

Módulo de Seguridad del Anfitrión (HSM)



- Apoya Aplicaciones de Cajero Automático, EFTPOS y Tarjetas de circuito integrado
- Funciones de Verificación de PIN y Tarjetas Visa/MasterCard/American Express
- Diseño Resistente a la Manipulación
- DES, Triple DES de dos y tres claves y RSA
- Apoya Cargas de VISA CASH
- Apoya las normas ANSI, ISO y las Normas de Seguridad Australianas.



Módulo de Seguridad del Anfitrión (HSM)

El módulo HSM es un dispositivo resistente a la manipulación que brinda los servicios criptográficos necesarios para asegurar las transacciones en las redes financieras.

El HSM se utiliza para asegurar múltiples aplicaciones financieras en todo el mundo, desde las redes de cajeros automáticos y los puntos de venta hasta las transferencias interbancarias de fondos y los sistemas de transacciones de bolsa. Está disponible en las variantes estándar y de alta velocidad, con un amplio rango de opciones y protocolos de conexión que permiten conectarse a todo tipo de sistemas anfitriones.

El Módulo de Seguridad del Anfitrión:

- Se utiliza por el 70 por ciento de las transacciones con tarjetas en el mundo
- Lo utilizan todas las principales asociaciones de tarjetas de crédito
- Se utiliza para Cajeros Automáticos, Puntos de Venta, Banca Empresarial, Emisión de Tarjetas, Transferencias de Fondos y Transacciones de Bolsa y Accionarias
- Se adapta fácilmente a las aplicaciones de los usuarios
- Se encuentra disponible con apoyo para un amplio rango de opciones de conexión y protocolos de transacción
- Disponible en variantes Estándar y de Alta Velocidad, a fin de facilitar el volumen requerido de transacciones
- Tiene capacidad de Triple DES, valiéndose de dos y tres claves, para todas las funciones, incluido el procesamiento de bloques de números PIN.

APLICACIONES TÍPICAS PARA MÓDULOS HSM

Intercambio de Cajeros Automáticos

El HSM está diseñado para el entorno de intercambio de cajeros automáticos y se utiliza en muchas de las principales redes de intercambio de cajeros automáticos. El HSM puede adaptarse a las condiciones de cada red y, de ser necesario, a los requisitos

particulares de cada miembro de la red. La amplia y creciente variedad de interfaces anfitriones en el módulo HSM significa que éste se puede acondicionar a las necesidades del sistema de cada miembro. En particular, los comandos de AMEX, VISA y MasterCard son parte integral de todas las versiones estándar de soporte lógico.

EFTPOS

El HSM brinda apoyo a varios sistemas EFTPOS (Transferencia de Fondos en el Punto de Venta) que se utilizan en el mundo. Muchos de los conceptos fundamentales de gestión necesarios para asegurar a EFTPOS, como el Método Racal de Claves de Transacción, fueron iniciados por Racal y se pusieron en práctica por primera vez en el HSM. También están disponibles los regímenes de Clave Derivada Única por Transacción y Clave Australiana de Transacciones.

Planta de Producción de Tarjetas

El módulo HSM se puede utilizar dentro del área de producción de tarjetas del cliente. Brinda un medio seguro para generar valores criptográficos de tarjetas como el CVV (Valor de Verificación de Tarjetas) de VISA, el CVC (Código de Verificación de Tarjetas) de MasterCard y el CSC (Código de Seguridad de Tarjetas) de American Express, así como



para generar de forma segura números PIN y correspondencia relativa a éstos.

Recarga de Tarjetas Visa Cash

El HSM brinda apoyo al proceso de recarga de tarjetas Visa Cash, de modo que los titulares puedan recargar sus tarjetas de forma segura en un cajero automático o terminal de recarga de tarjetas. El HSM efectúa el procesamiento criptográfico en el servicio anfitrión para proporcionar apoyo al cajero automático o terminal de recarga. Las funciones de carga en efectivo de Visa apoyan las más recientes especificaciones de Visa (ALGL = 4).

Integridad de los Datos

La integridad de la información que se transmite de un lugar a otro y que se guarda en los sistemas es de la mayor importancia para sus usuarios. La integridad de la información que se genera en terminales remotas se puede asegurar mediante códigos de autenticación de mensajes (MAC), mediante los Módulos de Seguridad de PC de Zaxus y las terminales de Tarjetas Inteligentes para su posterior verificación en un módulo HSM. De ésta manera se pueden asegurar varias aplicaciones, como las de Gestión de Efectivo y Conciliación de Bonos.

