

Certificaciones ISO del Fabricante de las Impresoras, el Mobile ID y el PKI

ISO 18013 para Android

YO, ANA MARIA FERIA, Intérprete Judicial del Juzgado de Primera Instancia del Distrito Nacional, debidamente juramentada para el ejercicio legal de mi cargo, CERTIFICO que he procedido a la traducción de un documento redactado en idioma inglés, cuya versión al español, según mi criterio, es la siguiente:

Papel membrete de FIME Services North America Inc., domiciliado en 1945 The Exchange, Suite 200 SE, Atlanta, GA 30339, Estados Unidos de América

Global Enterprise Technologies Corp
230 2nd Avenue, Waltham, Massachusetts, 02451, E.U.A.

15 de noviembre de 2024

Asunto: Confirmación de Conformidad de Android basado en mDL - GET Mobile ID, v.5.1.23 con ISO/IEC 18013-5:2021

Estimado Sr. Alexander:

Esta carta sirve para confirmar la conformidad de la aplicación mDL mencionada más arriba ('la aplicación') con ISO/IEC 18013-5:2021.

FIME probó la versión v.5.5.0 de esta aplicación mDL en diciembre 2022 y determinó que cumple con esta norma. El alcance de la prueba incluyó probar la aplicación en su interface con un lector mDL, ejecutando los casos de prueba enumerados en la última versión preliminar de ISO/IEC 18013-6. Las pruebas se limitaron a las características admitidas por la aplicación, como se indica en la Declaración de Conformidad de Implementación en el Apéndice de esta carta. Los detalles de la aplicación bajo prueba, el entorno de prueba y los dispositivos de prueba utilizados para la misma se pueden encontrar en la página siguiente. El número del Informe de Prueba que contiene la descripción completa de los casos de prueba ejecutados y todos los resultados de las pruebas es UL_eID_GET Group_Android_002.

En agosto de 2024, GET proporcionó a Fime notas de la versión que describen los cambios entre la versión 5.5.0 probada y la versión 5.1.23. Después de revisar esas notas de la versión, FIME concluyó que no es necesario volver a probar la versión 5.1.23, ya que es poco probable que los cambios descritos afecten la conformidad con la norma ISO/IEC 18013-5.

Como recordatorio, el correcto funcionamiento de la aplicación depende de varios factores de su entorno operativo. GET Group es el único y total responsable de la conformidad de la aplicación con todas las normas, especificaciones y requisitos aplicables.

Esta carta de confirmación es válida por un año a partir de su fecha de emisión.

De ustedes sinceramente,
Firma ilegible
FIME
David Bakker
Líder Técnico



Alcance Implementación mDL

Sistema bajo Prueba

Nombre y Versión Aplicación	mDL – GET Mobile ID, v.5.5.0
Sistema Operacional	Android
Aplicación disponible a través	Paquete Archivo Android (APK) de la Aplicación mDL que fue provisto por el cliente
Fecha de Recibo Aplicación	2021-10-26
Tipo Certificación	Certificación Integrada del Producto
Autoridad Emisora	División Licencias de Conducir de Utah

Resumen Declaración de Conformidad de la Implementación

Tecnologías Interacción con Dispositivos	Código QR, NFS Static Handover
Tecnologías Recuperación de Dispositivos	BLE en mdoc modo cliente central BLE en mdoc modo servidor periférico NFC, WiFi-Aware ¹
Tecnologías Recuperación de Servidores	WebAPI, OIDC
Mecanismos Seguridad para la Recuperación Dispositivos	Cifrado de sesión, autenticación de datos del emisor, autenticación mdoc, autenticación del lector mdoc

Ambiente de la Prueba

Estándar	ISO/IEC 1803-5:2021
Especificación Caso Prueba	Especificación Caso Prueba FIME mDL
Conjunto de Pruebas	Conjunto Prueba v1.1.11 Aplicación UL mDL
Aplicación Prueba mDL	Mdlttestapp-1.1.4
Dispositivo de Prueba donde se instala la Aplicación Prueba mDL	Google Pixel 3 ^a
Versión OS del Dispositivo de Prueba donde se instala la Aplicación de Prueba mDL	Android 12

Dispositivos y Plataforma de la Prueba

Marca y Tipo Dispositivo	Google Pixel 6	Samsung Galaxy S9
Versión OS	Android 13	Android 8

A.1 Resumen Declaración de Conformidad de la Implementación

Las Declaraciones de Conformidad de la Implementación que aparecen más adelante fueron proporcionadas a FIME por el Grupo GET y se han usado para determinar qué casos de prueba se deben ejecutar.

