REF:	2004-1-INF-25 v1	Creado:	CERT3
Difusión:	Pública	Revisado:	RTECNICO
Fecha:	11 de marzo de 2005	Aprobado:	JEFEAREA

INFORME DE CERTIFICACION

Expediente: 2004-1
Datos del solicitante: A61930046 SAFELAYER SECURE COMMUNICATIONS

Referencias: Declaración de Seguridad – OC53A113 V2.0
Informe Técnico de Evaluación – KEY/TRE/2042/001/INTA/04

Informe de certificación del producto KEY ONE , versión 2.1 04S1R2, solicitada el nueve de julio de dos mil cuatro, y evaluado por el laboratorio CESTI /INTA, conforme se detalla en el correspondiente informe de evaluación, emitido el pasado veinte de diciembre de 2004.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

ÍNDICE

Nivel de evaluación y garantía de seguridad 3
Descripción del producto 3
KeyOne CA: Autoridad de Certificación. 3
KeyOne LRA: Autoridad de Registro Local. 4
KeyOne VA: Servicio de Gestión de Certificados Revocados. 4
KeyOne TSA Server: Autoridad de Sellado de Tiempo. 4
Plataforma y configuración del producto evaluado. 5
Entorno de uso del producto 6
Hipótesis de uso 6
H1. Seguridad física y del entorno. 6
H2. Sistema de gestión de la seguridad de la información. 6
H3. Instalación y mantenimiento. 6
H4. Gestión de incidentes y de la continuidad del negocio. 6
H5. Cumplimiento de las obligaciones legales. 6
H6. Prácticas y políticas de certificación. 6
H7. Competencia del personal. 6
H8. Programa de concienciación y formación. 6
H9. Fuente fiable de tiempo. 6
H10. Módulo criptográfico. 7
H11. Dispositivo seguro de creación de firma. 7
H12. Mecanismos de control de acceso. 7
Políticas organizativas 8
Amenazas 9
Amenazas 9
T1. Violación de las políticas y prácticas de certificación del producto. 9
T2. Abuso de código. 9
T3. Ataques externos. 9
Producto y su documentación. 10
Pruebas del producto 11
Pruebas realizadas por el fabricante 11
Pruebas realizadas por el laboratorio 11
Resultados de la Evaluación 12
Recomendaciones del certificador 12
Glosario de términos 13
Bibliografía 13
Declaración de seguridad 14

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

Nivel de evaluación y garantía de seguridad

La declaración de seguridad garantiza la funcionalidad de seguridad del producto según el nivel de evaluación EAL2. Este nivel de evaluación proporciona, a través de la evaluación, una garantía baja o moderada de la seguridad del producto.

Las funciones de seguridad son analizadas a partir de su especificación funcional, los manuales de administración y el diseño de alto nivel del producto, lo que permite una comprensión de su comportamiento en términos de seguridad.

Este análisis se complementa con pruebas independientes por parte del laboratorio de parte de las funciones de seguridad del producto, así como por la revisión de las pruebas del fabricante, que están basadas en la especificación funcional, la confirmación selectiva de los resultados de estas pruebas del fabricante, el análisis de la fortaleza de las funciones y de las vulnerabilidades del producto, a partir del análisis realizado por el propio fabricante. Por último, se obtienen garantías adicionales de la integridad del código fuente y del producto a partir de la exigencia y revisión de prácticas de gestión de la configuración de los mismos, y de procedimientos seguros de distribución.

La fortaleza de los mecanismos de seguridad se declara “básica”, lo que supone que el producto es resistente ante agentes con poca capacidad de ataque, siendo vulnerable ante agentes con mayores capacidades. La resistencia declarada, además, se garantiza únicamente en las condiciones de entorno de uso definidas en la propia declaración de seguridad y resumidas más adelante.

Descripción del producto

El producto Keyone 2.1 04S1R2 es un producto software que implementa una infraestructura de clave pública (PKI), proporcionando los siguientes servicios:

- **Servicios de Registro**: Verifica la identidad y los atributos del solicitante de certificado. Los resultados de este servicio se pasan al servicio de generación de certificado.
- **Servicios de Generación de Certificado**: Crea y firma los certificados entregados por la autoridad de registro.
- **Servicio de Gestión de Revocación de Certificado**: Si la clave privada de un usuario pudiera estar comprometida, este servicio gestiona la petición para una suspensión. También gestiona las peticiones de revocación cuando el suscriptor considera que su clave ya no es segura.
- **Servicio de Estado de Revocación de Certificado**: Aporta información sobre el estado de revocación de un certificado a la parte confiable. Esta información se actualiza periódicamente.

