Gestión del Ciclo de Vida y Seguridad

Esta sección aborda los casos de uso administrativos y de seguridad que son fundamentales para garantizar la integridad, confiabilidad y sostenibilidad a largo plazo del ecosistema de la licencia de conducir digital. Estos procesos son gestionados por personal técnico y de seguridad de la **OGTIC** y del **INTRANT**.

Caso de Uso 1: Gestión del Esquema de la Credencial (Schema)

Este caso de uso se activa cuando los requisitos de negocio o legales de la licencia de conducir cambian (ej. se añade un campo nuevo como "Donante de Órganos").

- **Actor**: Administrador de Credenciales (INTRANT), con aprobación de OGTIC.
- **Trigger**: Decisión administrativa o cambio en la normativa de tránsito.
- **Mecanismo Técnico**:
  1. **Definición de la Nueva Versión**: Se crea una nueva versión del esquema JSON que define la estructura de la VC. Se le asigna un nuevo identificador de versión o URI.
     JSON
     ```
     // old_schema_uri: "https://intrant.gob.do/schemas/licencia/v1.0"
     // new_schema_uri: "https://intrant.gob.do/schemas/licencia/v1.1"
     ```
  2. **Actualización del Portal de Emisión**: El administrador actualiza la configuración en el portal `Inji-Certify` a través de una interfaz administrativa segura.
     - **Llamada API (Interna)**: Se podría ejecutar una llamada `PUT` a un endpoint administrativo.
       - **Endpoint**: `https://admin.inji-certify.intrant.gob.do/api/v1/schemas/driving-license`
       - **Body (JSON)**:
         JSON
         ```
         {
           "schemaUri": "https://intrant.gob.do/schemas/licencia/v1.1",
         ```

```
  "schemaDefinition": { ... nuevo esquema JSON ... },
  "isActive": true
}
```

3. **Plan de Transición**:
   - **Nuevas Emisiones**: Todas las licencias emitidas o renovadas a partir de este punto utilizarán el nuevo esquema v1.1.
   - **Credenciales Antiguas**: Las licencias existentes (v1.0) siguen siendo válidas hasta su fecha de expiración o hasta que sean renovadas. Las aplicaciones de los verificadores deben estar programadas para entender y validar ambas versiones del esquema.
- **Impacto en el Ecosistema**: Requiere coordinación para que las aplicaciones de verificadores se actualicen y puedan interpretar correctamente tanto el esquema antiguo como el nuevo.

Caso de Uso 2: Gestión de Claves Criptográficas del Emisor (INTRANT)

Este es uno de los procesos más críticos para la seguridad y confianza de todo el sistema.

- **Actor**: Oficial de Seguridad (OGTIC/INTRANT).
- **Trigger**:
  - **Rotación Programada**: Política de seguridad que exige cambiar las claves cada 1-2 años.
  - **Compromiso de Clave**: Sospecha o confirmación de que la clave privada ha sido expuesta.
- **Mecanismo Técnico (Rotación Programada)**:
  1. **Generación de Nueva Clave**: Se genera un nuevo par de claves (privada/pública) dentro del **HSM**. La nueva clave privada nunca sale del HSM.
  2. **Actualización del Documento DID**: Se debe actualizar el documento DID del emisor (`did:web:intrant.gob.do`) para reflejar este cambio. El `did.json` se modifica para:
     - Añadir la nueva clave pública en la sección `verificationMethod`.
     - Mantener la clave antigua en la misma sección, pero marcándola como histórica o expirada si es posible.
     - Actualizar las secciones `assertionMethod` y `authentication` para que apunten a la nueva clave.

