

5. PLATAFORMA DIGITAL PARA CÉDULAS



Para garantizar la autenticidad, integridad y seguridad de los documentos electrónicos dentro del nuevo sistema de cédulas de identidad, el **Consorcio IDSecure IDS** ha seleccionado a **TOPPAN**



SECURITY SAS (antiguo HID Global) como proveedor de la Infraestructura de Clave Pública (PKI), implementando su solución **GoID**. **GoID** es una plataforma avanzada de identidad digital que permite la emisión segura de certificados digitales, la gestión de claves criptográficas y la autenticación de identidad en entornos físicos y digitales. Esta tecnología cumple con los estándares internacionales establecidos por la OACI (Doc 9303), ISO 15408 y eIDAS, asegurando la interoperabilidad, seguridad y confiabilidad del sistema.

5.1 GoID™: Introducción de Identidad Móvil Nacional

La solución de identidad digital **gold** consiste en una **SDK** que facilita la generación de un documento digital de alta seguridad en el dispositivo móvil del usuario, representando una alternativa conveniente, segura e instantánea a los documentos de identificación físicos tradicionales. Utilizando avanzados algoritmos de cifrado de datos y estrictas medidas de seguridad en la comunicación, **gold** reduce significativamente el riesgo de robo de identidad y mejora la privacidad de los ciudadanos.

GoID convierte un dispositivo móvil en un medio confiable para la verificación de identidad, eliminando la necesidad de portar documentos físicos que pueden ser perdidos, robados o falsificados. Esta solución aprovecha la tecnología de vanguardia para garantizar que solo el propietario legítimo del dispositivo pueda acceder a su identidad digital, proporcionando una capa adicional de seguridad.

Los robustos algoritmos de cifrados empleados por **gold** aseguran que los datos de identidad estén protegidos en todo momento, tanto en almacenamiento como en tránsito. Esto significa que cualquier intento de interceptar o manipular los datos será infructuoso, manteniendo la integridad y confidencialidad de la información del usuario.

Además, las medidas de seguridad de comunicación implementadas por **gold** garantizan que cada transacción y verificación de identidad se realice de manera segura. Estas medidas incluyen autenticación de dos factores, biometría y otras tecnologías avanzadas que hacen que la falsificación o el acceso no autorizado sean prácticamente imposibles.

La adopción de **gold** no solo mejora la seguridad, sino que también simplifica el proceso de verificación de identidad, haciendo que sea más rápida y eficiente. Esto es especialmente útil en situaciones donde la verificación rápida de identidad es crucial, como en el acceso a servicios gubernamentales, financieros y de salud.



GoID representa el futuro de la identidad digital, combinando seguridad avanzada, conveniencia y eficiencia para ofrecer una solución robusta que protege la identidad de los ciudadanos y facilita su uso en la vida cotidiana.

5.1.1 Características Generales

De acuerdo con el Pliego de Especificaciones, ITEM VI - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL. Nuestra solución es diseñada para cumplir con los requisitos y criterios técnicos, asegurando cumplimiento con el Doc. 9303 de la OACI.

Es parte el alcance de suministro, software, hardware, licencias y cualquier otro requisito necesario para implementar el servicio de identificación digital en dispositivos móviles y cumplir con los estándares ISO18013-5. Estamos conscientes del “Guiding Core Principles for the Development of Digital Travel Credential (DTC) de octubre de 2020” y nuestra solución es también compatible con la implementación de DTC. La solución implementada será escalable y optimizable para adaptarse a la evolución de la demanda de este tipo de documentos.

Se implementará la solución de identidad digital dentro de un plazo menor al de 4.5 meses, después de la firma del contrato. Esta solución será administrada por la JCE e integrada al sistema nacional de identidad mediante el uso de API's para la identificación y verificación de la identidad de los ciudadanos. La tarjeta digital podrá ofrecer (si las leyes lo permiten) las mismas garantías jurídicas al titular que el CEI o CI.

El Consorcio será responsable del desarrollo y exposición de las APIs necesarias para la integración del sistema de identidad digital con la infraestructura de la JCE, asegurando la interoperabilidad con las bases de datos existentes en SQL Server 2022 y siguiendo el modelo de arquitectura cliente-servidor.

Los datos son entregados firmados electrónicamente por la JCE. Esta firma electrónica certificada permitirá que terceros validen tanto la integridad como la procedencia de los datos presentados por el ciudadano. Tanto la firma de los datos como su validación se realizarán utilizando los certificados electrónicos administrados por la JCE, como Autoridad Certificadora descrita en el apartado de Infraestructura de Clave Pública.



