XVII JORNADAS STIC CCN-CERT

V JORNADAS DE CIBER_DEFENSA: ESPDEF-CERT

¿Cómo evaluar soluciones biométricas para incluir productos de videoidentificación en el catálogo CPSTIC / CCN STIC-105

ÍNDICE

1. LINCE, ENCSTI, CPSTIC y otras hierbas
2. Los sistemas de vídeo identificación en el MundoReal ®
3. El anexo F11 y la Instrucción Técnica 14
4. Conclusiones

LINCE, ENECSTI, CPSTIC y otras hierbas

¿Quién es quién?

OC-CCN

1 autoriza

Laboratorio acreditado

Certificación Nacional Esencial de Seguridad CCN

COMMON CRITERIA

3 evalúa

4 es incluido

2 define requisitos de seguridad

PRODUCTO SEGURIDAD TIC ens CATEGORÍA ALTA CCN CUALIFICADO

PRODUCTO SEGURIDAD TIC ens CATEGORÍA MEDIA CCN CUALIFICADO

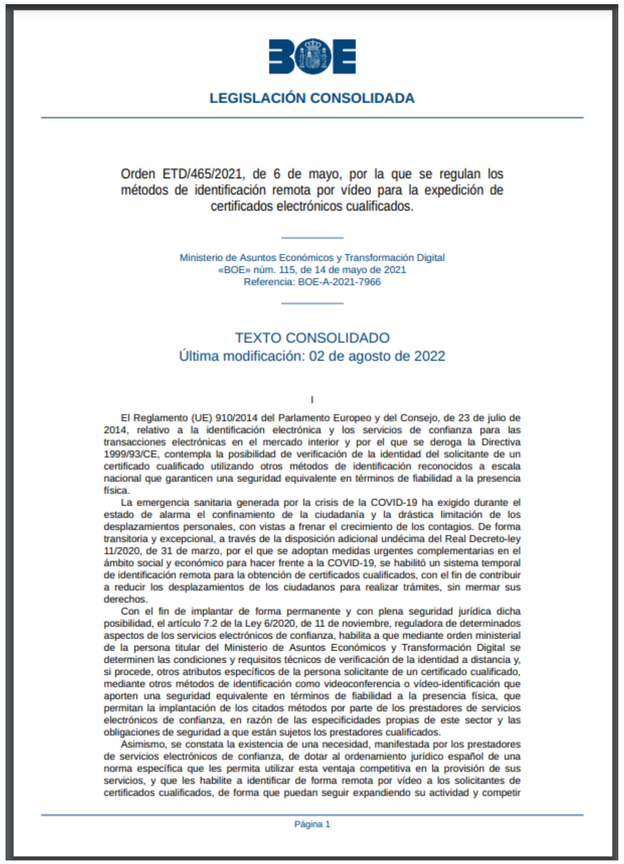
PRODUCTO STIC APROBADO CCN Centro Criptológico Nacional INFORMACION CLASIFICADA

cpSTIC

Catálogo de Productos y Servicios STIC

LINCE, ENECSTI, CPSTIC y otras hierbas

Un caso de uso particular: las herramientas de videoidentificación



BOE

LEGISLACIÓN CONSOLIDADA

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.

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 115, de 14 de mayo de 2021
Referencia: BOE-A-2021-7966

TEXTO CONSOLIDADO
Última modificación: 02 de agosto de 2022

I

El Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, contempla la posibilidad de verificación de la identidad del solicitante de un certificado cualificado utilizando otros métodos de identificación reconocidos a escala nacional que garanticen una seguridad equivalente en términos de fiabilidad a la presencia física.

La emergencia sanitaria generada por la crisis de la COVID-19 ha exigido durante el estado de alarma el confinamiento de la ciudadanía y la drástica limitación de los desplazamientos personales, con vistas a frenar el crecimiento de los contagios. De forma transitoria y excepcional, a través de la disposición adicional undécima del Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente a la COVID-19, se habilitó un sistema temporal de identificación remota para la obtención de certificados cualificados, con el fin de contribuir a reducir los desplazamientos de los ciudadanos para realizar trámites, sin mermar sus derechos.

Con el fin de implantar de forma permanente y con plena seguridad jurídica dicha posibilidad, el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, habilita a que mediante orden ministerial de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se determinen las condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, que permitan la implantación de los citados métodos por parte de los prestadores de servicios electrónicos de confianza, en razón de las especificidades propias de este sector y las obligaciones de seguridad a que están sujetos los prestadores cualificados.

Asimismo, se constata la existencia de una necesidad, manifestada por los prestadores de servicios electrónicos de confianza, de dotar al ordenamiento jurídico español de una norma específica que les permita utilizar esta ventaja competitiva en la provisión de sus servicios, y que les habilite a identificar de forma remota por vídeo a los solicitantes de certificados cualificados, de forma que puedan seguir expandiendo su actividad y competir

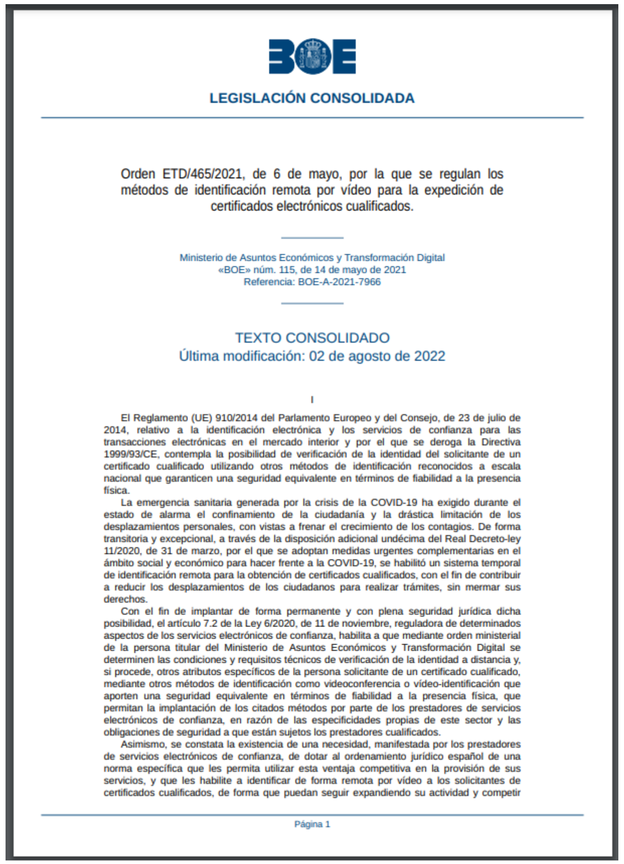
Página 1

La **emergencia sanitaria** generada por la crisis de la **COVID-19** ha exigido durante el estado de alarma el confinamiento de la ciudadanía y la drástica limitación de los desplazamientos personales, con vistas a frenar el crecimiento de los contagios. De forma transitoria y excepcional, a través de la disposición adicional undécima del Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente a la COVID-19, se habilitó un **sistema temporal de identificación remota para la obtención de certificados cualificados**, con el fin de contribuir a reducir los desplazamientos de los ciudadanos para realizar trámites, sin mermar sus derechos.

Con el fin de **implantar de forma permanente y con plena seguridad jurídica** dicha posibilidad, el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, habilita a que mediante orden ministerial de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se determinen las condiciones y **requisitos técnicos de verificación de la identidad a distancia** y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación **que aporten una seguridad equivalente en términos de fiabilidad a la presencia física**, que permitan la implantación de los citados métodos por parte de los prestadores de servicios electrónicos de confianza, en razón de las especificidades propias de este sector y las obligaciones de seguridad a que están sujetos los prestadores cualificados

LINCE, ENECSTI, CPSTIC y otras hierbas

Un caso de uso particular: las herramientas de videoidentificación



BOE

LEGISLACIÓN CONSOLIDADA

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.

