

## Cryptosec 2048

El objetivo de este laboratorio es el análisis y evaluación de Cryptosec 2048 de Realia Technologies S.L. (REALSEC). Cryptosec 2048 está compuesto de un módulo de seguridad hardware (HSM, Hardware Security Module) y un completo interfaz que facilita el proceso de integración con cualquier sistema, así como, el desarrollo de nuevos sistemas que necesiten utilizar alguno de los servicios proporcionados por Cryptosec. El sistema está compuesto por un módulo criptográfico cuyas principales funciones son la generación, almacenamiento y protección de claves criptográficas pero, además, aporta aceleración hardware para operaciones criptográficas tales como cifrado/descifrado. El hardware se integra fácilmente al servidor a través de un interfaz PCI. Además, cumple con la certificación del estándar FIPS 140-2 nivel 3 que certifica la seguridad del producto.

### IDENTIFICACIÓN DEL PRODUCTO

Cryptosec proporciona soporte a operaciones criptográficas de forma segura y con un alto rendimiento.

**Producto:** Cryptosec 2048

**Compañía:** Realia Technologies, S.L. (REALSEC)

**Detalles de contacto:** [www.realsec.com](http://www.realsec.com)

Cada día más la criptografía es un factor clave en los procesos de negocio de las organizaciones. El uso apropiado de la criptografía permite resolver los principales problemas de seguridad: privacidad, integridad, autenticación y no repudio. La base de la



criptografía son las claves criptográficas.

En la protección de estas claves se asienta el modelo de seguridad de los procesos basados en criptografía. De ahí la importancia del almacenamiento seguro de las claves criptográficas, así como, la necesidad de soporte de alta seguridad a las operaciones criptográficas. Los módulos de seguridad hardware, también conocidos como HSM (Hardware Security Module) son la solución más apropiada en la actualidad al problema de custodia y gestión de claves criptográficas y otros datos sensibles. Las soluciones hardware ofrecen un mayor nivel de protección que sus homólogas basadas en software, de ahí, que

sean las más utilizadas en entornos con altas exigencias de seguridad.

El producto evaluado en este laboratorio, HSM de Realsec, es un módulo de seguridad hardware, que incluye aceleración hardware para operaciones de cifrado como la generación de claves criptográficas simétricas y asimétricas a través de un generador de números aleatorios, exportación e importación de claves criptográficas, operaciones de cifrado/descifrado con distintos algoritmos criptográficos, funcionalidad criptográfica de clave pública (PKI) a través de distintas funciones resumen o HASH, entre otras. La aceleración hardware permite realizar las operaciones criptográficas, de forma eficiente, evitando así la ralentización que estos procesos suelen añadir a los sistemas basados en criptografía.

El producto hardware HSM se acompaña de una aplicación, Cryptosec, que sirve como interfaz de pruebas con el módulo hardware. Dicha aplicación permite probar todas las funcionalidades que provee el módulo de seguridad hardware.

Entre las principales aplicaciones de

Cryptosec 2048 es un producto de alta capacidad que proporciona una potente solución de alta seguridad y rendimiento al problema recurrente en todo sistema basado en criptografía de custodia y gestión de claves criptográficas.

Cryptosec 2048 podemos encontrar:

- Infraestructura de clave pública (PKI).
- Cifrado de comunicaciones.
- Cifrado masivo de ficheros y de discos.
- Protección de datos.
- Ejecución de código de aplicación de forma segura.
- Cajas fuertes digitales.
- Desarrollo de sistemas de cifrado partiendo del módulo criptográfico: medios de pago (tarjetas EMV – Visa, Mastercard - , cifrado de comunicaciones con TPVs y cajeros), procesos de validación de firma digital.

## DESCRIPCIÓN FÍSICA DEL PRODUCTO

El módulo hardware evaluado es una tarjeta PCI que debe instalarse en un equipo con una ranura libre compatible con PCI 2.1. La conexión al módulo hardware se realiza a través de una conexión RS-232.

El módulo tiene una protección externa con resina epoxi, además de una carcasa metálica de blindaje en chapa de acero de 0,9 mm. Además consta de sensores de temperatura, acceso físico y tensión que se utilizan para detectar posibles intrusiones al sistema borrando la información en caso de intrusión para imposibilitar el acceso no autorizado a las misma (tamper-resistant).

