centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1218

Procedimiento de empleo seguro
Personal Code de HUBOX

Julio 2022

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

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
2022.09.20 17:31:03 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-202-X

Fecha de Edición: septiembre de 2022

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. *Personal Code* es una solución de identidad digital que resuelve el problema de fraudes por suplantación de identidad. Se puede entender la solución como una secuencia de bits que almacena, de forma segura, características biométricas e información biométrica de un individuo. Estos datos son firmados y reconocidos por una autoridad y se protegen mediante criptografía asimétrica para su posterior verificación a través de una aplicación que no requiere conectividad ni consultas a bases de datos.
2. *Personal Code* consiste en un SDK de generación de claves criptográficas para la inclusión de información que identifique de forma unívoca a un usuario determinado que utilice una aplicación final.
3. A su vez, dispone de una SDK de validación que permite realizar, en términos generales, el procedimiento inverso, validando la autenticidad de la información confidencial generada por el SDK de generación y extrayendo la información propiamente dicha.
4. La funcionalidad del producto consiste en la generación de dos códigos QR para la inserción de los datos personales de un usuario determinado y su posterior validación. Estos datos personales son aquellos que le permiten identificarlo de forma unívoca ante cualquier entidad.

2. OBJETO Y ALCANCE

5. El objeto del presente documento es facilitar la instalación y configuración segura del producto **Personal Code, versión 2020.3.2**, junto con el bastionado del entorno en el que se despliega.
6. El producto deberá ejecutarse sobre un sistema operativo Windows, con arquitectura x64 y con soporte de *.NET Framework 4.8* y *VC Redistributable 2015-2019.*

3. ORGANIZACIÓN DEL DOCUMENTO

7. Este documento está organizado en diferentes capítulos, de acuerdo con diferentes fases del ciclo de vida del producto:

   a) Apartado 4: Fase de despliegue.

   b) Apartado 5: Fase de instalación.

   c) Apartado 6: Recomendaciones en la fase de configuración y administración.

   d) Apartado 7: Recomendaciones en la fase de operación.

   e) Apartado 8: *Checklist* de las tareas a realizar.

   f) Apartado 9: Referencias.

   g) Apartado 10: Abreviaturas.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. El producto está formado por dos (2) SDK: uno de generación y otro de validación. Estos se reciben vía correo electrónico por parte de HuBOX en un fichero comprimido y protegido por contraseña.
9. Dicha contraseña será establecida entre la organización y HuBOX a través de una reunión, presencial o remota, una vez adquirido el producto.

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. Por razones de seguridad, el producto **debe instalarse en un Centro de Proceso de Datos (CPD)** o, en su defecto, en aquellos equipos cuyo acceso estará limitado a una persona o conjunto de personas que posean una autorización expresa.

4.3 REGISTRO Y LICENCIAS

11. El uso de los SDK de generación y validación se encuentra limitado por una licencia entregada por HuBOX. Para conseguir dicha licencia, la organización deberá obtener un identificador único de *hardware* (*Hardware ID*), mediante una herramienta proporcionada por HuBOX. Una vez obtenido el identificador se genera un fichero, el cual se deberá proporcionar a HuBOX, para la creación de la licencia correspondiente.
12. De esta forma se asocia dicho *Hardware ID* en el momento de la instalación a un único equipo, de forma que, si se intenta hacer una instalación en otro equipo, el producto no podrá utilizarse.
13. Se deberá verificar que la licencia se encuentra activa, a través de los mecanismos de revisión de estado que determina HuBOX en el apartado "*Criptografía*" del *Manual de Configuración de Ambiente - REF1*. De lo contrario deberá solicitar la renovación/regeneración de licencias.

4.4 CONSIDERACIONES PREVIAS

14. Se debe considerar el despliegue del producto en equipos con sistema operativo Windows con soporte de *.NET Framework 4.8* y *VC Redistributable 2015-2019*.
15. La organización deberá acondicionar el entorno de desarrollo o productivo acorde con los documentos *Manual de Configuración de Ambiente - REF1* e *Instalacion NeurotechnologyTrial – REF4,* proporcionados por HuBOX en conjunto con el producto; de tal forma que instale las dependencias necesarias para su correcto funcionamiento.
16. Dependiendo de la solución, para asegurar un funcionamiento continuo, se recomienda considerar un ambiente de alta disponibilidad donde se replique la

funcionalidad de los SDK en dos (2) líneas productivas (ver apartado 5.7 Alta disponibilidad).

5. INSTALACIÓN

17. Para la instalación del producto se deben seguir las instrucciones de los documentos *Manual de Configuración de Ambiente - REF1* e *Instalacion NeurotechnologyTrial – REF4*, entregados junto con el producto.
18. Dicho manual contempla las configuraciones mínimas de los equipos de desarrollo y de producción en los que se instalará el producto, así como la obtención de licencias correspondientes para el uso de los SDK de generación y validación.

6. FASE DE CONFIGURACIÓN

6.1 AUTENTICACIÓN

19. El producto no cuenta con mecanismos de autenticación propios. La autenticación del producto queda relegada en el sistema operativo sobre el cual se realice su instalación.
20. En caso de emplear autenticación basada en usuario/contraseña, **se deberá hacer uso de una política de contraseñas** para el acceso al sistema en el que se instale el producto que cumpla, al menos, con las siguientes características:
    - Longitud mínima de, al menos, 12 caracteres.
    - Composición con al menos una letra mayúscula, una minúscula, un número y un carácter especial.
    - Impedir reutilizar las últimas cinco contraseñas.
    - Establecer un periodo de validez de las contraseñas de 60 días y exigir su cambio una vez caduquen.
    - No permitir un nuevo cambio de contraseña hasta pasados, al menos, 10 días.

6.2 ADMINISTRACIÓN DEL PRODUCTO

21. El producto no cuenta con medidas propias de administración, sino que estas medidas recaen en el dispositivo y sistema operativo sobre el cual se instalen los SDK.
22. De tal forma, **se recomienda realizar la instalación del producto sobre un dispositivo que cuente con las cuentas de usuarios y permisos necesarios para permitir el acceso únicamente a aquellos usuarios que lo requieran**.
23. **Se recomienda acceder de forma local al dispositivo o, en caso de acceder remotamente, emplear protocolos de comunicación seguros como TLSv1.2 o superior, SSHv2 o IPsec**.
24. La funcionalidad de los SDK de generación y validación se encuentra ligada únicamente al equipo donde se realice su instalación.

6.3 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

25. El producto no implementa comunicaciones, si no que estas se deberán configurar e implementar en los sistemas que empleen los SDK de generación y validación. **Se recomienda por tanto implementar protocolos seguros de comunicación para hacer uso de las funciones del producto**. Se consideran protocolos seguros:
    - TLS, versión 1.2 o superiores.
    - IPsec.

- SSH versión 2.

6.4 GESTIÓN DE CLAVES Y CERTIFICADOS

26. Toda la gestión y generación de las claves y certificados empleados por el producto se lleva a cabo antes de la entrega del mismo, por parte de HuBOX. Esto incluye:
    - El par de claves empleadas para la generación y validación de los códigos QR. Dichas claves disponen de una validez de un año, tras la cual deberán regenerarse. Dicha regeneración está también a cargo de HuBOX.
    - Las claves de envoltura, RSA y AES, que cifrarán el fichero de claves del anterior punto. **Para proteger estas claves será necesario emplear cifrado de disco en los dispositivos que ejecuten los SDK**, como *BitLocker*.
27. Las claves y algoritmos utilizados son:
    - AES-256.
    - RSA con una longitud de clave de 8192 bits.
    - ECC/ECDSA con una longitud de clave de 256 bits.
    - SHA-256.

6.5 SINCRONIZACIÓN HORARIA

28. **Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados** para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.
29. El producto tomará la fecha y hora del sistema sobre el que se encuentre instalado, por lo que **se deberá asegurar la fiabilidad de la sincronización de dichos dispositivos**.

6.6 ACTUALIZACIONES

30. Las actualizaciones del producto se llevarán a cabo mediante la entrega de un nuevo par de SDKs por parte de HuBOX a la organización. Dicha entrega se realizará en los mismos términos indicados en el apartado 4.1 Entrega segura del producto.
31. Los SDK actualizados se entregarán con su documentación correspondiente.

6.7 ALTA DISPONIBILIDAD

32. El producto cuenta con la capacidad de soportar llamadas multi-hilo por lo que, para soluciones que consuman los SDK, se recomienda aprovechar al máximo la capacidad de procesamiento, de tal forma que se configuren las herramientas de generación y validación para el uso de un número de hilos adecuado a los que

permita el procesador del dispositivo sobre el cual se instale. Ver *Manual de usuario SDK Generación - REF2 y Manual de usuario SDK Validación – REF3*.

33. Adicionalmente, si desea lograrse un despliegue de alta disponibilidad, se deberá hacer uso de la duplicación de los recursos, adquiriendo y configurando dos SDKs adicionales.

6.8 AUDITORÍA

34. Cada transacción ejecutada por los SDK de generación y validación es registrada en ficheros tipo *log*. Cada fichero captura la siguiente información:
    - Fecha y hora de transacción.
    - Identificador "*Token*" mediante la cual se solicitó la transacción.
    - Resultado de la transacción (éxito/error con descripción).
35. El almacenamiento local de registros de auditoría se realiza de manera automática. En caso de alcanzar el límite en memoria se procede a la sobrescritura de los registros más antiguos, de tal forma que se mantenga el registro de las transacciones.
36. Debido a esto **se recomienda salvar periódicamente los registros de auditoría en una ubicación externa**, previniendo así la perdida en caso de llenarse el almacenamiento local.

6.9 MEDIDAS DE PROTECCIÓN IMPLEMENTADAS

37. Los SDK se encuentran protegidos de forma estática y dinámica (no configurable):
    - Ofuscación de instrucciones aritméticas, control de flujo, código nativo y nombres de bibliotecas, recursos y métodos de llamada del SDK.
    - Cifrado de clases, cadenas, *assets*, archivos de recursos y bibliotecas nativas.
    - Empaquetado del código con *bytecode* combinado.
    - Detección de herramientas de depuración, protección contra herramientas de desensamblado (*ILdasm*), generación de proxy dinámico (interno y externo), protección contra *reflection* y *tampering*.

6.10 *BACKUP*

38. El producto no dispone de ningún mecanismo de respaldo. Sin embargo, es posible copiar los ficheros correspondientes al SDK de generación o validación, así como las claves o licencias de funcionamiento y dependencias especificadas en los manuales de funcionamiento REF2 y REF3 (apartado "Configuración del proyecto"). Con la finalidad de poder recuperar el estado de la aplicación en caso de error y/o pérdida de información.

7. FASE DE OPERACIÓN

39. Una vez desplegada la solución, se deberán llevar a cabo las siguientes actividades:

- Comprobaciones periódicas del *software* para el aseguramiento de la integridad de los componentes del producto.
- Revisiones y limpiezas periódicas de los registros de auditoría. Estos deben estar protegidos de borrados y modificaciones no autorizadas y solamente el personal de seguridad autorizado podrá acceder a ellos.
- Aplicación regular de parches de seguridad, según sea necesario, con objeto de mantener el producto actualizado.
- Renovación/reactivación de licencias según sea necesario.

8. *CHECKLIST*

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Activación de las licencias	☐	☐	
CONFIGURACIÓN			
Establecimiento de una política de contraseñas (S.O.)	☐	☐	
Configuración de protocolos seguros (S.O.)	☐	☐	
Configuración de la sincronización de los sistemas	☐	☐	
Configuración del envío remoto de registros	☐	☐	
Planificación de las copias de seguridad	☐	☐	
OPERACIÓN			
Comprobación de la integridad	☐	☐	
Revisión y limpieza de registros	☐	☐	
Actualización periódica	☐	☐	
Renovación/Reactivación de licencias	☐	☐	

9. REFERENCIAS

40. Los manuales se entregan tras la obtención del producto.

REF1 Manual de Configuración de Ambiente

REF2 Manual de usuario SDK Generación

REF3 Manual de usuario SDK Validación

REF4 Instalación NeurotechnologyTrial

10.ABREVIATURAS

CLI	*Command Line Interface*
CRL	*Certificate Revocation List*
DNS	*Domain Name Servers*
ENS	Esquema Nacional de Seguridad.
IPSec	*Internet Protocol Security*
PKI	*Public Key Infrastructure*
SDK	*Software Development Kit*
SSH	*Secure Shell*
TLS	*Transport Layer Security*

PUBLICACIONES DE DEFENSA

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