Aplicación Cl@ve de la AEAT para Android

Declaración de Seguridad

Versión 6 – (08/01/2025)

Creado para

Agencia Tributaria

Creado por:

CLOVER TECHNOLOGIES

Contenido

1 Introducción 3
1.1 Información del patrocinador, TOE y evaluación 3
1.2 Metodología y criterios de evaluación 3
2 Descripción del TOE 4
2.1 Descripción funcional del TOE 4
2.1.1 Arquitectura 5
2.1.2 Descripción detallada de las funcionalidades 6
2.2 Identificación de las guías de uso, instalación y configuración seguras del TOE8
3 Entorno de ejecución 9
3.1 Descripción del entorno de ejecución 9
4 Problema de seguridad 10
4.1 Hipótesis sobre el entorno de ejecución 10
4.2 Activos sensibles a proteger 10
4.3 Descripción de las amenazas 11
5 Funciones de seguridad 13
5.1 Especificación de las funciones de seguridad del producto 13
5.1.1 Comunicaciones Seguras 13
5.1.2 Criptografía 13
5.1.3 Identificación y Autenticación 14
5.1.4 Protección De Credenciales Y Datos Sensibles 14
5.1.5 Instalación y actualización 15
5.1.6 Configuración por defecto segura 16
5.1.7 Gestión de la autenticación 16
5.1.8 Protección del ejecutable 17
5.1.9 Autenticación frente a la AEAT 17
5.2 Correspondencia de las funciones de seguridad con las amenazas identificadas. 19
6 Anexo I: Librerías de terceros utilizadas 20
7 Referencias 21
8 Acrónimos 22
9 Índice de tablas 23
10 Índice de figuras 24

1 Introducción

1.1 Información del patrocinador, TOE y evaluación

Datos del Solicitante (Nombre y Dirección)	Agencia Estatal de Administración Tributaria C. de Uruguay, 16, 28016, Madrid
Datos del Desarrollador (Nombre y Dirección)	Agencia Estatal de Administración Tributaria C. de Uruguay, 16, 28016, Madrid
Nombre del TOE	Cl@ve
Versión del TOE	5.8.3
Taxonomía del producto según CCN-STIC-140 y su versión	Otras herramientas
Tipo de evaluación	LINCE
Manuales de uso del producto y su versión	Guías de uso APP Cl@ve. Versión 1.4

Tabla 1 Información del patrocinador, TOE y evaluación

1.2 Metodología y criterios de evaluación

CCN-STIC-2001	CCN-STIC-2001 - Definición de la Certificación Nacional Esencial de Seguridad, versión 2.0. Marzo 2022.
CCN-STIC-2002	CCN-STIC-2002 - Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad, versión 2.0. Marzo 2022.

Tabla 2 Metodología y criterios de evaluación

2 Descripción del TOE

2.1 Descripción funcional del TOE

El producto a evaluar se trata de la aplicación **Cl@ve** para dispositivos móviles con sistema operativo Android, actualización de la aplicación actual **Cl@ve PIN.** El objetivo de este producto es ofrecer a los ciudadanos los servicios relacionados con la identificación y autenticación.

Este producto cuenta con el Proveedor de Identidad de AEAT.

Actualmente, en función de la forma y el nivel de garantía del registro, diferenciamos dos niveles:

- **Nivel Básico**: El usuario facilita los datos de forma telemática sin necesidad de una autenticación previa mediante el uso de un certificado electrónico cualificado. De esta forma, la identificación se lleva a cabo mediante el uso de datos conocidos por el usuario y la Administración.
- **Nivel avanzado**: Los datos se comunican de dos formas:
    - En una oficina, de forma presencial y ante un empleado de la Administración Pública habilitado para esta tarea.
    - De forma telemática, autenticado previamente con un certificado electrónico cualificado.

