

652



ISO 18013-5



Traducción jurada del inglés

[Logotipo de la empresa fime]

Copia notarial

Veridos

Nicholas Larter

Oranienstraße 91, 10969 Berlín

27 de agosto de 2024

Asunto: Confirmación de la conformidad del VD CheckID basado en iOS, versión 1.0.6 (6) con la norma ISO/IEC 18013-5:2021

Estimado Sr. Larter:

Nos dirigimos a usted para confirmarle que el lector mDL mencionado anteriormente ha sido probado 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 del lector mDL con un 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 del lector mDL, 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 del lector mDL depende de diversos factores dentro de su entorno operativo. Veridos es el único y pleno responsable de la conformidad del lector mDL con todas las normas, especificaciones y requisitos aplicables.

El informe de pruebas que acompaña a esta carta lleva el número FIME_eID_Veridos_iOS_01. Este protocolo contiene una descripción completa de los casos de prueba ejecutados y todos los resultados de las pruebas.

Atentamente

FIME

[Firma]

David Bakker

Director técnico



Ámbito de aplicación de mDL

Sistema probado

Nombre y versión de la aplicación	VD CheckID Versión 1.0.6(6)
Aplicación recibida el	23 de julio de 2024

Resumen de la declaración de conformidad de la aplicación

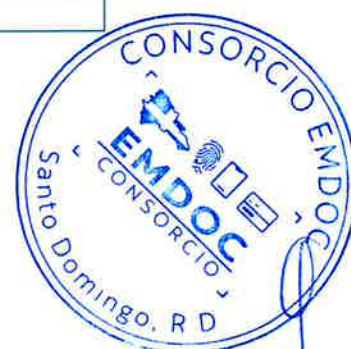
Tecnologías para la interacción con el dispositivo	Código QR NFC Static Handover NFC Negotiated Handover
Tecnologías para la consulta de dispositivos	BLE en el modo cliente central del Mdoc BLE en el modo servidor periférico del Mdoc NFC
Tecnologías para la consulta del servidor	Ninguna
Mecanismos de 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 para el lector mDL
Conjunto de pruebas	FIME Test Suite v1.4.0 para el lector mDL
Aplicación de prueba mDL	mdlreadertestapp-1.4.0.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 17.6.1	iOS 15.5



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 v1.6 de ICS.

A.1.1 Información general

Propietario del mDL	
Nombre del propietario de la aplicación	Veridos
Dirección	Oranienstraße 91, 10969 Berlín
Ciudad	Berlín
Estado Federal	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 el lector mDL		
-	Nombre y versión de la aplicación del lector	VD CheckID Versión 1.0.6(6)
-	Versión iOS compatible más baja	iOS 15



1.	Especifique qué DocType(s) admite el lector mDL	1
2.	Para cada DocType, especifique qué espacio/s de nombres admite el lector mDL.	org.iso.18013.5.1.mdl
3.	Para cada espacio de nombres, introduzca los identificadores de todos los elementos de datos que pueden ser consultados por el lector mDL.	family_name given_name birth_date document_number driving_privileges issue_date expiry_date issuing_authority issuing_country portrait un_distinguishing_sign sex height weight eye_colour hair_colour age_in_years age_birth_year birth_place nationality portrait_capture_date resident_address resident_city resident_state resident_postal_code resident_country signature_usual_mark family_name_national_character given_name_national_character age_over_18 age_over_19 age_over_20 age_over_21 age_over_22 age_over_23 age_over_24 age_over_25 age_over_26
4.	El lector mDL es capaz de solicitar múltiples documentos en un único mensaje DeviceRequest. ¹	☐ Sí ☒ NO
5.	El lector mDL es capaz de solicitar múltiples documentos en un único mensaje DeviceRequest. ²³	☐ Sí ☒ NO



6.	El lector mDL puede consultar el elemento de datos «issuing_jurisdiction» del espacio de nombres «org.iso.18013.5.1».	☐ SÍ ☒ NO
7.	El lector mDL puede consultar el elemento de datos «age_over_NN» del espacio de nombres «org.iso.18013.5.1».	☒ SÍ ☐ NO
8.	El lector mDL puede consultar el elemento de datos «issuing_country» del espacio de nombres «org.iso.18013.5.1».	☒ SÍ ☐ NO