El módulo incorpora un sistema auxiliar de batería de litio (ER17/50) y una clavija DB-15 para la alimentación eléctrica de la misma. No es necesario conectar la batería para que el módulo funcione aunque es recomendable para mantener el acceso al contenido del módulo en ausencia de alimentación del PCI. La batería puede reemplazarse mientras en módulo está en funcionamiento.



Figura 1. Aspecto del módulo Cryptosec

### Especificaciones hardware

- Procesador con arquitectura RISC ARM7TDMI.
- Bus a 50 MHz (según versión).
- Dos co-procesadores RSA.
- Bus de propósito específico para operaciones de cifrado simétrico de muy alta velocidad.
- 128 Kbytes de memoria interna de alta seguridad (se borra automáticamente ante una intrusión).
- 2,1 Mbytes de almacenamiento interno de alta velocidad.
- Generador de números aleatorios hardware.
- Capacidad de puerto de comunicaciones asíncronas configurable como RS-232, I2C, USB, etc., aislado del procesador y la memoria.
- Interfaz PCI 2.1.
- Reloj de tiempo real.
- Protección de cobertura con resina epoxi más carcasa metálica de blindaje en chapa de acero de 0,9 mm.
- Sensores de intrusión (temperatura, acceso físico, tensión,...).

### ESPECIFICACIONES FUNCIONALES

El sistema está compuesto por un módulo criptográfico con un software flexible que interactúa con el servidor, con las siguientes funcionalidades:

- Cifrado de clave simétrica: Data Encryption Standard (DES), TDES de 2 y 3 claves, Secure And Fast Encryption Routine (SAFER) en 64 y 128 bits y en modos K y SK. Todos ellos pueden llevarse a cabo en los siguientes modos:
  - o Electronic Code Book (ECB),
  - o Ciphre Block Chaining (CBC),
  - o Cipher FeedBack 64 bit (CFB-64),
  - o Output FeedBack 64 bit (OFC-64).
- Funciones HASH: MD5, SHA-1 y RIPEMD en 128 y 160 bits.
- Estándar de clave pública RSA con longitud de clave de hasta 4096 bits.
- Control de tiempo a efectos de marcas de tiempo (*Time Stamping*).
- Generación de claves a través de un generador de números aleatorios, según lo especificado en FIPS 186-2 con nota de modificación y aprobado por FIPS 140-2. El módulo puede almacenar más de 15000 claves DES y TDES y más de 1000 RSA (hasta 2048 bits).
- Generación de Bloques PIN cifrados o EPB (Encrypt PIN Block) para operaciones en entornos bancarios. Los formatos soportados para EPB por Cryptosec son:

- ISO-0 (o ANSI X9.8, VISA-1, ECI)
- ISO-1 (o ECI-4)
- ISO-2
- IBM 3624

Todas las funciones de Cryptosec han sido probadas con resultados positivos durante la evaluación del producto. Para ello, se ha utilizado una aplicación que se proporciona junto con el módulo hardware que implementa todas las funciones disponibles en el mismo. La aplicación requiere conexión a través de un terminal VT100. A continuación se muestran algunas de las funciones principales:

1. Abrir/cerrar sesiones. Lo primero que hacer cada vez que se desea operar con Cryptosec es abrir una sesión con el módulo hardware. Para ello, Cryptosec 2048 realiza autenticación basada en identidad (fig. 2).
2. Cargar/borrar firmware.
3. Gestión de usuarios. Cryptosec permite añadir más de 1000 usuarios. Los usuarios pueden así gestionar sus claves con el HSM.
4. Copia/recuperación de datos. Permite hacer copias y restaurar claves. También permite hacer copias y recuperaciones de una imagen del contenido del módulo.
5. Ajustar el RTC (Real Time Clock) del módulo.
6. Operaciones con claves públicas. Se pueden obtener, cargar o borrar claves públicas.
7. Verificación de encendido. Permite forzar los chequeos ejecutados en el arranque excepto el de firmware (ver figura 3).
8. Operación RSA. Proporciona comandos de generación, borrado, exportación, importación, cifrado, descifrado, generación de firmas, chequeo de consistencia, entre otros.
9. Operación DES. Proporciona comandos de generación, borrado, exportación, importación, cifrado, descifrado, operaciones hash y creación de clave de transporte para la exportación segura de claves, entre otras.
10. Operaciones de Bloque PIN Cifrado o EPB (Encrypt PIN Block) para entornos bancarios. Permite generar y cifrar el Bloque PIN, verificación del EPB, cambio entre diferentes formatos, etc. También permite realizar funciones con VISA y American Express. Como la generación y comprobación del valor de verificación de tarjetas VISA (CVV, Card Verification Value) y American Express (CSC, Card Security Code).

