ÍTEM IV - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL

4.1 INTRODUCCIÓN - GET MOBILE ID

La solución de identidad digital GET Mobile ID proporciona una identidad de alta seguridad en el dispositivo móvil de un usuario, que representa una alternativa conveniente, segura e instantánea a los documentos de identificación físicos tradicionales, y utiliza formidables algoritmos de cifrado de datos y medidas de seguridad de comunicación para reducir el robo de identidad y mejorar la privacidad de los ciudadanos.

4.1.1 GET MOBILE ID

Los ciudadanos quieren que sus documentos de identificación sean móviles y esperan poder administrar sus datos de identidad mejor que con las tarjetas de identificación físicas. GET Mobile ID brinda control de identificación por parte del usuario y permite una verificación de edad y una comprobación de identidad rápida y segura en todo tipo de negocios.

GET Mobile ID es el único producto en el mercado compatible con Android e iOS. Los gobiernos pueden emitir cualquier documento de identificación en GET Mobile ID. También permite que las organizaciones de todos los sectores (educación, empresa, comercio minorista y finanzas, así como instituciones públicas) acepten identificaciones digitales de alta seguridad. La autenticación es instantánea, las identidades son seguras, las interacciones están estandarizadas. Es la base para una amplia gama de servicios de identidad.

- La aplicación Direct to Consumer permite el control ciudadano del mID
- Tu identificación oficial en tu teléfono
- Totalmente compatible con ISO 18013-5
- Cambia cómo se protege la identidad
- No se puede falsificar

4.1.2 GET MOBILE ADMINISTRATOR

GET Mobile Administrator permite a los emisores de tarjetas de identificación del gobierno, hacer el cambio a lo digital de forma rápida y segura. Los gobiernos con visión de futuro podrán digitalizar sus documentos de identidad y dar a los ciudadanos el control de sus propios datos de identidad. GET Mobile ID cumple con la norma ISO/IEC 18013-5 de cinco estrellas con todos los canales de comunicación y modos de interacción estandarizados, dando como resultado la mejor experiencia de usuario y aceptación en la mayor cantidad de ubicaciones y casos de uso.

- Conectividad simple al sistema del JCE.
- Diseñado para Alta Disponibilidad.
- Conecta a los emisores para emitir identidades digitales en teléfonos móviles.
- Habilita todos los modos de interacción ISO 18013-5 en línea y fuera de línea
- Mantener actualizadas las identidades digitales
- Administrar el ciclo de vida de la identificación digital móvil

4.2 GET MOBILE ID – COMPONENTES

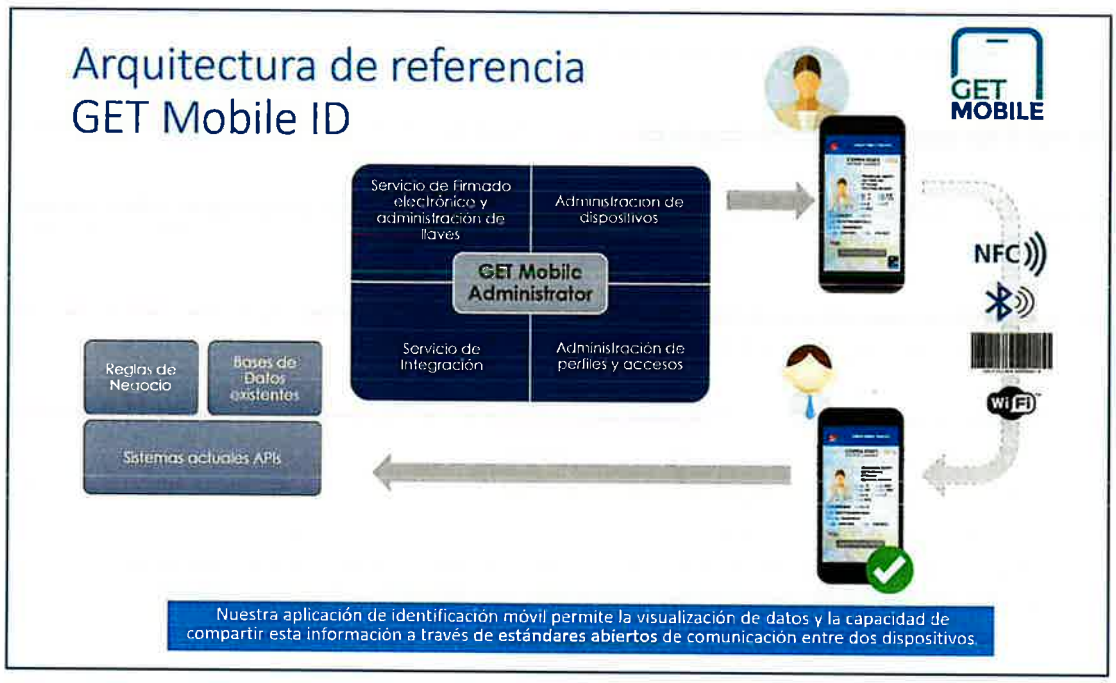
4.2.1 GET MOBILE ADMINISTRATOR

El módulo GET Mobile Administrator es fundamental para el concepto de producto mID, puesto que proporciona a la autoridad expedidora los siguientes servicios y funciones:

- Conectividad sencilla con el sistema de Identidad y Emisión del JCE.
- Diseñado para alta disponibilidad al 99,99% cuando se aloja en plataformas en nube o centros de datos redundantes y distantes.
- Conecta a los Emisores (el JCE) para que puedan emitir documentos de identidad firmados ISO 18013-5 en Teléfonos Móviles para sus ciudadanos.
- Incluye la más alta seguridad a nivel de pasaportes para la firma de datos mID a partir de su estructura de claves o de claves generadas
- Valida a los ciudadanos para garantizar que sólo reciben su documento de identidad.
- Permite solicitudes de verificadores compatibles con ISO 18013-5 en línea (WebAPI u OIDC).
- Mantiene los mID actualizados con los cambios de datos del Sistema del Emisor.

Los servicios prestados por GET Mobile Administrator son:

- Servicio de firma y gestión de claves: firma de forma segura los mID en nombre del emisor para transmitirlos a los dispositivos de los ciudadanos. Mediante la integración con la solución de PKI propuesta para el proyecto, se realizan los procesos de encripción sugeridos por la norma ISO 18013-5.
- Personalización y gestión de dispositivos: portal del consumidor para gestionar dispositivos, incluidos teléfonos perdidos, nuevos o actualizados.
- Fácil integración con sistemas de registro: conexiones API seguras con sistemas de registro que mantienen los datos actualizados.
- Gestión de Identidad y Acceso - Inicio de sesión y registro para verificadores que necesitan acceso a servicios ISO en línea.
- Caché mID – Puede mantener los datos mID durante un tiempo predeterminado para aligerar las solicitudes de los verificadores en la base de datos SOR.



