

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL LA “COORDINACIÓN DE LOS PROCESOS DE VIRTUALIZACIÓN DE LA TARJETA DE TRANSPORTE DEL CRTM”

ÍNDICE

1.	ANTECEDENTES	2
2.	OBJETO	2
3.	DESCRIPCIÓN GENERAL DEL SISTEMA BIT.....	3
4.	DESCRIPCIÓN DE SECEBIT Y LAT-SECU	7
4.1.	SECEBIT	7
	Subsistemas de HSMs	8
4.1.1	Subsistemas de balanceo de carga y alta disponibilidad	13
4.1.2.	<i>Subsistemas de registro de operaciones de HSMs.</i>	14
4.2.	Sistema LAT	16
4.3.	Sistema SECU	22
5.	ACTIVIDADES A DESARROLLAR	24
5.1.	Generación automática de TLVs de configuración de tarifas sistema BIT.	24
5.2.	Supervisión SECEBIT	26
5.3.	Supervisión evolución hacia la Virtualización	29
6.-	Equipo técnico	34
7	CONDICIONES GENERALES	34
7.1	Introducción.	34
7.2	Dirección del proyecto.	35
7.3	Seguimiento y control en la ejecución de trabajos.	36
7.4	Carácter llave en mano.	36
8	GLOSARIO DE TERMINOS	37
9	ANEXO: TLVs NECESARIOS	40

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE “SUPERVISIÓN Y COORDINACIÓN DE LA ADAPTACIÓN DEL SISTEMA BIT, SECEBIT, LAT y SECU”

1. ANTECEDENTES

Desde al año 2018 todos los títulos de transporte público de competencia del Consorcio Regional de Transportes Públicos Regulares de de Madrid (en adelante Crtm) se encuentran ya incluidos en el sistema de billeteaje a través de tarjeta sin contacto, ya sean títulos de carácter personales (TTP), o bien anónimos (tarjeta Multi).

Ello quiere decir que han desaparecido todos los anteriores modelos físicos que soportaban los diversos títulos de transporte existentes, existiendo ahora mismo una base tecnológica que permite que en un único soporte físico (tarjeta sin contacto) puedan introducirse todos los títulos de viaje existentes. Y que toda la información asociada a ellos, si bien a través de ese soporte físico, sea tratada telemáticamente.

No obstante, la evolución en el tratamiento de los soportes físicos (tarjetas) ya sea para este tipo de títulos u otras actividades, como las típicamente bancarias, señala que no solo se está diseñando una forma más sencilla de agrupar servicios a través de tarjetas de plástico si no que, en definitiva, se plantee la sustitución, o al menos la coexistencia, de tales elementos físicos con la existencia de tarjetas virtuales, habitualmente insertadas en dispositivos de comunicación móviles (smartphones).

Desde el organismo CRTM se han estudiado posibilidades ampliar los mecanismos puestos a disposición de los usuarios del transporte público, de manera que puedan contar con sistemas alternativos a la tarjeta física, posibilitando la futura puesta en funcionamiento de tarjetas virtuales, que almacenen, con las mismas condiciones de seguridad, la información que ahora mismo es depositada en tales tarjetas, permitiendo con ello el acceso al sistema de transporte a todos los usuarios que utilicen tales medios sin necesidad de contar con un soporte físico (tarjeta) sino mediante la integración de todas las características y utilidades de ese soporte en un dispositivo de telefonía móvil (Smartphone).

2. OBJETO

Como se ha mencionado, la continua evolución de las tarjetas (en este caso, en particular, las de transporte público) continúa ahora con las posibilidades que ofrece la

telefonía actual, mediante los dispositivos conocidos como Smartphones, hacia la virtualización (sin descartar otras alternativas que coexistan).

El objeto de este documento es establecer el alcance y las condiciones de carácter técnico que han de regir la contratación por Procedimiento Abierto de los trabajos necesarios para la “COORDINACIÓN DE LOS PROCESOS DE VIRTUALIZACIÓN DE LA TARJETA DE TRANSPORTE DEL CRTM”. También es objeto de este documento definir los procedimientos de ejecución y seguimiento de los trabajos contemplados.

