

652



ISO 18013-5



Traducción jurada del alemán

Traducción jurada del inglés

Copia notarial

Veridos

Oranienstraße 91, 10969 Berlín

2 de agosto de 2024

Asunto: Confirmación de la conformidad del VD Mobile ID basado en iOS, versión 1.0.10 (14)
con la norma ISO/IEC 18013-5:2021

Estimado Sr. Nicholas:

Nos dirigimos a usted para confirmarle que la aplicación mDL mencionada anteriormente (la «aplicación») ha sido probada por FIME y ha resultado ser conforme con la norma ISO/IEC 18013-5:2021 a partir de la fecha de esta carta.

Parte de las pruebas consistió en comprobar la interfaz de la aplicación con un lector de mDL mediante la ejecución de los casos de prueba enumerados en la última versión del borrador de la norma ISO/IEC 18013-6. Solo se realizaron aquellas pruebas compatibles con las funciones de la aplicación, tal y como se especifica en la Declaración de Conformidad de la Implementación adjunta a esta carta. Para más información sobre la aplicación probada, el entorno de prueba y el equipo utilizado para la prueba, consulte la página siguiente.

Debe tenerse en cuenta que el correcto funcionamiento de la aplicación depende de diversos factores dentro de su entorno operativo. Veridos es el único y pleno responsable de la conformidad de la aplicación con todas las normas, especificaciones y requisitos aplicables.

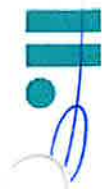
El informe de pruebas que acompaña a esta carta lleva el número FIME_Veridos_iOS_02. Este protocolo contiene una descripción completa de los casos de prueba ejecutados y todos los resultados de las pruebas.

Atentamente
[firma ilegible]

FIME

David Bakker
Director técnico





Ámbito de aplicación de mDL

Sistema probado

Nombre y versión de la aplicación	VD Mobile ID Versión 1.0.10 (14)
Aplicación recibida el	23 de julio de 2024

Resumen de la declaración de conformidad de la aplicación

Tecnologías para la interacción con el dispositivo	Código QR
Tecnologías para la consulta de dispositivos	BLE en el modo cliente central del Mdoc BLE en el modo servidor periférico del Mdoc
Tecnologías para la consulta del servidor	Ninguna
Mecanismos de seguridad para la consulta del dispositivo	Cifrado de las sesiones, autenticación de los datos del emisor, autenticación Mdoc ECDSA/EdDSA, autenticación de los lectores Mdoc

Entorno de prueba

Norma	ISO/IEC 18013-5: 2021
Especificación de casos de prueba	Especificación de casos de prueba FIME mDL
Conjunto de pruebas	Conjunto de pruebas de la aplicación FIME mDL v1.3.14
Aplicación de prueba mDL	mdltestapp-1.3.1.apk
Dispositivo de prueba en el que está instalada la aplicación de prueba mDL	Samsung Galaxy S24
Versión del sistema operativo del dispositivo de prueba en el que está instalada la aplicación de prueba mDL	Android 14

Dispositivos de prueba y plataforma

Marca y tipo de dispositivo	iPhone 15	iPhone SE (2ª generación)
Versión del sistema operativo	iOS 17.5.1	iOS 13.5.1



655

A.1 Declaración de conformidad de la implementación

Veridos envió a la FIME las siguientes declaraciones de conformidad de la implementación (Implementation Conformance Statement, ICS). Se han utilizado para determinar los casos de prueba que deben ejecutarse.

Veridos utiliza la versión v1.10 de ICS.

A.1.1 Informaciones generales

Propietario del mDL	
Nombre del propietario de la aplicación	Veridos
Dirección	Oranienstraße 91
Ciudad	Berlín
Estado	Berlín
C.P.	10969
País	Alemania
Nombre de la persona de contacto	Nicholas Larter
Cargo	Senior Solutions Manager
Correo electrónico de la persona de contacto	nick.larter@veridos.com
Número de teléfono de la persona de contacto	+49 1525 1334198

N.º Información general sobre la aplicación mDL	
- Tipo de certificación	☒ Certificación de funciones ¹ ☐ Certificación de producto integrado ²
- Nombre y versión de la aplicación	VD Mobile ID Versión 1.0.10 (14)
- Versión iOS compatible más baja	iOS 13
¿Cuántos documentos se pueden consultar en el mDL?	1
Especifique el tipo de documento de cada documento	org.iso.18013.5.1. mDL
Para cada documento, especifique todos los espacios de nombres de elementos de datos utilizados por el documento respectivo	org.iso.18013.5.1
Para cada espacio de nombres distinto del espacio de nombres mDL («org.iso.18013.5.1»), especifique la identificación de todos los elementos de datos presentes en el documento.	

El conjunto de datos del mDL para la certificación de funciones puede ser un conjunto de datos de muestra que el propietario del mDL desee personalizar en el

² Para la certificación integrada de productos, el registro mDL debe ser creado y personalizado por un sistema de registro (System of Record, SoR) emisor y debe ser representativo del mDL utilizado en la fabricación.





656

A.1.2 Para los casos de prueba del modelo de datos mDL

Nota: Todos los elementos de datos de esta sección están contenidos en el espacio de nombres de datos mDL por defecto («org.iso.18013.5.1»). El ICS de esta sección sólo debe cumplimentarse para los documentos del tipo «org.iso.18013.5.1. mDL».

