EMDOC
CONSORCIO

ÍTEM IV. PROPUESTA TÉCNICA PARA LA TARJETA DE IDENTIDAD DIGITAL

PARA LA CONTRATACIÓN DE LA EMPRESA QUE SE ENCARGARÁ DE SUPLIR LOS EQUIPOS, MATERIALES Y SERVICIOS PARA LA IMPRESIÓN DE LA CÉDULA DE IDENTIDAD Y ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)

CONSORCIO EMDOC
EMDOC
CONSORCIO
Santo Domingo, R.D.

EMDOC CONSORCIO

CONTENIDO

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo R.D.

EMDOC CONSORCIO

1 Respuesta técnica a PUNTO IV - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL

1.1. Resumen de la solución

La plataforma ofrece un ecosistema de identidad digital interoperable que garantiza el acceso seguro a servicios tanto públicos como privados. Un elemento clave de esta solución es la Cédula Digital, que cuenta con un monedero móvil y un verificador móvil con certificación ISO 18013-5, que supera los requisitos de seguridad mediante una sólida validación criptográfica. El sistema de identidad digital está diseñado para ser modular, escalable y capaz de adaptarse a una demanda fluctuante. Aprovecha la tecnología API REST en entornos de nube pública o privada y emplea credenciales verificables (VC) del W3C para una autenticación digital segura. La plataforma integra funciones esenciales de ciberseguridad, como la lectura electrónica de chips y la verificación facial 1 a 1 para dispositivos compatibles, lo que garantiza un marco de alta seguridad y una verificación de identidad sin fisuras. Además, los dispositivos móviles incorporan medidas de protección contra la ingeniería inversa, la manipulación del código y el acceso no autorizado.

Tanto la aplicación móvil del titular como la del verificador son compatibles con iOS y Android y cuentan con la certificación FIME para 18013-5 . Funciones configurables que ofrecen compatibilidad con funciones de seguridad como la autenticación multifactor (AMF) y, previa aprobación del usuario, la verificación facial compatible con el dispositivo para acceder al monedero de identificación del titular. La activación remota de las identidades digitales se facilita a través de enlaces temporales enviados por correo electrónico o mensaje de texto, con periodos de caducidad controlados para mejorar la seguridad. Además, admite la visualización de datos fuera de línea para mejorar la accesibilidad de los casos de uso de verificación por parte del gobierno o las fuerzas de seguridad.

La plataforma se desplegará como un entorno de alta disponibilidad con capacidades de conmutación por error que limitan el tiempo de inactividad a no más de cinco minutos. La plataforma basada en microservicios será compatible con la interoperabilidad y la escalabilidad, lo que permitirá una integración perfecta con los servicios existentes y futuros.

Un sistema de identidad digital seguro, escalable y eficiente que pueda desplegarse in situ o en la nube que mantenga la confianza pública y mejore la accesibilidad mediante el cumplimiento de las normas mundiales de seguridad e interoperabilidad proporcionará la infraestructura sólida y preparada para el futuro que busca el honorable JCE.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

1.2. Plataforma de microservicios de identificación digital

- **Emisión de tarjetas de identidad digital (CD) y gestión de perfiles de usuario:** La plataforma permite a la JCE crear procesos personalizados de registro de usuarios y gestión de perfiles aprovechando el requisito de integración de su actual sistema central de gestión de tarjetas. Esto se hace mediante la configuración de los recorridos de identidad, personalizando los flujos de incorporación, inscripción, adjudicación, autenticación y autorización. Esta flexibilidad permite al JCE adaptarse a diversos requisitos normativos y políticas internas . La plataforma también permite la incorporación de un sistema integral de gestión del ciclo de vida de las credenciales digitales. Esto soportará el ciclo de vida completo de las credenciales, incluyendo su emisión, activación y revocación. También admite el registro de los eventos de acceso de cada credencial para garantizar la trazabilidad y la seguridad. También proporciona las aplicaciones o interfaces necesarias para apoyar la integración e implantación de nuevas soluciones.

- **Visión general de la plataforma:**

  La plataforma multiarrendamiento utiliza una arquitectura de microservicios, que se divide en unidades modulares y escalables, cada una de las cuales se encarga de funciones específicas.

  - Entre sus principales servicios figuran:
    - **Pasarela WEB-API**
    - **Gestión de la orquestación**
    - **Gestión de usuarios**
    - **Gestión de credenciales**
    - **Gestión de informes**
    - **Servicio de notificación**
    - **Servicio de verificación biométrica**

  - **Gestión de identidades y accesos:**
    La plataforma cuenta con un proveedor de identidades (IdP) integrado que autentica y autoriza a los usuarios para acceder de forma segura a los servicios y aplicaciones de la plataforma. Puede emitir y gestionar identidades de usuario, como Mobile Wallets, e integrarse con proveedores de identidad externos como OpenID Connect (OIDC), Security Assertion Markup Language (SAML) o Active Directory (AD).

    La plataforma VeriGO MobileID contiene múltiples plataformas de interfaz como SAML, OIDC, LDAP y varios protocolos de bases de datos. Realizaremos la interfaz basándonos en las interfaces elegidas de JCE.

  Características principales:

- **Autenticación centralizada:** Control de acceso unificado en toda la organización.

- **Políticas personalizadas:** Se alinea con las políticas de seguridad de tu organización.

- **Autenticación multifactor (MFA):** Añade una capa adicional de seguridad a los servicios y aplicaciones de la plataforma.

- **Compatibilidad con la API REST:**
  La plataforma expone una API REST que permite a los desarrolladores interactuar con sus servicios mediante programación. La API REST está diseñada para ser:
  - **Sin estado:** Cada petición API del cliente contiene toda la información necesaria para que el servidor la entienda y procese, haciendo que el servicio sea escalable y fiable.
  - **Orientada a recursos:** La API está estructurada en torno a recursos como usuarios, credenciales e informes, a los que se puede acceder y manipular mediante métodos HTTP estándar (GET, POST, PUT, DELETE).
  - **Segura:** Todas las interacciones a través de la API REST están protegidas mediante HTTPS, lo que garantiza el cifrado de los datos en tránsito.

- **Soporte de aplicaciones heredadas:**
  Las aplicaciones heredadas sin soporte OAuth2-OIDC o SAML aún pueden integrarse con la plataforma utilizando Claves de Acceso API para el acceso seguro a recursos HTTPS.

- **Gestión del ciclo de vida del DNI digital**

  - **Creación y modificación de usuarios**

    - La plataforma ofrece un portal administrativo fácil de usar para crear y gestionar perfiles de usuario. Admite trayectos de usuario personalizables, lo que permite controles de acceso flexibles basados en funciones para administradores, operadores, ciudadanos y usuarios temporales. El JCE puede adaptar estos itinerarios a sus políticas y requisitos específicos actuales y futuros, incluida la activación remota mediante SNS para enviar enlaces de tiempo limitado por correo electrónico o SMS, garantizando la seguridad con un método de autenticación de dos factores (2FA) PIN y verificación facial como mínimo.

- Aprovisionamiento automatizado basado en eventos de registro, flujos de trabajo o secuencias de comandos.
- Puede admitir la definición de atributos de identidad personalizados y el control de las correspondencias y los valores de los datos.
- La plataforma se integra perfectamente con sistemas externos a través de un sólido marco de API. Esta integración permite sincronizar los datos de usuario, la autenticación y los procesos de autorización con otras aplicaciones y servicios. Al adherirse a estándares del sector como las API RESTful, la plataforma garantiza la interoperabilidad y la flexibilidad.
- Desaprovisionamiento automatizado basado en eventos o flujos de trabajo específicos.

