



CONSEJERÍA DE TRANSPORTES,  
INFRAESTRUCTURAS Y VIVIENDA

**Comunidad de Madrid**



**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN POR  
PROCEDIMIENTO ABIERTO DE LA “ADQUISICIÓN DE HSM PARA LA  
ESCALABILIDAD DEL SISTEMA DE SEGURIDAD CENTRALIZADO DEL  
SISTEMA BIT (SECEBIT) DEL CRTM”**



## 1 OBJETO DEL DOCUMENTO

El objeto del presente documento es establecer las condiciones de carácter técnico que han de regir la contratación, por procedimiento abierto para el “ADQUISICIÓN DE HSM PARA LA ESCALABILIDAD DEL SISTEMA DE SEGURIDAD CENTRALIZADO DEL SISTEMA BIT (SECEBIT) DEL CRTM” para el Consorcio Regional de Transportes de Madrid, durante el ejercicio de 2018.

## 2 ANTECEDENTE Y JUSTIFICACIÓN

El CRTM inició el proyecto de migración del billete basado en tecnología Edmonson al billete basado en tecnología sin contacto, con una arquitectura de seguridad para los procesos de pre-personalización, personalización y carga/recarga, basada en sistemas SECEBIT.

Los HSM custodian de forma segura las claves maestras del sistema además de proveer de los comandos necesarios de autenticación y cifrado. En los SECEBIT se almacenan todos los contadores transaccionales del sistema asegurando su inviolabilidad.

Debido al gran aumento de tarjetas TTP en la Comunidad de Madrid, unido al futuro cambio de sede del CRTM que hará necesario disponer de un sistema redundante SECEBIT mientras se hace el traslado de sede, se hace preciso redimensionar y adaptar dicha arquitectura hardware de seguridad del sistema adquiriendo nuevos servidores y placas HSM.

### 3 OBJETO DEL CONTRATO

El objeto del presente contrato es la adquisición de diez unidades de servidores criptográficos "ProtectServer externo PL-1500", además de un núcleo "ProtectServer interno PL-1500", que deben ajustarse a las especificaciones del sistema de Seguridad Centralizada del sistema BIT, que se citan en el apartado siguiente a continuación

### 4 DESCRIPCIÓN DEL SISTEMA

Los distintos elementos que forman un sistema **SECEBIT** son tres:

- Balanceador.
- Servidor criptográfico.
- Módulo de seguridad (o núcleo).

#### BALANCEADOR

Cada balanceador tiene:

- Por lo menos un microprocesador INTEL Xeon de núcleo cuádruple modelo 5400 @ 3,33GHz o 2,66GHz o de doble núcleo modelo 5200 @ 3,5GHz.
- Memoria RAM mínimo de 8 GBytes.
- Sistema operativo: LINUX (distribución DEBIAN LENNY o cualquier otra 100% compatible).
- Dos discos duros (RAID 1) SAS de 146 GBytes cada uno (balanceador maestro y esclavo).
- CD o DVD drive.
- Tarjeta Gigabit Ethernet (con capacidad de funcionar con fibra óptica - opcionalmente).



- Unidades de disco duro de conexión en caliente.
- Fuente de alimentación redundante de conexión en caliente.
- Refrigeración redundante.
- Chasis montable en RACK ocupando solo 1U.
- 4 puertos USB, 1 conector de serie, 1 conector de video, 1 puerto RJ45.
- Temperatura de funcionamiento: 10°C a 35°C.
- Humedad de funcionamiento: 20% a 80%.
- Controladores (drivers) para todos los periféricos del servidor.

### SERVIDOR CRIPTOGRÁFICO

Las características del servidor criptográfico, (que alberga uno o más módulos de seguridad) son:

- Arquitectura INTEL (Pentium D o Pentium 4) y seguridad física de acceso a dispositivos removibles.
- Memoria RAM de 4 GBytes.
- Tarjeta gráfica de 1280x1024 pixels.
- 2 discos duros en RAID 1
- CD o DVD.
- Sistema operativo LINUX (distribución CentOS o cualquier otra 100% compatible).
- Conectividad TCP/IP y tarjeta de red que soporta 10Mb/s, 100Mb/s y 1Gb/s transmisión de datos.
- Puertos USB (mínimo 4), puerto VGA, puerto de serie, puerto de paralelo, 1 mini DIN-6 PS/2 puerto para ratón y 1 mini DIN-6 PS/2 para teclado.