La versión de ICS que utiliza el Grupo GET es la v1.5.

A.1.1 Información General

Propietario mDL	
Nombre Propietario de la Aplicación	GET Group
Dirección	230 2da Avenue
Ciudad	Waltham
Estado	MA
Código Postal	02451
País	EUA
Nombre del Contacto	Alexander Kambanis

¹ Wi-Fi Aware fue probado solo con el dispositivo Google Pixel 6 funcionando con Android 13.

Título del Contado	Director Gerente
Dirección correo electrónico de Contacto	akambanis@gelgroupna.com
Número de teléfono del Contacto	+1 (617) 901-1700

Información General Autoridad Emisora (Aplicable únicamente a la Certificación del Producto Integrada)	
Nombre Autoridad Emisora	Departamento de Seguridad Pública de Utah, División Licencia de Conducir
Dirección Autoridad Emisora	Departamento de Seguridad Pública de Utah
Ciudad	Ciudad Salt Lake
Estado	Utah
Código Postal	84114-4501
País	EUA
Nombre del Contacto	Brittaney Akagi
Título del Contado	IT / Gerente Aseguramiento de Calidad
Dirección correo electrónico de Contacto	bakagi@utah.gov

Información General Aplicación mDL	
Tipo Certificación	☐ Funcional ² ☒ Producto Integrado ³
Nombre y Versión de la Aplicación	GET Mobile ID, v. 5.5.0
La versión mínima de soporte iOS	Android 8.0 (Nivel API 26)
¿Cuántos documentos están presentes en la prueba mDL?	1

Para cada documento, por favor especifique el DocType [Tipo de Documento] que aplique	org.iso.18013.5.1.mDL
Para cada documento, por favor especifique todos los espacios de nombres de los elementos usados en el documento.	org.iso.18013.5.1, com.scytales.18013.5.1, org.aamva.us, org.iso.18013.5.1.aamva
Para cada espacio de nombres diferente del nombre del espacio mDL ("org.iso.18013.5.1"), por favor, especifique los identificadores de todos los datos de los elementos presentes en el documento.	<pre>{ "org.iso.18013.5.1.mDL" : { "com.scytales.18013.5.1" : ["status", "categoría_vehículo", "lista_categoría_vehículo", "dirección_completa", "e-mail", "número_móvil"], "org.aamva.us" : ["real_id"], "org.iso.18013.5.1.aamva" : ["DHS_compliance"] } }</pre>

A.1.2 Modelo de Datos mDL para casos de prueba

Nota: todos los elementos de datos de esta sección se encuentran en el espacio predeterminado de nombres de datos mDL ("org.iso.18013.5.1"). Las declaraciones ICS de esta sección deben completarse solo para documentos que tengan

²Para la certificación funcional, el conjunto de datos mDL puede ser un conjunto de datos de muestra que el propietario del mDL desea personalizar en el mDL.

³La certificación integrada de productos requiere que el conjunto de datos mDL sea preparado y personalizado por un Sistema de registro (SoR) del emisor y el conjunto de datos mDL debe ser representativo del mDL que se utilizará en producción



DocType = "org.iso.18013.5.1.mDL".