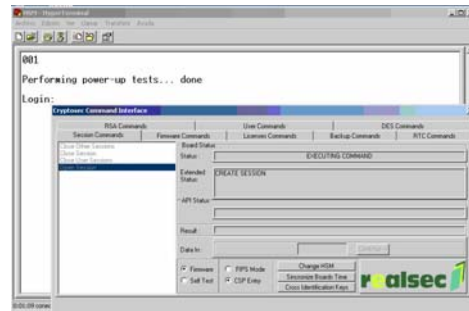


Figura 2. Detalle de la operación “Abrir sesión”.

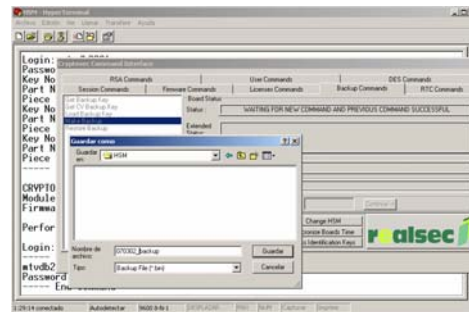


Figura 3. Detalle copia de seguridad.

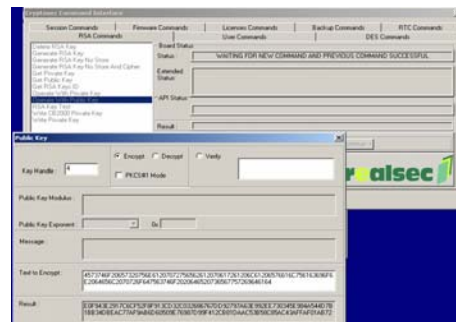


Figura 4. Detalle de cifrado de texto con RSA.



Figura 5. Detalle de generación de clave RSA.

En relación a la facilidad de integración del HSM de Cryptosec con las aplicaciones de seguridad que requieren de su uso, Realsec

proporciona en su HSM interacción a través del estándar PKCS#11 y un API nativo para el desarrollo de aplicaciones criptográficas. Las interfaces PKCS#11 permiten el uso de hardware a una gran variedad de aplicaciones criptográficas y es, en la actualidad, el interfaz utilizado en la mayoría de las tarjetas inteligentes, por ejemplo. También se proporciona un completo toolkit (API) que hace más fácil el proceso de integración con cualquier clase de sistemas que necesiten utilizar alguno de los servicios proporcionados por Cryptosec. De hecho, además del interfaz con el estándar PKCS#11, existen otros interfaces específicos con el HSM, como por ejemplo, interfaces para operativas online bancarias, de personalización de tarjetas o para peajes de autopista. Así, la funcionalidad del producto puede ser fácilmente ampliada pudiendo crearse interfaces a medida para la aplicación con la que se desee integrar el HSM, se facilita así la integración con productos ya existentes que no utilicen interfaces estándar.

En relación a la compatibilidad hardware/software, los únicos requisitos del producto es disponer de una ranura PCI en el servidor en el que se instala el módulo hardware y que dicho servidor tenga un sistema operativo win32 por disponer en la actualidad sólo de drivers para dichos sistemas operativos.