- Escalabilidad y reparto de carga en configuraciones con más de un HSM embebido.
- Mínimo de cuatro ranuras de expansión de tipo PCI.
- Temperatura de funcionamiento: 0°C a 60°C.
- Humedad de funcionamiento: 10% a 90%.
- Chasis montable en RACK ocupando 4U.
- Controladores (drivers) para todos los periféricos del servidor.

#### Núcleo: MÓDULO SEGURIDAD HSM

Las características más importantes del módulo de seguridad HSM (ProtectServer interno PL-1500) son:

Certificación FIPS 140 2 Nivel 3, que confirma que el módulo está adaptado para detectar y ofrecer protección contra ataques físicos y lógicos.

#### Cryptographic APIs

>> PKCS#11, CAPI/CNG, JCA/JCE, JCPProv, OpenSSL

#### Cryptographic Processing

#### Asymmetric Algorithms

>> RSA (up to 4096 bit) , DSA, ECDSA Diffie Hellman (DH),  
ECC Brainpool Curves (named and user-defined)

#### Symmetric Algorithms

>> AES, DES, 3DES, CAST-128, RC2, RC4, SEED, ARIA

>> Modes supported include ECB, CBC, OFB64, CFB-8 (BCF)



### Hashing Algorithms

>> MD5, SHA-1, SHA-256, SHA- 384, SHA- 512, MD2,  
RIPEMD128, RIPEMD160, DES MDC-2 PAD1

### Message Authentication Codes

>> SHA-1, SHA-256, SHA-384, SHA-512, MD2, RIPEMD128,  
RIPEMD160, DES MDC-2 PAD1, SSL3 MD5 MAC, AES MAC,  
CAST-128 MAC, DES MAC, DES3 MAC, DES3 Retail CFB  
MAC, DES30x9.19 MAC, IDEA MAC, RC-2 MAC, SEED MAC,  
ARIA MAC, VISA CVV

### Physical Characteristics

>> Dimensions: Full Height, Half Length 4.16" x 6.6" (106.7mm  
x 167.65mm)  
>> Power Consumption: 12W maximum, 8W typical  
>> Temperature: operating 0°C – 50°C

### Security Certifications

>> FIPS 140-2 Level 3  
>> BAC & EAC ePassport Support

### Safety and Environmental Compliance

>> UL, CSA, CE  
>> FCC, KC Mark, VCCI, CE  
>> RoHS, WEEE

### Host Interface

>> PCI-Express X4, PCI CEM 1.0a

### Reliability

>> MTBF 216,204 hrs



## SERVIDOR CRIPTOGRÁFICO INTEGRADO

Es la suma de un servidor criptográfico y un núcleo HSM (ProtectServer interno PL-1500). Las características más importantes son:

### Operating Systems

>> Windows, Linux, AIX, HP\_UX, Solaris

### Cryptographic APIs

>> PKCS#11, CAPI/CNG, JCA/JCE, JCPov, OpenSSL

### Cryptographic Processing

#### Asymmetric Algorithms

>> RSA (up to 4096 bit), DSA, ECDSA Diffie Hellman (DH), ECC  
Brainpool Curves (named and user-defined), plus others

#### Symmetric Algorithms

>> AES, DES, 3DES, CAST-128, RC2, RC4, SEED, ARIA, BIP32  
and SECP256k1, Milenage, plus others  
>> Modes supported include ECB, CBC, OFB64, CFB-8 (BCF)

#### Hashing Algorithms

>> MD5, SHA-1, SHA-256, SHA- 384, SHA- 512, MD2,  
RIPEMD128, RIPEMD160, DES MDC-2 PAD1

#### Message Authentication Codes

>> SHA-1, SHA-256, SHA-384, SHA-512, MD2, RIPEMD128,  
RIPEMD160, DES MDC-2 PAD1, SSL3 MD5 MAC, AES MAC,  
CAST-128 MAC, DES MAC, DES3 MAC, DES3 Retail CFB  
MAC, DES30x9.19 MAC, IDEA MAC, RC-2 MAC, SEED MAC,  
ARIA MAC, VISA CVV



## Physical Characteristics

### Dimensions

>> 437 mm (W) x 270 mm (D) x 44 mm (H) (PSE2 model)

Página 12 de 23—

Copyright © 2017, Seglan. Todos los derechos reservados.