#	Declaraciones ICS para los casos de prueba del Modelo de Datos mDL ⁴	
1.	El elemento de datos número_administrativo está presente en los datos mDL.	☒ SI ☐ No
2.	El elemento de datos sexo_ está presente en los datos mDL.	☒ SI ☐ No
3.	El elemento de datos altura_ está presente en los datos mDL.	☒ SI ☐ No
4.	El elemento de datos peso_ está presente en los datos mDL.	☒ SI ☐ No
5.	El elemento de datos color de ojos_ está presente en los datos mDL.	☒ SI ☐ No
6.	El elemento de datos color de pelo_ está presente en los datos mDL.	☒ SI ☐ No
7.	El elemento de datos lugar de nacimiento_ está presente en los datos mDL.	☒ SI ☐ No
8.	El elemento de datos dirección de residencia_ está presente en los datos mDL.	☒ SI ☐ No
9.	El elemento de datos captura de imagen_ está presente en los datos mDL.	☒ SI ☐ No
10.	El elemento de datos edad en años_ está presente en los datos mDL.	☒ SI ☐ No
11.	El elemento de datos edad_año de nacimiento_ está presente en los datos mDL.	☒ SI ☐ No
12.	El elemento de datos edad_mayor de_NN está presente en los datos mDL En caso de seleccionar SI, favor dar los elementos de datos edad_mayor de_NN en los datos mDL con su correspondiente valor (VERDADERO/FALSO) durante la personalización	☒ SI ☐ No
	NN	Valor Retorno
	Edad_mayor de_15	Verdadero
	Edad_mayor de_18	Verdadero
	Edad_mayor de_21	Verdadero
	Edad_mayor de_60	Falso
	Edad_mayor de_65	Falso
	Edad_mayor de_68	Falso
13.	El elemento de datos jurisdicción_emisora_ está presente en los datos mDL.	☒ SI ☐ No
14.	El elemento de datos nacionalidad_ está presente en los datos mDL.	☒ SI ☐ No
15.	El elemento de datos ciudad_de residencia_ está presente en los datos mDL.	☒ SI ☐ No
16.	El elemento de datos estado_de residencia_ está presente en los datos mDL.	☒ SI ☐ No
17.	El elemento de datos código_postal_de residencia_ está presente en los datos mDL.	☒ SI ☐ No
18.	El elemento de datos país_de residencia_ está presente en los datos mDL.	☒ SI ☐ No
19.	El elemento de datos plantilla_biométrica_cara_ está presente en los datos mDL.	☐ SI ☒ No
20.	El elemento de datos plantilla_biométrica_voz_ está presente en los datos mDL.	☐ SI ☒ No
21.	El elemento de datos plantilla_biométrica_dedo_ está presente en los datos mDL.	☐ SI ☒ No
22.	El elemento de datos plantilla_biométrica_iris_ está presente en los datos mDL.	☐ SI ☒ No
23.	El elemento de datos plantilla_biométrica_retina_ está presente en los datos mDL.	☐ SI ☒ No
24.	El elemento de datos plantilla_biométrica_mano_geométrica está presente en los datos mDL.	☐ SI ☒ No
25.	El elemento de datos plantilla_biométrica_firma_ está presente en los datos mDL.	☐ SI ☒ No
26.	El elemento de datos plantilla_biométrica_pulsación de teclas_ está presente en los datos mDL.	☐ SI ☒ No
27.	El elemento de datos plantilla_biométrica_movimiento de labios_ está presente en los datos mDL.	☐ SI ☒ No
28.	El elemento de datos plantilla_biométrica_cara_térmica_ está presente en los datos mDL.	☐ SI ☒ No
29.	El elemento de datos plantilla_biométrica_mano_térmica_ está presente en los datos mDL.	☐ SI ☒ No
30.	El elemento de datos plantilla_biométrica_pasos_ está presente en los datos mDL.	☐ SI ☒ No
31.	El elemento de datos plantilla_biométrica_olor_corporal_ está presente en los datos mDL.	☐ SI ☒ No
32.	El elemento de datos plantilla_biométrica_adn_ está presente en los datos mDL.	☐ SI ☒ No
33.	El elemento de datos plantilla_biométrica_oído_ está presente en los datos mDL.	☐ SI ☒ No
34.	El elemento de datos plantilla_biométrica_geometría_dedo_ está presente en los datos mDL.	☐ SI ☒ No
35.	El elemento de datos plantilla_biométrica_geometría_palma manos_ está presente en los	☐ SI ☒ No

