

Sistema HSM

Especificaciones Técnicas

- Procesador con arquitectura RISC ARM7TDMI.
- Bus a 50 MHz (Según versión).
- Dos Co-procesadores RSA.
- Co-procesador DES simétrico.
- Bus de propósito específico para operaciones de cifrado simétrico de muy alta velocidad.
- 128 Kbytes de memoria interna de alta seguridad (esta memoria se borra automáticamente ante una intrusión).
- 2,1 Mbytes de almacenamiento interno de alta seguridad.
- Generador de números aleatorios por hardware.
- Capacidad de puerto de comunicaciones asíncronas. Configurable como: RS-232, I2C, USB etc... aislado del procesador y la memoria.
- Interface 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...)



Características Funcionales

El sistema está compuesto por un módulo criptográfico con un software flexible que transmite su funcionalidad al servidor, con las siguientes capacidades:

- Cifrado de clave simétrica, tanto Data Encryption Standard (DES), triple DES de dos claves, triple DES de tres claves, como Secure And Fast Encryption Routine (SAFER) en 64 y 128 bit y en modos K y SK, todos ellos pueden llevarse a cabo en los siguientes modos:

- Electronic Code Book (ECB),
- Cipher Block Chaining (CBC),
- Cipher FeedBack 64 bit (CFB-64),
- Output FeedBack 64 bit (OFB-64).

- Funciones HASH: MD5, SHA-1 y RIPEMD en 128 y 160 bit.

- Estándar de clave pública RSA con longitud de clave de hasta 4.096.

- Control de tiempo, a efectos de 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

Niveles de Seguridad

El hardware cumple con la certificación del estándar **FIPS 140-2 nivel 3**.

- El firmware del módulo impide la salida de datos confidenciales.

- Se imposibilita el acceso a las diversas partes de la tarjeta criptográfica con sensores que detectan intrusiones o anomalías, borrando la información. Además, todos los componentes están cubiertos por una resina epoxi opaca y una cubierta metálica protege el conjunto.

- Sistema seguro para carga y custodia de claves de procedencia externa mediante conexión directa a la placa de un terminal asíncro.

- Posibilidad de asignación de propiedad de claves por usuarios.

Otras Características

Se destacan aquí otros aspectos de interés:

- Una de las versiones del firmware interno incorpora el interfaz estándar PKCS#11. Con ello el hardware queda dispuesto para trabajar con cualquier aplicación que respete dicho interfaz. Otras versiones incorporarán firmware específico para usarse en otros entornos.
- Funciones de manejo de PINblock para entornos bancarios.
- Permite la utilización de varios módulos de forma simultánea.
- El firmware permite su actualización, a través de un mecanismo seguro de autenticación.
- Las características constructivas del hardware, permiten implementar otra serie de capacidades, como las curvas elípticas.
- Es también posible portar al módulo código de aplicación que el cliente desee que se ejecute de forma segura.

Prestaciones

- Clave simétrica:

Las prestaciones indicadas a continuación, son válidas al trabajar con una corriente sostenida de datos. Las prestaciones reales dependerán del modo de acceso empleado para los datos.

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

- Hash:

Valgan los comentarios anteriores también en este caso:

Función	Rendimiento (Mbps)
MD5	393
RIPMD-128	393
RIPMD-160	316
SHA-1	316

- Clave asimétrica:

Las prestaciones del manejo de clave asimétrica dependen en gran medida de la longitud de las claves y sus valores en concreto. El sistema dispone de dos unidades de proceso de clave asimétrica. Se muestra el rendimiento de ambos. El de una sola unidad es la mitad del indicado en la tabla.

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

En la siguiente tabla se indican 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}

Tamaño del módulo	Rendimiento (parejas de claves/hora)
768 bit	13.846
1024 bit	7.826
2048 bit	1.358