

Guía de Seguridad de las TIC CCN-STIC 1641

Procedimiento de Empleo Seguro Mi eID eSIGN 1.2



Mayo 2025





Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025

NIPO: 083-25-207-0

Fecha de Edición: Abril de 2025

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN	3
2 OBJETO Y ALCANCE	4
3 ORGANIZACIÓN DEL DOCUMENTO	5
4 FASE PREVIA A LA INSTALACIÓN.....	6
4.1 ENTREGA SEGURA DEL PRODUCTO	6
4.2 ENTORNO DE INSTALACIÓN SEGURO	6
4.3 REGISTRO Y LICENCIAS	6
4.4 CONSIDERACIONES PREVIAS	6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN.....	7
5 FASE DE INSTALACIÓN.....	8
6 FASE DE CONFIGURACIÓN.....	9
6.1 MODO DE OPERACIÓN SEGURO	9
6.2 AUTENTICACIÓN.....	9
6.3 ADMINISTRACIÓN DEL PRODUCTO	10
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA	10
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES	11
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS.....	11
6.5 GESTIÓN DE CERTIFICADOS.....	11
6.6 SERVIDORES DE AUTENTICACIÓN	11
6.7 SINCRONIZACIÓN	11
6.8 ACTUALIZACIONES	11
6.9 AUTO-CHEQUEOS.....	12
6.10 ALTA DISPONIBILIDAD	12
6.11 AUDITORÍA	12
6.11.1 REGISTRO DE EVENTOS	12
6.11.2 ALMACENAMIENTO LOCAL	12
6.11.3 ALMACENAMIENTO REMOTO	12
6.12 BACKUP	12
7 REFERENCIAS	14
8 ABREVIATURAS.....	15

1 INTRODUCCIÓN

1. ANF Certification Authority, S.L. (ANF CA) proporciona Mi eID eSIGN, un sistema de identificación remota no asistido para la emisión de certificados cualificados, *onboarding*, contratación en línea, certificación de manifestaciones de voluntad y actos de presencia en remoto.
2. Incorpora inteligencia artificial y tecnología NFC (lectura chip DN1e). Emplea técnicas biométricas de identificación y reconocimiento facial basados en algoritmos debidamente certificados por el NIST.
3. Verifica de manera automática la identidad de la persona; comprueba la autenticidad, vigencia e integridad de los documentos de identificación y su correspondencia con la persona que está en su posesión, obtiene evidencia certificada de video y sonido. Comprueba que el sujeto está vivo, no utiliza máscaras, ni emplea instrumentos de falsificación de imagen.
4. Cumple la Orden ETD/743/2022 [REF1], relativa a los métodos de identificación remota para la expedición de certificados electrónicos cualificados.
5. Incorpora servicio de firma y sellado electrónico cualificado, estampación de tiempo electrónico cualificado, servicio cualificado de conservación de evidencias a largo plazo, y servicio cualificado de validación de firmas y sellos electrónicos, en la generación de sus evidencias con plena eficacia jurídica.

2 OBJETO Y ALCANCE

6. El objeto del presente documento es brindar las medidas técnicas a tener en cuenta para el empleo seguro del sistema Mi eID eSIGN (versión 1.2).
7. Para su correcto funcionamiento, tanto desde el punto de vista funcional como de empleo seguro, la aplicación Mi eID eSIGN debe ser instalada en un dispositivo móvil (smartphone o equivalente) que cumpla las siguientes características:
 - a) La aplicación es compatible con dispositivos con sistemas Android, versión 8 o superior.
 - b) El dispositivo debe disponer de una cámara frontal y trasera con capacidad de capturar imágenes en resolución HD (1.280 x 720 píxeles) o superior.
 - c) El dispositivo debe soportar conexión NFC.
 - d) El dispositivo debe poderse conectar a Internet mediante protocolo HTTPS con velocidad media mayor o igual a 25Mbit/s.
8. El producto Mi eID eSign en su versión 1.2 ha sido cualificado en el catálogo CPSTIC para la familia “Herramientas de videoidentificación” para categoría ENS Alta.