A.1.2 Para casos de pruebas de tecnología

N.º	Declaraciones de conformidad de la implementación para los casos de prueba de tecnología	
9.	El lector Mdoc admite la interacción de dispositivos mediante el traspaso estático NFC. ⁴	☒ SÍ ☐ NO
10.	El lector Mdoc es compatible con la interacción de dispositivos vía NFC Negotiated Handover. ⁴	☒ SÍ ☐ NO
11.	El lector Mdoc admite la interacción de dispositivos mediante un código QR. ⁴	☒ SÍ ☐ NO
12 de	El lector Mdoc admite el escaneado de dispositivos mediante NFC. ⁴	☒ SÍ ☐ NO
13.	El lector Mdoc admite consultas de dispositivos a través de BLE en el modo de cliente central del Mdoc. ⁴	☒ SÍ ☐ NO
14.	El lector Mdoc admite consultas de dispositivos a través de BLE en el modo de servidor periférico del Mdoc. ⁴	☒ SÍ ☐ NO
15.	El lector Mdoc admite la consulta de dispositivos mediante BLE versión 5.0 (o superior) y LE 2M PHY.	☐ SÍ ☒ NO
16.	El lector Mdoc admite el sondeo de dispositivos a través de Wi-Fi Aware.	☐ SÍ ☒ NO
17.	El lector Mdoc admite consultas al servidor a través de OIDC	☐ SÍ ☒ NO
18.	El lector Mdoc admite consultas al servidor a través de WebAPI.	☐ SÍ ☒ NO
19.	El lector Mdoc admite APDUs extralargos para consultas de dispositivos a través de NFC.	☒ SÍ ☐ NO
20.	El lector Mdoc admite el perfil de transmisión L2CAP cuando actúa como cliente GATT para la consulta de dispositivos a través de BLE.	☐ SÍ ☒ NO
21.	El lector Mdoc admite el perfil de transmisión L2CAP si actúa como servidor GATT para la consulta de dispositivos a través de BLE.	☐ SÍ ☒ NO
22.	El lector Mdoc envía una estructura ReaderEngagement como parte del mensaje Handover Request Message durante la interacción con el dispositivo a través de un	☐ SÍ ☒ NO



NFC Negotiated Handover.		
23.	El lector Mdoc establece un Time-out para el periodo entre la inicialización de la transacción y la recepción de los datos de interacción del dispositivo.	☐ SÍ ☒ NO
24.	Si selecciona SÍ, introduzca la duración del Time-out (en segundos).	xx segundos
25.	El lector Mdoc establece un Time-out para el periodo entre la recepción de los datos de interacción del dispositivo y el establecimiento satisfactorio de una conexión de consulta del dispositivo.	☐ SÍ ☒ NO
26.	Si selecciona SÍ, introduzca la duración del Time-out (en segundos).	xx segundos

A.1.3 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		
27.	El lector Mdoc es compatible con la autenticación de lectores Mdoc.	☒ SÍ ☐ NO
28.	Si se selecciona SÍ, durante la comprobación se dispone de una CRL de prueba para todos los certificados de autenticación de lectores Mdoc utilizados por el lector Mdoc.	☒ SÍ ☐ NO
29.	Si se selecciona SÍ, la autoridad de certificación que ha firmado todos los certificados de autenticación de lectores Mdoc utilizados por el lector Mdoc dispone de un servicio OCSP.	☐ SÍ ☒ NO
30.	Si se selecciona SÍ, se dispone de un OCSP-Responder de prueba durante la comprobación de todos los certificados de autenticación para lectores Mdoc utilizados por el lector Mdoc.	☐ SÍ ☒ NO
31.	Si se selecciona SÍ, ¿qué curva utiliza el lector Mdoc para la autenticación de los lectores Mdoc?	☒ Curva P-256 ☒ Curva P-384 ☒ Curva P-521 ☒ Ed25519 ☒ Ed448 ☒ brainpoolP256r1 ☒ brainpoolP320r1 ☒ brainpoolP384r1 ☒ brainpoolP512r1
32.	El lector de Mdoc admite el intercambio de más de una solicitud y respuesta de Mdoc para la consulta del dispositivo en el Mdoc en una única sesión.	☐ SÍ ☒ NO
33.	El lector Mdoc admite el intercambio de más de una solicitud y respuesta para la consulta del servidor en la infraestructura de la autoridad de certificación emisora en una única sesión.	☐ SÍ ☒ NO
34.	El lector Mdoc admite la recuperación de información OCSP (si está disponible) al verificar un certificado de servidor TLS. ⁵	☐ SÍ ☒ NO