5.1.2 Aspectos de la Tarjeta Digital

De acuerdo con el Pliego de Especificaciones, ITEM VI - ESPECIFICACIONES TÉCNICAS TARJETA DE IDENTIDAD DIGITAL. La solución de Tarjeta Digital cumple con las siguientes características:

- La solución incluye el sistema de gestión del ciclo de vida de las credenciales digitales, de forma que se registren los eventos de acceso a cada credencial, así como proporcionar las aplicaciones o interfaces necesarias para la implantación de nuevas soluciones.
- La solución incluye un canal de comunicación que utiliza algoritmos de cifrado para conectar los dispositivos y ejecutar el proceso de verificación. Dependiendo del caso de uso y de la disponibilidad del dispositivo, se emplean protocolos NFC (Near Field Communication) y/o BLE (Bluetooth Low Energy), asegurando siempre el cumplimiento de la norma ISO 18013-5.
- La solución tiene las funciones de recepción, almacenamiento y protección segura de credenciales digitales en aplicaciones móviles, así como el uso de notificaciones PUSH para enviar mensajes masivos o personalizados al titular de la credencial digital.
- La solución utilizará durante el proceso de emisión o activación de la identidad digital, el mecanismo de *liveness detection* (prueba de vida), para prevenir ataques de presentación. El mecanismo de *liveness detection* utilizará la plataforma de *liveness* de Magallanes Media que cuenta la certificación ISO 30107-3. Los documentos que acreditan esta certificación se incluyen en esta propuesta.
- La aplicación móvil proporcionará al titular del documento de identidad digital el desbloqueo de la App mediante autenticación de dos factores (2FA).
- La aplicación móvil propuesta funciona sin conexión con la internet, permitiendo la visualización local de los datos de las credenciales digitales, utilizando un método de verificación de la autenticidad de la identidad digital. También tendrá la capacidad de realizar consultas en línea, en caso de que se requiera llevar a cabo algún tipo de verificación de la información del titular de la identidad digital.
- La aplicación móvil permite que la visualización del documento de identidad digital se diseñe según las especificaciones de la JCE, ofreciendo una vista de pantalla completa con las visualizaciones del anverso y reverso al tocar la credencial, y mostrando los mismos datos que el documento de identidad físico. Sin embargo, para prevenir situaciones potenciales de fraude, como el conocido *Flashpass*, donde el portador del documento digital muestra solo una foto del documento en pantalla para hacerse pasar por verdadero, recomendamos que los datos visualizados en las credenciales digitales sean mínimos para reforzar la verificación a través de la app y garantizar su autenticidad.



- La aplicación móvil tiene la capacidad de compartir únicamente la información que el titular de la identidad digital desee compartir, en el momento de la verificación de la identidad.
- Las aplicaciones móviles informarán al titular cuando su identidad digital ha sido revocada, mediante una alerta al entrar en la App, indicando el cambio en la validez de su documento digital.
- La solución propuesta incluye mecanismos de protección contra ataques que incluyan, entre otros, ingeniería inversa, manipulación de código, detección de rooting/jailbreak/debugging, etc.
- La solución propuesta posee capacidad de incorporar información en las imágenes de los solicitantes como medidas de seguridad complementarias.
- Incluir información en imágenes de solicitantes
- La solución permitirá la incorporación de información visual de seguridad en las imágenes de los solicitantes (por ejemplo, marcas de agua, códigos cifrados, etc.).

5.2 Características Técnicas de la solución propuesta

En complemento a los aspectos mencionados anteriormente, la solución cuenta con las siguientes características técnicas:

- **Certificación:** ISO/IEC 18013 Parte 5. La solución ofrecida contará con la certificación ISO/IEC 18013 Parte 5.
- **Herramientas de Desarrollo:** Se hará disponible la SDK y API para uso del personal técnico de la JCE o terceros.
- **Integración de Servicios:** Integrará con los sistemas de identificación de la JCE.
- **Infraestructura PKI:** La solución utilizará la PKI para emisión de documentos digitales (IACA).
- **Aplicaciones Móviles:** La solución será multiplataforma compatibles con iOS y Android.
- **Seguridad:** La solución incluirá protección contra ingeniería inversa y clonación.
- **Activación Remota:** La solución incluirá un mecanismo para activación remota de identidad digital, considerando el tiempo de validez del enlace (unas horas), el mismo se podrá enviar por correo electrónico, mensaje de texto u otro medio a determinar. Se manejará un doble factor de autenticación 2FA.
- **Liveness Detection:** La solución utilizará *liveness detection*, como mencionado anteriormente, para el proceso de activación de identidad digital remota para la prevención de suplantación de identidad. El sistema estará de acuerdo con el estándar de referencia ISO 30107-3, y se presentará certificación de cumplimiento de ISO 30107-3.



