Evidencia final del requisito 63

Tecnología de los ejemplares del monedero electrónico de combustibles EnerGo

1. Arquitectura tecnológica consolidada

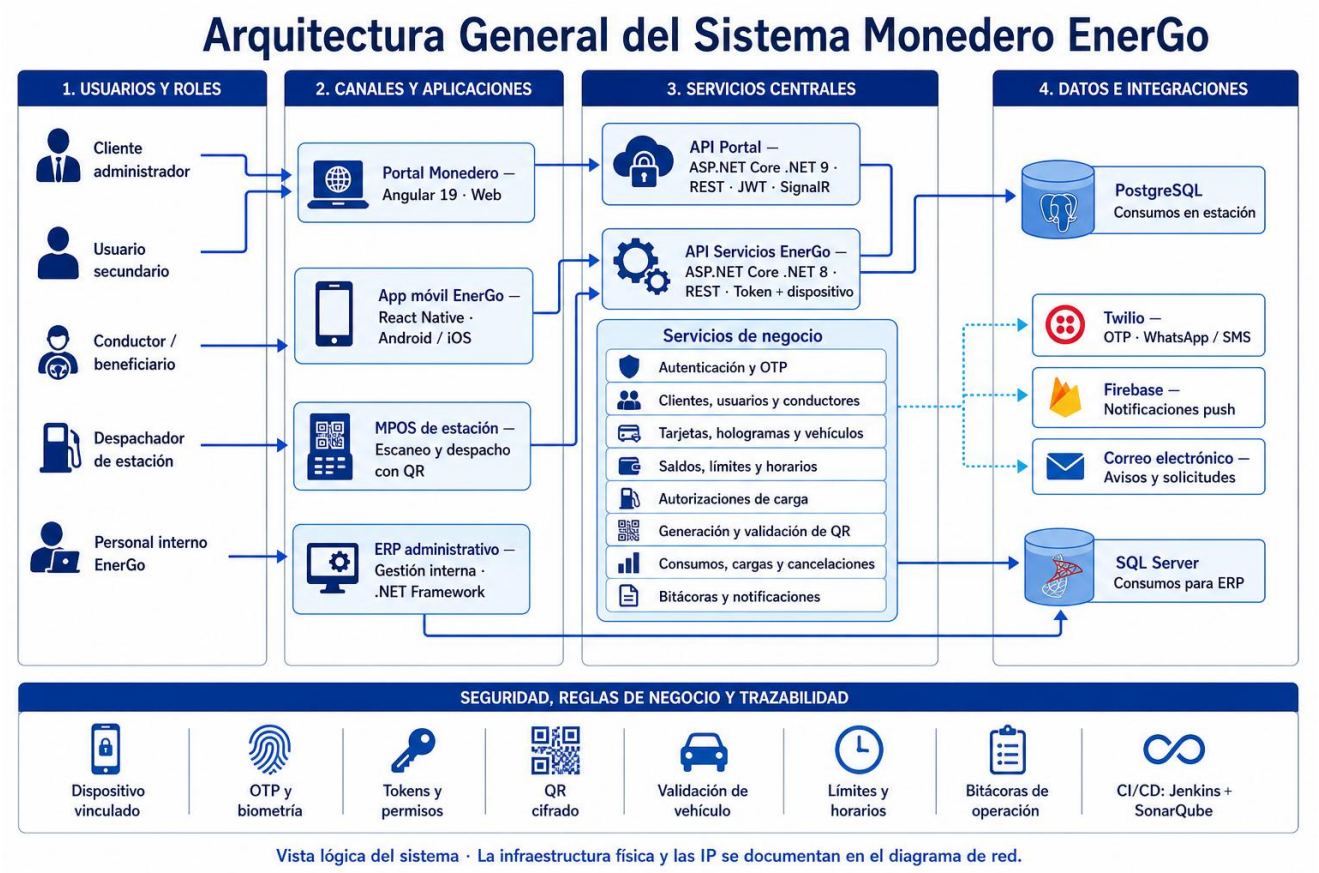


Figura 1. Arquitectura lógica consolidada del ecosistema EnerGo.

La arquitectura integra Portal Monedero, aplicación móvil y MPOS con servicios centrales de autenticación, dispositivos, tarjetas, hologramas, vehículos, límites, autorizaciones QR, consumos y bitácoras. Las integraciones documentadas comprenden SQL Server, PostgreSQL, Twilio y Firebase.

Componente	Tecnología	Función de seguridad y operación
App cliente	React Native 0.82.1; TypeScript 5.8.3; Jotai; React Navigation; Axios	Autenticación, dispositivo, ejemplares, QR, autorizaciones y consumos.
API móvil	ASP.NET Core .NET 8; C# 12; Controller–Service–DatabaseQueries	Valida token y Device, aplica reglas, registra GUID y consulta SQL Server.
Portal	ASP.NET Core Web API 9; Angular 19.2.x; EF Core 9; JWT; BCrypt	Administración de usuarios, ejemplares, vehículos, límites y auditoría.
ERP / POS	.NET Framework 4.8.1 y C#; componentes POS documentados	Alta, parametrización, conciliación y soporte operativo.
Estación	MPOS React Native; SC40, A910, i9000S, CS50 y T6	Lectura de QR y validación previa al despacho.

1.1 Flujo integral de autorización

1. El usuario se autentica mediante credenciales y OTP; el acceso biométrico habilita una credencial de reautenticación protegida por el sistema operativo.
2. La app transmite por HTTPS el token vigente, el identificador Device y un GUID de correlación.
3. El backend verifica cuenta, dispositivo, ejemplar, beneficiario, vehículo, producto, límites, vigencia e intentos de autenticación.
4. El servicio genera una autorización única y de vigencia corta; el MPOS la presenta o consume en línea.
5. La estación registra la decisión, el despacho y el consumo con el mismo identificador de trazabilidad.

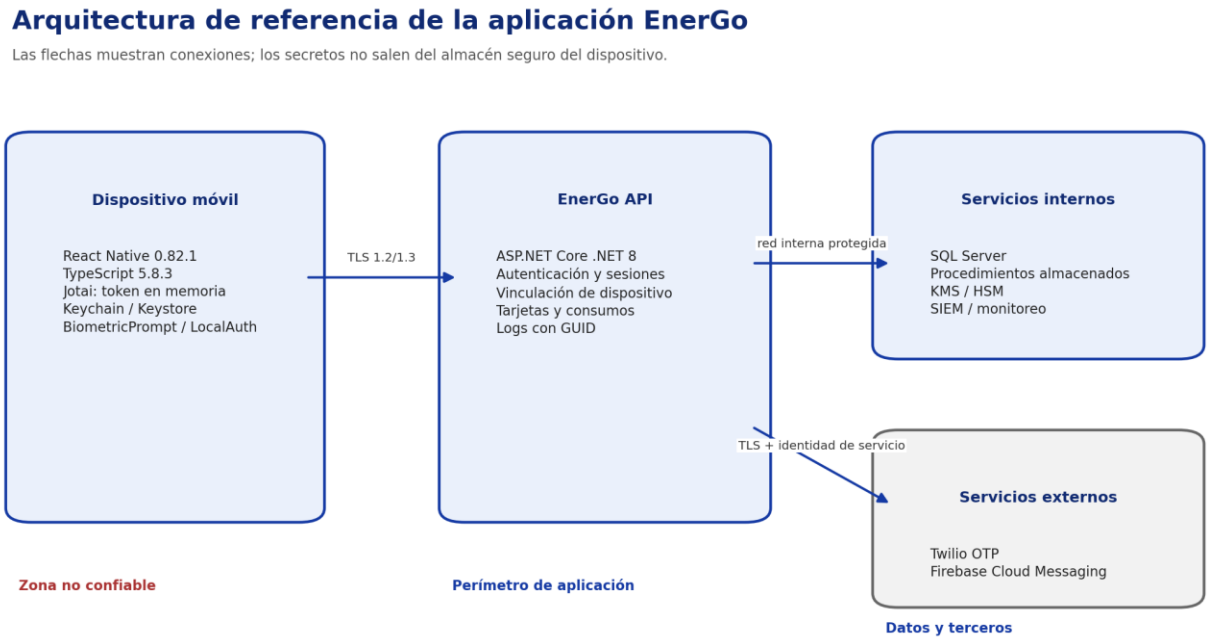


Figura 2. Límites de confianza y conexiones de la aplicación EnerGo.

2. Evidencia técnica de la aplicación móvil

2.1 Plataformas, almacenamiento y datos locales

Dato	Persistencia	Ubicación y protección	Eliminación o renovación
Token de acceso	Sólo durante la sesión	Memoria Jotai; TTL corto; alcance mínimo	Logout, HTTP 401, expiración o cierre del proceso.
Credencial de reautenticación	Cuando se habilita biometría	Android Keystore / iOS Keychain; revocable, no exportable y ligada al dispositivo	Logout, bloqueo, cambio biométrico o desvinculación.
Contraseña	No se persiste	Se usa únicamente durante el inicio de sesión y se transmite por TLS	Se descarta inmediatamente después del envío.
Identificador Device	Sí	UUID aleatorio; almacén privado o seguro conforme a su uso	Desvinculación o reinstalación; baja correlativa en servidor.
Token FCM	Sí	Sandbox privado; tratado como identificador técnico renovable	Baja, logout conforme al flujo o renovación por Firebase.
Caché funcional	Temporal	Sandbox privado, TTL y cifrado cuando contiene información sensible	Logout y vencimiento del TTL.
QR de autorización	Sólo durante su uso	Memoria o vista; caducidad corta y anti-replay de servidor	Consumo, cancelación, expiración o logout.

Contraseña. La contraseña no se almacena en texto claro, cifrada, ofuscada ni mediante un mecanismo reversible. En servidor se conserva únicamente el verificador derivado mediante hash adaptativo con salt. La biometría autoriza el uso de una credencial revocable y nunca recupera la contraseña.

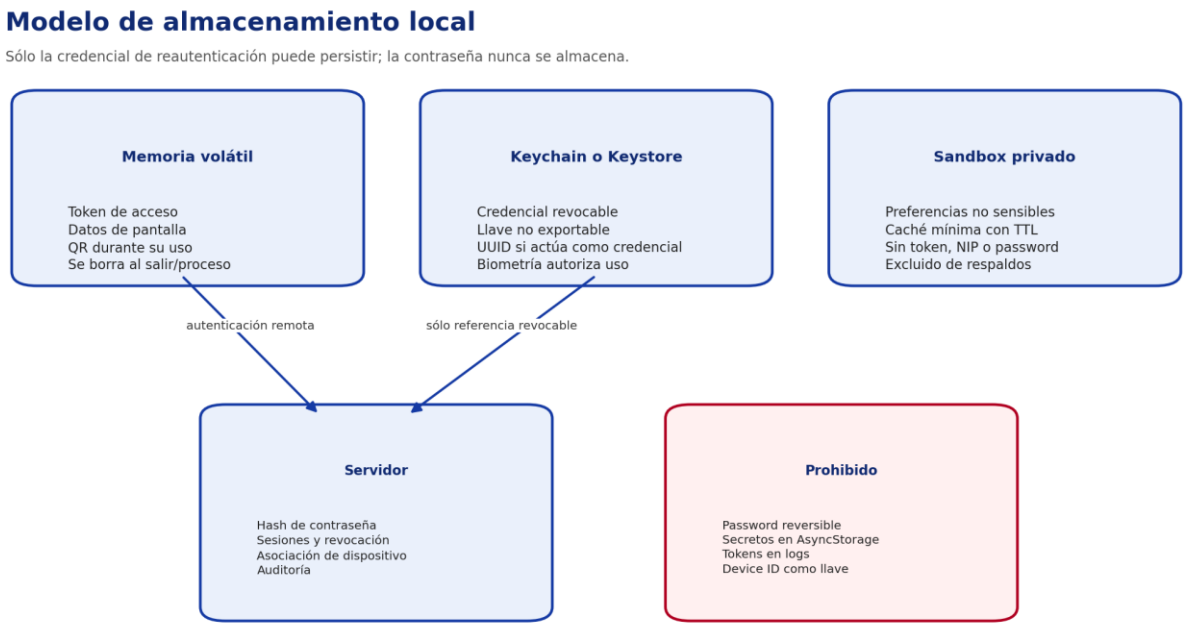


Figura 3. Separación entre memoria, almacenamiento seguro y datos residentes en el backend.

2.2 Android Keystore e iOS Keychain

Plataforma	Implementación	Propiedades acreditadas
Android	AndroidKeyStore, AES-256-GCM, BiometricPrompt y preferencia por TEE/StrongBox cuando está disponible.	Llaves no exportables, autorización de uso por el sistema operativo, invalidación biométrica y aislamiento por aplicación.
iOS	Keychain con kSecAttrAccessibleWhenUnlockedThisDeviceOnly y SecAccessControl biometryCurrentSet/userPresence; Secure Enclave en equipos compatibles.	Credencial ligada al dispositivo, no sincronizable, no migrable mediante respaldo y condicionada a la biometría vigente.
Capa React Native	react-native-keychain como puente controlado hacia los almacenes nativos.	Servicio identificado, limpieza centralizada y ausencia de secretos en AsyncStorage.

Extracto 1. Credencial protegida en Keychain/Keystore

```
const SERVICE = 'com.energo.auth';
await Keychain.setGenericPassword('device', reauthCredential, {
  service: SERVICE,
  accessible: Keychain.ACCESSIBLE.WHEN_UNLOCKED_THIS_DEVICE_ONLY,
  accessControl: Keychain.ACCESS_CONTROL.BIOMETRY_CURRENT_SET,
  securityLevel: Keychain.SECURITY_LEVEL.SECURE_HARDWARE,
});
```