Se mantienen las gestiones ofrecidas anteriormente por la aplicación “Cl@ve PIN”, por ejemplo, la opción de **visualizar el PIN** que se ha obtenido mediante una gestión a través de un navegador web, aplicación móvil con “Cl@ve PIN” o aplicaciones de terceros. También se añaden funcionalidades relacionadas a la gestión de contraseña de “Cl@ve Permanente”, por ejemplo, recuperación de código de activación, activación de contraseña, etc.

2.1.1 Arquitectura

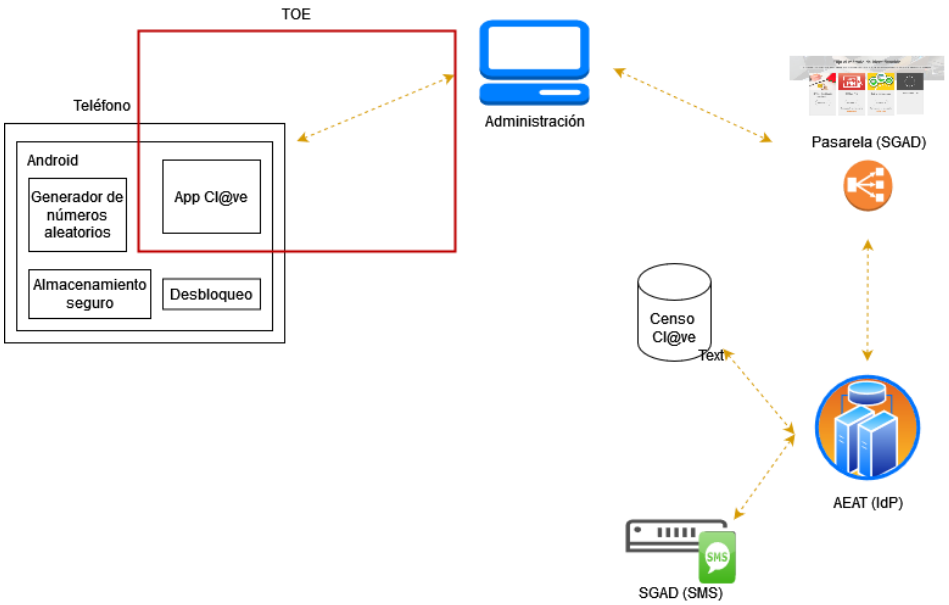

Figura 1: Arquitectura

Se compone de cuatro componentes principales:

- **Proveedor de Identidad** (IdP): Almacena las identidades obtenidas en el proceso de registro y previamente contrastadas con la Dirección General de la Policía. Este componente, autentica e identifica a los usuarios mediante las peticiones generadas por los Proveedores de Servicio (SP) y pueden pasar por la Pasalera Cl@ve. El IdP actual es: AEAT (Agencia Estatal de Administración Tributaria).
- **Proveedor de Servicios** (SP): Aplicación, API o conjunto de aplicaciones que aportan funcionalidad al usuario, exceptuando el proceso de autenticación. Dentro de nuestro contexto, se refiere a la aplicación de una identidad que ofrece servicios de cara al ciudadano.
- **Pasarela Cl@ve**: Intermediario entre SP y los IdPs. Responsabilidad de SGAD.
- **Autoridad de certificación**: Emisora de los certificados centralizados del DNI para permitir a los ciudadanos autenticarse durante el alta de la aplicación en el dispositivo. Responsabilidad de la DGP.

2.1.2 Descripción detallada de las funcionalidades

2.1.2.1 Dispositivo activo con “Cl@ve”

El ciudadano podrá tener únicamente un dispositivo activo asociado a su DNI. Si se activa en otro dispositivo, quedará automáticamente desactivado del primero.

2.1.2.2 Activación de “Cl@ve”

En referencia a la activación de la aplicación, podemos distinguir tres escenarios diferentes:

1. Ciudadano (registrado en “Cl@ve”) que ya está activado en “Cl@ve PIN” y se actualiza a “Cl@ve”: en el primer acceso tras la actualización desde “Cl@ve PIN”, se le solicita el factor de autenticación configurado en el móvil para que se active “Cl@ve”.

