binaria

Ficha técnica de producto

Binaria Wallet

www.binariatechnologies.com

Resumen Ejecutivo

Con nuestro mundo cada vez más conectado, ¿Cómo pueden las personas tomar el control de sus identidades digitales?

El necesitar intercambiar información todos los días con cientos de aplicaciones nos vuelve vulnerables a los ataques cibernéticos que cada vez son más sofisticados y **nuestra identidad digital está constantemente en riesgo.** Muchas empresas hacen uso de nuestros datos personales sin nuestro **consentimiento claro.**

Memorizar y cambiar constantemente decenas de contraseñas ya no es viable, y los códigos enviados a teléfonos o correos han demostrado claramente no ser suficientes para protegernos.

Es necesario evolucionar hacia un uso de internet donde la identidad se proteja y sea confiable.

Las credenciales digitales Binaria, están construidas sobre **estándares globales abiertos**, compatibles con las redes de identidad de mayor alcance. Son **reutilizables** y cualquier empresa sin importar su tamaño, tipo de sistemas o grado de automatización, puede beneficiarse de su utilidad.

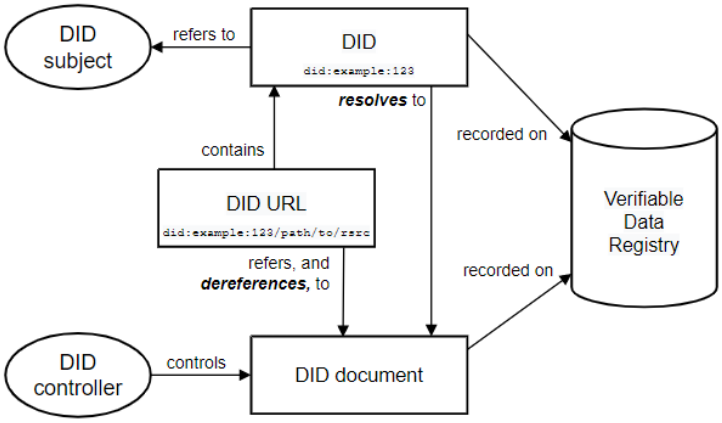
Esta ficha técnica de producto cubre con los desafíos para las personas y las organizaciones en la validación de identidades digitales, y como pueden ayudar las soluciones que ofrece Binaria basadas en estándares de descentralización interoperables.

Por lo que, este documento, adicionalmente cuenta con la capacidad de compartir información útil sobre su arquitectura, modelos de seguridad y requerimientos mínimos.

Como funciona nuestra tecnología

Nuestra tecnología se rige por los principios de una identidad descentralizada bajo un modelo de confianza de un ecosistema empresarial, nuestro sistema principal cuenta con un mecanismo basado en tecnología blockchain que es respaldado bajo la funcionalidad del Trust System en dos elementos esenciales, indicadores descentralizados y credenciales verificables. Los identificadores descentralizados son DID, que los usuarios crean, poseen y controlan independientemente de cualquier organización o gobierno, una credencial verificable es la información certificada por algún participante del ecosistema basado en el identificador DID.

A continuación, se muestra una descripción de los principales componentes de la arquitectura del identificador descentralizado.