⁴ Nota: todos los elementos de datos de esta sección se encuentran en el espacio predeterminado de datos mDL ("org.iso.18013.5.1"). Las declaraciones ICS de esta sección deben completarse solo para documentos que tengan DocType = "org.iso.18013.5.1.mDL".

	datos mDL	
36.	El elemento de datos plantilla biométrica patrón venas está presente en los datos mDL	☐ Si ☒ No
37.	El elemento de datos plantilla biométrica huella pié está presente en los datos mDL	☐ Si ☒ No
38.	El elemento de datos apellido carácter nacional está presente en los datos mDL	☒ Si ☐ No
39.	El elemento de datos nombre carácter nacional está presente en los datos mDL	☒ Si ☐ No
40.	El elemento de datos marca usual firma está presente en los datos mDL	☒ Si ☐ No

A.1.3. Para Casos de Prueba de Tecnología

#	Declaraciones ICS para los casos de prueba de Tecnología	
41.	mDL admite interacción con el dispositivo usando NFC Static Handover	☒ Si ☐ No
42.	mDL admite interacción con el dispositivo usando NFC Negotiated Handover ⁵	☐ Si ☒ No
43.	mDL admite interacción con el dispositivo usando Código QR	☒ Si ☐ No
44.	mDL admite recuperación del dispositivo usando NFC	☒ Si ☐ No
45.	mDL admite APDU de longitud extendida para la recuperación del dispositivo usando NFC	☒ Si ☐ No
46.	mDL admite BLE versión 4.2 (o la que antecede) y Paquete de Datos LE de longitud extendida	☒ Si ☐ No
47.	mDL admite recuperación del dispositivo usando BLE modo cliente central	☒ Si ☐ No
48.	Si utiliza BLE en modo cliente central para la recuperación de dispositivos, verifique el valor de la característica Ident	☒ Si ☐ No
49.	mDL admite el perfil de transmisión L2CAP si actúa como cliente GATT para la recuperación del dispositivo usando BLE	☐ Si ☒ No
50.	mDL admite recuperación de dispositivos usando BLE en modo de servidor periférico	☒ Si ☐ No
51.	mDL admite el perfil de transmisión L2CAP si actúa como servidor GATT para la recuperación del dispositivo usando BLE	☐ Si ☒ No
52.	mDL admite recuperación del dispositivo usando Wi-Fi Aware	☐ Si ☒ No
53.	mDL admite el conjunto cifrado NCS-PK-2WDH-128 para Wi-Fi Aware ⁶	☐ Si ☒ No
54.	mDL admite la recuperación del servidor usando OIDC	☒ Si ☐ No
55.	mDL admite la recuperación del servidor usando WebAPI	☒ Si ☐ No
56.	mDL admite la transferencia de información de recuperación desde la estructura de interacción del dispositivo	☒ Si ☐ No
57.	mDL implementa un tiempo de espera entre el tiempo de envío de datos de interacción del dispositivo y establecimiento de la recepción del mensaje	☐ Si ☒ No
58.	En caso afirmativo, ¿cuántos segundos es el período de espera para la finalización de la sesión implementada por el mDL?	

A.1.4 Para Casos de Prueba de los Mecanismos de Seguridad

#	Declaraciones ICS para los casos de prueba de los Mecanismos de Seguridad	
59.	¿Cuáles curvas admite mDL para el establecimiento de sesiones? Marque todas las compatibles. ⁷	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
60.	mDL admite el intercambio de más de una solicitud y respuesta de mDOC para la recuperación del dispositivo con el lector mDOC en una	☐ Si ☒ No

⁵ Tenga en cuenta que la transferencia NFC Static Handover y NFC Negotiated Handover no se pueden admitir simultáneamente si un mDL admite ambas tecnologías

⁶ Solo se aplica en caso de que el mDOC admita Wi-Fi Aware para la recuperación del dispositivo y admita NFC Negotiated Handover para la interacción con el dispositivo