2. Ciudadano (registrado en “Cl@ve”) que se instala “Cl@ve” o actualiza “Cl@ve PIN” y no está activado en ese dispositivo: El primer paso será la activación con la AEAT introduciendo el DNI, un dato de contraste y un código de activación que se recibirá en el móvil registrado en “Cl@ve”.

3. Ciudadano (no registrado en Cl@ve) que se instala la app Cl@ve o actualiza la app Cl@ve PIN y no está activado en ese dispositivo: El ciudadano al intentar pasar el proceso de activación en la app Cl@ve con la AEAT, tras introducir su DNI y el dato de contraste, le indicará que no está registrado en Cl@ve con las siguientes opciones disponibles para su registro:

    a. Mediante videollamada.

    b. A través del envío de una carta a su domicilio fiscal.

    c. Mediante certificado o DNI electrónico.

2.1.2.3 Autenticación con “Cl@ve Móvil”

Para el uso de autenticación con el sistema “Cl@ve Móvil” es necesario que el usuario haya activado previamente “Cl@ve”.

2.1.2.3.1 Interacción con los IdP

La autenticación del IdP de AEAT se basa en una clave aportada por el usuario más un código recibido en el dispositivo móvil con una validez limitada en el tiempo. "Cl@ve" tiene la capacidad de capturar y enviar el código de manera automática al IdP de AEAT.

2.1.2.3.2 Operativa al acceder a un SP

Tras solicitar el acceso al SP, se redirige al usuario a la pasarela de "Cl@ve" para autenticarse, ofreciéndose la opción de realizarlo utilizando "Cl@ve Móvil". Esta autenticación se realiza contra el IdP basándose en algo que el usuario sabe (DNI) y un dato de contraste (fecha de caducidad del DNI). El IdP verifica que el usuario está registrado en "Cl@ve", instándole a realizarlo en caso contrario, y si tiene un dispositivo activo, instándole a instalar (si no lo estuviese) y activar la aplicación "Cl@ve" en un dispositivo, facilitándole el acceso a la misma a través de un código QR.

Si el usuario tiene un dispositivo activo, le enviará una notificación push (si tiene el token "Firebase") o le indicará que acceda a su aplicación "Cl@ve", mostrándole un código de petición que el ciudadano acepte esa y sólo esa petición. Por su parte, la aplicación "Cl@ve" al iniciarse valida que está activa en ese dispositivo y si el ciudadano tiene peticiones de firma o autenticación pendientes, mostrando la última si hubiese varias. En este caso, como estamos tratando con peticiones de autenticación de Cl@ve Móvil, se le muestra al usuario la información de la petición para que la confirme o rechace, solicitándole que confirme la operación introduciendo el factor de autenticación configurado en el dispositivo. Si todo se completa con éxito la aplicación "Cl@ve" le indica al usuario que puede volver al trámite que estaba realizando.

Por último, el IdP se encarga de redirigir la pasarela "Cl@ve" con los datos de identidad para que el usuario acceda de forma autenticada al SP al que había solicitado el acceso.

2.1.2.4 Recursos del sistema operativo

La aplicación utiliza los siguientes recursos del sistema operativo Android:

- Generador de números aleatorios. Para la creación de la contraseña con la que se activa el dispositivo en el sistema Cl@ve.

- Almacenamiento seguro. Para el almacenamiento de las credenciales asociadas al dispositivo.
- Desbloqueo. Para la autenticación y autorización del usuario para acceder a las funcionalidades protegidas de la aplicación.

2.2 Identificación de las guías de uso, instalación y configuración seguras del TOE

Nombre	Guías de uso APP Cl@ve
Versión	Versión 1.4
Fecha de emisión	23/10/2024

Tabla 3 Identificación de guías de uso y configuración seguras del TOE

3 Entorno de ejecución

3.1 Descripción del entorno de ejecución

Esta aplicación está desarrollada para ejecutarse en un dispositivo móvil con sistema operativo Android (versión 8 en adelante).