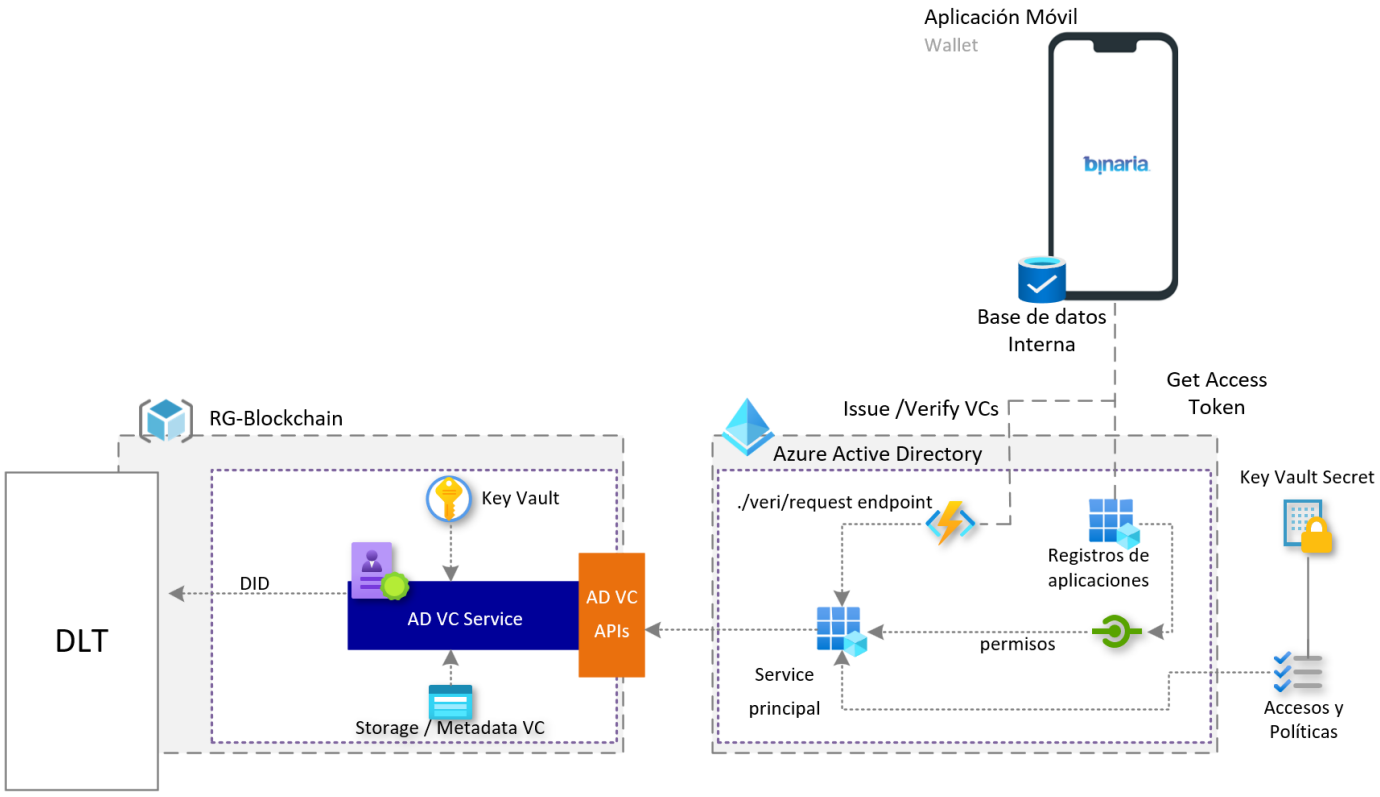


Narrativa del diagrama estándar de la W3C: Dentro del diagrama existen seis formas etiquetadas internamente, con flechas etiquetadas entre ellas, de la siguiente manera.

Los puntos anteriores describen el flujo que se debe de considerar entre el subject de un DID hasta la expedición y registro del documento bajo un DID.

Nuestro diagrama de comunicación de DID se centra bajo el protocolo de Microsoft ION el cual presenta a continuación:

Nota: Nuestra comunicación a los servicios de DLT esta diseñada para que pueda comunicarse con cualquier otro DLT sin problemas de compatibilidad.

