Fime test session confirmation letter

Conformity test of the iOS-based GoID Sample App (2.18.0.645) application to

ISO/IEC 18013-5:2021

Test session carried out for

TOPPAN Security

Fime hereby confirms that the iOS-based GoID Sample App (2.18.0.645) application, developed by TOPPAN Security, built using SDK name and version TOPPAN VC SDK for iOS (2.18.0.645), has completed mDL application compliance testing carried out in accordance with the test plan(s) listed below as of the date of this letter.

This test session was conducted from January 20, 2026, to January 29, 2026, at Fime's Montreal Lab, using samples received on 19 January 2026. The tested product is an mDL application implementation based on the ISO/IEC 18013-5:2021 standard. The results of the test session demonstrate that the tested samples meet the applicable requirements, where applicability was determined based on the Implementation Conformance Statement (ICS) mentioned below.

The detailed results are provided in the official Fime test report C26CPG00-094_iOS.

The test scope solely included testing the application on its interface to an mDL reader, by executing the applicable test cases listed in the ISO/IEC 18013-6:2025 standard. Testing was limited to the features supported by the application, as indicated by TOPPAN Security in the ICS reproduced in the Appendix to this letter.

Details of the application under test, the test environment, and the test devices used for testing can be found on the next page. As a reminder, the correct functioning of the application is dependent on several factors in its operational environment. TOPPAN Security is solely and fully responsible for the conformity of the application to all applicable standards, specifications, and requirements.

This confirmation letter is valid for 1 year from the date of issuance.

Jerrin Jose Thomas

Service Line Manager
2026.03.06 15:34:10-05'00'

March 6th 2026

Fime test session confirmation letter

System under test

Application name and version	GoID Sample App (2.18.0.645)
Date of receipt of application	2026-01-19
Operating system	iOS
Number of Samples	1

SDK information

SDK name and version	TOPPAN VC SDK for iOS (2.18.0.645)
Operating system	iOS
SHA-256 Hash over SDK	9c235388260f095fd6b7e841245c367653bf8c14cd866212dbb2d3ca3cf4f0a0

Implementation conformance statement summary

Device engagement technologies	QR code
Device retrieval technologies	BLE in mdoc central client mode
Server retrieval technologies	None
Security mechanisms for device retrieval	Session encryption, issuer data authentication, mdoc MAC authentication, mdoc reader authentication

Test environment

Standard	ISO/IEC 18013-5:2021
Test case specification	ISO/IEC 18013-6:2025
Test suite	Fime Digital Identity Application Test Suite v1.6.3
mDL test app	mdoctestapp-1.4.4.apk

Fime test session confirmation letter

Test device on which the mDL test app is installed	Google Pixel 9a
OS version of the test device on which the mDL test app is installed	Android 16

Test devices and platform

Device brand and type	iPhone 16e	iPhone 13 Pro Max
OS version	iOS 26.2	iOS 17.3



Fime test session confirmation letter

A.1 Appendices

Appendix A: Implementation conformance statement

----------END OF DOCUMENT----------

Fime test session confirmation letter

Dear TOPPAN Security,

The purpose of this document is for you to document the Implementation Conformance Statement (ICS), indicating which standardized functions and/or protocols are supported in the Android-based mDL application provided to Fime for conformity testing. The details from the ICS form will be used by the Fime to understand the scope of certification and generate the applicable test cases for conformity testing.

Please fill the form providing the technical details regarding your Android-based mDL application implementation and return the form.

Depending on the number of different options your application supports and the nature of these options, it may not be possible to combine all these options in a single sample. After we have received you ICS form, Fime will let you know how many different samples we would need to receive in order to fully test all supported options. By combining options in a smart way, we will try to minimize this number. We will let you know how each of these samples needs to be configured.

Finally, please note that Fime will treat all information provided via this form as confidential, subject to the terms of confidentiality between Fime and TOPPAN Security.