Proporciona igualmente los siguientes servicios adicionales:

- **Servicios de Provisión de Dispositivos**: Proporciona un dispositivo de creación de firma a los usuarios.
- **Servicios de Sellado de Tiempo**: Proporciona la capacidad para generar sellos de tiempo para la validación temporal de los datos.

La arquitectura del sistema está compuesta de los siguientes elementos:

KeyOne CA: Autoridad de Certificación.

El objetivo principal del KeyOne CA es la generación de certificados a partir de las peticiones solicitadas a través de la Autoridad de Registro. KeyOne CA genera, además, las listas de revocación.

La Autoridad de Certificación procesa lotes de entrada enviados por la Autoridad de Registro y gen-era lotes de salida con los certificados o las listas de revocación. Incluye un repositorio donde almacena los certificados y listas de revocación y ofrece servicios de recuperación de claves de cifrado y autenticación.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

KeyOne LRA: Autoridad de Registro Local.

KeyOne LRA proporciona los servicios básicos para el registro de usuarios y para la solicitud de los certificados a la autoridad de certificación. Una vez recibido el certificado, lo almacena en una tarjeta inteligente. También es la autoridad encargada de enviar las peticiones de revocación de certificado a la Autoridad de Certificación.

KeyOne VA: Servicio de Gestión de Certificados Revocados.

KeyOne VA permite la consulta del estado de revocación de los certificados.

El usuario solicita a través de una petición OCSP el estado de revocación de un certificado. KeyOne VA realiza una consulta en su base de datos interna, donde se encuentra actualizada la lista de certificados revocados, y devuelve al usuario un mensaje utilizando el protocolo OCSP. El mensaje devuelto se encuentra firmado y constituye una garantía de la validez del certificado.

KeyOne TSA Server: Autoridad de Sellado de Tiempo.

KeyOne TSA Server implementa una autoridad de sellado de tiempo, creando tokens de sellado con la fecha y hora para indicar que unos determinados datos son válidos en la fecha indicada.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

Plataforma y configuración del producto evaluado.

El producto requiere de los siguientes componentes para su correcta operación, y que han sido utilizados en la plataforma de evaluación:

- Ordenadores de tipo PC, compatibles y soportados por el sistema operativo indicado a continuación.
- Sistema operativo Windows 2000
- Gestor de base de datos Oracle 9i
- Módulo criptográfico nCipher nShield Ultrasign 1.82.7
- Tarjeta inteligente GPK 16000
- Reloj de precisión NTP8
- Otros componentes, como
    - Microsoft Internet Explorer v 6.0
    - LDAP Netscape 4.0
    - Lector de tarjeta inteligente GemplusPC410

La relación de componentes y de subsistemas del producto se sintetiza en la tabla siguiente:

Subsistema	**SO**	**BBDD**	**HSM**	**SCDSSCD**	**CLOCK**	**Others**
KeyOne CA	Microsoft Windows 2000	Oracle 9i	nChiper nShield Ultrasign 1.82.7		TimeFrequency Solutions Modelo:NTP8. Firmware version: 0123NTP v11.00	Microsoft Internet Explorer 6.0. LDAP Netscape 4.0
KeyOne LRA	Microsoft Windows 2000			GPK 16000		Microsoft Internet Explorer 6.0. GemPlus GemPC410 Reader
KeyOne VA	Microsoft Windows 2000	Oracle 9i	nChiper nShield Ultrasign 1.82.7		TimeFrequency Solutions Modelo:NTP8. Firmware version: 0123NTP v11.00	Microsoft Internet Explorer 6.0
KeyOne TSA	Microsoft Windows 2000	Oracle 9i	nChiper nShield Ultrasign 1.82.7		TimeFrequency Solutions Modelo:NTP8. Firmware version: 0123NTP v11.00	Microsoft Internet Explorer 6.0

Estos productos no forman parte del objeto a evaluar, ni del alcance de la certificación del KeyOne 2.1 04S1R2. La configuración y uso de los mismos debe ser tal que se cumplan las restricciones e hipótesis definidas en la declaración como entorno de uso del producto, y que se resumen a continuación.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

Entorno de uso del producto

Hipótesis de uso

Las siguientes hipótesis de uso restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la declaración de seguridad, y resumidas a continuación. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de si las vulnerabilidades identificadas son explotables.

H1. Seguridad física y del entorno.

Que deberá garantizar que se controla el acceso a los activos relacionados con la generación de certificados, el suministro de tarjetas inteligentes o los servicios de gestión de revocación de certificados.

H2. Sistema de gestión de la seguridad de la información.

Que deberá estar definido y en práctica, de manera que identifique todas las amenazas relevantes y potenciales relacionadas con los servicios de la infraestructura de clave pública, así como las salvaguardas necesarias para eliminar o reducir dichas amenazas.

