EMDOC
CONSORCIO

Informaciones técnicas relacionadas a la prueba de concepto (POC)

Consorcio EMDOC

Proceso: Referencia JCE-LPI-2024-0001

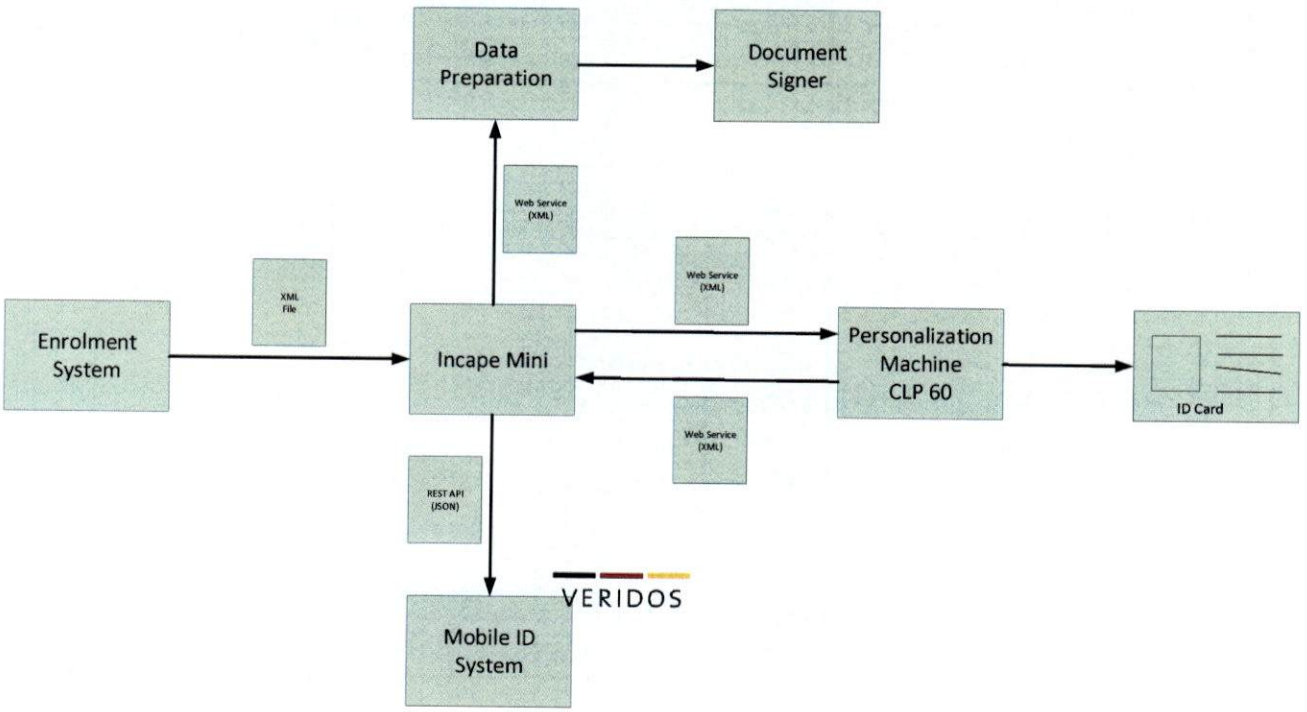
Índice

1 Resumen de la solución:

El objetivo de esta solución de prueba de concepto es la personalización de tarjetas (ópticamente y con chip) basada en el registro en vivo y la emisión y verificación correcta de una identificación móvil.