Apoyo a las Tarjetas de Chip

El HSM brinda apoyo a aplicaciones de tarjetas de chip de Crédito y Débito y Cartera Electrónica de Visa, MasterCard y Europay. Si así se solicita, las funciones de procesamiento de transacciones se encuentran disponibles como funciones estándar de emisión de tarjetas. Para más información, contacte a su representante local.

PRESTACIONES DE HSM

Variantes Estándar y de Alta Velocidad

Dado que las industrias bancaria y financiera siguen estableciendo sistemas de seguridad basados en números PIN y con Tarjetas

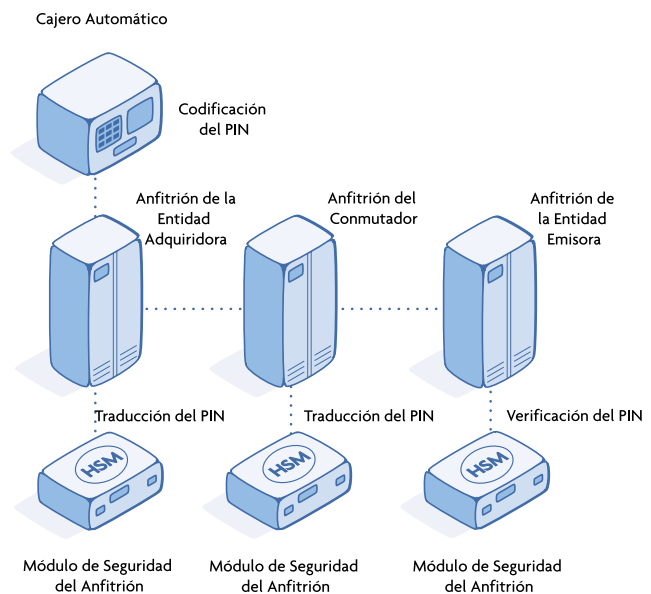
Inteligentes, la demanda de una mayor velocidad en las transacciones, nunca ha sido más grande.

En su variante de alta velocidad, el módulo HSM puede procesar transacciones de forma sustancialmente más rápida que el HSM estándar, con lo que se reducen significativamente el tiempo de procesamiento de transacciones y el costo por transacción. Además, el hecho de que el módulo HSM de alta velocidad cuenta con unidades más grandes de almacenamiento intermedio de entrada y salida permite el procesamiento de largos mensajes criptográficos sin requerir llamadas múltiples en cadenas.

Sistema Flexible de Gestión de Claves

En la práctica, la calidad de la seguridad que ofrece cualquier aplicación depende del sistema de gestión de claves que se haya diseñado para dicha aplicación. El HSM brinda apoyo para distintos sistemas de gestión de claves, incluidos el de Claves Maestras/de Sección, Clave Racal de

Aplicación Típica de Intercambio de Cajero Automático



Transacciones, Clave Australiana de Transacciones, DUKPT y Clave Pública.

Apoyo a Claves Públicas RSA (Opcional)

El módulo HSM ofrece un subsistema de alta velocidad de Claves Públicas. La criptografía de Claves Públicas RSA se utiliza con dos funciones principales:

- 1) generar y verificar las firmas digitales y
- 2) distribuir claves DES codificadas con una Clave Pública RSA.

El HSM puede procesar claves RSA de 320 a 2048 bits. Gracias a esta prestación, el HSM se puede utilizar en sistemas en los que se usen claves de distinta longitud para diferentes funciones, como las firmas digitales y la gestión de claves. Además, protege la inversión de la compañía en medios tecnológicos, pues se prevé que la industria aumentará los requisitos de longitud de claves para mantenerse a salvo de las crecientes amenazas.

Resistencia a la Manipulación

El módulo HSM está diseñado de acuerdo con los requisitos FIPS 140-1 de 'seguridad física' de nivel 3. En consecuencia, su diseño es de primera línea y protege contra los siguientes ataques: inspección interna, escudriñamiento, movimientos y fluctuaciones anormales de temperatura y voltaje.

Almacenamiento y Generación de Claves Seguras

Una vez que se haya formado la Clave Maestra Local (LMK) dentro del HSM, todas las demás claves quedan almacenadas en forma codificada bajo esta clave en el anfitrión y, opcionalmente, dentro del propio HSM. El módulo utiliza tecnología de tarjeta inteligente para almacenar los componentes fundamentales del LMK.

El diseño del generador de números aleatorios cumple los requisitos del procedimiento de verificación FIPS 140-1.

Amplio Apoyo al Software Anfitrión

El HSM puede conectarse con muchos anfitriones distintos, incluido: Amdahl®, Bull®, IBM, ICL, DEC, HP®, NCR®, Stratus®, Tandem®, Unisys® y PC.