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 115, de 14 de mayo de 2021
Referencia: BOE-A-2021-7966

TEXTO CONSOLIDADO
Última modificación: 02 de agosto de 2022

I

El Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, contempla la posibilidad de verificación de la identidad del solicitante de un certificado cualificado utilizando otros métodos de identificación reconocidos a escala nacional que garanticen una seguridad equivalente en términos de fiabilidad a la presencia física.

La emergencia sanitaria generada por la crisis de la COVID-19 ha exigido durante el estado de alarma el confinamiento de la ciudadanía y la drástica limitación de los desplazamientos personales, con vistas a frenar el crecimiento de los contagios. De forma transitoria y excepcional, a través de la disposición adicional undécima del Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan medidas urgentes complementarias en el ámbito social y económico para hacer frente a la COVID-19, se habilitó un sistema temporal de identificación remota para la obtención de certificados cualificados, con el fin de contribuir a reducir los desplazamientos de los ciudadanos para realizar trámites, sin mermar sus derechos.

Con el fin de implantar de forma permanente y con plena seguridad jurídica dicha posibilidad, el artículo 7.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, habilita a que mediante orden ministerial de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se determinen las condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física, que permitan la implantación de los citados métodos por parte de los prestadores de servicios electrónicos de confianza, en razón de las especificidades propias de este sector y las obligaciones de seguridad a que están sujetos los prestadores cualificados.

Asimismo, se constata la existencia de una necesidad, manifestada por los prestadores de servicios electrónicos de confianza, de dotar al ordenamiento jurídico español de una norma específica que les permita utilizar esta ventaja competitiva en la provisión de sus servicios, y que les habilite a identificar de forma remota por vídeo a los solicitantes de certificados cualificados, de forma que puedan seguir expandiendo su actividad y competir

Página 1

...

Empleará un producto de identificación remota por vídeo que cumpla los requisitos mínimos de seguridad indicados en el **anexo F.11** de la Guía de Seguridad de las TIC CCN-STIC-140, del Centro Criptológico Nacional de categoría alta. El prestador cualificado deberá seguir las indicaciones de configuración y uso seguro del producto. El cumplimiento de dicha obligación deberá ser certificado siguiendo **metodologías de evaluación reconocidas por el Organismo de Certificación del ENECSTI** (Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información), por un organismo acreditado según la norma ISO/IEC 17065.

No obstante, en caso de indisponibilidad de metodologías de evaluación aplicables para la certificación del producto, se admitirá la acreditación de cumplimiento de la citada obligación mediante la evaluación de su seguridad e inclusión en el **listado de productos cualificados del Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación** (Guía de Seguridad de las TIC CCN-STIC-105) publicado por el Centro Criptológico Nacional.

...

LINCE, ENECSTI, CPSTIC y otras hierbas

LINCE

LINCE es una **metodología de evaluación** y certificación para productos de seguridad TIC desarrollada por el Centro Criptológico Nacional enfocada en el **análisis de vulnerabilidades y las pruebas de penetración**.

Se ha desarrollado para ser un medio objetivo que permita valorar y acreditar la capacidad de un producto TIC para manejar información de forma segura.

A diferencia de otras certificaciones, como Common Criteria, la evaluación LINCE se realiza dentro de un **tiempo y esfuerzo bien acotados**. De esta forma, los costes son accesibles para todo tipo de fabricantes.

LINCE Básica: 25 días de esfuerzo, 8 semanas de duración

5 días de esfuerzo, 2 semanas de duración por cada módulo adicional:
+ Módulo **MEC**: Evaluación criptográfica
+ Módulo **MCF**: Análisis de código fuente

+ Módulo **MEB**: Evaluación Biométrica

“El CCN proporcionará las instrucciones técnicas y guías que se deben seguir para realizar la evaluación de cada una de las modalidades biométricas”

Los sistemas de video identificación en el MundoReal®

Casos de uso

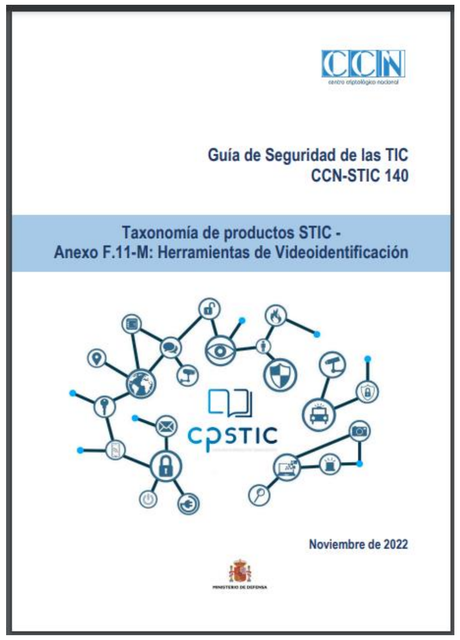
- Apertura de cuentas bancarias mediante firma electrónica cualificada en toda la UE
- Aprobación de operaciones entre la entidad y el consumidor en otros servicios financieros
- Procesos de firma electrónica cualificada disponibles en plataforma online, destinado a ser usado por PYMES.

El Anexo F11 y la Instrucción Técnica 14

Inyección de video

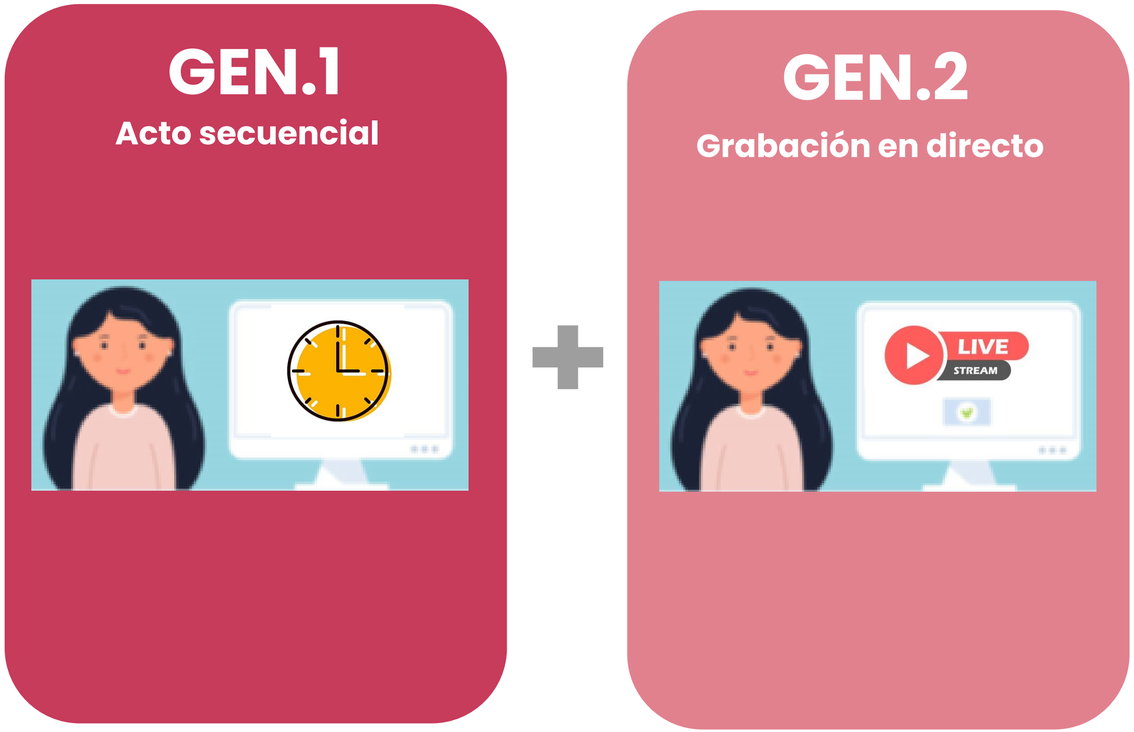
El Anexo F11 define los requisitos de seguridad esperables en una solución de video identificación:

° Administración confiable ° Identificación y autenticación ° Canales seguros ° Auditoría
° Protección frente a la captura de evidencias ° Verificación biométrica
° Validación de los documentos presentados



Protección frente a la captura de evidencias

=



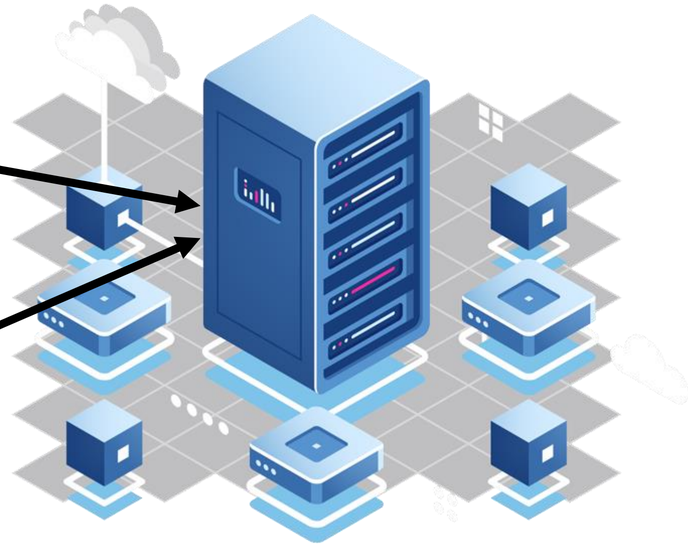
El Anexo F11 y la Instrucción Técnica 14

Inyección de video

El dispositivo de captura de video (la webcam) está bajo el control del sistema operativo, dos escenarios posibles:

Navegador web en PC

Aplicación nativa



Servidor de video identificación

El Anexo F11 y la Instrucción Técnica 14

Inyección de video

OBS es tu amigo

Soluciones implementadas por algunos fabricantes:
- Detección del nombre de la cámara o del número de cámaras

Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
CLSID	REG_SZ	{A3FCE0F5-3493-419F-958A-ABA1250EC20B}
FilterData	REG_BINARY	02 00 00 00 00 00 20 00 01 00 00 00 00 00 00 00 30...
FriendlyName	REG_SZ	Logitech C615

- Al ejecutarse el código en el navegador, manipular las peticiones suele ser trivial

El Anexo F11 y la Instrucción Técnica 14

Inyección de video

BlueStacks

Play Bigger

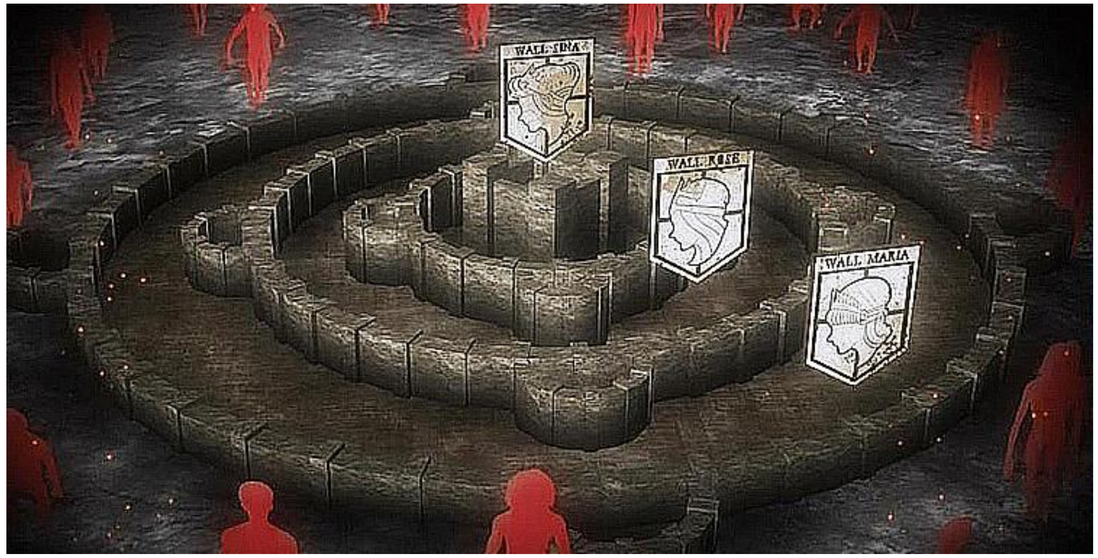
- Ninguna herramienta disponible
- Pequeña prueba de concepto usando Frida e interceptando y reemplazando el buffer de la cámara

FRIDA

Pepephone
14:15
15%
Atrás
Sergio jtsec
Llamando...
cámara
silenciar
voltear
Javata
Audio de Telegram...
Incoming Video Call
camera
mute
flip
Decline
Accept
Alt Gr
Ctrl
Mayús

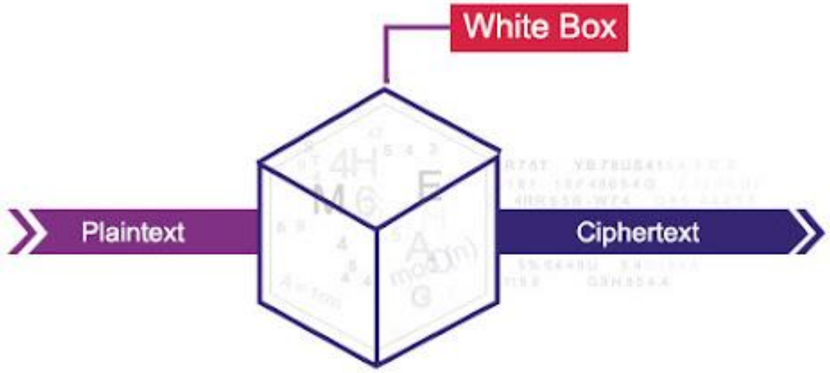
El Anexo F11 y la Instrucción Técnica 14

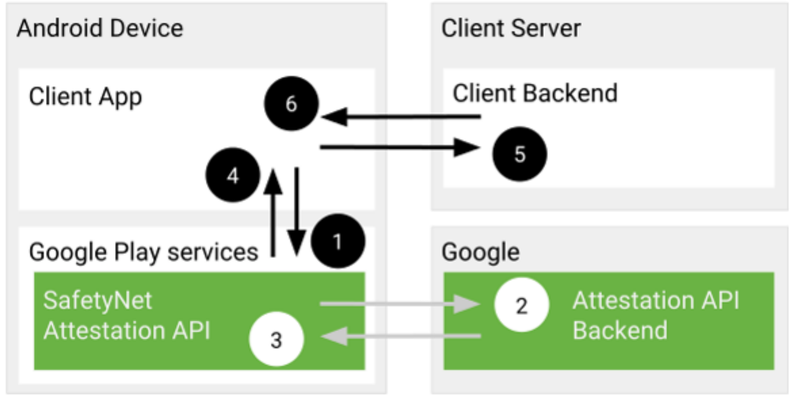
Inyección de video



Defenderse es complejo. Hay que garantizar que la petición viene de un dispositivo no comprometido:

- Certificate pinning
- Peticiones firmadas
- Detección de jailbreak
- Criptografía de caja blanca / Ofuscación
- Android SafetyNet + Hardware attestation // iOS AppAttest



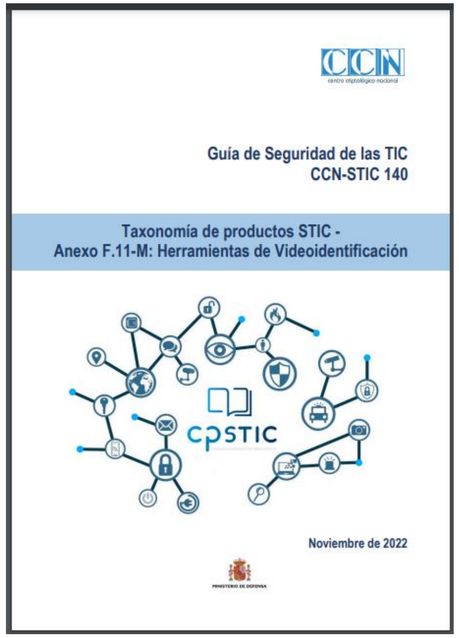


El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación

El Anexo F11 define los requisitos de seguridad esperables en una solución de video identificación:

° Administración confiable ° Identificación y autenticación ° Canales seguros ° Auditoría
° Protección frente a la captura de evidencias ° Verificación biométrica
° Validación de los documentos presentados



Verificación biométrica

=

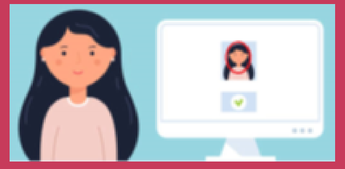
SOL.1

Verificación biométrica facial

Foto del documento

vs

Imagen capturada



+

SOL.2

Detección de vida

+

SOL.3

Mecanismos de detección de ataques de presentación

El Anexo F11 y la Instrucción Técnica 14

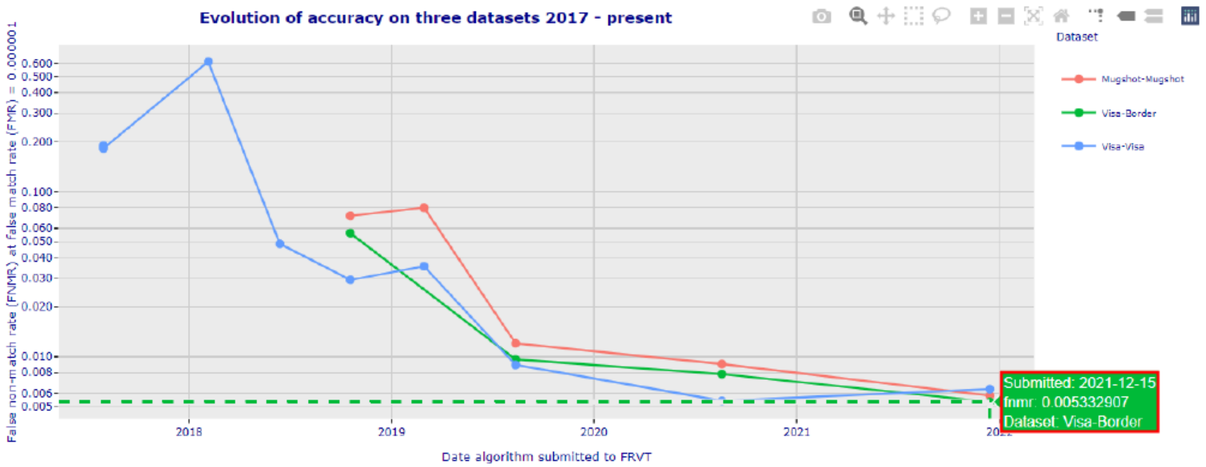
Pruebas funcionales y ataques de presentación – Setup de pruebas

- Elgato HD60 X Capturadora de vídeo externa
- Caja Razer Core X + GEForce RTX 3080 Trinity OC LHR 10GB 320BIT GDDR6x
- TV Samsung QLED UltraHD 4K HDR10+ 75”
- Webcam Logitech C920e
- Maquillaje
- Máscaras

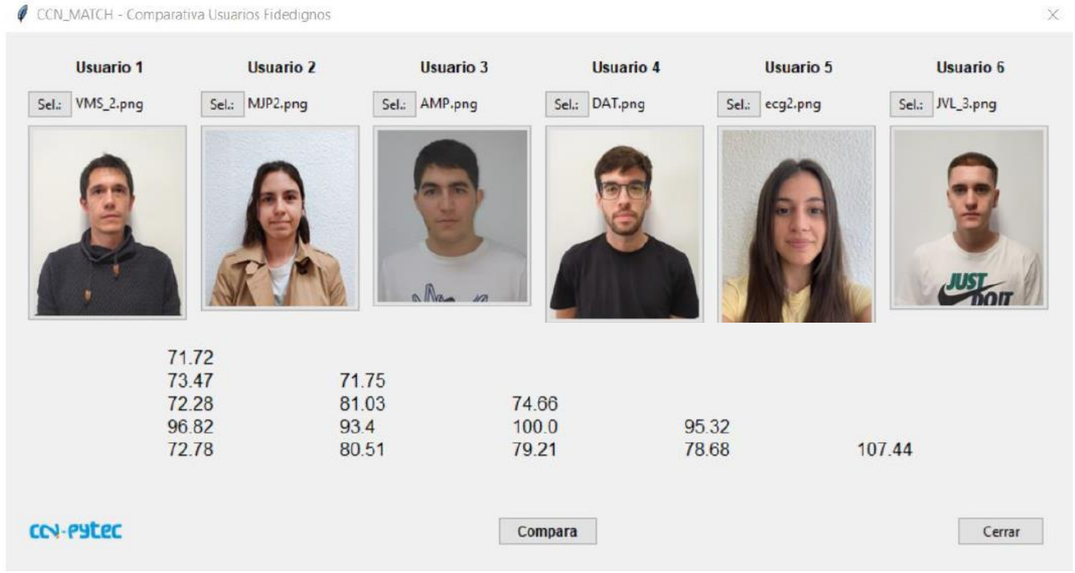
- CCN Match
- DeepFaceLab: Framework Open Source para facilitar la creación de deepfakes.
- DeepFaceLive: Framework Open Source para ejecutar deepfakes en tiempo real.
- Google Colab: Integración de Jupyter Notebooks en la nube por parte de Google.

El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación – Pruebas funcionales



Face Recognition Vendor Test (FRVT) en la categoría VISABORDER del NIST con una tasa de FNMR (False Non Match Rate) menor o igual a 5% para un FMR (False Match Rate) de menor o igual a 1/1000000.



Comprobar que el producto funciona correctamente en los casos habituales de uso, suponiendo un uso cooperativo por parte del sujeto fidedigno.

El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación – Ataques de impostor

Parecidos razonables

El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación – Ataques de impostor