## SEGURIDAD

Se han identificado y valorado positivamente los dos modos de operación que provee Cryptosec:

- Modo FIPS. En este modo aparecen sólo disponibles las funciones permitidas y/o aprobadas en la evaluación de seguridad realizada por el NIST (National Institute of Standards and Technology) donde Cryptosec obtuvo el nivel 3 de certificación de seguridad para el estándar FIPS 140-2. Los algoritmos soportados en modo FIPS son: generación de claves y firmas RSA y verificación de firmas RSA, generación y cifrado/descifrado DES y TDES y función resumen SHA-1.
- Modo general. En este modo hay funcionalidad extendida no requerida en la evaluación de FIPS 140-2 y, por tanto, su seguridad no ha sido evaluada por el NIST. Además, Cryptosec provee en este modo de los siguientes algoritmos: cifrado/descifrado con RSA, funciones resumen MD5 y RIPEMD.

El NIST evalúa las características de seguridad que un producto debe cumplir según niveles de seguridad del 1 al 4. En el caso de HSM aplica la evaluación de la seguridad de módulos criptográficos FIPS 140-2. El nivel 3 verificado para Cryptosec es el nivel más alto otorgado a módulos criptográficos y corresponde al nivel EAL3 o superior del estándar de evaluación de de seguridad Common Criteria 2.1 (ISO/IEC 15408).

El nivel 3 de seguridad del FIPS 140-2 supone:

- Protección del dispositivo de accesos físicos no autorizados (tamper-evidence). Todos los componentes del HSM están recubiertos de resina epoxi opaca y, además, el conjunto está protegido de una cubierta metálica. Además, dispone de mecanismo de respuesta ante posibles intrusiones (tamper-response). En estos casos, la memoria interna es borrada. Esta memoria contiene el firmware y la clave maestra del firmware, lo que imposibilita el acceso a la información sensible.
- Autenticación basada en identidad. El módulo autentica al usuario verificando su identidad, con un robusto sistema de autenticación, y su role en el sistema para comprobar si tiene autorización para realizar los servicios requeridos. Cryptosec consta de dos roles: super-usuario (o Crypto-Officer) y usuario, distinguiendo de ese modo las tareas administrativas de las que no lo son.
- Los datos críticos son físicamente separados del resto y la entrada y salida de los mismos se realiza de forma cifrada. Toda la información sensible es introducida en el módulo o enviada desde el mismo a través del puerto RS-232 (requiere conexión por consola al servidor en el que está instalado el módulo). Además, el firmware del módulo impide la salida de datos confidenciales.
- El servidor en el que se instale el módulo debe cumplir los requisitos del Common Criteria de nivel EAL 3 o superior. Actualmente los sistemas operativos soportados por Cryptosec (Microsoft Windows 2000 y 2003) cumplen este requisito.
- Se proporciona un lenguaje de alto nivel para la interacción con el módulo. Cryptosec provee de una completa documentación sobre las clases C++ utilizadas para ocultar al usuario el protocolo de comunicación de



bajo nivel con el módulo, de forma que se pueda desarrollar código para programar aplicaciones que utilicen el HSM sin tener que conocer dicho protocolo.

Junto con el producto se proporciona documentación descriptiva sobre las capacidades del producto directamente relacionadas con la seguridad, que van desde la descripción del producto hasta el funcionamiento interno del mismo. Destacar que dicha documentación también incluye recomendaciones sobre el uso seguro del producto a incluir en la política de seguridad.

## PRESTACIONES

En las tablas 1 a 4<sup>1</sup> pueden observarse las prestaciones, suponiendo un flujo continuo de datos, para los algoritmos soportados.

Función	Rendimiento (Mbps)			
	ECB	CBC	OFB64	CFB64
DES	400	355	355	355
3DES doble o triple longitud de clave	400	128	128	128
SAFER_K64 6 iteraciones	533	457	457	457
SAFER_SK64 8 iteraciones	400	355	355	355
SAFER_K128 10 iteraciones	320	291	291	291
SAFER_SK128 10 iteraciones	320	291	291	291

Tabla 1. Rendimiento para algoritmos simétricos

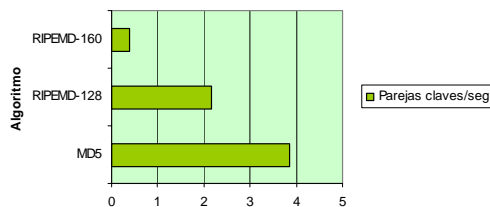


Tabla 2. Rendimiento para funciones hash

En el caso de los algoritmos asimétricos, el rendimiento depende en gran medida de la longitud de la clave. El HSM dispone de dos unidades de procesamiento de clave asimétrica. Los datos de la tabla 3 muestran el rendimiento obtenido con estas dos unidades (y un único HSM).

