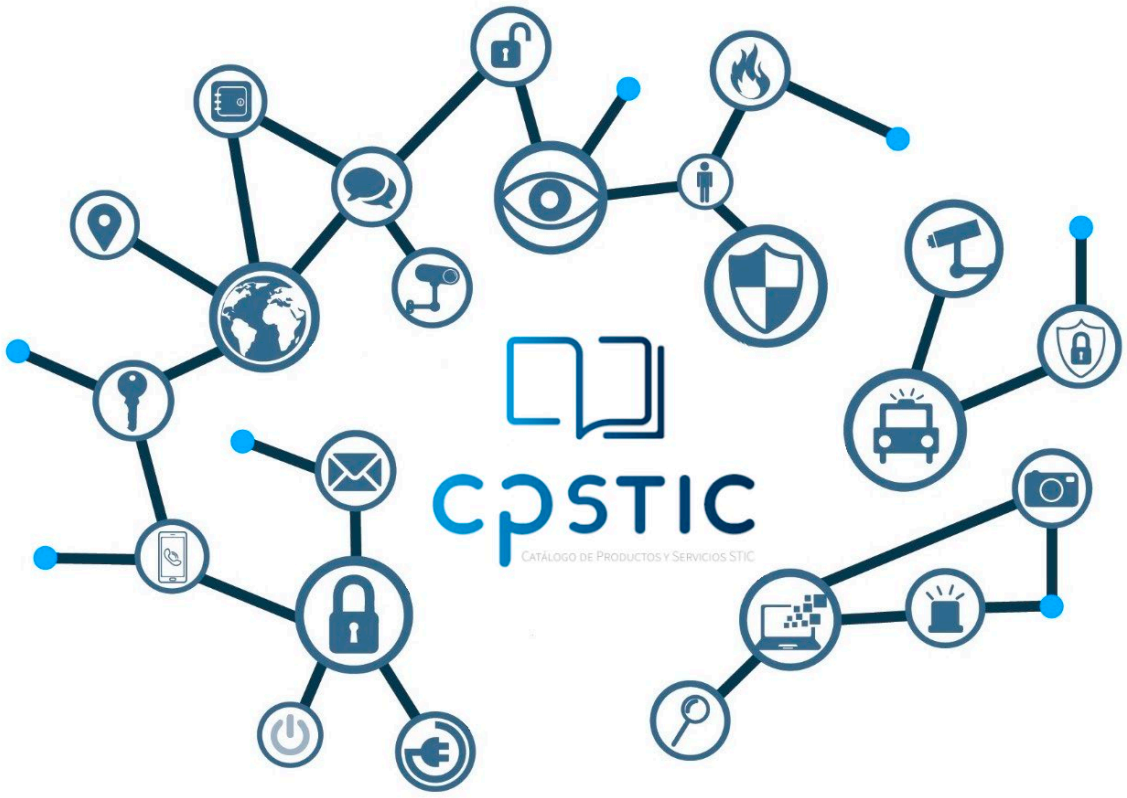
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1627

Procedimiento de Empleo Seguro
CertificadoElectronico.es



Agosto de 2023

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.15 12:04:07 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-288-1.
Fecha de Edición: agosto de 2023.

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

ÍNDICE

1. INTRODUCCIÓN

1. Bewor ofrece un producto de VideoID, **certificadoelectronico.es**, que consiste en una **solución de video identificación para la verificación de identidad**. Esta verificación es llevada a cabo de manera remota, realizando una comparación biométrica de la persona que ejecuta el proceso y la fotografía de su documento de identidad.
2. Durante el proceso, para poder realizar las comprobaciones, la persona deberá mostrar el rostro y ambos lados del documento de identidad. La solución de VideoID realiza las siguientes comprobaciones:
    - **Verificación biométrica**: Durante el proceso se ejecuta una comparación biométrica entre la persona y la foto extraída del documento. Como parte de la verificación, se comprueba la prueba de vida mediante un proceso pasivo, no requiere al usuario la realización de movimientos.
    - **Lectura de OCR**: El proceso realiza captura de ambos lados del documento de identidad, sobre estas capturas se ejecuta un proceso de lectura de texto vía CR que extrae la información del documento.
    - **Veracidad del documento**: Tanto con el análisis de la información extraída en texto como con la detección de holograma, se evalúa si hay intento de fraude, la vigencia del documento y la veracidad de la información extraída.
3. Por otro lado, Bewor también ofrece una aplicación a través de la cual un operador realiza la revisión de las evidencias extraídas del proceso de videoID y la revisión del proceso completo realizado por la persona. Esta aplicación permite aprobar o rechazar cada solicitud recibida, registrado un log de acciones realizadas.

2. OBJETO Y ALCANCE

4. El objeto de este documento es especificar la configuración para el uso de la solución VideoID, **certificadoelectronico.es**, y la aplicación de revisión (CMS) de Bewor.