El Anexo F11 y la Instrucción Técnica 14

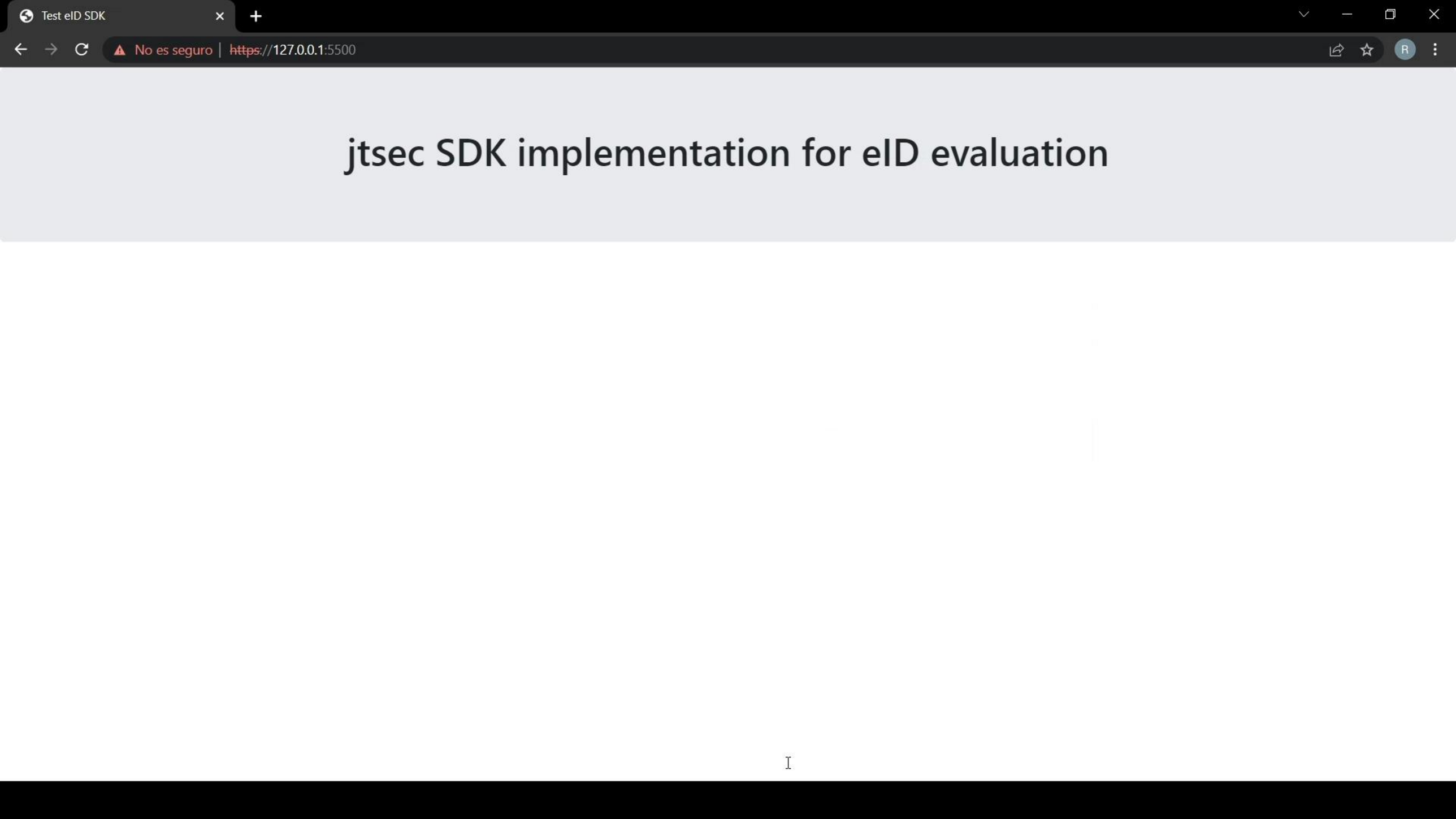
Pruebas funcionales y ataques de presentación – Video en pantalla

Objetivo de la prueba: Comprobar que el producto no es vulnerable a la suplantación de un sujeto fidedigno por parte de un atacante que utilice un vídeo de un sujeto fidedigno.

Ataque: Reproducimos un video del sujeto fidedigno en la TV de 75” realizando una identificación de manera correcta.

Prerrequisitos: El escenario de ataque contempla que el atacante ha robado el DNI del sujeto fidedigno y ha sido capaz de grabar una prueba de vida del usuario.

Posible defensa: Aleatorización de la prueba de vida.


Test eID SDK
No es seguro | https://127.0.0.1:5500
jtsec SDK implementation for eID evaluation

El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación – Máscaras de bajo coste

Objetivo de la prueba: Comprobar que el producto no es vulnerable a la suplantación de un sujeto fidedigno por parte de un atacante que utilice una máscara de bajo coste como artefacto.

Ataque: Utilizamos dos tipos de máscaras:
- Máscara impresa en papel
- Máscara “segunda piel”

El atacante tiene que taparse la boca para simular la prueba de vida del producto (sonreír).

Prerrequisitos: El escenario de ataque contempla que el atacante ha robado el DNI del sujeto fidedigno y ha sido capaz de generar una máscara de bajo coste a partir de una foto del sujeto fidedigno.

Posible defensa: Aleatorización de la prueba de vida. Detección de brillos.

Test eID SDK

https://127.0.0.1:5500

jtsec SDK implementation for eID evaluation

El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación – Máscaras avanzadas

Objetivo de la prueba: Comprobar que el TOE no es vulnerable a la suplantación de un sujeto fidedigno por parte de un atacante que utilice una máscara avanzada como artefacto.

Ataque: Limitado por el coste de las máscaras. Dos máscaras para todos los laboratorios (~800€ c/u). El CNP genera especímenes de DNI para realizar la prueba.
El atacante tiene que taparse la boca para simular la prueba de vida del producto (sonreír).

Prerrequisitos: El escenario de ataque contempla que el atacante ha robado el DNI del sujeto fidedigno y ha sido capaz de generar una máscara avanzada a partir de una foto del sujeto fidedigno.

Posible defensa: Aleatorización de la prueba de vida. Detección de pesadillas.

https://www.etsy.com/jp/shop/maskshopOMOTE

http://www.barbatosfx.com/

El Anexo F11 y la Instrucción Técnica 14

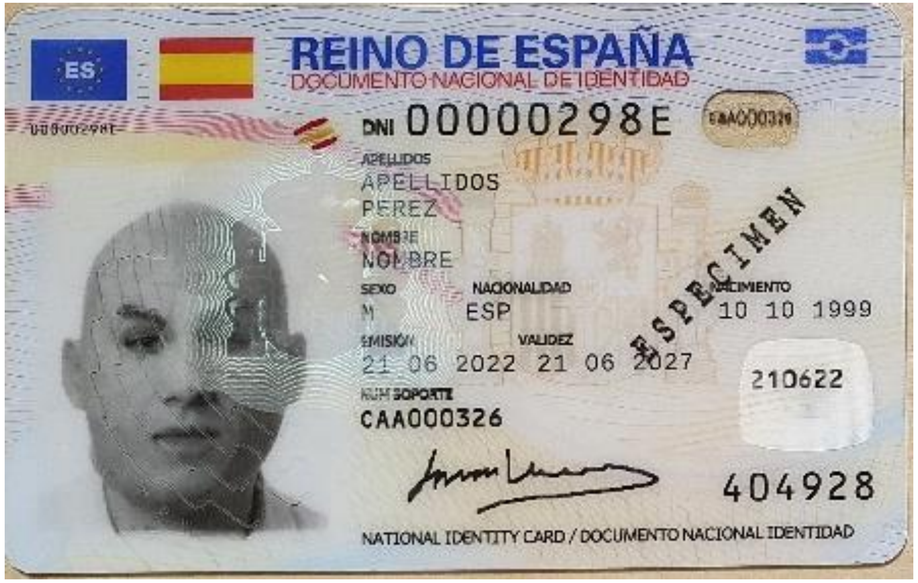
Pruebas funcionales y ataques de presentación – Máscaras avanzadas

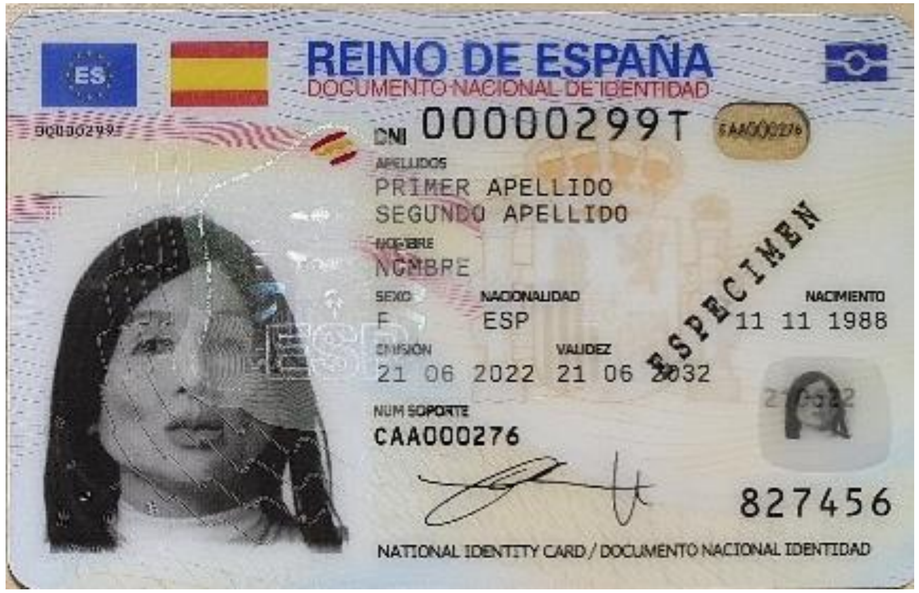
El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación – Máscaras avanzadas