⁷ Si mDL admite varias curvas para el establecimiento de sesiones, entonces, a los efectos de la prueba, el propietario de mDL debe proporcionar una muestra separada para cada una de las curvas admitidas

	sola sesión.	
61.	Si es afirmativo, ¿cuántos segundos es el periodo de espera para la finalización de la sesión implementada por mDL?	
62.	¿Cuáles curvas admite la autoridad emisora mDL para la autenticación de los datos del emisor? Marque todas las compatibles ⁸	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
63.	El mDL admite la autenticación MAC de mDOC	☒ Si ☐ No
64.	Si afirmativo, ¿cuáles curvas admite el mDL para la autenticación MAC de mDOC? Marque todas las compatibles ⁹	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
65.	El mDL admite la autenticación ECDSA/EdDSA de mDOC	☒ Si ☐ No
66.	Si es así, ¿cuáles curvas utiliza el mDL para la autenticación ECDSA/EdDSA de mDOC? Marque todas las compatibles ¹⁰	☒ Curva P-256 ☐ Curva P-384 ☐ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
67.	El mDL admite la autenticación de lectores mDOC	☒ Si ☐ No
68.	Si afirmativo, ¿cuáles curvas admite el mDOC para la autenticación del lector mDOC? Marque todas las compatibles ¹¹	☒ Curva P-256 ☒ Curva P-384 ☒ Curva P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1

⁸ Si hay varios documentos en la mDL, la autoridad emisora puede, en teoría, utilizar una curva diferente para firmar la MSO de cada uno de ellos. Sin embargo, tenga en cuenta que UL espera que se utilice la misma curva para todos los documentos de la muestra dada. Para pruebas, el propietario del mDL debe proveer una muestra independiente para cada una de las curvas admitidas.

⁹ Si hay varios documentos en el mDL, el mDL puede, en teoría, utilizar una curva de autenticación MAC de mDOC diferente para cada uno de ellos. Sin embargo, tenga en cuenta que UL espera que se utilice la misma curva para todos los documentos de la muestra dada. Para pruebas, el propietario del mDL debe proveer una muestra independiente para cada una de las curvas admitidas.

¹⁰ Tenga en cuenta que para cada documento de un mDL, podría haber varios pares de SDeviceKey para la autenticación mDOC, cada uno en un MSO independiente. Por tanto, es teóricamente posible que un solo documento utilice la autenticación MAC y la autenticación ECDSA/EdDSA de forma alternada o utilice diferentes curvas para ECDSA/EdDSA de forma alternada. Sin embargo, tenga en cuenta que UL espera que se utilice de forma constante el mismo mecanismo de autenticación mDOC (MAC o ECDSA/EdDSA) para todos los documentos de una muestra determinada. Además, UL espera que se utilice la misma curva ECDSA/EdDSA para todos los documentos de una muestra determinada. Para realizar pruebas, el propietario del mDL debe proporcionar una muestra independiente para cada una de las curvas admitidas.

¹¹ UL asume que todas las muestras de mDL que se nos proporcionan admitirán todas las curvas de autenticación de lectores mDOC seleccionadas (siempre que se instalen los correctos certificados CA).



69.	Si es así, ¿para qué elementos de datos se requiere una autenticación exitosa del lector antes de que mDOC los libere? ¹²	<pre>{ "org.iso.18013.5.1.mDL": { "org.iso.18013.5.1": { "número_administrativo", "sexo", "peso", "color_ojos", "color_pelo", "lugar_nacimiento", "dirección_residencia", "fecha_captura_retrato", "edad_en_años", "edad_año_nacimiento", "edad_más_de_15", "edad_más_de_18", "edad_más_de_21", "edad_más_de_60", "edad_más_de_65", "edad_más_de_68", "jurisdicción_emisora", "nacionalidad", "ciudad_residencia", "estado_residencia", "código_postal_residencia", "país_residencia", "apellido_carácter_nacional", "nombre_carácter_nacional", "firma_marca_usual" } } }</pre>
70.	En caso afirmativo, mDOC admite la recuperación de la información de OCSP, si disponible, al verificar un certificado de autenticación del lector mDOC	☐ Si ☒ No

A.1.5 Para uso en los casos de Casos de Pruebas

#	Declaraciones ICS para Uso en los Casos de Casos de Pruebas	
71.	El mDL permite al titular de mDL rechazar el consentimiento para compartir el elemento de datos del retrato, si así lo solicita el lector	☐ Si ☒ No

EN FE DE LO CUAL, firmo y sello la presente **Certificación**, a pedimento de parte interesada, en Santo Domingo, Distrito Nacional, Capital de República Dominicana, a los doce (12) días del mes de febrero del año dos mil veinticinco (2025), habiéndola inscrito en el registro a mi cargo, bajo el No. 224/25.

