiometricTemplateXX_06	Not Applicable	
mDL_DM_BiometricTemplateXX_07	Not Applicable	
mDL_DM_BiometricTemplateXX_08	Not Applicable	
mDL_DM_BiometricTemplateXX_09	Not Applicable	
mDL_DM_BiometricTemplateXX_10	Not Applicable	
mDL_DM_BiometricTemplateXX_11	Not Applicable	
mDL_DM_BiometricTemplateXX_12	Not Applicable	
mDL_DM_BiometricTemplateXX_13	Not Applicable	
mDL_DM_BiometricTemplateXX_14	Not Applicable	
mDL_DM_BiometricTemplateXX_15	Not Applicable	
mDL_DM_BiometricTemplateXX_16	Not Applicable	
mDL_DM_BiometricTemplateXX_17	Not Applicable	
mDL_DM_BiometricTemplateXX_18	Not Applicable	
mDL_DM_BiometricTemplateXX_19	Not Applicable	
mDL_DM_BiometricTemplateXX_20	Not Applicable	
mDL_DM_BiometricTemplateXX_21	Not Applicable	
mDL_DM_BiometricTemplateXX_22	Not Applicable	
mDL_DM_BiometricTemplateXX_23	Not Applicable	
mDL_DM_BiometricTemplateXX_24	Not Applicable	
mDL_DM_BiometricTemplateXX_25	Not Applicable	
mDL_DM_BiometricTemplateXX_26	Not Applicable	
mDL_DM_BiometricTemplateXX_27	Not Applicable	
mDL_DM_BiometricTemplateXX_28	Not Applicable	
mDL_DM_BiometricTemplateXX_29	Not Applicable	
mDL_DM_BiometricTemplateXX_30	Not Applicable	
mDL_DM_BiometricTemplateXX_31	Not Applicable	
mDL_DM_BiometricTemplateXX_32	Not Applicable	
mDL_DM_BiometricTemplateXX_33	Not Applicable	
mDL_DM_BiometricTemplateXX_34	Not Applicable	

mDL_DM_BiometricTemplateXX_35	Not Applicable	
mDL_DM_BiometricTemplateXX_36	Not Applicable	
mDL_DM_BiometricTemplateXX_37	Not Applicable	
mDL_DM_BiometricTemplateXX_38	Not Applicable	
mDL_DM_BiometricTemplateXX_39	Not Applicable	
mDL_DM_BiometricTemplateXX_40	Not Applicable	
mDL_DM_FamilyNameNationalCharacter_01	Not Applicable	
mDL_DM_FamilyNameNationalCharacter_02	Not Applicable	
mDL_DM_GivenNameNationalCharacter_01	Not Applicable	
mDL_DM_GivenNameNationalCharacter_02	Not Applicable	
mDL_DM_SignatureUsualMark_01	Not Applicable	
mDL_DM_SignatureUsualMark_02	Not Applicable	
mDL_DM_SignatureUsualMark_03	Not Applicable	

4.2 MESSAGE STRUCTURE TEST CASES

4.2.1 MESSAGE STRUCTURE\DEVICE ENGAGEMENT\GENERAL

Test	Verdict	Paragraph
mDL_MS_DE_Gen_01	Pass	
mDL_MS_DE_Gen_02	Pass	
mDL_MS_DE_Gen_03	Pass	
mDL_MS_DE_Gen_04	Pass	
mDL_MS_DE_Gen_05	Pass	
mDL_MS_DE_Gen_06	Pass	
mDL_MS_DE_Gen_07	Pass	
mDL_MS_DE_Gen_08	Pass	
mDL_MS_DE_Gen_09	Pass	
mDL_MS_DE_Gen_10	Not Applicable	
mDL_MS_DE_Gen_11	Pass	
mDL_MS_DE_Gen_12	Pass	
mDL_MS_DE_Gen_13	Not Applicable	
mDL_MS_DE_Gen_14	Not Applicable	
mDL_MS_DE_Gen_15	Not Applicable	
mDL_MS_DE_Gen_16	Not Applicable	
mDL_MS_DE_Gen_17	Not Applicable	
mDL_MS_DE_Gen_18	Not Applicable	
mDL_MS_DE_Gen_19	Not Applicable	
mDL_MS_DE_Gen_20	Not Applicable	

mDL_MS_DE_Gen_21	Not Applicable	
mDL_MS_DE_Gen_22	Not Applicable	
mDL_MS_DE_Gen_23	Not Applicable	
mDL_MS_DE_Gen_24	Not Applicable	

