REF: 2005-8-INF-164 v2
Difusión: Expediente
Fecha: 05.09.2007

Creado: CERT3
Revisado: TECNICO
Aprobado: JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2005-8 CRYPTO TOKEN USB
Datos del solicitante: B80860521 DATATECH Sistemas Digitales Avanzados

Referencias:
- [EXT112] Solicitud de Certificación del Crypto Token USB
- [EXT357] Informe Técnico de Evaluación del Crypto Token USB
- [CC] Common Criteria for Information Technology Security Evaluation, v2.3
- [CEM] Common Evaluation Methodology for Information Technology Security, v2.3.

Informe de certificación del producto Crypto Token USB, versión TK01S1.47, según la solicitud de referencia [EXT-112], de fecha 19 de diciembre de 2005, y evaluado por el laboratorio INTA-CESTI, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-357], de acuerdo a [CC] y a [CEM].

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

ÍNDICE

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

RESUMEN

Este documento constituye el Informe de Certificación del producto Crypto Token USB, versión TK01S1.47.

Producto: Crypto Token USB, versión TK01S1.47.

Fabricante: DATATECH Sistemas Digitales Avanzados.

Patrocinador: DATATECH Sistemas Digitales Avanzados.

Declaración de Seguridad: Declaración de Seguridad del Crypto Token USB, versión 3.1, de 17 de mayo de 2007.

Perfil de Protección: Ninguno.

Nivel de Evaluación: EAL3.

Fortaleza de las Funciones: Baja.

Organismo de Certificación: CENTRO CRIPTOLÓGICO NACIONAL (CCN).

Laboratorio de Evaluación: Centro de Evaluación de la Seguridad de las TI (CESTI), del Instituto Nacional de Técnica Aeroespacial "Esteban Terradas" (INTA).

Informe Técnico de Evaluación: DTU/TRE/2042/001/INTA/07, Ed. 1.0 de 5 de junio de 2007.

Fecha de inicio de la evaluación: 06-06-2006.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL3, con fortaleza de las funciones BAJA, presentan el veredicto de PASA. Por consiguiente, el laboratorio INTA-CESTI asigna el VEREDICTO de PASA a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL3, definidas en la Parte 3 de los Criterios Comunes [CC] y en la Metodología de Evaluación [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Crypto Token USB, versión TK01S1.47, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

El Objeto a Evaluar (OE) es un dispositivo portátil USB, que permite el cifrado off-line de datos provenientes del ordenador al que se conecta. Es un dispositivo hardware con firmware embebido. El OE puede ser utilizado por cualquier host USB que implemente el protocolo a nivel de aplicación de los comandos del OE. Para facilitar su uso, el OE se entrega al usuario con una aplicación y drivers para la plataforma Windows, que está fuera del OE.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

El OE tiene, además de cifrar y descifrar, la capacidad de almacenar datos, en forma de ficheros cifrados, en una memoria interna no volátil. Las capacidades de cifrado del OE se basan en el algoritmo AES, con claves de 256 bits, que se importan y exportan desde el OE, permitiendo el intercambio de ficheros cifrados entre varios OEs.

Por último, y para las dos funciones anteriores, el OE es capaz de almacenar de manera segura las distintas claves que utiliza en cada proceso, y de garantizar la confidencialidad del firmware interno que realiza todas estas funciones.

El Crypto Token USB está diseñado para su uso en organismos o empresas con administración de los soportes de almacenamiento externo, y cuenta con capacidades para la configuración y gestión del OE por parte de un Administrador, distintas de las operaciones básicas de cifrado y soporte de almacenamiento USB que presta a los usuarios.

El OE permite su identificación única mediante un identificador de CPU, lo que resulta de utilidad en la gestión de múltiples Crypto Token USB. Igualmente, la carga de aplicaciones en el Crypto Token USB se realiza a partir de una autenticación basada en una clave de cerrado.

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de garantía de evaluación EAL3.

