Arquitectura del Proyecto

Esta documentación describe la arquitectura técnica para la emisión, gestión y verificación de una Licencia de Conducir Digital en la República Dominicana. El diseño se basa en el modelo de **Identidad Auto-Soberana (SSI)**, utilizando los estándares de **Credenciales Verificables (VCs)** del W3C para garantizar la seguridad, interoperabilidad y el control del ciudadano sobre sus datos.

Actores Principales y sus Roles

En este ecosistema, cada entidad juega un papel crucial:

- **Propietario (Holder):** Es el **ciudadano** titular de la licencia de conducir. Utiliza la aplicación móvil **"Soy Yo RD" (Carpeta Ciudadana)** para recibir, almacenar y presentar su licencia digital de forma segura.
- **Emisor (Issuer):** Es el **Instituto Nacional de Tránsito y Transporte Terrestre (INTRANT)**. Esta entidad es la única autoridad responsable de verificar la identidad del ciudadano, validar el cumplimiento de los requisitos para conducir y emitir la licencia de conducir en formato de Credencial Verificable.
- **Verificador (Verifier):** Son las entidades que necesitan comprobar la validez de la licencia de conducir. Principalmente, serán los agentes de la **Dirección General de Seguridad de Tránsito y Transporte Terrestre (DIGESETT)**, pero también podrían ser otras entidades como compañías de alquiler de vehículos o aseguradoras.
- **Proveedor de Identidad (Identity Provider):** Es **"Cuenta Única"**, el sistema de autenticación centralizado del Estado Dominicano. Se utiliza para que el ciudadano pueda autenticarse de forma segura ante el INTRANT antes de solicitar su licencia digital.
- **Desarrollador y Mantenedor:** La **Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)** es la responsable del desarrollo y mantenimiento de la wallet "Soy Yo RD" y de la integración de los componentes tecnológicos necesarios.

Componentes Tecnológicos Clave

La arquitectura integra un conjunto de tecnologías de código abierto, principalmente de la plataforma **Inji**, que facilitan la implementación del modelo de VCs.

- **Soy Yo RD (Wallet/Carpeta Ciudadana):** Es la aplicación móvil (wallet) del ciudadano. Basada en **Mimoto**, esta aplicación permite:
  - Generar y gestionar pares de claves criptográficas.

    - Crear y gestionar Identificadores Descentralizados (DIDs).
    - Solicitar la emisión de la licencia al INTRANT.
    - Almacenar de forma segura la Licencia de Conducir Verificable.
    - Crear Presentaciones Verificables (VPs) para compartir la información de la licencia con un verificador, sin ceder el control de la credencial.
- **Inji-Certify (Portal de Emisión):** Es la plataforma que utilizará el **INTRANT** para emitir las licencias. Inji-Certify proporciona una interfaz para:
    - Definir el esquema de la credencial (los campos que contendrá la licencia: nombre, número de licencia, categorías, fecha de expiración, etc.).
    - Conectarse con la base de datos interna del INTRANT para obtener los datos del conductor.
    - Firmar criptográficamente la credencial con la clave privada del INTRANT, convirtiéndola en una Credencial Verificable a prueba de manipulaciones.
    - Enviar la credencial firmada de forma segura al wallet "Soy Yo RD" del ciudadano.
- **Registro de DIDs (DID Registry):** Es un componente fundamental que funciona como un libro de contabilidad descentralizado (puede ser una blockchain o una base de datos distribuida). Su función es almacenar los **DIDs** y sus documentos DID asociados. Un documento DID contiene la clave pública del emisor (INTRANT), permitiendo que cualquier verificador pueda encontrarla para comprobar la autenticidad de la firma en la licencia. La OGTIC gestionará la infraestructura de este registro.
- **Cuenta Única (IdP):** Actúa como el puente de confianza inicial. Antes de que el INTRANT emita la credencial, el ciudadano debe probar quién es. Lo hará autenticándose con su **Cuenta Única** a través de un protocolo estándar como OpenID Connect (OIDC). Una vez autenticado, el sistema del INTRANT asocia la sesión del usuario con su registro en la base de datos de licencias.

Flujo de Emisión y Verificación

Flujo de Emisión de la Licencia Digital

1. **Inicio (Ciudadano):** El ciudadano abre la app **"Soy Yo RD"** y selecciona la opción para solicitar su licencia de conducir digital.
2. **Autenticación (Ciudadano):** La app redirige al ciudadano al portal de **Cuenta Única**. El usuario ingresa sus credenciales para autenticarse.
3. **Autorización (Ciudadano):** Una vez autenticado, Cuenta Única devuelve una prueba de autenticación (un token) a la app "Soy Yo RD".
4. **Solicitud de Credencial (Wallet):** La app "Soy Yo RD" envía una solicitud de emisión al portal **Inji-Certify** del INTRANT. Esta solicitud incluye el token de autenticación y el DID del ciudadano.
5. **Validación de Datos (INTRANT):** Inji-Certify utiliza el token para verificar la identidad del usuario y busca en la base de datos del INTRANT la licencia de conducir asociada a esa persona.

6. **Creación y Firma (INTRANT):** Con los datos confirmados, Inji-Certify genera la Credencial Verificable con el formato estándar W3C, incluyendo los datos de la licencia, el DID del ciudadano (sujeto de la credencial) y la firma digital del INTRANT (usando su clave privada).
7. **Emisión (INTRANT):** Inji-Certify envía la VC firmada directamente a la app **"Soy Yo RD"** del ciudadano.
8. **Almacenamiento (Wallet):** La app recibe la VC, verifica la firma del INTRANT usando la clave pública obtenida del registro de DIDs y la almacena de forma segura en el dispositivo del ciudadano.

Flujo de Verificación de la Licencia (Ej. Agente de DIGESETT)

1. **Solicitud de Verificación (Verificador):** El agente de la DIGESETT le solicita al conductor que presente su licencia. El agente muestra un código QR en su dispositivo de verificación.
2. **Presentación (Ciudadano):** El ciudadano abre su app **"Soy Yo RD"**, selecciona su licencia de conducir y escanea el código QR del agente.
3. **Creación de Presentación Verificable (Wallet):** La app del ciudadano crea una **Presentación Verificable (VP)**. Esta VP es un paquete que contiene la VC de la licencia y está firmada con la clave privada del ciudadano, demostrando que él es el portador legítimo y que consiente la presentación.
4. **Envío (Wallet):** La VP se envía al dispositivo del agente a través de un canal seguro (ej. Bluetooth, NFC o a través de la red).
5. **Verificación (Verificador):** El dispositivo del agente realiza dos comprobaciones criptográficas de forma automática:
   - **Verifica la firma del ciudadano en la VP:** Confirma que el portador de la wallet es quien dice ser.
   - **Verifica la firma del INTRANT en la VC:** Busca el DID del INTRANT en el registro público, obtiene su clave pública y confirma que la licencia es auténtica y no ha sido alterada desde su emisión.
6. **Resultado:** El dispositivo del verificador muestra el resultado: **"Válido"** o **"Inválido"**, junto con los datos de la licencia (nombre, foto, categoría, estado).

Revisión #2
Creado 17 junio 2025 15:11:11 por Tomás Familia
Actualizado 17 junio 2025 15:58:04 por Tomás Familia