3 ORGANIZACIÓN DEL DOCUMENTO

- a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
- b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
- c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- d) Apartado **7**. En este apartado se brindan las referencias: enlaces de interés a otros documentos citados y referenciados en este documento.
- e) Apartado **8**. En este apartado se definen las distintas abreviaturas presentes a lo largo del documento.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. La aplicación Mi eID eSIGN se distribuye directamente, previa demanda del cliente, por ANF Certification Authority. Esto garantiza que la aplicación pueda ser instalada en el dispositivo del cliente de forma segura, garantizándose la autenticidad e integridad de la aplicación mediante firma digital.
10. ANF Certification Authority no publica la aplicación Mi eID eSIGN en plataformas externas. En ningún caso los clientes deberán instalar la aplicación Mi eID eSIGN en formato APK o similar, que se encuentren publicados en sitios externos a ANF Certification Authority.

4.2 ENTORNO DE INSTALACIÓN SEGURO

11. El cliente solo es responsable de instalar la parte del sistema (aplicación) en su dispositivo móvil, acorde a los requerimientos descritos en la sección 2 OBJETO Y ALCANCE y siguiendo los pasos especificados en la sección 5 FASE DE INSTALACIÓN.
12. El sistema no requiere ningún tipo de despliegue o instalación por parte del cliente en un servidor propio en un Centro de Proceso de Datos (CPD).
13. La aplicación instalada por el cliente en su dispositivo móvil accede a la capa de servicio propia del sistema, que se encuentra en un entorno Cloud con certificación ENS (nivel ALTO) ubicado en la región europea, y que es administrado exclusivamente por ANF Certification Authority.

4.3 REGISTRO Y LICENCIAS

14. La aplicación Mi eID eSIGN no requiere que el cliente cree una cuenta (proceso de registro) o adquiera una licencia para su uso.
15. Durante la primera ejecución de la aplicación, el cliente solo debe leer y aceptar las Condiciones del Acuerdo de Licencia de Usuario Final ofrecida por la aplicación, para poder usar los servicios brindados por esta.

4.4 CONSIDERACIONES PREVIAS

16. Para un empleo seguro del sistema, se recomienda que el dispositivo móvil disponga:
 - a) Sistema Operativo Android con un usuario de mínimo privilegio preestablecido por el fabricante del dispositivo (no usuario *root*).
 - b) Sistema Operativo Android actualizado con la última versión disponible ofrecida por el fabricante para el dispositivo en cuestión.

- c) Un antivirus instalado en el Sistema Operativo Android y que se encuentre debidamente actualizado.
 - d) Sistema Operativo Android actualizado.
17. La aplicación Mi eID eSIGN a instalar por el cliente en su dispositivo móvil, tiene preconfigurado los parámetros de seguridad para establecer una comunicación segura con los servicios de ANF Certification Authority (ej. protocolo HTTPS sobre TLS v1.2 o superior). Dicha configuración no es accesible al cliente, con lo cual no se requiere que realice ningún cambio.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

18. La aplicación Mi eID eSIGN es instalada en el dispositivo móvil del cliente. No requiere que el cliente instale o configure ningún otro componente de operación adicional para su correcto funcionamiento.

5 FASE DE INSTALACIÓN

19. Como se comenta en la sección [4.1 ENTREGA SEGURA DEL PRODUCTO](#), el cliente instala la aplicación Mi eID eSIGN de forma convencional. No se requiere de ningún paso adicional para instalar la aplicación.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

20. Las configuraciones de seguridad de la aplicación Mi eID eSIGN están predeterminadas por defecto para cumplir con los requisitos y criterios definidos en la guía CCN-STIC 140.F11 [REF3] y en su mayoría, no son accesibles por el cliente. De esta forma, se evita que el cliente realice una configuración indebida de la aplicación o que tenga que realizar una configuración determinada para alcanzar un mayor grado de seguridad.
21. Las configuraciones que puede hacer el cliente en la aplicación Mi eID eSIGN, son exclusivamente las siguientes:
 - a) Por defecto, en cada uso de la aplicación, se le muestra al cliente los derechos de protección de datos que dispone al hacer uso de la misma. El cliente tiene la posibilidad de deshabilitar esta opción.
 - b) Por defecto, la lectura automática del CAN del documento de identidad se encuentra deshabilitada y se le pide al cliente que introduzca dicho valor manualmente. En caso que el cliente no pueda localizar directamente el número CAN en su documento de identidad, la aplicación brinda la posibilidad de realizar una lectura automatizada de dicho número, pero advierte las consecuencias activar la cámara para captar la imagen del documento de identidad.
 - c) Por defecto, la opción de fotografiar el documento de identidad se encuentra deshabilitada y no es requerida para llevar a cabo el proceso de video identificación. No obstante, el cliente puede habilitar esta opción y fotografiar su documento de identidad como prueba adicional de identificación, aunque se le advierte del riesgo de fotografiar el documento de identidad.
 - d) En el escenario en que el cliente ya dispone de un certificado cualificado, puede configurarlo en la aplicación como mecanismo de identificación/autenticación.