CLASE DE REQUISITOS	COMPONENTES
Gestión de configuración	ACM_CAP.3, ACM_SCP.1
Distribución y operación	ADO_DEL.1, ADO_IGS.1
Desarrollo	ADV_FSP.1, ADV_HLD.2, ADV_RCR.1
Manuales	AGD_ADM.1, AGD_USR.1
Ciclo de vida	ALC_DVS.1
Pruebas	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
Análisis vulnerabilidades	AVA_MSU.1, AVA_SOF.1, AVA_VLA.1

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

REQUISITOS FUNCIONALES DE SEGURIDAD

Los requisitos funcionales que satisface el producto son los siguientes:

- Control total de acceso (FDP_ACC.2).
- Control de acceso basado en atributos de seguridad (FDP_ACF.1).
- Destrucción de claves criptográficas (FCS_CKM.4).
- Funcionamiento criptográfico (FCS_COP.1).
- Secuencia de autenticación (FIA_UAU.1).
- Secuencia de identificación (FIA_UID.1).
- Gestión de fallos de autenticación (FIA_AFL.1).
- Gestión de los atributos de seguridad (FMT_MSA.1).
- Inicialización de atributos (FMT_MSA.3).
- Roles de seguridad (FMT_SMR.1).
- Especificación de funciones administrativas (FMT_SMF.1).
- Detección pasiva de ataque físico (FPT_PHP.1).
- Importación de datos de usuario sin atributos de seguridad (FDP_ITC.1).
- Exportación de datos de usuario sin atributos de seguridad (FDP_ETC.1).

POLÍTICAS DE SEGURIDAD

Para garantizar el funcionamiento seguro del Crypto Token USB, se han definido dos políticas de seguridad cuyo cumplimiento completa las características de seguridad del producto. Estas políticas hacen referencia a la capacidad del OE para detectar ataques físicos y a los roles de los distintos tipos de usuario:

- **P.Tamper.**

  El OE no se diseñará con capacidad de reacción y protección de sus activos ante escenarios de ataque físico. Sin embargo, se incluirán los mecanismos físicos necesarios que permitan detectar este tipo de ataques.

- **P.Roles.**

  El OE soportará los siguientes roles: Super-administrador, Administrador y Usuario.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

P.Admin.

El *Super-administrador* podrá realizar las siguientes operaciones: cargar y actualizar el firmware (sw, boot y aplicación) del OE.

El *Administrador* del OE podrá realizar las siguientes operaciones: asignar y cambiar las claves de autenticación PIN y PUK propios y del usuario; asignar, cambiar, borrar, importar y exportar claves de cifrado y de almacenamiento de ficheros.

- **P.Usuarioc.**

  El usuario del OE podrá realizar las siguientes operaciones en las que intervienen las claves y los mecanismos criptográficos: asignar y cambiar sus claves de autenticación PIN y PUK; asignar, cambiar, borrar, importar y exportar claves de cifrado y de almacenamiento de ficheros; cifrar y descrifrar ficheros, tanto con claves predefinidas como con claves suministradas para cada operación; realizar un reset del OE.

- **P.UsuariosF.**

  El usuario del OE podrá utilizar la memoria no volátil del OE como un sistema de ficheros, con los siguientes servicios: lectura, escritura y borrado de ficheros y directorios; formateo del sistema de ficheros; obtención del almacenamiento disponible; asignación de la fecha y hora de un fichero o directorio.

HIPÓTESIS

Las siguientes hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la declaración de seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas.

HIPÓTESIS DE USO

- **A.Pcuso – Plataforma de uso.**

  El ordenador donde se utiliza el OE es fiable y no contiene, ni es manejado por elementos hostiles de interceptación de activos de cifrado o de autenticación.

HIPÓTESIS RELATIVAS AL ENTORNO

Los mecanismos y garantías de seguridad del OE son válidos para ataques directos sobre el interfaz de comunicaciones del dispositivo, sin relación con el ordenador donde se utiliza, o con datos extraídos del mismo. Tal escenario, por ejemplo, se dará cuando se sustrae un OE a su usuario legítimo.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

FUNCIONALIDAD DEL ENTORNO

El entorno del OE está formado únicamente por el ordenador donde se utiliza y, en el ámbito de esta evaluación, lo único a considerar del mismo es lo establecido en las Hipótesis.

ARQUITECTURA

El interfaz del OE es de tipo USB, tanto en su aspecto físico como en lo relativo a las comunicaciones a nivel de enlace.

A nivel de aplicación, el OE define su propio interfaz, que define sus capacidades y sobre el que se esperan los ataques a los activos del "Crypto Token USB". El interfaz de aplicación se define mediante los correspondientes comandos, que se agrupan según las funciones de seguridad del OE. Estas funciones de seguridad del OE son:

- F1. Función de gestión de claves y usuarios.
- F2. Función de autenticación de usuarios.
- F3. Función de control de acceso.
- F5. Función de protección física.
- F6. Función de cifrado.

CONFIGURACIÓN EVALUADA

La configuración evaluada del producto es la que se especifica a continuación.

- Producto: Crypto Token USB, versión TK01S1.47.
- Declaración de Seguridad: Declaración de Seguridad del Crypto Token USB, versión 3.1, de 17 de mayo de 2007.

Los detalles de configuración, en cuanto a componentes del producto se pueden consultar en la documentación entregada durante el proceso de evaluación.

PRUEBAS DEL PRODUCTO

Tanto el desarrollador como el laboratorio de evaluación han diseñado y realizado pruebas para confirmar el correcto funcionamiento del producto.

Se ha revisado la documentación de pruebas del desarrollador para valorar su esfuerzo en la realización de pruebas sobre el OE.

La estrategia de pruebas usada por el desarrollador se resume de la siguiente forma:

- Cantidad de pruebas del desarrollador. Se han probado todas las funciones de seguridad excepto la funcion F5 de protección física del OE, cuyo único

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

interfaz es la envolvente plástica del CryptoToken USB. Sin embargo, esto no se considera incorrecto pues las pruebas de detección pasiva de ataques a la envolvente plásica del OE son elementales. Para cada función, se han probado todos los aspectos posibles. Los tests realizados sobre el OE tratan de demostrar que se cumplen los comportamientos asociados a cada función de seguridad. También se han probado todos los subsistemas que soportan las TSF, excepto el subsistema S6 "Protección física". Sin embargo, esto no se considera incorrecto pues las pruebas de detección pasiva de ataques a la carcasa y el poliuretano interior son elementales.

- Enfoque de pruebas. Se han abordado desde el análisis de los requisitos que deben cumplir las Funciones de Seguridad en correspondencia con las acciones que se pueden realizar con el OE y que prueban dichos requisitos. De este modo, las Funciones de Seguridad quedan probadas demostrando el funcionamiento de las acciones relacionadas con cada una de ellas.
- Configuración de pruebas del OE. Para cada una de las pruebas se define el entorno que debería presentar el OE como paso previo a la realización de la prueba. La prueba se compone, además, de una o más acciones a desarrollar. Por último, se especifica el resultado esperado para cada prueba.
- Resultados de las pruebas. La documentación de pruebas suministra las evidencias de las pruebas realizadas. Todas las pruebas tienen un veredicto PASA. Las pruebas del desarrollador demuestran que las funciones de seguridad se comportan tal y como se especifica.

Por tanto, se concluye que el desarrollador ha realizado un gran esfuerzo para definir y ejecutar las pruebas.

Por otro lado, la realización de pruebas sobre el OE, por parte del equipo evaluador, es un mecanismo de ayuda para determinar si se cumplen los requisitos funcionales establecidos para el OE. La realización de pruebas garantiza que el OE satisface, al menos, sus requisitos de seguridad, aunque no permite determinar si dicho OE no hace más de lo especificado.

El conjunto de pruebas puede incluir tanto pruebas "positivas", para comprobar el cumplimiento de los requisitos, como pruebas "negativas", para verificar la ausencia de comportamientos no deseados.

En el conjunto de pruebas no se incluyen pruebas de penetración encaminadas directamente a la búsqueda de vulnerabilidades que permitan violar la política de seguridad. Este conjunto de pruebas se llevan a cabo en el análisis de vulnerabilidades (clase AVA).

El objetivo de este conjunto de pruebas es determinar si las funciones de seguridad se realizan tal y como se ha especificado.

Para alcanzar este objetivo, el equipo evaluador elabora su propia documentación de pruebas en la que se describe la estrategia de pruebas a seguir. El diseño de estas pruebas se ha llevado a cabo con la finalidad de obtener confianza en la correcta operación del OE a través de la ejecución de un conjunto

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

de pruebas representativo, más que con la finalidad de llevar a cabo todas las posibles pruebas.

Para generar la documentación de las pruebas para el subconjunto de pruebas independientes realizadas por el evaluador se ha seguido el método de probar las funciones de seguridad a través de los subsistemas que procesan las señales de los interfaces.

El resultado de las pruebas independientes del evaluador confirma que la funcionalidad del OE es tal y como se describe en la documentación aportada por el desarrollador, siendo el comportamiento de las funciones de seguridad del OE el especificado.

Los resultados obtenidos por el equipo evaluador, al repetir las pruebas del fabricante, coinciden con resultados proporcionados por el propio fabricante.

RESULTADOS DE LA EVALUACIÓN

El equipo de evaluación ha completado todas las unidades de trabajo en las que se descompone cada subactividad y ha verificado, de manera justificada, si se satisface o no cada una de ellas.

En función de la satisfación o no de las unidades de trabajo, se asigna un veredicto de PASA/NO PASA. Este veredicto se escala para asignar, en última instancia, un veredicto a cada actividad.

De acuerdo a la evaluación llevada a cabo por el **CESTI**, se concluye que:

- Todas las actividades tienen asignado un veredicto PASA . Por lo tanto, el evaluador ha asignado un veredicto PASA a la evaluación del producto Token USB DATATECH TK01S1.47.
- El OE Token USB DATATECH TK01S1.47 satisface su Declaración de Seguridad, Declaración de Seguridad Crypto Token USB v3.1 , conforme a [CC], EAL 3 , SOF Baja.

Los resultados de la evaluación, recogidos en este informe, son válidos sólo para la configuración evaluada del producto. El OE ha sido probado con esta configuración, por lo que todos los resultados de la evaluación son válidos únicamente para esta versión del OE:

Producto: Token USB DATATECH TK01S1.47.

Declaración de Seguridad: Declaración de Seguridad Crypto Token USB v3.1.

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

Se describen a continuación características que, a juicio del equipo evaluador, hay que considerar para un uso seguro del OE:

- Debe tenerse en cuenta el cumplimiento de las suposiciones de seguridad del entorno. Estas suposiciones se encuentran recogidas en Declaración de

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Seguridad Crypto Token USB v3.1 sección 3.1 'Entorno de Seguridad del OE: Hipótesis'.

- Debe tenerse en cuenta el cumplimiento de los objetivos de seguridad del entorno. Estos objetivos se encuentran recogidos en Declaración de Seguridad Crypto Token USB v3.1 sección 4.2 'Objetivos de Seguridad del Entorno'.

Por otro lado, es necesario subrayar que cualquier modificación sobre la configuración evaluada (producto, declaración de seguridad), realizada por el desarrollador, queda fuera del alcance de esta evaluación. Los resultados de la evaluación de la nueva configuración pueden ser diferentes a los presentes. Cualquier modificación sobre la configuración evaluada debe ser comunicada a la autoridad de certificación.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Crypto Token USB, versión TK01S1.47, se propone la resolución estimatoria de la misma.

GLOSARIO DE TÉRMINOS

CESTI	Centro de Evaluación de la Seguridad de las Tecnologías de la Información
EAL	Evaluation assurance level
INTA	Instituto Nacional de Técnica Aeroespacial "Esteban Terradas".
OE	Objeto de Evaluación

BIBLIOGRAFÍA

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

[CCP1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 2.3, August 2005.

[CCP2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.3, August 2005.

[CCP3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.3, August 2005.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 2.3, August 2005.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

DECLARACIÓN DE SEGURIDAD

Conjuntamente con este informe de certificación, se dispone en el Organismo de Certificación de la declaración de seguridad completa de la evaluación: "Declaración de Seguridad del Crypto Token USB, versión 3.1" de 17 de mayo de 2007.

La versión ***pública*** que se hace disponible por medio de la página web del OC http://www.oc.ccn.cni.es, es la **"Declaración de Seguridad del Crypto Token USB, versión 3.2", de 20 de julio de 2007**. Esta declaración de seguridad corresponde a la versión completa de la evaluación, pero sin la información de diseño interno sensible para el fabricante, y sin perjuicio de permitir conocer las propiedades de seguridad del TOE o del alcance de la evaluación efectuada.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es