H3. Instalación y mantenimiento.

Se deberá realizar un análisis de requisitos de seguridad en la fase de especificación y diseño de todo proyecto de desarrollo complementario al despliegue del producto KeyOne, de manera que se garantice el mantenimiento de su seguridad. En particular, deberán establecerse medidas de gestión de cambios, y de instalación de parches para todo el software operacional.

H4. Gestión de incidentes y de la continuidad del negocio.

Que deberá establecerse de manera que se garantice que, en el caso de ocurrencia de desastres, fundamentalmente el compromiso de las claves privadas de firma de la infraestructura, se puede recuperar el servicio en el menor plazo posible.

H5. Cumplimiento de las obligaciones legales.

La instalación y uso del producto KeyOne 2.1 deberá realizarse de tal manera que se garantice el cumplimiento de las obligaciones legales que sean de aplicación, y en particular, las relativas a la protección de datos de carácter personal.

H6. Prácticas y políticas de certificación.

Las prácticas y las políticas de certificación bajo las cuales se opera el producto KeyOne 2.1 deben cumplir con las restricciones normativas indicadas en la declaración de seguridad y en la documentación de uso.

H7. Competencia del personal.

El personal afecto a la operación y administración del producto debe ser competente y fiable, sin que se considere el uso de personal deshonesto.

H8. Programa de concienciación y formación.

Que deberá establecerse, aplicarse y mantenerse, garantizando que todo el personal afecto al uso del producto KeyOne 2.1 tiene conocimientos apropiados para realizar sus funciones.

H9. Fuente fiable de tiempo.

Que deberá utilizarse como origen de tiempos para los registros y sellados de tiempo emitidos por el producto KeyOne 2.1.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

H10. Módulo criptográfico.

Que se utilizará para el almacenamiento seguro de los secretos de las claves utilizadas por el producto KeyOne, de manera que se garantice la imposibilidad de su modificación, destrucción o conocimiento no autorizado.

H11. Dispositivo seguro de creación de firma.

La inicialización, creación de la estructura de ficheros se realizará por el vendedor del dispositivo seguro de creación de firma, de manera que se garantice su consideración como tal.

H12. Mecanismos de control de acceso.

Se utilizarán los mecanismos de control de acceso del sistema oerativo para restringir el acceso no autorizado a los recursos críticos (memoria, discos) de la plataforma sobre la que se ejecuta el producto KeyOne 2.1.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

Políticas organizativas

El uso del producto KeyOne 2.1. como software de infraestructura de clave pública debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

Se distinguen las políticas organizativas aplicables al uso del producto en su conjunto de las aplicables a los diferentes servicios o funcionalidades que presta. El detalle de las mismas se encuentra en la declaración de seguridad. En síntesis, se establece la necesidad de implementar políticas organizativas relativas a:

Código	Política organizativa
P.SO.	Operaciones y sistemas
P.IA	Identificación y autenticación
P.KM	Gestión de claves
P.AA	Auditoría y contabilidad
P.AR	Archivo
P.BK	Salvaguarda y recuperación
P.SM	Seguridad de los mensajes
P.RS	Relativas al servicio de registro
P.CGS	Relativas al servicio de generación de certificados
P.CRMS	Relativas al servicio de gestión de revocación de certificados
P.CRRS	Relativas al servicio de validación de certificados
P.TSS	Relativas al servicio de sellado de tiempo

.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

Amenazas

Las siguientes amenazas no suponen un riesgo explotable para el producto KeyOne 2.1, siempre que los agentes que realicen ataques tengan poca capacidad, y que se cumplan las hipótesis de uso e implementen las políticas de seguridad.

T1. Violación de las políticas y prácticas de certificación del producto.

Los usuarios de KeyOne 2.1 podrían no realizar algunas funciones esenciales a la seguridad del producto, modificando sus datos de seguridad de manera que no es consistente con las políticas y prácticas de certificación, causando la modificación o el conocimiento no autorizado de las claves privadas de la infraestructura.

T2. Abuso de código.

Los usuarios de KeyOne 2.1 podrían explotar vulnerabilidades del producto, no identificadas con anterioridas, y creadas en su desarrollo.

T3. Ataques externos.

Un agente hostil podría acceder al sistema utilizando ingeniería social o suplantando a un usuario autorizado para realizar operaciones con el producto KeyOne 2.1 que serían imputadas a un usuario o proceso legítimo.

Un agente hostil podría modificar información interceptada de manera inadvertida en un canal de comunicación, lanzando ataques de denegación de servicio.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

Producto y su documentación.

El producto está formado por el software y los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión certificada.