N.º	Declaraciones de conformidad de la implementación para los casos de prueba del modelo de datos mDL ³	
5.	El elemento de datos administrative_number (número administrativo) está presente en los datos mDL.	☐ SÍ ☒ NO
6.	El elemento de datos sex (género) está presente en los datos mDL.	☒ SÍ ☐ NO
7.	El elemento de datos height (altura) está presente en los datos mDL.	☒ SÍ ☐ NO
8.	El elemento de datos weight (peso) está presente en los datos mDL.	☐ SÍ ☒ NO
9.	El elemento de datos eye_color (color de ojos) está presente en los datos mDL.	☒ SÍ ☐ NO
10.	El elemento de datos hair_color (color de pelo) está presente en los datos mDL.	☒ SÍ ☐ NO
11.	El elemento de datos birth_place (lugar de nacimiento) está presente en los datos mDL.	☒ SÍ ☐ NO
12.	El elemento de datos resident_address (dirección de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
13.	El elemento de datos portrait_capture_date (fecha de toma de la fotografía) está presente en los datos mDL.	☒ SÍ ☐ NO
14.	El elemento de datos age_in_years (edad en años) está presente en los datos mDL.	☒ SÍ ☐ NO
15.	El elemento de datos age_birth_year (edad año de nacimiento) está presente en los datos mDL.	☒ SÍ ☐ NO
16.	El elemento de datos age_over_NN (edad mayor que NN) está presente en los datos mDL.	☐ SÍ ☒ NO

Si se marca SÍ: Proporcione seis (6) elementos de datos age_over_NN en los datos mDL, incluidos tres (3) valores NN inferiores con valor TRUE y tres (3) valores NN superiores con valor FALSE. Asegúrese de que el conjunto de elementos de datos age_over_NN (edad mayor que NN) sea consistente. Enumere los valores para NN1 NN6 presentes en los datos mDL.

Valor para NN en el identificador del	Valor (VERDADERO/FALSO)

³ Nota: Todos los elementos de datos de esta sección están contenidos en el espacio de nombres de datos mDL estándar («org.iso.18013.5.1»). El ICS de esta sección sólo debe rellenarse para documentos del tipo «org.iso.18013.5.1. mDL».



657

elemento de datos	
age_over_NN1(N)	VERDADERO
age_over_NN2(N)	VERDADERO
age_over_NN3(N)	VERDADERO
age_over_NN4(H)	FALSO
age_over_NN5(H)	FALSO
age_over_NN6(H)	FALSO

EJEMPLO: La frase siguiente corresponde a las reglas anteriores:

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

17.	El elemento de datos issuing_jurisdiction (país emisor) está disponible en los datos mDL.	☐ SÍ ☒ NO
18.	El elemento de datos nationality (nacionalidad) está disponible en los datos mDL.	☒ SÍ ☐ NO
19.	El elemento de datos resident_city (ciudad de residencia) está disponible en los datos mDL.	☒ SÍ ☐ NO
20.	El elemento de datos resident_state (estado federal de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
21.	El elemento de datos resident_postal_code (código postal del lugar de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
22.	El elemento de datos resident_country (país de residencia) está presente en los datos mDL.	☒ SÍ ☐ NO
23.	El elemento de datos biometric_template_face (plantilla biométrica de cara) está presente en los datos mDL.	☐ SÍ ☒ NO
24.	El elemento de datos biometric_template_voice (plantilla biométrica de voz) está presente en los datos mDL.	☐ SÍ ☒ NO
25.	El elemento de datos biometric_template_finger (plantilla biométrica del dedo) está presente en los datos mDL.	☐ SÍ ☒ NO
26.	El elemento de datos biometric_template_iris (plantilla biométrica del iris) está presente en los datos mDL.	☐ SÍ ☒ NO
27.	El elemento de datos biometric_template_retina (plantilla biométrica de retina) está presente en los datos mDL.	☐ SÍ ☒ NO
28.	El elemento de datos biometric_template_hand_geometry (plantilla biométrica de la geometría de la mano) está presente en los datos mDL.	☐ SÍ ☒ NO
29.	El elemento de datos biometric_template_signature_sign (plantilla biométrica de firma) está presente en los datos mDL.	☐ SÍ ☒ NO



30.	El elemento de datos biometric_template_keystroke (plantilla biométrica de pulsación de tecla) está presente en los datos mDL.	☐ SÍ ☒ NO
31.	El elemento de datos biometric_template_lip_movement (plantilla biométrica del movimiento de los labios) está presente en los datos mDL.	☐ SÍ ☒ NO
32.	El elemento de datos biometric_template_thermal_face (plantilla biométrica facial térmica) está presente en los datos mDL.	☐ SÍ ☒ NO
33.	El elemento de datos biometric_template_thermal_hand (plantilla biométrica de mano térmica) está presente en los datos mDL.	☐ SÍ ☒ NO
34.	El elemento de datos biometric_template_gait (plantilla biométrica de la marcha) está presente en los datos mDL.	☐ SÍ ☒ NO
35.	El elemento de datos biometric_template_body_odor (plantilla biométrica del olor corporal) está presente en los datos mDL.	☐ SÍ ☒ NO
36.	El elemento de datos biometric_template_dna (plantilla biométrica de ADN) está presente en los datos mDL.	☐ SÍ ☒ NO
37.	El elemento de datos biometric_template_ear (plantilla biométrica de la oreja) está presente en los datos mDL.	☐ SÍ ☒ NO
38.	El elemento de datos biometric_template_finger_geometry (plantilla biométrica de la geometría de los dedos) está presente en los datos mDL.	☐ SÍ ☒ NO
39.	El elemento de datos biometric_template_palm_geometry (plantilla biométrica de la geometría de la palma de la mano) está presente en los datos mDL.	☐ SÍ ☒ NO
40.	El elemento de datos biometric_template_vein_pattern (plantilla biométrica del patrón de las venas) está presente en los datos mDL.	☐ SÍ ☒ NO
41.	El elemento de datos biometric_template_foot_print (plantilla biométrica de huella del pie) está presente en los datos mDL.	☐ SÍ ☒ NO
42.	El elemento de datos family_name_national_character (carácter nacional del apellido) está presente en los datos mDL.	☐ SÍ ☒ NO
43.	El elemento de datos given_name_national_character (carácter nacional del nombre) está presente en los datos mDL.	☐ SÍ ☒ NO
44.	El elemento de datos signature_usual_mark (carácter habitual de la firma) está presente en los datos mDL.	☐ SÍ ☒ NO