35.	El lector Mdoc consulta la información de estado OCSP del certificado del servidor en el protocolo de enlace TLS. ⁵	☐ SÍ ☒ NO
36.	El lector Mdoc admite TLS v 1.3. ⁵	☐ SÍ ☒ NO
37.	El lector Mdoc admite la autenticación de clientes TLS.	☐ SÍ ☒ NO
38.	En caso afirmativo, se dispone de una CRL de prueba durante la prueba para todos los certificados de cliente TLS utilizados por el lector de Mdoc.	☐ SÍ ☒ NO
39.	Si se selecciona SÍ en el punto 34, la autoridad de certificación que ha firmado todos los certificados de autenticación de clientes TLS utilizados por el lector Mdoc dispone de un servicio OCSP.	☐ SÍ ☒ NO
40.	Si la respuesta es afirmativa, se dispondrá de un OCSP-Responder de prueba durante las pruebas para todos los certificados de autenticación de cliente TLS utilizados por el lector Mdoc.	☐ SÍ ☒ NO
41.	¿Cuántos segundos dura el Time-out de finalización de sesión establecido por el lector Mdoc?	300 segundos

¹ Si se selecciona SÍ, el lector mDL debe de apoyar por lo menos dos diferentes DocTypes.

² Esa declaración sólo es aplicable si el lector mDL apoya consultas al servidor a través de WebAPI.

³ Si se selecciona SÍ, el lector mDL debe de apoyar por lo menos dos diferentes DocTypes.

⁴ Por favor tenga en cuenta que eso es mandatorio para apoyar lectores mDL, pero opcional para lectores mdoc en general.

⁵ Esa declaración sólo es aplicable si el lector mdoc apoya consultas al servidor a través de WebAPI.



762

Yo, representante notarial, certifico que este documento es una copia fiel de un archivo pdf.

En Múnich, a 15/01/2025

[Sello del notario]

[Firma]

Dr. Christian Linke,
representante notarial de

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

Por la presente se certifica la autenticidad de la firma precedente del Dr. Christian Linke, representante notarial, y del sello aquí estampado.
Asimismo, se certifica que la persona arriba mencionada estaba autorizada para llevar a cabo este acto oficial.

Múnich, 16 de enero de 2025
El Presidente del Tribunal Regional I de Múnich [Landgericht]
Por poder

[Firma ilegible]

Lea Adelsberger
Empleada del Tribunal

[Sello redondo del Tribunal
Regional de Múnich, Baviera]



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

München, den 01. Februar 2025

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

Múnich, a 1 de febrero del 2025

Unterschrift und Stempel:

Firma y sello:



 Susanne Bernhardt – Ravensburger Ring 18 – 81243 München

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

München, 07. Februar 2025

Die Präsidentin des Landgerichts München I
 Im Auftrag


 Lea Adelsberger
 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
Sr./a. LEA- JUSTICIA REGIONAL
CIUDAD MUNCHEN y que es
la misma que acostumbra a usar en todos sus
actos y la cual es de su entera fé y crédito.
FECHA 12.2.2025


ROCIO PELLERANO
MINISTRA CONSEJERA



Beglaubigte Übersetzung aus dem Englischen

764

[Firmenlogo von fime]

Beglaubigte Abschrift

Veridos

Nicholas Larter

Oranienstraße 91, 10969 Berlin

27. August 2024

Betreff: Bestätigung der Konformität der auf iOS basierenden VD CheckID, Version 1.0.6 (6) mit ISO/IEC 18013-5:2021

Sehr geehrter Herr Larter,

mit diesem Schreiben bestätigen wir, dass das oben genannte mDL-Lesegerät von FIME getestet und im Ergebnis festgestellt wurde, dass es mit Stand zum Datum dieses Schreibens der Norm ISO/IEC 18013-5:2021 entspricht.