4.2.1.1 OPCIONES DE INTEGRACIÓN:

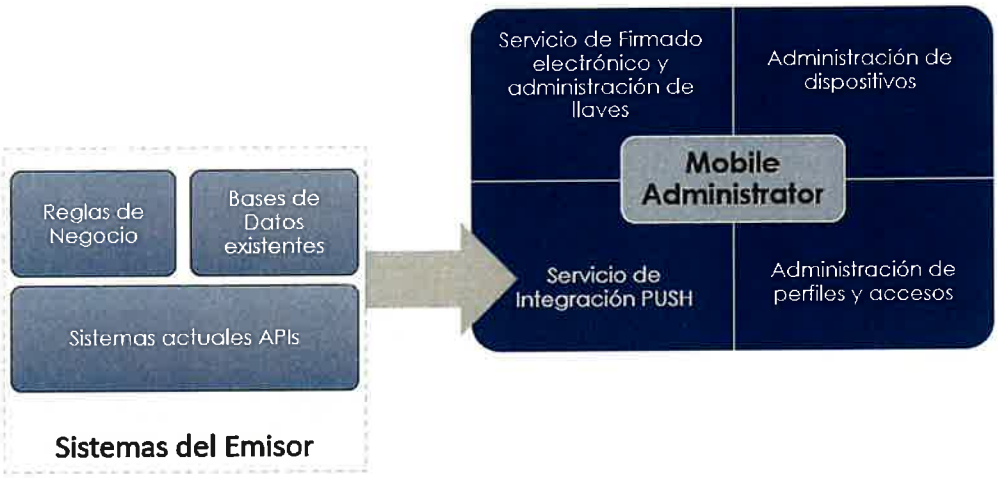
GET Mobile Administrator provee diferentes métodos de integración, buscando que la integración con el sistema de emisión del Emisor se pueda realizar de la forma más eficiente, y de esa manera, permitir un escalamiento progresivo en el desarrollo de casos de uso:

- **Modelo sin integración:** El modelo sin integración se basa únicamente en el aprovisionamiento diligenciado y aprobado por el administrador, se pueden aprobar nuevas solicitudes para Mobile ID sin una integración con la base de datos. El Administrador es responsable de revisar las solicitudes de mID, corregir cualquier error de datos, verificar la identidad y la confianza del solicitante y aprobar el mID que se proporcionará. Los datos mID están autocontenidos en la caché mID y el sistema se ejecuta basándose únicamente en esos datos.

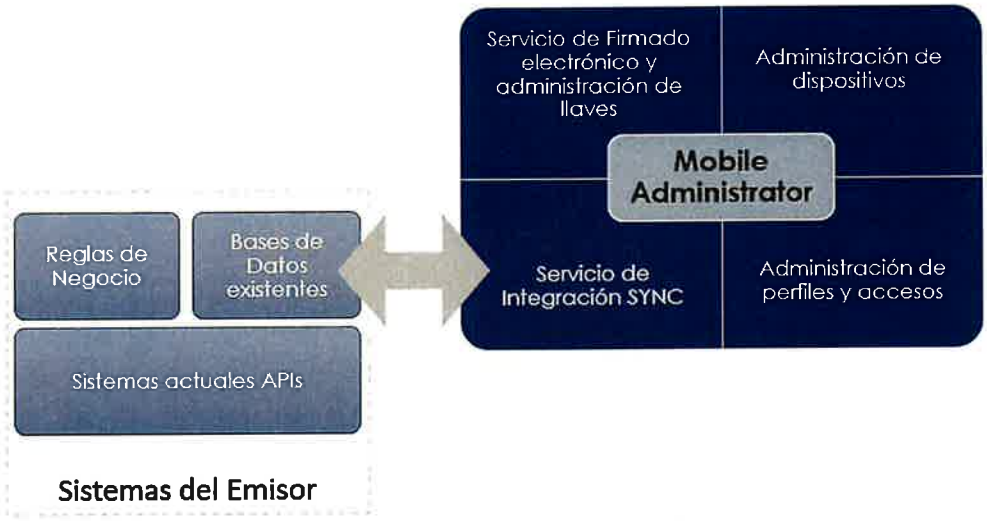
- **Modelo Push:** En el modelo Push, el sistema del emisor, como parte de su lógica empresarial, determina los momentos adecuados para llamar a GET Mobile Administrator con a través del API, usando un método de Creación de Licencia según los documentos de swagger para su instancia del software GET Mobile Administrator.

- **Los documentos Swagger están disponibles al navegar a la URL de la instancia de la página GET Mobile Administrator Services del Emisor**. Este modelo Push brinda el máximo control al entorno del sistema del emisor a expensas del tiempo de programación para la integración (el uso de la API es sencillo, rápido y fácil de usar según un enfoque tecnológico popular; el esfuerzo de programación puede variar dependiendo de la integración necesaria con los sistemas existentes).

El JCE puede crear sus propios informes a partir del software cuando utiliza este modelo porque tiene pleno conocimiento de qué mID están activos.

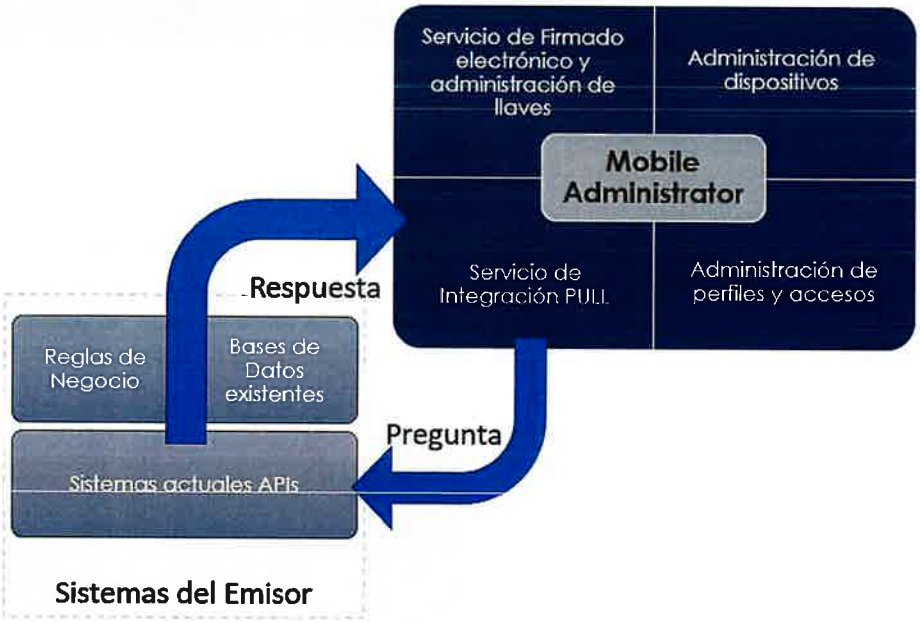


- **Modelo SYNC:** Para el modelo de sincronización, es posible realizar una conexión ODBC o similar entre el sistema del emisor y GET Mobile Administrator, cache que sincroniza el último registro del ciudadano en su registro en caché mID. La rutina de sincronización se puede configurar para sincronizar solo registros SOR estatales aprobados para mID, o para sincronizar todos los registros.