6.2 AUTENTICACIÓN

22. El cliente no necesita realizar autenticación alguna en la aplicación para llevar a cabo el proceso de identificación remota no asistido.
23. En el escenario en que el cliente ya tiene un certificado cualificado y vigente (emitido por un prestador de servicio cualificados acreditado), pero no tiene un DNI electrónico, el sistema permite tramitar la solicitud del certificado sin video identificación. En ese caso, la autenticación del cliente se realizará mediante firma electrónica empleando para ello su certificado cualificado vigente.
24. Los pasos para configurar los certificados del cliente en la aplicación Mi eID eSIGN para realizar la autenticación son los siguientes:

25. En la aplicación, el usuario debe seleccionar si certificado a configurar es de tipo “Centralizado” (gestionado por ANF AC) o archivo PKCS #12 (comúnmente con extensión “.pfx”)
26. Para certificados de tipo “Centralizado”:
 - a) Introducir Identificador y Contraseña para la autenticación en el servicio de “Centralizado” y dar click en el botón Autenticar.
 - b) La aplicación lista al usuario los certificados propios disponibles en el servicio de “Centralizado”. El usuario selecciona el certificado que desea emplear.
 - c) Una vez seleccionado, el usuario debe introducir el PIN del certificado para proceder a su uso.
27. Para certificados de tipo PKCS #12:
 - a) La aplicación usa los certificados que el usuario ya tenga instalados en el dispositivo móvil. En caso de no existir ningún certificado instalado, la aplicación brinda la posibilidad de instalar un nuevo certificado en el dispositivo móvil.
 - b) El usuario localiza y selecciona en el sistema de archivo del dispositivo móvil, el certificado que desea instalar.
 - c) Una vez seleccionado el certificado, el usuario debe introducir el PIN del mismo para proceder su instalación.
 - d) La aplicación procede a instalar el certificado en el dispositivo móvil y solicita al usuario que indique el tipo de uso que se dará al certificado. El usuario debe seleccionar la opción “Certificado de aplicación o VPN”.
 - e) El usuario debe escribir el nombre del certificado para identificarlo en el dispositivo y en la aplicación. Posteriormente podrá hacer uso del mismo.
28. La aplicación Mi eID eSIGN se autentica con la capa de servicio del sistema que se encuentra en el entorno Cloud mediante protocolo OAuth 2.0 y OpenID Connect sobre TLS v1.2 o superior. Este proceso de autenticación es desatendido y transparente para el cliente.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

29. El cliente no realiza ninguna operación de administración del sistema, ya sea de forma local en su dispositivo móvil en la aplicación Mi eID eSIGN o remota con la capa de servicio.
30. Todas las configuraciones de la aplicación Mi eID eSIGN están predefinidas (salvo las especificadas en la sección 6.1 MODO DE OPERACIÓN SEGURO) y no requieren de gestión o administración por parte del cliente.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

31. Dado que la aplicación no incluye ninguna funcionalidad de administración para el cliente, no existe una distinción de roles por parte del cliente al usar la aplicación Mi eID eSIGN.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

32. La aplicación Mi eID eSIGN se comunica con la capa de servicio del sistema que se encuentra en el entorno Cloud mediante protocolo HTTPS sobre TLS v1.2 o superior (en correspondencia con la guía CCN-STIC 807 [REF4]). Esta comunicación es transparente para el cliente, con lo cual no se requiere que el mismo realice ninguna configuración de interfaces, puertos o servicios.
33. La red que a la cual se conecta el cliente para realizar la verificación de identidad al usar la aplicación Mi eID eSIGN, no debe tener bloqueada la comunicación del protocolo HTTPS en los puertos predefinidos para dicho protocolo (puertos 443 o 8443) mediante algún cortafuego o sistema equivalente.

6.5 GESTIÓN DE CERTIFICADOS

34. No es necesario que el cliente se encargue de configurar y gestionar certificados la aplicación Mi eID eSIGN para establecer comunicación con la capa de servicios Cloud, que es gestionada únicamente por ANF Certification Authority.
35. El cliente solo deberá configurar sus certificados para autenticación solo en caso que sea necesario (ver sección [6.2 AUTENTICACIÓN](#)).