Teil des Testumfangs war die Prüfung des mDL-Lesegeräts auf seiner Schnittstelle zu einem mDL durch Ausführung der in der neuesten Entwurfsfassung von ISO/IEC 18013-6 aufgeführten Testfälle. Die Prüfung bezog sich nur auf vom mDL-Lesegerät 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 des mDL-Lesegeräts von verschiedenen Faktoren innerhalb ihrer Betriebsumgebung abhängt. Für die Konformität des mDL-Lesegeräts mit allen geltenden Normen, Spezifikationen und Anforderungen trägt Veridos die alleinige und volle Verantwortung.

Das zu diesem Schreiben gehörende Prüfprotokoll trägt die Nummer FIME_eID_Veridos_iOS_01. Dieses Protokoll enthält eine vollständige Übersicht der ausgeführten Testfälle und aller Testergebnisse.

Mit freundlichen Grüßen

[Unterschrift]

FIME

David Bakker

Technischer Leiter





765

mDL-Implementierungsumfang

Getestetes System

Bezeichnung und Version der Anwendung	VD CheckID Version 1.0.6(6)
Anwendung erhalten am	23. Juli 2024

Zusammenfassung der Erklärung zur Konformität der Implementierung

Technologien zur Geräteinteraktion	QR-Code NFC Static Handover NFC Negotiated Handover
Technologien zur Geräteabfrage	BLE im zentralen Client-Modus des Mdoc BLE im Peripherieserver-Modus des Mdoc NFC
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 Testfallspezifikation für mDL-Lesegerät
Test Suite	FIME Test Suite v1.4.0 für mDL-Lesegerät
mDL-Testapp	mdlreadertestapp-1.4.0.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 17.6.1	iOS 15.5



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 v1.6.

A.1.1 Allgemeine Informationen

mDL-Eigentümer	
Name des Eigentümers der Anwendung	Veridos
Anschrift	Oranienstraße 91, 10969 Berlin
Stadt	Berlin
Bundesland	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 zum mDL-Lesegerät		
-	Bezeichnung und Version der Lesegeräteanwendung	VD CheckID Version 1.0.6(6)
-	Niedrigste unterstützte iOS-Version	iOS 15



1.	Geben Sie an, welche DocType(s) vom mDL-Lesegerät unterstützt werden	1
2.	Geben Sie für jeden DocType an, welche Namespace(s) vom mDL-Lesegerät unterstützt werden.	org.iso.18013.5.1.mdl
3.	Geben Sie für jeden Namespace die Kennungen aller Datenelemente an, die vom mDL-Lesegerät abgefragt werden können.	family_name given_name birth_date document_number driving_privileges issue_date expiry_date issuing_authority issuing_country portrait un_distinguishing_sign sex height weight eye_colour hair_colour age_in_years age_birth_year birth_place nationality portrait_capture_date resident_address resident_city resident_state resident_postal_code resident_country signature_usual_mark family_name_national_character given_name_national_character age_over_18 age_over_19 age_over_20 age_over_21 age_over_22 age_over_23 age_over_24 age_over_25 age_over_26
4.	Das mDL-Lesegerät ist in der Lage, mehrere Dokumente in einer einzigen DeviceRequest-Meldung abzufragen. ¹	☐ JA ☒ NEIN





768

5.	Das mDL-Lesegerät ist in der Lage, mehrere Dokumente in einer einzigen ServerRequest-Meldung abzufragen. ^{2 3}	☐ JA ☒ NEIN
6.	Das mDL-Lesegerät ist in der Lage, das „issuing_jurisdiction“-Datenelement vom Namespace „org.iso.18013.5.1“ abzufragen	☐ JA ☒ NEIN
7.	Das mDL-Lesegerät ist in der Lage, das „age_over_NN“-Datenelement vom Namespace „org.iso.18013.5.1“ abzufragen	☒ JA ☐ NEIN
8.	Das mDL-Lesegerät ist in der Lage, das „issuing_country“-Datenelement vom Namespace „org.iso.18013.5.1“ abzufragen	☒ JA ☐ NEIN

