Referencia: 2021-11-INF-3630- v1
Difusión: Limitada al expediente
Fecha: 04.03.2022

Creado por: CERT9
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente #	**2021-11**
TOE	**Personal Code, versión 2020.3.2**
Solicitante	**HUB130326868 - HuBOX**
Referencias	

[EXT-7135] 2021-09-03_2021-11_ETR_v1.1 Personal Code, version 2020.2

Informe de Certificación del producto Personal Code, versión 2020.3.2, según la solicitud de referencia [EXT-6585], de fecha 25/02/2021, evaluado por el laboratorio jtsec Beyond IT Security, S.L., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-7135], recibido el pasado 03/09/2021.

https://oc.ccn.cni.es
organismo.certificacion@cni.es

CONTENIDOS

RESUMEN 3
RESUMEN DEL TOE 3
ACTIVIDADES DE EVALUACIÓN 4
IDENTIFICACIÓN DEL TOE 5
HIPÓTESIS Y ENTORNO DE USO 5
ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS 5
FUNCIONES DE SEGURIDAD 5
PRUEBAS DEL PRODUCTO 6
CONFIGURACIÓN EVALUADA 6
RESULTADOS DE LA EVALUACIÓN 6
RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES 7
RECOMENDACIONES DEL CERTIFICADOR 7
VALIDEZ DEL CERTIFICADO 7
GLOSARIO DE TÉRMINOS 7
BIBLIOGRAFÍA 8
DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA) 8

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto Personal Code, versión 2020.3.2.

El TOE es una solución software cuya finalidad es la generación y validación de códigos QR que almacenan datos personales del usuario, permitiendo su identificación unívoca ante cualquier entidad.

Fabricante:	HuBOX.
Patrocinador:	HuBOX.
Organismo de Certificación:	Centro Criptológico Nacional (CCN).
Laboratorio de Evaluación:	jtsec Beyond IT Security, S.L..
Tipo de Evaluación:	LINCE
Taxonomía según CCN-STIC-140:	N/A.
Fecha de término de la evaluación:	02/09/2021.
Fecha de validez recomendada[1]:	05/03/2024

Todos los componentes de garantía requeridos por el tipo de evaluación LINCE presentan el veredicto de “PASA”. Por consiguiente, el laboratorio jtsec Beyond IT Security, S.L. asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador para LINCE, definidas por la norma Certificación Nacional Esencial de Seguridad, versión 0,1.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Personal Code, versión 2020.3.2, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El TOE es una solución software que permite la generación y validación de códigos QR que almacenan datos personales para permitir la identificación unívoca del usuario ante cualquier entidad. La funcionalidad del TOE la proporcionan dos elementos principales:

[1] Ver sección VALIDEZ DEL CERTIFICADO

- SDK de generación: inclusión en dos códigos QR de la información necesaria para permitir la identificación unívoca de un usuario frente a otra entidad. Las operaciones realizadas por este elemento son las siguientes:
  - Compresión.
  - Cifrado inicial.
  - Firma digital.
  - Cifrado por capas.
  - Reordenación de la información.
  - Generación de códigos QR.

- SDK de validación: comprobación de la validez de los códigos QR que se le presentan y extracción de la información almacenada en ellos. Las operaciones realizadas por este elemento son las siguientes:
  - Verificación de los códigos QR.
  - Reordenación de la información.
  - Descifrado por capas.
  - Verificación de la firma.
  - Descifrado.
  - Descompresión.

ACTIVIDADES DE EVALUACIÓN

El producto se evaluó con todas las evidencias necesarias para la satisfacción del tipo de evaluación LINCE según la norma Certificación Nacional Esencial de Seguridad, versión 0,1

Las actividades de evaluación realizadas en el transcurso de la evaluación han sido:

- ANÁLISIS DE LA DECLARACIÓN DE SEGURIDAD
- INSTALACIÓN DEL PRODUCTO
- ANÁLISIS DE CONFORMIDAD – ANÁLISIS DE LA DOCUMENTACIÓN
- ANÁLISIS DE CONFORMIDAD –PRUEBAS FUNCIONALES
- ANÁLISIS DE VULNERABILIDADES
- PRUEBAS DE PENETRACIÓN DEL TOE

IDENTIFICACIÓN DEL TOE

Objeto de evaluación (TOE): Personal Code, versión 2020.3.2..

Declaración de Seguridad: Personal Code - Declaración de Seguridad v1.3 (2 septiembre 2021).

HIPÓTESIS Y ENTORNO DE USO

Las hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la Declaración de Seguridad. Dichas hipótesis, se relacionan en el apartado 4.1 ("*Hipótesis sobre el entorno de ejecución*") de la Declaración de Seguridad [ST].