4.2.2 MESSAGE STRUCTURE\DEVICE ENGAGEMENT\DATA RETRIEVAL BLE

Test	Verdict	Paragraph
mDL_MS_DE_DRBLE_01	Pass	
mDL_MS_DE_DRBLE_02	Not Applicable	
mDL_MS_DE_DRBLE_03	Pass	
mDL_MS_DE_DRBLE_04	Pass	
mDL_MS_DE_DRBLE_05	Not Applicable	
mDL_MS_DE_DRBLE_06	Pass	
mDL_MS_DE_DRBLE_07	Pass	
mDL_MS_DE_DRBLE_08	Not Applicable	
mDL_MS_DE_DRBLE_09	Not Applicable	
mDL_MS_DE_DRBLE_10	Pass	
mDL_MS_DE_DRBLE_11	Not Applicable	
mDL_MS_DE_DRBLE_12	Not Applicable	
mDL_MS_DE_DRBLE_13	Pass	
mDL_MS_DE_DRBLE_14	Not Applicable	
mDL_MS_DE_DRBLE_15	Pass	
mDL_MS_DE_DRBLE_16	Pass	
mDL_MS_DE_DRBLE_17	Not Applicable	
mDL_MS_DE_DRBLE_18	Not Applicable	
mDL_MS_DE_DRBLE_19	Not Applicable	
mDL_MS_DE_DRBLE_20	Pass	

4.2.3 MESSAGE STRUCTURE\DEVICE ENGAGEMENT\DATA RETRIEVAL NFC

Test	Verdict	Paragraph
mDL_MS_DE_DRNFC_01	Not Applicable	
mDL_MS_DE_DRNFC_02	Pass	
mDL_MS_DE_DRNFC_03	Not Applicable	
mDL_MS_DE_DRNFC_04	Not Applicable	
mDL_MS_DE_DRNFC_05	Not Applicable	
mDL_MS_DE_DRNFC_06	Not Applicable	

4.2.4 MESSAGE STRUCTURE\DEVICE ENGAGEMENT\DATA RETRIEVAL\WIFI-AWARE

Test	Verdict	Paragraph
mDL_MS_DE_DRWiFi_01	Not Applicable	
mDL_MS_DE_DRWiFi_02	Pass	
mDL_MS_DE_DRWiFi_03	Not Applicable	
mDL_MS_DE_DRWiFi_04	Not Applicable	
mDL_MS_DE_DRWiFi_05	Not Applicable	
mDL_MS_DE_DRWiFi_06	Not Applicable	

4.2.5 MESSAGE STRUCTURE\SESSIONDATA

Test	Verdict	Paragraph
mDL_MS_SD_01	Pass	
mDL_MS_SD_02	Pass	
mDL_MS_SD_03	Pass	
mDL_MS_SD_04	Pass	

4.2.6 MESSAGE STRUCTURE\DEVICEREQUEST

Test	Verdict	Paragraph
mDL_MS_DReq_01	Pass	
mDL_MS_DReq_02	Pass	
mDL_MS_DReq_03	Pass	
mDL_MS_DReq_04	Pass	
mDL_MS_DReq_05	Pass	

4.2.7 MESSAGE STRUCTURE\DEVICE RESPONSE\HAPPY FLOW\GENERIC

Test	Verdict	Paragraph
mDL_MS_DR_HF_Gen_01	Pass	
mDL_MS_DR_HF_Gen_02	Pass	
mDL_MS_DR_HF_Gen_03	Pass	
mDL_MS_DR_HF_Gen_04	Pass	
mDL_MS_DR_HF_Gen_05	Pass	
mDL_MS_DR_HF_Gen_06	Pass	
mDL_MS_DR_HF_Gen_07	Pass	
mDL_MS_DR_HF_Gen_08	Pass	
mDL_MS_DR_HF_Gen_09	Pass	