A.1.2 Für Technologie-Testfälle

Nr. Erklärungen zur Konformität der Implementierung für Technologie-Testfälle		
9.	Das Mdoc-Lesegerät unterstützt Geräteinteraktion über NFC Static Handover. ⁴	☒ JA ☐ NEIN
10.	Das Mdoc-Lesegerät unterstützt Geräteinteraktion über NFC Negotiated Handover. ⁴	☒ JA ☐ NEIN
11.	Das Mdoc-Lesegerät unterstützt Geräteinteraktion über einen QR-Code. ⁴	☒ JA ☐ NEIN
12.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über NFC. ⁴	☒ JA ☐ NEIN
13.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über BLE im zentralen Client-Modus des Mdoc. ⁴	☒ JA ☐ NEIN
14.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über BLE im Peripherieserver-Modus des Mdoc. ⁴	☒ JA ☐ NEIN
15.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über BLE Version 5.0 (oder höher) und LE 2M PHY.	☐ JA ☒ NEIN
16.	Das Mdoc-Lesegerät unterstützt Geräteabfrage über Wi-Fi Aware.	☐ JA ☒ NEIN
17.	Das Mdoc-Lesegerät unterstützt Serverabfrage über OIDC	☐ JA ☒ NEIN
18.	Das Mdoc-Lesegerät unterstützt Serverabfrage über WebAPI.	☐ JA ☒ NEIN
19.	Das Mdoc-Lesegerät unterstützt überlange APDUs für die Geräteabfrage über NFC.	☒ JA ☐ NEIN

¹ Falls hier JA ausgewählt wird, sollte das mDL-Lesegerät mindestens zwei verschiedene DocTypes unterstützen.

² Diese Aussage trifft nur zu, falls das mDL-Lesegerät Serverabfragen über WebAPI unterstützt.

³ Falls hier JA ausgewählt wird, sollte das mDL-Lesegerät mindestens zwei verschiedene DocTypes unterstützen.

⁴ Dies ist zur Unterstützung von mDL Lesegeräten obligatorisch, jedoch optional für Mdoc-Lesegeräte im Allgemeinen.



20.	Das Mdoc-Lesegerät unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Client für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
21.	Das Mdoc-Lesegerät unterstützt das Übermittlungsprofil L2CAP, wenn es als GATT-Server für die Geräteabfrage über BLE fungiert.	☐ JA ☒ NEIN
22.	Das Mdoc-Lesegerät sendet während der Geräteinteraktion über ein NFC Negotiated Handover eine ReaderEngagement-Struktur als Teil der Handover Request Message.	☐ JA ☒ NEIN
23.	Das Mdoc-Lesegerät richtet ein Time-out für den Zeitraum zwischen der Transaktionsinitialisierung und dem Empfang der Geräteinteraktionsdaten ein.	☐ JA ☒ NEIN
24.	Bei Auswahl von JA geben Sie die Dauer des Time-outs (in Sekunden) an.	xx Sekunden
25.	Das Mdoc-Lesegerät richtet ein Time-out für den Zeitraum zwischen dem Empfang der Geräteinteraktionsdaten und der erfolgreichen Einrichtung einer Geräteabfrageverbindung ein.	☐ JA ☒ NEIN
26.	Bei Auswahl von JA geben Sie die Dauer des Time-outs (in Sekunden) an.	xx Sekunden