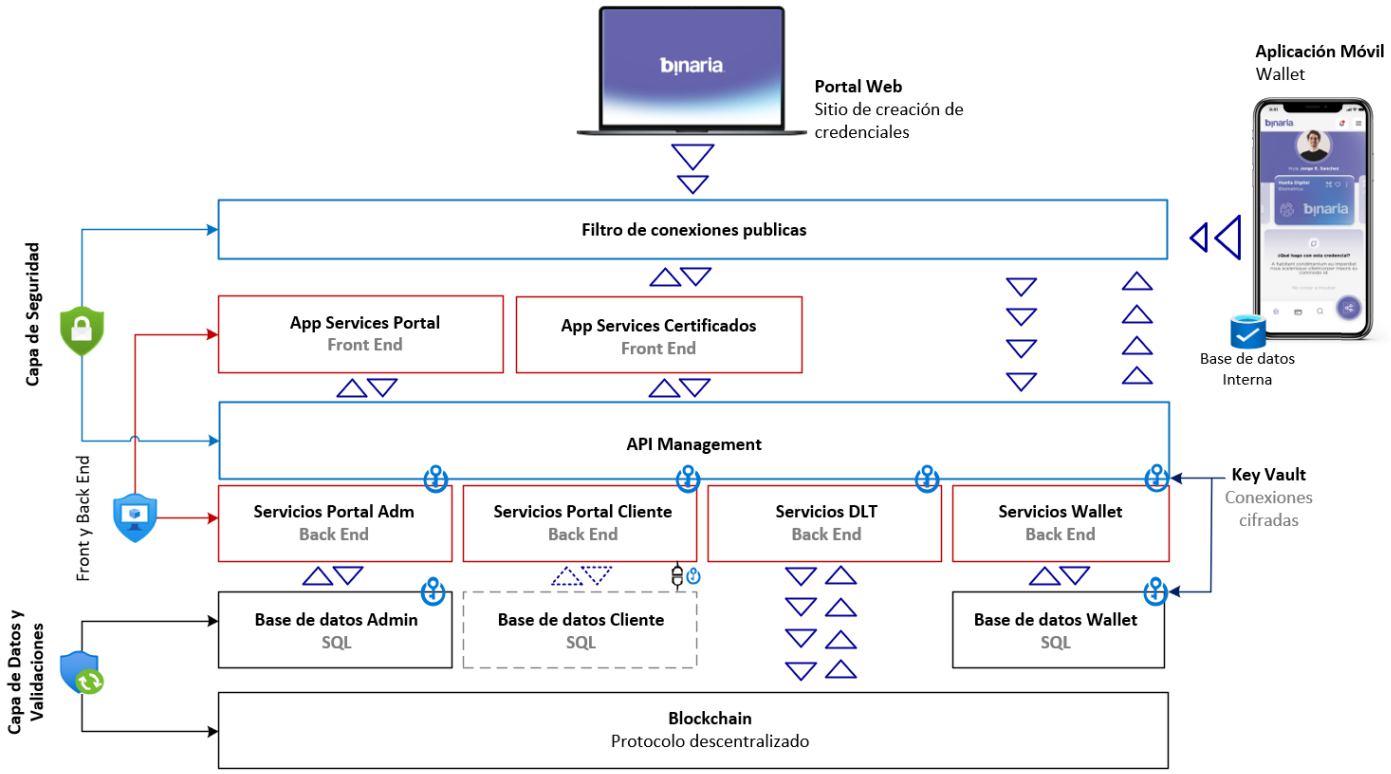


Nuestros componentes tecnológicos

Pre-requisitos Hardware

	Android		IOS	
	Mínimo	Recomendado	Mínimo	Recomendado
Pantalla	Resolución 1.080 x 2.340 píxeles	Resolución 1.440 x 2.560 píxeles	Resolución de 1920 x 1080 pixeles a 401 ppi	Resolución de 2532 x 1170 pixeles a 460 ppi
Procesador	Quad-core 2.4 GHz	Octa-core 3.0 GHz	Chip A11 Bionic de 2.4 GHz	Chip A14 Bionic de 3.0 GHz
RAM	4 GB	6 GB	4 GB	6 GB
Cámara	12 mp	12 mp	12 mp	12 mp
Almacenamiento	Disponible 1 GB	Disponible 2 GB	Disponible 1 GB	Disponible 2 GB
Sistema Operativo	Android 11	Android 13	IOS 15	IOS 16

Diagrama de arquitectura general



Esta arquitectura contempla los siguientes elementos:

API Management: Este servicio permite controlar las conexiones de consumo de APIs para los diferentes back end que se tienen en la plataforma, adicional a que maneja por llaves dichas peticiones robusteciendo el tema de seguridad.