mDL_MS_DR_HF_Gen_10	Pass	
mDL_MS_DR_HF_Gen_11	Pass	
mDL_MS_DR_HF_Gen_12	Pass	
mDL_MS_DR_HF_Gen_13	Pass	
mDL_MS_DR_HF_Gen_14	Pass	
mDL_MS_DR_HF_Gen_15	Pass	
mDL_MS_DR_HF_Gen_16	Pass	
mDL_MS_DR_HF_Gen_17	Pass	
mDL_MS_DR_HF_Gen_18	Pass	
mDL_MS_DR_HF_Gen_19	Pass	
mDL_MS_DR_HF_Gen_20	Pass	
mDL_MS_DR_HF_Gen_21	Pass	
mDL_MS_DR_HF_Gen_22	Pass	
mDL_MS_DR_HF_Gen_23	Pass	
mDL_MS_DR_HF_Gen_24	Pass	
mDL_MS_DR_HF_Gen_25	Pass	
mDL_MS_DR_HF_Gen_26	Pass	
mDL_MS_DR_HF_Gen_27	Pass	
mDL_MS_DR_HF_Gen_28	Pass	
mDL_MS_DR_HF_Gen_29	Pass	
mDL_MS_DR_HF_Gen_30	Pass	
mDL_MS_DR_HF_Gen_31	Pass	
mDL_MS_DR_HF_Gen_32	Not Applicable	
mDL_MS_DR_HF_Gen_33	Not Applicable	
mDL_MS_DR_HF_Gen_34	Not Applicable	
mDL_MS_DR_HF_Gen_35	Pass	
mDL_MS_DR_HF_Gen_36	Pass	
mDL_MS_DR_HF_Gen_37	Pass	
mDL_MS_DR_HF_Gen_38	Pass	
mDL_MS_DR_HF_Gen_39	Pass	
mDL_MS_DR_HF_Gen_40	Pass	
mDL_MS_DR_HF_Gen_41	Pass	
mDL_MS_DR_HF_Gen_42	Pass	
mDL_MS_DR_HF_Gen_43	Pass	
mDL_MS_DR_HF_Gen_44	Not Applicable	
mDL_MS_DR_HF_Gen_45	Not Applicable	
mDL_MS_DR_HF_Gen_46	Not Applicable	
mDL_MS_DR_HF_Gen_47	Not Applicable	
mDL_MS_DR_HF_Gen_48	Not Applicable	

mDL_MS_DR_HF_Gen_49	Not Applicable	
mDL_MS_DR_HF_Gen_50	Not Applicable	
mDL_MS_DR_HF_Gen_51	Not Applicable	
mDL_MS_DR_HF_Gen_52	Not Applicable	
mDL_MS_DR_HF_Gen_53	Not Applicable	
mDL_MS_DR_HF_Gen_54	Not Applicable	
mDL_MS_DR_HF_Gen_55	Not Applicable	
mDL_MS_DR_HF_Gen_56	Not Applicable	

4.2.8 MESSAGE STRUCTURE\DEVICE RESPONSE\HAPPY FLOW\MOBILESECURITYOBJECT

Test	Verdict	Paragraph
mDL_MS_DR_HF_MSO_01	Pass	
mDL_MS_DR_HF_MSO_02	Pass	
mDL_MS_DR_HF_MSO_03	Pass	
mDL_MS_DR_HF_MSO_04	Pass	
mDL_MS_DR_HF_MSO_05	Pass	
mDL_MS_DR_HF_MSO_06	Pass	
mDL_MS_DR_HF_MSO_07	Pass	
mDL_MS_DR_HF_MSO_08	Pass	
mDL_MS_DR_HF_MSO_09	Pass	
mDL_MS_DR_HF_MSO_10	Pass	
mDL_MS_DR_HF_MSO_11	Pass	
mDL_MS_DR_HF_MSO_12	Pass	
mDL_MS_DR_HF_MSO_13	Pass	
mDL_MS_DR_HF_MSO_14	Pass	
mDL_MS_DR_HF_MSO_15	Pass	
mDL_MS_DR_HF_MSO_16	Pass	
mDL_MS_DR_HF_MSO_17	Pass	
mDL_MS_DR_HF_MSO_18	Pass	
mDL_MS_DR_HF_MSO_19	Pass	
mDL_MS_DR_HF_MSO_20	Pass	
mDL_MS_DR_HF_MSO_21	Pass	
mDL_MS_DR_HF_MSO_22	Pass	
mDL_MS_DR_HF_MSO_23	Pass	
mDL_MS_DR_HF_MSO_24	Pass	
mDL_MS_DR_HF_MSO_25	Pass	
mDL_MS_DR_HF_MSO_26	Pass	
mDL_MS_DR_HF_MSO_27	Pass	

mDL_MS_DR_HF_MSO_28	Pass	
mDL_MS_DR_HF_MSO_29	Pass	
mDL_MS_DR_HF_MSO_30	Pass	
mDL_MS_DR_HF_MSO_31	Pass	
mDL_MS_DR_HF_MSO_32	Pass	
mDL_MS_DR_HF_MSO_33	Pass	
mDL_MS_DR_HF_MSO_34	Pass	
mDL_MS_DR_HF_MSO_35	Pass	

4.2.9 MESSAGE STRUCTURE\DEVICE RESPONSE\UNHAPPY FLOW

Test	Verdict	Paragraph
mDL_MS_DR_UF_01	Pass	
mDL_MS_DR_UF_02	Pass	
mDL_MS_DR_UF_03	Pass	
mDL_MS_DR_UF_04	Pass	
mDL_MS_DR_UF_05	Pass	
mDL_MS_DR_UF_06	Pass	
mDL_MS_DR_UF_07	Pass	
mDL_MS_DR_UF_08	Pass	
mDL_MS_DR_UF_09	Pass	
mDL_MS_DR_UF_10	Pass	
mDL_MS_DR_UF_11	Pass	
mDL_MS_DR_UF_12	Pass	
mDL_MS_DR_UF_13	Pass	