Ana María Ferra
Ana María Ferra

¹² UL asume que si se admite la autenticación de lectores mDOC, hay por lo menos un elemento de datos que no se liberará si la autenticación de lectores mDOC no se realiza o falla.





Global Enterprise Technologies Corp
230 2nd Avenue, Waltham, Massachusetts, 02451, USA

15th November 2024

Subject: Confirmation of conformity of Android-based mDL - GET Mobile ID, v.5.1.23
with ISO/IEC 18013-5:2021

Dear Mr. Alexander,

This letter serves to confirm the conformity of the abovementioned mDL application ('the application') to ISO/IEC 18013-5:2021.

FIME tested v5.5.0 of this mDL application in December 2022 and found it to be compliant with this standard. 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. The number of the Test Report containing the full overview of executed test cases and all test results is UL_eID_GET Group_Android_002.

In August 2024, GET provided Fime with release notes describing the changes between the tested version 5.5.0 and version 5.1.23. After reviewing these release notes, FIME concluded there is no need for re-testing version 5.1.23, since the described changes are not likely to impact the conformity to ISO/IEC 18013-5.

As a reminder, the correct functioning of the application is dependent on several factors in its operational environment. GET Group is solely and fully responsible for the conformity of the application to all applicable standards, specifications, and requirements.

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

Yours sincerely,



FIME

David Bakker
Technical Lead



mDL implementation scope

System Under Test

Application name and version	mDL - GET Mobile ID, v.5.5.0
Operating System	Android
Application available through	Android Package File (APK) of the mDL Application was provided by the customer
Date of receipt of application	2022-10-26
Certification Type	Integrated Product Certification
Issuing Authority	Utah Driver License Division

Implementation Conformance Statement Summary

Device engagement technologies	QR code, NFC Static Handover
Device retrieval technologies	BLE in mdoc central client mode BLE in mdoc peripheral server mode NFC, WiFi-Aware ¹
Server retrieval technologies	WebAPI, OIDC
Security mechanisms for device retrieval	Session encryption, issuer data authentication, mdoc authentication, mdoc reader authentication

Test Environment

Standard	ISO/IEC 18013-5:2021
Test Case Specification	FIME mDL Test Case Specification
Test Suite	UL mDL Application Test Suite v1.1.11
mDL Test App	mdltestapp-1.1.4
Test device on which the mDL Test App is installed	Google Pixel 3a
OS version of the test device on which the mDL Test App is installed	Android 12

Test Devices and Platform

Device brand and type	Google Pixel 6	Samsung Galaxy S9
OS version	Android 13	Android 8

¹ Wi-Fi Aware was tested only on the Google Pixel 6 device running Android 13.

A.1 Implementation conformance statement

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

The ICS version used by GET Group is v1.5.

A.1.1 General information

mDL owner	
Application owner Name	GET Group
Address	230 2nd Avenue
City	Waltham
State	MA
Zip Code / Postal Code	02451
Country	USA
Contact Name	Alexander Kambanis
Contact Title	Managing Director
Contact Email Address	akambanis@getgroupna.com
Contact Phone Number	+1 (617) 901-1700

Issuing Authority General Information (Applicable for Integrated Product Certification Only)	
Issuing Authority Name	Utah Department of Public Safety, Driver License Division
Issuing Authority Address	Utah Department of Public Safety
City	Salt Lake City
State	Utah
Zip Code / Postal Code	84114-4501
Country	USA
Contact Name	Brittaney Akagi
Contact Title	IT / Quality Assurance Manager
Contact Email Address	bakagi@utah.gov

mDL Application General Information	
Certification Type	☐ Functional ² ☒ Integrated Product ³
Application name and version	GET Mobile ID, v.5.5.0
The minimum version of iOS supported	Android 8.0 (API level 26)
How many documents are present on the mDL under test?	1