Back End: Se cuenta con diferentes servicios de Back End los cuales permitirán a esta arquitectura tener un mecanismo de desacoplamiento por cualquier evolutivo que se tenga en tecnología o ledger.

Front End: Este servicio está destinado para el portal de empresas el cual sirve como mecanismo de emisión y validación de credenciales y certificados, adicional se cuenta con un portal web que permite la vista rápida de un certificado o credencial sin ingresar a la app móvil (Wallet).

Base de Datos Admin: Esta base de datos contiene información de conexión como metadatos, los cuales soportarán el servicio del portal de empresas, con esta base de datos se permite la conexión de los usuarios a las diferentes instancias, esta información se encuentra cifrada y enmascarada como Dynamic Data Masking.

Los datos cifrados son:

Datos de usuario para login:

- Name – Valor Predeterminado
- LastName – Valor Predeterminado
- FullName – Valor Predeterminado
- Address – Valor Predeterminado
- UserName – Valor Predeterminado
- Email – Correo Electrónico
- NormalizedEmail – Valor Predeterminado
- PhoneNumber – Valor Predeterminado

Base de Datos Cliente: Esta base de datos siempre radica en la infraestructura del cliente, esta base de datos contiene los datos de los certificados y credenciales que emiten las organizaciones, su método de conexión es bajo una llave administrada por Kay Vault para no comprometer las credenciales de conexión, también cuenta con un mecanismo de firewall y reglas de conexión para no permitir el acceso desde otras unidades organizacionales o servicios externos.

Base de Datos Wallet: Esta base de datos contiene los metadatos de conexión para un Login de usuarios, adicional se genera un ID único el cual permite identificar al usuario dentro del ecosistema, este ID está ligada al DID Público que se maneja en la blockchain. Como protocolo de seguridad de los datos, esta base contiene Dynamic Data Masking para algunas tablas las cuales se enlistan a continuación.

Datos de usuario para login:

- UserName – Valor Predeterminado
- Email – Correo Electrónico
- NormalizedEmail – Valor Predeterminado
- PhoneNumber – Valor Predeterminado

Biometría

Se tiene considerada la arquitectura de un componente de reconocimiento biométrico como un elemento de validación facial y comprobación de identidad bajo el mecanismo de Match, el cual se compone de elementos de prueba de vida, comparativa de rostros y extracción OCR.

DLT: Se utiliza el mecanismo de DLT de Microsoft llamado The Verifiable Credentials Data Model 1.0, el cual se basa en estos pasos:

1. Identificadores descentralizados (DID) del W3C Identificadores que los usuarios crean, poseen y controlan independientemente de cualquier organización o gobierno. Los DID son identificadores únicos a nivel mundial vinculados a metadatos de Infraestructura de clave pública descentralizada (DPKI) compuestos por documentos JSON que contienen material de clave pública, descriptores de autenticación y puntos finales de servicio.