- **Soporte para el ciclo de vida completo de las credenciales, incluida la emisión, activación y revocación**
- **Desduplicación de ID de usuario**
  - Mecanismos sólidos de eliminación de duplicados para evitar la duplicación de ID de usuario.
  - Algoritmos avanzados de concordancia para identificar posibles duplicados.
- **Alertas y notificaciones**
  - VeriGO MobileID ofrece la posibilidad de proporcionar notificaciones a través del servicio SNS (notificaciones push móviles en la aplicación o en la pantalla de inicio del dispositivo, así como por correo electrónico). La forma, el contenido y la audiencia de los mensajes tendrían que definirse conjuntamente con JCE.
  - En lo que respecta a las notificaciones de ID Wallet durante la activación del dispositivo Según la norma ISO/IEC 18013-5, Veridos desea destacar que un código de barras está destinado únicamente a la activación del dispositivo.
    - Cuando un ciudadano abre su aplicación, se le presenta la imagen de su credencial digitalizada. Desde esta pantalla puede ver sus propios datos o presentar la credencial de forma verificable. Desde la perspectiva del ciudadano, la transacción de identidad

se inicia con su entrada a través del icono "Permitir inspección". La participación del dispositivo facilita la comunicación entre el dispositivo del titular y el dispositivo del verificador a través de un canal de comunicación seguro . Esta comunicación se realiza mediante tecnología BLE o NFC. Tras la conexión del dispositivo, el titular recibirá una lista de los atributos que se solicita compartir como parte de la transacción de identidad. En esta fase, el titular puede dar su consentimiento o revocarlo en cualquier momento. Esto se aplica tanto a la transmisión de la credencial completa como a los atributos de identidad individuales; por ejemplo, un usuario puede negarse a compartir su fecha de nacimiento exacta y confirmar que tiene más de 18, 19 o 21 años.

1.3. Autenticación

Autenticación basada en el riesgo

- Autenticación adaptativa: Ajuste el nivel de autenticación necesario en función de factores de riesgo, como la dirección IP, el tipo de dispositivo o el comportamiento del usuario.

Inicio de sesión único (SSO) - (SAML, OAuth, OpenID Connect)

- Estándares compatibles para facilitar la integración de las organizaciones, la integración de las partes confiantes y otros casos de uso para permitir el acceso sin problemas a múltiples aplicaciones con un único inicio de sesión.

1.4. Arquitectura de confianza cero

Es un modelo de seguridad que asume que ningún usuario o dispositivo es intrínsecamente fiable. Requiere la verificación continua de usuarios y dispositivos antes de conceder acceso a los recursos.

Los principios clave de la plataforma incluyen:

- No confíe nunca, verifique siempre: Valida continuamente la identidad del usuario y el estado del dispositivo.
- Modelo de acceso de mínimo privilegio: Conceder a los usuarios sólo los permisos mínimos necesarios.
- Microsegmentación: Aísle los segmentos de la red para limitar el impacto de posibles brechas.

- Supervisión y registro continuos: Supervise el tráfico de red y la actividad de los usuarios en busca de anomalías.

Consideraciones adicionales

- Experiencia del usuario: Garantice una experiencia de autenticación fluida y fácil de usar.
- Mejores prácticas de seguridad: Adhiérase a las normas y mejores prácticas del sector para una autenticación segura.
- Evaluaciones periódicas de la seguridad: Realice evaluaciones de seguridad periódicas para identificar y mitigar vulnerabilidades.
- Plan de respuesta a incidentes: Disponga de un plan de respuesta a incidentes bien definido para hacer frente a las brechas de seguridad.
- Al adoptar un modelo de credenciales sin contraseña y resistente al phishing, las organizaciones pueden mejorar significativamente su postura de seguridad y proteger los datos confidenciales.
- Datos de identificación de la persona (DIP)
    - Los Datos de Identificación Personal (DIP) son la forma más importante y segura de credenciales verificables. Los PID son expedidos directamente por las autoridades gubernamentales y sirven como la más fundamental de la identidad de una persona. Los PID son credenciales emitidas por el gobierno que vinculan a una persona con su estatus legal.
    - En el caso de las personas jurídicas, los PID suelen denominarse LPID (Legal Person Identification Data, datos de identificación de la persona jurídica), que son cruciales para interacciones seguras y verificadas entre servicios públicos y privados.
  - Ejemplos:
    - Documento de identificación móvil (mID) expedido por el Gobierno, credencial digital de viaje (DTC), permiso de conducir móvil (mDL).
    - LPID - certificado de registro de empresa que acredita la personalidad jurídica.

Autoservicio de restablecimiento de contraseña:

- Restablecimiento de contraseña iniciado por el usuario a través de un proceso seguro que implica la autenticación multifactor.
- Bloqueo automático de la cuenta tras varios intentos fallidos de inicio de sesión.
- Procedimientos de desbloqueo de cuentas, incluido el restablecimiento de la contraseña o la intervención administrativa.

1.5. Verificación y validación de la identidad

- **Verificación de la prueba de identidad**
  - Verificación de documentos de identidad mediante procesos manuales o automatizados aprovechando los servicios existentes de la organización, utilizando los servicios IDV integrados o integrando servicios ahora en el futuro mediante API o el SDK de ID Wallet.
- **Autenticación biométrica**
  - Integración con tecnologías de autenticación biométrica (por ejemplo, reconocimiento facial, huella dactilar) para mejorar la seguridad.
  - La detección de actividad o la integración con tecnologías existentes o emergentes pueden aplicarse para mitigar los ataques de suplantación de identidad.

1.6. Aprovisionamiento y desaprovisionamiento de usuarios

- **Aprovisionamiento automatizado**
  - Creación automática de cuentas de usuario basada en reglas y flujos de trabajo predefinidos.
  - Integración con sistemas organizativos mediante API basadas en estándares, como las API RESTful, para sincronizar los datos de los usuarios.
- **Desaprovisionamiento automático**
  - Eliminación automática de cuentas de usuario en caso de rescisión u otros eventos específicos.
  - Al darse de baja el usuario, el sistema borrará de forma segura los datos personales, revocará los privilegios de acceso y archivará la información necesaria. Las políticas de conservación y supresión de datos se revisarán

periódicamente para garantizar el cumplimiento de la normativa.

- **Borrado de datos**: Borrado seguro de todos los datos personales asociados al usuario, incluidos, entre otros:
  - Información personal identificable (IPI)
  - Datos sensibles (por ejemplo, historiales médicos, información financiera)
  - Preferencias y ajustes del usuario

- **Recuperación de recursos:** Revocación de todos los privilegios de acceso y eliminación de los permisos de usuario de sistemas y aplicaciones.

- **Conservación de registros de auditoría:** Conservación de los registros de auditoría necesarios con fines de cumplimiento y seguridad, al tiempo que se anonimiza o redacta la información sensible.

- **Archivo de datos:** Archivar los datos necesarios para fines legales o reglamentarios, garantizando medidas de seguridad y controles de acceso adecuados.

- **Verificación del cumplimiento:** Revisión y actualización periódicas de las políticas de conservación y eliminación de datos para alinearlas con la evolución de la normativa (por ejemplo, GDPR, CCPA, HIPAA).

Siguiendo estas buenas prácticas, la Plataforma garantizará que los datos de los usuarios se traten de forma responsable y segura, minimizando los riesgos potenciales y manteniendo el cumplimiento de la normativa aplicable.