A.1.3 Für Sicherheitsmechanismus-Testfälle

Nr. Erklärungen zur Konformität der Implementierung für Sicherheitsmechanismus-Testfälle		
27.	Das Mdoc-Lesegerät unterstützt die Authentifizierung von Mdoc-Lesegeräten.	☒ JA ☐ NEIN
28.	Bei Auswahl von JA steht während der Prüfung eine Test-CRL für alle vom Mdoc-Lesegerät verwendeten Authentifizierungszertifikate für Mdoc-Lesegeräte zur Verfügung	☒ JA ☐ NEIN
29.	Bei Auswahl von JA besitzt die Zertifizierungsstelle, die alle vom Mdoc-Lesegerät verwendeten Authentifizierungszertifikate des Mdoc-Lesegeräts signiert hat, einen OCSP-Dienst.	☐ JA ☒ NEIN
30.	Bei Auswahl von JA steht während der Prüfung ein Test-OCSP-Responder für alle vom Mdoc-Lesegerät verwendeten Authentifizierungszertifikate für Mdoc-Lesegeräte zur Verfügung.	☐ JA ☒ NEIN
31.	Bei Auswahl von JA welche Kurven verwendet das Mdoc-Lesegerät für die Authentifizierung von Mdoc-Lesegeräten?	☒ Kurve P-256 ☒ Kurve P-384 ☒ Kurve P-521 ☒ Ed25519 ☒ Ed448 ☒ brainpoolP256r1 ☒ brainpoolP320r1 ☒ brainpoolP384r1 ☒ brainpoolP512r1
32.	Das Mdoc-Lesegerät unterstützt den Austausch von mehr als einer Mdoc-Anfrage und -Antwort zur Geräteabfrage beim Mdoc in einer einzigen Sitzung.	☐ JA ☒ NEIN



33.	Das Mdoc-Lesegerät unterstützt den Austausch von mehr als einer Anfrage und Antwort zur Serverabfrage bei der Infrastruktur der ausstellenden Zertifizierungsstelle in einer einzigen Sitzung.	☐ JA ☒ NEIN
34.	Das Mdoc-Lesegerät unterstützt den Abruf von OCSP-Informationen (sofern vorhanden) bei der Verifizierung eines TLS-Serverzertifikats. ⁵	☐ JA ☒ NEIN
35.	Das Mdoc-Lesegerät fragt OCSP-Statusinformationen für das Serverzertifikat im TLS-Handshake ab ⁵	☐ JA ☒ NEIN
36.	Das Mdoc-Lesegerät unterstützt TLS v 1.3. ⁵	☐ JA ☒ NEIN
37.	Das Mdoc-Lesegerät unterstützt die Authentifizierung von TLS-Clients.	☐ JA ☒ NEIN
38.	Falls ja, steht während der Prüfung eine Test-CRL für alle vom Mdoc-Lesegerät verwendeten TLS-Clientzertifikate zur Verfügung	☐ JA ☒ NEIN
39.	Falls unter Punkt 34 ja ausgewählt wird, besitzt die Zertifizierungsstelle, die alle vom Mdoc-Lesegerät verwendeten TLS-Clientauthentifizierungszertifikate signiert hat, einen OCSP-Dienst.	☐ JA ☒ NEIN
40.	Falls die Antwort ja lautet, steht während der Tests ein Test-OCSP-Responder für alle vom Mdoc-Lesegerät verwendeten TLS-Clientauthentifizierungszertifikate zur Verfügung.	☐ JA ☒ NEIN
41.	Wie viele Sekunden beträgt das vom Mdoc-Lesegerät eingerichtete Time-out für die Beendigung der Sitzung?	300 Sekunden

⁵ Diese Aussage trifft nur zu, falls das Mdoc-Lesegerät eine Serverabfrage über WebAPI unterstützt.



I, notary representative, hereby certify that this document is a true copy of a pdf file.

Munich, this 15.01.2025

[Notary's seal]

[Signature]

Dr Christian Linke,

notary representative of

Dr Bernhard Schaub

Notary Public in Munich,

Federal Republic of Germany

(commission expires: October 31, 2032)

The authenticity of the preceding signature of Dr Christian Linke, notary representative, and the seal hereto affixed is hereby certified.
It is also certified that the above-mentioned person was authorized to carry out this official act.

Munich, January 16, 2025

The President of the Munich Regional Court I [*Landgericht*]

By proxy

[Illegible signature]

Lea Adelsberger
Court Employee

[Round seal of the Munich
Regional Court, Bavaria]



772

Als vom Präsidenten des Landgerichts München I öffentlich bestellter und allgemein beeidigter Übersetzer für die englische Sprache bestätige ich:
Vorstehende Übersetzung des mir in englischer Sprache als beglaubigte Abschrift vorgelegten Dokuments ist richtig und vollständig.

München, den 30. Januar 2025

In my capacity as a public certified translator for the English language, duly commissioned and sworn by the President of the Regional Court I of Munich, Bavaria, I hereby certify the above to be a true and correct translation of the English document presented to me as a certified copy.