Thank you,
Fime

Fime test session confirmation letter

mDL owner general information

Application Owner Name	TOPPAN Security
Address	Maplewood, Crockford Lane, Chineham Business Park
City	Basingstoke
State	
Zip code / postal code	RG24 8YB
Country	United Kingdom
Contact name	Fabrice Jogand-Coulomb
Contact title	VP Solutions TOPPAN Digital Business Unit
Contact email address	Fabrice.jogandcoulomb@toppansecurity.com
Contact phone number	+971 50 113 5950

Issuing authority general information
(Applicable for integrated product certification only)

Issuing authority name	
Issuing authority address	
City	
State	
Zip code / postal code	
Country	
Contact name	
Contact title	
Contact email address	
Contact phone number	

Fime test session confirmation letter

mDL application general information		
	Certification type	☒ Functional[1] ☐ Integrated Product[2]
	Application name and version	GoID Sample App (2.18.0.645)
	Is the mDL Application developed based on an SDK? If yes, please provide the answer to the two questions below	☒ YES ☐ NO
	SDK Name and Version	TOPPAN VC SDK for Android (2.18.0.645)
	SHA-256 Hash of the SDK	9c235388260f095fd6b7e841245c367653bf8c14cd866212dbb2d3ca3cf4f0a0
-	Minimum version of iOS supported	14
1.	How many documents are present on the mdl under test?	1
2.	For each document, please specify the applicable doctype	org.iso.18013.5.1. mDL
3.	For each document, please specify all data element namespaces used by the document	• org.iso.18013.5.1 • iso.org.dod.internet.private.enterprise.toppansecurity.goID.sdk.data.1
4.	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.toppansecurity.goID.sdk.data.1": ["objectDataJSON", "objectIssuerJson"],

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

2 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.



Fime test session confirmation letter

ICS statements for mDL data model test cases [3]		
5.	Data element administrative_number is present in the mDL data.	☐ YES ☒ NO
6.	Data element sex is present in the mDL data.	☒ YES ☐ NO
7.	Data element height is present in the mDL data.	☐ YES ☒ NO
8.	Data element weight is present in the mDL data.	☐ YES ☒ NO
9.	Data element eye_color is present in the mDL data.	☐ YES ☒ NO
10.	Data element hair_color is present in the mDL data.	☐ YES ☒ NO
11.	Data element birth_place is present in the mDL data.	☐ YES ☒ NO
12.	Data element resident_address is present in the mDL data.	☒ YES ☐ NO
13.	Data element portrait_capture_date is present in the mDL data.	☐ YES ☒ NO
14.	Data element age_in_years is present in the mDL data.	☐ YES ☒ NO
15.	Data element age_birth_year is present in the mDL data.	☐ YES ☒ NO

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



Fime test session confirmation letter

<table>
<tr><td>16.</td><td>Data element age_over_NN is present in the mDL data.

In case you select YES, please provide six (6) age_over_NN data elements in the mDL data, of which three (3) lower NN values with the value TRUE and three (3) higher values with the value FALSE. Please make sure the set of age_over_NN data elements is consistent. List the values for NN1 – NN6 present in the mDL data.

<table>
<tr><th>Value for NN in data element identifier</th><th>Value (TRUE / FALSE)</th></tr>
<tr><td>age_over_15(L)</td><td>TRUE</td></tr>
<tr><td>age_over_18(L)</td><td>TRUE</td></tr>
<tr><td>age_over_21(L)</td><td>TRUE</td></tr>
<tr><td>age_over_60(H)</td><td>FALSE</td></tr>
<tr><td>age_over_65(H)</td><td>FALSE</td></tr>
<tr><td>age_over_68(H)</td><td>FALSE</td></tr>
</table>

EXAMPLE: The following set complies with the above rules:
age_over_15 = TRUE (NN1 = 15)
age_over_18 = TRUE (NN2 = 18)
age_over_21 = TRUE (NN3 = 21)
age_over_60 = FALSE (NN4 = 60)
age_over_65 = FALSE (NN5 = 65)
age_over_68 = FALSE (NN6 = 68)</td><td>☒ YES
☐ NO</td></tr>
<tr><td>17.</td><td>Data element issuing_jurisdiction is present in the mDL data.</td><td>☐ YES
☒ NO</td></tr>
<tr><td>18.</td><td>Data element nationality is present in the mDL data.</td><td>☐ YES
☒ NO</td></tr>
<tr><td>19.</td><td>Data element resident_city is present in the mDL data.</td><td>☒ YES
☐ NO</td></tr>
<tr><td>20.</td><td>Data element resident_state is present in the mDL data.</td><td>☒ YES
☐ NO</td></tr>
<tr><td>21.</td><td>Data element resident_postal_code is present in the mDL data.</td><td>☒ YES
☐ NO</td></tr>
</table>