Estas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas. Por tanto, para garantizar el uso seguro del TOE, se parte de las hipótesis declaradas para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las siguientes amenazas no suponen un riesgo explotable para el producto Personal Code, versión 2020.3.2, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a moderado según lo definido en Certificación Nacional Esencial de Seguridad, versión 0,1, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Las amenazas cubiertas por las propiedades de seguridad del TOE se relacionan en el apartado 4.3 ("*Descripción de las amenazas*") de la Declaración de Seguridad [ST].

FUNCIONES DE SEGURIDAD

El TOE declara en el apartado 5 ("*Funciones de seguridad*") de la declaración de seguridad [ST] las funciones de seguridad que han sido verificadas por el CCN respecto a su cumplimiento con la Taxonomía de productos declarada con respecto de la guía CCN-STIC-140 y han sido evaluadas por el laboratorio para verificar su efectividad en el entorno operacional definido.

GUÍAS DE OPERACIÓN E INSTALACIÓN DEL TOE

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada:

- Manual de configuración de ambiente (versión 2.1).
- Manual de usuario SDK Generación (versión 2.0).
- Manual de usuario SDK Validación (versión 2.1).
- Instalación Neurotechnology Trial (versión 2.1).

PRUEBAS DEL PRODUCTO

Para verificar la funcionalidad de seguridad declarada, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados, así obtenidos, son consistentes con lo declarado en la Declaración de Seguridad [ST].

Adicionalmente, el laboratorio ha realizado un análisis de vulnerabilidades teniendo en cuenta las funcionalidades de seguridad declaradas en la [ST] y el nivel de resistencia a atacantes con potencial de ataque moderado tal y como se define en [CCN-LINCE-002]. Teniendo en cuenta las potenciales vulnerabilidades extraídas de dicho análisis, el laboratorio evaluador ha realizado pruebas de penetración para verificar la explotabilidad de las mismas en el entorno de operación declarado en [ST].

Todas las pruebas se han realizado sobre un mismo escenario de pruebas, acorde al entorno de operación, identificado en la Declaración de Seguridad [ST].

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no supone una merma en la capacidad funcional del producto conforme a lo declarado en su Declaración de Seguridad [ST].

CONFIGURACIÓN EVALUADA

Para el funcionamiento del producto conforme a la evaluación evaluada del TOE Personal Code, versión 2020.3.2 es necesario disponer de los componentes software que se indican en la sección 1.1 (“*Información del patrocinador, TOE y evaluación*”) de la declaración de seguridad [ST].

- Personal Code versión 2020.3.2

RESULTADOS DE LA EVALUACIÓN

El producto Personal Code, versión 2020.3.2 ha sido evaluado en base a la Declaración de Seguridad Personal Code - Declaración de Seguridad v1.3 (2 septiembre 2021).

Todas las actividades de evaluación requeridas por el tipo de evaluación LINCE presentan el veredicto de "PASA". Por consiguiente, el laboratorio jtsec Beyond IT Security, S.L. asigna el **VEREDICTO de "PASA"** a toda la evaluación por satisfacer todas las acciones del evaluador, definidas por la norma LINCE para el tipo de evaluación Certificación Nacional Esencial de Seguridad, versión 0,1

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

A continuación, se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

El evaluador no ha incluido en su informe ninguna recomendación o comentario para los usuarios.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Personal Code, versión 2020.3.2, se propone la resolución estimatoria de la misma.

VALIDEZ DEL CERTIFICADO

Un certificado LINCE se emite indicando la versión específica del producto que fue evaluada. Si este producto evoluciona, sus nuevas versiones no serán certificadas por defecto. El proceso de "*Assurance Continuity*" o continuidad de la garantía [AC] se usa para facilitar el mantenimiento del certificado en versiones nuevas del producto. Este proceso es aplicable a la certificación LINCE.

Se recomienda revisar la validez del certificado a los veinticuatro meses desde su emisión. En todo momento el desarrollador podrá optar al proceso de renovación del certificado o re-certificación del mismo, según lo establecido en el procedimiento de certificación PO-005.

GLOSARIO DE TÉRMINOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAFÍA

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CCN-LINCE-001] Guía CCN-STIC-2001 - Definición de la Certificación Nacional Esencial de Seguridad (LINCE), versión 0.1. Enero 2020. Centro Criptológico Nacional.

[CCN-LINCE-002] Guía CCN-STIC-2002 - Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), versión 0.1. Enero 2020. Centro Criptológico Nacional.

[CCN-LINCE-003] Guía CCN-STIC-2003 - Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), versión 0.1. Enero 2020. Centro Criptológico Nacional.

[CCN-LINCE-004] Guía CCN-STIC-2004 - Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), versión 0.1. Enero 2020. Centro Criptológico Nacional.

[ST] Personal Code - Declaración de Seguridad v1.3 (2 septiembre 2021)

DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA)

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación:

Personal Code - Declaración de Seguridad v1.3 (2 septiembre 2021).