Título del documento	Código	Versión
Security Target KeyOne 2.1	0C53A113	v. 1.54
CD Producto Keyone 2.1, 04S1R2 Sistema Operativo Windows	O4S1R2	O4S1R2
Configuration Guide CC EAL 2 Certification	0F92B8A5	v. 1.8
KeyOne 2.1 -Script Signing	DB4586F8	v.13
KeyOne CA 2.1 -Installation	A2362E54	v. 1.3
KeyOne CA 2.1 -Start-up and maintenance	9A08B9AA	v. 1.3
Manual de puesta en marcha y mantenimiento de KeyOne CA	E04DC2FD	v. 1.3
KeyOne CA online server 2.1 Installation	74CBAD1C	v. 1.3
Manual de instalación de KeyOne CA Online	B37DFA60	v. 1.3
KeyOne CertStatus Server 2.1 -Start-up Manual	F8690A83	v. 1.3
Manual de puesta en marcha de KeyOne CertStatus Server	FFD5B9EE	v.1.3
KeyOne LRA 2.1 -Installation and Start-Up	8B9C0115	v.1.3
Manual de instalación y puesta en marcha de KeyOne LRA	4566017C	v.1.3
KeyOne VA 2.1 Manual	D967013A	v.1.3
Manual de KeyOne VA	28446A95	v.1.3
KeyOne 2.1 - PSS Manager	BC34FCB0	v.1.3
PSS Manager	01D88E2B	v.1.3
KeyOne TSA Server 2.1 Manual	234BC855	v.1.3

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

Pruebas del producto

Pruebas realizadas por el fabricante

El fabricante ha realizado pruebas para todas las funciones de seguridad, excepto para las funciones de seguridad FXT_XSP2.1 y FXT_XSP3.2. Los requisitos de garantía en los Criterios Comunes a nivel EAL2 no exigen una cobertura completa de las funciones de seguridad.

La evaluación ha verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea cubrir.

Todas las pruebas se han realizado sobre un mismo escenario de pruebas acorde a la arquitectura identificada en la declaración de seguridad.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados. Todos las pruebas ha sido realizados por el desarrollador en sus instalaciones con resultado satisfactorio.

Pruebas realizadas por el laboratorio

Para verificar los resultados de los las pruebas del fabricante, el laboratorio ha repetido en las instalaciones del fabricante todas estas pruebas funcionales. Igualmente, ha escogido y repetido un 25 % de las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación, seleccionando una prueba por cada una de las clases funcionales más relevantes: funciones de generación de auditoría, funciones criptográficas y funciones de protección de los datos de usuario.

Adicionalmente, 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 los resultados obtenidos por el desarrollador.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

Resultados de la Evaluación

El producto Keyone 2.1 04S1R2 sobre sistema operativo Microsoft Windows ha sido evaluado frente a la declaración de seguridad “Security Target Keyone 2.1”, de código 0C53A113 y versión 1.54.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2 presentan el veredicto de pasa. Por consiguiente, el laboratorio CESTI /INTA asigna al VEREDICTO de PASA a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL 2, definidas en la parte tercera de los Criterios Comunes.

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto KEY ONE, versión 2.1 04S1R2 sobre sistema operativo Microsoft Windows, se propone la resolución estimatoria de la misma.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

Glossario de términos

EAL – Evaluation assurance level

LDAP -- Lightweight Directory Access Protocol

OCSP -- Online Certificate Secure Protocol

PKI -- Public Key Infrastructure

Bibliografía

Las siguientes normas se han utilizado en la evaluación del producto:

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, septiembre 2004, Version 2.2, rev 311.

[CC_P2] Common Criteria for Information Technology Security Evaluation
Part 2: Security functional requirements, septiembre 2004, Version 2.2, rev 311.

[CC_P3] Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance requirements, septiembre 2004, Version 2.2, rev 311.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, septiembre 2004, Version 2.2, rev 311.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es

Declaración de seguridad

Se dispone, y se publican conjuntamente con este informe de certificación, de dos versiones de la misma declaración de seguridad, la utilizada durante la evaluación, en idioma inglés, y su correspondiente versión con los apartados fundamentales en idioma español:

Título	Código	Versión
Security Target KeyOne 2.1	0C53A113	2.0
Declaración de Seguridad KeyOne 2.1	040A5EBD	2.0

El Organismo de Certificación ha comprobado la equivalencia entre ambas versiones, así como de la versión 2.0 a la versión utilizada por el laboratorio y referenciada en su informe de evaluación, 0C53A113 versión 1.54.

 Avenida del Padre Huidobro s/n
Fax: + 34 91 372 65 68
Email: organismo.certificacion@cni.es