4 Problema de seguridad

4.1 Hipótesis sobre el entorno de ejecución

H.PLATAFORMA[1] El TOE se ejecuta en un dispositivo confiable con un reloj en hora. Esto incluye tanto la plataforma como el entorno de ejecución que el dispositivo proporciona.

H.USUARIO_REGISTRADO El usuario ya está registrado y dado de alta en el servicio "Cl@ve".

H.SERVIDOR_CONFIABLE El servidor con el que se comunica el TOE y que es controlado por el fabricante (*.agenciatributaria.gob.es y *.agenciatributaria.es) se trata de un servidor confiable.

4.2 Activos sensibles a proteger

S.NIF_USUARIO Documento de identidad del usuario.

S.OTP Código enviado al dispositivo para realizar la autenticación fuerte.

S.DEVICE_ID Identificador del dispositivo asociado al DNI del usuario.

S.USER_PASSWORD Credencial almacenada en el dispositivo usada para la autenticación.

S.CERTIFICADO_ELECTRONICO Certificado electrónico importado a la APP que se guarda en almacén de certificado propio.

S.ALMACEN_CERTIFICADOS Almacén de certificados propio donde se almacenan los certificados importados.

S.CLAVE_PRIVADA Clave privada con la que se cifra el almacén de certificados propio.

La siguiente tabla, muestra las propiedades de seguridad de los activos descritos anteriormente:

Activo	*Propiedades de seguridad*
S.NIF_USUARIO	Confidencialidad, integridad
S.OTP	Confidencialidad

[1] [PP-APP]: 4.2 Security Objectives for the Operational Environment. OE.PLATFORM

Activo	*Propiedades de seguridad*
S.USER_PASSWORD	Confidencialidad, disponibilidad
S.CERTIFICADO_ELECTRONICO	Integridad, autenticidad
S.ALMACEN_CERTIFICADOS	Confidencialidad, integridad
S.DEVICE_ID	Confidencialidad, integridad
S.CLAVE_PRIVADA	Confidencialidad, integridad

Tabla 3: Propiedades de seguridad activos sensibles.

4.3 Descripción de las amenazas

A.ATAQUE_RED[2] Un atacante se posiciona en un canal de comunicación o en otro lugar de la infraestructura de red. Los atacantes podrían realizar comunicaciones con la aplicación o alterar las comunicaciones entre la aplicación y otros dispositivos para comprometerla. Este tipo de ataque amenaza a los siguientes activos sensibles: S.OTP.

A.INTERVENCION_RED[3] Un atacante se posiciona en un canal de comunicación o en otro lugar de la infraestructura de red. Los atacantes podrían monitorizar y acceder a la información intercambiada entre la aplicación y otros dispositivos. Este tipo de ataque amenaza a los siguientes activos sensibles: S.OTP.

A.ATAQUE_LOCAL[4] Un atacante puede utilizar software sin privilegios especiales en el mismo dispositivo en el que se ejecuta la aplicación. Los atacantes podrían introducir datos con un formato malicioso en la aplicación a través de ficheros u otras comunicaciones locales. Este tipo de ataque amenaza a los siguientes activos sensibles: S.NIF_USUARIO, S.USER_PASSWORD, S.CERTIFICADO_ELECTRONICO,

S.ALMACEN_CERTIFICADOS, S.DEVICE_ID, S.CLAVE_PRIVADA.

A.ACCESO_FISICO[5] Un atacante podría tener acceso físico al dispositivo. Este tipo de ataque amenaza a los siguientes activos sensibles: S.OTP.