Munich, January 30, 2025

Unterschrift u. Stempel:
Signature & stamp:


Patrick Hampp | Annelies-Kupper-Allee 20 | 85540 Haar



Veridos

Nicholas Larter
Oranienstraße 91, Berlin, Germany 10969

27th August 2024

Subject: Confirmation of conformity of iOS-based VD CheckID Version 1.0.6(6)
with ISO/IEC 18013-5:2021

Dear Mr. Larter,

This letter serves to confirm that the abovementioned mDL reader 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 mDL reader on its interface to an mDL, 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 mDL reader, 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 mDL reader is dependent on several factors in its operational environment. Veridos is solely and fully responsible for the conformity of the mDL reader to all applicable standards, specifications, and requirements.

The number of the Test Report corresponding to this letter is FIME_eID_Veridos_iOS_01. This report contains the full overview of executed test cases and all test results.

Yours sincerely,



FIME

David Bakker
Technical Lead



mDL implementation scope

System Under Test

Application name and version	VD CheckID Version 1.0.6(6)
Date of receipt of application	2024-07-23

Implementation Conformance Statement Summary

Device engagement technologies	QR code NFC Static Handover NFC Negotiated Handover
Device retrieval technologies	BLE in mdoc central client mode BLE in mdoc peripheral server mode NFC
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 Reader Test Case Specification
Test Suite	FIME mDL Reader Test Suite v1.4.0
mDL Test App	mdlreadertestapp-1.4.0.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 17.6.1	iOS 15.5



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 v1.6.

A.1.1 General information

mDL owner	
Application owner Name	Veridos
Address	Oranienstraße 91, Berlin, Germany 10969
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 reader General Information	
- Reader Application name and version	VD CheckID Version 1.0.6(6)
- Minimum version of iOS supported	iOS 15



1.	Specify which DocType(s) the mDL reader supports	1
2.	For each DocType, specify which namespace(s) the mDL reader supports.	org.iso.18013.5.1.mdl
3.	For each namespace, specify the identifiers of all data elements that can be requested by the mDL reader.	family_name given_name birth_date document_number driving_privileges issue_date expiry_date issuing_authority issuing_country portrait un_distinguishing_sign sex height weight eye_colour hair_colour age_in_years age_birth_year birth_place nationality portrait_capture_date resident_address resident_city resident_state resident_postal_code resident_country signature_usual_mark family_name_national_character given_name_national_character age_over_18 age_over_19 age_over_20 age_over_21 age_over_22 age_over_23 age_over_24 age_over_25 age_over_26
4.	mDL reader is able to request multiple documents in a single DeviceRequest message. ¹	☐ YES ☒ NO
5.	mDL reader is able to request multiple documents in a single ServerRequest message. ^{2,3}	☐ YES ☒ NO



6.	mDL reader is able to request the issuing_jurisdiction data element from namespace org.iso.18013.5.1	☐ YES ☒ NO
7.	mDL reader is able to request the age_over_NN data element from namespace org.iso.18013.5.1	☒ YES ☐ NO
8.	mDL reader is able to request the issuing_country data element from namespace org.iso.18013.5.1	☒ YES ☐ NO

A.1.2 For technology test cases

#	ICS statements for Technologies Test cases	
9.	mdoc reader supports device engagement using NFC Static Handover. ⁴	☒ YES ☐ NO
10.	mdoc reader supports device engagement using NFC Negotiated Handover. ⁴	☒ YES ☐ NO
11.	mdoc reader supports device engagement using a QR code. ⁴	☒ YES ☐ NO
12.	mdoc reader supports device retrieval using NFC. ⁴	☒ YES ☐ NO
13.	mdoc reader supports device retrieval using BLE in mdoc central client mode. ⁴	☒ YES ☐ NO
14.	mdoc reader supports device retrieval using BLE in mdoc peripheral server mode. ⁴	☒ YES ☐ NO
15.	mdoc reader supports device retrieval using BLE version 5.0 (or above) and LE 2M PHY.	☐ YES ☒ NO
16.	mdoc reader supports device retrieval using Wi-Fi Aware.	☐ YES ☒ NO
17.	mdoc reader supports server retrieval using OIDC	☐ YES ☒ NO
18.	mdoc reader supports server retrieval using WebAPI.	☐ YES ☒ NO
19.	mdoc reader supports extended-length APDUs for device retrieval using NFC.	☒ YES ☐ NO
20.	mdoc reader supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE.	☐ YES ☒ NO

¹ If this is set to YES, the mDL reader should support at least two different DocTypes.