A.1.3 Para casos de pruebas de tecnología

N.º Declaraciones de conformidad de la implementación para los casos de prueba de tecnología		
45.	mDL es compatible con la interacción de dispositivos mediante NFC Static Handover.	☐ SÍ ☒ NO
46.	mDL es compatible con la interacción de dispositivos vía NFC Negotiated Handover. ⁴	☐ SÍ ☒ NO

⁴ Nota: NFC Static Handover y NFC Negotiated Handover no se admiten simultáneamente si un mDL es compatible con ambas tecnologías



659

47.	El mDL admite la interacción de dispositivos mediante código QR.	☒ SÍ ☐ NO
48.	El mDL admite la consulta de dispositivos mediante NFC.	☐ SÍ ☒ NO
49.	El mDL admite APDUs muy largos para consulta de dispositivos mediante NFC.	☐ SÍ ☒ NO
50.	El mDL es compatible con BLE versión 4.2 (o superior) y LE Data Packet Length Extension.	☒ SÍ ☐ NO
51.	El mDL admite la consulta de dispositivos a través de BLE en el modo de cliente central del Mdoc.	☒ SÍ ☐ NO
52.	Si se utiliza BLE para la consulta de dispositivos en el modo de cliente central del Mdoc, el Mdoc verifica el valor de la característica Ident.	☐ SÍ ☒ NO
53.	El mDL admite el perfil de transmisión L2CAP cuando actúa como GATT-Client para la consulta de dispositivos a través de BLE.	☐ SÍ ☒ NO
54.	El mDL admite el sondeo de dispositivos mediante BLE en el modo de servidor periférico del Mdoc.	☒ SÍ ☐ NO
55.	El mDL admite el perfil de transmisión L2CAP cuando actúa como GATT-Server para la consulta de dispositivos mediante BLE.	☐ SÍ ☒ NO
56.	El mDL admite la consulta de dispositivos mediante Wi-Fi Aware.	☐ SÍ ☒ NO
57.	El mDL admite el conjunto de cifrado NCS-PK-2WDH-128 para Wi-Fi Aware. ⁵	☐ SÍ ☒ NO
58.	El mDL admite la consulta al servidor a través de OIDC	☐ SÍ ☒ NO
59.	El mDL admite la consulta del servidor a través de WebAPI	☐ SÍ ☒ NO
60.	El mDL admite la transmisión de información de consulta al servidor dentro de la estructura de interacción del dispositivo.	☐ SÍ ☒ NO
61.	El mDL establece un tiempo de espera entre el envío de los datos de interacción con el dispositivo y la recepción del mensaje de establecimiento de sesión cuando la interacción con el dispositivo se realiza mediante código QR.	☐ SÍ ☒ NO
62.	En caso afirmativo, introduzca la duración del tiempo de espera establecido por mDL en segundos.	Ninguna
63.	El mDL establece un tiempo de espera entre el envío de los datos de interacción con el dispositivo y la recepción del mensaje de establecimiento de sesión cuando la interacción con el dispositivo se realiza mediante código NFC.	☐ SÍ ☒ NO
64.	En caso afirmativo, introduzca la duración del tiempo de espera establecido por mDL en segundos.	Ninguna

⁵ Sólo se aplica si el Mdoc admite Wi-Fi Aware para el sondeo de dispositivos y NFC Negotiated Handover para la interacción de dispositivos.





660

A.1.4 Para casos de prueba de mecanismos de seguridad

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de mecanismos de seguridad	
65.	¿Qué curvas admite el mDL para el establecimiento de sesión? Marque todas las curvas admitidas. ⁶	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
66.	El mDL admite el intercambio de más de una solicitud y respuesta Mdoc para la interrogación del dispositivo con el lector Mdoc en una única sesión.	☐ Sí ☒ NO
67.	En caso afirmativo, introduzca la duración del tiempo de espera establecido por el mDL para finalizar la sesión en segundos.	
68.	¿Qué curvas admite la autoridad emisora del mDL para la autenticación de los datos del emisor? Marque todas las curvas compatibles. ⁷	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
69.	El mDL admite la autenticación Mdoc MAC.	☐ Sí ☒ NO
70.	En caso afirmativo, ¿qué curvas admite el mDL para la autenticación Mdoc MAC? Marque todas las curvas admitidas. ⁸	☐ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1

⁶ Si el mDL admite varias curvas de configuración de sesión, el propietario del mDL debe proporcionar una muestra de cada curva admitida para fines de prueba.

⁷ Si hay varios documentos en el mDL, la autoridad emisora puede utilizar teóricamente una curva diferente para la firma MSO en cada uno de estos documentos.

Sin embargo, debe tenerse en cuenta que FIME asume que se utiliza la misma curva para todos los documentos de una muestra. A efectos de prueba, el propietario del mDL deberá proporcionar una muestra para cada curva admitida.

Si hay varios documentos en el mDL, el mDL puede utilizar teóricamente una curva de autenticación Mdoc MAC diferente para cada uno de estos documentos. Sin embargo, debe tenerse en cuenta que FIME asume que se utiliza la misma curva para todos los documentos de una muestra. A efectos de prueba, el propietario del mDL debe proporcionar una muestra para cada curva admitida.



	☐ brainpoolP512r1
71. El mDL admite la autenticación Mdoc ECDSA/EdDSA.	☒ Sí ☐ NO
72. En caso afirmativo, ¿qué curvas utiliza el mDL para la autenticación Mdoc ECDSA/EdDSA? Marque todas las curvas admitidas. ⁹	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
73. El mDL admite la autenticación de lectores Mdoc.	☒ Sí ☐ NO
74. En caso afirmativo, ¿qué curvas admite el mDL para la autenticación de lectores Mdoc? Marque todas las curvas admitidas. ¹⁰	☒ Curva P-256 ☒ Curva P-384 ☒ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
75. En caso afirmativo, ¿notifica el Mdoc al propietario del Mdoc en caso de que falle la autenticación del lector del Mdoc de que no se ha podido verificar la identidad del comprobador?	☒ Sí ☐ NO
76. En caso afirmativo, ¿hay algún dato que el Mdoc no comunique en caso de que falle la autenticación del lector? Si procede, enumérelas por espacio de nombres e identificador. ¹¹	☐ Sí, es decir... ☒ NO
77. En caso afirmativo, ¿permite Mdoc la consulta de información OSCP, si está disponible, para verificar un certificado para la autenticación de lectores Mdoc?	☐ Sí ☒ NO
78. En caso afirmativo, ¿permite Mdoc la consulta de información CRL para verificar un certificado para la autenticación de lectores Mdoc?	☒ Sí ☐ NO