1.7. Experiencia de usuario y autoservicio

La Plataforma ha sido diseñada para ser lo más intuitiva y sencilla posible. Maximiza la facilidad de uso, al tiempo que mantiene el máximo nivel de seguridad y privacidad.

- **Interfaz fácil de usar**
  - Interfaz de usuario intuitiva para facilitar la navegación y la realización de tareas.
- **Experiencia personalizada**

- Experiencias de usuario personalizadas en función de sus funciones y preferencias.
- Recomendaciones y notificaciones contextuales.

- **Verificación y validación de la identidad**
  - Procesos sólidos de verificación de la identidad, incluida la validación de documentos, la autenticación biométrica y la compatibilidad con los dispositivos requeridos por el cliente.
  - Integración con proveedores de identidad externos para una autenticación sin fisuras.
  - Mecanismos de autenticación y autorización basados en el riesgo para garantizar la seguridad.

- **Billetera digital**
  - El identificador visual configurable utiliza un SVG cifrado y las credenciales se generan en el momento de la emisión: digitalmente son únicas. La información visualmente oculta (como el IPI) puede entregarse en el momento de la emisión. La orientación de la identificación visual es configurable, incluidos los elementos de la interfaz de usuario.
  - Almacenamiento seguro del carné de identidad digital (CD)
  - Fácil acceso a los documentos a través de la aplicación móvil.
  - Soporte para NFC, verificación basada en código QR y fichas digitales de un solo uso de serie con el monedero móvil.
  - Política de inicio de sesión de dispositivos configurable, los dispositivos también pueden limitarse en función de la política establecida por el JCE a medida que evolucionan los requisitos.
  - Admite procesos de cambio de dispositivo basados en flujos de trabajo, incluidos el inicio, la verificación y la autenticación de usuarios, la validación de dispositivos y las actualizaciones de perfiles. Prioriza la seguridad mediante una autenticación sólida y medidas de protección de datos.
  - *ISO 18013-5 Certificado por FIME*
  - VeriGO MobileID admite tanto el modo de recuperación por servidor como por dispositivo. La posibilidad de que los ciudadanos presenten su información para su inspección y de que las partes de confianza verifiquen dicha información

incluso sin conexión a Internet es una característica de VeriGO MobileID definida en ISO/IEC 18013-5. El periodo de validez de una credencial en modo fuera de línea (recuperación del dispositivo) está sujeto a las normas empresariales de JCE y se aclarará durante la fase de proyecto.

- Una característica estándar de VeriGO MobileID para priorizar la privacidad y la comodidad del usuario. La minimización de datos definida por el usuario es un principio básico de la especificación ISO/IEC 18013-5. Tras la activación del dispositivo, se solicitará al titular una lista de los atributos que se desea compartir como parte de la transacción de identidad. En esta fase, el titular puede dar su consentimiento o revocarlo en cualquier momento. Esto se aplica tanto a la transmisión de la credencial completa como a los atributos de identidad individuales; por ejemplo, un usuario puede negarse a compartir su fecha de nacimiento exacta y confirmar que tiene más de 18, 19 o 21 años.

- Todos los datos presentados se firmarán electrónicamente para garantizar que terceros puedan validar la integridad y el origen de los datos proporcionados por el ciudadano. Esto forma parte de la norma ISO/IEC 18013-5 que Veridos cumple.

- Las credenciales se almacenan en un elemento seguro (enclave). Cuando se instala la aplicación VeriGO MobileID, se comprueba si el dispositivo móvil está rooteado o jailbreakeado antes de proceder a la instalación. Las aplicaciones móviles están firmadas digitalmente y ofuscadas - esto significa que todo el código ha sido codificado intencionadamente impidiendo cualquier intento de ingeniería inversa . Cada vez que VeriGO MobileID se comunica con el servidor a través de TLS, la comunicación se cifra sistemáticamente.

- Una representación digital de la credencial puede verse después de que el usuario abra VeriGO MobileID y haya completado los requisitos 2FA. Cuando, tras completar los requisitos 2FA, un ciudadano abre su aplicación, se le presenta una imagen de su credencial digitalizada. Desde esta pantalla puede ver sus propios datos o presentar la credencial de forma verificable. Desde la perspectiva del ciudadano, la transacción de identidad se inicia con su entrada a través del icono "Permitir inspección".

- **Verificador móvil:**
  - Los verificadores, como los funcionarios, dependen actualmente de comprobar la identificación de un usuario con un documento físico. Con el verificador móvil, el funcionario puede confirmar la identidad de un usuario a través de su dispositivo móvil.
  - Utiliza métodos rigurosos y exhaustivos para verificar los documentos de identificación de un usuario. Los verificadores pueden estar seguros de que los documentos son auténticos y válidos.
  - Se obtiene el consentimiento de los usuarios para garantizar que comprenden y aceptan compartir sólo la información necesaria con el proveedor de servicios.
  - Verificación basada en NFC: Verificación offline de credenciales de identidad mediante tecnología NFC.
  - Verificación por código QR configurable: Verificación offline mediante códigos QR generados y almacenados en el dispositivo del usuario.
  - Tokens digitales de un solo uso: Verificación fuera de línea mediante tokens de un solo uso para la verificación segura de la identidad en ubicaciones de terceros.
  - *ISO 18013-5 Certificado por FIME*
- **Registro y auditoría**
  - Registro y auditoría exhaustivos de todas las actividades de los usuarios y eventos del sistema.
  - Supervisión de la salud y la seguridad del sistema.
- **e-KYC y renovación**
  - Procesos automatizados de e-KYC para verificar periódicamente la identidad de los usuarios.
  - Recordatorios puntuales de renovación y expiración de documentos.
- **Notificaciones configurables**
  - Admite notificaciones personalizables JCE para satisfacer requisitos específicos del usuario o del sistema.

- El JCE de apoyo debe registrar los eventos de acceso para cada credencial, garantizando la trazabilidad y mejorando la seguridad.

- API y SDK disponibles para la plataforma MobileID

2 Arquitectura del sistema

2.1. Integración de microservicios con Feign Client y plantillas

Aprovechando la potencia de Feign, la plataforma simplifica las complejas interacciones API, mejora la legibilidad del código y la fiabilidad general del sistema. La solución propuesta proporcionará una capa de integración sin fisuras, permitiendo una comunicación eficiente y el intercambio de datos entre microservicios y sistemas heredados

Visión general de alto nivel del proceso:

- **Definir interfaces de cliente falsas:**
  - Cree interfaces Java para representar las API del servicio remoto.
  - Anote los métodos de la interfaz con los métodos HTTP apropiados (GET, POST, PUT, DELETE) y los parámetros de solicitud/respuesta.

- **Crear plantillas falsas:**
  - Defina plantillas para encapsular patrones comunes en las llamadas a la API, como la construcción de URL, cabeceras y parámetros de consulta.
  - Utilice variables de plantilla para parametrizar las solicitudes, haciéndolas flexibles y reutilizables.
- **Configurar clientes falsos:**
  - Especifique la URL base del servicio remoto.
  - Configure la gestión de errores, los reintentos y otros ajustes del lado del cliente.
  - Integración con mecanismos de equilibrio de carga para distribuir el tráfico entre varias instancias del servicio remoto.
- **Invocación al Servicio:**
  - Inyecte clientes Feign en sus microservicios.
  - Invoca servicios remotos llamando a métodos de la interfaz de cliente Feign, pasando los parámetros necesarios a las plantillas.