4.3 TECHNOLOGIES TEST CASES

4.3.1 TECHNOLOGIES\DEVICE ENGAGEMENT\NFC

Test	Verdict	Paragraph
mDL_Tech_DE_NFC_01	Not Applicable	
mDL_Tech_DE_NFC_02	Not Applicable	
mDL_Tech_DE_NFC_03	Not Applicable	
mDL_Tech_DE_NFC_04	Not Applicable	
mDL_Tech_DE_NFC_05	Not Applicable	
mDL_Tech_DE_NFC_06	Not Applicable	
mDL_Tech_DE_NFC_07	Not Applicable	
mDL_Tech_DE_NFC_08	Not Applicable	

mDL_Tech_DE_NFC_09	Not Applicable	
mDL_Tech_DE_NFC_10	Not Applicable	
mDL_Tech_DE_NFC_11	Not Applicable	
mDL_Tech_DE_NFC_12	Not Applicable	
mDL_Tech_DE_NFC_13	Not Applicable	
mDL_Tech_DE_NFC_14	Not Applicable	
mDL_Tech_DE_NFC_15	Not Applicable	
mDL_Tech_DE_NFC_16	Not Applicable	
mDL_Tech_DE_NFC_17	Not Applicable	

4.3.2 TECHNOLOGIES\DEVICE ENGAGEMENT\QR CODE

Test	Verdict	Paragraph
mDL_Tech_DE_QR_01	Pass	

4.3.3 TECHNOLOGIES\DEVICE RETRIEVAL\BLE

Test	Verdict	Paragraph
mDL_Tech_DR_BLE_01	Pass	
mDL_Tech_DR_BLE_02	Pass	
mDL_Tech_DR_BLE_03	Not Applicable	
mDL_Tech_DR_BLE_04	Not Applicable	
mDL_Tech_DR_BLE_05	Pass	
mDL_Tech_DR_BLE_06	Not Applicable	
mDL_Tech_DR_BLE_07	Not Applicable	
mDL_Tech_DR_BLE_08	Not Applicable	
mDL_Tech_DR_BLE_09	Not Applicable	
mDL_Tech_DR_BLE_10	Not Applicable	
mDL_Tech_DR_BLE_11	Not Applicable	
mDL_Tech_DR_BLE_12	Not Applicable	
mDL_Tech_DR_BLE_13	Not Applicable	
mDL_Tech_DR_BLE_14	Pass	
mDL_Tech_DR_BLE_15	Not Applicable	
mDL_Tech_DR_BLE_16	Not Applicable	
mDL_Tech_DR_BLE_17	Not Applicable	
mDL_Tech_DR_BLE_18	Not Applicable	
mDL_Tech_DR_BLE_19	Not Applicable	
mDL_Tech_DR_BLE_20	Not Applicable	
mDL_Tech_DR_BLE_21	Not Applicable	

4.3.4 TECHNOLOGIES\DEVICE RETRIEVAL\NFC

Test	Verdict	Paragraph
mDL_Tech_DR_NFC_01	Not Applicable	
mDL_Tech_DR_NFC_02	Not Applicable	
mDL_Tech_DR_NFC_03	Not Applicable	
mDL_Tech_DR_NFC_04	Not Applicable	
mDL_Tech_DR_NFC_05	Not Applicable	
mDL_Tech_DR_NFC_06	Not Applicable	
mDL_Tech_DR_NFC_07	Not Applicable	

4.3.5 TECHNOLOGIES\DEVICE RETRIEVAL\WIFI-AWARE

Test	Verdict	Paragraph
mDL_Tech_DR_WiFi_01	Not Applicable	
mDL_Tech_DR_WiFi_02	Not Applicable	
mDL_Tech_DR_WiFi_03	Not Applicable	
mDL_Tech_DR_WiFi_04	Not Applicable	
mDL_Tech_DR_WiFi_05	Not Applicable	
mDL_Tech_DR_WiFi_06	Not Applicable	
mDL_Tech_DR_WiFi_07	Not Applicable	
mDL_Tech_DR_WiFi_08	Not Applicable	

4.4 SECURITY MECHANISMS TEST CASES

4.4.1 SECURITY MECHANISMS\ISSUER DATA AUTHENTICATION

Test	Verdict	Paragraph
mDL_SM_IDA_01		
mDL_SM_IDA_02		

4.4.2 SECURITY MECHANISMS\MDOC AUTHENTICATION\GENERAL

Test	Verdict	Paragraph
mDL_SM_mdocAuth_Gen_01		

4.4.3 SECURITY MECHANISMS\MDOC AUTHENTICATION\MAC

Test	Verdict	Paragraph
mDL_SM_mdocAuth_MAC_01	Not Applicable	
mDL_SM_mdocAuth_MAC_02	Not Applicable	
mDL_SM_mdocAuth_MAC_03	Not Applicable	