⁹ Nota: Podría haber varios pares SDeviceKey para la autenticación Mdoc para cada documento en un mDL, cada uno en un MSO separado. Por lo tanto, es teóricamente posible que un único documento utilice alternativamente autenticación MAC y autenticación ECDSA/EdDSA o que utilice alternativamente curvas diferentes para la autenticación ECDSA/EdDSA. Sin embargo, debe tenerse en cuenta que FIME asume que el mismo método de autenticación Mdoc (MAC o ECDSA/EdDSA) se utiliza de forma coherente para todos los documentos de una plantilla. FIME también asume que se utiliza la misma curva ECDSA/EdDSA para los documentos de una muestra. A efectos de prueba, el propietario del mDL debe proporcionar una muestra para cada curva admitida. FIME asume que todas las muestras de mDL que se nos proporcionan admiten todas las curvas marcadas para la autenticación de lectores de Mdoc (siempre que se instalen los certificados CA correctos).

¹¹ Al menos debe marcarse Sí para el nº 75 y el nº 76. De lo contrario, la no autenticación de un lector no tendrá ningún efecto.



79.	Durante las pruebas, se dispone de una CRL de prueba proporcionada por el cliente para todos los certificados raíz IACA.	☐ SÍ ☒ NO
80.	Durante la prueba, está disponible una CRL de prueba para todos los certificados de firmante de documentos utilizados por el Mdoc.	☐ SÍ ☒ NO

A.1.5 Para casos de prueba de casos de aplicación

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de casos de aplicación	
81.	El mDL permite que el titular del mDL deniegue el consentimiento para compartir la fotografía, pero siga consintiendo en compartir otros elementos de datos solicitados como parte de la misma solicitud.	☒ SÍ ☐ NO



663

Yo, representante notarial, certifico que este documento es una copia fiel del documento original.

En Múnich, a 29/01/2025

[Sello del notario]

[Firma]

Dr. Bernhard Schaub
Notario en Múnich,
República Federal de Alemania
(el mandato expira el 31 de octubre de 2032)



669

Als in Bayern öffentlich bestellte und allgemein beeidigte Dolmetscherin für die englische und spanische Sprache bestätige ich: Vorstehende Übersetzung des mir in deutscher Sprache vorgelegten Dokuments ist richtig und vollständig.

München, den 06. Februar 2025

Como traductora jurada y nombrada públicamente para los idiomas alemán, inglés y español en Baviera, confirmo que la traducción que precede del documento que se me ha presentado en lengua alemana es correcta y completa.

Múnich, a 6 de febrero del 2025

Unterschrift und Stempel:

Firma y sello:



Susanne Bernhardt – Ravensburger Ring 18 – 81243 München



Veridos

Oranienstraße 91, 10969 Berlin

2. August 2024

Betreff: Bestätigung der Konformität des auf iOS basierenden VD Mobile ID, Version 1.0.10 (14) mit ISO/IEC 18013-5:2021

Sehr geehrter Herr Nicholas,

mit diesem Schreiben bestätigen wir, dass die oben genannte mDL-Anwendung (die „Anwendung“) von FIME getestet und im Ergebnis festgestellt wurde, dass sie mit Stand zum Datum dieses Schreibens der Norm ISO/IEC 18013-5:2021 entspricht.

Teil des Testumfangs war die Prüfung der Anwendung auf ihre Schnittstelle zu einem mDL-Lesegerät durch Ausführung der in der neuesten Entwurfsfassung von ISO/IEC 18013-6 aufgeführten Testfälle. Die Prüfung bezog sich nur auf von der Anwendung unterstützte Funktionen, wie in der diesem Schreiben beigefügten Erklärung zur Konformität der Implementierung angegeben. Nähere Informationen zu der getesteten Anwendung, der Testumgebung und den für den Test verwendeten Prüfgeräten sind der folgenden Seite zu entnehmen.

Es wird darauf hingewiesen, dass die ordnungsgemäße Funktion der Anwendung von verschiedenen Faktoren innerhalb ihrer Betriebsumgebung abhängt. Für die Konformität der Anwendung mit allen geltenden Normen, Spezifikationen und Anforderungen trägt Veridos die alleinige und volle Verantwortung.

Das zu diesem Schreiben gehörende Prüfprotokoll trägt die Nummer FIME_Veridos_iOS_02. Dieses Protokoll enthält eine vollständige Übersicht der ausgeführten Testfälle und aller Testergebnisse.

Mit freundlichen Grüßen

*[unlesbare Unterschrift]***FIME**David Bakker
Technischer Leiter



666

mDL-Implementierungsumfang

Getestetes System

Bezeichnung und Version der Anwendung	VD Mobile ID Version 1.0.10 (14)
Anwendung erhalten am	23. Juli 2024

Zusammenfassung der Erklärung zur Konformität der Implementierung

Technologien zur Geräteinteraktion	QR-Code
Technologien zur Geräteabfrage	BLE im zentralen Client-Modus des Mdoc BLE im Peripherieserver-Modus des Mdoc
Technologien zur Serverabfrage	Keine
Sicherheitsmechanismen für die Geräteabfrage	Verschlüsselung von Sitzungen, Authentifizierung von Ausstellerdaten, Mdoc ECDSA-/EdDSA-Authentifizierung, Authentifizierung von Mdoc-Lesegeräten

Testumgebung

Standard	ISO/IEC 18013-5: 2021
Testfallspezifikation	FIME mDL Testfallspezifikation
Test Suite	FIME mDL Application Test Suite v1.3.14
mDL-Testapp	mdltestapp-1.3.1.apk
Prüfgerät, auf dem die mDL-Testapp installiert ist	Samsung Galaxy S24
Version des Betriebssystems auf dem Prüfgerät, auf dem die mDL-Testapp installiert ist	Android 14

Prüfgeräte und -plattform

Marke und Typ des Geräts	iPhone 15	iPhone SE (2. Generation)
Version des Betriebssystems	iOS 17.5.1	iOS 13.5.1



A.1 Erklärung zur Konformität der Implementierung

Die folgenden Erklärungen zur Konformität der Implementierung (Implementation Conformance Statement, ICS) wurden FIME von Veridos vorgelegt. Anhand dieser wurde ermittelt, welche Testfälle auszuführen sind.