El Anexo F11 y la Instrucción Técnica 14

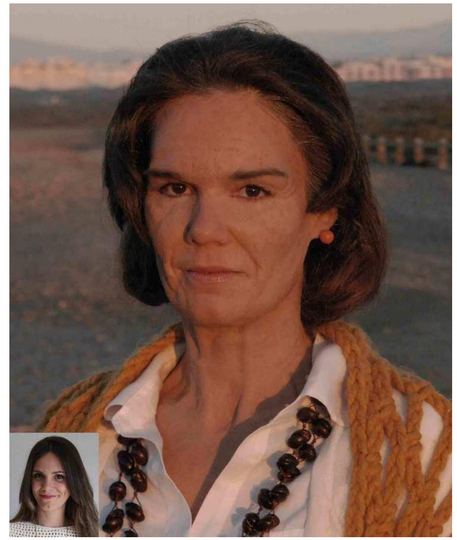
Pruebas funcionales y ataques de presentación – Máscaras avanzadas





El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación – Maquillaje



Objetivo de la prueba: Comprobar que el TOE no es vulnerable a la suplantación de un sujeto fidedigno por parte de un atacante que utilice maquillaje protésico como artefacto.

Ataque: Limitado por el coste de las prótesis y el maquillaje.

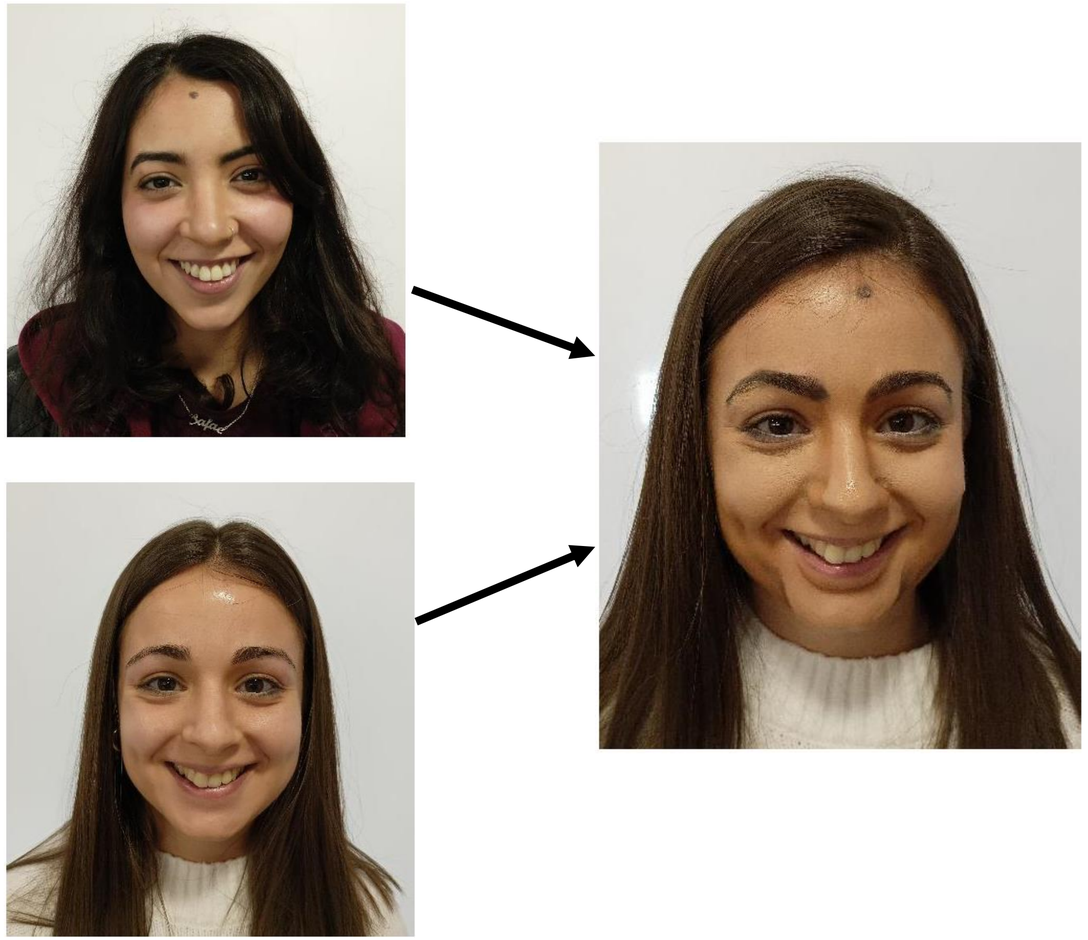
Prerrequisitos: El escenario de ataque contempla que el atacante ha robado el DNI del sujeto fidedigno y ha sido capaz de generar una máscara a partir de una foto del sujeto fidedigno.

Posible defensa: ¿?¿?¿?¿?¿?¿?

El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación – Maquillaje

rostro serio



rostro sonriendo

plementation for eID evaluation
Done!

El Anexo F11 y la Instrucción Técnica 14

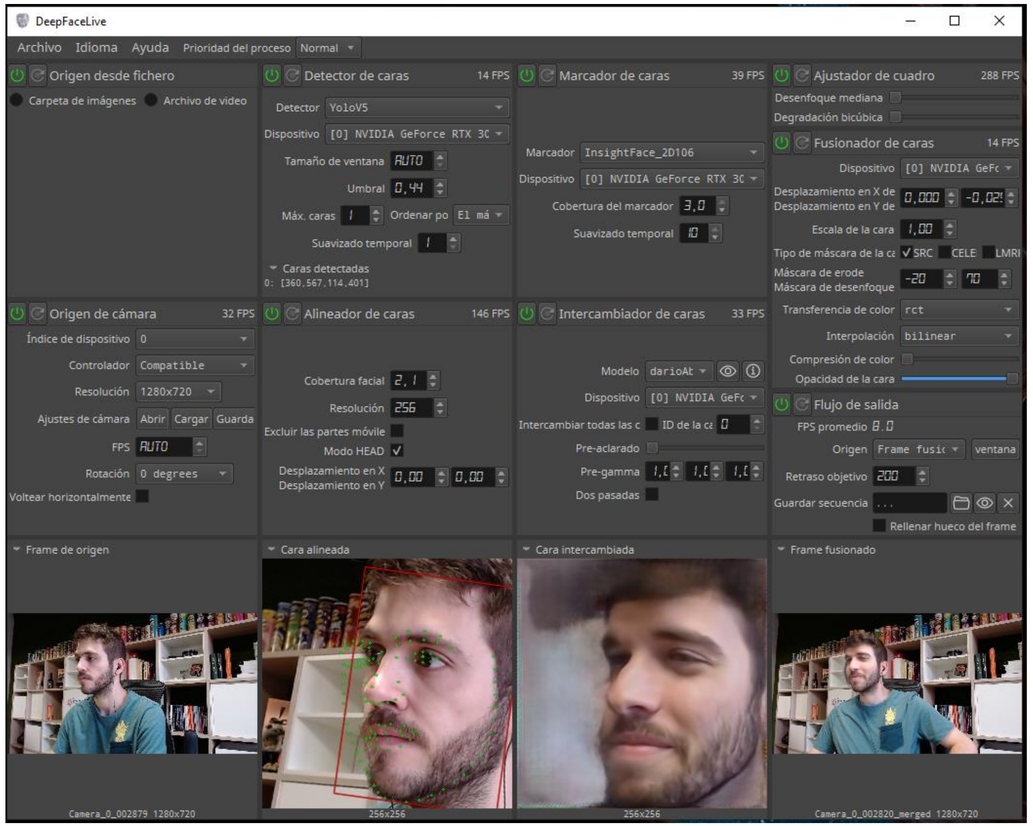
Pruebas funcionales y ataques de presentación – DeepFake