[2] [PP-APP]: 3.1 Threats. T.NETWORK_ATTACK

[3] [PP-APP]: 3.1 Threats. T.NETWORK_EAVESDROP

[4] [PP-APP]: 3.1 Threats. T.LOCAL_ATTACK

[5] [PP-APP]: 3.1 Threats. T.PHYSICAL_ACCESS

A.ATAQUE_AUTENTICACION Un atacante podría intentar tener acceso a todas las peticiones de autenticación de otro usuario. Este tipo de ataque amenaza a los siguientes activos sensibles: S.OTP.

5 Funciones de seguridad

5.1 Especificación de las funciones de seguridad del producto

5.1.1 Comunicaciones Seguras

COM.1 La aplicación deberá establecer canales seguros cuando intercambie información sensible [con el servidor de la AEAT] empleando funciones, algoritmos y protocolos que estén de acuerdo con lo establecido en la guía CCN-STIC-807.

En este caso, haciendo uso del framework "Retrofit", la comunicación se cifra usando TLSv1.3 con posibilidad de renegociar a TLSv1.2. El servidor utiliza las *suites* de cifrado que se recogen en CIF.1. La aplicación se comunica con el servidor web de la AEAT mediante TLS para llevar a cabo la gestión de la autenticación del ciudadano.

COM.2 El TOE debe permitir que los canales de comunicación definidos en COM.1 sean iniciados por él mismo o por las entidades autorizadas.

En concreto, se considera el canal que se abre entre el TOE y el servidor web de la AEAT para Cl@ve. También existe un canal con el servidor de notificaciones de Google Firebase, pero se haya fuera del alcance del TOE.

COM.3 El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en COM.1.

Dichos certificados utilizan PKCS #1 SHA-256 con RSA de 3072 bits para firma digital y autenticación.

5.1.2 Criptografía

CIF.1 La aplicación permitirá exclusivamente el empleo de funciones, algoritmos y protocolos que utilicen suites de cifrado que estén incluidas entre las autorizadas para Categoría MEDIA del ENS, de acuerdo con lo establecido en la guía CCN-STIC-807.

Concretamente se utilizan los siguientes parámetros de seguridad:

Uso	*Parámetros de securidad*	
Protección de las Comunicaciones	Ciphersuites versión 1.2	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384

Uso	*Parámetros de securidad*	
mediante TLS	Ciphersuites versión 1.3	TLS13-AES128-GCM-SHA256 TLS13-AES256-GCM-SHA384 TLS13-CHACHA20-POLY1305-SHA256
Firma digital y autenticación	Utilizan PKCS #1 SHA-256 con RSA de 3072	
Funciones resumen	SHA-512	

Tabla 4: Parámetros de seguridad

CIF.2 Generador de bits aleatorios. El TOE debe utilizar la clase Java.Security.SecureRandom de Android para la generación de números aleatorios. Dicha clase cumple el estándar FIPS 140-2.

CIF.6 Funciones Resumen. El TOE debe implementar funciones resumen que cumplan lo indicado en CIF.1.

5.1.3 Identificación y Autenticación

IAU.4. La aplicación deberá bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

La aplicación, tras 5 minutos de inactividad, ofusca parcialmente el DNI/NIE y elimina de la sesión las cookies y/o certificado de la sesión.

IAU.6E La aplicación deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.

Las credenciales se almacenan en el almacén *EncryptedSharedPreferences* del sistema operativo, que se encuentra cifrado por una clave criptográfica que se encuentra en el almacén de *AndroidKeyStore,* que a su vez implementa control de acceso para asegurar que solo la aplicación puede acceder a dicha clave.

5.1.4 Protección De Credenciales Y Datos Sensibles

PSC.1 En el caso en que el TOE almacene contraseñas, estas no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con CIF.1.

El TOE almacena las contraseñas en el almacén de clave-valor *EncryptedSharedPreferences*. Este almacén cifra sus datos internos con AES_GCM_256, cuya clave se encuentra protegida (*key wrapping*) mediante AES_SIV_CMAC_256.