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

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





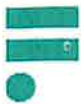
For each document, please specify the applicable DocType	org.iso.18013.5.1.mDL
For each document, please specify all data element namespaces used by the document	org.iso.18013.5.1, com.scytales.18013.5.1, org.aamva.us, org.iso.18013.5.1.aamva
For each namespace different from the mDL namespace ("org.iso.18013.5.1"), please specify the identifiers of all data elements present in the document	<pre>{ "org.iso.18013.5.1.mDL" : { "com.scytales.18013.5.1" : ["status", "vehicle_category", "vehicle_category_list", "full_address", "email", "mobile_number"], "org.aamva.us" : ["real_id"], "org.iso.18013.5.1.aamva" : ["DHS_compliance"] } }</pre>

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 ⁴	
1.	Data element administrative_number is present in the mDL data.	☒ YES ☐ NO
2.	Data element sex is present in the mDL data.	☒ YES ☐ NO
3.	Data element height is present in the mDL data.	☒ YES ☐ NO
4.	Data element weight is present in the mDL data.	☒ YES ☐ NO

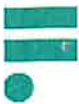
⁴ Note: all of the data elements in this section are in the default mDL data namespace ("org.iso.18013.5.1"). The ICS statements in this section have to be filled in only for documents having DocType = "org.iso.18013.5.1.mDL".



5.	Data element eye_color is present in the mDL data.	☒ YES ☐ NO
6.	Data element hair_color is present in the mDL data.	☒ YES ☐ NO
7.	Data element birth_place is present in the mDL data.	☒ YES ☐ NO
8.	Data element resident_address is present in the mDL data.	☒ YES ☐ NO
9.	Data element portrait_capture_date is present in the mDL data.	☒ YES ☐ NO
10.	Data element age_in_years is present in the mDL data.	☒ YES ☐ NO
11.	Data element age_birth_year is present in the mDL data.	☒ YES ☐ NO
12.	Data element age_over_NN is present in the mDL data. In case you select YES, please provision the following age_over_NN data elements in the mDL data with the corresponding values (TRUE / FALSE) during personalization.	☒ YES ☐ NO
	NN	Return Value
	age_over_15	TRUE
	age_over_18	TRUE
	age_over_21	TRUE
	age_over_60	FALSE
	age_over_65	FALSE
	age_over_68	FALSE
13.	Data element issuing_jurisdiction is present in the mDL data.	☒ YES ☐ NO
14.	Data element nationality is present in the mDL data.	☒ YES ☐ NO
15.	Data element resident_city is present in the mDL data.	☒ YES ☐ NO
16.	Data element resident_state is present in the mDL data.	☒ YES ☐ NO
17.	Data element resident_postal_code is present in the mDL data.	☒ YES ☐ NO
18.	Data element resident_country is present in the mDL data.	☒ YES ☐ NO
19.	Data element biometric_template_face is present in the mDL data.	☐ YES ☒ NO



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



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

A.1.3 For technology test cases

#	ICS statements for Technology test cases	
41.	mDL supports device engagement using NFC Static Handover	☒ YES ☐ NO
42.	mDL supports device engagement using NFC Negotiated Handover ⁵	☐ YES ☒ NO
43.	mDL supports device engagement using QR code	☒ YES ☐ NO
44.	mDL supports device retrieval using NFC	☒ YES ☐ NO
45.	mDL supports extended-length APDUs for device retrieval using NFC	☒ YES ☐ NO
46.	mDL supports BLE version 4.2 (or above) and LE Data Packet Length Extension	☒ YES ☐ NO
47.	mDL supports device retrieval using BLE in mdoc central client mode	☒ YES ☐ NO
48.	If BLE in mdoc central client mode is used for device retrieval, mdoc verifies the value of the Ident characteristic	☒ YES ☐ NO
49.	mDL supports the L2CAP transmission profile if it is acting as the GATT client for device retrieval using BLE	☐ YES ☒ NO
50.	mDL supports device retrieval using BLE in mdoc peripheral server mode	☒ YES ☐ NO
51.	mDL supports the L2CAP transmission profile if it is acting as the GATT server for device retrieval using BLE	☐ YES ☒ NO
52.	mDL supports device retrieval using Wi-Fi Aware	☐ YES ☒ NO
53.	mDL supports the NCS-PK-2WDH-128 cipher suite for Wi-Fi Aware ⁶	☐ YES ☒ NO

⁵ Note that NFC Static Handover and NFC Negotiated Handover cannot be supported simultaneously if an mDL supports both technologies

⁶ Only applicable in case the mdoc supports Wi-Fi Aware for device retrieval and supports NFC Negotiated Handover for device engagement.