Fime test session confirmation letter

22.	Data element resident_country is present in the mDL data.	☒ YES ☐ NO
23.	Data element biometric_template_face is present in the mDL data.	☐ YES ☒ NO
24.	Data element biometric_template_voice is present in the mDL data.	☐ YES ☒ NO
25.	Data element biometric_template_finger is present in the mDL data.	☐ YES ☒ NO
26.	Data element biometric_template_iris is present in the mDL data.	☐ YES ☒ NO
27.	Data element biometric_template_retina is present in the mDL data.	☐ YES ☒ NO
28.	Data element biometric_template_hand_geometry is present in the mDL data.	☐ YES ☒ NO
29.	Data element biometric_template_signature_sign is present in the mDL data.	☐ YES ☒ NO
30.	Data element biometric_template_keystroke is present in the mDL data.	☐ YES ☒ NO
31.	Data element biometric_template_lip_movement is present in the mDL data.	☐ YES ☒ NO
32.	Data element biometric_template_thermal_face is present in the mDL data.	☐ YES ☒ NO
33.	Data element biometric_template_thermal_hand is present in the mDL data.	☐ YES ☒ NO
34.	Data element biometric_template_gait is present in the mDL data.	☐ YES ☒ NO
35.	Data element biometric_template_body_odor is present in the mDL data.	☐ YES ☒ NO



Fime test session confirmation letter

36.	Data element biometric_template_dna is present in the mDL data.	☐ YES ☒ NO
37.	Data element biometric_template_ear is present in the mDL data.	☐ YES ☒ NO
38.	Data element biometric_template_finger_geometry is present in the mDL data.	☐ YES ☒ NO
39.	Data element biometric_template_palm_geometry is present in the mDL data.	☐ YES ☒ NO
40.	Data element biometric_template_vein_pattern is present in the mDL data.	☐ YES ☒ NO
41.	Data element biometric_template_foot_print is present in the mDL data.	☐ YES ☒ NO
42.	Data element family_name_national_character is present in the mDL data.	☐ YES ☒ NO
43.	Data element given_name_national_character is present in the mDL data.	☐ YES ☒ NO
44.	Data element signature_usual_mark is present in the mDL data.	☐ YES ☒ NO

Fime test session confirmation letter

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

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

		☒ NO
59.	mDL supports server retrieval using WebAPI	☐ YES ☒ NO
60.	mDL supports transferring server retrieval information in the device engagement structure	☐ YES ☒ NO
61.	mDL implements a time-out between sending device engagement data and receiving the session establishment message when using QR code for device engagement.	☐ YES ☒ NO
62.	If yes, how many seconds does the mDL implement the time-out period?	N/A
63.	mDL implements a time-out between sending device engagement data and receiving the session establishment message when using NFC for device engagement.	☐ YES ☒ NO
64.	If yes, how many seconds does the mDL implement the time-out period?	N/A

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



Fime test session confirmation letter

ICS statements for security mechanisms test cases		
65.	Which curves does the mDL support for session establishment? Select all that are supported.[6]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
66.	mDL supports exchanging more than one device retrieval mdoc request and response with the mdoc reader in a single session.	☒YES ☐ NO
67.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	N/A
68.	Which curves does the mDL issuing authority support for issuer data authentication? Select all that are supported.[7]	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
69.	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 Fime expects that 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

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

75.	If yes, if mdoc reader authentication fails, does the mdoc notify the mdoc holder that the mdoc verifier's identity could not be verified?	☒ YES ☐ NO
76.	If yes, are there any data elements that the mdoc will not release if the reader authentication fails? If so, please list them all by namespace and identifier. [11]	☐ YES, namely…. ☒ NO
77.	If yes, mdoc supports retrieving OCSP information, if available, when verifying a mdoc reader authentication certificate.	☐ YES ☒ NO
78.	If yes, mdoc supports retrieving CRL information when verifying an mdoc reader authentication certificate.	☒ YES ☐ NO
79.	A test CRL for all IACA root certificates provided by the customer is available during testing.	☒ YES ☐ NO
80.	A test CRL for all Document Signer certificates used by the mdoc is available during testing.	☒ YES ☐ NO

ICS statements for Use Cases test cases		
81.	The mDL enables the mDL holder to refuse consent for sharing the portrait, but give consent for sharing other data elements requested in the same request.	☒ YES ☐ NO

[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 Fime expects that 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 alternately or uses different curves for ECDSA/EdDSA alternately. However, please note that Fime expects that the same mdoc authentication mechanism (either MAC or ECDSA/EdDSA) is consistently used for all documents on a given sample. Moreover, Fime 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] Fime assumes that all mDL samples provided to us will support all mdoc reader authentication curves selected (provided that the correct CA certificates are installed).

[11] At least one of ICS # 75 and ICS # 76 should be answered with Yes. Otherwise, failing reader authentication would not have any consequences.