     Llamada API (para publicar el did.json en el servidor web):
     PUT /var/www/html/.well-known/did.json (Ejemplo de despliegue en servidor web)
  3. **Activación de la Nueva Clave**: El portal `Inji-Certify` se configura para usar la nueva clave (`key-2`) para firmar todas las nuevas credenciales.
- **Mecanismo Técnico (Compromiso de Clave de Emergencia)**:

1. **Revocación Inmediata**: El Documento DID se actualiza inmediatamente para eliminar la clave comprometida de `assertionMethod`. Esto invalida su uso para nuevas firmas.
2. **Plan de Re-emisión**: Se debe notificar a todos los ciudadanos que necesitan solicitar una re-emisión de su licencia, ya que las antiguas, aunque no expiradas, podrían no ser confiables.
3. **Actualización de Verificadores**: Las aplicaciones de los verificadores deben forzar una actualización de la caché de la clave del INTRANT para asegurarse de que ya no confían en la clave comprometida.

- **Impacto**: Una rotación bien planificada es transparente para los usuarios. Un compromiso de clave es un incidente de seguridad grave que requiere una comunicación pública clara y una acción rápida de re-emisión.

Caso de Uso 3: Mantenimiento de la Lista de Estado de Credenciales

Garantiza que el mecanismo de revocación funcione de manera eficiente y escalable.

- **Actor**: Administrador del Sistema (OGTIC).
- **Trigger**: La lista de estado actual (bitmap) se está llenando o ha alcanzado un tamaño que afecta el rendimiento.
- **Mecanismo Técnico**:
  1. **Creación de una Nueva Lista**: Se genera una nueva lista de estado vacía.
     - **Llamada API (Interna)**: `POST https://api.intrant.gob.do/v1/statuslists`
     - **Respuesta**: Devuelve el ID y la URL de la nueva lista (ej. `.../status/2`).
  2. **Configuración del Emisor**: El portal `Inji-Certify` se configura para que todas las nuevas credenciales emitidas apunten a esta nueva lista en su propiedad `credentialStatus`.
  3. **Archivado de la Lista Antigua**: La lista antigua (`.../status/1`) se mantiene activa y disponible para que las credenciales ya emitidas que apuntan a ella puedan seguir siendo verificadas, pero ya no se le añaden nuevas revocaciones.
- **Impacto**: Es una tarea de mantenimiento rutinario y transparente para los usuarios finales, pero crucial para el rendimiento y la escalabilidad del sistema de revocación.

Caso de Uso 4: Monitoreo, Auditoría y Alertas del Sistema

Es el proceso continuo de vigilancia para asegurar la salud y seguridad del ecosistema.

- **Actor**: Administrador del Sistema y Oficial de Seguridad (OGTIC).
- **Trigger**: Continuo (24/7).
- **Mecanismo Técnico**:
  1. **Recolección de Logs**: Todos los componentes (servidores de API, HSM, portal de emisión, base de datos) envían sus logs a un sistema **SIEM** centralizado. Los logs deben incluir:
     - Intentos de acceso (exitosos y fallidos).
     - Cada emisión de credencial (quién la autorizó, a quién, cuándo).
     - Cada verificación de estado de revocación.
     - Errores del sistema y métricas de rendimiento (latencia, tasa de errores).
  2. **Creación de Paneles (Dashboards)**: Se configuran paneles en el SIEM o en herramientas como Grafana para visualizar en tiempo real:
     - Disponibilidad (Uptime) de las APIs críticas.
     - Número de credenciales emitidas por día/hora.
     - Latencia promedio de las verificaciones.
     - Mapa de geolocalización de las solicitudes de verificación.
  3. **Configuración de Alertas**: Se definen reglas para generar alertas automáticas (vía email, Slack, PagerDuty) ante eventos anómalos.
     - **Ejemplos de Alertas de Seguridad**:
       - Múltiples intentos de inicio de sesión fallidos para un administrador.
       - Emisión de credenciales fuera del horario laboral normal.
       - Una tasa de error del 5% o más en la API de verificación.
       - Un intento de acceso al HSM desde una IP no autorizada.
- **Impacto**: Permite la detección proactiva de problemas de rendimiento y brechas de seguridad, reduciendo el tiempo de respuesta ante incidentes. Genera un registro de auditoría inmutable crucial para investigaciones forenses.

Revisión #2
Creado 17 junio 2025 18:55:19 por Tomás Familia
Actualizado 17 junio 2025 19:30:00 por Tomás Familia