5. El servicio de VideoID ofrece una API que permite su integración con la aplicación del cliente.

6. La solución completa CertificadoElectronico.es, que incluye el servicio de video-identificaicón, el CMS y la API, **ha sido cualificada e incluido en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) en la familia *"Herramientas de Videoidentificación".***

3. ORGANIZACIÓN DEL DOCUMENTO

7. El documento sigue la siguiente estructura:

   a) **Apartado 4**. En este apartado se recogen **aspectos y recomendaciones** a considerar, antes y durante la instalación del producto.

   b) **Apartado 5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la **fase de configuración** del producto, para lograr una configuración segura.

   c) **Apartado 6**. En este apartado se recogen las tareas recomendadas para la **fase de operación** o mantenimiento del producto.

   d) **Apartado 7**. Referencias utilizadas en el presente documento.

   e) **Apartado 8**. En este apartado se hace referencia a las diferentes abreviaturas utilizadas.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. El uso de la VideoID de Bewor es mediante API. El cliente que solicite la integración con los servicios ofrecidos recibirá mediante correo electrónico el *API key* generado al cliente y el acceso a la documentación de cómo utilizar la API.

9. El acceso a la documentación de la API es privado, mediante el usuario y contraseña facilitado al cliente. Además, se mantiene una reunión con el equipo técnico que realizará la integración para indicar los requisitos que deben cumplir para el uso del servicio.

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. El entorno donde se ejecuta el servicio se encuentra en VPC (*Virtual Private Cloud*) de Amazon en el centro de datos de Irlanda (región eu-west-1).

11. El cliente vía API, solicita una video identificación, como respuesta recibe una URL donde la persona accede para realizar el proceso.

4.3 REGISTRO Y LICENCIAS

12. El servicio de VideoID no requiere ningún tipo de licencia de instalación, ya que se ofrece en modo SaaS (*Software as a Service*).

4.4 CONSIDERACIONES PREVIAS

13. Al ser un servicio en nube, no aplica consideraciones previas.

14. Si se desea ser notificado al finalizar el proceso de VideoID, se debe indicar al crear una solicitud de video identificación una URL a modo de *callback*. También se permite indicar una página de OK y otra de KO. Este punto está especificado en la documentación que se entrega al cliente.

15. El cliente puede indicar colores y logotipo a modo de configuración al solicitar un proceso de video identificación. Esta información es enviada en los parámetros de la llamada vía API.

4.5 INSTALACIÓN

16. La VideoID es ofrecida como un API, por lo que no requiere instalación.

17. El cliente debe realizar el proceso de integración y Bewor dará el soporte y seguimiento necesarios.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

18. Bewor ofrece la solución completa en un paquete cerrado. El servicio de video-identificación es ejecutado al completo dentro de su infraestructura, ofreciendo al cliente una URL para realizar el proceso, por lo que este punto no recae sobre el cliente.

5.2 AUTENTICACIÓN

19. Cada cliente dispone de un *API Key* único que garantiza la seguridad de sus comunicaciones y le permite acceder a la API. Esta comunicación está protegida mediante un certificado SSL.
20. El acceso a la documentación de la API es mediante email y contraseña. El cliente recibe en su email un enlace a través del cual configura su contraseña de acceso.
21. El acceso al CMS donde el agente puede validar una solicitud se realiza mediante *email* y contraseña, además debe introducir un OTP que recibe en cada proceso de *login*.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

22. El servicio VideoID es accesible de forma segura a través del protocolo HTTPS con TLS v1.2 o superior.

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

23. En el servicio existen tres (3) roles:
    - Operador. Encargado de revisar las evidencias y decidir su aprobación/rechazo. Tiene acceso a la sección del listado de solicitudes realizadas y puede ver el detalle de cada una.
    - Auditor. Puede consultar el *log* de auditoría que va generando la aplicación y el listado de solicitudes realizadas, sin poder ver el detalle de cada una.
    - Administrador. Rol designado para creación de usuarios. Además, puede realizar las mismas acciones que el auditor.
24. El personal autorizado de Bewor es quien posee el usuario Administrador, encargado de crear usuarios y asignarles el rol.
25. El usuario recibe en su email un enlace a través del cual configura su contraseña de acceso. Los requisitos de la contraseña son:
    - 8 caracteres como mínimo. Sin embargo, las contraseñas configuradas deben tener, al menos, 12 caracteres.
    - Al menos 2 letras
    - Al menos 2 números

- No puede tener más de 3 caracteres consecutivos

26. El usuario tiene obligaciones para cumplir:
    - No compartir la contraseña
    - No guardar la contraseña en papel o en formato digital
    - Cerrar sesión cuando el puesto de trabajo sea abandonado
    - Modificar la contraseña si hay sospecha de haber sido comprometida
27. La sesión tiene la siguiente configuración:
    - No se permiten sesiones concurrentes.
    - Las sesiones caducan pasado un tiempo de inactividad de 15 minutos.
    - En el caso de 3 intentos fallidos de *login*, es necesario esperar 10 minutos para volver a realizar otro intento.