- **Alta Disponibilidad:** La plataforma contará con un esquema de alta disponibilidad de servicio.
- **Interoperabilidad:** La plataforma permitirá la interoperabilidad y escalabilidad del servicio para la implementación de diferentes mecanismos de control de dispositivos.
- **Intercambio de Datos:** La aplicación de identidad móvil permitirá intercambio de datos personales iniciado por el titular de acuerdo con la norma ISO/IEC 18013-5.
- **Selección de Datos:** La aplicación de identidad móvil permitirá la selección de campos específicos para compartir y las categorías de campos.
- **Administración de Emisiones:** La solución incluirá el sistema para administración de la emisión de identidades digitales para evidenciar el registro de eventos y accesos, incluyendo las interfaces necesarias para nuevas soluciones.
- **Seguridad de Comunicaciones:** Asegurará todas las comunicaciones entre aplicaciones móviles, incluyendo las interacciones en línea y fuera de línea.
- **Canales de Comunicación:** La solución propuesta utiliza algoritmos de encriptación en canales de comunicación, en detalle en la sección de Componentes.
- **Funcionalidades de App:** La solución proveerá las funciones para recibir, guardar y proteger credenciales digitales. Se demostrará el uso de notificaciones PUSH y almacenamiento seguro.
- **Autenticación:** Las aplicaciones móviles permitirán el desbloqueo de la App mediante autenticación de dos factores (2FA), como mínimo PIN y verificación facial.
- **Funcionalidad Online / Offline:** Las aplicaciones móviles permitirán el funcionamiento offline para visualización de datos y también permitirán consultas en línea.
- **Visualización de Documentos:** Permitirán la visualización de documentos de identificación digital en pantalla completa y el cambio de anverso a reverso, conforme especificado por la JCE.
- **Compartir Información:** Tendrán la capacidad de compartir información seleccionada durante la verificación de identidad.
- **Notificaciones de Revocación:** Informarán al titular sobre la revocación de su identidad digital mediante alertas en la App.
- **Capacidad de Servicio:** Al menos 5,000 solicitudes diarias de credenciales digitales. La solución será modular y escalable para adaptarse a la evolución en la demanda de este tipo de documentos.
- **Interfaces de Comunicación:** Utilizarán e integrarán con interfaces de comunicación existentes para el envío de órdenes de emisión por parte de la JCE.
- **Análisis de Interfaces:** Se proporcionará un plan de análisis y pruebas para el ajuste de interfaces de comunicación propuestas por la JCE, incluyendo la definición de escenarios de prueba.



- **Consistencia de Datos:** Mantendrán la consistencia de estados entre soluciones para el proceso de actualización y sincronización al sistema institucional para la identificación de personas.
- **Disponibilidad de Operación:** Garantizamos disponibilidad del 99.95% durante horas de producción, excepto por razones atribuibles a la JCE.
- **La aplicación permitirá generar un código bidimensional** que contendrá los datos del ciudadano y su respectiva firma electrónica certificada. Además, el usuario podrá seleccionar qué datos compartir a través de dicho código bidimensional, garantizando privacidad y seguridad en el intercambio de información

5.3 App Ciudadana

Dentro del alcance de esta propuesta se incluye el desarrollo y mantenimiento a dos años de lo que se denomina la app ciudadana contenedora de la credencial digital.

La app tendrá las siguientes funcionalidades y características

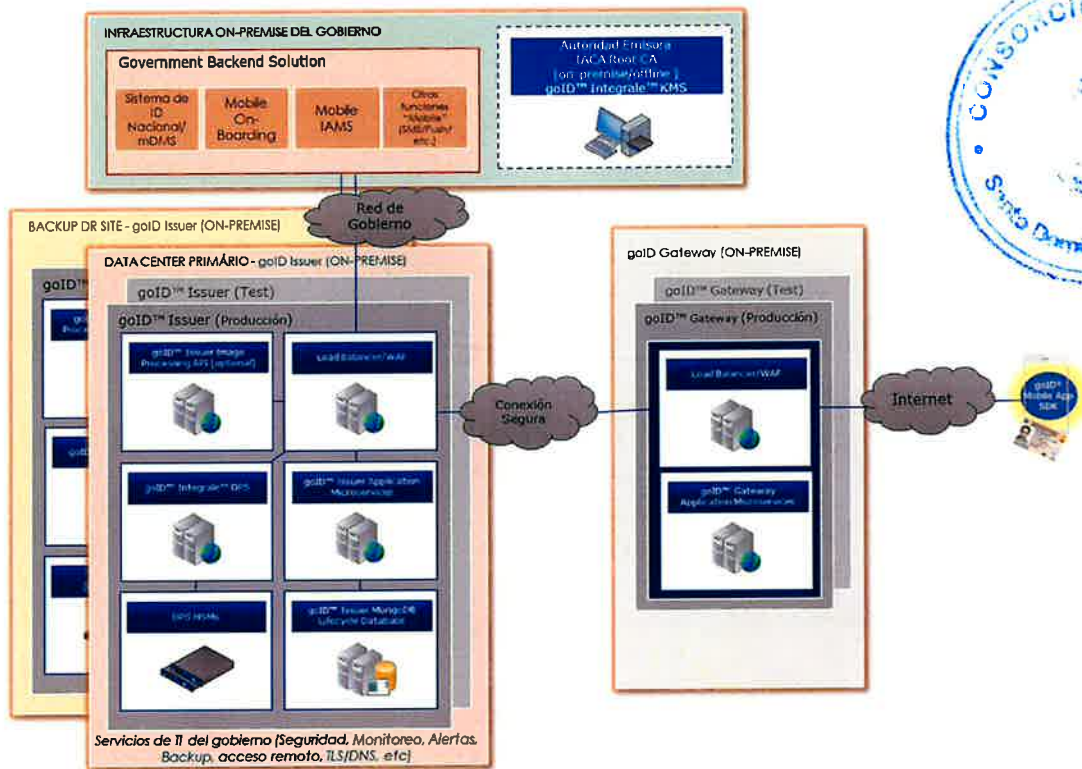
- Integración del SDK goID para poder alojar y verificar la cédula digital
- Flujo de verificación de identidad del ciudadano previo a la solicitud y emisión de la cédula digital. El flujo de provisionamiento de la credencial digital será de la siguiente manera. O a convenir entre el consorcio y la JCE.
 - Enrolamiento y onboarding del ciudadano en la app. Creación de usuario
 - Lectura del MRZ de la cédula física mediante OCR y la cámara del dispositivo móvil.
 - Desbloqueo del chip contactless mediante NFC para Basic Access Control (BAC) y levantar los datos biométricos y biográficos del chip.
 - Verificación biométrica con reconocimiento facial y prueba de vida (liveness detection) entre el usuario tenedor de la app y los datos biométricos del chip contactless en la cédula física. La prueba de vida será pasiva con el sistema de Magallanes Media que cumple con **la certificación ISO/IEC 30107-3**.
 - Emisión y descarga de la cédula digital en base a los datos biométricos y biográficos del chip contactless en la cédula física.
- Módulo para compartir datos de la credencial digital con otros dispositivos verificadores
- Capacidad de actuar como verificador de otras cédulas digitales si la JCE lo desea.
- Diseño gráfico y UI a convenir con la JCE.
- Se incluyen apps para los sistemas operativos Android e iOS.