- Feign gestiona las peticiones HTTP subyacentes, incluida la construcción de URL, la serialización de petición/respuesta y la gestión de errores.

Principales ventajas de utilizar el cliente falso y las plantillas:

- **Consumo simplificado de la API:** Feign abstrae la complejidad de las peticiones HTTP.
- **Enfoque declarativo:** Define las API mediante interfaces Java, lo que mejora la legibilidad y el mantenimiento del código.
- **Reutilización:** Las plantillas pueden reutilizarse en varios clientes Feign, lo que reduce la duplicación de código.
- **Flexibilidad:** Personaliza fácilmente las peticiones pasando parámetros a las plantillas.
- **Mecanismos de tratamiento de errores y reintentos:** Soporte integrado para la gestión de errores, reintentos y disyuntores.
- **Equilibrio de carga:** Integración con mecanismos de equilibrio de carga para un rendimiento óptimo.

Al aprovechar Feign Client y las plantillas, la plataforma puede integrar eficazmente microservicios con sistemas locales, fomentando la modularidad, la escalabilidad y la capacidad de mantenimiento.

2.2. Normas de seguridad de la plataforma:

Normas de seguridad de la plataforma VeriGO MobileID

Norma de seguridad	Protocolos
Clave simétrica	AES: 128, 256 Longitudes de clave configurables.
Clave asimétrica	RSA: 2048, 4096 Longitudes de clave configurables. ECC: 256, 384, 521 Longitudes de clave configurables.
Resumen de mensajes	SHA: 256,384, 512 Bits configurables.
mID/mDL Estándar	Permiso de conducir conforme a ISO/IES 18013-5-ISO.
Código de autenticación del mensaje	HMAC: SHA-256, SHA-384, SHA-512 Bits configurables.

Https seguros	TLS: v1.3 v1.2 están configurados con suites de cifrado fuertes.
Autenticación y verificación multifactoriales	Orden precedente: FIDO2 - PUSH - PKI - OTP - Código QR.

Directrices de seguridad de la plataforma VeriGO MobileID

Normas	Acciones
Datos cifrados en tránsito	Activar el cifrado de la capa de transporte TLS 1.3 o TLS 1.2.
SSO MFA y verificación	Habilite la autenticación multiactor: FIDO2, PUSH, PKI, OTP, código QR
Proteger el acceso a aplicaciones y puntos finales	Es obligatorio acceder a todos los puntos finales y a la aplicación mediante tokens JWT válidos a través de OAUTH o claves de acceso a la API.
Controles de acceso basados en funciones	Aplicar políticas y gobernanza para limitar el acceso de los usuarios en función de la función asignada es fundamental .
Desconfiguración de la seguridad	Aplique las configuraciones sólo después de revisarlas y aprobarlas mediante la comprobación del cumplimiento de la seguridad .
Prevención de la pérdida de datos	Copias de seguridad frecuentes en cintas para mitigar la pérdida de datos y respaldar el BCP (Business Continuity Plan) .
Comprobación de seguridad antes de la implantación	Asegure la infraestructura y la red antes del despliegue : VPN, inicio de sesión con clave SSH.
Registro y control	Habilitar el registro de aplicaciones que ayudaría en caso de compromiso.

Tal y como se define en la norma ISO/IEC 18013-5, VeriGO MobileID proporciona canales de comunicación cifrados para las transacciones de identidad a través de NFC y BLE. Tanto la autenticación de datos como el cifrado de sesiones se realizan utilizando ES256 (ECDSA con SHA-256), ES384 (ECDSA con SHA-384) y AES-256.

Cifrado de datos: Todos los datos transferidos hacia y desde la aplicación son seguros y no pueden ser accedidos por partes no autorizadas, incluyendo Veridos. La aplicación sólo recoge y almacena la

información esencial necesaria para su funcionamiento, evitando la recopilación innecesaria de datos.

- Se facilitan políticas de privacidad transparentes y comprensibles que detallan cómo se utilizan, almacenan y protegen los datos de los usuarios.
- El derecho al olvido: permite a los usuarios que lo soliciten borrar completamente sus datos de la aplicación.
- Dentro de la aplicación, los datos del usuario sólo se almacenan durante el periodo necesario para el fin con el que se recogieron.

Autenticación segura: Implanta mecanismos de autenticación fuertes, como la autenticación multifactor.

Control de acceso: Aplique estrictos controles de acceso para proteger los datos confidenciales.

Auditorías de seguridad periódicas: Realice auditorías de seguridad periódicas para identificar y abordar las vulnerabilidades.

Cumplimiento de la normativa: Adherirse a la normativa pertinente sobre protección de datos (por ejemplo, GDPR, CCPA).

2.3. Consideraciones generales sobre el hardware para dimensionar la infraestructura

Servidores:

- **Servidores de aplicaciones**
  - CPU de alto rendimiento de 64 núcleos (por ejemplo, Intel Xeon o AMD EPYC)
  - RAM (por ejemplo, 128 GB o más)
  - Alta capacidad de almacenamiento rápido SSD para archivos de aplicaciones y datos con al menos 500 GB de almacenamiento.
  - Equilibradores de carga para distribuir el tráfico entre varios servidores
- **Servidores de bases de datos**
  - CPU de alto rendimiento de 32 núcleos (por ejemplo, Intel Xeon o AMD EPYC)

CONSORCIO EMDOC Santo Domingo, R.D.

- RAM (por ejemplo, 64 GB o más)
- Alta capacidad de almacenamiento rápido SSD para archivos de aplicaciones y datos con al menos 1 TB de almacenamiento.
- Técnicas de optimización de bases de datos (por ejemplo, indexación, optimización de consultas)

- **Servidores de autenticación**
  - CPU de alto rendimiento de 16 núcleos (por ejemplo, Intel Xeon o AMD EPYC)
  - RAM (por ejemplo, 32 GB o más)
  - Alta capacidad de almacenamiento rápido SSD para archivos de aplicaciones y datos con al menos 100 GB de almacenamiento.
  - Técnicas de optimización de bases de datos (por ejemplo, indexación, optimización de consultas)

Infraestructura de red:

- **Red de alta velocidad**
  - Red Gigabit Ethernet o 10GbE para una transferencia de datos de alto rendimiento
  - Conmutadores y enrutadores de red con baja latencia y gran ancho de banda
- **Equilibradores de carga:** Distribuye el tráfico de red o de aplicaciones entre varios servidores para mejorar el rendimiento, la fiabilidad y la escalabilidad.
- **Cortafuegos:**
  - Proteger el sistema de accesos no autorizados y ciberamenazas.

Almacenamiento de alto rendimiento

- Unidades SSD o NVMe para un acceso rápido a los datos
- Configuraciones RAID para redundancia y rendimiento

Copias de seguridad y recuperación en caso de catástrofe

- Copias de seguridad periódicas para garantizar la integridad de los datos y la continuidad de la actividad

- Plan de recuperación en caso de catástrofe para minimizar el tiempo de inactividad en caso de avería

2.4. Consideraciones adicionales

Almacenamiento en caché: Implemente mecanismos de almacenamiento en caché para reducir la carga de la base de datos y mejorar los tiempos de respuesta.

Pruebas de carga: Realice pruebas de carga rigurosas para identificar cuellos de botella en el rendimiento y optimizar el sistema.

Supervisión y alertas: Configure herramientas de supervisión para realizar un seguimiento del rendimiento del sistema y abordar los problemas de forma proactiva.

Seguridad: Aplique medidas de seguridad sólidas para proteger los datos confidenciales de los usuarios.

Escalabilidad: Diseñe el sistema de forma que sea escalable para adaptarse al crecimiento futuro.

2.5. Método de despliegue: Multi-Host On-Premise - Contenedores Docker

Visión general

Este método de despliegue utiliza servidores físicos o virtuales en un centro de datos, extendiendo la contenedorización a múltiples hosts. Este enfoque proporciona un mayor control y optimización, ya que las tareas se ejecutan localmente antes de enrutarse en línea.

Alcance y escalabilidad:

Para llevar a cabo esta implantación, se necesitarán los siguientes servidores (virtuales o físicos):

1. **Servidor de bases de datos**
2. **Servidor de autenticación**
3. **Servidor de aplicaciones**

Cada servidor requiere una configuración de hardware específica. La Plataforma proporcionará opciones de hardware básicas y recomendadas para garantizar la escalabilidad y la capacidad de gestionar un aumento del tráfico.

Requisitos de hardware recomendados:

1. **Servidor de base de datos:**

Recomendado: 64 GB de RAM, 1 TB de disco duro, sistema operativo Linux (Ubuntu 22.04 o Red Hat 8/9.3)

2. **Servidor de autenticación:**

Recomendado: 32 GB de RAM, 100 GB de disco duro, sistema operativo Linux (Ubuntu 22.04 o Red Hat 8/9.3)

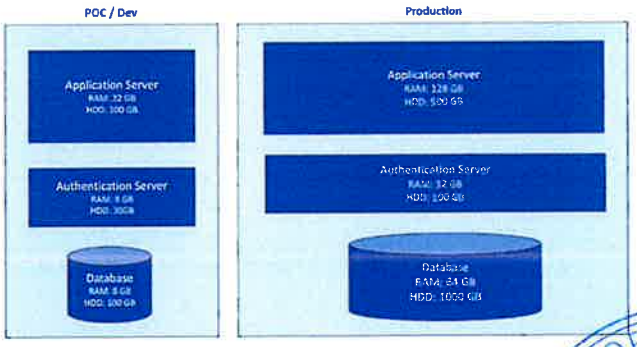
3. **Servidor de aplicaciones:**

Recomendado: 128 GB de RAM, 500 GB de disco duro, sistema operativo Linux (Ubuntu 22.04 o Red Hat 8)

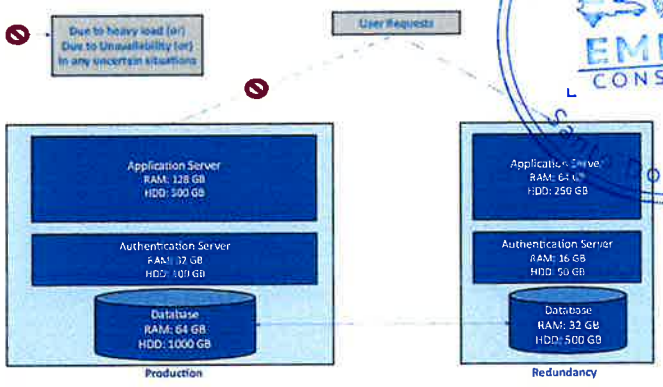
Modelos de infraestructura:

Al adherirse a estas especificaciones, el método de despliegue multihost on-premise garantizará un rendimiento, una escalabilidad y un control sólidos, adaptados para satisfacer las demandas de su infraestructura. A continuación encontrará ejemplos de los modelos POC, Producción, Redundancia y Recuperación ante desastres:

POC/Modelo de producción:

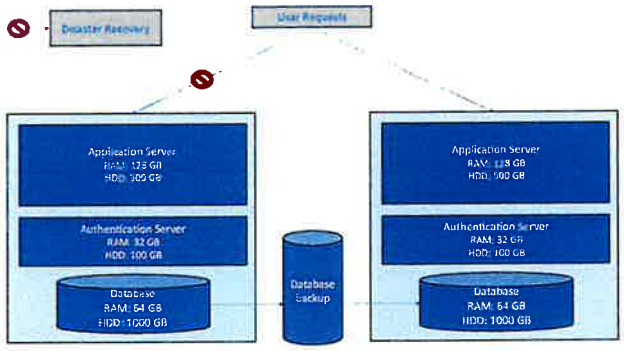


Modelo de redundancia:



EMDOC CONSORCIO

Modelo de recuperación en caso de catástrofe:



2.6. Proceso de actualización local para Docker

Proceso de actualización de Docker local

Objetivo:
Garantizar una actualización fluida de Docker con una interrupción mínima de los servicios.

Preparación:

1. **Haga una copia de seguridad de los datos esenciales:**
   Antes de la actualización, hay que hacer una copia de seguridad de todos los datos y configuraciones esenciales para garantizar que puedan restaurarse en caso necesario.
2. **Notificar a las partes interesadas:**
   Informe a todas las partes interesadas de la actualización programada, incluidos los plazos previstos y las posibles interrupciones del servicio.

Pre-Check:

1. **Confirme la versión actual de Docker:**
   Verifique la versión de Docker existente para comprender el alcance de la actualización.
2. **Revise los cambios de la nueva versión:**
   Evalúe las notas de la versión y los cambios en la nueva versión de Docker para anticipar cualquier impacto en las operaciones actuales.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo, R.D.

Actualización:

1. **Detener contenedores en ejecución:**
   Detenga de forma segura todos los contenedores activos para evitar la corrupción de datos durante el proceso de actualización.

2. **Actualice Docker:**
   Ejecuta la actualización a la última versión de Docker, siguiendo los procedimientos adecuados para tu sistema operativo.

3. **Verifique la actualización:**
   Confirme que Docker se ha actualizado correctamente comprobando la versión y asegurándose de que todos los componentes funcionan como se espera.

Reiniciar y probar:

1. **Reiniciar Contenedores:**
   Inicia todos los contenedores detenidos previamente para reanudar el funcionamiento normal.

2. **Compruebe la funcionalidad de los servicios:**
   Compruebe que todos los servicios funcionan correctamente revisando los registros del contenedor y realizando pruebas básicas de funcionalidad.

Retroceso (si es necesario):

1. **Revertir versión Docker:**
   Si surge algún problema, vuelva a la versión anterior de Docker utilizando las copias de seguridad.

2. **Restaurar datos:**
   Si es necesario, restaura los datos de las copias de seguridad para asegurarte de que no se ha producido ninguna pérdida de datos.

Finaliza:

1. **Documente el proceso de actualización:**
   Registre todo el proceso de actualización, anotando los problemas encontrados y cómo se resolvieron.

2. **Notificar a las partes interesadas:**
   Comunique a las partes interesadas que se ha completado la actualización y facilite cualquier detalle o medida de seguimiento pertinente.

Despliegue azul-verde (local) - Estrategia de actualización

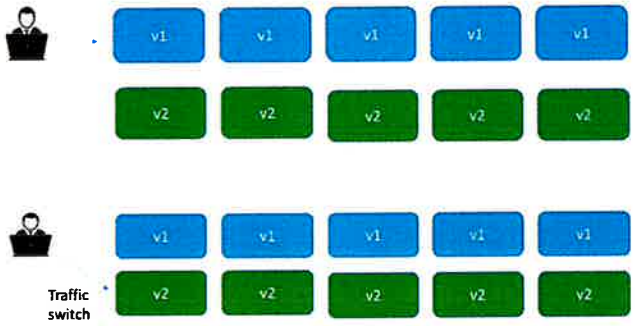
Blue-Green Deployment es una estrategia para lanzar nuevas versiones de software con un tiempo de inactividad y un riesgo mínimos. Requisito previo: Se utilizan dos entornos idénticos:

- **Entorno Azul:** La versión actual en vivo (por ejemplo, la versión 1.0.1 del servicio IAM) a la que acceden los usuarios.
- **Entorno verde:** La nueva versión (por ejemplo, la versión 1.0.2 del servicio IAM) que está lista pero aún no está en funcionamiento.

Pasos de actualización Ejemplo:

1. **Configuración actual:** La versión 1.0.1 está activa y atendiendo a los usuarios.
2. **Nueva versión desplegada:** La versión 1.0.2 está desplegada pero aún no sirve a los usuarios.
3. **Cambiar el tráfico:** Una vez que se confirma que la versión 1.0.2 funciona correctamente, se activa y los usuarios son redirigidos a ella.
4. **Monitor:** Si todo funciona según lo previsto, se elimina la versión antigua (1.0.1).
5. **Fallback:** Si hay problemas, el tráfico vuelve a la versión 1.0.1.

Modelo de reserva:



2.7. Mantenimiento de la Plataforma

Visión general

El mantenimiento de la plataforma de Mobile ID en un entorno local es fundamental para garantizar la fiabilidad del sistema, la escalabilidad y un tiempo de inactividad mínimo. En esta sección se describen procedimientos estructurados que abarcan la redistribución de servicios, las actualizaciones de clústeres Kubernetes, el escalado automático de nodos de trabajadores y las copias de seguridad de bases de datos. Estos procesos están diseñados para mantener la eficiencia operativa al tiempo que se minimizan las interrupciones del servicio.

Redistribución de servicios

Los servicios de Mobile ID utilizan una estrategia de despliegue Blue-Green para garantizar transiciones de servicio fluidas con un tiempo de inactividad mínimo. Cada servicio mantiene dos configuraciones de implantación con distintas versiones de imagen almacenadas en un registro de contenedores interno. Para IAM, ConfigServer y WebUI, las configuraciones de implantación hacen referencia a diferentes versiones de imagen. Cualquier cambio en la configuración, los certificados, las imágenes base o la funcionalidad requiere la reconstrucción de la imagen más reciente utilizando el archivo Docker, enviándola al registro interno y desplegándola mediante un script de

redespliegue. Las actualizaciones se gestionan mediante modificaciones del archivo YAML. La misma estrategia de despliegue se aplica a los servicios CMS, UserManagement y Gateway para garantizar la coherencia y los despliegues controlados.

Actualizaciones del clúster Kubernetes

Para mantener la estabilidad y la seguridad de Kubernetes, el proceso de actualización del clúster sigue metodologías de actualización no disruptivas. Las actualizaciones pueden realizarse mediante herramientas nativas de Kubernetes, como kubectl, kubeadm o la automatización de Ansible. Estas actualizaciones garantizan que las versiones de Kubernetes permanezcan actualizadas sin afectar a las cargas de trabajo en ejecución. Los administradores pueden modificar los archivos de configuración para gestionar eficazmente los cambios de versión, manteniendo la estabilidad del clúster y el cumplimiento de las normas de seguridad.

Autoescalado del nodo de trabajo

El autoescalado se implementa para ajustar dinámicamente la asignación de recursos, garantizando la optimización de costes y el rendimiento del sistema. El servidor de métricas recopila datos de CPU y memoria en tiempo real para facilitar una supervisión eficaz. El Cluster Autoscaler añade automáticamente nodos trabajadores cuando los pods permanecen en estado pendiente debido a recursos insuficientes.

El autoescalado de pods ajusta dinámicamente el número de réplicas por microservicio en función de la CPU, la memoria o métricas personalizadas. El autoescalado horizontal de pods (HPA) garantiza que siempre haya disponible un mínimo de dos réplicas, al tiempo que aumenta la escala a medida que aumenta la demanda. Las políticas de escalado definen las tasas de adición y eliminación de pods, con ventanas de estabilización que garantizan ajustes suaves. El escalado automático se activa cuando la utilización de la CPU o la memoria supera el 75%, lo que evita la degradación del rendimiento.

Copia de seguridad y recuperación de bases de datos

Las estrategias de copia de seguridad de bases de datos se gestionan mediante scripts de automatización y herramientas de gestión de la configuración como Ansible o Terraform para garantizar la integridad de los datos y las capacidades de recuperación.

Protección contra el borrado: Se aplican medidas de protección contra el borrado para evitar el borrado accidental de la base de datos.

Configuración de instantáneas: Se toman instantáneas automáticas antes de finalizar la base de datos, lo que garantiza que las copias de seguridad sigan estando disponibles.

Retención de copias de seguridad: Las copias de seguridad se conservan durante siete días, con una ventana de copia de seguridad diaria que minimiza la posible pérdida de datos.

En caso de fallo, se puede crear una nueva instancia de base de datos a partir de la instantánea más reciente. Las actualizaciones de los registros DNS internos

garantizan una redirección sin problemas a la nueva instancia de base de datos. El proceso de restauración implica la identificación de la última instantánea, la recreación de la base de datos y la actualización de las configuraciones DNS para reflejar el nuevo punto final.

Siguiendo estos procedimientos de mantenimiento, la plataforma Mobile ID garantiza una alta disponibilidad, escalabilidad y una sólida protección de los datos. El enfoque estructurado del despliegue, las actualizaciones, el autoescalado y las copias de seguridad garantiza la continuidad operativa con un impacto mínimo en los usuarios finales. Estos procesos contribuyen a la fiabilidad de la plataforma, reduciendo el tiempo de inactividad y optimizando el rendimiento del sistema.

2.8. Análisis de interfaces y plan de pruebas para interfaces de comunicación

Análisis de interfaces y plan de pruebas para interfaces de comunicación

Reconocemos la necesidad de un análisis exhaustivo y un plan de pruebas para garantizar el éxito del ajuste y la integración de las interfaces de comunicación propuestas por el CCE. Nuestro enfoque está diseñado para proporcionar una evaluación exhaustiva de la arquitectura de interfaz, garantizando el cumplimiento, la interoperabilidad y el rendimiento, al tiempo que aborda los posibles desafíos durante la fase de implementación.

Enfoque del análisis de interfaces

Nuestra metodología de análisis de interfaces se centra en comprender los requisitos, evaluar la compatibilidad e identificar los posibles problemas de integración. Los pasos clave de nuestro enfoque incluyen:

1. **Recopilación de requisitos:**
   - Revisar las especificaciones propuestas para la interfaz de comunicación del JCE.
   - Identificar las dependencias técnicas y los puntos de contacto de integración.
   - Cumplir las normas del sector, como ISO/IEC 18013-5, y las directrices del NIST.
2. **Evaluación de interfaces:**
   - Evalúe la estructura de la interfaz (API RESTful, OIDC, SAML, colas de mensajes, etc.).
   - Analizar formatos de datos (JSON, XML, etc.) y protocolos de comunicación (HTTPS, NFC, BLE).

- Identificar posibles problemas de interoperabilidad con los sistemas existentes.

3. **Evaluación de la seguridad:**
   - Realizar una evaluación de riesgos para identificar posibles vulnerabilidades en el proceso de intercambio de datos.
   - Garantizar el cumplimiento de los requisitos de cifrado, autenticación y control de acceso.
4. **Consideraciones sobre escalabilidad y rendimiento:**
   - Evalúe la capacidad de la interfaz para gestionar grandes volúmenes de solicitudes.
   - Evalúe la latencia, los tiempos de respuesta y el consumo de recursos.