4.4.4 SECURITY MECHANISMS\MDOC AUTHENTICATION\ECdDSA

Test	Verdict	Paragraph
mDL_SM_mdocAuth_ECdDSA_01		
mDL_SM_mdocAuth_ECdDSA_02	Not Applicable	
mDL_SM_mdocAuth_ECdDSA_03	Not Applicable	

4.4.5 SECURITY MECHANISMS\MDOC READER AUTHENTICATION\HAPPY FLOW

Test	Verdict	Paragraph
mDL_SM_mdocRAuth_HF_01	Not Applicable	
mDL_SM_mdocRAuth_HF_02	Not Applicable	
mDL_SM_mdocRAuth_HF_03	Not Applicable	
mDL_SM_mdocRAuth_HF_04	Not Applicable	
mDL_SM_mdocRAuth_HF_05	Not Applicable	

4.4.6 SECURITY MECHANISMS\MDOC READER AUTHENTICATION\UNHAPPY FLOW

Test	Verdict	Paragraph
mDL_SM_mdocRAuth_UF_01	Not Applicable	
mDL_SM_mdocRAuth_UF_02	Not Applicable	
mDL_SM_mdocRAuth_UF_03	Not Applicable	
mDL_SM_mdocRAuth_UF_04	Not Applicable	
mDL_SM_mdocRAuth_UF_05	Not Applicable	
mDL_SM_mdocRAuth_UF_06	Not Applicable	
mDL_SM_mdocRAuth_UF_07	Not Applicable	
mDL_SM_mdocRAuth_UF_08	Not Applicable	
mDL_SM_mdocRAuth_UF_09	Not Applicable	
mDL_SM_mdocRAuth_UF_10	Not Applicable	
mDL_SM_mdocRAuth_UF_11	Not Applicable	
mDL_SM_mdocRAuth_UF_12	Not Applicable	
mDL_SM_mdocRAuth_UF_13	Not Applicable	
mDL_SM_mdocRAuth_UF_14	Not Applicable	
mDL_SM_mdocRAuth_UF_15	Not Applicable	
mDL_SM_mdocRAuth_UF_16	Not Applicable	
mDL_SM_mdocRAuth_UF_17	Not Applicable	
mDL_SM_mdocRAuth_UF_18	Not Applicable	
mDL_SM_mdocRAuth_UF_19	Not Applicable	
mDL_SM_mdocRAuth_UF_20	Not Applicable	
mDL_SM_mdocRAuth_UF_21	Not Applicable	
mDL_SM_mdocRAuth_UF_22	Not Applicable	
mDL_SM_mdocRAuth_UF_23	Not Applicable	
mDL_SM_mdocRAuth_UF_24	Not Applicable	
mDL_SM_mdocRAuth_UF_25	Not Applicable	
mDL_SM_mdocRAuth_UF_26	Not Applicable	
mDL_SM_mdocRAuth_UF_27	Not Applicable	
mDL_SM_mdocRAuth_UF_28	Not Applicable	

mDL_SM_mdocRAuth_UF_29	Not Applicable	

4.4.7 SECURITY MECHANISMS\SESSION ENCRYPTION\DEVICE ENGAGEMENT

Test	Verdict	Paragraph
mDL_SM_SEnc_DE_01	Pass	
mDL_SM_SEnc_DE_02	Pass	

4.4.8 SECURITY MECHANISMS\SESSION ENCRYPTION\SESSION DATA

Test	Verdict	Paragraph
mDL_SM_SEnc_SD_01	Not Applicable	

4.4.9 SECURITY MECHANISMS\SESSION ENCRYPTION\SESSION ESTABLISHMENT\HAPPY FLOW

Test	Verdict	Paragraph
mDL_SM_SEnc_SEst_HF_01	Pass	
mDL_SM_SEnc_SEst_HF_02	Not Applicable	
mDL_SM_SEnc_SEst_HF_03	Not Applicable	

4.4.10 SECURITY MECHANISMS\SESSION ENCRYPTION\SESSION ESTABLISHMENT\UNHAPPY FLOW

Test	Verdict	Paragraph
mDL_SM_SEnc_SEst_UF_01	Pass	
mDL_SM_SEnc_SEst_UF_02	Pass	
mDL_SM_SEnc_SEst_UF_03	Pass	
mDL_SM_SEnc_SEst_UF_04	Pass	
mDL_SM_SEnc_SEst_UF_05	Pass	
mDL_SM_SEnc_SEst_UF_06	Pass	
mDL_SM_SEnc_SEst_UF_07	Pass	
mDL_SM_SEnc_SEst_UF_08	Pass	
mDL_SM_SEnc_SEst_UF_09	Pass	
mDL_SM_SEnc_SEst_UF_10	Pass	