Función de Cifrado	Rendimiento (exp/seg)	
	Sin CRT	Con CRT
Exponenciación con clave pública de 1024 bit	7240	ND
Exponenciación con clave pública de 2048 bit	2275	ND
Exponenciación con clave privada de 1024 bit	337	688
Exponenciación con clave privada de 2048 bit	43	166

Tabla 3. Rendimiento para algoritmos asimétricos.

Por último, en la tabla 4 se muestran los tiempos de generación de claves RSA con un número de pasadas del test de Miller-Rabin tal que se asegura una probabilidad de falsos positivos menor que  $2^{100}$ .

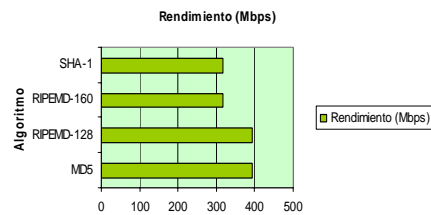


Tabla 4. Generación de claves RSA.

## OTRAS CARACTERÍSTICAS

Según la metodología de evaluación de calidad del software propia utilizada, además de las características vistas hasta el momento, se han evaluado por su importancia en la calidad final del software la fiabilidad del producto y la facilidad de administración del mismo.

### SATISFACCIÓN CON EL PRODUCTO

Como apoyo a los resultados obtenidos en la evaluación de las características externas del producto, se han realizado encuestas para medir el grado de satisfacción con Cryptosec 2048 a diferentes empresas usuarias del módulo y obtener así una medida de la calidad en uso del producto.

En la tabla 5 se puede observar los resultados obtenidos en las encuestas realizadas en las que los clientes de Cryptosec han valorado con una puntuación de 1 a 10 las distintas características dadas en el producto.

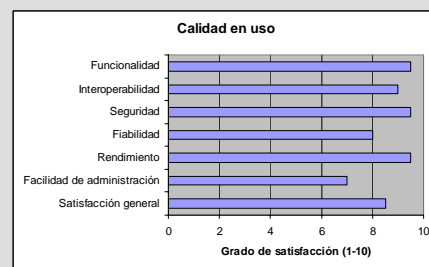


Tabla 5. Grado de satisfacción de clientes con Cryptosec 2048.

EURO 6000 es uno de las empresas usuarias de Cryptosec 2048. EURO 6000 desarrolló junto con Realsec un interfaz específico para proporcionar una solución adaptada a los requisitos de las Cajas de Ahorros EURO 6000. Entre las aplicaciones principales destacan el soporte a las operativas de gestión y administración estándares del sector, así como, a las nuevas operativas (EMV, comercio electrónico, Vía T o la gestión dinámica de claves en los terminales, entre otras). Además se posibilita el acceso seguro para aplicativos "online" y "offline" y se dota de interfaz preciso para las tareas administrativas y de impresión segura de códigos PIN y componentes de claves.

<sup>1</sup> Los datos de rendimiento han sido tomados en un entorno controlado del laboratorio de Realsec con equipos Pentium III a 700 Mhz con 256 MB de RAM y sistemas operativos Microsoft Windows 2000 y XP.

En relación a la fiabilidad del producto, aunque Cryptosec no proporciona mecanismos específicos de tolerancia a fallos, sí ofrece la posibilidad de trabajar con varios HSM simultáneamente, de forma que se pueda implementar mecanismos de este tipo a un nivel superior del HSM (software). Por otra parte, el HSM carece de sistema operativo, u otras características como gestión de memoria dinámica. Esta simplicidad en el diseño hace del HSM un dispositivo altamente robusto al evitar todos los puntos posibles de fallo relacionados con dichos elementos. Además, Cryptosec 2048 separa las áreas de memoria y los datos temporales del área de almacenamiento de datos críticos como claves y usuarios. En cuanto a la capacidad de recuperación, proporciona opciones para realizar backups y recuperaciones de los datos. Por último, Cryptosec dispone de una función que permite realizar pruebas de verificación de integridad del firmware y las claves almacenadas y que puede ejecutarse desde el interfaz en cualquier momento.

