



Fime test session confirmation letter

Conformity test of the iOS-based Cosmo mDL v1.0.1 application to ISO/IEC 18013-5:2021

Test session carried out for Cosmocolor SA de CV

Fime hereby confirms that the iOS-based Cosmo mDL v1.0.1 application, developed by Cosmocolor SA de CV, 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 August 28, 2025, to September 26, 2025, at Fime's Montreal Lab, using samples received on 26 August 2025. 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 ICS mentioned below. The detailed results are provided in the official Fime test report M25REP00-247 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 18013-6:2024 standard. Testing was limited to the features supported by the application, as indicated by Cosmocolor SA de CV in the Implementation Conformance Statement 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. Cosmocolor SA de CV 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.

November 4th 2025



Fime test session confirmation letter

System under test

Application name and version	Cosmo mDL v1.0.1
Date of receipt of application	2025-08-26
Operating system	iOS
Number of Samples	1

Implementation conformance statement summary

Device engagement technologies	QR code
Device retrieval technologies	BLE in mdoc central client mode
Server retrieval technologies	WebAPI
Security mechanisms for device retrieval	Session encryption, issuer data authentication, mdoc ECDSA/EdDSA authentication

Test environment

Standard	ISO/IEC 18013-5:2021
Test case specification	ISO/IEC 18013-6:2024
Test suite	Fime Digital Identity Application Test Suite v1.5.5
mDL test app	mdoctestapp-1.4.2.apk
Test device on which the mDL test app is installed	Google Pixel 8a
OS version of the test device on which the mDL test app is installed	Android 14

Test devices and platform

Device brand and type	iPhone 16e	iPhone 13 Pro Max
OS version	iOS 18.4	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 Cosmocolor,

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 iOS-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 iOS-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 your 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 Cosmocolor

Thank you,
Fime



Fime test session confirmation letter

mDL owner general information

Address	5295 Prolongación Paseo de la Reforma
City	Ciudad de México
State	
Zip code / postal code	05000
Country	Mexico
Contact name	Ruben Pacheco
Contact title	Technology Director
Contact email address	rpacheco@kcosmocolor.com
Contact phone number	+525561669877

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	<input checked="" type="checkbox"/> Functional ¹ <input type="checkbox"/> Integrated Product ²
-	Application name and version	Cosmo_md1_demo
-	Minimum version of iOS supported	iOS 17
1.	How many documents are present on the mdl under test?	2
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

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 cases³

5.	Data element administrative_number is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
6.	Data element sex is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
7.	Data element height is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
8.	Data element weight is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
9.	Data element eye_color is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
10.	Data element hair_color is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
11.	Data element birth_place is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
12.	Data element resident_address is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
13.	Data element portrait_capture_date is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
14.	Data element age_in_years is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
15.	Data element age_birth_year is present in the mDL data.	<input type="checkbox"/> YES <input type="checkbox"/> NO



Fime test session confirmation letter

16.	<p>Data element age_over_NN is present in the mDL data.</p> <p>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.</p> <table border="1"><thead><tr><th>Value for NN in data element identifier</th><th>Value (TRUE / FALSE)</th></tr></thead><tbody><tr><td>age_over_15</td><td>TRUE</td></tr><tr><td>age_over_18</td><td>TRUE</td></tr><tr><td>age_over_21</td><td>TRUE</td></tr><tr><td>age_over_60</td><td>FALSE</td></tr><tr><td>age_over_75</td><td>FALSE</td></tr><tr><td>age_over_80</td><td>FALSE</td></tr></tbody></table> <p>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)</p>	Value for NN in data element identifier	Value (TRUE / FALSE)	age_over_15	TRUE	age_over_18	TRUE	age_over_21	TRUE	age_over_60	FALSE	age_over_75	FALSE	age_over_80	FALSE	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
Value for NN in data element identifier	Value (TRUE / FALSE)															
age_over_15	TRUE															
age_over_18	TRUE															
age_over_21	TRUE															
age_over_60	FALSE															
age_over_75	FALSE															
age_over_80	FALSE															
17.	Data element issuing_jurisdiction is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO														
18.	Data element nationality is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO														
19.	Data element resident_city is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO														
20.	Data element resident_state is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO														
21.	Data element resident_postal_code is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO														
22.	Data element resident_country is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO														
23.	Data element biometric_template_face is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO														



Fime test session confirmation letter

24.	Data element biometric_template_voice is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
25.	Data element biometric_template_finger is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
26.	Data element biometric_template_iris is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
27.	Data element biometric_template_retina is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
28.	Data element biometric_template_hand_geometry is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
29.	Data element biometric_template_signature_sign is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
30.	Data element biometric_template_keystroke is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
31.	Data element biometric_template_lip_movement is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
32.	Data element biometric_template_thermal_face is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
33.	Data element biometric_template_thermal_hand is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
34.	Data element biometric_template_gait is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
35.	Data element biometric_template_body_odor is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
36.	Data element biometric_template_dna is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
37.	Data element biometric_template_ear is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
38.	Data element biometric_template_finger_geometry is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
39.	Data element biometric_template_palm_geometry is present in the mDL data.	<input type="checkbox"/> YES