Veridos verwendet die ICS-Version v1.10.

A.1.1 Allgemeine Informationen

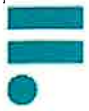
mDL-Eigentümer	
Name des Eigentümers der Anwendung	Veridos
Adresse	Oranienstraße 91
Stadt	Berlin
Status	Berlin
PLZ	10969
Land	Deutschland
Name des Ansprechpartners	Nicholas Larter
Positionsbezeichnung	Senior Solutions Manager
E-Mail-Adresse des Ansprechpartners	nick.larter@veridos.com
Telefonnummer des Ansprechpartners	+49 1525 1334198

Nr. Allgemeine Informationen zur mDL-Anwendung	
- Art der Zertifizierung	☒ Funktionszertifizierung ¹ ☐ Integrierte Produktzertifizierung ²
- Bezeichnung und Version der Anwendung	VD Mobile ID Version 1.0.10 (14)
- Niedrigste unterstützte iOS-Version	iOS 13
Wie viele Dokumente sind auf dem zu prüfenden mDL vorhanden?	1
Geben Sie bitte die jeweilige Dokumentart jedes Dokuments an	org.iso.18013.5.1.mDL
Geben Sie bitte für jedes Dokument alle vom jeweiligen Dokument verwendeten Datenelement-Namensräume an	org.iso.18013.5.1
Geben Sie bitte für jeden vom mDL-Namensraum („org.iso.18013.5.1“) abweichenden Namensraum die Bezeichner aller im Dokument vorhandenen Datenelemente an	

¹ Bei dem mDL-Datensatz für die Funktionszertifizierung kann es sich um einen Musterdatensatz handeln, den der mDL-Eigentümer auf dem mDL personalisieren möchte.

² Für die integrierte Produktzertifizierung muss der mDL-Datensatz von einem Aussteller-Aufzeichnungssystem (System of Record, SoR) erstellt und personalisiert werden und muss repräsentativ für den in der Herstellung verwendeten mDL sein.





668

A.1.2 Für mDL-Datenmodell-Testfälle

Hinweis: Alle Datenelemente in diesem Abschnitt sind im standardmäßigen mDL-Daten-Namensraum („org.iso.18013.5.1“) enthalten. Die ICS in diesem Abschnitt müssen nur für Dokumente der Dokumentart „org.iso.18013.5.1.mDL“ ausgefüllt werden.

Nr.	Erklärungen zur Konformität der Implementierung für mDL-Datenmodell-Testfälle ³	
5.	Das Datenelement administrative_number (Verwaltungsnummer) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
6.	Das Datenelement sex (Geschlecht) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
7.	Das Datenelement height (Größe) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
8.	Das Datenelement weight (Gewicht) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
9.	Das Datenelement eye_color (Augenfarbe) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
10.	Das Datenelement hair_color (Haarfarbe) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
11.	Das Datenelement birth_place (Geburtsort) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
12.	Das Datenelement resident_address (wohnt in) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
13.	Das Datenelement portrait_capture_date (Aufnahmedatum Lichtbild) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
14.	Das Datenelement age_in_years (Alter in Jahren) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
15.	Das Datenelement age_birth_year (Alter Geburtsjahr) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
16.	Das Datenelement age_over_NN (älter als NN) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN

Wenn JA angekreuzt wird: Bitte geben Sie sechs (6) age_over_NN Datenelemente in den mDL-Daten an, davon drei (3) niedrigere NN-Werte mit dem Wert WAHR und drei (3) höhere NN-Werte mit dem Wert FALSCH. Bitte achten Sie darauf, dass der age_over_NN Datenelemente-Satz konsistent ist. Führen Sie die in den mDL-Daten vorhandenen Werte für NN1 – NN6 auf.

Wert für NN in Datenelement-Bezeichner	Wert (WAHR/FALSCH)
age_over_NN1(N)	WAHR

³ Hinweis: Alle Datenelemente in diesem Abschnitt sind im standardmäßigen mDL-Daten-Namensraum („org.iso.18013.5.1“) enthalten. Die ICS in diesem Abschnitt sollen nur für Dokumente der Dokumentart „org.iso.18013.5.1.mDL“ ausgefüllt werden.



age_over_NN2(N)	WAHR
age_over_NN3(N)	WAHR
age_over_NN4(H)	FALSCH
age_over_NN5(H)	FALSCH
age_over_NN6(H)	FALSCH

BEISPIEL: Der folgende Satz entspricht den oben angeführten Regeln:

age_over_15 = WAHR (NN1 = 15)

age_over_18 = WAHR (NN2 = 18)

age_over_21 = WAHR (NN3 = 21)

age_over_60 = FALSCH (NN4 = 60)

age_over_65 = FALSCH (NN5 = 65)

age_over_68 = FALSCH (NN6 = 68)

17.	Das Datenelement issuing_jurisdiction (Ausstellungsland) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
18.	Das Datenelement nationality (Nationalität) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
19.	Das Datenelement resident_city (Wohnort) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
20.	Das Datenelement resident_state (Bundesland des Wohnorts) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
21.	Das Datenelement resident_postal_code (PLZ des Wohnorts) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
22.	Das Datenelement resident_country (Land des Wohnorts) ist in den mDL-Daten vorhanden.	☒ JA ☐ NEIN
23.	Das Datenelement biometric_template_face (biometrisches Template Gesicht) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
24.	Das Datenelement biometric_template_voice (biometrisches Template Stimme) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
25.	Das Datenelement biometric_template_finger (biometrisches Template Finger) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
26.	Das Datenelement biometric_template_iris (biometrisches Template Iris) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
27.	Das Datenelement biometric_template_retina (biometrisches Template Retina) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
28.	Das Datenelement biometric_template_hand_geometry (biometrisches Template Handgeometrie) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
29.	Das Datenelement biometric_template_signature_sign (biometrisches Template Unterschrift) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
30.	Das Datenelement biometric_template_keystroke (biometrisches Template Tastendruck) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN



31.	Das Datenelement biometric_template_lip_movement (biometrisches Template Lippenbewegung) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
32.	Das Datenelement biometric_template_thermal_face (biometrisches Template Gesicht, thermisch) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
33.	Das Datenelement biometric_template_thermal_hand (biometrisches Template Hand, thermisch) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
34.	Das Datenelement biometric_template_gait (biometrisches Template Gangart) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
35.	Das Datenelement biometric_template_body_odor (biometrisches Template Körpergeruch) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
36.	Das Datenelement biometric_template_dna (biometrisches Template DNS) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
37.	Das Datenelement biometric_template_ear (biometrisches Template Ohr) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
38.	Das Datenelement biometric_template_finger_geometry (biometrisches Template Fingergeometrie) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
39.	Das Datenelement biometric_template_palm_geometry (biometrisches Template Handinnenflächengeometrie) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
40.	Das Datenelement biometric_template_vein_pattern (biometrisches Template Venenmuster) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
41.	Das Datenelement biometric_template_foot_print (biometrisches Template Fußabdruck) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
42.	Das Datenelement family_name_national_character (nationale Prägung des Nachnamens) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
43.	Das Datenelement given_name_national_character (nationale Prägung des Vornamens) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN
44.	Das Datenelement signature_usual_mark (übliches Zeichen in der Unterschrift) ist in den mDL-Daten vorhanden.	☐ JA ☒ NEIN

A.1.3 Für Technologie-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Technologie-Testfälle	
45.	mDL unterstützt Geräteinteraktion über NFC Static Handover.	☐ JA ☒ NEIN
46.	mDL unterstützt Geräteinteraktion über NFC Negotiated Handover. ⁴	☐ JA ☒ NEIN
47.	mDL unterstützt Geräteinteraktion über QR-Code.	☒ JA ☐ NEIN

⁴ Hinweis: NFC Static Handover und NFC Negotiated Handover können nicht gleichzeitig unterstützt werden, wenn ein mDL beide Technologien unterstützt.



48.	mDL unterstützt Geräteabfrage über NFC.	☐ JA ☒ NEIN
49.	mDL unterstützt überlange APDUs für die Geräteabfrage über NFC.	☐ JA ☒ NEIN
50.	mDL unterstützt BLE Version 4.2 (oder höher) und LE Data Packet Length Extension.	☒ JA ☐ NEIN
51.	mDL unterstützt Geräteabfrage über BLE im zentralen Client-Modus des Mdoc.	☒ JA ☐ NEIN
52.	Wird BLE im zentralen Client-Modus des Mdoc für die Geräteabfrage verwendet, verifiziert das Mdoc den Wert des Ident-Merkmals.	☐ JA ☒ NEIN
53.	mDL unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Client für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
54.	mDL unterstützt Geräteabfrage über BLE im Peripherieserver-Modus des Mdoc.	☒ JA ☐ NEIN
55.	mDL unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Server für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
56.	mDL unterstützt Geräteabfrage über Wi-Fi Aware.	☐ JA ☒ NEIN
57.	mDL unterstützt die Cipher Suite NCS-PK-2WDH-128 für Wi-Fi Aware. ⁵	☐ JA ☒ NEIN
58.	mDL unterstützt Serverabfrage über OIDC	☐ JA ☒ NEIN
59.	mDL unterstützt Serverabfrage über WebAPI	☐ JA ☒ NEIN
60.	mDL unterstützt die Übermittlung von Serverabfrage-Informationen innerhalb der Geräteinteraktionsstruktur.	☐ JA ☒ NEIN
61.	mDL richtet für die Zeit zwischen dem Versand von Geräteinteraktionsdaten und dem Empfang der Mitteilung über den Aufbau der Sitzung ein Time-out ein, wenn die Geräteinteraktion über QR-Code erfolgt.	☐ JA ☒ NEIN
62.	Falls ja, geben Sie die Dauer des vom mDL eingerichteten Time-outs in Sekunden an.	keines
63.	mDL richtet für die Zeit zwischen dem Versand von Geräteinteraktionsdaten und dem Empfang der Mitteilung über den Aufbau der Sitzung ein Time-out ein, wenn die Geräteinteraktion über NFC erfolgt.	☐ JA ☒ NEIN
64.	Falls ja, geben Sie die Dauer des vom mDL eingerichteten Time-outs in Sekunden an.	Keine

⁵ Gilt nur, wenn das Mdoc Wi-Fi Aware für die Geräteabfrage und NFC Negotiated Handover für die Geräteinteraktion unterstützt.





672

A.1.4 Für Sicherheitsmechanismus-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Sicherheitsmechanismus-Testfälle	
65.	Welche Kurven unterstützt der mDL für den Aufbau von Sitzungen? Kreuzen Sie alle unterstützten Kurven an. ⁶	☒ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
66.	mDL unterstützt den Austausch von mehr als einer Mdoc-Anfrage und -Antwort zur Geräteabfrage mit dem Mdoc-Lesegerät in einer einzigen Sitzung.	☐ JA ☒ NEIN
67.	Falls ja, geben Sie die Dauer des vom mDL eingerichteten Time-outs für die Beendigung der Sitzung in Sekunden an.	
68.	Welche Kurven unterstützt die Behörde, die den mDL ausstellt, für die Authentifizierung von Ausstellerdaten? Kreuzen Sie alle unterstützten Kurven an. ⁷	☒ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
69.	mDL unterstützt Mdoc MAC-Authentifizierung.	☐ JA ☒ NEIN
70.	Falls ja, welche Kurven unterstützt der mDL für die Mdoc MAC-Authentifizierung? Kreuzen Sie alle unterstützten Kurven an. ⁸	☐ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ X25519 ☐ X448 ☐ brainpoolP256r1

⁶ Unterstützt der mDL mehrere Kurven für den Aufbau von Sitzungen, sollte der mDL-Eigentümer für Testzwecke jeweils ein Muster für jede unterstützte Kurve bereitstellen.