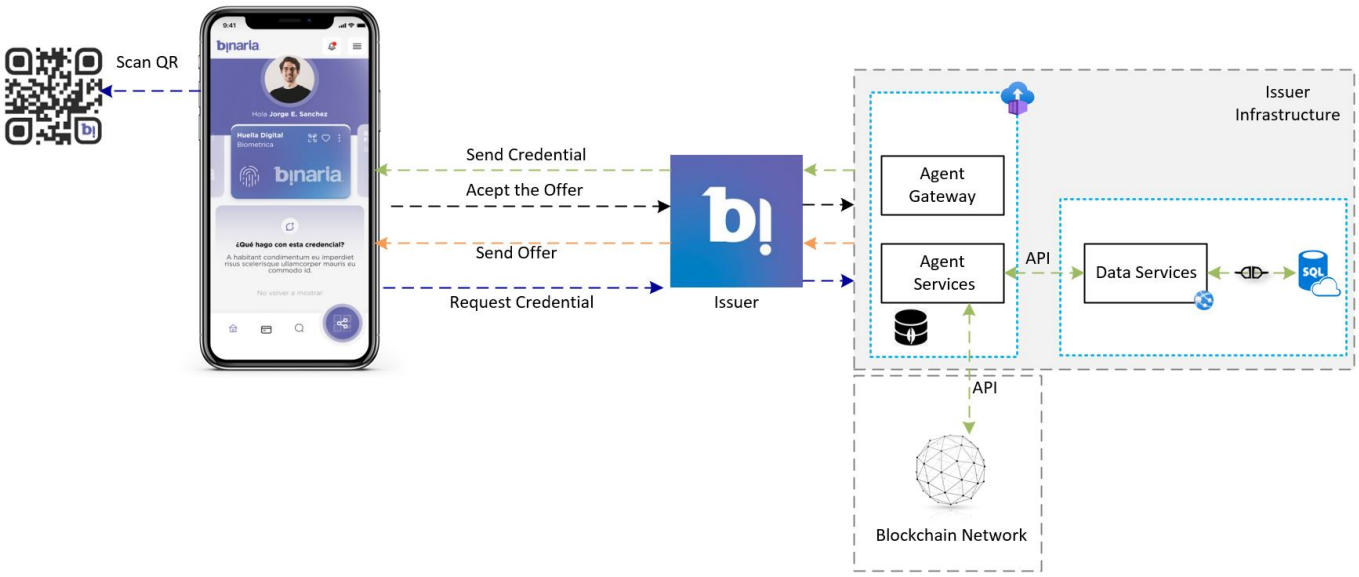
2. Sistema descentralizado ION (Red de Superposición de Identidad) ION es una red abierta sin permiso de Capa 2 basada en el protocolo Sidetree puramente determinista, que no requiere tokens especiales, validadores confiables u otros mecanismos de consenso. La progresión lineal de la cadena de tiempo de Bitcoin es todo lo que se requiere para su funcionamiento. Hemos abierto un paquete npm para que trabajar con la red ION sea fácil de integrar en sus aplicaciones y servicios. Las bibliotecas incluyen la creación de un nuevo DID, la generación de claves y el anclaje de su DID en la cadena de bloques de did:webes un modelo basado en permisos que permite confiar usando la reputación existente de un dominio web.

3. DID User Agent/Wallet: la aplicación Binaria Wallet permite que personas reales utilicen identidades descentralizadas y credenciales verificables. Binaria Wallet crea DID, facilita las solicitudes de emisión y presentación de credenciales verificables y administra la copia de seguridad de la semilla de su DID a través de un archivo de billetera encriptado.