54.	mDL supports server retrieval using OIDC	☒ YES ☐ NO
55.	mDL supports server retrieval using WebAPI	☒ YES ☐ NO
56.	mDL supports transferring server retrieval information in the device engagement structure	☒ YES ☐ NO
57.	mDL implements a time-out for the time between sending device engagement data and receiving the session establishment message	☐ YES ☒ NO
58.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	

A.1.4 For security mechanism test cases

ICS statements for Security Mechanisms test cases		
59.	Which curves does the mDL support for session establishment? Tick all that are supported. ⁷	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ X25519 ☐ X448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
60.	mDL supports exchanging more than one device retrieval mdoc request and response with the mdoc reader in a single session.	☐ YES ☒ NO
61.	If yes, how many seconds is the time-out period for session termination implemented by the mDL?	
62.	Which curves does the mDL issuing authority support for issuer data authentication? Tick all that are supported. ⁸	☒ Curve P-256 ☐ Curve P-384 ☐ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1

⁷ 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.

⁸ If multiple documents are present on the mDL, the issuing authority can in theory use a different curve for signing the MSO on each of them. However, please note that UL expects the same curve to be used



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

for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

⁹ If multiple documents are present on the mDL, the mDL can, in theory, use a different mdoc MAC authentication curve for each of them. However, please note that UL expects the same curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.

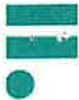
¹⁰ Note that for each document on an mDL, there could potentially be multiple SDeviceKey pairs for mdoc authentication, each in a separate MSO. It is therefore theoretically possible that a single document uses MAC authentication and ECDSA/EdDSA authentication alternately or uses different curves for ECDSA/EdDSA alternately. However, please note that UL expects that the same mdoc authentication mechanism (either MAC or ECDSA/EdDSA) is consistently used for all documents on a given sample. Moreover, UL expects that the same ECDSA/EdDSA curve is used for all documents on a given sample. For testing, the mDL owner should provide a separate sample for each of the curves supported.



68.	If yes, which curves does the mdoc support for mdoc reader authentication? Tick all that are supported ¹¹ .	☒ Curve P-256 ☒ Curve P-384 ☒ Curve P-521 ☐ Ed25519 ☐ Ed448 ☐ brainpoolP256r1 ☐ brainpoolP320r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1
69.	If yes, for which data elements is successful reader authentication required before the mdoc will release them ¹²	<pre>{ "org.iso.18013.5.1.mDL" : { "org.iso.18013.5.1" : ["administrative_number", "sex", "weight", "eye_colour", "hair_colour", "birth_place", "resident_address", "portrait_capture_date", "age_in_years", "age_birth_year", "age_over_15", "age_over_18", "age_over_21", "age_over_60", "age_over_65", "age_over_68", "issuing_jurisdiction", "nationality", "resident_city", "resident_state", "resident_postal_code", "resident_country", "family_name_national_character", "given_name_national_character", "signature_usual_mark] } }</pre>
70.	If yes, mdoc supports retrieving OCSP information, if available, when verifying an mdoc reader authentication certificate.	☐ YES ☒ NO

¹¹ UL assumes that all mDL samples provided to us will support all of the mdoc reader authentication curves selected (provided that the correct CA certificates are installed).

¹² UL assumes that if mdoc reader authentication is supported, there is at least one data element that will not be released if mdoc reader authentication is not performed or fails.



A.1.5 For use case test cases

#	ICS statements for Use Case test cases	
71.	The mDL allows the mDL holder to refuse consent for sharing the portrait data element if requested by the reader	☐ YES ☒ NO