- **Modelo Pull:** En el modelo Pull, el administrador de GET Mobile se puede configurar para llamar a una API del sistema del emisor que busca registros actuales pendientes de emisión. La caché mID retiene registros de identidad para que el número de llamadas al sistema del emisor sea limitado.

La caché mID también se puede configurar para que no retenga datos. Si el sistema del emisor puede manejar los altos volúmenes de transacciones de los verificadores en el momento de uso, y existen requisitos contra el almacenamiento en caché de los registros más recientes detrás de la API en línea ISO (consulte la sección Medidas de seguridad para la API en línea a continuación), se puede configurar GET Mobile Administrator para llamar una API del sistema del Emisor que busca registros actuales. La carga completa de tráfico mID en el momento de uso (consulte la sección Tiempo de verificación (uso de mID) a continuación) alcanzará el SOR del emisor en esta configuración. (Cuando se hace referencia a SOR (Sistemas del Emisor), también puede ser un espejo local sincronizado de SOR).



4.2.1.2OPCIONES DE FIRMADO DIGITAL

La implementación de una identidad digital móvil ISO 18013-5 requiere llaves privadas del emisor que firmen los datos mID antes de que se aprovisionen en los dispositivos móviles. Estas llaves privadas pueden generarse a partir de la CA estatal. La CA no tiene que ser pública porque no existe una verificación de la cadena de certificados. Si se utiliza una CA estatal, se deben planificar ceremonias de certificación segura en el proyecto para obtener la clave privada en el servicio de firma o HSM. El Certificado Público IACA puede distribuirse por separado de la jurisdicción o colocarse en una "Lista Maestra" (también conocida como VICAL) con otros certificados confiables y ser distribuido por cualquier entidad. Los verificadores son responsables de garantizar que obtengan Listas Maestras confiables.

4.2.1.3 MODELO DE DATOS Y CODIFICACIÓN.

JSON Identity Suite es el modelo de objetos sobre el que se construye Open ID Connect. Sus estructuras de datos JSON Web Token (JWT) están definidas en https://tools.ietf.org/html/draft-ietf-oauth-json-web-token-19 especificaciones IETF, con los campos de datos registrados en el registro JWT de la Autoridad de Números http://www.iana.org/assignments/jwt/jwt.xhtml. El estándar ISO 18013-5 ha ampliado el modelo de datos JWT con atributos de identidad específicos de las tarjetas de identificación (+ privilegios de conducción).

Este mismo modelo de datos JWT estándar se ejecuta a través de ISO 18013-5 y grupos de trabajo de OpenID Foundation (OIDF) para que las identidades digitales puedan ser utilizadas ampliamente y confiables por la más amplia gama de dispositivos autenticadores y dispositivos POS posible. La transmisión de datos "fuera de línea" ISO 18013-5 utiliza una representación compacta de objetos binarios (CBOR por sus siglas en ingles) de este modelo de datos JWT. Esto une los casos de uso en línea y en persona.

La codificación de los datos mID ha ser codificados en el dispositivo móvil, serán codificados de acuerdo al numeral 7.2 del estándar ISO 18013-5, campos que serán discutidos y coordinados con el JCE para que su integración tenga una correlación a los campos mencionados en el estándar. La definición de campos adicionales conlleva un análisis adicional para su inclusión y lectura por parte de los verificadores ISO 18013-5.

4.2.1.4 PROCEDIMIENTO DE ACTIVACIÓN

Para el aprovisionamiento, o emisión y descarga de la identidad móvil en el dispositivo del ciudadano, GET Mobile Administrator presenta estas opciones de activación:

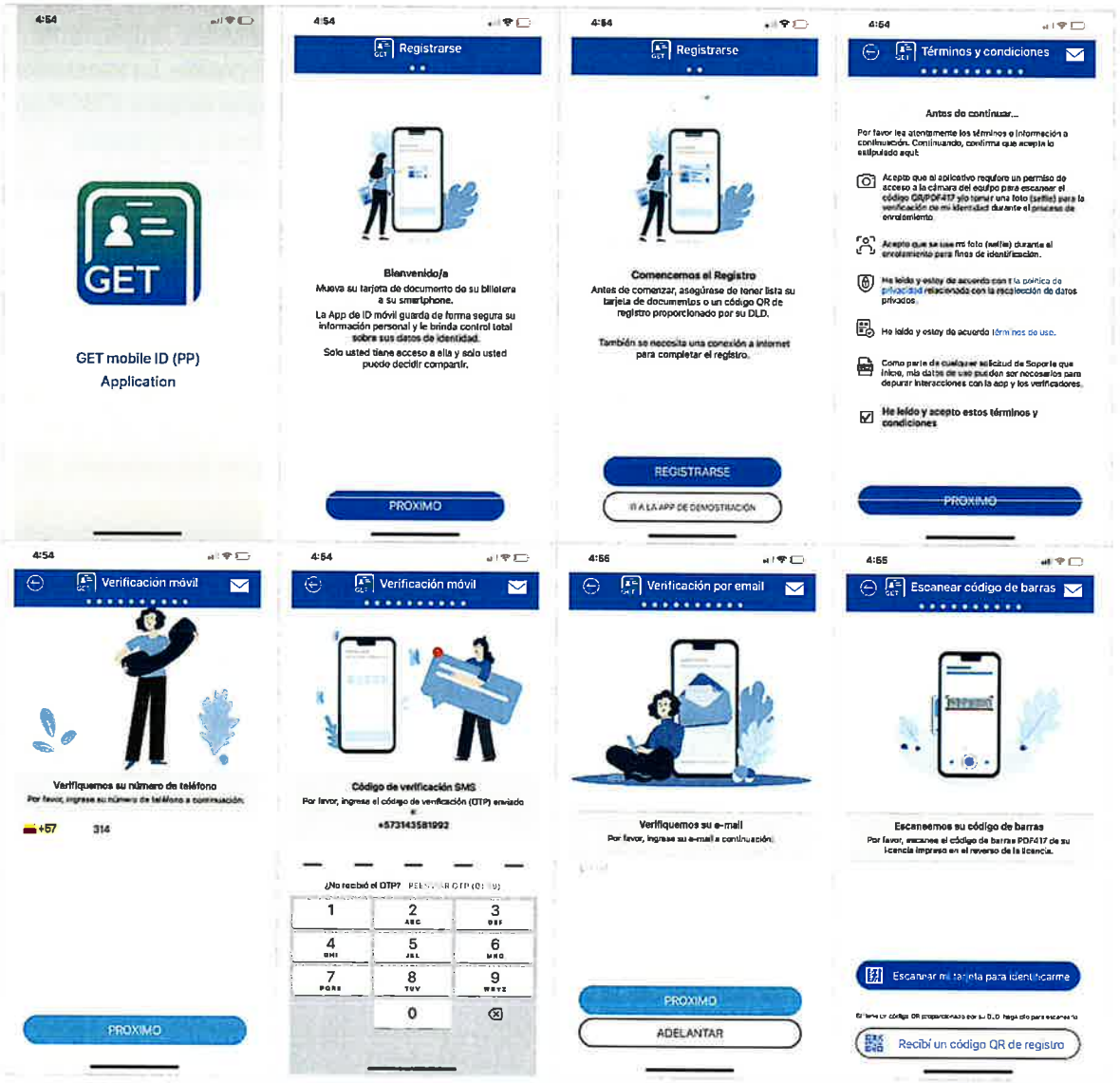
- **Aprobador por Administrador:** Para el aprovisionamiento aprobado por el administrador, los datos se ingresan a través de GET Mobile Administrator. El Administrador aprueba el registro verificando la identidad del solicitante e ingresa la información en el Administrador de GET Mobile ya sea de forma manual o automática desde el sistema del emisor (ver opciones de integración arriba). Una vez que se inserta el registro, los datos mID están listos para publicarse en la aplicación móvil. Es opción es ideal para un programa piloto, donde el titular puede recibir una invitación por correo electrónico para descargar la aplicación y luego completar un breve formulario para personalizar su aplicación con los datos de mID.