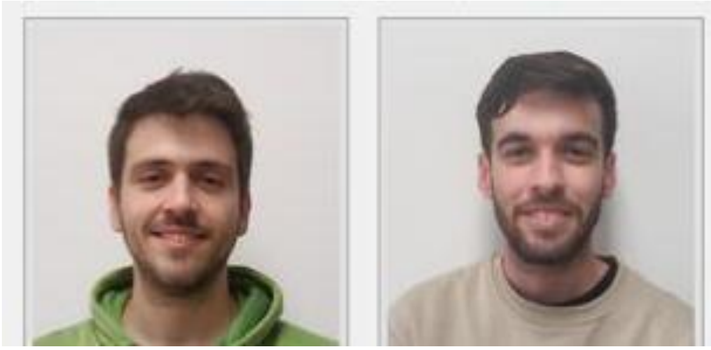
Objetivo de la prueba: Comprobar que el TOE no es vulnerable a la suplantación de un sujeto fidedigno por parte de un atacante que utilice herramientas de DeepFake

Ataque: Limitado por el parecido máximo según CCN-MATCH. Hay que ejecutarlo en tiempo real.

Prerrequisitos: El escenario de ataque contempla que el atacante ha robado el DNI del sujeto fidedigno y ha sido capaz de generar un DeepFake a partir de múltiples fotos del sujeto fidedigno.

Posible defensa: Aleatorización de la prueba de vida. Detección de artefactos en la imagen. Evitar la inyección de vídeo / Detectar pantallas.





New Tab

Test eID SDK

https://127.0.0.1:5500/index_fixed.html

jtsec SDK implementation for eID evaluation

Type here to search

21°C Mostly cloudy

ENG
ES

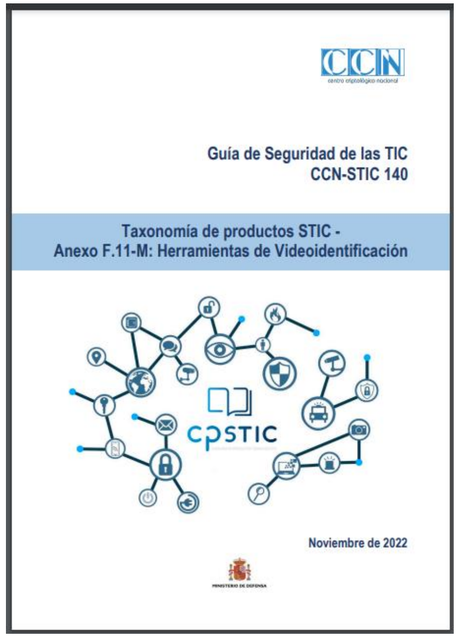
13:18
04/11/2022

El Anexo F11 y la Instrucción Técnica 14

Validación de documentos

El Anexo F11 define los requisitos de seguridad esperables en una solución de video identificación:

° Administración confiable ° Identificación y autenticación ° Canales seguros ° Auditoría
° Protección frente a la captura de evidencias ° Verificación biométrica
° Validación de los documentos presentados



Validación de los documentos presentados

=

DOC.1

Detectar ataques de replicación e impresión

+

DOC.2

Verificar fecha de validez

+

DOC.3

Zona de inspección visual (VIZ) == la MRZ (zona de lectura mecanizada).

El Anexo F11 y la Instrucción Técnica 14

Validación de documentos

cd42221a-a401-4418-91dc-0b6f5fcb0665

Chip · Header · Signature
Hologram · Flag 2 · Photo
Flag 1 · OVI · Badge

impresión en papel

39947e3a-df39-418c-9e21-68f43e235ad0

Chip · Header · Signature
Hologram · Flag 2 · Photo
Flag 1 · OVI · Badge

sobre tarjeta de PVC foto del DNI en pantalla

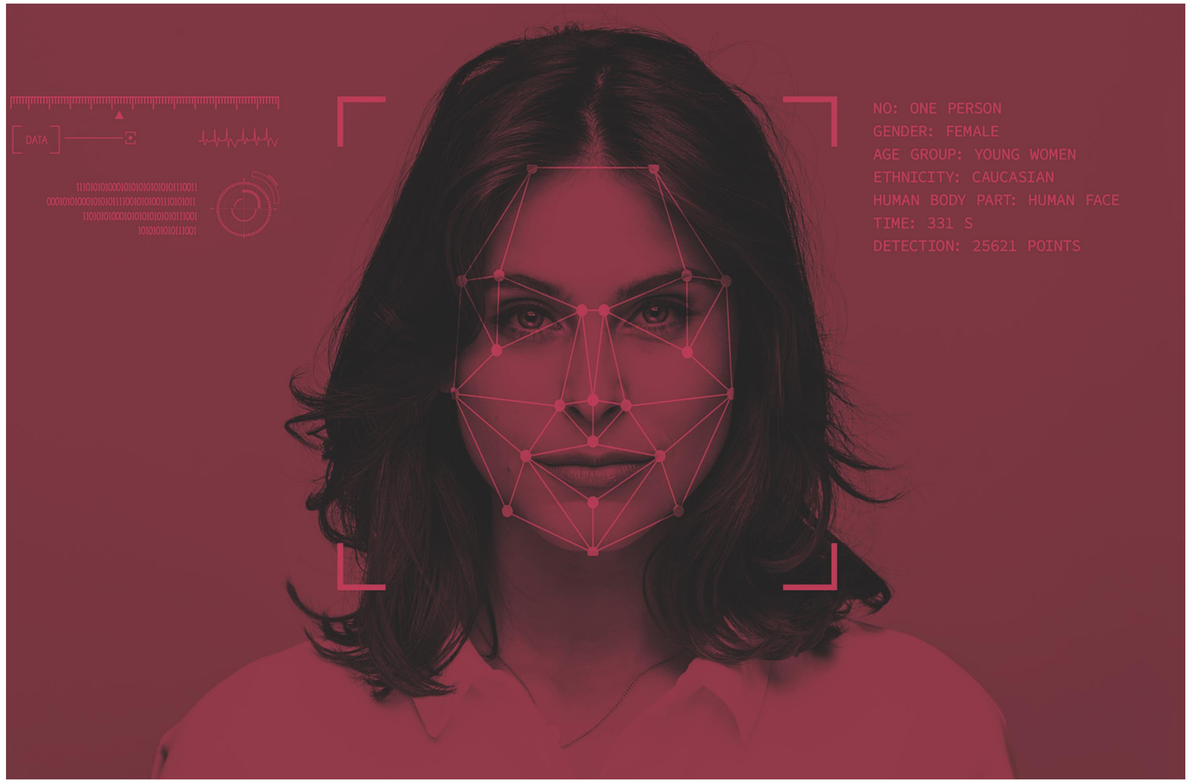
39947e3a-df39-418c-9e21-68f43e235ad0

Chip · Header · Signature
Hologram · Flag 2 · Photo
Flag 1 · OVI · Badge

e78f937a-66b8-49de-a3b7-30d487ef1d26

Chip · Header · Signature
Hologram · Flag 2 · Photo
Flag 1 · OVI · Badge

recorte de papel sobre foto del DNI



Conclusiones
(breves)

- **Hackear sistemas de video identificación es divertido**
- Todos los productos que hemos probado son mejorados como resultado de la evaluación
- Propuesta española presentada en CEN / TC 224 / WG 18 Biometrics → Se aprobó como Elemento de Trabajo Preliminar (PWI) en diciembre de 2022
- El estado del arte hace difícil (pero no imposible) evitar la inyección de video y el DeepFake
- El proceso completo aporta una garantía adicional por la presencia de un operador humano
- No esperar más de un sistema automático que de uno manual (e.g. gemelos, maquillajes o DeepFake avanzados, etc)

Conclusiones

Extra slide!