Mantenimiento correctivo y evolutivo por 24 meses.



5.4 ARQUITECTURA DE LA SOLUCIÓN

El siguiente diagrama resume la Arquitectura del Sistema propuesta para la solución de emisión gold para República Dominicana:



La solución se desplegará en las instalaciones (on-premise) en la infraestructura de TI proporcionada localmente. Esto funcionará en una plataforma de infraestructura de Máquina Virtual (VM) para proporcionar la elasticidad y capacidad de expansión adecuadas.

La solución se desplegará en un Centro de Datos Primario (PDC) y un sitio de Recuperación de Desastres (DR). Dado que hay pocos requisitos definidos sobre el sitio DR, hemos asumido que será una versión offline y simplificada del sitio primario (basada en un solo nodo para la mayoría de los componentes) con replicación básica de la base de datos o, en el peor de los casos, simplemente respaldos que ocurren en el PDC y se restauran en el sitio DR. Este diseño implicaría un cambio manual en caso de emergencia con la redirección del tráfico de Internet del Sitio Primario al sitio DR (a realizarse por el cliente). La solución final que se implementará dependerá mucho de la ubicación del sitio DR, la opción que tenga el cliente para redirigir el tráfico de Internet y la conectividad de red proporcionada.

5.4.1 GoID – Componentes

La solución comprende los siguientes productos de la plataforma de emisión gold:

1. El componente Integrale™ KMS, que actuará como la Autoridad Certificadora de la Autoridad de Emisión ISO 18013-5 (IACA) y será la CA raíz fuera de línea para la PKI.
2. El componente gold™ Issuer, que incluye:
 - a. La API del emisor gold™, que se integrará en el sistema de gestión de documentos móviles del gobierno (mDMS).
 - b. El Integrale™ DPS, el firmante de documentos ISO 18013-5 utilizado para crear la firma digital del Objeto de Seguridad Móvil (MSO) del mID de la República Dominicana.
3. El componente gold™ Gateway.
4. El componente gold™ SDK (Kit de Desarrollo de Software), que se integrará en la aplicación del gobierno, en las plataformas Android e iOS.

5.4.2 gold™ Issuer - Sistema de Emisión

El sistema de Emisión gold™ es un grupo de componentes que exponen una API REST a la autoridad emisora y su IDMS con el fin de emitir credenciales móviles. Coordina todos los procesos y pasos necesarios en los subcomponentes para aprovisionar y administrar las credenciales de gold™.

El sistema de emisión de gold™ abarca múltiples componentes y propone una arquitectura que:

- Garantiza una fuerte protección de los componentes del firmante del documento.
- Permite la gestión de colas para optimizar los costos y asegurar que el sistema pueda diseñarse para manejar una carga promedio en lugar de los picos de demanda.



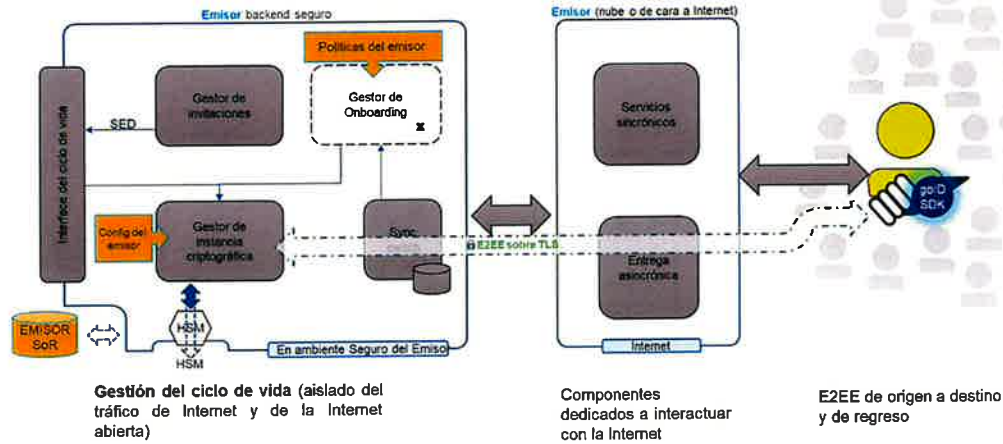


Ilustración 1 - Diagrama del sistema de Emisión

El sistema gold™ se encarga de:

- Formatear, codificar y preparar las credenciales móviles conforme a las normas ISO/IEC 18013-5 e ISO/IEC 23220.
- Admitir documentos dentro de un contenedor ISO (OACI para documentos de viaje, permisos, certificados, registro de vehículos, vacunación, etc.).
- Recibir e inscribir la aplicación móvil para proporcionar los datos necesarios para la firma, combatiendo la clonación.
- Firmar los datos para asegurar su autenticidad.
- Gestionar el protocolo de emisión móvil seguro con cifrado de extremo a extremo, desde los componentes de emisión en las instalaciones hasta la aplicación móvil con gold SDK.