Administradores de Recursos de Seguridad

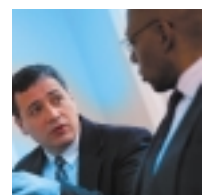
Los Administradores de Recursos de Seguridad (SRM) son productos opcionales de software para los sistemas IBM MVS, Tandem Guardian y UNIX®. Los SRM permiten que múltiples aplicaciones utilicen un solo Interfaz de Programación de Aplicaciones (API) para acceder a los recursos criptográficos proporcionados por un conjunto de módulos HSM. El SRM permite el uso transparente de distintos modelos de HSM con las aplicaciones de los clientes.

- Versión IBM – opera con el sistema OS/390 y brinda apoyo a las aplicaciones CICS, IMS y de proceso por lotes. También se ofrece apoyo para los programas de lenguaje de ensamblaje y para los lenguajes de alto nivel, como el COBOL y el PL/I.
- Versión Tandem – opera con el sistema operativo Guardian como aplicación de Pathway y acepta solicitudes a través de un módulo de interfaz de aplicaciones o una interfaz de servidor. Además, puede proporcionarles a las aplicaciones una base de datos de claves que se puede administrar mediante la aplicación o mediante una interfaz de usuario de gestión de claves (incluido).
- Versión UNIX – opera con distintos estilos de UNIX. Opera como servidor de las aplicaciones de cliente que se ejecuten en la misma máquina que el SRM o desde cualquier máquina de la red. La interfaz API brinda apoyo a aplicaciones escritas en C o en C++.



Módulo de Seguridad del Anfitrión (HSM) – Especificaciones Técnicas

Desempeño Típico en la Función de Verificar Números PIN de VISA	RG7110	180 tps (transacciones por segundo)
	RG7210	720 tps
	RG7310	220 tps
	RG7100	60 tps
	RG7200	80 tps
	RG7300	70 tps
	RG7400	10-15 tps
	RG7500	8 tps
Apoyo Criptográfico	RG7600	25 tps
	Algoritmos DES y Triple DES – Brindan la posibilidad de codificar el PIN y autenticar mensajes. Algoritmo RSA (opcional) – Brinda gestión de claves de alto nivel y apoya la generación y validación de las firmas digitales. La longitud de las claves de RSA se puede seleccionar de 320 a 2048 bits. Componentes Locales de Clave Maestra – Se guardan en las Tarjetas Inteligentes (ISO 7816) para almacenarlos o distribuirlos de manera segura.	
Interfaces de Comunicaciones	RG7100/ 7110	TTCP/IP Y UDP, Ethernet; Asincrónico, RS-232
	RG7200/7210	Interfaz de canal de IBM (FIPS 60)
	RG7300/7310	SDLC, RS-449; Asincrónico, RS-232
	RG7400	Asincrónico y sincrónico binario, RS-232
	RG7500	SNA/SDLC, RS-232
	RG7600	SNA/SDLC, V.35
Resistencia a la Manipulación	Conforme con las Normas FIPS 140-1 de Nivel 3 sobre Seguridad Física y EFP.	
Alimentación eléctrica	Voltaje	90-132 VAC y 175-264 VAC, autoseleccionado
	Frecuencia	47-63 Hz
	Fusible	1.6A acción retardada
Entorno	Temperatura de Operación	10° a 40° C
	Humedad	10% a 90%, sin condensación
Dimensiones Físicas	Altura	133 mm (5.25")
	Ancho	483 mm (19")
	Profundidad	489 mm (19.25")
	Peso	18 kg (40 lb.)





THALES

Europa, Oriente Medio, África

THALES e-SECURITY LTD.
Meadow View House
Long Crendon, Aylesbury
Buckinghamshire, HP18 9EQ,
Reino Unido
Tel: +44 (0)1844 201800
Fax: +44 (0)1844 208550
Correo electrónico:
emea.sales@thales-esecurity.com

Américas

THALES e-SECURITY, INC.
Sawgrass Technology Park
1601 North Harrison Parkway
Building A, Suite 100
Sunrise, FL 33323, USA
Tel: +1 888 744 4976
ó: +1 954 846 4700
Fax: +1 954 846 3935
Correo electrónico:
americas.sales@thales-esecurity.com

Asia y Pacífico

THALES e-SECURITY (ASIA) LTD.
Asia Pacific
Units 2205-06, 22/F Vicwood Plaza,
199 Des Voeux Road
Central, Hong Kong, PRC
Tel: +852 2815 8633
Fax: +852 2815 8141
Correo electrónico:
asia.sales@thales-esecurity.com

www.thales-esecurity.com