Plan de pruebas para el ajuste de la interfaz

Nuestro plan de pruebas propuesto esboza un enfoque estructurado para validar la integración de la interfaz, garantizando que la funcionalidad, la seguridad y el rendimiento cumplen las normas deseadas. El plan de pruebas incluye:

Objetivos de la prueba

- Validar la comunicación fluida entre sistemas.
- Garantizar la integridad y exactitud de los datos.
- Verificar el cumplimiento de los requisitos del JCE y de las normas aplicables.
- Identifique posibles cuellos de botella y optimice el rendimiento del sistema.

Fases de prueba

Pruebas unitarias:

- Aislar y probar los componentes individuales de la interfaz.
- Valide los puntos finales de la API, los formatos de solicitud/respuesta y la gestión de errores.

Pruebas de integración:

- Garantizar una interacción fluida entre nuestro sistema y la interfaz JCE.
- Verificar la corrección del mapeo y la transformación de datos.
- Pruebe la interoperabilidad con sistemas de terceros.

CONSORCIO EMDOC Santo Domingo, RD

Pruebas funcionales:

- Evaluar los flujos de trabajo de extremo a extremo que implican el intercambio de datos entre sistemas.
- Confirmar la correcta gestión de la autenticación de usuarios, el control de acceso y los registros de transacciones.

Pruebas de seguridad:

- Realizar pruebas de penetración para identificar vulnerabilidades.
- Validar el cifrado de datos en tránsito y en reposo.
- Evaluar los mecanismos de autenticación y autorización.

Pruebas de rendimiento:

- Realizar pruebas de carga para medir la respuesta del sistema bajo cargas máximas.
- Realizar pruebas de estrés para determinar los límites del sistema.
- Evalúe los tiempos de respuesta y el rendimiento.

Pruebas de aceptación del usuario (UAT):

- Colaborar con las partes interesadas para validar la alineación de los procesos empresariales.
- Recoger opiniones para perfeccionar las interacciones de la interfaz.

Definición de escenarios de prueba

Nuestros escenarios de pruebas están diseñados para cubrir una amplia gama de casos de uso, lo que garantiza una validación exhaustiva de la funcionalidad de la interfaz:

Escenarios de intercambio de datos:

- Recuperación satisfactoria de datos de los sistemas JCE (por ejemplo, solicitudes de verificación de la identidad de los ciudadanos).
- Envío de datos a los sistemas JCE (por ejemplo, solicitudes de emisión de documentos).
- Tratamiento de entradas de datos incorrectas o incompletas.

Escenarios de gestión de errores:

- Mecanismos de tiempo de espera y reintento durante los fallos de comunicación.
- Uso incorrecto de la API (por ejemplo, tokens de autenticación no válidos).
- Tratamiento de casos extremos y entradas inesperadas.

Escenarios de seguridad:

- Intentos de acceso no autorizados.
- Gestión y expiración de sesiones.
- Cumplimiento del GDPR y otros requisitos normativos.

Escenarios de rendimiento:

- Pruebas con usuarios simultáneos accediendo al sistema.
- Medición de los tiempos de respuesta en transacciones de gran volumen.
- Evaluación del comportamiento del sistema durante la latencia de la red.

Entregables

Como parte de nuestra respuesta, proporcionaremos los siguientes entregables para apoyar el proceso de ajuste de la interfaz:

Informe exhaustivo de análisis de interfaces:

- Resumen de conclusiones y recomendaciones.
- Identificación de riesgos de integración y estrategias de mitigación.

Documento detallado del plan de pruebas:

- Plan de ejecución paso a paso para cada fase de las pruebas.
- Criterios de aceptación para una integración satisfactoria.

Informes de ejecución de pruebas:

- Resultados de los casos y escenarios de prueba realizados.
- Puntos de referencia de rendimiento y seguimiento de problemas.

Confiamos en que nuestro enfoque garantice un proceso de integración fluido y eficaz, manteniendo al mismo tiempo los más altos niveles de calidad, seguridad y rendimiento. Esperamos poder colaborar con JCE y ofrecerle más información durante la fase de implantación.

CONSORCIO EMDOC EMDOC CONSORCIO Santo Domingo

Anexo

Apéndice 1- Visión general de la arquitectura de la plataforma

Diagrama de la plataforma de identificación móvil

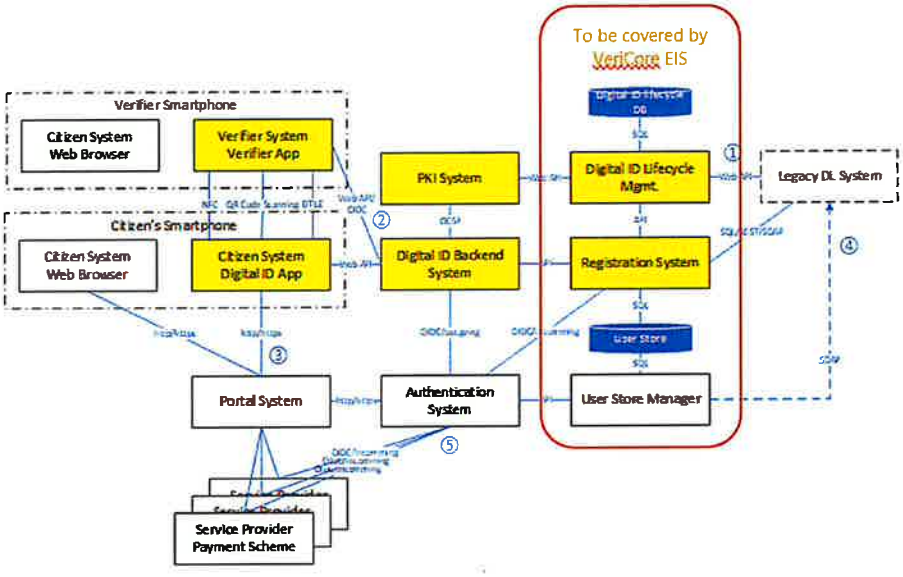
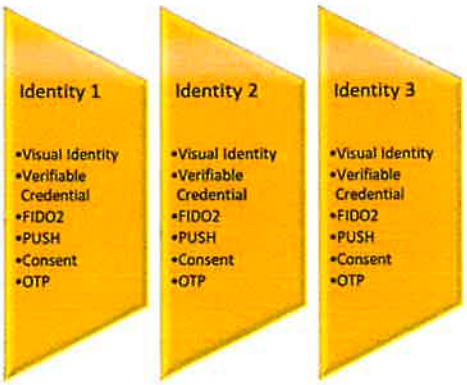
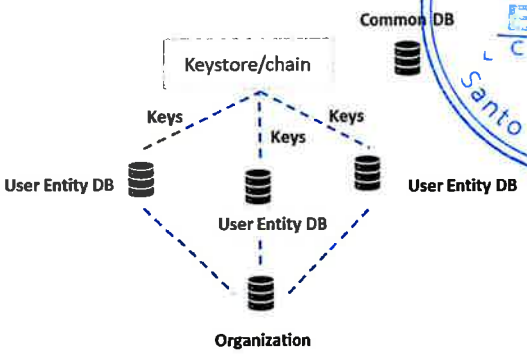