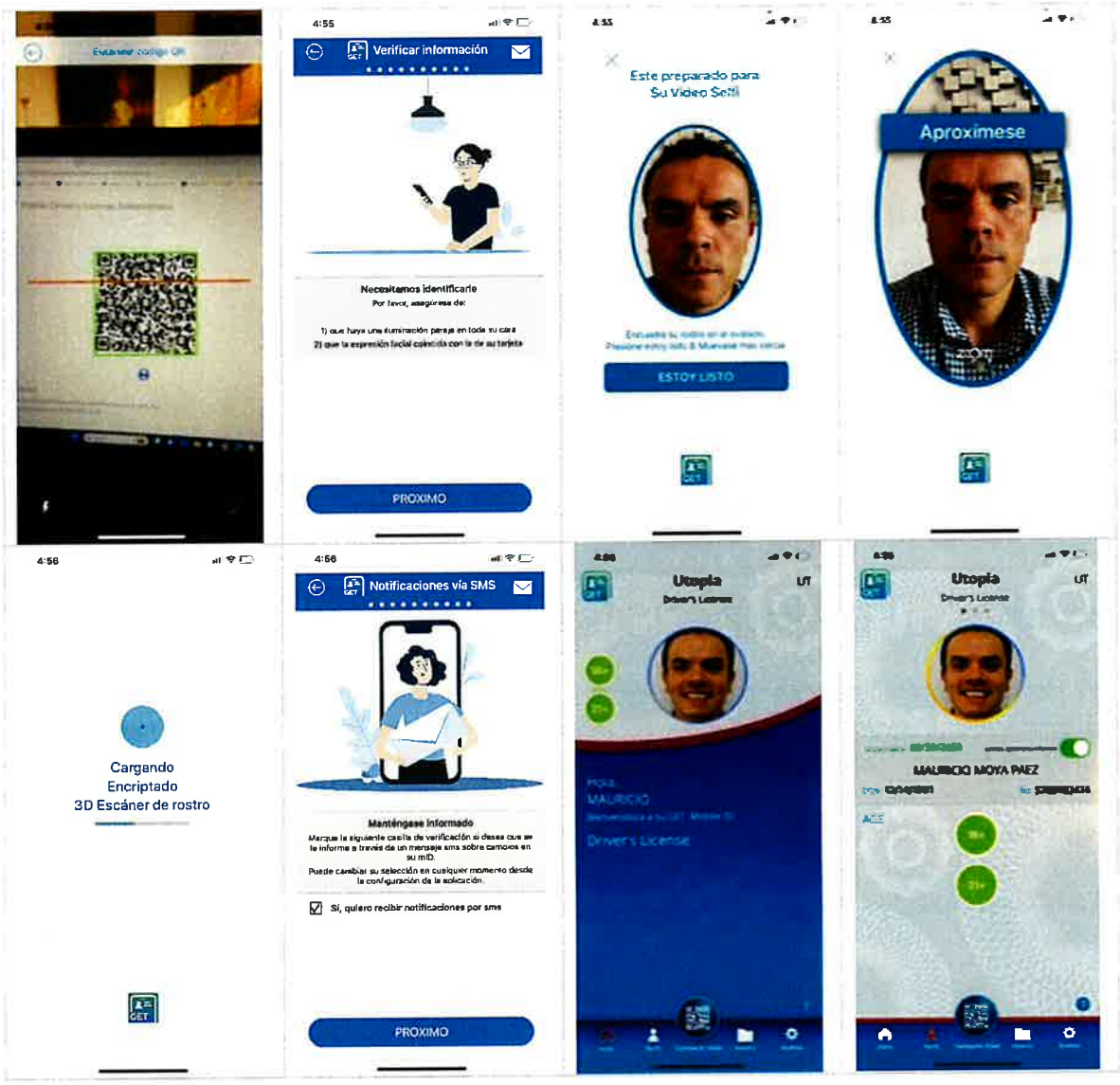
- **Aprovisionamiento en Persona:** Para el aprovisionamiento en persona supervisado por un operador, el administrador de GET Mobile o la aplicación del sistema del emisor del operador pueden mostrar un código QR que identifica un registro mID adecuado y permite que la aplicación GET Mobile ID acceda a ese registro mID adecuado para descargarlo en el dispositivo móvil. (personalización). Alternativamente, el titular puede rellenar un breve formulario para personalizar su aplicación con los datos mID.

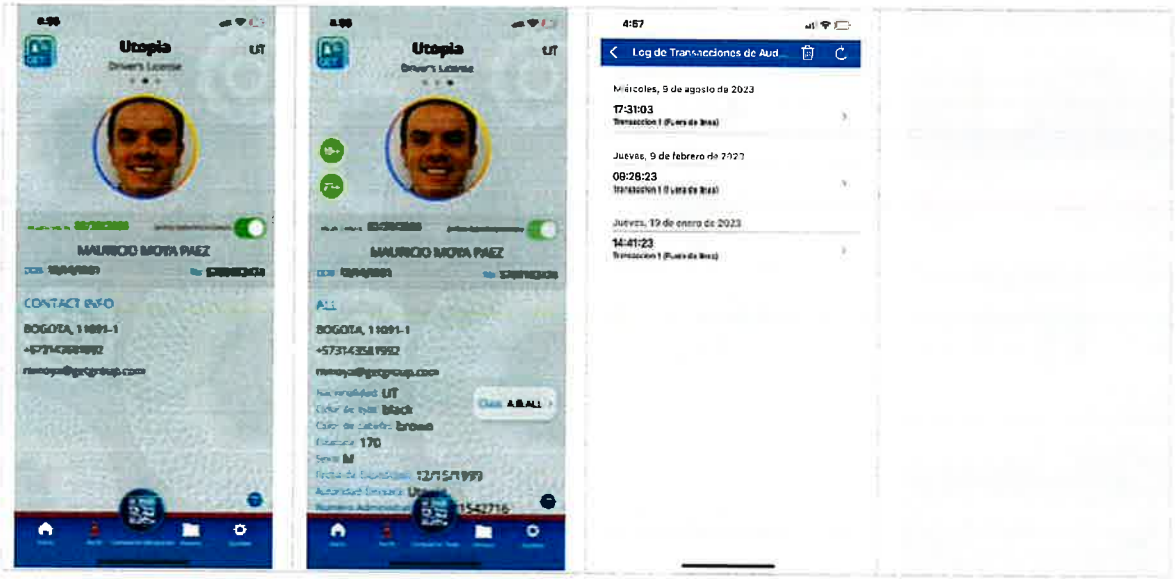
- **Aprovisionamiento remoto:** Para el aprovisionamiento remoto/selfie + liveness, la función del GET Mobile Administrator es verificar a una persona basándose en un escaneo de su identificación estatal emitida por el gobierno, o mediante la lectura de un código QR enviado por correo