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

28. Las conexiones con el producto se realizarán mediante conexión HTTPS mediante protocolo seguro TLS v1.2 o superior. No es necesario realizar ninguna configuración adicional por parte del cliente.
29. El producto emplea las siguientes ciphersuites, todas admitidas en la guía CCN-STIC 807 [REF2]:
    - *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256*
    - *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384*
    - *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
    - *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
    - *TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256*
30. Para el almacenamiento de credenciales se utiliza un cifrado admitido en la guía CCN-STIC 807 [REF2].

5.5 GESTIÓN DE CERTIFICADOS

31. No es necesario configurar la gestión de certificados.

5.6 SERVIDORES DE AUTENTICACIÓN

32. No es necesario configurar servidores de autenticación.

5.7 SINCRONIZACIÓN HORARIA

33. No es necesario realizar ningún tipo de configuración para la sincronización horaria.

5.8 ACTUALIZACIONES

34. Al ser un servicio SaaS, la actualización del servicio es transparente al cliente. Este es informado de los cambios introducidos en cada actualización.

5.9 AUDITORÍA

5.9.1 REGISTRO DE EVENTOS

35. El servicio almacena los siguientes registros de auditoría:
    - Inicio y cierre de sesión
    - Cambio de credenciales
    - Creación de usuario
    - Cambio de permisos a un usuario
    - Visualización de las evidencias de una solicitud
    - Aprobación/Rechazo de una solicitud, en caso de rechazo es registrado el motivo.
36. Además, el servicio registra cada consumo realizado a la API y su resultado.

5.9.2 ALMACENAMIENTO DE REGISTROS

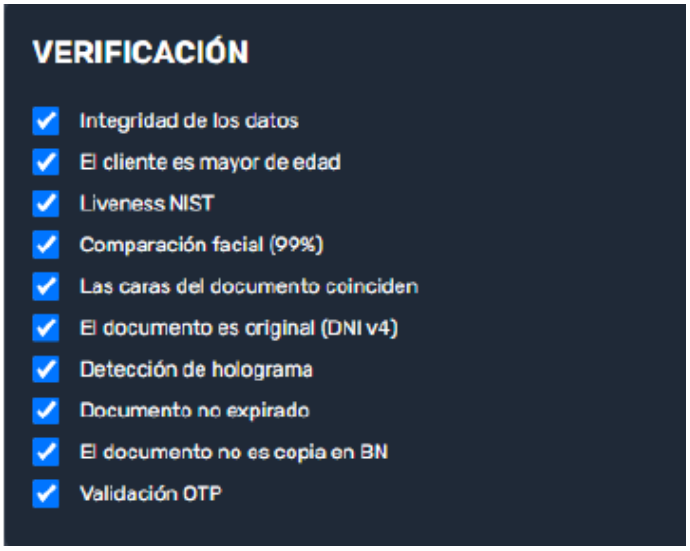
37. Los logs son almacenados en la infraestructura en la nube, no requiere configuración para almacenamiento local.

5.10 BACKUP

38. Se realiza una copia de seguridad íntegra y de forma separada diariamente. Esta copia se mantiene al menos, durante 7 días. Las copias de seguridad son inmutables y almacenadas en la zona de disponibilidad de EU-West-1.

5.11 SERVICIOS DE SEGURIDAD

39. La seguridad del servicio la proporciona la infraestructura de AWS, por lo que el cliente no necesita aplicar ninguna configuración de seguridad.
40. Los controles de seguridad para el cumplimiento de los RFS recogidos en la guía CCN-STIC 140.F11 [REF1] son regulados por Bewor.
41. Para considerar la video identificación válida, todas las verificaciones deben haberse superado con éxito.



42. La solicitud entrante a la API debe ser autenticada incluyendo un API Key con la credencial de cliente correspondiente. Se rechazan las solicitudes con el encabezado de clave de API incorrecto.
43. La aplicación cuenta con un servicio que controla el número de peticiones recibidas, bloqueando la IP si es detectado un número alto de peticiones. Hay instalado un cortafuegos para limitar el tráfico entrante.

6. FASE DE OPERACIÓN

44. Para el correcto funcionamiento del producto debe cumplir las siguientes características:

- El producto debe tener al día las actualizaciones relacionadas con seguridad.
- Se debe mantener la configuración del producto.
- Se deben analizar periódicamente los registros de auditoría.
- Se deben gestionar correctamente los certificados SSL.

7. REFERENCIAS

REF1 CCN-STIC 140 Taxonomía de productos STIC. Anexo F.11. Herramientas de Video de identificación.

https://www.ccn-cert.cni.es/ca/ultimas-guias/5461-guia-140-anexo-f-11-herramientas-de-videoidentificacion/file.html

REF2 CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad.

https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

8. ABREVIATURAS

API	*Application Programming Interaces*
AWS	*Amazon Web Services*
CMS	*Content Management System*
HTTPS	*HyperText Transfer Protcol Secure*
IP	*Internet Protocol*
OCR	*Optical Character Recognition*
OTP	*One Time Password*
RFS	Requisitos Fundamentales de Seguridad
SaaS	*Software as a Service*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*
URL	*Uniform Resource Locator*
VPC	*Virtual Private Cloud*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL