Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

MiDNI iOS

Declaración de Seguridad

21/11/2024

Versión 1.9

Historial de Cambios

Versión	Fecha	Cambios
1.0	08-04-2024	Primera versión
1.1	16-04-2024	Actualización
1.2	05-07-2024	Actualización
1.3	18-09-2024	Actualización
1.4	03-10-2024	Cambios menores según indicaciones
1.5	16-10-2024	Cambios menores según indicaciones
1.6	17-10-2024	Cambios menores según indicaciones
1.7	08-11-2024	Cambios menores según indicaciones
1.8	14-11-2024	Eliminación de referencia errónea.
1.9	21-11-2024	Corrección de tabla

CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1 INTRODUCCIÓN

Esta Declaración de Seguridad especifica los requisitos de Seguridad de la APP MiDNI iOS v1.0.0 (preproducción), un visor de datos de identidad del usuario en dispositivos móviles. En la misma se incluyen los siguientes puntos:

1) Información acerca de este documento
2) Descripción de la funcionalidad de la solución y casos de uso, que permite a las entidades hacer frente a las amenazas y riesgos que se describen en el documento.
3) Descripción del entorno de ejecución
4) Análisis de amenaza y riesgos de los dispositivos móviles.
5) Requisitos fundamentales de seguridad que esta solución cubre y cómo los cubre para implementar cada función de seguridad.

1.1 Información del Patrocinador, TOE y Evaluación

Tabla 1 Información del Patrocinador, TOE y Evaluación

Datos del Solicitante (Nombre y Dirección)	Real Casa de la Moneda Fábrica Nacional de Moneda y Timbre C/Jorge Juan 106, 28009 Madrid
Datos del Desarrollador (Nombre y Dirección)	Real Casa de la Moneda Fábrica Nacional de Moneda y Timbre C/Jorge Juan 106, 28009 Madrid
Nombre del TOE	MiDNI iOS
Versión del TOE	1.0.0 (preproducción)
Taxonomía del producto según CCN- STIC-140 y su versión	No aplica
Tipo de evaluación (incluir los módulos opcionales)	LINCE
Manuales de uso del producto y su versión	La información detallada sobre cada guía incluyendo su versión se puede encontrar en la sección **2.2. Identificación de las Guías de Uso, Instalación y configuración Seguras del TOE** en el presente documento

NOTA: El TOE en la *TestFlight* store se identificará con el nombre: “MiDNI Versión 1.0.0”. Esta versión se corresponde con la versión 1.0.0 (preproducción)

1.2 Metodología y Criterios de Evaluación

Tabla 2 Metodología de Evaluación

[CCN-LINCE-2001]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 2.0
[CCN-LINCE-2002]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), Versión 2.0
[CCN-LINCE-2003]	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 2.0
[CCN-LINCE-2004]	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 2.0

2 DESCRIPCIÓN DEL TOE

2.1 Descripción Funcional del TOE

El objetivo de la evaluación (desde ahora en adelante las siglas TOE) es MiDNI iOS v1.0.0 (preproducción), una aplicación APP que se ejecuta en un dispositivo móvil IOS. Es responsable del establecimiento de un canal seguro TLS v1.3 de comunicación entre el TOE y los servidores de datos de los ciudadanos perteneciente a la Dirección General de la Policía de España. El canal de información establecido está cifrado y autenticado en el extremo servidor, asegurando que dicha comunicación es segura. La integridad de los datos va protegida por los *token* de integridad de Apple.

El TOE MiDNI iOS v1.0.0 (preproducción) es desarrollado por la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (desde ahora en adelante las siglas FNMT) para los dispositivos iOS. El TOE proporciona la interfaz para la visualización de sus datos identificativos, que serán descargados de servicios web externos, pero no almacenará en el dispositivo dichos datos, sólo los esenciales para el correcto funcionamiento.

NOTA: Al tratarse de una aplicación en estado de preproducción, la aplicación no se encontrará disponible en ningún market de aplicaciones.

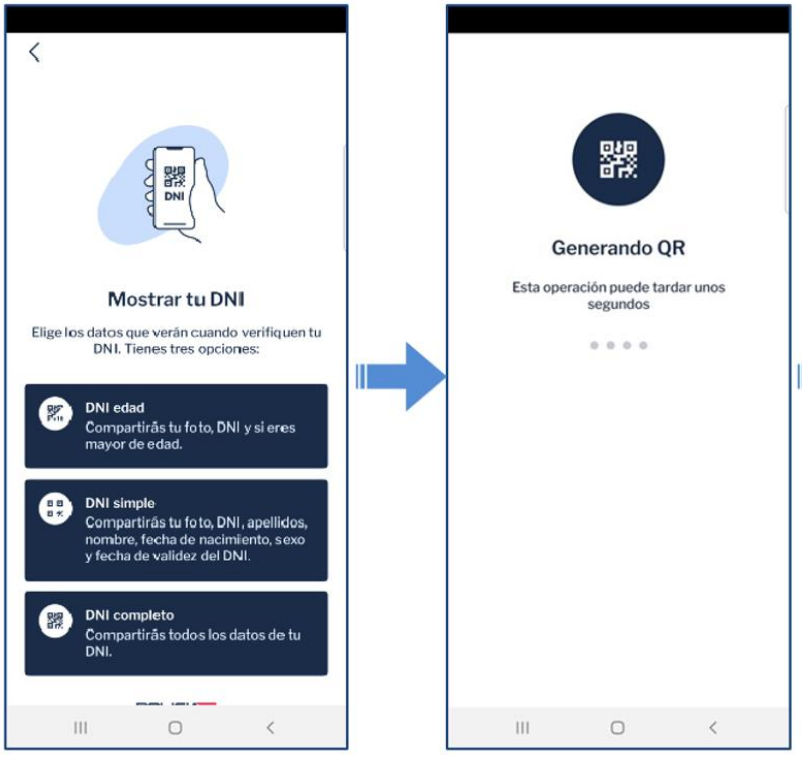

Ilustración 1: Generación de Código QR

Además, el TOE codifica y muestra en un código QR (*Quick Response*) los datos identificativos del usuario registrado y permite verificar los datos de un tercero.

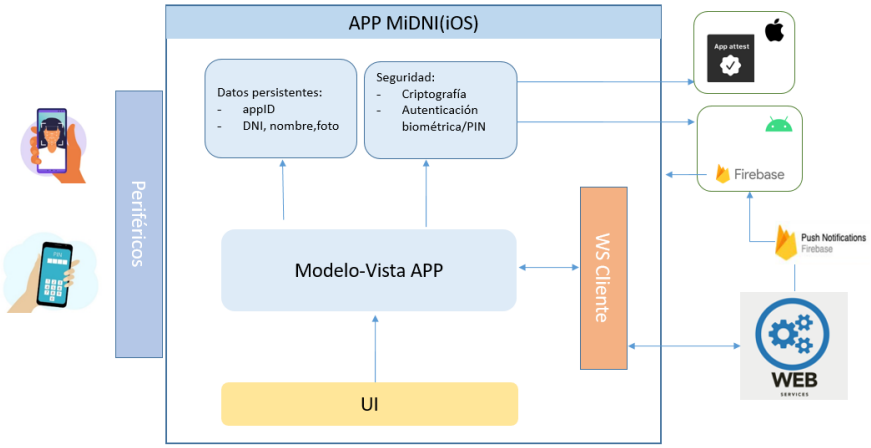

Ilustración 2: Arquitectura TOE[1]

La funcionalidad principal del TOE es mostrar parte de la información contenida en el Documento Nacional de Identidad (desde ahora en adelante las siglas DNI) de España en formato virtual (código QR) en vez del formato tradicional físico (tarjeta de policarbonato). Permite seleccionar entre tres únicas vistas virtuales:

- DNI EDAD: muestra la foto, número de DNI y si se es mayor de edad o no.
- DNI SIMPLE: muestra la foto, número de DNI, nombre completo, fecha nacimiento, sexo y fecha de validez.
- DNI COMPLETO: muestra el contenido completo de nuestro DNI virtual (destacar que no se incluye el número de soporte ni el equipo de expedición).

[1] Nótese que desde iOS también se requieren los servicios de Google para el *RemoteConfig* y las notificaciones (sección 2.1.1).

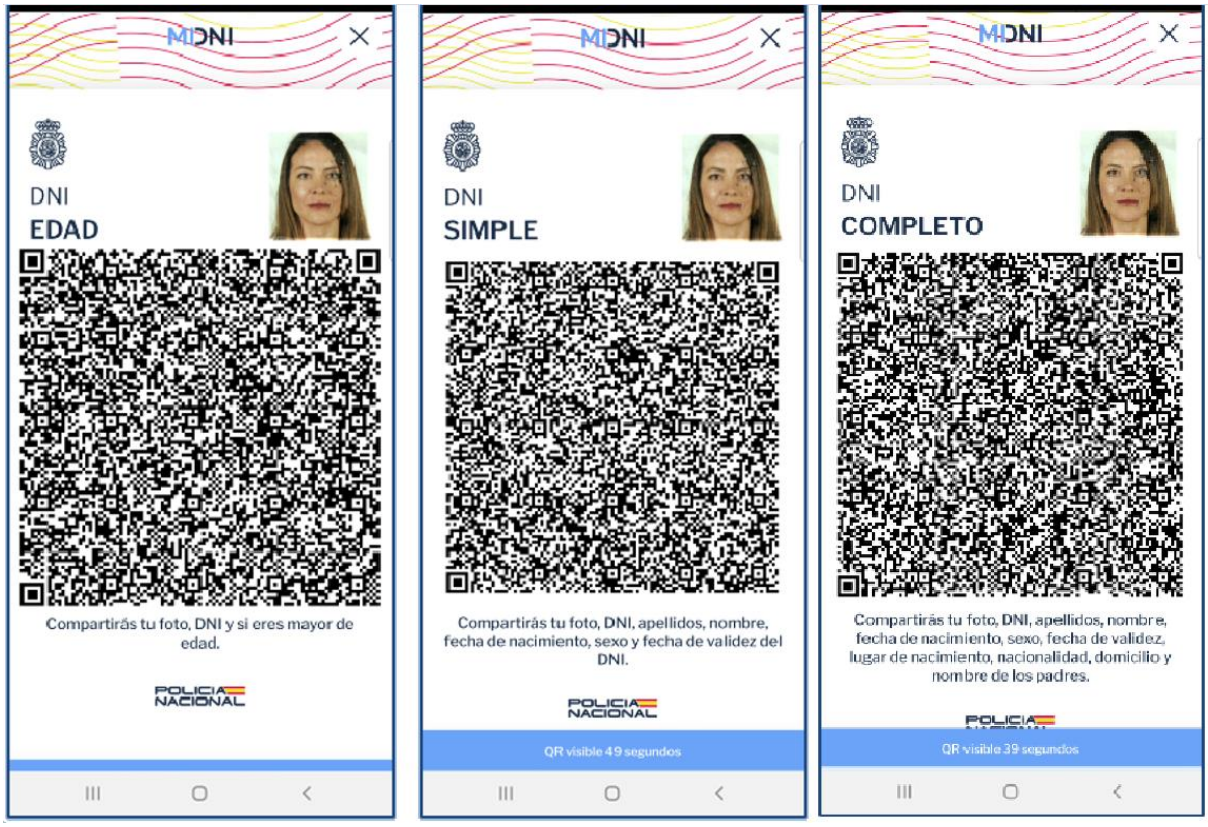

Ilustración 3: Funcionalidad principal del TOE (Generación QRs)

Estas vistas no son mostradas directamente en el dispositivo móvil IOS del usuario, sino que el TOE genera un código QR temporal que deber ser escaneado por otro usuario (en adelante el validador) usando la funcionalidad de verificación que también se proporciona en el TOE.

Nota: Cualquier usuario con el TOE puede verificar otro DNI virtual. No es necesario haberse registrado en el servicio “DNIe en el móvil” y haber virtualizado nuestro DNI para hacerlo.

Al verificar un documento, se mostrarán los datos que incluyese el código QR temporalmente generado por el titular de dicho DNI virtual:

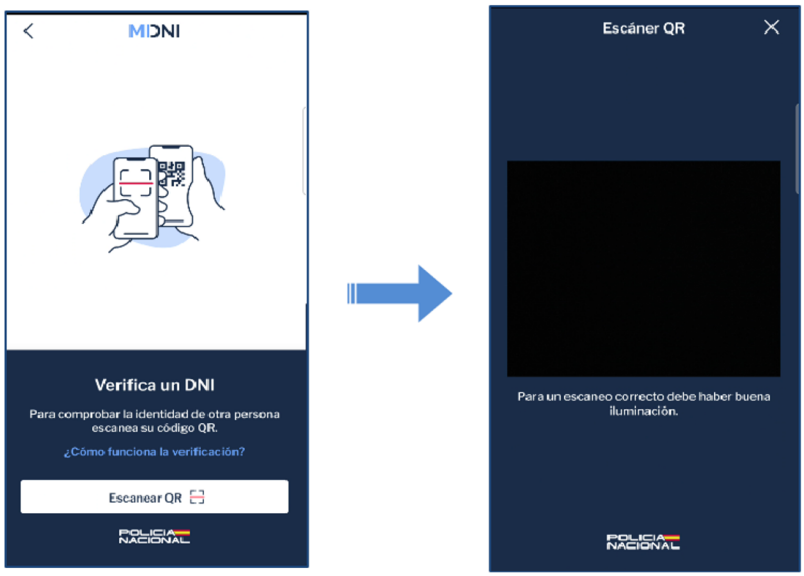

Ilustración 4: Verificación de Código QR

El TOE nos mostrará los datos del usuario incluidos en el código QR en función del tipo al que corresponde: mayor de edad, simple o completo.

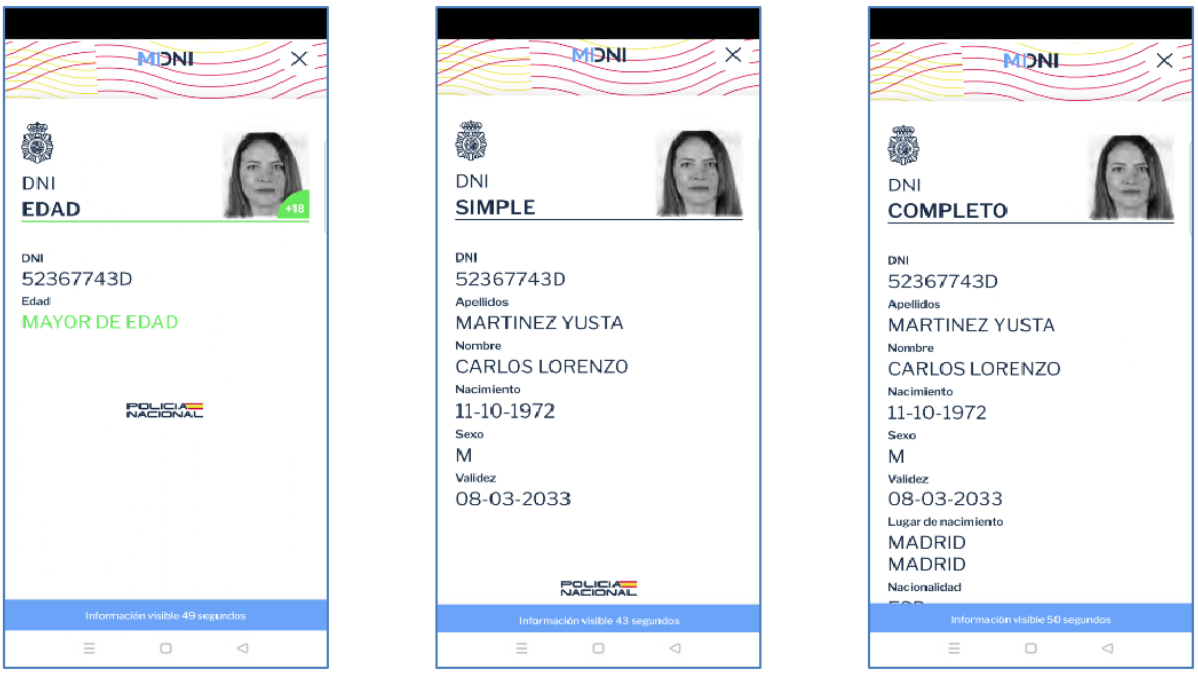

Ilustración 5: Funcionalidad principal del TOE (Verificación QRs)

El código QR generado con los datos del usuario tiene un tiempo máximo de visualización. Pasado ese tiempo, la pantalla se cierra automáticamente. En esta fase de desarrollo el tiempo en pantalla es de 1 minuto.

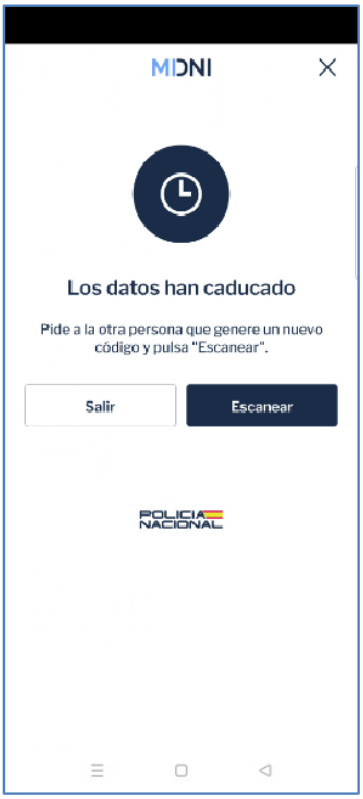

Ilustración 6: Mensaje de Caducidad de Visualización

Para realizar la funcionalidad de Virtualización o descarga de identidad (Generación de QR), se debe haber realizado previamente el registro del teléfono e identidad de una persona en una de las comisarías del Cuerpo de Policía Nacional. El registro del DNIe en el Backend del Cuerpo de Policía Nacional es accesible desde:

- **Registro en la comisaría** ante un funcionario que registre el alta en el servicio.
- **Registro en PAD** de comisaría con el DNIe en vigor.
- **Registro en página web** con **autenticación** con certificado DNIe válido.

2.1.1 Delimitación del TOE

2.1.1.1 Servicios ofrecidos por el entorno de ejecución

El entorno de ejecución está formado por el sistema operativo iOS y por los servicios del Backend del Cuerpo Nacional de Policía.

El enclave seguro del Sistema Operativo (S.O.) iOS donde se ejecuta el TOE ofrece los siguientes servicios:

- Generación de claves EC y Registro de credencial.
- Generación de token de autenticación. Este token de autenticación la solicitará el TOE cada vez que vaya a realizar una operación autenticada con los servicios del Cuerpo Nacional de Policía.
- Generación del objeto attestation a través de la API.

El backend del Cuerpo Nacional de Policía ofrece los siguientes servicios:

- Casos de uso no autenticados:
- Obtención del challenge: para pedir los desafíos a firmar
- Registro de la credencial

Casos de uso autenticados:

- Activación del usuario/DNI.
- Recuperación o cambio de contraseña.
- Visualización de los datos identificativos del usuario activado.
- Generación QR a partir de Sello Digital Visible.
- Baja en el Servicio.
- Servicio de notificaciones.

2.1.1.2 Servicios del TOE

El TOE ofrece los siguientes servicios mediante comunicación y soporte del backend del Cuerpo Nacional de Policía:

2.1.1.2.1 Registro de la instancia de la APP

El TOE, para poder autenticarse frente al servicio de Backend Policial en cada una de las llamadas que así lo requieran, ha de generar un token de integridad que presentará en la cabecera http “authorization”.

La operativa para generar los tokens de integridad es la siguiente:

Tras la instalación del TOE y previo a la activación, del usuario, el TOE pide al servicio de Backend Policial un challenge. Con este challenge, el TOE realizará una solicitud a API Apple Attest para generar claves en el enclave seguro del SO. El API le devolverá un objeto attestation que contiene:

- Un certificado firmado por CA de Apple con la clave pública atestada.
- El challenge firmado con la clave privada atestada que permitirá vincular en servidor el identificador de la APP con su credencial.

El proceso completo junto con los procesos realizados por el entorno operacional se puede encontrar en la *Ilustración 7: Registro de la credencial iOS*.

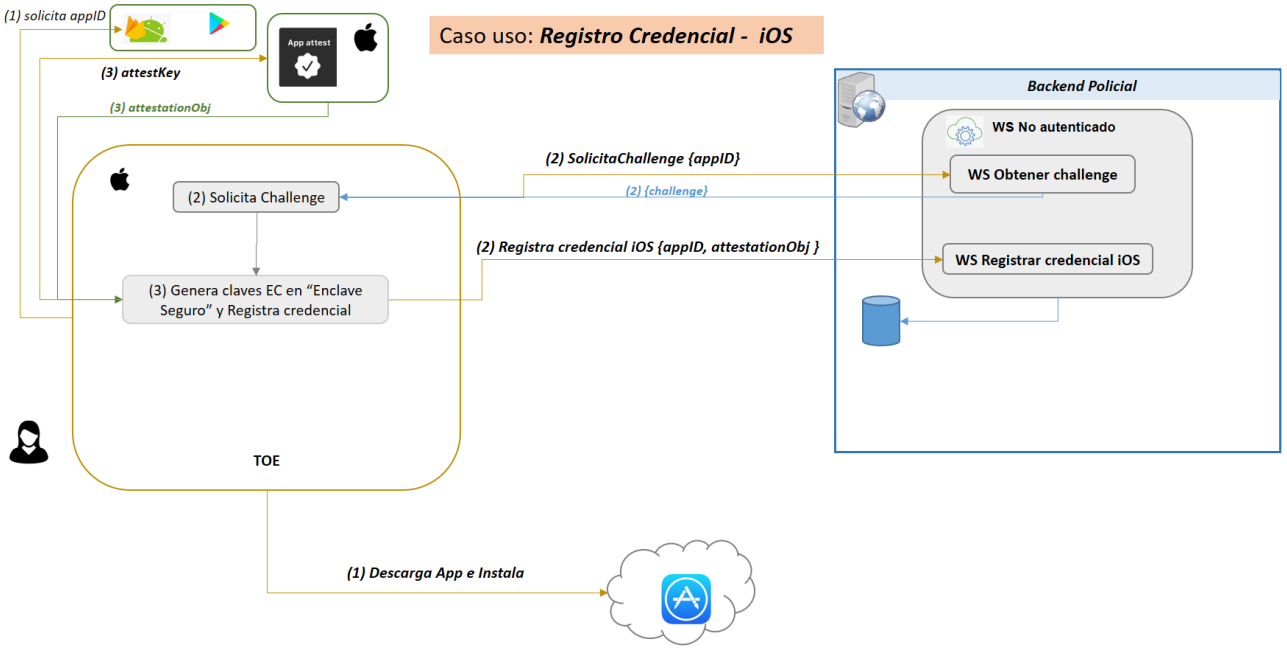

Ilustración 7: Registro de la credencial iOS

2.1.1.2.2 Activación del usuario

El TOE solicitará al backend del Cuerpo Nacional de Policía la vinculación de la app con un usuario/DNI. Se completa en dos pasos y el acceso a los dos servicios de activación requiere la autenticación del TOE (envío de un token de autenticación en cabecera http).

Para ello, el TOE solicitará el token (denominado assertion por Apple) al servicio API Apple Attest, que no es más que la firma de un nonce (que incluye el desafío generado por el servidor) y otros datos que identifican al TOE y que permiten saber si se trata de una APP genuina (pasos (3)(5) de la *Ilustración 8: Proceso de Activación del Usuario en el TOE*).

1. En el primer paso ((4) de la *Ilustración 8: Proceso de Activación del Usuario en el TOE*), se pedirá el número de DNI y un dato del DNI físico (número de soporte), y se enviará petición al servicio "Activacion Paso1" para que compruebe si es un usuario registrado. Si es correcto se enviará un OTP (One Time Password) por SMS al número de móvil indicado en el proceso de registro (sección 2.1.1.2.1Registro de la instancia de la APP).

2. En el segundo paso ((6) de la *Ilustración 8: Proceso de Activación del Usuario en el TOE*), se solicitará al usuario que establezca una contraseña de acceso al TOE y que introduzca el OTP recibido en el primer paso para completar la activación. Tras enviar la petición al servicio "Activación Paso2", si todo es correcto, el usuario quedará como activo en el servicio y su número de teléfono y DNI quedan ya asociados para posteriores pasos con su DNI. Para enviar la contraseña al servidor se le añade un "salt" y se aplica un "hash" SHA256, de forma que la contraseña nunca se transmita en claro y que el servidor no pueda conocer la contraseña de usuario en claro.

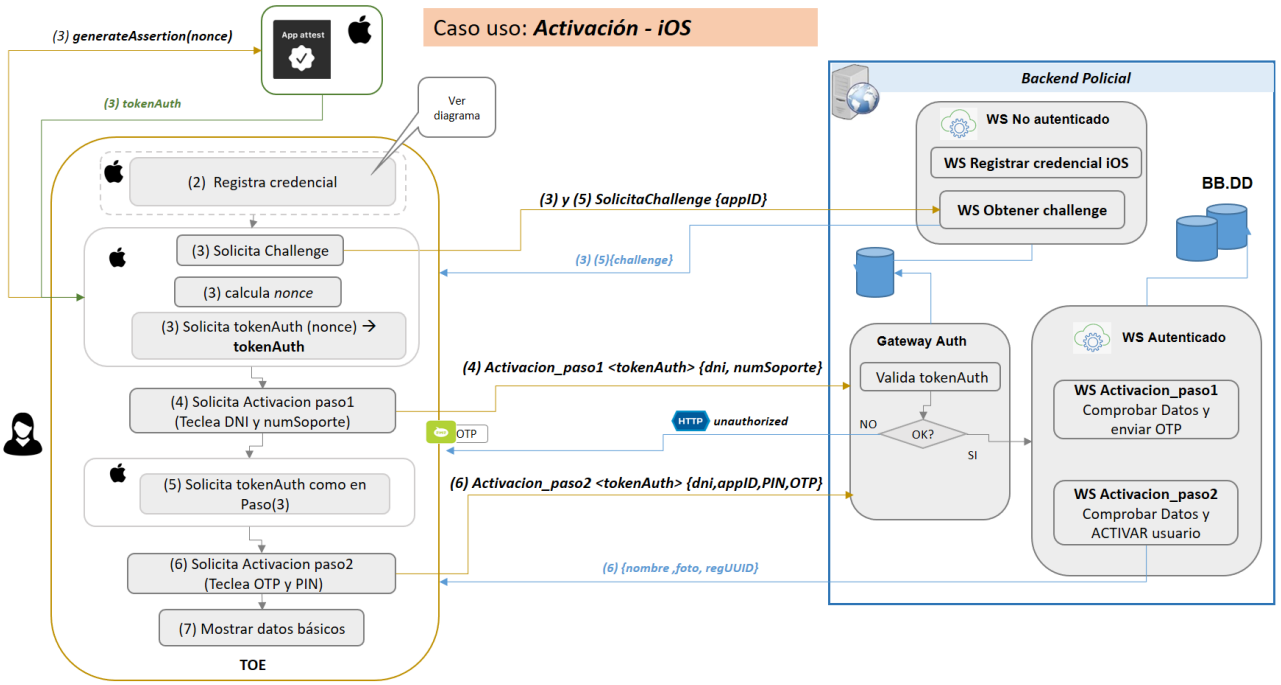

Ilustración 8: Proceso de Activación del Usuario en el TOE

2.1.1.2.3 Autenticación del TOE.

Para cada petición a cualquiera de los servicios autenticados, se solicitará al servidor un challenge que, junto con los datos de la petición se firmará en el enclave seguro del SO con la clave privada previamente atestada, obteniendo el token de autenticación que Apple denomina assertion.

El TOE ofrece el servicio de validar que la contraseña introducido para autenticarse coincide con la contraseña que se establecido en el proceso descrito en la sección *2.1.1.2.2 Activación del usuario*. Antes de realizar los pasos descritos a continuación el TOE tiene que validarse en el Backend, para esto tiene que obtener el token de autenticación que será mandado en las cabeceras HTTP. La obtención de este token esta descrita en la sección *2.1.1.2.2 Activación del usuario*.

El TOE enviará el *appID*, la contraseña (junto con el "*salt*" y aplicando un "*hash*" SHA256) y número de DNI al Backend para autenticarse. La respuesta de esta petición estará firmada, y esta firma tendrá una fecha de caducidad. El TOE no continuará con el proceso en caso de que la firma no sea válida o haya caducado.

El usuario que no haya configurado el acceso al servicio por biometría, tendrá que introducir la contraseña de acceso que estableció en la activación para poder acceder a la funcionalidad protegida del TOE.

El proceso completo junto con los procesos realizados por el entorno operacional se puede encontrar en la *Ilustración 9: Proceso de Autenticación*.

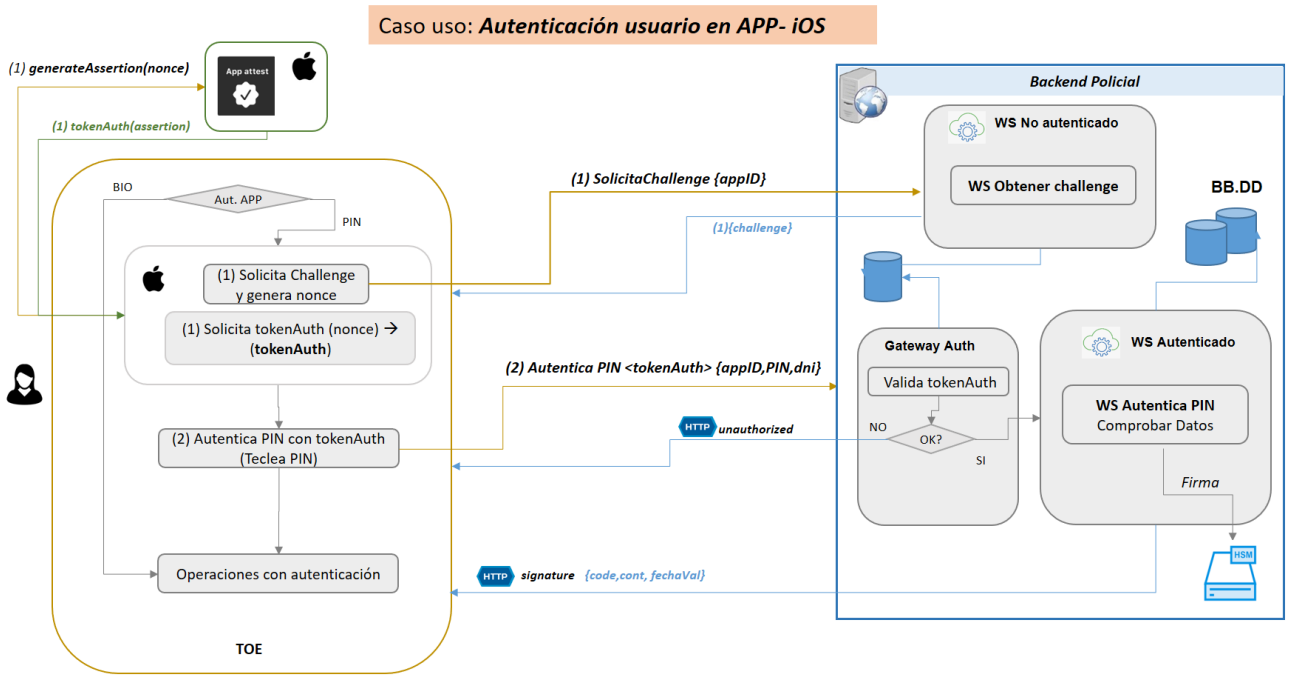

Ilustración 9: Proceso de Autenticación del TOE

En caso de que el usuario olvide o quiera cambiar su contraseña , podrá establecer una nueva contraseña de la misma forma que se establece en la activación (proceso descrito en la sección *2.1.1.2.2 Activación del usuario*), esto es, introduciendo primero el número de DNI y el número de soporte y posteriormente la nueva contraseña y el OTP enviado por SMS tras el primer paso.

El proceso completo para cambiar la contraseña junto con los procesos realizados por el entorno operacional se puede encontrar en la *Ilustración 10: Cambio de Contraseña*.

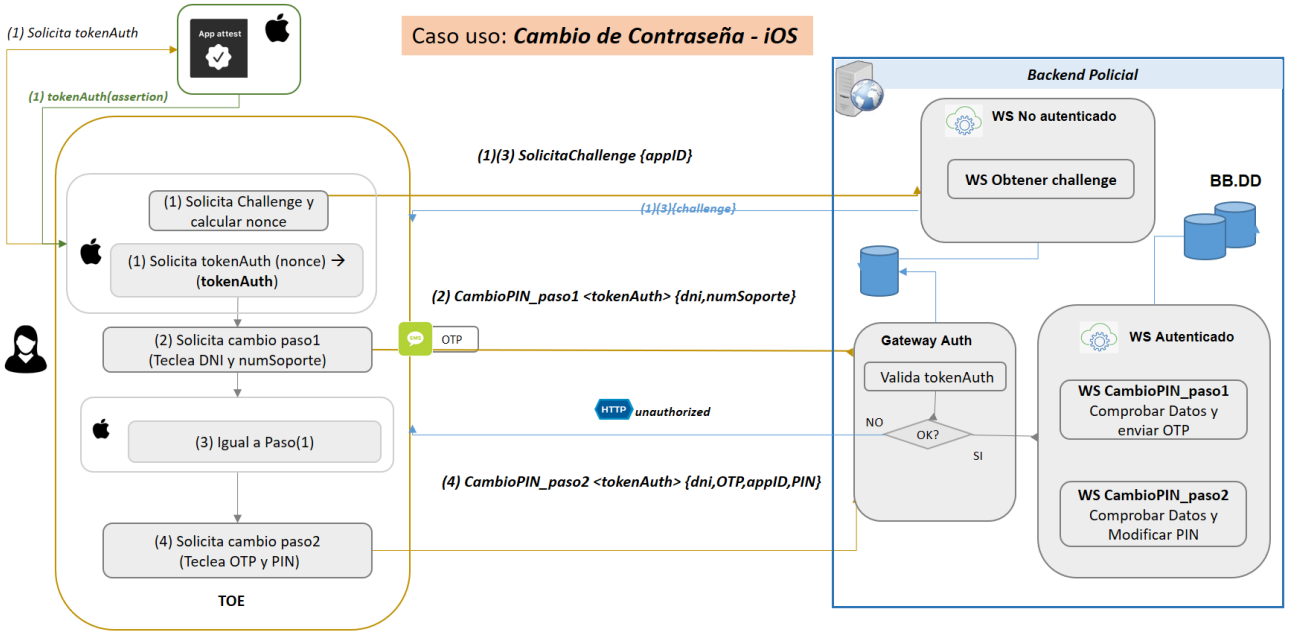

Ilustración 10: Cambio de Contraseña

2.1.1.2.4 Virtualización o descarga de la identidad

El TOE ofrece el servicio de obtención de los datos que aparecen en el DNI físico del ciudadano, datos de caducidad y estado de sus certificados electrónicos, etc. Para el acceso a esta funcionalidad el usuario tiene que autenticarse en el TOE a través del servicio descrito en la sección 2.1.1.2.3 Autenticación del TOE.. Antes de realizar los pasos descritos a continuación el TOE tiene que validarse en el Backend, para esto tiene que obtener el token de autenticación que será mandado en las cabeceras HTTP. La obtención de este token esta descrita en la sección *2.1.1.2.2 Activación del usuario*.

El TOE enviará el *appID* junto con el número de DNI al Backend. El paquete completo de datos devueltos por el Backend irá firmado con una clave privada de componente emitida para tal uso (HSM) y la firma y caducidad se incluirán en la respuesta. El TOE validará la firma y la fecha antes de mostrar los datos, que permanecerán por 1 minuto en la pantalla del dispositivo móvil.

El proceso completo para virtualizar la identidad con los procesos realizados por el entorno operacional se puede encontrar en la *Ilustración 11: Proceso de Visualización del DNIe Virtual*.

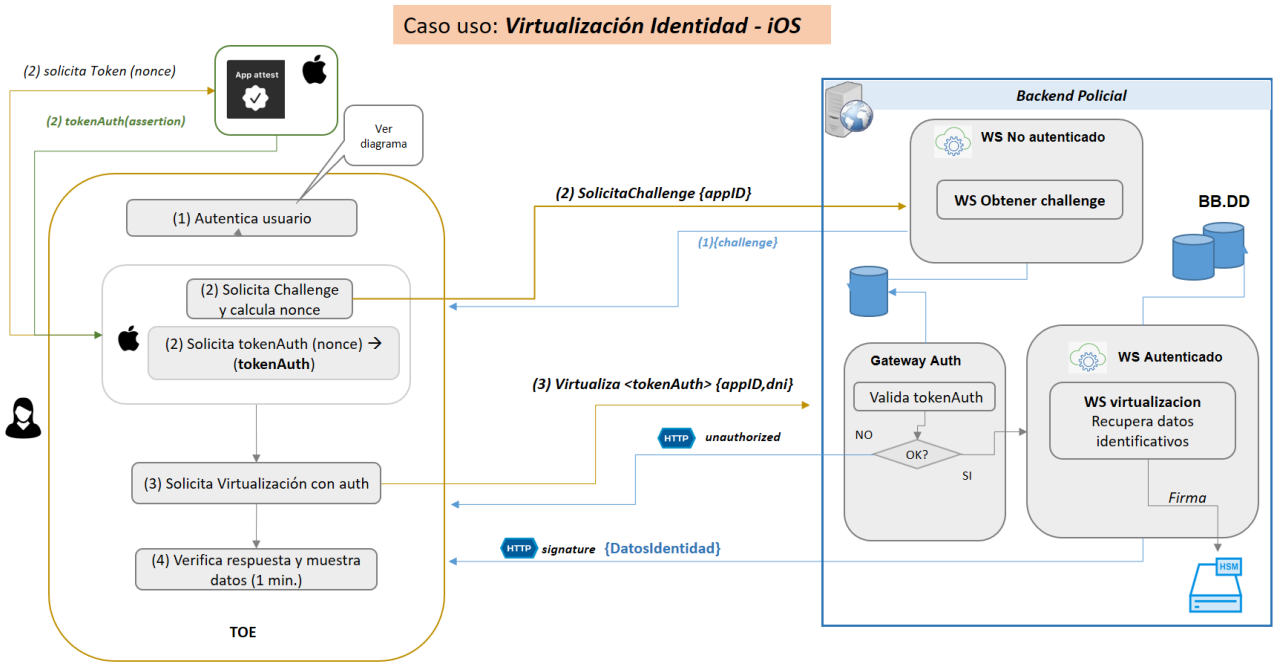

Ilustración 11: Proceso de Visualización del DNIe Virtual

2.1.1.2.5 Descarga datos QR y generación de código QR

El TOE ofrece el servicio de descarga de datos a través de los códigos QR. Este servicio devuelve datos ya conformados y firmados para la creación de los códigos QR. El formato de estos datos es el de Sello Digital

Visible (definido por la OACI (Organización de Aviación Civil Internacional)). Antes de realizar los pasos descritos a continuación el TOE tiene que validarse en el Backend, para esto tiene que obtener el token de autenticación que será mandado en las cabeceras HTTP. La obtención de este token esta descrita en la sección *2.1.1.2.2 Activación del usuario*.

Esta funcionalidad solo puede ser solicitada en el TOE desde la pantalla de visualización de los datos del DNI virtualizado.

Además, para el acceso al servicio de generación de códigos QR el usuario tiene que autenticarse en el TOE a través del servicio descrito en la sección 2.1.1.2.3 Autenticación del TOE. El TOE enviará el *appID*, el número de DNI y el tipo de sello solicitado dependiendo de los datos identificativos solicitados (hay 3 conjuntos de datos que se pueden solicitar: mayoría de edad, simple y completo). El TOE generará el código QR a partir del sello recibido y se mostrará por 1 minuto en la pantalla del dispositivo móvil.

El proceso completo para descargar los datos del DNI (obtener sello) junto con los procesos realizados por el entorno operacional se puede encontrar en la *Ilustración 12: Proceso de Descarga de Datos*.

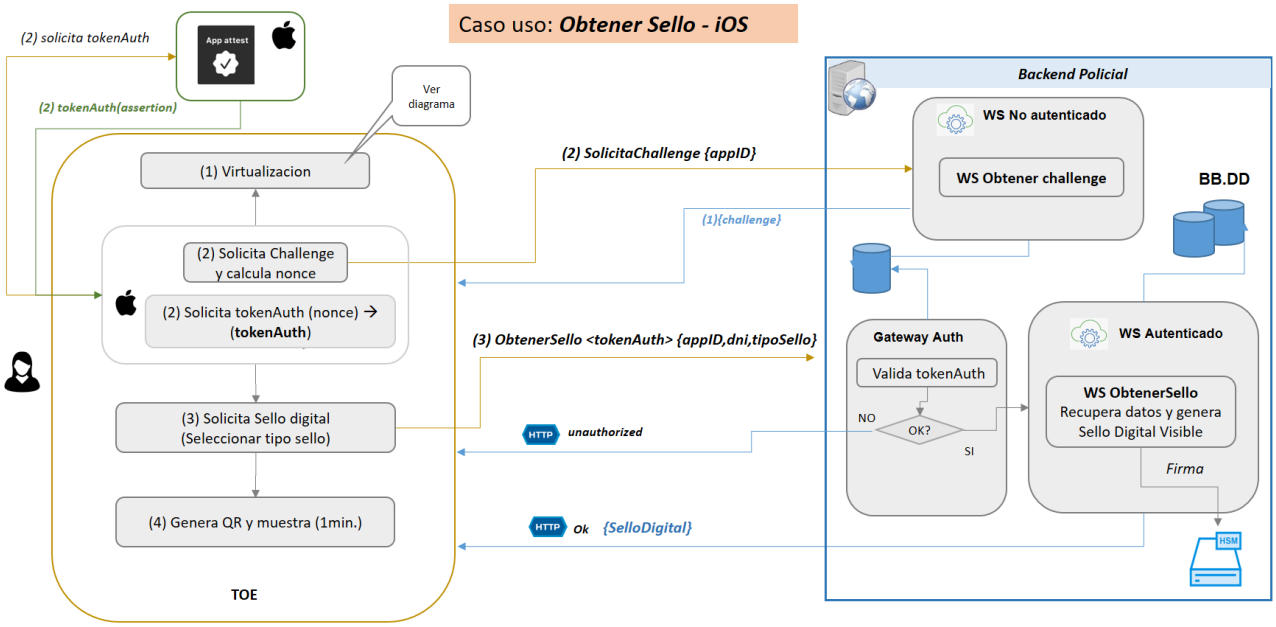

Ilustración 12: Proceso de Descarga de Datos

2.1.1.2.6 Verificación de código QR

El TOE ofrece el servicio de leer los datos de un QR compartido por otra instancia del TOE de otro ciudadano. Para ello la aplicación deberá contar con el certificado público de firma con el que el Cuerpo Nacional de Policía firmará los datos que conforman el QR y verificar dicha firma, así como la validez de tiempo de dicha firma.

Este uso no requiere de servicios web externos, se gestiona en el TOE y, además, no es necesario tener el TOE vinculado a la identidad de un ciudadano.

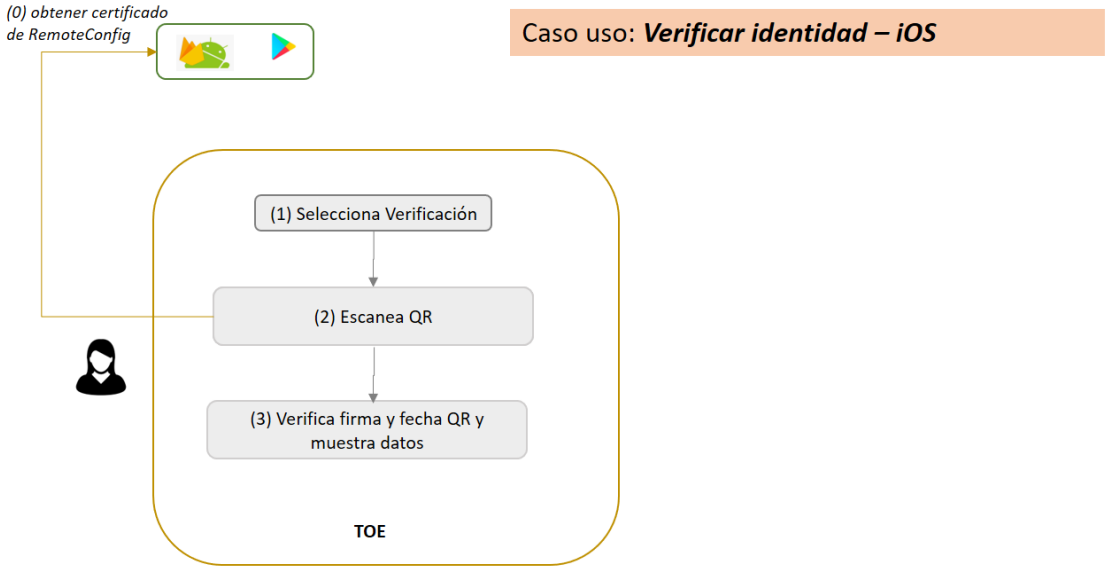

Ilustración 13: Proceso de Verificación de Código QR

2.1.1.2.7 Baja del servicio

El TOE ofrece el servicio de darse de baja del servicio de DNIe en el dispositivo móvil. Para el acceso a esta funcionalidad el usuario tiene que autenticarse en el TOE a través del servicio descrito en la sección 2.1.1.2.3 Autenticación del TOE. Antes de realizar los pasos descritos a continuación el TOE tiene que validarse en el Backend, para esto tiene que obtener el token de autenticación que será mandado en las cabeceras HTTP. La obtención de este token esta descrita en la sección *2.1.1.2.2 Activación del usuario*.

El TOE enviará el *appID* junto con el número del DNI al Backend, y el Backend de la Policía Nacional dará de baja del sistema este DNI.

El proceso completo para dar de baja el servicio junto con los procesos realizados por el entorno operacional se puede encontrar en la *Ilustración 14: Proceso de Baja*.

1.9 Declaración Seguridad de MiDNI iOS

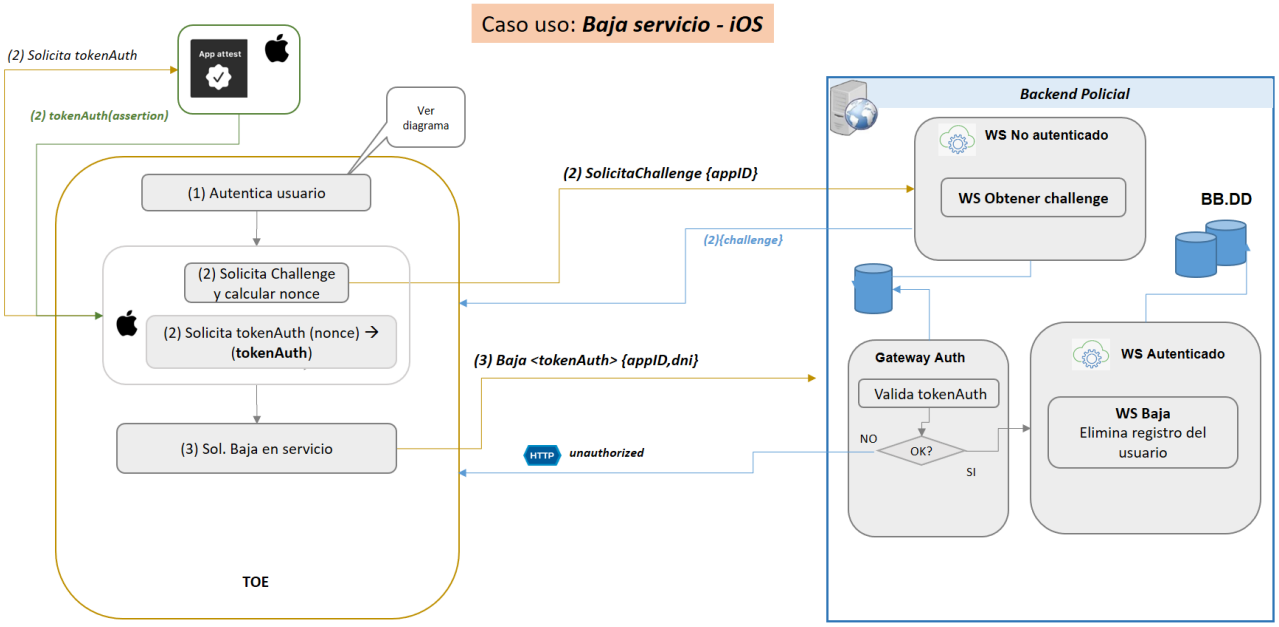

Ilustración 14: Proceso de Baja

2.2 Identificación de las Guías de Uso, Instalación y Configuración Seguras del TOE

La siguiente tabla contiene el alcance físico del TOE compuesto por la aplicación y sus guías correspondientes:

Tabla 3 Información del TOE

Nombre del Documento	Versión	Fecha
MiDNI IOS App	1.0.0 (preproducción)	22/03/2024
Guía de Instalación MiDNI iOS	1.2	08/11/2024
Guía operacional MiDNI iOS	1.2	08/11/2024

2.3 Librerías de terceras partes del TOE

El TOE ha sido desarrollado utilizando la funcionalidad de las siguientes librerías de terceras partes:

Librería	Versión
Abseil	v1.2022062300.0
Firebase	v10.20.0
GoogleDataTransport	v9.3.0
gRPC	v1.49.1
InterOpForGoogle	v100.0.0
Lottie	v4.3.4
Promises	v2.3.1
Appcheck	v10.18.0
GoogleAppMeasurement	v10.17.0
GoogleUtilities	v7.12.1
GTMSessionFetcher	v2.3.0
Leveldb	v1.22.2
Nanopb	v2.30909.0

SwiftProtobuf	v1.21.0

3 ENTORNO DE EJECUCIÓN

Para hacer uso del TOE en su versión certificada, es necesario el entorno que se describe a continuación.

3.1 Descripción del Entorno de Ejecución

El entorno operacional del TOE consiste en la aplicación móvil, el hardware móvil donde se instala ésta y el servidor de la información de los usuarios.Si bien el TOE se considera compatible con iOS 14.0 o superior, la configuración evaluada ha sido la siguiente: MiDNI 1.0.0 (preproducción) corriendo sobre el dispositivo móvil iPhone Xr, con iOS 17.4.1.

Tabla 4 Identificación de los componentes del entorno operacional

Componente entorno operacional	Tipo componente	Versión Componente	Software requerido	Hardware requerido
iOS	Dispositivo móvil	iOS17.4.1	iOS 17.4.1	iPhone Xr
Backend Policía Nacional	Kubernetes	1.28	VMware ESXi 7.0.3	BLADE DELL MX7000 PowerEdge MX740c

3.1.1 Comprobación de la Integridad del Software

El TOE se descarga a través de la aplicación TestFlight, una herramienta nativa de iOS que permite a los desarrolladores invitar a evaluadores a probar sus aplicaciones en fase de prueba. TestFlight facilita la distribución de versiones preliminares de aplicaciones, permitiendo a los usuarios probar funciones en desarrollo y reportar problemas antes de su lanzamiento oficial.

Cada vez que se establece un canal de comunicación entre el TOE y el endpoint del Cuerpo Nacional de Policía, este último realiza una comprobación de integridad de la aplicación. Esta operación verifica que el TOE no ha sido modificado.

4 PROBLEMA DE SEGURIDAD

4.1 Hipótesis sobre el Entorno de Ejecución

Esta sección específica las hipótesis que tienen que ser satisfechas por el entorno del TOE para proporcionar funcionalidad de seguridad. Si el TOE se encuentra en un entorno operacional en el que no se cumplan estas hipótesis, el TOE no será capaz de proporcionar toda su funcionalidad de seguridad.

Tabla 5 Hipótesis

Hipótesis	Descripción
H.PROTECCION_FISICA_SERVIDOR	El servidor de datos del Cuerpo Nacional de Policía desde donde se obtiene la información de los usuarios está protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación, lo que incluye una localización segura y no accesible para usuarios ajenos a la administración del entorno.
H.ENDPOINT_SERVIDOR	El servidor de datos del Cuerpo Nacional de Policía estará actualizado y configurado de forma segura para realizar la operativa solicitada por el TOE. Además, la función de la comprobación de la integridad del TOE se delega en el propio endpoint del CNP.
H.DISPOSITIVO_CONFIABLE	El dispositivo donde se ejecutará el TOE estará actualizado a los últimos parches de seguridad, no estará rooteado y solo contara con la tienda oficial de aplicaciones confiables (App Store). Esta comprobación la realiza el TOE con la comprobación mínima del SO.
H.MARKETPLACE_CONFIABLE	El Marketplace donde el TOE se aloja se considera confiable.

4.2 Activos Sensibles a Proteger

En esta sección se describen los activos a proteger por el TOE. La vulneración de cualquiera de las dimensiones de cualquier activo listado a continuación constituye una vulnerabilidad en el TOE.

Tabla 6 Activos

Activo	Descripción del activo	Dimensiones a proteger
AC.DATOS_DNI	Datos personales de un usuario tales como los datos de su DNI o las notificaciones provenientes del Cuerpo Nacional de Policía.	Integridad Autenticidad
AC.CREDENCIALES_USUARIO	Credenciales y datos de conexión del usuario que puedan ser utilizados para una suplantación de identidad.	Integridad Confidencialidad

4.3 Descripción de las Amenazas

4.3.1 Agentes

Se asume que hay dos tipos diferentes de agentes de las amenazas: autorizados y no autorizados. Los agentes autorizados son usuarios confiables que han recibido formación específica y entrenamiento relacionado con el funcionamiento del TOE en términos de uso, gestión y administración. Se asume que tienen acceso y habilidades requeridas para realizar cambios en la funcionalidad del TOE o en su entorno operacional. Finalmente, tienen acceso físico al dispositivo donde se ejecuta el TOE. Por otro lado, los agentes no autorizados tienen solamente conocimiento público del TOE y sus operaciones. También se asume que no tienen acceso físico al servidor de datos del Cuerpo de Policía Nacional pero sí al dispositivo donde se ejecuta el TOE.

Los agentes de las amenazas se asumen que sean capaces de tener acceso y monitorizar el tráfico cifrado de red entre el TOE y el entorno operacional sin tener la habilidad de descifrar y acceder al tráfico de datos en texto plano.

Tabla 7 Agentes

Agente	Descripción del agente
AG.TOE	Un usuario autorizado con acceso a una instancia legítima del TOE.
AG.EXTERNO_DISPOSITIVO	Cualquier agente no autorizado que tiene acceso al dispositivo donde está instalado una instancia legítima del TOE.
AG.EXTERNO_ENTORNO	Cualquier agente no autorizado que está presente en el entorno físico de una comunicación realizada por un usuario legítimo.

4.3.2 Amenazas

A continuación, se describen las amenazas que tienen que ser contrarrestadas por el TOE y su entorno operacional. Se asume que el nivel de conocimiento técnico del atacante en todas las amenazas identificadas a continuación no es sofisticado.

Las definiciones de las amenazas son:

A.COMUNICACIÓN

Un agente externo con acceso a la red captura el tráfico de la comunicación de un usuario legítimo para recuperar los datos del DNI del usuario o sus datos de conexión con el servidor de datos.

Activos: AC.CREDENCIALES_USUARIO, AC.DATOS_DNI

Agentes de la amenaza: AG.EXTERNO_ENTORNO

A.AUTENTICACIÓN_SECRETA

Un agente externo en el entorno intenta espiar las credenciales de autenticación de un usuario en un dispositivo legítimo durante su introducción.

Activos: AC.CREDENCIALES_USUARIO

Agentes de la amenaza: AG.EXTERNO_ENTORNO

A.ACCESO

Un agente externo con acceso físico a un dispositivo con un TOE legítimo accede a la aplicación para generar un QR del que derivar la información del DNI del usuario o revisar las notificaciones.

Activos: AC.DATOS_DNI

Agentes de la amenaza: AG.EXTERNO_DISPOSITIVO

A.IMPERSONACIÓN

Un usuario legítimo intenta obtener una imagen de la interfaz del TOE donde se presenta el código QR para modificarlo y enseñarlo a un usuario verificador.

Activos: AC.DATOS_DNI

Agentes de la amenaza: AG.TOE

5 FUNCIONES DE SEGURIDAD

Las siguientes secciones describen las funciones de seguridad que implementa el TOE. Cada una de estas funciones de seguridad está a su vez subdividida en requisitos de seguridad

5.1 Característica de seguridad 1: Identificación y Autenticación

Estas funciones mitigan la amenaza **A.ACCESO**.

IAU.1: El usuario debe ser autenticado antes de tener acceso al TOE y a sus funciones excepto para:

- Registrar la instancia del TOE
- Activación del usuario
- Función de verificar un código QR
- Cambiar contraseña
- Desactivar DNI

las cuales no necesita ninguna identificación ni autenticación previa.

IAU.2: El TOE fuerza que la contraseña cumpla la siguiente política:

- La contraseña debe configurarse con una longitud mínima de 8 caracteres y máxima de 16 caracteres.
- La contraseña debe estar compuesta por al menos tres de estos cuatro grupos: letras minúsculas, letras mayúsculas, números y caracteres especiales del tipo [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “].

Nota: El TOE soporta algoritmos criptográficos para el cálculo del hash y salt de la contraseña **del usuario: SHA256**(CONTRASEÑA + SALT)

IAU.3: El TOE debe permitir autenticación mediante usuario y contraseña o delegarlo a la autenticación biométrica del dispositivo.

IAU.4: El TOE implementa mecanismos que impiden ataques de autenticación por fuerza bruta. El TOE detecta 5 intentos fallidos de autenticación por parte del usuario bloqueando su acceso. Para poder realizar un nuevo proceso de autenticación en el TOE, el usuario debe realizar de nuevo el proceso de activación para obtener una nueva contraseña.

IAU.5: El TOE asegura el proceso de desautenticación de un usuario transcurridos 1 minuto desde la visualización de información confidencial.

IAU.6: El TOE forzará el asignar unas credenciales al usuario durante el proceso de activación del usuario.

IUA.7: El TOE solo permite identificar y autenticar a un solo usuario en una única instancia del TOE.

IUA.8: El TOE permite el cambio o restablecimiento de la contraseña del usuario.

5.2 Característica de seguridad 2: Usuario Único

Estas funciones mitigan la amenaza **A.IMPERSONACIÓN**

ACT.1: El TOE verifica la integridad y autenticidad en los siguientes casos:

- Cuando solicita los datos del DNI (virtualización y descarga de identidad) al endpoint del Cuerpo Nacional de Policía, verifica la firma de los datos recibidos.
- Cuando solicita el código QR, verifica el sello recibido por parte del endpoint del Cuerpo Nacional de Policía.
- Cuando solicita una autenticación de contraseña para comprobar si es válida, verifica la validez de la firma de la respuesta del endpoint del Cuerpo Nacional de Policía. El TOE se encargará de no continuar con el proceso en caso de que la firma no sea válida o haya caducado.
- Cuando actúa como verificador, una instancia del TOE verifica la integridad del código QR de otra instancia del TOE.

El código QR generado por los datos del sello recibido del endpoint del Cuerpo Nacional de Policía, se firma con el algoritmo ECDSA con SHA256. En caso que la verificación de la firma falle, el TOE mostrará un mensaje de error informando de ello.

ACT.2: El TOE verifica la marca de tiempo del código QR enviado por el endpoint por el Cuerpo Nacional de Policía. Esta marca de tiempo sólo es utilizada por el TOE para verificar que los datos enviados por el endpoint han sido emitidos dentro del periodo válido de tiempo.

NOTA: Los datos del DNI del usuario contenidos en el QR no están cifrados, por tanto, podrán ser leídos por cualquier lector de QR genérico.

5.3 Característica de seguridad 3: Canales Seguros

Estas funciones mitigan la amenaza **A.COMUNICACION**

COM.1: El TOE establece canales seguros siempre que intercambia información sensible con el Servidor de datos del Cuerpo Nacional de Policía. La comunicación se establece mediante TLS versión 1.3. Ciphersuites:

- TLS_AES_128_GCM_SHA256.
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

COM.2: El TOE solo permite que los canales de comunicación definidos en COM.1 sean iniciados por él.

COM.3: El TOE hace uso de certificados digitales para la autenticación cuando utilice cualquiera del protocolo TLS definido en COM.1.

5.4 Característica de seguridad 4: Borrado de datos

Estas funciones mitigan la amenaza **A.ACCESO**

BOR.1: El TOE no almacena credenciales ni claves privadas de los usuarios en ningún caso.

BOR.2: El TOE borra los datos del usuario (fotografía y el nombre del usuario) almacenados en el dispositivo subyacente, haciendo imposible la recuperación de datos tras el borrado, cuando se seleccione la funcionalidad "*Desactivar mi DNI*" y/o "*Darme de baja en el sistema*".

Nota: Después de dar de baja del sistema, el usuario tiene que volver a realizar el registro previo en comisaría para activar el DNI en una instancia del TOE.

5.5 Característica de seguridad 5: Protección de Datos Confidenciales

Estas funciones mitigan la amenaza **A.AUTENTICACION_SECRETA**

PDC.1: El TOE oscurece mediante puntos la contraseña del usuario en el proceso de autenticación.

PDC.2: El TOE utiliza Apple Attest para generar un objeto attestation que contien:

- Un certificado firmado por CA de Apple con la clave pública atestada.
- El challenge firmado con la clave privada atestada que permitirá vincular en servidor el identificador de la APP con su credencial.

PDC.3: El TOE proporciona mecanismos para proteger la confidencialidad de las contraseñas. Para ello, el TOE añade un "*salt*" a la contraseña y le aplica un "*hash*" SHA256.

PDC.4: El QR recibido en el TOE y enviado desde el endpoint del servicio del Cuerpo Nacional de Policía tiene un tiempo máximo de visualización de 1 minuto. Pasado ese tiempo, la pantalla se cierra automáticamente y los datos son borrados de la memoria del teléfono.

5.6 Característica de seguridad 6: Criptografía

Estas funciones mitigan la amenaza **A.COMUNICACION, A. AUTENTICACIÓN SECRETA, A.IMPERSONACIÓN**

CIF.1: El TOE únicamente permite mecanismos criptográficos autorizados de acuerdo a lo establecido en la guía CCN-STIC-807. La fortaleza de clave empleada será la indicada en esa guía para Categoría ALTA de ENS, y de acuerdo con el nivel de amenaza establecido.

6 REFERENCIAS

Tabla 8 Referencias

[CCN-LINCE-2001]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 2.0
[CCN-LINCE-2002]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), Versión 2.0
[CCN-LINCE-2003]	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 2.0
[CCN-LINCE-2004]	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), Versión 2.0
[CCN-STIC-807]	Criptología de empleo en el Esquema Nacional de Seguridad. Mayo 2022
[CCN-STIC-140]	Taxonomía de referencia para productos de Seguridad TIC
[CCN-STIC-141]	Taxonomía de referencia para productos de Seguridad TIC para ENS Medio y Bajo

7 ACRÓNIMOS

Tabla 9 Acrónimos

API	Application Programming Interface
BBDD	Base de Datos
CCN	Centro Criptológico Nacional
DNI	Documento Nacional Identidad
DNIe	Documento Nacional Identidad Electronico
ECC	Eliptic Curve Cryptography
ENS	Esquema Nacional de Seguridad
FNMT	Fábrica Nacional de Moneda y Timbre
HTTP	Hyper-Text Transfer Protocol
ICV	Integrity Check Value
LINCE	Certificación Nacional Esencial de Seguridad
MCF	Módulo Revisión de Código Fuente
MEB	Módulo de Evaluación Biométrica
MEC	Módulo de Evaluación Criptográfica
NIST	National Institute of Standards and Technology
QR	Quick Response Code
ST	Security Target - Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TIC	Tecnologías de la Información y Comunicación
TLS	Transport Layer Security
TOE	Target Of Evaluation – Objeto a evaluar