electrónico, y una selfie en vivo, incluyendo validación de vida certificada ISO 30107-3 , ambas tomadas en el momento del proceso de inscripción de la aplicación GET Mobile ID. Esta opción incluye la instalación de un componente de que facilita la verificación de datos biométricos y demográficos durante el proceso de registro de emisión de mID. Luego de la emisión, se solicita al usuario digitar un PIN Personal, para permitir la apertura de la aplicación de forma segura. Se cuenta con la funcionalidad de Apple FaceID para realizar este proceso de autenticación.

DEMOSTRACIÓN DE APROVISIONAMIENTO REMOTO:







4.2.2 GET MOBILE ID – APLICACIÓN MÓVIL

GET Mobile ID estará disponible en las tiendas de aplicaciones públicas de cada plataforma móvil en el momento del lanzamiento. Dado que es una aplicación de consumo, se espera que las características del producto se aceleren continuamente y se les dé prioridad según las solicitudes de los ciudadanos/usuarios y lo que esté sucediendo en el mercado mID. El uso de una aplicación de las tiendas de aplicaciones proporciona la experiencia de aplicación que los usuarios esperan de sus bancos, emisores de tarjetas de crédito, proveedores de atención médica y entretenimiento. Todos los usuarios de la aplicación en todas las jurisdicciones experimentarán el mismo conjunto de funciones y se podrán implementar nuevas funciones en todo el país.

El CONSORCIO trabajará con el JCE para configurar ("personalizar") el interior de la aplicación GET Mobile ID cuando un ciudadano lleva su credencial digital como mID. El sello estatal, los patrones de fondo entrecruzado, las fuentes de encabezado y las banderas, así como los tipos de licencia, están disponibles como configuraciones. El GET Mobile ID no es una tarjeta y no tiene una representación de tarjeta; está diseñado para ser intervenido, compartido y utilizado electrónicamente porque la prueba criptográfica de identidad es fácil de presentar utilizando ISO 18013-5.

El CONSORCIO se asegurará de que los campos de la credencial digital estén asignados a los campos ISO 18013-5. Si alguno permanece sin asignar, se puede agregar opcionalmente según se define en los campos específicos de las jurisdicciones, pero no podrán ser leídos por todos los dispositivos o aplicaciones lectores estandarizados. Por lo general, esto no es un problema en los casos de uso de identidad, ya que los campos específicos de la jurisdicción no suelen ser necesarios para aprobar transacciones generalizadas.

Soporte de cumplimiento y estándares

- Cumple con las especificaciones y directrices de la AAMVA
- Certificado de cumplimiento de las normas ISO/IEC18013
- Comunicación entre pares compatible con NFC, Bluetooth y WiFi nativos
- Manejo de llaves conforme a ICAO 9303
- Protección de acceso básica mejorada mediante clave de acceso dinámica

Soporte de comunicaciones

- HTTP/S
- Modo par NFC
- Modo Bluetooth Peer to Peer
- Wifi aware
- Código de barras 2D

Funciones de control de seguridad

- Seguridad redundante mediante almacenes de claves respaldados por hardware.
- Encripción de datos en reposo y transmisión encriptada basada en sesiones.
- Los datos de mID están firmados por la autoridad emisora de confianza a prueba de manipulaciones.
- La ofuscación de aplicaciones significa que el código ejecutable no se puede piratear.
- Protección de análisis estático y dinámico. Se logran protecciones integrales de análisis estático y dinámico a través de técnicas de encriptación y ofuscación en capas complementadas con verificaciones RASP automatizadas y defensas antimalware integradas. Protección contra jailbreaking y rooting.
- OAuth habilitado para autorización de agentes del orden.
- Revocación automática desde el GET Mobile Administrator.
- Criptografía soportada: RSA y Eliptic Curves.

4.2.2.1 OPCIONES DE PERSONALIZACIÓN

GET utilizará componentes existentes sobre una base de desarrollo personalizado para crear una aplicación de emisor personalizada que funcione según los requisitos y el diseño del emisor. Una vez determinado el tamaño y el alcance de los requisitos de la aplicación, se procede con los ajustes de personalización. Además, si el JCE desea publicar la aplicación a través de su propia tienda de aplicaciones (también conocida como marca blanca), se requerirá una coordinación significativa con el personal de Desarrollo de productos de GET para coordinar las actualizaciones del servicio con las actualizaciones de la aplicación.

PERSONALIZACIÓN DE APP MÓVIL

Personalización disponible para la JCE

- ***Pocket, Card,*** y ***Slash Color*** (opción de modo Dia/Noche es automático)
- ***Nombre del Emisor (Issuer Name),*** y el tipo de fuente en la que es desplegado
- ***Tipo de documento (Issuer Card Type) y la Fuente en la que es desplegado*** (Ej.: Cedula Digital)
- ***Sello del Emisor (Issuer Seal)*** (Icono del sello del TSE)
- ***Bandera del Emisor (Issuer Flag)*** (Icono con la bandera del emisor)
- ***Simulación de Diseño de Tarjeta*** (gráficos debajo de la foto)
- ***Diseños Guilloches (Pocket Guilloche Pattern y Pocket Issuer Seal***)

GET trabajará en conjunto con el JCE para presentar una propuesta de diseño que cumpla con los requerimientos de diseño de la marca JCE y de la marca PAIS.

Así mismo, el sistema GET Mobile Administrator, en conjunto con las aplicaciones móviles, permiten la generación de notificaciones PUSH, permitiendo la comunicación con los ciudadanos portadores del GET Mobile ID.

4.2.2.2CONTROL TOTAL Y PROTECCIÓN DE LA PRIVACIDAD

Todos los ciudadanos tienen el derecho básico a controlar su información de identidad. Deberían poder elegir qué datos comparten, ser transparentes en su uso y tener un registro claro de dónde han compartido sus datos. En línea o fuera de línea, GET Mobile ID permanece bajo el control del ciudadano y siempre se requiere su consentimiento para compartir datos, proporcionando un registro claro para el titular del mID de dónde se utilizaron los datos del mID y, cuando sea posible, por quién.

Actualmente, cuando una persona quiere acceder a un colegio de abogados, por ejemplo, está obligada a demostrar su edad. Sin embargo, al presentar un documento de identificación físico, el individuo se ve obligado a exponer toda su información personal (incluida la dirección y otros datos personales sensibles), algunos de los cuales tal vez desee mantener en privado. Al escanear los códigos de barras se crea un registro permanente de sus datos. Con el mID compatible con ISO de GET, un ciudadano puede proteger su privacidad eligiendo la cantidad y el tipo de datos que pueden transferirse a los verificadores. Sólo ciertos verificadores necesitan acceso a todos los elementos de datos. GET Mobile Verify puede limitar los niveles de acceso a datos según la función, la suscripción y la autorización del verificador.