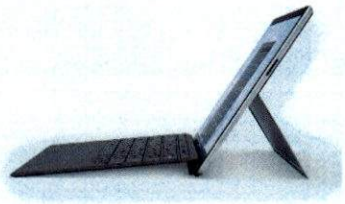
La solución aplica un enfoque de emisión instantánea, que comienza con una inscripción en vivo de los datos biográficos, demográficos y biométricos del solicitante (es decir, imagen facial, huellas dactilares -hasta 10- y firma). Después de cada inscripción, los datos necesarios para la personalización se preparaban y firmaban digitalmente en el backend y se enviaba un trabajo de una sola tarjeta a la máquina de personalización. La máquina de personalización cargaba el trabajo en su software de gestión de la personalización y se encargaba de los procesos de personalización óptica (láser) y eléctrica (chip). Una vez que la tarjeta se personalizaba correctamente, los datos se cargaban automáticamente en el sistema de identificación móvil y se podía proceder a la emisión de la identificación móvil, una vez iniciada por el propietario de la tarjeta de identificación.

El siguiente diagrama muestra los componentes implicados en el POC y ofrece una visión general del flujo de datos, hasta la carga en el sistema Mobile ID.



1.1 Descripción de los componentes de la solución

1.1.1 Sistema de enrolamiento de ciudadanos



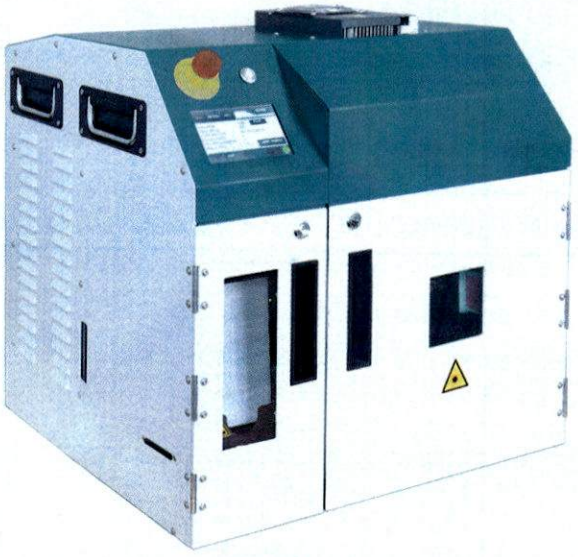
Cliente	Componente de software	Hardware
PC/Tableta de enrolamiento	**MB GetID** con los siguientes módulos: • Servicio de registro 5.0.1 • Servicio Gateway 5.0.6 • Adaptador de interfaz 1.0.0 • UI GetID Tablet 1.0.1 • Procesador de datos biométricos 5.0.4 • MB Device Engine 5.0.14 • Navegador	- Tableta MS Surface Pro 9 • CPU - Intel i5-1245U, 10 núcleos - 2,50Ghz • RAM - 16GB DDR4 • SSD - 256 GB - Escáner de huellas dactilares • Suprema RealScan-S60

1.1.2 Gestión de la personalización

Componente del sistema	Versión	Descripción
PC de Gestión del sistema personalización	MS Windows 10	• CPU - Intel i7-11850HX, 8 núcleos - 2,50Ghz • RAM - 32GB DDR4 • SSD - 512 GB
MB Incape Mini	13.4.1	Servicio de envío de trabajos a máquinas de personalización.
MB Preparación de datos	Webapp 6.3.0/ Configuración 1.0.2	Componente para preparar todos los datos visuales, MRZ, datos de chip para obtener resultados de impresión óptimos.
MB TRUST ICAO PKI - DocumentSigner	6.0.0	Document Signer (DS) firma digitalmente todos los datos almacenados en un documento de viaje electrónico

Componente del sistema	Versión	Descripción
MB Gestión de usuarios	Servidor de Administración 5.0.4/ Servidor de acceso 5.0.3	Sistema centralizado para asegurar la solución

1.1.3 Máquina de personalización (Impresora de Grabado Láser)



Componente del sistema	Versión	Descripción
CLP 60 - Sistema de personalización de tarjetas	Norma CLP 60	Dispositivo de sobremesa de personalización de tarjetas para codificación de chips y grabado por láser
PC integrado con sistema operativo	MS Windows 10 LTSC 2021	Mini-ITX-PC • CPU - Intel Core i3-3120M, 2,50Ghz • RAM - 4 GB DDR3 • SSD - 120 GB
MCES		2.28.320
Base de datos	MS SQL	SQL Server 2012
Codificador de chip	Versión estándar	MB 1301 Firmware: #2.48
Codificación DLL		2.28.1.2
Láse	Versión estándar	MB, tipo LES 20 FP • Yterbium-Láser de fibra de escala de grises, 1064 nm • refrigerado por aire, 20 W • 256 valores reales de gris • Resolución 300-1.200 ppp • Unidad giratoria CL/MLF
Sistema de visión	Versión estándar	Cámara uEye UI-1460-C-GE Iluminación MB 1439 WH-IR