### DOCUMENTO CONFIDENCIAL

>> 482.6mm (W) x 533.4mm (D) x 43.815mm (H) (PSE2+ model)

### Power Consumption

>> 220/110 Volts switchable (PSE2 model)

>> 110W maximum, 43W typical (PSE2 model)

>> 220/110 Volts automatic switching (PSE2+ model)

>> 180W maximum, 155W typical (PSE2+ model)

### Temperature

>> Operating 0°C - 35°C

### Security Certifications

>> FIPS 140-2 Level 3

### Safety and Environmental Compliance

>> UL, CSA, CE

>> FCC, KC Mark, VCCI, CE

>> RoHS

## Principales funcionalidades que debe ofrecer el sistema global

- Almacenaje de claves maestras embebidas en el núcleo.
- Autenticación con tarjetas (tipo DESFire). Antes de realizar cualquier tipo de operación con la tarjeta sin contacto Sube-T, es imprescindible que cada una de las dos partes (es decir tarjeta y lector) demuestre a la otra que posee la clave correcta para la operación. Por un lado, la tarjeta tiene almacenadas las claves, y por el otro el lector tendrá que acceder a SECEBIT para realizar la autenticación DESFire en tres



pasos. Así que el lector en este caso tiene el rol de intermediario, siendo el módulo de seguridad quien se encarga de: primero confirmar que la tarjeta posee la clave correcta, y segundo demostrar que el mismo tiene la clave. Durante estas comprobaciones no se emite ninguna clave.

- Diversificación de claves de tarjetas. Cada tarjeta contiene un conjunto único de claves que se calcula por SECEBIT.
- Firma de registros de operaciones con tarjetas. Cada vez que se realiza una transacción con la tarjeta, se genera un registro donde se refleja la operación que se ha realizado (según especificaciones técnicas). Con el objetivo de evitar modificaciones del registro después de su generación y detectar errores durante el envío al CRTM, se ha creado la función de generación de firma, donde a través de un algoritmo secreto (implementado en el núcleo HSM SafeNet), se calcula una trama de bytes (que es realmente la firma) que se concatena al propio registro.
- Búsqueda en lista de tarjetas no permitidas. Cuando una tarjeta solicita algún tipo de operación, antes de iniciar el proceso de autenticación, el sistema SECEBIT comprueba que la tarjeta no está incluida en la lista de tarjetas no permitidas. Dicha lista se genera por el CRTM y se puede distribuir diariamente a las BBDD a las que apuntan los HSM21.
- Encriptación y desencriptación de datos personales. Existe una operación donde se generan datos personales. Esta operación se denomina personalización, asocia una tarjeta a un usuario, y genera un registro de datos personales que no pueden quedar en claro. El núcleo HSM se utiliza para cifrar /descifrar los datos personales del registro, mediante la capa de alto nivel HSM21.
- Suministro de cupo a módulos de seguridad local (SAM). Cuando un terminal que principalmente opera con SECEBIT se queda sin conexión, no podrá trabajar con las tarjetas subeT. Una forma de superar temporalmente esta limitación, es autorizar el módulo de seguridad local (SAM) del terminal, para realizar un número limitado de operaciones. Esta autorización se realiza por SECEBIT.
- Control de comandos por IP.



- SECEBIT está asociado a una BBDD que almacena toda la información centralizada del sistema. En esta BBDD se centralizan las LNS y todas las transacciones que se producen en el sistema mediante el sistema SECEBIT.
- Funcionamiento en modo degradado. SECEBIT es capaz de seguir funcionando aun cuando no dispone de conectividad con la base de datos. En este caso, almacena provisionalmente la información en fichero y cuando recupera la visibilidad con la BBDD vuelca la información a ésta, manteniendo un registro centralizado de cualquier operación producida con el HSM.

## **5 SEGUIMIENTO Y CONTROL DEL CONTRATO**

Para el seguimiento y control del contrato se designará por parte del CRTM un Director del Contrato y por parte de la empresa adjudicataria un Responsable del Suministro ante el CRTM, que actuará como interlocutor ante el citado organismo.

Madrid, 20 de julio de 2018

EL DIRECTOR GERENTE,

  
Alfonso Sánchez Vicente

CONFORME,  
EL ADJUDICATARIO