PSC.2 Destrucción de PSC. El TOE deberá borrar todos los PSC que utilice una vez finalice su uso. Al desinstalar la aplicación, los almacenes *SharedPreferences* y *EncryptedSharedPreferences* son eliminados, y con ellos, los datos sensibles.

Los ficheros correspondientes a dichos almacenes son borrados utilizando los mecanismos del sistema operativo, y se solicita al sistema operativo que invalide las claves criptográficas que almacena en *AndroidKeyStore* para la aplicación.

PSC.3E Las credenciales secretas solo deberán accederse cuando el usuario introduzca un desbloqueo seguro.

La aplicación obliga al usuario a introducir dicho desbloqueo antes de acceder al *user_password*, el cual se encuentra almacenado y protegido en el almacén *EncryptedSharedPreferences.*

Por otro lado, el DNI se encuentra ofuscado en la aplicación. Tras introducir el código seguro, este DNI se mostrará en claro, y se mantendrá así hasta la que sesión de la aplicación sea cerrada, ya sea por acción del usuario o por inactividad.

PSC.4E Las credenciales secretas deberán quedar inaccesibles si se elimina el desbloqueo seguro, no permitiendo identificar al usuario.

Las funcionalidades de la aplicación para la confirmación de una petición de Cl@ve Móvil o la visualización de un código de Cl@ve PIN, quedará inaccesible si se desactiva el desbloqueo seguro del dispositivo. Si se vuelva a activar dicho desbloqueo seguro, las funcionalidades descritas vuelven a ser accesibles.

5.1.5 Instalación y actualización

ACT.1 La aplicación delegará la gestión de actualizaciones en la plataforma y permitirá consultar la versión actual de la misma.

La aplicación delega la gestión de actualizaciones en el *Google Play Store*. Por otro lado, la aplicación permite consultar en la opción “Acerca de la APP Cl@ve” la versión actual.

ACT.4[6] La aplicación deberá estar en formato *Android application package (APK)* y no deberá dejar rastro tras su eliminación, con la excepción de archivos de salida.

La instalación de la aplicación a través del *Google Play Store* se realiza en formato APK. Además, la eliminación de dicha aplicación implica el borrado de todos los datos de la misma, con la única excepción de posibles archivos de salida.

ACT.5[7] La aplicación no deberá descargar, modificar, reemplazar o actualizar su propio código binario.

La actualización es la única operación que se realiza sobre el código binario de la aplicación, y es llevada a cabo por *Google Play Store*, sin permitir otros métodos de actualización dentro de la misma.

5.1.6 Configuración por defecto segura

CDS.1[8] La aplicación únicamente deberá proveer funcionalidades para definir nuevas credenciales durante el proceso de activación del dispositivo.

Cuando se abre la aplicación por primera vez, la única funcionalidad accesible por el usuario es la definición de nuevas credenciales para activar el dispositivo.

5.1.7 Gestión de la autenticación

AUM.1 La aplicación deberá transmitir los datos de identidades y credenciales a otras entidades autorizadas del entorno operacional que lo requieran. La transmisión de estos datos deberá efectuarse a través de un canal seguro tal y como establece COM.1, y con autenticación mutua.

El dispositivo del TOE se identifica en las llamadas a los servicios que dan soporte funcional en los servidores de la AEAT mediante el uso del DNI/NIE y el *device_id*, a través del canal de comunicación definido en COM.1.

[6] [PP-APP]: FPT_TUD_EXT.2.1

[7] [PP-APP] : FPT_TUD_EXT.1.3

[8] [PP_APP]: FMT_CFG_EXT.1.1

Además, en peticiones que requieran la autenticación del usuario, como es el caso de la confirmación de una petición de autenticación de Cl@ve Móvil o visualizar el PIN de una petición de Cl@ve PIN, dichas llamadas contendrán el *user_password*.

5.1.8 Protección del ejecutable

EXP.1 Cuando el TOE se encuentre en ejecución, este no solicitará la asignación de ninguna dirección explícita de memoria del sistema, ni asignará memoria con permisos simultáneos de escritura y ejecución.