4.2.2.3 SIEMPRE ACTUALIZADO

Las aplicaciones móviles son dinámicas, a diferencia de las credenciales físicas estáticas, lo que permite definir una frecuencia para actualizar los datos mID. El Administrador de GET Mobile permite al Emisor establecer una política de actualización y aplica e implementa automáticamente esa política para que todos los mID conectados dentro de GET Mobile ID se actualicen de forma natural. Ni el ciudadano ni el administrador necesitan preocuparse por mantenerse al día. Además, GET Mobile Administrator admite múltiples mecanismos, a elección del Emisor, para transmitir datos de identificación modificados desde el sistema de registro (SOR) a los usuarios con mID.

Cuando el emisor cambia el estado de una identificación, el emisor transmite ese cambio al administrador de GET Mobile para que lo transmita inmediatamente al dispositivo móvil del usuario. Si un ciudadano reporta la pérdida de una tarjeta o un teléfono, es posible que se le dé de baja de forma remota. Más convenientemente, las funciones de teléfono perdido o extraviado disponibles en cada plataforma están completamente disponibles. Los usuarios pueden borrar los datos del teléfono utilizando sus inicios de sesión individuales en la plataforma. Estas funcionalidades de actualización también aplican en los escenarios de revocación que la Administración decida implementar.

4.2.2.4 INTEROPERABILIDAD

El concepto de interoperabilidad en el marco de la norma ISO 18013-5 hace referencia la capacidad que deben tener las identidades móviles en poder ser usadas dentro de la jurisdicción del emisor (en este caso, la Republica Dominicana) y cualquier otra jurisdicción que requiere poder leer la información de una identidad digital.

Con relación a lo anterior, la norma ISO 18013-5 es la guía para que los gobiernos puedan emitir identidades móviles a sus ciudadanos de manera que están puedan ser leídas, comprobadas y verificadas dentro de otras jurisdicciones. Por ejemplo, en Colombia, país que ha implementado la identidad móvil digital desde el año 2020, a razón de haber implementado el estándar ISO 18013-5, es ahora permitido viajar en los diferentes países de la CAN y MERCOSUR con tan solo mostrar su identidad móvil en su teléfono inteligente, puesto que, al ser una identidad estandarizada, la interoperabilidad le permite identificar que la identidad sigue siendo original y sin modificaciones.

Es así que al decir que una solución de emisión de identidades móviles digitales se encuentra CERTIFICADA para el estándar ISO 18013-5, confirma que esta solución permite la interoperabilidad de las identidades emitidas por esta solución, en conjunto con las diferentes opciones de integraciones y API disponibles para acceder a información adicional y verificaciones.

4.2.3 GET MOBILE VERIFIER

Contrariamente a lo que se cree erróneamente, aceptar identificaciones móviles no significa mirar la pantalla del teléfono de sus clientes ni manipular su teléfono en absoluto. Las herramientas de manipulación de fotografías hacen que el uso visual no sea confiable y usted nunca debe asumir la responsabilidad de manipular el teléfono de su cliente.

Los mecanismos de transmisión ISO 18013-5 permiten modos de interacción flexibles que mantienen a su cliente en control de su dispositivo y sus datos, al tiempo que le brindan al verificador prueba criptográfica indiscutible de la identidad de su cliente, incluso sin sobrecarga de datos.

Cuando intercambia datos electrónicos y valida pruebas criptográficas, ya no está sujeto a los requisitos de "línea de visión" de las tarjetas de identificación físicas.

A medida que la identificación se vuelve cada vez más digital, el mercado debe estar preparado para aceptar rápidamente identificaciones móviles desde cualquier parte del mundo como forma legal de identidad o verificación de edad. La aplicación GET Mobile Verify le proporcionará una transacción de cliente más fácil y segura.

- Aplicación directa a la parte que confía: verificar la edad y la identidad del titular.
- Lectura estándar ISO 18013-5 en línea y fuera de línea.
- Trabaja con todas las jurisdicciones a nivel mundial a través de una lista confiable
- Disponible para iOS y Android: GET Mobile Verify admite NFC, BLE, Wi-Fi Aware y WebAPI en plataformas iOS y Android. Disponible como motor para dispositivos Windows y POS.
- Reduce la complejidad de la inspección de documentos de identificación globales: mantenerse al día con los cambios de los documentos de identificación en constante cambio es difícil. ¿Cómo puedes saber qué es real o qué es simplemente una muy buena tarjeta de identificación falsa? Las identificaciones móviles mID presentan su prueba de identificación electrónicamente y de la misma manera siempre: grande, en negrita, mostrando prueba de edad o identificación. No requiere del entrenamiento laborioso del personal y hay menos errores cuando los documentos parecen ser legítimos.
- Obtiene una prueba criptográfica de identificación: el simple hecho de mirar los documentos de identificación, especialmente en dispositivos móviles, no descarta las identificaciones falsas. GET Mobile Verify solo acepta documentos de emisores de identificación gubernamentales conocidos, lo que reduce su responsabilidad y exposición.
- Respeta la confidencialidad de sus clientes: reducir los datos intercambiados durante las transacciones de identificación mejora la privacidad de sus clientes y alivia sus preocupaciones sobre privacidad y seguridad, al tiempo que reduce su exposición y responsabilidad de recopilar y almacenar datos personales.
- Transacciones de identidad más saludables: proteja la salud de sus empleados y clientes con transacciones de identificación sin contacto. Un toque o un escaneo desde la distancia social garantiza que no esté manipulando documentos de identidad ni asumiendo responsabilidad por el manejo de los teléfonos móviles de sus clientes. GET Mobile Verify permite a tus clientes comprobar su identidad desde una distancia segura y saludable.

El estándar ISO/IEC 18013-5 introduce dos pasos en una interacción mID: La interacción del dispositivo (Device engagement) es cuando el mID y el dispositivo lector negocian cómo conectarse en el intercambio de datos mID en línea; Y fuera de línea, a través de un canal de transmisión mutuamente compatible. Una vez elegido un canal, los dispositivos realizan la transmisión de datos mediante solicitud-respuesta.