Las aplicaciones de wallet que implementan gold™ SDK interactúan con gold Gateway que aloja los componentes orientados a Internet. La información de Gateway se recibe de la invitación canjeada en la aplicación de wallet del usuario objetivo. Luego, el sistema gold™ se encarga de entregar la actualización y revocar las credenciales móviles.

5.4.3 Emitir credencial móvil

Para emitir una credencial móvil, el sistema IDMS llamará a la API del sistema de Emisión gold™ y la solicitará para EMITIR una nueva credencial móvil. La carga útil de esta solicitud incluirá los datos personales necesarios para ser aprovisionados en la credencial.

El sistema permite la utilización e implementación, durante el proceso de emisión o activación de la identidad digital, mecanismos de seguridad como de *liveness detection* (prueba de vida), para prevenir ataques de suplantación de identidad.

5.4.4 Actualizar/Modificar credencial móvil

Para actualizar/modificar una credencial móvil emitida anteriormente, el sistema IDMS del cliente llamará a la API del sistema de Emisión goID™ y le solicitará que ACTUALICE la credencial existente. La solicitud incluirá una referencia al registro existente para que pueda ser procesado. La carga útil de esta solicitud incluirá una versión actualizada de los datos personales para que se pueda revocar la credencial anterior y se pueda aprovisionar la nueva versión.

De la misma manera, si el ciudadano necesita aprovisionar su credencial en un nuevo teléfono, entonces el sistema IDMS del cliente tendrá la capacidad de llamar a la API del sistema de Emisión goID™ y solicitar que se proporcione una nueva INVITACIÓN. Esto permitirá que la credencial se mueva de un teléfono a otro.

5.4.5 Revocar/Eliminar Credencial Móvil

Para eliminar una credencial móvil, el sistema IDMS llamará a la API del sistema de Emisión goID™ y le solicitará que REVOQUE la credencial. La solicitud incluirá una referencia al registro existente para que pueda ser revocado.

En caso de revocación de una credencial digital, el sistema enviará una notificación inmediata al usuario a través de múltiples canales, incluyendo correo electrónico, mensaje SMS y alertas dentro de la aplicación móvil. Esta notificación indicará el motivo de la revocación y proporcionará instrucciones sobre los pasos a seguir para su posible recuperación o reactivación.

5.4.6 Firma de documentos em identidad digital

Los componentes del firmante de documentos (DS) permiten al sistema procesar las operaciones de firma digital necesarias para firmar las solicitudes de credenciales.

- Operación genkey asimétrica, utilizando un HSM de acuerdo con FIPS-140-2 Nivel 2 o Nivel 3.
- Preparación de la Solicitud de Firma de Certificado (CSR) y exportación como archivo.



- Importe el certificado DS certificado después de la certificación por parte de la CSCA.
- Compruebe que el certificado DS pertenece a la entidad de certificación CSCA esperada.
- Compruebe que la clave pública contenida en el certificado DS está relacionada con la clave privada DS generada anteriormente.
- Mantener más de un certificado electrónico DS: se utilizará el que tenga la fecha de emisión más reciente.
- Comprobará si el certificado DS ha caducado: si todos los certificados DS han caducado, se detendrá e informará de un error específico.

El módulo DS se puede instalar en una configuración de alta disponibilidad para mejorar el rendimiento y proporcionar redundancia. Por razones de seguridad, la clave de firma de documentos normalmente no se compartirá entre los nodos: cada instancia del DS tendrá su propio par de claves y su propio certificado DS.

5.5 El SDK de gold

El SDK de gold es un SDK de aplicaciones para Android y iOS que:

- Maneja documentos móviles de cualquier tipo si utiliza contenedores ISO 23220-4 y 18013-5.
- Funciona con gold Issuer para provisionar, actualizar o revocar documentos.
- Se puede provisionar con marcadores para servicios en línea.
- Habilita cualquier aplicación para una versión de documento de acuerdo con ISO 18013-5 y 23220-4 (QR code + transferencia de datos BLE)
- Protege el documento y hace cumplir la privacidad
- Control desde el backend del Emisor: presentaciones de documentos, acciones disponibles, marcadores, etc.
- Incluye protección contra análisis estáticos y dinámicos, es ofuscado y comprueba si hay dispositivos rooteados/jailbreak, emuladores, etc.
- Incluye ofuscación de código para evitar cualquier intento de ingeniería inversa como, por ejemplo:
 - Ofuscación de nombre
 - Ofuscación de flujo de control
 - Ofuscación de código nativo
 - Ofuscación aritmética
 - Código de embalaje y encriptación
 - Ocultamiento de llamadas API
 - Compatibilidad con la protección de código dinámico como, por ejemplo:



- Detección de sabotaje
- Detección de gancho
- Detección de raíz (del inglés root)
- Protección contra la inserción de malware

Aprovecha la seguridad del hardware para proteger claves, como firmar una presentación según ISO 18013-5 y 23220-4

El SDK de la aplicación gold™ está diseñado para Android 11 o superior y iOS 13 o superior, donde se dispone de una seguridad de hardware más robusta.

5.5.1 Gateway de gold™

GoID™ Gateway es un servicio alojado en la nube proporcionado por TOPPAN. Gestiona aplicaciones móviles, puntos finales y emisores, proporcionando la transmisión desde el sistema de aprovisionamiento gold™ hasta el punto final del teléfono móvil. Mantiene el cifrado de los datos recibidos hasta su entrega al entorno seguro de los ciudadanos dentro de la aplicación móvil gold™.

GoID™ Gateway admite:

- Aprovisionamiento de identificaciones móviles a dispositivos móviles designados;
- Servicios de generación y gestión de claves para mejorar la seguridad del SDK móvil;
- Cifrado de extremo a extremo (E2EE) de los datos de los ciudadanos desde el sistema de aprovisionamiento gold™ hasta el SDK de gold™ en el teléfono móvil del ciudadano.
- GoID™ Gateway está organizado de forma totalmente segura y confidencial. No se almacena información de identificación personal (PII) en el Gateway y todos los datos de Ciudadano que pasan a través del Gateway están cifrados de extremo a extremo y solo puede ser descifrado por el dispositivo móvil de destino utilizando claves que son específicas de ese dispositivo.



Ilustración 2 - Diagrama del Gateway



5.6 Dimensionamiento de la Plataforma

Para dimensionar correctamente nuestra oferta, asumimos que emitiremos/actualizaremos 800,000 credenciales durante el período de 24 meses, con una producción distribuida uniformemente durante este período.

- El entorno de producción se ha dimensionado para este período.

Este pronóstico de dimensionamiento deberá ser gestionado y monitoreado durante la duración del proyecto, realizando los ajustes apropiados en el dimensionamiento del sistema según sea necesario.

La plataforma ofrecida permite la escalabilidad de su capacidad según la necesidad y el rendimiento real, proporcionando la continuidad de la solución a futuro.

Monitoreo para la Aplicación Móvil:

El Consorcio garantizará un servicio de monitoreo 24x7 de todos los sistemas, aplicaciones y componentes de la solución de identidad digital. Se implementará un Centro de Operaciones de Seguridad (SOC) con herramientas de monitoreo en tiempo real para la detección de incidentes y alertas. El sistema generará reportes periódicos y enviará notificaciones automáticas ante eventos críticos para garantizar la continuidad del servicio.

Registros de eventos para la Aplicación Móvil:

La solución implementará un sistema integral de gestión del ciclo de vida de las credenciales digitales, incluyendo su emisión, activación y revocación. Todos los eventos relacionados con cada credencial serán registrados y almacenados de forma segura en el sistema. Se garantizará la interoperabilidad con las aplicaciones y sistemas de la JCE, asegurando la actualización y sincronización en tiempo real de los estados de las credenciales.

Seguridad para la Aplicación Móvil:

La aplicación móvil y los sistemas asociados incluirán medidas avanzadas de seguridad contra ingeniería inversa y manipulación de código. Se emplearán técnicas como detección de root/jailbreak, cifrado de código, protección contra debugging y validación de integridad del binario en cada inicio de sesión. Además, se implementará un mecanismo de actualización segura para mitigar vulnerabilidades y garantizar la protección continua contra ataques.



5.7 Casos de Éxito

TOPPAN goID™ Proporciona Seguridad e Interoperabilidad en la Innovadora Aplicación de Identificación Ciudadana de Filipinas

En una era de rápida transformación digital, el gobierno de Filipinas, liderado por el Departamento de Tecnología de la Información y Comunicaciones (DICT), ha lanzado una iniciativa pionera para optimizar los servicios gubernamentales y empoderar a sus ciudadanos con una identidad digital segura y compatible con los estándares ISO. En el centro de esta innovación se encuentra el Kit de Desarrollo de Software (SDK) TOPPAN goID, integrado perfectamente en la aplicación eGovPH, la primera plataforma digital gubernamental integral del país. Esta iniciativa, innovadora tanto en Asia como a nivel mundial, introduce un enfoque móvil y seguro para la gestión de identidad, beneficiando a más de 118 millones de filipinos y permitiendo la interoperabilidad global.

A través de una asociación estratégica con **FMC Research Solutions Inc.**, un integrador líder de sistemas de seguridad en Filipinas, TOPPAN está proporcionando el marco de seguridad avanzado necesario para impulsar esta transformación nacional. La aplicación eGovPH funciona como una plataforma digital integral donde los ciudadanos filipinos pueden almacenar y acceder de manera segura a sus identificaciones gubernamentales, incluyendo la nueva identificación digital nacional, y realizar transacciones esenciales como pagos de impuestos, seguridad social y acceso a servicios de salud. Con el cumplimiento de los estándares ISO, las identificaciones móviles emitidas a través de eGovPH son válidas para uso internacional, lo que refuerza el compromiso de Filipinas con soluciones de identidad digital robustas y universalmente aceptadas.

DESAFÍO

Con aproximadamente 10.2 millones de filipinos residiendo en el extranjero, Filipinas tiene una de las poblaciones de trabajadores en el exterior más grandes del mundo. Por esta razón, era crucial que eGovPH cumpliera con los estándares de compatibilidad ISO, garantizando la interoperabilidad global y permitiendo la verificación sin problemas en diversas plataformas y países. Este nivel de interoperabilidad refleja la dedicación de Filipinas a la adopción de soluciones digitales seguras y universalmente aceptadas.



"El cumplimiento con ISO 23220 significa que todas las credenciales (identificaciones móviles u otros documentos digitales) emitidas en la plataforma eGovPH pueden ser interoperables a nivel global, permitiendo su reconocimiento por otros países que sigan los mismos estándares ISO", explicó el Secretario del DICT, Ivan John E. Uy.

SOLUCIÓN

El DICT recurrió a TOPPAN, que colaboró con FMC Research Solutions Inc. para integrar el Kit de Desarrollo de Software (SDK) TOPPAN gold, proporcionando la infraestructura segura de la aplicación eGovPH y su capacidad para almacenar múltiples documentos de identidad móvil en una cartera digital.

La plataforma gold proporciona una infraestructura segura para la emisión de identidades móviles en dispositivos, permitiendo su verificación mediante estándares ISO interoperables.

Respaldada por la tecnología gold de TOPPAN, la aplicación eGovPH protege las identidades de los ciudadanos con medidas de seguridad avanzadas como cifrado y múltiples métodos de autenticación (reconocimiento facial, huellas dactilares, PIN) para acceder a la aplicación. La emisión remota a través de actualizaciones por aire permite que las identificaciones móviles se gestionen de forma remota, protegiendo la privacidad de los usuarios al compartir solo los datos esenciales durante la verificación.

"Este proyecto de identificación digital nacional optimiza los servicios gubernamentales y ofrece a los ciudadanos una comodidad sin precedentes al mejorar significativamente el acceso y la usabilidad de sus identificaciones. Al adoptar TOPPAN gold, el gobierno filipino ha lanzado la primera plataforma digital gubernamental de Asia compatible con ISO, proporcionando una experiencia segura y fácil de usar para sus ciudadanos", afirmó Uy.

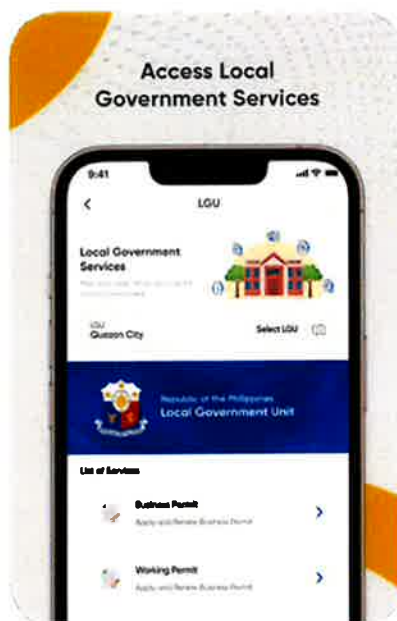


RESULTADO

Con TOPPAN gold, la aplicación eGovPH se ha convertido en un referente en la digitalización de las identificaciones nacionales y en la expansión del acceso de los ciudadanos a los servicios gubernamentales electrónicos.



“Al adoptar TOPPAN gold, el gobierno filipino está entregando la primera plataforma digital gubernamental compatible con ISO en Asia y proporcionando a sus ciudadanos una experiencia digital segura y fácil de usar”.



- Ivan John E. Uy, secretario Departamento de Tecnología de la Información y Comunicaciones (DICT)

Consortio IDSecure IDS

PROYECTO IMPRESIÓN NUEVA CÉDULA DE IDENTIDAD Y
ELECTORAL (CIE) Y CÉDULA DE IDENTIDAD (CI)
JCE-CCC-LPI-2024-0001

En solo unos meses desde su lanzamiento, la aplicación eGovPH ya ha alcanzado seis millones de descargas, permitiendo a los usuarios acceder a sus identificaciones digitales nacionales y a una gama de servicios gubernamentales. Para 2025, los usuarios podrán acceder y almacenar un conjunto ampliado de documentos de identidad emitidos por el gobierno para transacciones gubernamentales y privadas, que serán reconocidos legalmente por las instituciones pertinentes. Gracias a TOPPAN y FMC, Filipinas está posicionada para liderar uno de los programas de identificación digital nacional más ambiciosos del mundo.



TOPPAN goID™ Smart DNI: La Revolución en Identidad Móvil de Argentina

Argentina, un país de 45 millones de personas en América Latina, tiene una larga tradición en identificación nacional. Desde 1968 se expide el Documento Nacional de Identidad (DNI), el cual se otorga al nacer y debe actualizarse periódicamente durante la vida del ciudadano. El DNI es requerido para múltiples trámites administrativos y privados, tales como votar, abrir una cuenta bancaria o cumplir con el servicio militar. La emisión del DNI está a cargo del Registro Nacional de las Personas de Argentina (RENAPER).