⁷ Wenn auf dem mDL mehrere Dokumente vorhanden sind, kann die ausstellende Behörde theoretisch für die MSO-Unterschrift auf jedem dieser Dokumente eine andere Kurve verwenden. Es wird jedoch darauf hingewiesen, dass FIME davon ausgeht, dass für alle Dokumente in einem Muster die gleiche Kurve verwendet wird. Für Testzwecke sollte der mDL-Eigentümer jeweils ein Muster für jede unterstützte Kurve bereitstellen.

⁸ Wenn auf dem mDL mehrere Dokumente vorhanden sind, kann der mDL theoretisch für jedes dieser Dokumente eine andere Mdoc MAC-Authentifizierungskurve verwenden. Es wird jedoch darauf hingewiesen, dass FIME davon ausgeht, dass für alle Dokumente in einem Muster die gleiche Kurve verwendet wird. Für Testzwecke sollte der mDL-Eigentümer jeweils ein Muster für jede unterstützte Kurve bereitstellen.



	☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
71. mDL unterstützt Mdoc ECDSA-/EdDSA-Authentifizierung.	☒ JA ☐ NEIN
72. Falls ja, welche Kurven verwendet der mDL für die Mdoc ECDSA-/EdDSA-Authentifizierung? Kreuzen Sie alle unterstützten Kurven an. ⁹	☒ P-256 Kurve ☐ P-384 Kurve ☐ P-521 Kurve ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
73. mDL unterstützt die Authentifizierung von Mdoc-Lesegeräten.	☒ JA ☐ NEIN
74. Falls ja, welche Kurven unterstützt der mDL für die Authentifizierung von Mdoc-Lesegeräten? Kreuzen Sie alle unterstützten Kurven an. ¹⁰	☒ P-256 Kurve ☒ P-384 Kurve ☒ P-521 Kurve ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
75. Falls ja, benachrichtigt das Mdoc den Mdoc-Inhaber im Falle einer fehlgeschlagenen Authentifizierung des Mdoc-Lesegeräts darüber, dass die Identität des Prüfers nicht verifiziert werden konnte?	☒ JA ☐ NEIN
76. Falls ja, gibt es Datenelemente, die das Mdoc im Falle einer fehlgeschlagenen Authentifizierung des Lesegeräts nicht freigibt? Bitte führen Sie diese ggf. anhand von Namensraum und Bezeichner auf. ¹¹	☐ JA, und zwar ... ☒ NEIN

⁹ Hinweis: Es könnten für jedes Dokument auf einem mDL mehrere SDeviceKey-Paare für die Mdoc-Authentifizierung, jeweils in einer eigenen MSO, vorhanden sein. Daher ist es theoretisch möglich, dass ein einzelnes Dokument abwechselnd MAC-Authentifizierung und ECDSA-/EdDSA-Authentifizierung oder abwechselnd unterschiedliche Kurven für die ECDSA-/EdDSA-Authentifizierung verwendet. Es wird jedoch darauf hingewiesen, dass FIME davon ausgeht, dass für alle Dokumente in einem Muster durchgängig die gleiche Mdoc-Authentifizierungsmethode (MAC oder ECDSA/EdDSA) verwendet wird. Außerdem geht FIME davon aus, dass für alle Dokumente in einem Muster die gleiche ECDSA-/EdDSA-Kurve verwendet wird. Für Testzwecke sollte der mDL-Eigentümer jeweils ein Muster für jede unterstützte Kurve bereitstellen.

FIME geht davon aus, dass alle uns bereitgestellten mDL-Muster alle angekreuzten Kurven für die Authentifizierung von Mdoc-Lesegeräten unterstützen (sofern die richtigen CA-Zertifikate installiert sind).

¹¹ Es sollte mindestens bei Nr. 75 ODER Nr. 76 JA angekreuzt werden. Andernfalls hat das Fehlschlagen der Authentifizierung eines Lesegeräts keinerlei Auswirkungen.



77.	Falls ja, unterstützt Mdoc den Abruf von OCSP-Informationen, sofern vorhanden, zur Verifizierung eines Zertifikats für die Authentifizierung von Mdoc-Lesegeräten?	☐ JA ☒ NEIN
78.	Falls ja, unterstützt Mdoc den Abruf von CRL-Informationen zur Verifizierung eines Zertifikats für die Authentifizierung von Mdoc-Lesegeräten?	☒ JA ☐ NEIN
79.	Während der Tests steht eine vom Kunden bereitgestellte Test-CRL für alle IACA-Root-Zertifikate zur Verfügung.	☐ JA ☒ NEIN
80.	Während der Tests steht eine Test-CRL für alle vom Mdoc verwendeten Document Signer Zertifikate zur Verfügung.	☐ JA ☒ NEIN

A.1.5 Für Anwendungsfall-Testfälle

Nr.	Erklärungen zur Konformität der Implementierung für Anwendungsfall-Testfälle	
81.	Der mDL ermöglicht es dem mDL-Inhaber, seine Zustimmung zum Teilen des Lichtbilds zu verweigern, aber dennoch dem Teilen anderer im Rahmen derselben Anfrage angeforderter Datenelemente zuzustimmen.	☒ JA ☐ NEIN



675

Als Notar bestätige ich hiermit, dass dieses Dokument eine originalgetreue Abschrift des Originaldokuments ist.