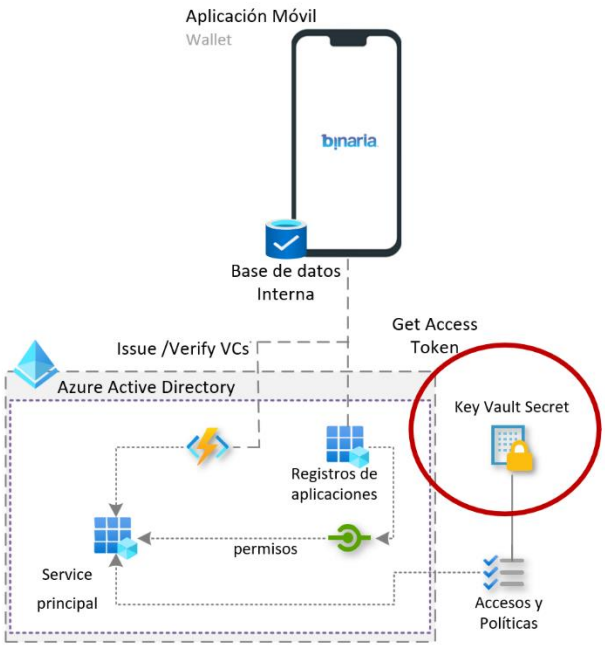
4. Microsoft Resolver Una API que se conecta a nuestro nodo ION para buscar y resolver DID utilizando el did:ion método y devolver el objeto de documento DID (DDO). El DDO incluye metadatos DPKI asociados con el DID, como claves públicas y puntos finales de servicio.

5. Servicio de credenciales verificadas de Azure Active Directory Un servicio de emisión y verificación en Azure y una API REST para credenciales verificables W3C que están firmadas con el did:ionmétodo. Permiten a los propietarios de identidades generar, presentar y verificar reclamos. Esto forma la base de la confianza entre los usuarios de los sistemas.

MultiLedger: Se agrega también a este diagrama la compatibilidad de conexión con otros servicios de DLT como Velocity, el cual puede verificar instantáneamente las credenciales de carrera y educación en línea compartidas por los solicitantes, estudiantes y empleados. Esta capa permite que Binaria Wallet tenga la capacidad de selección de cualquier tipo de DLT basado en contratos.



Seguridad



Binaria Technologies cuenta con un mecanismo de llaves seguras bajo todos los servicios de comunicación de tipo back end, esto permite que todos los APIs que se utilizan en la comunicación del portal y wallet estén bajo un Azure Key Vault.

Azure Key Vault aplica el protocolo Seguridad de la capa de transporte (TLS) para proteger los datos cuando viajan entre Azure Key Vault y los back end que se encuentran publicados bajo un API Management. API Management negocian una conexión TLS con Azure Key Vault. TLS proporciona una autenticación sólida, privacidad de mensajes e integridad (lo que permite la detección de la manipulación, interceptación y falsificación de mensajes), interoperabilidad, flexibilidad de algoritmo, y facilidad de implementación y uso.

Las bases de datos que Binaria tiene como core, cuentan con un Cifrado de datos transparente (TDE) y en algunas tablas Dynamic Data Masking. La tecnología Cifrado de datos transparente, cifra las bases de datos, copias de seguridad y registros en reposo sin realizar cambios en la aplicación. Adicional cuenta con un mecanismo de monitoreo bajo Microsoft Defender for SQL que permite tener bajo observación cualquier anomalía sobre la base de datos. Como mecanismo de conexión también cuenta con un servicio de Firewall que permite bajo reglas de conexión IP la discriminación de IPs que cuentan con permiso de conexión hacia el recurso de base de datos.