Con un alto nivel de penetración de smartphones y una clara estrategia de digitalización, en 2018 Argentina decidió lanzar un proyecto para emitir una versión móvil de la cédula de identidad, denominada Smart DNI. La visión era que los ciudadanos pudieran disponer de su Smart DNI de forma segura, integrándolo en una aplicación móvil gubernamental llamada MiArgentina, que funciona como un portal digital integral y billetera móvil. Gracias a una legislación visionaria, esta versión digital tendría la misma validez que la cédula física, ofreciendo así una identidad nacional digital, segura y aceptada en cualquier lugar.

DESAFÍO

Los principales objetivos del cliente eran innovar sin asumir riesgos innecesarios y mantener el control total del proyecto durante todo su ciclo de vida. Un desafío importante fue que, en 2019, no existían estándares orientadores claros (la ISO 18013-5 se encontraba en un borrador avanzado sin publicar y la serie ISO 23220 estaba en una etapa muy temprana).

Otro reto estuvo relacionado con la participación intensiva de múltiples entidades gubernamentales de distintos ministerios, lo que obligaba a que la plataforma técnica fuese lo suficientemente flexible para satisfacer las demandas de todas las partes involucradas. Para ello, fue indispensable contar con un conjunto integral de capacitación y documentación, junto con un traspaso adecuado a cada entidad.

Finalmente, Argentina deseaba ser propietaria de la superaplicación gubernamental (portal/billetera móvil) sin tener que asumir la carga de cumplir con los estándares ISO de identidad móvil, los requisitos del ecosistema móvil (versiones de iOS y Android) ni con las exigencias de seguridad (ofuscación y protección de datos y código central). Por ello, el proveedor debía ofrecer un enfoque basado en SDK, en el que todos estos aspectos



estuvieran cubiertos, permitiendo que la aplicación se concentrara únicamente en la interfaz y experiencia del usuario. Este enfoque garantizaría que la superapp pudiera adaptarse de forma flexible a nuevos requisitos de experiencia, nuevos servicios gubernamentales o cambios normativos.

SOLUCIÓN

Tras una licitación organizada por el gobierno argentino en 2019, TOPPAN Security fue adjudicado el proyecto en mayo de ese mismo año, con el requisito de desplegar la solución en un plazo muy ajustado, siguiendo un cronograma agresivo:

- **Lanzamiento (técnico): 1 de septiembre de 2019**
Se proporcionó el entorno de desarrollo y se capacitó al cliente. Se desarrolló, implementó y probó la solución, logrando superar la prueba de aceptación del usuario.
- **Lanzamiento (político): 30 de septiembre de 2019**
En esta fecha, el gobierno comunicó el proyecto a los ciudadanos.
- **Lanzamiento (legal): 29 de octubre de 2019**
En esta fecha, la legislación otorgó plena equivalencia legal a la versión móvil de la cédula.
- **Lanzamiento (operacional): 14 de noviembre de 2019**
Se abrió el servicio para el ciudadano.



Comunicado de prensa de TOPPAN Security, (anteriormente bajo nombre de HID): 18 de diciembre de 2019

La solución implementada es la plataforma **TOPPAN Security gold™**, que se basa en tres componentes principales:

- **SDK**
- **Gateway**
- **Componente Emisor**

El Ministerio de Modernización fue capacitado en el SDK para completar la superapp gubernamental que integra la identidad móvil. Paralelamente, el Ministerio del Interior, a través de RENAPER, recibió capacitación sobre la API del componente Emisor para lograr la integración entre la base de datos de ciudadanos y dicho componente.

Todos los componentes on premise se han instalado en el centro de datos de RENAPER, además de en servidores seguros en la nube, proporcionados por el socio local argentino de TOPPAN Security, Megallanes. Este socio ofrece soporte local para la solución, complementado con soporte global cuando es necesario. TOPPAN Security ha capacitado a Megallanes para que cuente con total autonomía en la resolución de la mayoría de los incidentes, lo que permite tiempos de respuesta muy rápidos para el gobierno argentino y mantiene bajos los costos de soporte.

RESULTADO

Gracias a TOPPAN Security, Argentina cuenta ahora con el programa de identidad móvil más avanzado del mundo, con más de 6 millones de identidades móviles activas emitidas entre 2019 y 2025. Esta identidad móvil, denominada **Smart DNI**, se almacena de forma segura en el teléfono móvil del ciudadano y se integra en la superapp gubernamental llamada **MiArgentina**. El Smart DNI es aceptado en todas partes y está disponible tanto en iOS como en Android.



Entre los beneficios para el ciudadano destacan:

Control de datos: Los ciudadanos se benefician de la nueva app MiArgentina, ya que tienen el control total de sus datos. Al estar almacenados en su teléfono, pueden decidir con quién compartirlos y cuándo hacerlo, manteniéndose siempre informados.

Actualización inmediata: El Smart DNI móvil se actualiza de forma continua. Así, en caso de cambios como matrimonio, modificación de nombre o cambio de domicilio, el ciudadano no necesita acudir a una oficina; el cambio se realiza de forma remota y la app actualiza los datos de inmediato.