München, den 29. Januar 2025

[Notarielles Siegel]

[Unterschrift]

Dr. Bernhard Schaub

Notar in München, Deutschland

(Kommission endet am 31. Oktober 2032)



674

Als vom Präsidenten des Landgerichts München I öffentlich bestellte und allgemein
beeidigte Übersetzerin für die spanische und englische Sprache bestätige ich:
Vorstehende Übersetzung des mir in englischer Sprache vorgelegten Dokuments ist
richtig und vollständig.

München, den 06. Februar 2025

Unterschrift und Stempel:

S.



Susanne Bernhardt – Ravensburger Ring 18 – 81243 München

Die Echtheit vorstehender Unterschrift der
Übersetzerin Ute Tobiasch wird hiermit bestätigt.
Zugleich wird bescheinigt, dass die Vorgenannte
öffentlich bestellte und allgemein beeidigte
Übersetzerin für die französische, spanische Sprache
ist.

München, 12. Februar 2025
Die Präsidentin des Landgerichts München I
Im Auftrag

Lea Adersberger
Lea Adersberger
Justizsekretärin



**EMBAJADA DE LA REPÚBLICA DOMINICANA
EN ALEMANIA**

SECCIÓN CONSULAR

CERTIFICO, que la firma que aparece al pie de
esta documentación es la del/ de la
Sra. Adelsberger-Justicia Regional
CIUDAD München y que es
la misma que acostumbra a usar en todos sus
actos y la cual es de su entera fé y crédito.
FECHA 14-02-2025



Heidi Taveras
HEIDI TAVERAS
CONSEJERA



**Veridos**

Oranienstraße 91, Berlin, Germany 10969
Berlin, Germany

2nd August 2024

Subject: Confirmation of conformity of iOS-based VD Mobile ID Version 1.0.10 (14)
with ISO/IEC 18013-5:2021

Dear Mr. Nicholas,

This letter serves to confirm that the abovementioned mDL application ('the application') was tested by FIME and found to be compliant with ISO/IEC 18013-5:2021 as of the date of this letter.

The test scope included testing the application on its interface to an mDL reader, by executing the test cases listed in the latest draft version of ISO/IEC 18013-6. Testing was limited to the features supported by the application, as indicated in the Implementation Conformance Statement 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. Veridos is solely and fully responsible for the conformity of the application to all applicable standards, specifications, and requirements.

The number of the Test Report corresponding to this letter is FIME_Veridos_iOS_02. This report contains the full overview of executed test cases and all test results.

Yours sincerely,

A handwritten signature in black ink, appearing to read "D. Bakker", with a long horizontal flourish underneath.

FIME

David Bakker
Technical Lead



mDL implementation scope

System Under Test

Application name and version	VD Mobile ID Version 1.0.10 (14)
Date of receipt of application	2024-07-23

Implementation Conformance Statement Summary

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

Test Environment

Standard	ISO/IEC 18013-5:2021
Test Case Specification	FIME mDL Test Case Specification
Test Suite	FIME mDL Application Test Suite v1.3.14
mDL Test App	mdltestapp-1.3.1.apk
Test device on which the mDL Test App is installed	Samsung Galaxy S24
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 15	iPhone SE (2 nd Gen)
OS version	iOS 17.5.1	iOS 13.5.1

A.1 Implementation conformance statement

The Implementation Conformance Statements below were provided to FIME by Veridos and have been used to determine which test cases to execute.

The ICS version used by Veridos is v1.10.

A.1.1 General information

mDL owner	
Application owner Name	Veridos
Address	Oranienstraße 91
City	Berlin
State	Berlin
Zip Code / Postal Code	10969
Country	Germany
Contact Name	Nicholas Larter
Contact Title	Senior Solutions Manager
Contact Email Address	nick.larter@veridos.com
Contact Phone Number	+49 1525 1334198

# mDL Application General Information	
- Certification Type	☒ Functional ¹ ☐ Integrated Product ²
- Application name and version	VD Mobile ID Version 1.0.10 (14)
- Minimum version of iOS supported	iOS 13
How many documents are present on the mDL under test?	1
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
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	

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.

³



681

A.1.2 For mdl data model test cases

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 have to be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".

#	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
16.	Data element age_over_NN is present in the mDL data.	☐ YES ☒ NO
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.		

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".



Value for NN in data element identifier	Value (TRUE / FALSE)
age_over_NN1(L)	TRUE
age_over_NN2(L)	TRUE
age_over_NN3(L)	TRUE
age_over_NN4(H)	FALSE
age_over_NN5(H)	FALSE
age_over_NN6(H)	FALSE

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)

17.	Data element issuing_jurisdiction is present in the mDL data.	☐ YES ☒ NO
18.	Data element nationality is present in the mDL data.	☒ YES ☐ NO
19.	Data element resident_city is present in the mDL data.	☒ YES ☐ NO
20.	Data element resident_state is present in the mDL data.	☒ YES ☐ NO
21.	Data element resident_postal_code is present in the mDL data.	☒ YES ☐ NO
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
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

A.1.3 For technology test cases

#	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

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

47.	mDL supports device engagement using 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 ☒ 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 for the time 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 is the time-out period implemented by the mDL?	None
63.	mDL implements a time-out for the time 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 is the time-out period implemented by the mDL?	None

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

A.1.4 For security mechanism test cases

#	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?	
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
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

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



686

	☐ 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 reader authentication fails? If so, please list them all by namespace and identifier. ¹¹	☐ YES, namely.... ☒ NO
77. If yes, mdoc supports retrieving OSCP information, if available, when verifying an mdoc reader authentication certificate.	☐ YES ☒ NO

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 authentication. 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 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.



687

78.	If yes, mdoc supports retrieving CRL information when verifying a 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

A.1.5 For use case test cases

#	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



688

I, Notary Public, hereby certify that this document
is a true copy of the original document.

Munich, this 29.01.2025



Dr. Bernhard Schaub
Notary Public in Munich,
Federal Republic of Germany
(commission expires: October 31, 2032)



689