En lo que a administración del producto se refiere, la instalación del producto es muy sencilla. Tan solo hay que instalar el módulo en una ranura PCI y luego instalar los drivers proporcionados y cargar el firmware.

La administración se realiza después a través del interfaz con HSM proporcionado con el producto. Dicho interfaz es una aplicación gráfica basada en BSAFE de RSA fácil de usar. La configuración inicial del módulo también es muy simple, basta con abrir la sesión VT100 y luego una sesión con el interfaz. A partir de ahí, se pueden crear los usuarios, claves, etc. La actualización del producto es también muy sencilla. Lo único que hay que tener en cuenta es que hay que hacer un backup de los datos ya que la actualización del firmware borra todos los datos almacenados en el módulo. Por último, en lo referente a usabilidad del interfaz hacia Cryptosec, la aplicación es muy simple. Para su uso se proporciona una documentación muy completa: manual de usuario y del administrador, además de los ya mencionados anteriormente (manual del programador y documentación sobre políticas de seguridad). No dispone de ayuda online ni tampoco de mensajes de ayuda relacionados, por ejemplo, con errores en la entrada de datos a la aplicación que ayuden a corregir dicha entrada lo que puede dificultar el aprendizaje inicial del uso de

#### EQUIPOS USADOS EN LA EVALUACIÓN

- HSM Cryptosec 2048 con versión de firmware v.02.04 (Build 0001)
- PCs Pentium III 700 Mhz con 256 MB de RAM y 2800 Mhz con 1.8 GB de RAM con sistemas operativos Microsoft Windows 2000, 2003 y XP.
- Como infraestructura física se han utilizado redes locales Ethernet 100BaseT y equipos de comunicaciones CISCO (Catalist 2950 y routers 2800)
- Analizador de protocolos para la monitorización de las comunicaciones.
- Aplicación de pruebas para la medición de las prestaciones del HSM.
- Aplicación de simulación de ataques de intrusión y escáner de seguridad.

la misma pero, dada la sencillez de la herramienta y como no está orientada al usuario sino a administradores a los que se presupone conocimientos avanzados en el uso de las aplicaciones, no debería ser un problema. La interfaz de la aplicación es muy austera, siendo así, un fiel reflejo de la sencillez en la que se basa el producto para centrarse en la seguridad y fiabilidad como los principales objetivos en el desarrollo del mismo.

En relación a la portabilidad del producto, éste es capaz de exportar e importar claves hacia y desde módulos de otros fabricantes lo que aumenta su facilidad de sustituir a otros productos de similares características o ser sustituido por uno de ellos.

#### CONCLUSIONES

Cryptosec 2048 es un acelerador criptográfico de gama alta que proporciona servicios criptográficos y de almacenamiento

seguro de claves de cifrado esenciales en todo entorno con requisitos muy exigentes en relación a la seguridad.

Los resultados obtenidos tras someter el producto a pruebas continuas de evaluación durante un mes, demuestran que el producto tiene una alta calidad tanto por la completa funcionalidad de que dispone, como por su estabilidad y su seguridad demostrada a través de la certificación de seguridad internacional más importante en la actualidad. También cabe destacar sus altas prestaciones tanto en la generación de claves como en el cifrado/descifrado de datos. Además, el diseño sencillo en el que se apoya el producto, le otorgan una gran versatilidad permitiendo que sea fácilmente integrado y haciendo posible la extensión de sus características iniciales proporcionando, por ejemplo, la posibilidad de implementar mecanismos de tolerancia a fallos para proveer de fiabilidad a las aplicaciones que hacen uso del mismo.

#### EQUIPO DE EVALUACIÓN

**Prof. Maite Villalba de Benito**  
**Prof. Dr. Luis Fernández Sanz**  
 Grupo de Investigación DPRIS  
 (Programación e Ingeniería del Software).  
 UNIVERSIDAD EUROPEA DE MADRID