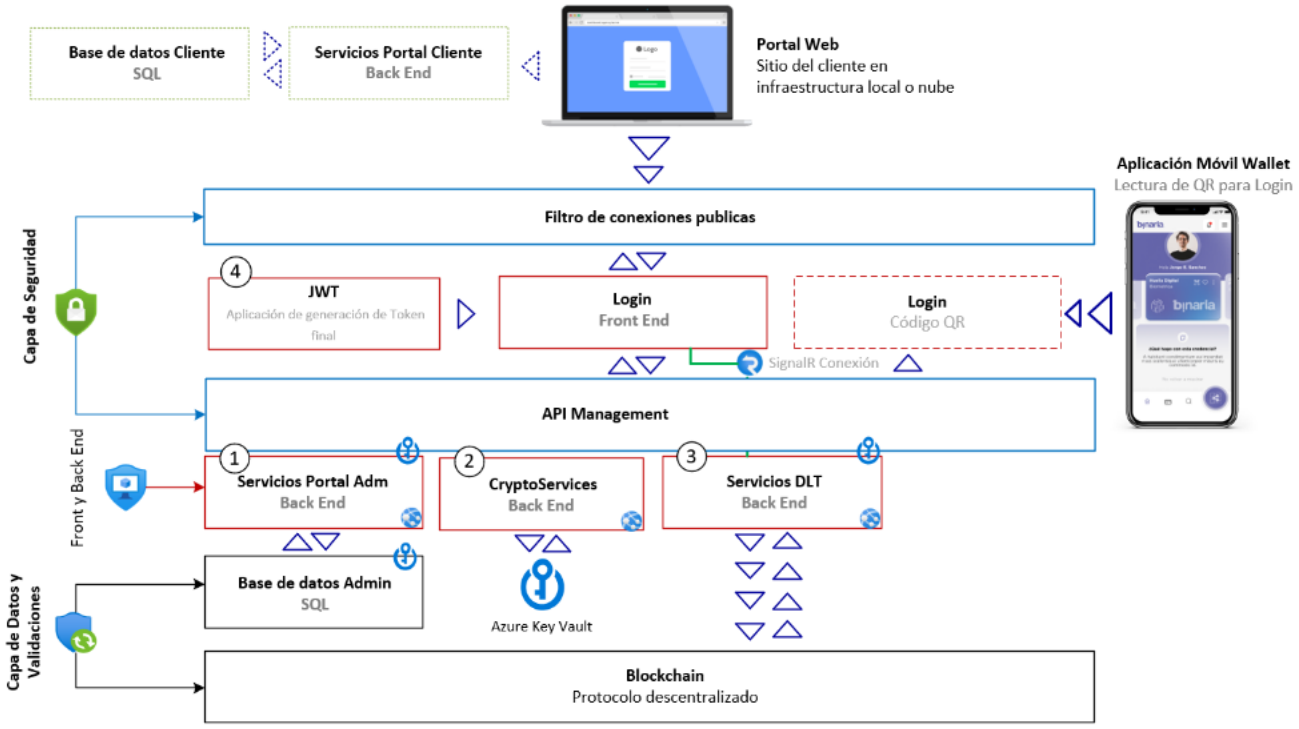
Nuestras bases de datos cuentan con Administración de seguridad basado en:

- Auditoria de SQL
- Auditoria de integración con análisis y registros en centros de eventos
- Azure Security Center
- Evaluación de vulnerabilidades

Nuestros servicios tanto Front End y Back End cuenta con protocolos de seguridad de comunicación bajo HTTPS, FTPS y SSL, los cuales permiten solo la comunicación por esas vías a IPs especificas en el caso de Back End y en el caso de Front End se realiza un monitoreo contante con Microsoft Advisor el cual muestra un tablero de recomendaciones para siempre tener protegidas las comunicaciones al API Management

Otra capa de seguridad con la que cuenta nuestra aplicación se basa en la comunicación a portales para poder realizar un Login bajo una credencial verificada.

A continuación, se muestra un diagrama de conexión de los procesos de seguridad por los cuales pasa el Login con una credencial verificada.



Descripción del diagrama:

1. El servicio de Login realiza una petición hacia los servicios del Portal de Administración para poder detectar, una suscripción vigente y un token de organización. Una vez que se detecta esta información se genera un QR para ser leído desde el Wallet.

2. Al leer el QR desde la App, el servicio de CryptoServices realiza un proceso de encriptación bajo los protocolos de RSA y almacena dicha información de llaves bajo un Key Vault. Estas llaves son utilizadas para encriptar los datos de la credencial verificada y no viajen de manera plana.

3. El Wallet realiza la entrega de dichas credenciales encriptadas por el servicio del DLT al portal del Login.

4. El Login consulta el proceso de generación de token el cual regresa un JWT al cliente final (Portal Cliente).