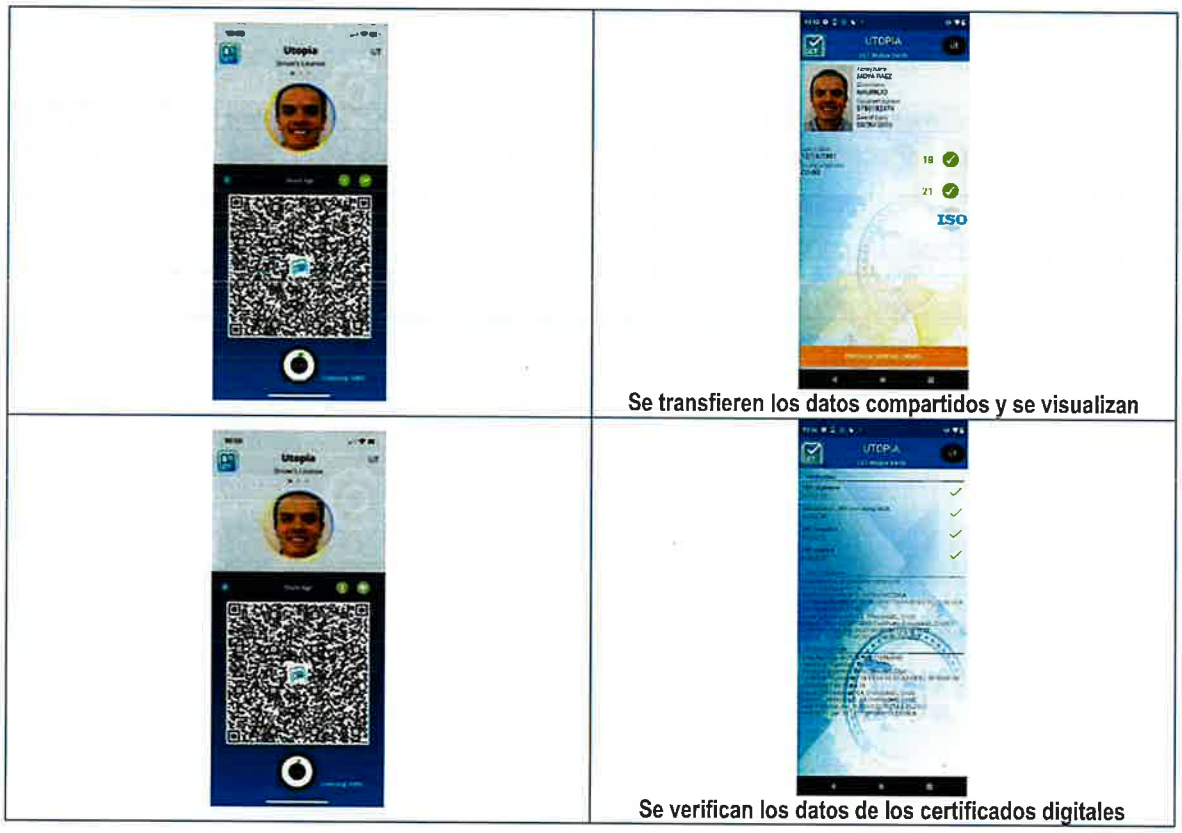
Se admiten dos modelos: verificación offline (sin necesidad de Internet) y verificación de búsqueda en línea.

Los métodos de interacción con dispositivos admitidos: NFC, QR, BLE (según la extensión en evolución del borrador del estándar internacional ISO).

Canales de transmisión de datos admitidos: NFC sin conexión (Android completo e iOS en alfa), BLE, WIFI Aware (en versión beta disponible solo en Android 10 o posterior), en línea a través de WebAPI y Open ID Connect.

Simulación de Verificación de mID

Aplicación mID	Aplicación Mobile Verifier
 Se inicia la Aplicación GET Mobile ID	 Se inicia la aplicación GET Mobile Verifier
 El usuario elije los datos que desea compartir	
 El usuario selecciona Compartir	 Se escanea el QR compartido



4.2.3.1 MODOS DE INTERACCIÓN

Las combinaciones de interacción con el dispositivo, transferencia de datos y en línea/fuera de línea crean "interacciones" únicas que, si se implementan por completo, permitirán a los verificadores reconfigurar el flujo de trabajo para adaptarlo a su negocio y brindar un servicio ampliado y más personalizado a los clientes de mID en comparación con lo que se ofrece tradicionalmente con Tarjetas físicas.

Estos modos de interacción combinados se pueden resumir a continuación. El soporte de todos los modos de interacción pasa a ser responsabilidad del Emisor al elegir la tecnología mID. Múltiples modos de interacción brindarán la experiencia de usuario óptima para los titulares de mID y brindarán la mejor opción para los verificadores de mID.

Los verificadores deberían poder elegir el modo de interacción que mejor respalde su negocio.

Modo de Interacción	Vinculación de Dispositivo	Transferencia de Datos	Autorización de Usuario [Si es no atendida]	Descripción
Tap & Go	NFC	BLE		El toque NFC establece BLE para la transferencia de datos y el usuario puede alejar el mID mientras transfiere datos al lector
Tap & Request	NFC	Online		NFC contiene un token WebAPI que devuelve datos con el retrato (fotografía) para el operador
Tap & Hold	NFC	NFC		Interacción y transferencia de datos complete por NFC

Scan & Go	QR	BLE	El usuario sostiene el código QR mID frente a la cámara del lector y luego puede mover el mID mientras se transfieren datos a través de un método cercano
Scan & Request	QR	Online	El usuario sostiene el código QR mID en la cámara del Reader y los datos aparecen en el Reader después de una rápida recuperación en línea

Dar soporte a estos múltiples modos de interacción no requiere ningún esfuerzo por parte del JCE más allá de elegir e implementar la tecnología de aplicación GET Mobile ID y realizar una opción de integración estándar como se describe en este documento. Será una opción clave para los ciudadanos y para construir una plataforma en la que la identidad móvil pueda florecer verdaderamente.

4.2.4 Herramientas de Desarrollo

GET Mobile ID tiene la posibilidad de brindar un soporte adicional con relación a las herramientas de desarrollo disponibles para la implementación de la emisión de una identidad digital móvil basada en estándar ISO 18013-5, dentro de las cuales se encuentran:

- SDK's para la emisión de identidades, para Android y iOS.
- API para la conexión e integración en el proceso de emisión de identidades móviles.
- SDK's disponibles para la verificación de identidades móviles, basadas en estándares, para su implementación en Android, iOS, Windows o sistemas POS.

Durante el proceso de análisis de requerimientos se establecerán los compromisos necesarios para realizar la entrega de los SDK's solicitados de acuerdo con la necesidad de implementación del JCE.

4.2.5 INFRAESTRUCTURA

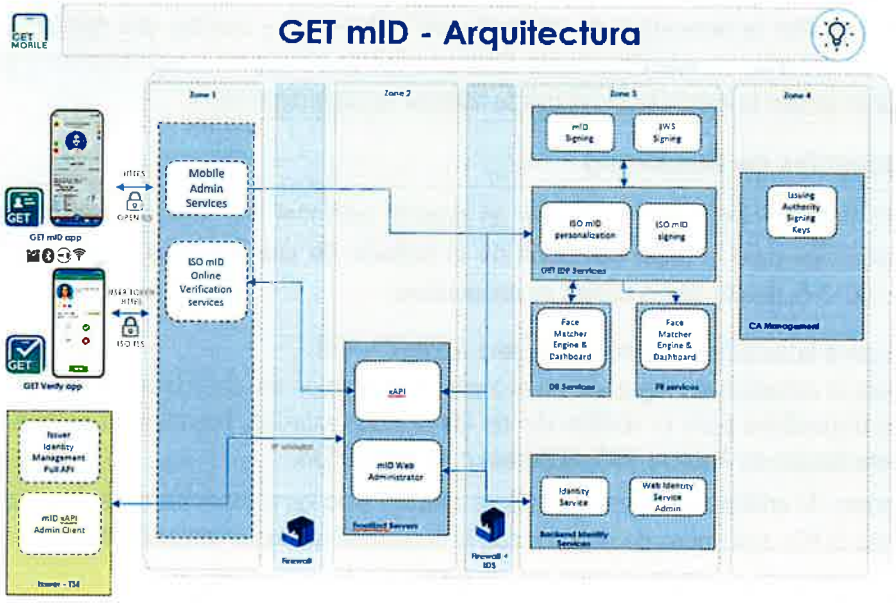
4.2.5.1 ARQUITECTURA DE ALTA DISPONIBILIDAD