2 Datos del ciudadano a ser capturados

2.1 Datos demográficos

Nombre del campo	Tipo	Obligatorio	Más información
Nombre Datos			
Nombre	Texto (60)	Sí	Ninguno
Segundo nombre	Texto (60)	No	Ninguno
Primer apellido	Texto (60)	Sí	Ninguno
Segundo apellido	Texto (60)	No	Ninguno
Nacionalidad	Texto	Sí	Lista desplegable según ICAO 9303
Número nacional de identidad	Texto (13)	Sí	Formato XXX-XXXXXXX-X (X es sólo números)
Género	Texto (1)	Sí	Lista desplegable: Masculino, Femenino
Estado civil	Texto	Sí	Lista desplegable: - si el sexo es Masculino: Soltero, Casado, Separado, Divorciado - si el género es Femenino: Soltera, Casada, Separada, Divorciada
Fecha de nacimiento	Fecha (MM/DD/AAAA)	Sí	Ninguno
Lugar de nacimiento			
País	Texto	Sí	Lista desplegable según ICAO 9303
Ciudad	Texto (60)	Sí	Ninguno
Número de partida de nacimiento	Texto (60)	Sí	Ninguno
Domicilio			
Dirección Línea 1	Texto (60)	Sí	Ninguno
Dirección Línea 2	Texto (60)	No	Ninguno
Sector	Texto (60)	Sí	Ninguno
Municipio	Texto (60)	Sí	Ninguno
Grupo sanguíneo	Texto (3)	Sí	Lista desplegable: A+, A-, B+, B-, O+, O-, AB+, AB-
Profesión y oficio	Texto (60)	Sí	Ninguno

Los datos de texto, que no se basan en listas desplegables, permitirán los siguientes caracteres:

- Todas las letras estándar ("a" a "z", "A" a "Z")
- Todos los dígitos ("0" a "9"; no para datos de nombres)
- Guión ("-", Unicode 0x002D)
- Apóstrofe ("'", Unicode 0x0027)
- En blanco (" ", Unicode 0x00A0)

- Caracteres especiales como se indican a continuación:

No	Char.	Descripción	Unicode
01	Á	A mayúscula con acento agudo	0x00C1
02	É	E mayúscula con acento agudo	0x00C9
03	Í	I mayúscula con acento agudo	0x00CD
04	Ñ	N mayúscula con tilde	Ox00D1
05	Ó	O mayúscula con acento agudo	0x00D3
06	Ü	U mayúscula con diéresis	0x00DC
07	Ú	U mayúscula con acento agudo	0x00DA
08	á	A minúscula con acento agudo	0x00E1
09	é	E minúscula con acento agudo	0x00E9
10	í	I minúscula con acento agudo	0x00ED
11	ñ	N minúscula con tilde	0x00F1
12	ó	O minúscula con acento agudo	0x00F3
13	ü	U minúscula con diéresis	0x00FC
14	ú	U minúscula con acento agudo	0x00FA

2.2 Datos biométricos

Se capturarán los siguientes datos biométricos:

- Imagen facial
- Huellas dactilares (hasta 10)
- Firma manuscrita del ciudadano

3 Preparación de datos

La preparación de los datos (proceso de un solo paso, sin paso adicional de preparación de datos durante la personalización) generó los siguientes datos:

- Número de documento en el formato "Vxxxxxxx", donde xxxxxxxx es un número consecutivo de 8 dígitos
- Fecha de expedición: fecha actual
- Fecha de caducidad: 5 años después de la fecha de expedición
  Estado de expedición: Utopía (UTO)
- Los datos de texto para el VIZ se acortarán en función del espacio disponible (los datos se cortan simplemente si son demasiado largos)
- Imagen facial principal
- Imagen facial para MLI
- Imagen facial para ventana transparente
- Código de barras para la identificación de documentos (Código 128)
- Código de barras para el número de identificación (Código 128)
- Código QR (contendrá el número de documento, la fecha de nacimiento y la fecha de caducidad, separadas por punto y coma)
- MRZ Línea 1 a 3 (sin datos opcionales)
- Datos del chip (véase el capítulo 5.4)
- La nacionalidad como texto

4 Personalización

En este capítulo se describen los distintos pasos de personalización dentro de la máquina de personalización CLP 60.

4.1 Tarjetas en blanco

Las tarjetas en blanco no tienen leyendas, pero están pre personalizadas con un número de cuerpo de tarjeta.

4.2 Lector de entrada

El lector de entrada leyó el número del cuerpo de la tarjeta, que fue devuelto por el Sistema de inventario de tarjetas (MCES en la POC) en el archivo de informe.

4.3 Personalización óptica

Las siguientes imágenes muestran el resultado necesario de la personalización con láser óptico.

Nota: La tarjeta personalizada real obtenida en el centro de operaciones quedó en poder del equipo de evaluación de la JCE.

Encontrará información detallada (por ejemplo, posiciones, fuentes, tamaños) en la especificación de personalización óptica.

Los siguientes datos eran estáticos, configurados en la disposición del láser y no fueron proporcionados por la inscripción / preparación de datos:

- Colegio Electoral (Código y 3 líneas de localización)
- Firma y nombre del presidente de la Junta Central Electoral

Las previsualizaciones de abajo muestran las características de seguridad implementadas para la Prueba de Concepto.

4.3.1 Grabado láser táctil (impresión en relieve):

Estructura lenticular (CLI)

4.3.2 Ventana transparente

Parte delantera

Parte trasera

4.4 Personalización de chips

Para el POC se personalizó un Applet de la OACI con los siguientes grupos de datos:

- DG 1
- DG 2
- DG 14
- SOD

El applet personalizado de la OACI sólo admite el protocolo PACE (ni BAC ni EAC), incluida la autenticación por chip.

4.5 Lector de salida

El lector de salida verificó los siguientes datos:

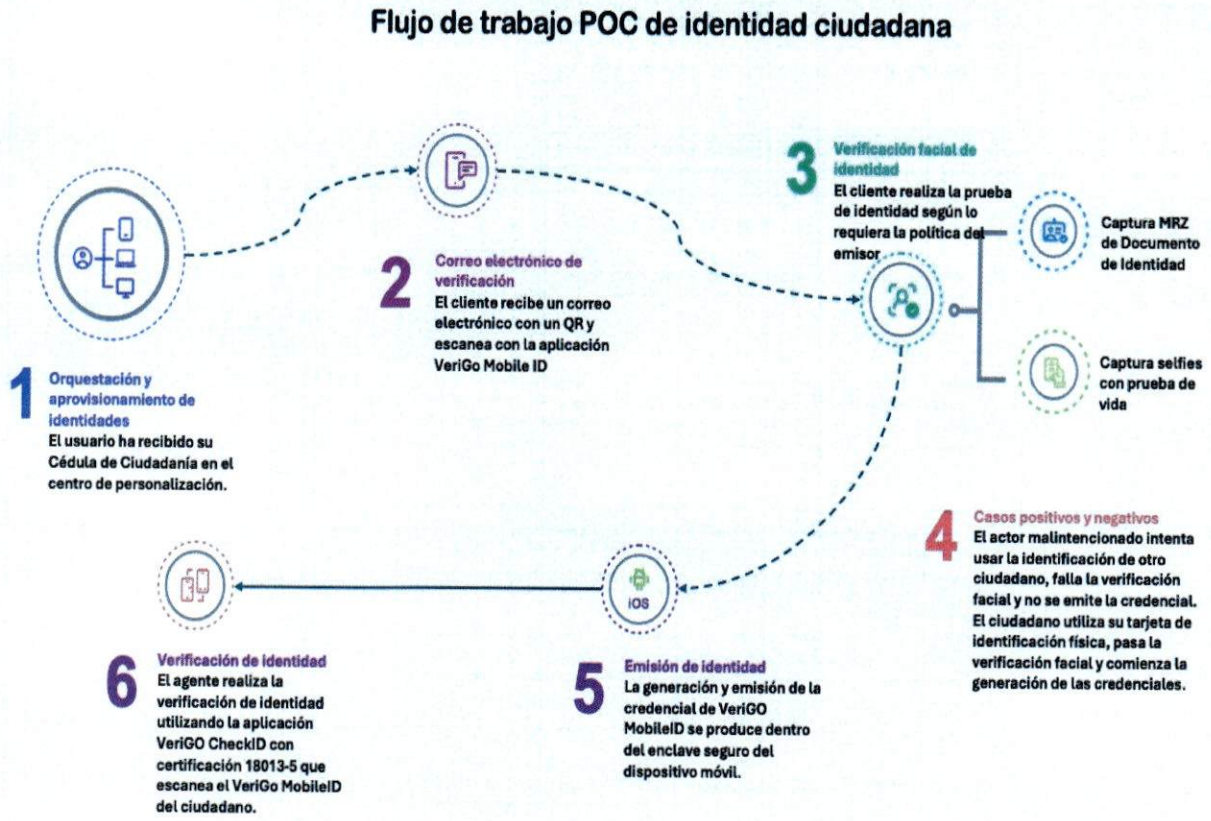
- Número de identificación
- Fecha de expiración