² This statement is only applicable if the mDL reader supports server retrieval using WebAPI.

³ If this statement is set to YES, the mDL reader should support at least two different DocTypes.

⁴ Note this is mandatory to support for mDL readers, but optional for mdoc readers in general.



21.	mdoc reader supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE.	☐ YES ☒ NO
22.	mdoc reader sends a ReaderEngagement structure as part of the Handover Request Message during device engagement using NFC Negotiated Handover.	☐ YES ☒ NO
23.	mdoc reader implements a time-out for the time between the transaction initialization and receiving device engagement data.	☐ YES ☒ NO
24.	If yes, indicate how long is the time-out (in seconds).	xx seconds
25.	mdoc reader implements a time-out for the time between receiving device engagement data and the successful set-up of a device retrieval connection.	☐ YES ☒ NO
26.	If yes, indicate how long is the time-out (in seconds).	xx seconds

A.1.3 For security mechanism test cases

#	ICS statements for Security Mechanisms test cases	
27.	mdoc reader supports mdoc reader authentication	☒ YES ☐ NO
28.	If yes, a test CRL for all mdoc reader authentication certificates used by the mdoc reader is available during testing	☒ YES ☐ NO
29.	If yes, the CA that signed all mdoc reader authentication certificates used by the mdoc reader has an OCSP service.	☐ YES ☒ NO
30.	If yes, a test OCSP Responder for all mdoc reader authentication certificates used by the mdoc reader is available during testing.	☐ YES ☒ NO
31.	If yes, which curves does the mdoc reader use for mdoc reader authentication?	☒ Curve P-256 ☒ Curve P-384 ☒ Curve P-521 ☒ Ed25519 ☒ Ed448 ☒ brainpoolP256r1 ☒ brainpoolP320r1 ☒ brainpoolP384r1 ☒ brainpoolP512r1
32.	mdoc reader supports exchanging more than one device retrieval mdoc request and response with the mdoc in a single session.	☐ YES ☒ NO
33.	mdoc reader supports exchanging more than one server retrieval request and response with the issuing authority infrastructure in a single session.	☐ YES ☒ NO
34.	mdoc reader supports retrieving OCSP information, if available when verifying a TLS server certificate. ⁵	☐ YES ☒ NO

⁵ This statement is only applicable if the mdoc reader supports server retrieval using WebAPI.



35.	mdoc reader requests OCSP status information for the server certificate in the TLS handshake ⁵	☐ YES ☒ NO
36.	mdoc reader supports TLS v 1.3. ⁵	☐ YES ☒ NO
37.	mdoc reader supports TLS Client Authentication.	☐ YES ☒ NO
38.	If yes, a test CRL for all TLS Client certificates used by the mdoc reader is available during testing	☐ YES ☒ NO
39.	If yes to #34, the CA that signed all TLS Client authentication certificates used by the mdoc reader has an OCSP service.	☐ YES ☒ NO
40.	If yes, a test OCSP Responder for all TLS Client authentication certificate used by the mdoc reader is available during testing.	☐ YES ☒ NO
41.	How many seconds is the time-out period for session termination implemented by the mdoc reader?	300 seconds

I, notary representative, hereby certify that this document is a true copy
of a pdf-file.

Munich, this 15.01.2025



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

Die Echtheit vorstehender Unterschrift des
Notarassessors Dr. Christian Linke und die Echtheit
des beigedruckten Dienstsiegels werden hiermit
bestätigt.

Zugleich wird bescheinigt, dass der Vorgenannte zur
Vornahme der Amtshandlung befugt war.

München, 16. Januar 2025

Die Präsidentin des Landgerichts München I
Im Auftrag



Lea Adelsberger
Justizsekretärin



781



**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 Sr./a. Adisberger - 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 12-02-2025