La aplicación no realiza el mapeo de ninguna dirección de memoria explícita y nunca se llama a la función mprotect ni a la función mmap con los flags PROT_WRITE y PROT_EXEC al mismo tiempo.

EXP.2 El TOE está configurado por defecto con permisos de ficheros que lo protejan de accesos no autorizados.

La aplicación tiene permisos exclusivos de acceso en lectura y escritura sobre el directorio en el que se crean los ficheros de la aplicación.

5.1.9 Autenticación frente a la AEAT

OTP.1 La aplicación permitirá recibir peticiones de autenticación del usuario frente a la AEAT.

Dichas peticiones se reciben inicialmente en forma de notificación y, una vez el usuario abre la aplicación, esta se comunica con el servidor de la AEAT a través del canal definido en COM.1 para autenticarse.

OTP.2 La aplicación permitirá al usuario aceptar o rechazar las peticiones de autenticación.

En Cl@ve Móvil, se muestra un cuadro de diálogo en la interfaz gráfica de la aplicación con información de la petición y las opciones “Confirmar” o “Rechazar”. Por otro lado, en Cl@ve PIN, se muestra un código que ha de ser introducido en la plataforma donde se haya seleccionado el uso de Cl@ve PIN.

OTP.3 La aplicación permitirá al usuario seleccionar a qué petición desea acceder si tiene al mismo tiempo dos peticiones válidas. Para tener dos peticiones válidas, una debe ser de Cl@ve PIN y la otra de Cl@ve Movil.

OTP.4 Las peticiones de autenticación caducarán tras un tiempo determinado después de haberse realizado.

Para las peticiones de Cl@ve Móvil, la interfaz gráfica muestra un temporizador de cinco minutos asociado a cada petición de autenticación. Cuando el temporizador llega a cero, la petición se rechaza automáticamente. Por otro lado, para las peticiones de Cl@ve PIN, el temporizador será de 10 minutos.

OTP.5 La aplicación podrá ser desactivada en el dispositivo desde la página web de la AEAT.

Un apartado de la página web de la AEAT permite desactivar el dispositivo activo asociado a la cuenta de Cl@ve de una persona física.

OTP.6 La aplicación sólo podrá estar activa para un usuario en un dispositivo simultáneamente.

Durante el proceso de registro de un nuevo dispositivo en la aplicación, se comprueba si hay algún dispositivo ya registrado para la cuenta y, de ser así, se desactiva este último.

OTP.7 La aplicación requerirá la autenticación del usuario para aceptar las peticiones de autenticación.

Para peticiones de Cl@ve Móvil, después de hacer uso del botón “Confirmar” asociado a una petición de autenticación, el dispositivo solicita el desbloqueo seguro configurado en el mismo, previamente a realizar la operación solicitada.

Por otro lado, para peticiones de Cl@ve PIN, tras recibir y pulsar sobre la notificación de petición de PIN pendiente, se solicitará al usuario el desbloqueo seguro para poder visualizar el PIN recibido.

OTP.8 La aplicación permitirá el uso de códigos QR para crear una solicitud de autenticación del usuario frente a distintos servicios.

La aplicación permite escanear un código QR (generado por la AEAT). Cuando dicho código es escaneado, la aplicación muestra inmediatamente el diálogo que permite aceptar o rechazar la autenticación.

5.2 Correspondencia de las funciones de seguridad con las amenazas identificadas.

La siguiente tabla especifica qué funciones de seguridad mitigan cada una de las amenazas identificadas en el apartado 4.3.