4.4.11 SECURITY MECHANISMS\SESSION ENCRYPTION\SESSION TERMINATION

Test	Verdict	Paragraph
mDL_SM_SEnc_ST_01	Not Applicable	
mDL_SM_SEnc_ST_02	Not Applicable	
mDL_SM_SEnc_ST_03	Not Applicable	
mDL_SM_SEnc_ST_04	Pass	
mDL_SM_SEnc_ST_05	Not Applicable	
mDL_SM_SEnc_ST_06	Pass	

4.5 USE CASES TEST CASES

Test	Verdict	Paragraph
mDL_UC_01	Pass	
mDL_UC_02	Not Applicable	
mDL_UC_03	Pass	
mDL_UC_04	Pass	
mDL_UC_05	Pass	
mDL_UC_06	Not Applicable	
mDL_UC_07	Not Applicable	
mDL_UC_08	Pass	
mDL_UC_09	Not Applicable	
mDL_UC_10	Pass	

5 AUTHORIZATION

5.1 REPORT VALIDITY

This report is valid for one year from the date of issuance of the current version of the application. If HID Global chooses to update the application to a new version, this certification does not apply to the new version/s. This certification also does not apply to previous versions of the application that were not tested and certified.

This report was prepared by the evaluation staff for the project:

Name: Jerrin Jose Thomas
Title: Test Analyst
Date: 2023-08-22

5.2 AUTHORIZATION

This report has been reviewed, confirmed, and authorized by the UL eID Technology Certification Scheme Technical Lead

Name: David Bakker
Title: Technical Lead
Date: 2023-08-31

Signature:

A.1 IMPLEMENTATION CONFORMANCE STATEMENT FOR HID GLOBAL

The Implementation Conformance Statements below were provided to UL by HID Global and have been used to determine which test cases to execute, in accordance with[1] and [2].

The ICS version used by HID Global is 1.7.

A.1.1 GENERAL INFORMATION

mDL Owner General Information	
Application owner Name	HID Global
Address	31 rue de Verdun
City	Suresnes
State	Iles de France
Zip Code / Postal Code	92150
Country	France
Contact Name	Fabrice Jogand-Coulomb
Contact Title	Director of Identity Products
Contact Email Address	Fabrice.jogandcoulomb@hidglobal.com
Contact Phone Number	+33678336199

mDL Application General Information	
Certification Type	☒ Functional [2] ☐ Integrated Product [3]
Application name and version	goID SDK
The minimum version of Android supported	Android 10
How many documents are present on the mDL under test?	2
For each document, please specify the applicable DocType	org.iso.18013.5.1.mDL
For each document, please specify all data element namespaces used by the document	org.iso.18013.5.1.mDL: - org.iso.18013.5.1 - iso.org.dod.internet.private.enterprise.hid.goID.sdk.data.1 - org.aamva.18013.5.1 - org.iso.18013.5.1.aamva

[2] For functional certification, the mDL data set can be a sample data set that the mDL owner would like to personalize onto the mDL.

[3] Integrated product certification requires the mDL data set to be prepared and personalized by an Issuer System of Record (SoR) and the mDL data set shall be a representative of the mDL that will be used in production.

For each namespace different from the mDL namespace ("org.iso.18013.5.1"), please specify the identifiers of all data elements present in the document	All mandatory data elements +: "iso.org.dod.internet.private.enterprise.hid.goID.sdk.data.1" : ["objectDataJSON", "objectIssuerJson"], "org.aamva.18013.5.1" : ["real_id"], "org.iso.18013.5.1.aamva" : ["DHS_compliance", "EDL_credential"]

A.1.2 FOR MDL DATA MODEL TESTS

Note: all the data elements in this section are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in this section must be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