- El ritmo de avance de estas técnicas es imparable
- El coste de atacar es bajo (menos de 100€ con Google Colab Pro+ con una GPU Nvidia A100 y 36-48 horas de entrenamiento)
- La actual instrucción técnica requiere mantenimiento continuo para permanecer state-of-art.
- **Tenemos que seguir subiendo la barrera**

MUCHAS GRACIAS

COMPARTIR PARA GANAR

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

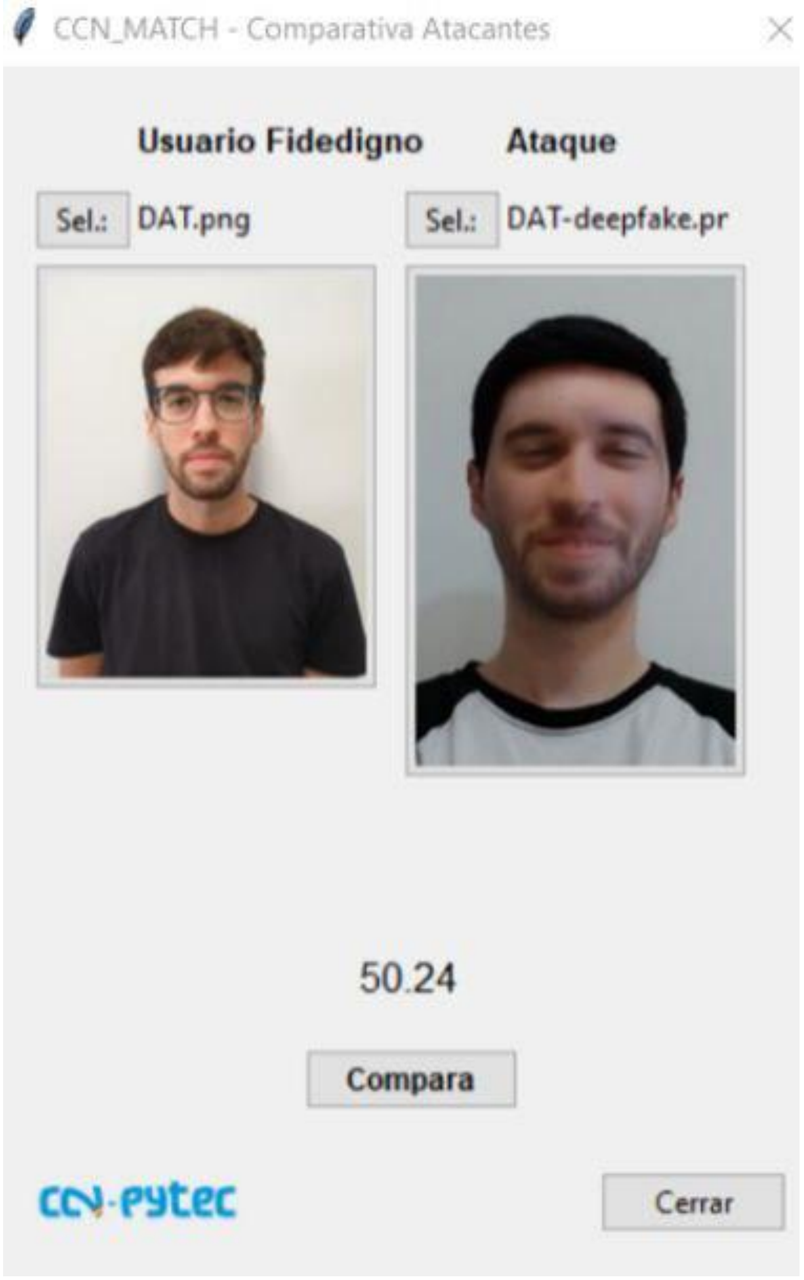
U 23 PRESIDENCIA ESPAÑOLA CONSEJO DE LA UNIÓN EUROPEA

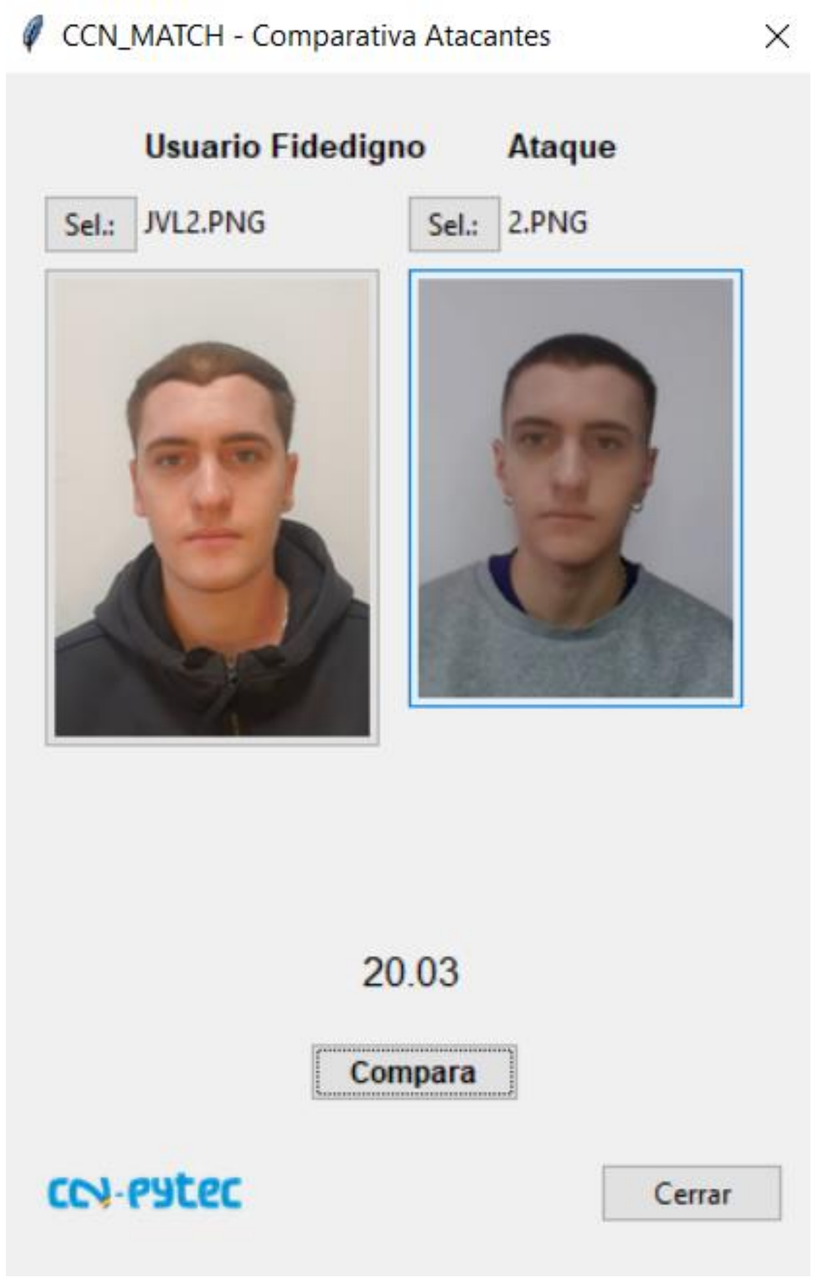
CCN centro criptológico nacional

ccn-cert centro criptológico nacional

espdef-cert Mando Conjunto del Ciberespacio

Conclusiones





Extra slide!

- Un laboratorio podría hacer un deepfake que de 50-60 (pasas los requisitos) y otro podría usar un deepfake más entrenado que de 20-30 y sería el caso de un ataque más profesional

El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación – Ataques de impostor

El Anexo F11 y la Instrucción Técnica 14

Pruebas funcionales y ataques de presentación – Ataques de impostor