5 Solución de identificación móvil

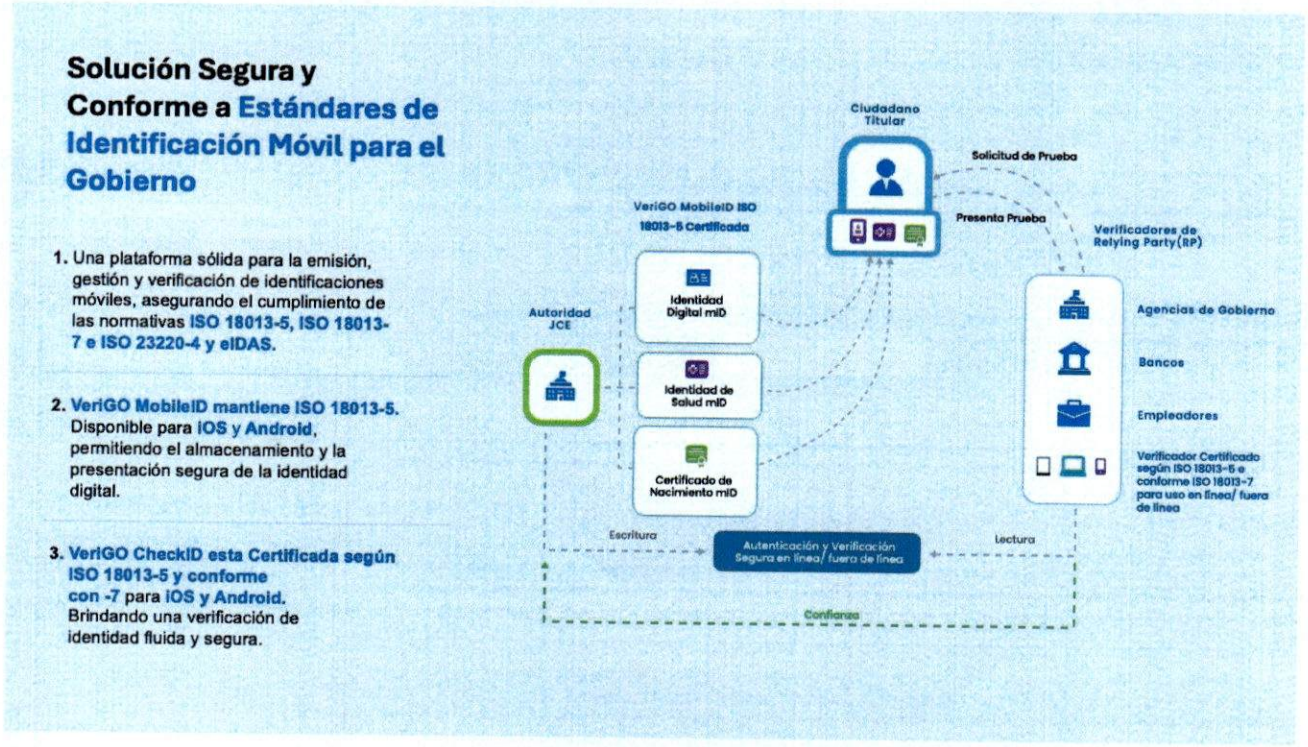
5.1 Resumen

En esta fase del POC, validaremos las capacidades de las aplicaciones 18013-5 VeriGO MobileID y 18013-5 CheckID certificadas por FIME (anteriormente UL) mediante casos de prueba positivos y negativos para la emisión y verificación. Los escenarios de prueba simularán a un ciudadano utilizando la aplicación VeriGO Mobile en iOS, con la verificación realizada a través de la versión Android de la aplicación VeriGO CheckID.

5.2 Flujo de trabajo de identificación móvil



5.3 Diagrama de identificación móvil



5.4 Dispositivos Smartphone utilizados en la demostración:

1. Dispositivo iOS: iPhone 15 - iOS 18.3.1
2. Dispositivos Android: Google Pixel 9 XL y Google Pixel 8 - Sistema Operativo Android 15
3. Utilizado para recibir correo electrónico: Dispositivo Android: Google Pixel 6a Sistema Operativo Android 15

5.5 Versiones de la aplicación:

1. Monedero (Wallet) de identificación utilizado para la Cedula Digital - iOS VeriGO MobileID v1.0.22
2. Verificador utilizado para la verificación de la Cedula Digital - Android VeriGO CheckID v1.0.7

5.6 Escenarios a ser considerados:

- **Escenario 1:** Un actor malicioso intenta emitir un documento de identidad digital utilizando la tarjeta de otro ciudadano.
- **Escenario 2:** El usuario legítimo emite correctamente una Tarjeta Digital (MobileID).

- **Escenario 3:** El titular de la tarjeta debe verificar su Tarjeta Digital (MobileID) con la aplicación VeriGO CheckID, nuestra aplicación oficial de verificación

- **Escenario 4:** Aplicación de verificación móvil (mediante QR seguro generado desde la aplicación), mostrando la funcionalidad de compartir todos los datos o compartir un grupo de datos específicos seleccionados por el ciudadano.

La aplicación (App) se mostrará en la pantalla de inicio, con una persona actuando como propietario y otra como verificador. El estudio garantizará escenarios tanto exitosos como fallidos para completar la POC.

5.6.1 PRUEBA nº 1 - Caso de Prueba Negativo

Escenario 1: Un actor malicioso intenta emitir un documento de identidad digital utilizando la tarjeta de otro ciudadano.

Pasos:

1. Asegúrese de que la aplicación VeriGO MobileID está instalada y en la pantalla de inicio del smartphone.
2. Abra la aplicación VeriGO MobileID. La pantalla inicial mostrará un escáner de código QR.
3. Escanee el código QR proporcionado en el correo electrónico emitido por Veridos y continúe con el escenario.
4. Al actor malicioso se le proporcionará una tarjeta de usuario. Esta prueba pretende simular un caso de fallo, impidiendo la emisión no autorizada de una identificación móvil.
5. El dispositivo se conectará a través de la API al inquilino, iniciando el flujo de trabajo preconfigurado.
6. La siguiente pantalla pedirá al usuario que escanee la MRZ que figura en el reverso de la tarjeta. El sistema indicará que el posicionamiento se ha realizado correctamente poniendo en verde la casilla de alineación.
7. Una vez leído correctamente el código MRZ, comienza el proceso de verificación facial.
    - **Pasos de la verificación facial:** Sonría, se captura la foto y parpadeo(aleatorio) se basan en el reconocimiento facial con detección de vida es un método de autenticación biométrica que no sólo identifica o verifica a una persona basándose en los rasgos faciales, sino que también garantiza que la cara presentada es un ser humano vivo y no un intento de suplantación (por ejemplo, foto, vídeo, máscara) de conformidad con la norma ISO/IEC 30107-3.
    - La resistencia del sistema a los ataques de suplantación o presentación se mide por su tasa de coincidencia de presentación de ataques de impostores (IAPMR). Un IAPMR más bajo indica una mayor resistencia a los ataques. Por ejemplo, un IAPMR de ≤ 1% significa que el sistema resiste con éxito el 99% de los intentos de suplantación en las condiciones de prueba especificadas.
8. La generación de credenciales debería fallar en este caso, impidiendo la emisión no autorizada.

5.6.2 PRUEBA nº 2 - Caso de prueba positivo

Escenario 2: El usuario legítimo emite con éxito un VeriGO MobileID.

Pasos:

1. El ciudadano recibe una tarjeta que registra su rostro en la base de datos.
2. Abra la aplicación Titular, que mostrará un escáner de códigos QR.
3. Escanee el código QR proporcionado. El dispositivo se vinculará a través de la API y comenzará el flujo de trabajo preconfigurado.
4. La siguiente pantalla pedirá al usuario que escanee la MRZ del reverso de la tarjeta. El sistema indicará que el posicionamiento se ha realizado correctamente poniéndose en verde.
5. Una vez leído correctamente el código MRZ, comienza el proceso de verificación facial.
    - Pasos de la verificación facial: Pasos de Verificación Facial: Sonría, foto capturada y parpadeo(aleatorio) se basan en el reconocimiento facial con detección de vida es un método de autenticación biométrica que no sólo identifica o verifica a una persona basándose en los rasgos faciales, sino que también garantiza que el rostro presentado es un ser humano vivo y no un intento de suplantación (por ejemplo, foto, vídeo, máscara) de conformidad con la norma ISO/IEC 30107-3.
    - La resistencia del sistema a los ataques de suplantación de identidad o de presentación se mide por su tasa de coincidencia de ataques de presentación de impostores (IAPMR). Un IAPMR más bajo indica una mayor resistencia a los ataques. Por ejemplo, un IAPMR de ≤ 1% significa que el sistema resiste con éxito el 99% de los intentos de suplantación en las condiciones de prueba especificadas.
6. Una vez completada la verificación, la credencial se generará dentro del VeriGO MobileID Waller, el dispositivo está ahora preparado para la etapa de verificación.

5.6.3 Fase de Verificación (Escenarios 3 y 4)

1. El titular de la tarjeta debe verificar su VeriGO MobileID con la aplicación VeriGO CheckID.
2. Abra el monedero (Wallet) MobileID utilizando la opción FaceID.
3. A continuación, el ciudadano encontrará el QR de escaneado en su monedero móvil para presentar la credencial a un agente.
4. El agente escanea el código QR con su aplicación VeriGO CheckID y se envía una solicitud al ciudadano.
5. El usuario tiene la opción de compartir atributos de forma selectiva y autoriza la solicitud.
6. El Agente recibe la respuesta firmada digitalmente que muestra el ID de foto del usuario y los atributos compartidos.
7. Escenario de verificación completado.

CONSORCIO EMDOC Santo Domingo, R.D.

5.7 **Conclusión**

Esta demostración POC garantiza la validación tanto de los casos de prueba positivos como de los negativos, confirmando la capacidad de la aplicación para emitir y verificar correctamente las credenciales digitales e impidiendo al mismo tiempo el acceso no autorizado.