Amenaza	*Función de seguridad*
A.ATAQUE_RED	COM.1, COM.2, COM.3, CIF.1, AUM.1
A.INTERVENCION_RED	COM.1, COM.2, COM.3, CIF.1, AUM.1
A.ATAQUE_LOCAL	EXP.1, EXP.2, PSC.1, PSC.2, PSC.3E, PSC.4E, IAU.6E, ACT.4, ACT.5, CDS.1, CIF.2
A.ACCESO_FISICO	EXP.1, EXP.2, PSC.1, PSC.2, PSC.3E, IAU.4, IAU.6E, IAU.4, OTP.5, CDS.1, CIF.2
A.SUPLANTACION	OTP.1, OTP.2, OTP.3, OTP.4, OTP.5, OTP.6, OTP.7, OTP.8

Tabla 5 Correspondencia entre funciones de seguridad y amenazas

6 Anexo I: Librerías de terceros utilizadas

Librería	*Versión*	*Librería*	*Versión*
Kotlin	1.8.20	Android X navigation testing	2.5.3
Android X core	1.10.0	Zxing	3.4.0
Android X appcompat	1.6.1	Android X browser	1.5.0
Android X biometric	1.2.0-alpha05	Play services auth	20.5.0
Material	1.8.0	Play services auth api phone	18.0.1
Android X lifecycle view model	2.6.1	Okhttp3 tls	4.10.0
Android X lifecycle extensions	2.2.0	Glide	4.12.0
Kotlin coroutines	1.6.4	DNIEdroid	2.3
Carousel view	0.1.5	Bouncycastle bcprov-jdk15on	1.67
Firebase crashlytics	18.3.7	Bouncycastle bcpkix-jdk15on	1.67
Firebase analytics	21.2.2	Bouncycastle bctls-jdk15on	1.65
Firebase core	21.1.1	Jsoup	1.13.1
Firebase messaging	23.1.2	Okhttp3	4.10.0
Android X work	2.8.1	Okhttp3 urlconnection	4.9.1
Gson	2.8.9	Okhttp3 logging interceptor	4.8.1
Hilt	2.45	Junit	4.13.2
Kotlin metadata JVM	0.5.0	Android X test junit	1.1.5
Android X security crypto	1.1.0-alpha06	Android X test espresso	3.5.1
Android X activity	1.7.1		
Android X coordinatorlayout	1.2.0		
Android X navigation	2.5.3		
Retrofit2	2.9.0		

Tabla 6 Librerías de terceros utilizadas

7 Referencias

Código	*Referencia*
[CCN-STIC-2001]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0, marzo 2022
[CCN-STIC-2002]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0, marzo 2022
[CCN-STIC-140]	Taxonomía de referencia para productos de Seguridad TIC, septiembre 2023
[CCN-STIC-807]	Criptología de empleo en el ENS, mayo 2022
[PP-APP]	*Protection Profile for Application Software* (*version* 1.4)

Tabla 7 Referencias del documento

8 Acrónimos

Acrónimo	*Descripción*
IdP	Proveedor de Identidades
SP	Proveedor de Servicios
eIDAS	*electronic IDentification, Authentication and trust Services*
AEAT	Agencia Estatal de Administración Tributaria
GISS	Gerencia de Informática de la Seguridad Social
SGAD	Secretaría General de Administración Digital
DGP	Dirección General de la Policía
SDK	*Sorfware Development Kit*
QR	*Quick Response*
SMS	*Short Message Service*
CCN	Centro Criptográfico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
LINCE	Certificación Nacional Esencial de Seguridad
ST	*Security Target* - Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TIC	Tecnologías de la Información y Comunicación
TOE	*Target Of Evaluation* – Objeto a evaluar

Tabla 8: Acrónimos

9 Índice de tablas

Tabla 1 Información del patrocinador, TOE y evaluación 3
Tabla 2 Metodología y criterios de evaluación 3
Tabla 3: Propiedades de seguridad activos sensibles. 11
Tabla 4: Parámetros de seguridad 14
Tabla 5 Correspondencia entre funciones de seguridad y amenazas 19
Tabla 6 Librerías de terceros utilizadas 20
Tabla 7 Referencias del documento 21
Tabla 8: Acrónimos 22

10Índice de figuras

Figura 1: Arquitectura 5