El diseño de la solución GET Mobile ID es un diseño innovador que está basado en la Alta Disponibilidad de cada uno de los componentes, en conjunto con el uso de diferentes zonas de seguridad para garantizar la implementación segura. El diseño de solución acá propuesto incluye la capacidad requerida para emitir al menos 5.000 GET Mobile ID por día.

Los módulos que componen la arquitectura de la solución son:

- Mobile Admin services: API para la Administración de la emisión en los teléfonos móviles.
- ISO mID Online Verification services: API para la verificación de identidades Mobile ID en línea.
- xAPI: API para el control de la emisión de identidades Mobile ID.
- mID Web Administrator: Modulo Web que permite la administración de la solución, su configuración, visualizar de eventos y auditoria, gestor de reportes.
- mID Signing: Modulo de firma de documentos digitales, utiliza las llaves del PKI para su función.
- JWS Signing: Modulo de firmado para archivos JSON.
- ISO mID Perso: API para emisión de identidades estándar ISO 18013-5
- ISO mID signing: API para el firmado ISO.

- Face matcher: Módulos de comparación y base de datos para la verificación biométrica y reconocimiento de vida.
- Identity Service: Modulo de administración de identidades.
- Web Identity Service Admin: Administración de usuario para módulos web.
- Issuing Authority Signing Keys: Solución PKI.



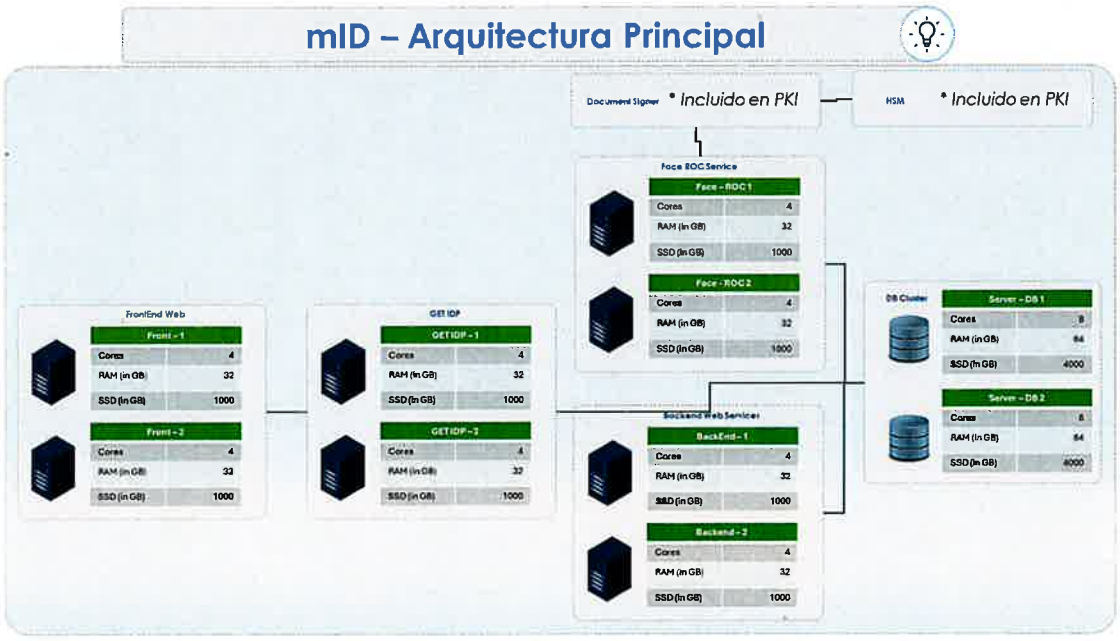
Se han tomado todas las previsiones del caso para poder brindar a la JCE una plataforma con mecanismos de alta disponibilidad del servicio tanto en hardware como en software contemplando los siguientes aspectos a nivel de diseño de la infraestructura para garantizar la continuidad de la operación:

Se dispondrá de una infraestructura Hiperconvergente el cual está diseñado con 4 nodos para brindar una redundancia y alta disponibilidad, además de una capa de interconexión media con dos switches en HA para realizar la configuración del ambiente de producción requerido. Esta solución de hiperconvergencia contempla una configuración vSAN para brindar alta disponibilidad a nivel de almacenamiento.

Esta solución contempla un esquema de respaldos sobre las máquinas virtuales requeridas para desplegar el servicio, el cual se define en 1 respaldo Full diario con retención de 30 días.
Además, se incluye una capa de red de borde compuesta por dos switches en configuración de alta disponibilidad y redundancia para brindar la interconexión entre la infraestructura de hiperconvergencia, la capa de seguridad dimensionada y la conexión hacia la infraestructura de la JCE.

A nivel de seguridad se contempla un diseño de alta disponibilidad de NG Firewalls, este es un componente crítico en la arquitectura de seguridad de redes modernas. Estos dispositivos desempeñan un papel fundamental en la protección de una organización contra amenazas cibernéticas, por lo que garantizar su continuidad operativa es esencial. Para lograr una alta disponibilidad, se implementan redundancias en la infraestructura del NG Firewall, lo que incluye configuraciones en clúster, así como elementos en su arquitectura física, como fuentes de poder redundantes.

Referente a la implementación del Web Application Firewall (WAF), el mismo es un elemento virtual dentro de la solución ofertada. De esta manera, teniendo lo anterior en consideración, es posible brindar todas las bondades de los ambientes de virtualización desarrollados en el presente diseño, lo que permite que el WAF tenga una alta disponibilidad en su infraestructura. Un Web Application Firewall (WAF) virtual de Alta Disponibilidad (HA) es una parte esencial de la estrategia de seguridad cibernética para proteger aplicaciones web y sitios web.



4.2.5.2DISPONIBILIDAD DEL 99.95% DE OPERACIÓN

Con el fin de garantizar un esquema de alta disponibilidad de operación durante las horas efectivas de producción definidas por el JCE el consorcio considera conveniente la inclusión de un recurso especializado en los equipos de procesamiento y seguridad en sitio para garantizar la atención inmediata de incidentes que se puedan presentar y reducir los tiempos de atención de la solución, esto en conjunto con los diseños explicados en el apartado de Infraestructura buscan garantizar al JCE el menor impacto posible en la operación y la continuidad del servicio.