Fig. 1: mID Architecture – Component View

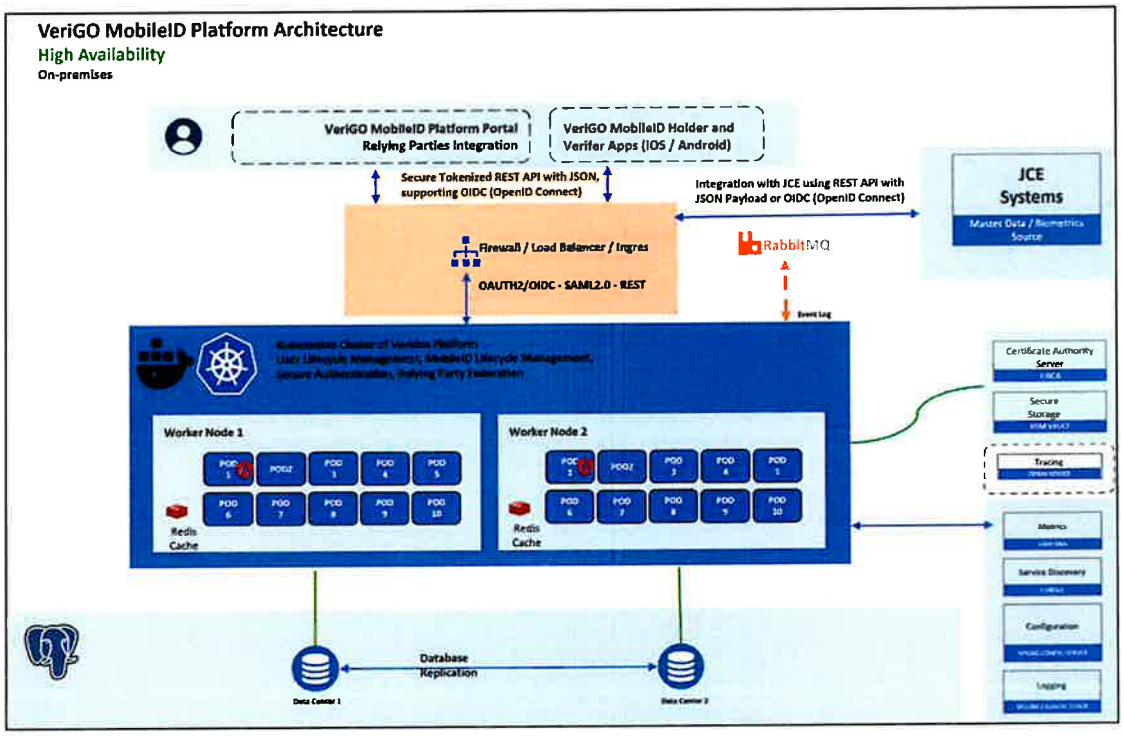
Plataforma ID Cartera Ilustración de credencial independiente dentro de la misma cartera.





EMDOC CONSORCIO

Integración con el sistema heredado JCE



La plataforma se ajusta a las normas internacionales pertinentes:

- Certificación ISO/IEC 18013-5 y compatibilidad con ISO/IEC 18013-7 en permisos de conducir móviles y otros casos de uso de mDoc como certificaciones, diplomas, matriculación de vehículos, etc.
- Directrices de implantación del mID/mDL de la AAMVA
- Norma del W3C sobre credenciales verificables

Tecnologías utilizadas en la plataforma VeriGO MobileID

Normas	Acciones
Inquilino a bordo	Proceso de aprovisionamiento gestionado internamente
Microservicio Spring Boot	- OpenJDK 8/17 - Config-server- añadir o eliminar tenant - URI Endpoints- incluir identificador de inquilino

Base de datos: (Compartida)	- Postgres v15.1 - RLS (Row Level Separation) en la base de datos - Todas las tablas con datos PII o de inquilinos contienen la columna de identificación del inquilino
Protocolos	OIDC, SAML 2.0, OAuth2.0, LDAP-AD, SCIM 2.0
Credenciales	Credencial verificable, FIDO2, PUSH(Consentimiento), PKI, OTP
Infraestructura	En las instalaciones / AWS en la nube

- Auditorías de seguridad periódicas: Se llevarán a cabo auditorías de seguridad periódicas para identificar y abordar las vulnerabilidades.
- Cumplimiento de la normativa: El sistema cumplirá la normativa pertinente sobre protección de datos, como el GDPR, para garantizar la privacidad de los usuarios.

Apéndice 2 Ejemplo de caso de prueba

Los casos de prueba de la plataforma móvil de identificación proporcionados se utilizan actualmente en nuestros calendarios de pruebas para la plataforma en relación con el uso de la misma, las pruebas de regresión cuando se añaden nuevas funciones y cuando se desarrolla la documentación para su uso a nivel de usuario, agente y administración. Nuestro enfoque, tal y como se ha explicado anteriormente, se dirigirá hacia el éxito del despliegue, mantenimiento, seguridad y rendimiento de la plataforma con la colaboración del JCE.

A continuación se ofrece un ejemplo del formato y los casos de prueba actuales que se tendrán en cuenta durante la transferencia de conocimientos

Información de cabecera

- **Nombre/Título del proyecto**: Indique claramente el nombre de la licitación o del proyecto.
- **Número de referencia de la licitación**: Incluya el número de referencia para facilitar su identificación.
- **Versión del documento del caso de prueba**: Menciona la versión para gestionar las actualizaciones.
- **Fecha**: Especifique la fecha de presentación del caso de prueba.

- **Preparado por**: Identifique al agente o departamento que proporciona los casos de prueba.

Visión general

- **Objetivo**: Indicar el propósito de los casos de prueba, como validar entregables específicos, garantizar el cumplimiento de requisitos funcionales o confirmar especificaciones no funcionales.
- **Alcance**: Definir el alcance de las pruebas, incluidos los límites y las exclusiones.
- **Supuestos/Dependencias**: Enumere las suposiciones o dependencias que deben existir para que se ejecuten las pruebas.

Detalles del caso de prueba

El formato tabular es la forma más habitual y eficaz de presentar los casos de prueba:

Issue Key	Test Summary	Execution Status	Order	Step	Expected Result	Step Result
EN-1766	Error message for Maximum number of allowed devices	PASS	1	Click on signin	Application Signin Page has to display	PASS
			2	Enter the Email address and click on signin	Password page has to display	PASS
			3	Enter the password and click on next	Dashboard page has to display	PASS
			4	Click on Management and click on mobile credentials holder	List of mobile credentials holders has to display	PASS
			5	Click on search box, select the email address checkbox, enter the email address and click on search icon	selected user has to display	PASS
			6	Click on issue identity Icon	Issue mobile credential page has to display	PASS
			7	Click on VD ID Wallet	It will display the error message as you have reached a maximum number of allowed devices.	PASS

Entorno de pruebas

- **Requisitos de hardware**: Mencione cualquier hardware específico necesario para las pruebas.
- **Requisitos de software**: Incluye sistemas operativos, herramientas o librerías necesarias para la ejecución.
- **Requisitos de red/conectividad**: Especifique si se necesita Internet, protocolos específicos o configuraciones.

Entregables

- Una lista de los resultados esperados de la fase de pruebas, por ejemplo:
  - Informes de ejecución de casos de prueba.
  - Capturas de pantalla, registros u otras pruebas de validación.
  - Informes de defectos, si procede.

Criterios de aceptación

- Definir los criterios de aceptación de los casos de prueba o de los resultados de las pruebas.
- Especifique parámetros de rendimiento, porcentajes mínimos de aprobados o umbrales de cumplimiento.

Notas/Instrucciones

- Incluya notas o instrucciones especiales para los revisores.

Si sigue una norma específica (por ejemplo, ISO, ISTQB), menciónela.