Fime test session confirmation letter

		<input checked="" type="checkbox"/> NO
40.	Data element biometric_template_vein_pattern is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
41.	Data element biometric_template_foot_print is present in the mDL data.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
42.	Data element family_name_national_character is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
43.	Data element given_name_national_character is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
44.	Data element signature_usual_mark is present in the mDL data.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> 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

ICS statements for technology test cases

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



Fime test session confirmation letter

60.	mDL supports transferring server retrieval information in the device engagement structure	<input type="checkbox"/> YES <input checked="" type="checkbox"/> 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.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
62.	If yes, how many seconds does the mDL implement the time-out period?	
63.	mDL implements a time-out between sending device engagement data and receiving the session establishment message when using NFC for device engagement.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
64.	If yes, how many seconds does the mDL implement the time-out period?	

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.



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	<input checked="" type="checkbox"/> Curve P-256 <input type="checkbox"/> Curve P-384 <input type="checkbox"/> Curve P-521 <input type="checkbox"/> X25519 <input type="checkbox"/> X448 <input type="checkbox"/> brainpoolP256r1 <input type="checkbox"/> brainpoolP320r1 <input type="checkbox"/> brainpoolP384r1 <input type="checkbox"/> brainpoolP512r1
66.	mDL supports exchanging more than one device retrieval mdoc request and response with the mdoc reader in a single session.	<input checked="" type="checkbox"/> YES <input checked="" type="checkbox"/> NO
67.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	
68.	Which curves does the mDL issuing authority support for issuer data authentication? Select all that are supported. ⁷	<input checked="" type="checkbox"/> Curve P-256 <input type="checkbox"/> Curve P-384 <input type="checkbox"/> Curve P-521 <input type="checkbox"/> Ed25519 <input type="checkbox"/> Ed448 <input type="checkbox"/> brainpoolP256r1 <input type="checkbox"/> brainpoolP320r1 <input type="checkbox"/> brainpoolP384r1 <input type="checkbox"/> brainpoolP512r1
69.	The mDL supports mdoc MAC authentication.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
70.	If yes, which curves does the mDL support for mdoc MAC authentication? Select all that are supported. ⁸	<input type="checkbox"/> Curve P-256 <input type="checkbox"/> Curve P-384 <input type="checkbox"/> Curve P-521 <input type="checkbox"/> X25519 <input type="checkbox"/> X448 <input type="checkbox"/> brainpoolP256r1 <input type="checkbox"/> brainpoolP320r1 <input type="checkbox"/> brainpoolP384r1 <input type="checkbox"/> brainpoolP512r1
71.	The mDL supports mdoc ECDSA/EdDSA authentication	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO



Fime test session confirmation letter

72.	If yes, which curves does the mDL use for mdoc ECDSA/EdDSA authentication? Select all that are supported.	<input checked="" type="checkbox"/> Curve P-256 <input type="checkbox"/> Curve P-384 <input type="checkbox"/> Curve P-521 <input type="checkbox"/> Ed25519 <input type="checkbox"/> Ed448 <input type="checkbox"/> brainpoolP256r1 <input type="checkbox"/> brainpoolP320r1 <input type="checkbox"/> brainpoolP384r1 <input type="checkbox"/> brainpoolP512r1
73.	The mDL supports mdoc reader authentication	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
74.	If yes, which curves does the mdoc support for mdoc reader authentication? Select all that are supported.	<input type="checkbox"/> Curve P-256 <input type="checkbox"/> Curve P-384 <input type="checkbox"/> Curve P-521 <input type="checkbox"/> Ed25519 <input type="checkbox"/> Ed448 <input type="checkbox"/> brainpoolP256r1 <input type="checkbox"/> brainpoolP320r1 <input type="checkbox"/> brainpoolP384r1 <input type="checkbox"/> 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?	<input type="checkbox"/> YES <input checked="" type="checkbox"/> 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.	<input type="checkbox"/> YES, namely.... <input checked="" type="checkbox"/> NO
77.	If yes, mdoc supports retrieving OCSP information, if available, when verifying a mdoc reader authentication certificate.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
78.	If yes, mdoc supports retrieving CRL information when verifying an mdoc reader authentication certificate.	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
79.	A test CRL for all IACA root certificates provided by the customer is available during testing.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
80.	A test CRL for all Document Signer certificates used by the mdoc is available during testing.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO



Fime test session confirmation letter

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.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> 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.

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.