6.6 SERVIDORES DE AUTENTICACIÓN

36. No es necesario que el cliente configure los servidores de autenticación en la aplicación Mi eID eSIGN; dichas configuraciones están predefinidas y no son accesibles al cliente.

6.7 SINCRONIZACIÓN

37. No es necesario que el cliente realice algún tipo de configuración de sincronización horaria en la aplicación Mi eID eSIGN; dichas configuraciones están predefinidas y no son accesibles al cliente.

6.8 ACTUALIZACIONES

38. La actualización de la aplicación Mi eID eSIGN es automática mediante avisos lanzados por la propia aplicación. En ningún caso el cliente deberá actualizar la aplicación desde otra fuente.
39. La capa de servicio desplegada en el entorno Cloud, es actualizada por ANF Certification Authority de forma automática y transparente para el cliente.

6.9 AUTO-CHEQUEOS

40. No se realizan auto chequeos de la aplicación Mi eID eSIGN ya instalada en el dispositivo.
41. La capa de servicio desplegada en el entorno Cloud es monitorizada 24x7 para garantizar una disponibilidad de la misma.

6.10 ALTA DISPONIBILIDAD

42. La aplicación Mi eID eSIGN siempre está disponible para el cliente, le será facilitada de inmediato, previa demanda, por ANF Certification Authority.
43. La gestión de la capa de servicios Cloud recae en ANF Certification Authority exclusivamente y, por tanto, ésta se encarga de que el servicio sea replicado en varias instancias simultáneas para garantizar una alta disponibilidad.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

44. El registro de eventos en la aplicación Mi eID eSIGN se realiza de forma transparente para el cliente y no requiere ninguna configuración por parte de este.

6.11.2 ALMACENAMIENTO LOCAL

45. La aplicación Mi eID eSIGN no realiza copias locales del registro de eventos en el dispositivo móvil de cliente.

6.11.3 ALMACENAMIENTO REMOTO

46. Todas las trazas de los eventos generados durante el proceso de video identificación en la aplicación Mi eID eSIGN, son enviados a la capa de servicio Cloud gestionado por ANF Certification Authority y almacenados de forma segura (firmados digitalmente en el servidor) para ser auditados en el momento requerido.
47. La configuración del envío de trazas hacia a la capa de servicio Cloud, están predeterminadas en la aplicación Mi eID eSIGN y no es necesario que el cliente realice configuración alguna.
48. La aplicación Mi eID eSIGN no permite enviar las trazas de los eventos generados durante el proceso de video identificación a ningún servidor o plataforma externa.

6.12 BACKUP

49. La aplicación Mi eID eSIGN no almacena información alguna en el dispositivo móvil del cliente, con lo cual no es necesario realizar copias de respaldo.

50. Los backups del entorno Cloud son gestionados únicamente por ANF Certification Authority de forma automatizada y transparente para el cliente, no requiriendo intervención alguna por parte de este.
51. ANF Certification Authority realiza las copias de seguridad acorde a lo definido en su política de SGSI.

7 REFERENCIAS

- [REF1] Orden ETD/743/2022, de 26 de julio, por la que se modifica la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.
<https://www.boe.es/eli/es/o/2022/07/26/etd743>
- [REF2] Usar Google Play Protect para proteger tus aplicaciones y la privacidad de tus datos
Usar Google Play Protect para proteger tus aplicaciones y la privacidad de tus datos.
<https://support.google.com/android/answer/2812853?hl=es>
- [REF3] Guía de Seguridad de las TIC CCN-STIC 140. Taxonomía de productos STIC Anexo F.11: Herramientas de Videoidentificación.
<https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/5461-guia-140-anexo-f-11-herramientas-de-videoidentificacion/file.html>
- [REF4] Guía de Seguridad de las TIC CCN-STIC 807. Criptología de empleo en el Esquema Nacional de Seguridad.
<https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html>

8 ABREVIATURAS

APK	Android Package
CPD	Centro de Proceso de Datos
DNle	Documento Nacional de Identidad Electrónico
ENS	Esquema Nacional de Seguridad.
HD	<i>High Definition</i>
HTTPS	<i>HyperText Transfer Protocol Secure</i>
NFC	<i>Near Field Communication</i>
NIST	<i>National Institute of Standards and Technology</i>
SGSI	Sistema de Gestión de Seguridad de la Información
TLS	<i>Transport Layer Security</i>