#	ICS statements for mDL Data Model test cases	
1.	Data element administrative_number is present in the mDL data.	☐YES ☒NO
2.	Data element sex is present in the mDL data.	☒YES ☐NO
3.	Data element height is present in the mDL data.	☐YES ☒NO
4.	Data element weight is present in the mDL data.	☐YES ☒NO
5.	Data element eye_color is present in the mDL data.	☐YES ☒NO
6.	Data element hair_color is present in the mDL data.	☐YES ☒NO
7.	Data element birth_place is present in the mDL data.	☐YES ☒NO
8.	Data element resident_address is present in the mDL data.	☒YES ☐NO
9.	Data element portrait_capture_date is present in the mDL data.	☐YES ☒NO
10.	Data element age_in_years is present in the mDL data.	☐YES ☒NO
11.	Data element age_birth_year is present in the mDL data.	☐YES ☒NO
12.	Data element age_over_NN is present in the mDL data. In case you select YES, please provision the following age_over_NN data elements in the mDL data with the corresponding values (TRUE / FALSE) during personalization.	☐YES ☒NO
	NN	**Return Value**
	age_over_15	TRUE
	age_over_18	TRUE
	age_over_21	TRUE
	age_over_60	FALSE
	age_over_65	FALSE
	age_over_68	FALSE
13.	Data element issuing_jurisdiction is present in the mDL data.	☐YES ☒NO
14.	Data element nationality is present in the mDL data.	☐YES ☒NO
15.	Data element resident_city is present in the mDL data.	☒YES ☐NO
16.	Data element resident_state is present in the mDL data.	☒YES ☐NO
17.	Data element resident_postal_code is present in the mDL data.	☒YES ☐NO

18.	Data element resident_country is present in the mDL data.	☒YES ☐NO
19.	Data element biometric_template_face is present in the mDL data.	☐YES ☒NO
20.	Data element biometric_template_voice is present in the mDL data.	☐YES ☒NO
21.	Data element biometric_template_finger is present in the mDL data.	☐YES ☒NO
22.	Data element biometric_template_iris is present in the mDL data.	☐YES ☒NO
23.	Data element biometric_template_retina is present in the mDL data.	☐YES ☒NO
24.	Data element biometric_template_hand_geometry is present in the mDL data.	☐YES ☒NO
25.	Data element biometric_template_signature_sign is present in the mDL data.	☐YES ☒NO
26.	Data element biometric_template_keystroke is present in the mDL data.	☐YES ☒NO
27.	Data element biometric_template_lip_movement is present in the mDL data.	☐YES ☒NO
28.	Data element biometric_template_thermal_face is present in the mDL data.	☐YES ☒NO
29.	Data element biometric_template_thermal_hand is present in the mDL data.	☐YES ☒NO
30.	Data element biometric_template_gait is present in the mDL data.	☐YES ☒NO
31.	Data element biometric_template_body_odor is present in the mDL data.	☐YES ☒NO
32.	Data element biometric_template_dna is present in the mDL data.	☐YES ☒NO
33.	Data element biometric_template_ear is present in the mDL data.	☐YES ☒NO
34.	Data element biometric_template_finger_geometry is present in the mDL data.	☐YES ☒NO
35.	Data element biometric_template_palm_geometry is present in the mDL data.	☐YES ☒NO
36.	Data element biometric_template_vein_pattern is present in the mDL data.	☐YES ☒NO
37.	Data element biometric_template_foot_print is present in the mDL data.	☐YES ☒NO
38.	Data element family_name_national_character is present in the mDL data.	☐YES ☒NO
39.	Data element given_name_national_character is present in the mDL data.	☐YES ☒NO

40.	Data element signature_usual_mark is present in the mDL data.	☐YES ☒NO

A.1.3 FOR TECHNOLOGY TESTS

#	ICS statements for Technology test cases	
41.	mDL supports device engagement using NFC Static Handover	☐YES ☒NO
42.	mDL supports device engagement using NFC Negotiated Handover [4]	☐YES ☒NO
43.	mDL supports device engagement using QR code	☒YES ☐NO
44.	mDL supports device retrieval using NFC	☐YES ☒NO
45.	mDL supports extended-length APDU for device retrieval using NFC	☐YES ☒NO
46.	mDL supports BLE version 4.2 (or above) and LE Data Packet Length Extension	☒YES ☐NO
47.	mDL supports device retrieval using BLE in mdoc central client mode	☒YES ☐NO
48.	If BLE in mdoc central client mode is used for device retrieval, mdoc verifies the value of the Ident characteristic	☐YES ☒NO
49.	mDL supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE	☐YES ☒NO
50.	mDL supports device retrieval using BLE in mdoc peripheral server mode	☐YES ☒NO
51.	mDL supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE	☐YES ☒NO
52.	mDL supports device retrieval using Wi-Fi Aware	☐YES ☒NO
53.	mDL supports the NCS-PK-2WDH-128 cipher suite for Wi-Fi Aware [5]	☐YES ☒NO
54.	mDL supports server retrieval using OIDC	☐YES ☒NO
55.	mDL supports server retrieval using WebAPI	☐YES ☒NO
56.	mDL supports transferring server retrieval information in the device engagement structure	☐YES ☒NO

4 Note that NFC Static Handover and NFC Negotiated Handover cannot be supported simultaneously if an mDL supports both technologies.

5 Only applicable in case the mdoc supports Wi-Fi Aware for device retrieval and supports NFC Negotiated Handover for device engagement.