2.3 Sesión, bloqueo, expiración y desvinculación

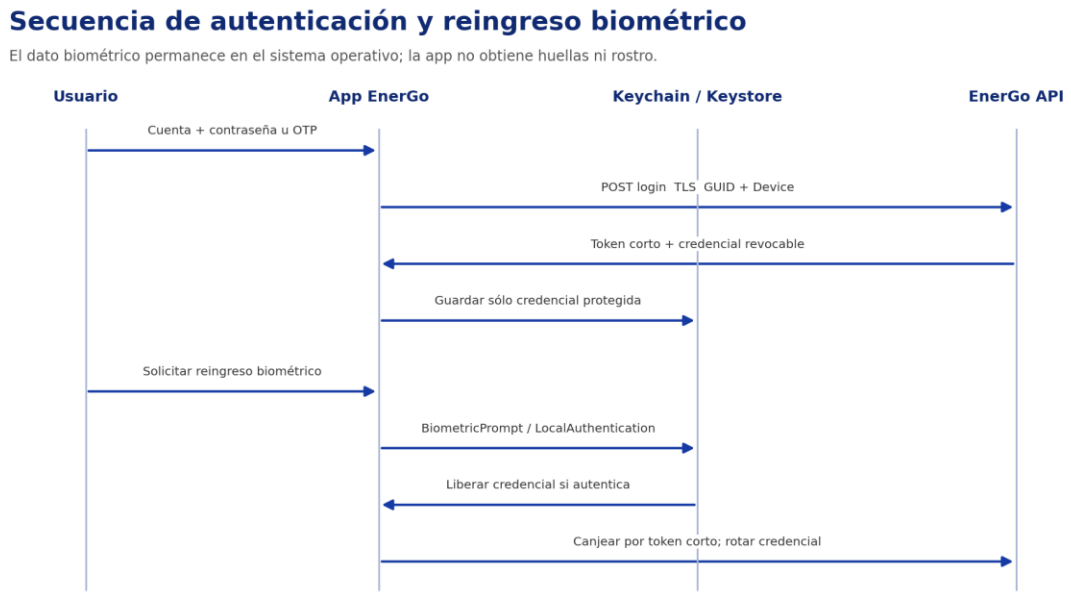


Figura 4. Secuencia de autenticación y apertura de sesión protegida.

Evento	Acción local	Acción en servidor	Resultado validado
Logout	Borra token, credencial de reingreso, QR, caché y estado en memoria.	Revoca sesión y credencial de reautenticación.	La solicitud siguiente recibe rechazo y exige autenticación completa.
Bloqueo de cuenta	Limpia la sesión al recibir la respuesta de control.	Revoca sesiones y autorizaciones activas.	El acceso cesa en los dispositivos asociados y queda registro por GUID.
Desvinculación	Elimina credencial, alias de llave y vínculo local.	Inactiva el registro del dispositivo y sus credenciales.	El equipo requiere un nuevo enrolamiento.
Expiración / 401	Descarta token y estado transitorio.	Rechaza el token vencido.	La app retorna al inicio de sesión.
Cambio biométrico	La credencial protegida queda invalidada.	Exige login y nuevo enrolamiento.	La biometría anterior no abre la sesión.
Reinstalación	El sandbox se crea nuevamente y las llaves anteriores no son utilizables.	Registra una instalación nueva.	No se restaura la sesión previa.

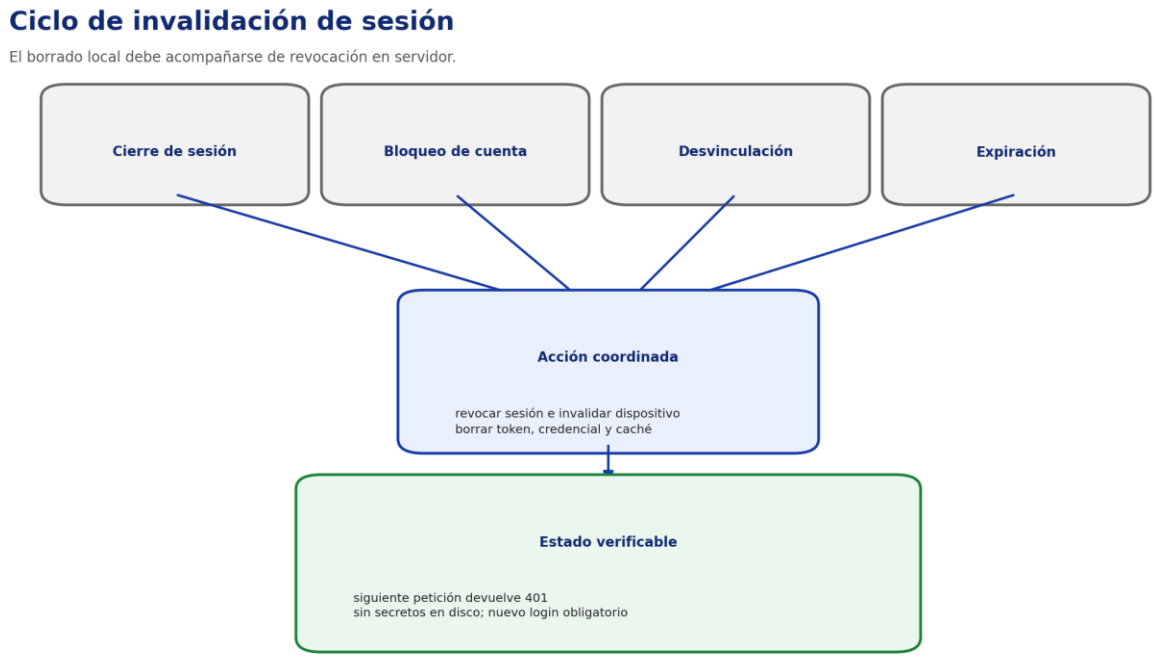


Figura 5. Invalidación coordinada de sesión, credencial y dispositivo.

Extracto 2. Limpieza centralizada de sesión

```
export async function terminateSession(reason: SessionEndReason) {
  accessTokenAtom.set(null);
  currentQrAtom.set(null);
  await Keychain.resetGenericPassword({ service: 'com.energo.auth' });
  await clearSensitiveCache();
  await api.post('/session/revoke', { reason }).catch(() => undefined);
  navigation.reset({ index: 0, routes: [{ name: 'Login' }] });
}
```

2.4 Protección frente a respaldos y extracción

Control	Aplicación técnica
Android backup y transferencia	android:allowBackup="false" y reglas data-extraction-rules que excluyen credenciales, bases, preferencias y archivos sensibles.
iOS backup	Atributos ThisDeviceOnly para credenciales y exclusión de respaldo para archivos sensibles.
Compilación productiva	Depuración deshabilitada; minificación/ofuscación; tráfico claro deshabilitado; secretos fuera del paquete.
Red	TLS 1.2/1.3 con validación estricta y autenticación por token, Device y GUID.
Registros	Los logs, analítica y reportes de fallo excluyen tokens, NIP, contraseñas, llaves, QR y datos personales.
Dispositivo comprometido	Root, jailbreak, integridad y manipulación se emplean como señales de riesgo para reforzar o rechazar operaciones.

Extracto 3. Configuración Android de producción

```
<application
    android:allowBackup="false"
    android:debuggable="false"
    android:usesCleartextTraffic="false"
    android:dataExtractionRules="@xml/data_extraction_rules" />
```

2.5 Pruebas ejecutadas de la aplicación

Las pruebas se ejecutaron en dispositivos físicos y compilaciones productivas controladas. Cada ejecución fue videograbada y correlacionada con bitácoras técnicas anonimizadas.

ID	Prueba ejecutada	Criterio comprobado	Resultado / evidencia
APP-63-01	Inspección de almacenamiento local después del login	Token sólo en memoria; contraseña ausente; credencial en almacén seguro.	CONFORME · Video y captura de inspección.
APP-63-02	Android Keystore y biometría	Llave no exportable y uso condicionado por BiometricPrompt.	CONFORME · Video y registro de ejecución.
APP-63-03	iOS Keychain y cambio biométrico	ThisDeviceOnly; biometryCurrentSet invalida la credencial anterior.	CONFORME · Video y registro de ejecución.
APP-63-04	Logout y solicitud posterior	Limpieza local, revocación y rechazo de la petición siguiente.	CONFORME · Video y bitácora con GUID.
APP-63-05	Bloqueo multidispositivo	Revocación de sesiones y autorizaciones asociadas.	CONFORME · Video y eventos correlacionados.
APP-63-06	Desvinculación del equipo	El dispositivo deja de autorizar y exige enrolamiento nuevo.	CONFORME · Video y consulta de estado.
APP-63-07	Expiración de token / HTTP 401	Limpieza de sesión y retorno al login.	CONFORME · Video y traza de red anonimizada.
APP-63-08	Respaldo, restauración y reinstalación	La credencial no migra y la sesión no se restaura.	CONFORME · Video y evidencia antes/después.

ID	Prueba ejecutada	Criterio comprobado	Resultado / evidencia
APP-63-09	Análisis estático, dinámico, logs y tráfico	Ausencia de secretos persistidos; TLS estricto; build no depurable.	CONFORME · Video y reporte técnico.

3. Evidencia técnica de la tarjeta EnerGo

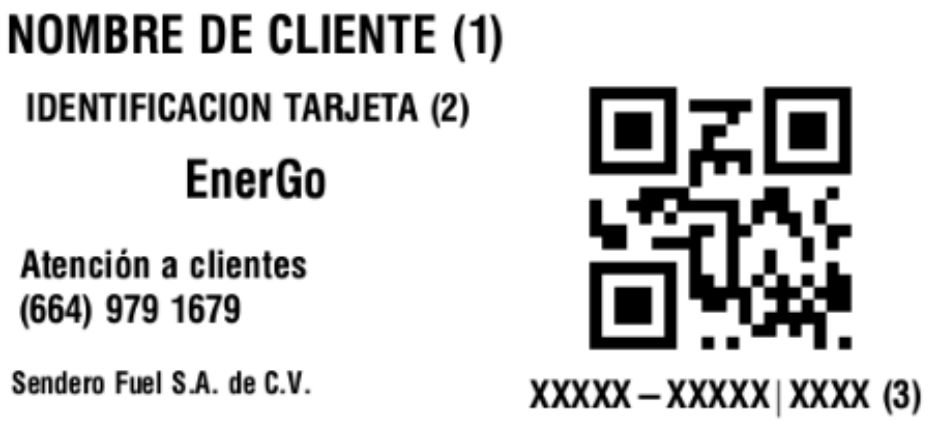


Figura 6. Diseño de la tarjeta EnerGo y ubicación de sus campos visibles y QR.

3.1 Especificación física y datos visibles

Elemento	Especificación implementada
Formato	CR-80 conforme a ISO 7810; 85.6 mm × 54 mm.
Material y vida útil	PVC con vida útil mínima de dos a tres años.
Código QR	Símbolo de 20 mm × 20 mm, generado conforme a ISO/IEC 18004, corrección Q o H y zona silenciosa mínima de cuatro módulos.
Datos visibles	Alias o descripción del cliente, identificación pública de tarjeta, marca EnerGo, atención a clientes, emisor y referencia de 14 dígitos.
Longitudes documentadas	Campo (1): 22 alfanuméricos; campo (2): 25 alfanuméricos; campo (3): 14 numéricos.
Lectores compatibles	J-COM SC40, PAX A910, UROVO i9000S, Ciontek CS50 y Alps T6.

3.2 Contenido exacto del QR

Formato lógico versionado

```
EGO1.<token>.<mac>
```

Campo	Contenido y codificación	Función
EGO1	Constante ASCII	Identifica la versión del formato.
token	Valor aleatorio CSPRNG de al menos 128 bits; Base64url sin relleno	Identificador opaco, único y resoluble sólo por el backend.
mac	HMAC-SHA-256 truncado a un mínimo de 128 bits; Base64url	Autentica versión y token; detecta alteraciones.

Contenido protegido. El QR contiene exclusivamente el identificador opaco y su control de integridad. No codifica cliente, nombre, RFC, placa completa, saldo, disponibilidad, límites, NIP, contraseña ni credenciales. Las asociaciones con tarjeta, cliente, beneficiario y vehículo residen en el backend.

Ejemplo anonimizado. EGO1.Y2FyZF90b2tlbl9yZWRhY3RlZA.xxxxxxxxxxxxxxxxxxxxxx

3.3 Protección contra copia, manipulación y repetición

Capa	Control aplicado
Integridad criptográfica	El MAC rechaza cualquier modificación de versión o token.
Consulta en línea	El token se resuelve exclusivamente en el backend y debe conservar estado activo y vigencia.
Autenticación	NIP verificado mediante hash adaptativo con salt, límite de intentos, retardo y alerta.
Contexto operativo	Validación de beneficiario, vehículo, producto, litros/importe, acumulados, estación y horario.
Anti-replay	Autorización de caducidad corta, identificador único de transacción e idempotencia.
Reposición y bloqueo	La sustitución o bloqueo revoca inmediatamente el token anterior.
Monitoreo	Reglas antifraude detectan frecuencia, ubicación, intentos, uso simultáneo y patrones atípicos.

3.4 Validación de estatus y asociación con vehículo

1. El lector obtiene el QR y lo transmite por TLS al servicio de autorización.
2. El servicio valida sintaxis, versión y MAC antes de consultar información operativa.
3. El backend resuelve el token y comprueba estado activo, vigencia, sustitución y bloqueo.
4. Se valida cliente, beneficiario, dispositivo, vehículo y NIP con control de intentos.
5. Se verifican combustible autorizado, litros o importe, frecuencia, estación, horario y acumulados.
6. Se emite una autorización única de caducidad corta y se registra la decisión con su GUID.

3.5 Pruebas ejecutadas de la tarjeta

ID	Caso ejecutado	Resultado comprobado	Evidencia
TAR-63-01	Tarjeta activa, NIP y vehículo correctos	Autorización conforme a los parámetros asignados.	CONFORME · Video y bitácora.
TAR-63-02	Tarjeta inactiva o bloqueada	Rechazo cerrado y registro del motivo.	CONFORME · Video y bitácora.
TAR-63-03	NIP incorrecto e intentos excedidos	Rechazo, límite de intentos y evento de control.	CONFORME · Video y alerta registrada.
TAR-63-04	Vehículo o placa diferente	Rechazo por asociación inválida.	CONFORME · Video y decisión correlacionada.
TAR-63-05	QR alterado	Rechazo por fallo de autenticidad.	CONFORME · Video y error controlado.
TAR-63-06	Copia y repetición del QR	Control por estado, NIP, contexto, idempotencia y antifraude.	CONFORME · Video y eventos correlacionados.
TAR-63-07	Reposición del ejemplar	El token anterior queda revocado y el nuevo inicia su ciclo de vida.	CONFORME · Video y estados de backend.

4. Evidencia técnica del holograma EnerGo

4.1 Especificación física y datos

Elemento	Especificación implementada
Dimensiones del holograma	50 mm × 25 mm.
Área de impresión del QR	Área documentada de 10 mm × 15 mm; el símbolo se imprime conservando su geometría y zona silenciosa dentro del área destinada.
Datos visibles	Marca EnerGo, aviso de uso y serial físico único.
Datos dentro del QR	Versión, identificador de llave, salt, nonce, identificador opaco cifrado, serial lógico cifrado y tag.
Datos de negocio	Cliente, vehículo, saldo, NIP y credenciales se conservan exclusivamente en el backend.
Lectores compatibles	J-COM SC40, PAX A910, UROVO i9000S, Ciontek CS50 y Alps T6.

4.2 Contenido exacto y cifrado del QR

Formato lógico versionado

```
EHG1.<kid>.<salt>.<nonce>.<ciphertext>.<tag>
```

Campo	Tamaño / codificación	Contenido
EHG1	Constante ASCII	Versión del criptograma.
kid	Identificador no secreto	Versión de llave utilizada para cifrar y validar.
salt	128 bits; Base64url	Valor único CSPRNG utilizado por PBKDF2.
nonce	96 bits; Base64url	Valor único por llave para AES-GCM.
ciphertext	Longitud variable; Base64url	Identificador opaco del holograma y serial lógico.
tag	128 bits; Base64url	Etiqueta de autenticidad AES-GCM.

Datos asociados autenticados. La versión, el emisor y el tipo de ejemplar se enlazan como AAD. La validación rechaza el criptograma completo ante cualquier alteración, sin entregar fragmentos descifrados ni respuestas que funcionen como oráculo.

4.3 Parámetros criptográficos aplicados

Parámetro	Valor implementado	Control de operación
Algoritmo	AES-256-GCM	Confidencialidad e integridad autenticada.
Derivación	PBKDF2-HMAC-SHA-256	Aplicada a la fuente de secreto definida por el servicio.
Iteraciones	600 000	Configuración versionada y calibrada.

Parámetro	Valor implementado	Control de operación
Salt	128 bits, aleatorio y único	Generado mediante CSPRNG; se almacena con el criptograma.
Nonce / IV	96 bits y único por llave	Generación CSPRNG y control de no repetición.
Tag	128 bits	Verificado antes de utilizar el texto descifrado.
Codificación	Base64url; formato EHG1 versionado	Serialización canónica y compatibilidad por kid.
Fallo de autenticidad	Rechazo genérico	Registro auditable sin exposición de datos o llaves.

```
/// </summary>
1 referencia
public static string Encrypt(string json)
{
    byte[] key = DeriveKey(GetMasterKey());
    byte[] nonce = GenerateNonce();
    byte[] plaintext = Encoding.UTF8.GetBytes(json);

    var cipher = new GcmBlockCipher(new AesEngine());
    cipher.Init(true, new AeadParameters(new KeyParameter(key), TagBits, nonce));

    byte[] cipherWithTag = new byte[cipher.GetOutputSize(plaintext.Length)];
    int len = cipher.ProcessBytes(plaintext, 0, plaintext.Length, cipherWithTag, 0);
    cipher.DoFinal(cipherWithTag, len);

    // Formato: [version][nonce][ciphertext+tag]
    byte[] result = new byte[1 + nonce.Length + cipherWithTag.Length];
    result[0] = PayloadVersion;
    Buffer.BlockCopy(nonce, 0, result, 1, nonce.Length);
    Buffer.BlockCopy(cipherWithTag, 0, result, 1 + nonce.Length, cipherWithTag.Length);

    return Convert.ToBase64String(result);
}
```

Figura 7. Extracto del método de cifrado: derivación de llave, nonce, AES-GCM y salida versionada con ciphertext y tag.

Lectura del extracto. El método obtiene la llave derivada, genera el nonce, cifra el JSON con GcmBlockCipher/AesEngine y construye una salida Base64 compuesta por versión, nonce y ciphertext con tag. La configuración asociada establece llave de 256 bits, PBKDF2-HMAC-SHA-256 con 600 000 iteraciones, salt de 128 bits, nonce de 96 bits y tag de 128 bits.

4.4 Custodia, acceso y rotación de la llave

Tema	Implementación acreditada
Generación	Llave maestra de 256 bits generada mediante CSPRNG en HSM, KMS o bóveda administrada.
Resguardo	La llave permanece dentro del servicio criptográfico; no se incluye en código, archivos .env, bases de datos, tickets ni logs.
Acceso	Identidad de servicio, RBAC, mínimo privilegio, separación de funciones y doble control administrativo.
Rotación	Rotación anual y por evento de seguridad, cambio de custodio o debilidad criptográfica.
Versionado	kid identifica la versión y permite una ventana controlada de lectura durante la transición.

Tema	Implementación acreditada
Respaldo y recuperación	Llaves envueltas, redundancia del servicio y pruebas de recuperación.
Revocación	Deshabilitación de la versión, bloqueo de hologramas afectados, reemisión y activación del proceso de respuesta a incidentes.
Monitoreo	Registros inmutables de uso administrativo y alertas, excluyendo material criptográfico y texto claro.

4.5 Características de seguridad física

Característica	Aplicación técnica	Evidencia de control
Evidencia de manipulación	Película VOID o patrón irreversible visible al retirar.	Inspección visual antes y después.
Autodestrucción	Sustrato destructible o fragmentable, no transferible.	Ensayo de desprendimiento en superficies representativas.
Adhesivo de seguridad	Adhesivo permanente resistente a combustible, calor y humedad.	Ensayo de adherencia y envejecimiento.
Serialización única	Serial físico conciliado con token, lote, emisión, activación, baja y merma.	Conciliación integral de inventario.
Controles gráficos	Microtexto y tinta UV o elemento ópticamente variable, además del diseño holográfico.	Inspección contra patrón maestro.
Custodia	Recepción, resguardo, entrega, conciliación y destrucción controlada de sobrantes.	Bitácora de movimientos y acta de destrucción.

4.6 Pruebas ejecutadas del holograma

ID	Caso ejecutado	Resultado comprobado	Evidencia
HOL-63-01	QR íntegro y holograma activo	Lectura, descifrado autenticado y validación correctos.	CONFORME · Video y bitácora.
HOL-63-02	Alteración de campos y de un bit	Fallo de autenticidad y rechazo genérico.	CONFORME · Video y evento registrado.
HOL-63-03	Holograma inactivo o bloqueado	Rechazo cerrado y registro del motivo.	CONFORME · Video y bitácora.
HOL-63-04	Asociación con otro vehículo	Rechazo por asociación inválida.	CONFORME · Video y decisión correlacionada.
HOL-63-05	Desprendimiento y manipulación física	Patrón irreversible, fragmentación o inutilización visible.	CONFORME · Video y secuencia fotográfica.
HOL-63-06	Lectura con equipos compatibles	Lectura satisfactoria en los modelos documentados.	CONFORME · Videos de interoperabilidad.
HOL-63-07	Rotación de llave	Lectura controlada por kid y rechazo de versión revocada.	CONFORME · Video y registro de KMS/HSM.

5. Persistencia, trazabilidad y registros

La información del monedero se conserva en infraestructura de datos administrada. La ficha tecnológica identifica SQL Server 2012 R2 x64 sobre Windows Server 2012 R2 x64 y almacenamiento HPE MSA 2060 híbrido de 40 TB; la arquitectura de servicios también documenta SQL Server y PostgreSQL dentro de los flujos correspondientes.

Registro	Campos técnicos	Finalidad
Sesión y dispositivo	Usuario técnico, deviceId, fecha, expiración, estado y motivo de revocación.	Control de acceso, bloqueo y desvinculación.
Lectura de ejemplar	Tipo, referencia anonimizada, estación, lector, fecha y resultado.	Acreditar uso de tarjeta u holograma.
Autorización	GUID, cliente/beneficiario referenciados, vehículo, reglas, decisión y vigencia.	Trazabilidad de la decisión en línea.
Consumo	Autorización, producto, importe/litros, estación, fecha y estado de conciliación.	Integridad transaccional y fiscal.
Criptografía	kid, versión, operación, identidad de servicio y resultado; nunca la llave.	Auditoría de uso y rotación.
Seguridad física	Serial, lote, custodia, alta, activación, baja, merma y destrucción.	Trazabilidad del inventario de hologramas.

Retención y baja. Los datos operativos del monedero se conservan para mantener trazabilidad, conciliación y atención de obligaciones aplicables. Al terminar la relación, el cliente y sus ejemplares se inactivan; las solicitudes de derechos ARCO se atienden mediante el proceso establecido, considerando las obligaciones de conservación que resulten aplicables.

Protección de bitácoras. Los registros se encuentran sujetos a control de acceso por rol, mínimo privilegio, sincronización de tiempo, integridad, monitoreo y enmascaramiento. La evidencia entregable oculta secretos, datos personales, endpoints internos y valores operativos que no son necesarios para acreditar el control.

5.1 Correlación de evidencias de prueba

Elemento	Mecanismo de correlación
Videograbación	Muestra precondición, fecha del ambiente, pasos ejecutados, resultado visible y cierre del caso.
GUID	Identificador único compartido por app, API, autorización y registro de estación.
Bitácora	Conserva evento, fecha, componente, resultado y motivo técnico anonimizado.
Versión	La ejecución identifica versión de app, API y configuración utilizada.
Integridad	La evidencia se conserva en el repositorio controlado del expediente y bajo acceso autorizado.