57.	mDL implements a time-out for the time between sending device engagement data and receiving the session establishment message	☒YES ☐NO
58.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	N/A

A.1.4 FOR SECURITY MECHANISM TESTS

	ICS statements for Security Mechanisms test cases	
59.	Which curves does the mDL support for session establishment? Tick all that are supported.[6]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
60.	mDL supports exchanging more than one device retrieval mdoc request and response with the mdoc reader in a single session.	☐YES ☒NO
61.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	
62.	Which curves does the mDL issuing authority support for issuer data authentication? Tick all that are supported.[7]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
63.	The mDL supports mdoc MAC authentication.	☐ YES ☒ NO

6 If the mDL supports multiple curves for session establishment, then for the purpose of testing, the mDL owner should provide a separate sample for each of the curves supported.

7 If multiple documents are present on the mDL, the issuing authority can in theory use a different curve for signing the MSO on each of them. However, please note that UL expects the same curve is used for all documents on a given sample. For the purpose of testing, the mDL owner should provide a separate sample for each of the curves supported.

64.	If yes, which curves does the mDL support for mdoc MAC authentication? Tick all that are supported [8]	☐ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
65.	The mDL supports mdoc ECDSA/EdDSA authentication	☒ YES ☐ NO
66.	If yes, which curves does the mDL use for mdoc ECDSA/EdDSA authentication? Tick all that are supported[9]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
67.	The mDL supports mdoc reader authentication	☐YES ☒NO
68.	If yes, which curves does the mdoc support for mdoc reader authentication? Tick all that are supported[10].	☐ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1

8 If multiple documents are present on the mDL, the mDL can in theory use a different mdoc MAC authentication curve for each of them. However, please note that UL expects the same curve is used for all documents on a given sample. For the purpose of testing, the mDL owner should provide a separate sample for each of the curves supported.

9 Note that for each document on an mDL, there could potentially be multiple SDeviceKey pairs for mdoc authentication, each in a separate MSO. It is therefore theoretically possible that a single document uses MAC authentication and ECDSA/EdDSA authentication alternatingly or uses different curves for ECDSA/EdDSA alternatingly. However, please note that UL expects that the same mdoc authentication mechanism (either MAC or ECDSA/EdDSA) is consistently used for all documents on a given sample. Moreover, UL expects that the same ECDSA/EdDSA curve is used for all documents on a given sample. For the purpose of testing, the mDL owner should provide a separate sample for each of the curves supported.

10 UL assumes that all mDL samples provided to us will support all of the mdoc reader authentication curves selected (provided that the correct CA certificates are installed).

69.	If yes, does the mdoc show an error message to the mdoc holder if reader authentication fails?	NA
70.	If yes, are there any of data elements that the mdoc will not release if reader authentication fails? If so, please list them all by namespace and identifier.[11]	☐YES ☒NO
71.	If yes, mdoc supports retrieving OCSP information, if available, when verifying a mdoc reader authentication certificate.	☐YES ☒NO
72.	A test CRL for all IACA root certificates provided by the customer is available during testing	☐YES ☒NO
73.	A test CRL for all Document Signer certificates used by the mdoc is available during testing	☐YES ☒NO

A.1.5 FOR USE CASE TESTS

#	ICS statements for Use Case test cases	
74.	The mDL allows the mDL holder to refuse consent for sharing the portrait, while allowing the sharing of other data elements requested in the same request	☒YES ☐NO

11 UL assumes that if mdoc reader authentication is supported, there is at least one data element that will not be released if mdoc reader authentication is not performed or fails.

A.2 OVERVIEW OF SAMPLES USED FOR TESTING

A.2.1 Overview

To fully test the HID Global's Android-based mDL application, UL used 1 samples which is goID Starter App Version 1.0.2.5. The table below detail how HID Global personalized these samples.

A.2.2 Sample HID Global_Android_01

Sample Identification	
Application name and version	goID Starter App Version 1.0.2.5
Sample Identification Number	HID Global_Android_01
Date of Receipt of Sample	2023-08-17

Sample ID	HID Global_Android_01
Sample supporting curve	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
Sample supporting the above curve for security mechanism	☒ Session establishment ☒ Issuer data authentication ☐ mdoc MAC authentication ☒ mdoc ECDSA/EdDSA authentication ☐ mdoc reader authentication
Device engagement configured	☒ QR code ☐ NFC Static Handover ☐ NFC Negotiated Handover
Data elements personalized	Sample mDL data set personalized by HID Global.

To fully test the HID Global's Android-based mDL applications, UL used the following certificates.

Certificates	
IACA root certificate(s)	goIDmDLIACA.cer
Date of receipt of IACA root certificates	2023-07-07

- End of Report -