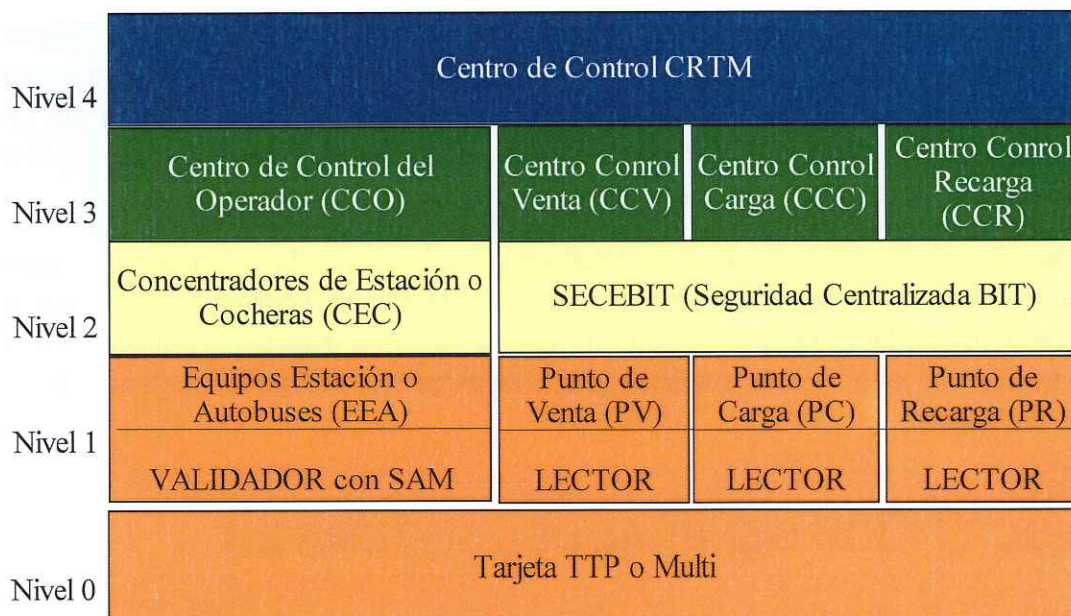
Todas las actividades a desarrollar, detalladas en el epígrafe 5, son necesarias para alcanzar la virtualización de tarjetas de transportes sobre teléfonos móviles. Es decir, que el teléfono pueda comportarse también como una tarjeta física de transporte público, con la que será posible acceder a los servicios de transporte de cualquier operador de la Comunidad de Madrid.

3. DESCRIPCIÓN GENERAL DEL SISTEMA BIT

El sistema BIT (Billeteaje Inteligente del Transporte) es la evolución del sistema basado en billetes magnéticos hacia sistemas basados en tarjetas sin contacto, ya sean estas últimas físicas o virtuales. Este aparente simple cambio de soporte ha supuesto profundos cambios técnicos y funcionales en todos los niveles del transporte público de la Comunidad de Madrid.

El sistema BIT concibe la tarjeta sin contacto como un contenedor de títulos de transporte, cuyo chip contiene toda la información necesaria que permite operar directamente con dispositivos de validación, carga e inspección. Previamente, las tarjetas han requerido de las fases de pre-personalización y personalización

Para explicar el flujo de información entre el CRTM y cualquier otro actor nos hemos centrado por simplificar, en operadores de transportes, pero con cualquier otro actor el proceso es similar. El intercambio de información se realiza en ambos sentidos. Cuando se detecta la tarjeta en los validadores hasta que llega a la autoridad de transportes, es decir, al Consorcio Regional de Transportes de Madrid (CRTM).



El usuario entra en el operador de transportes y sitúa la tarjeta sin contacto (ISO 14443-A) sobre la antena del validador; esta es una operación muy rápida, del orden de milisegundos. En este instante se activa el proceso que consiste en la comprobación de que al menos uno de los títulos que residen en la tarjeta sin contacto es válido en dicho instante. Este proceso se realiza enviando tramas de información por radiofrecuencia, (aclaramos que no se envían datos personales, ya que ni siquiera existen en el interior de la tarjeta). Independientemente del resultado del envío y/o recepción de tramas por radiofrecuencia, se genera un registro de la operación, al que llamaremos registro de validación o transacción. Este registro de validación, que es firmado digitalmente por el dispositivo de seguridad (SAM), incluye, entre otros datos; el número de serie de la tarjeta, el resultado de validación, la fecha y hora. El proceso descrito forma parte del nivel 0/1.

Cuando el validador o el subconcentrador (concentrador de validadores de una batería o vestíbulo) puede comunicar con el concentrador (nivel 2) le envía todos los registros de validación. Todos los concentradores de estación o cocheras envían sus registros al centro de control del correspondiente operador de transportes (CCO, nivel 3)

Para la transmisión de la información de validación entre el nivel 3 (CCO) y el nivel 4 (CRTM) se elegirá una ventana de tiempo que garantice la velocidad de transmisión de los procesos, normalmente en modo nocturno, aunque pueden darse comunicaciones diurnas. El canal entre el nivel 3 y 4, es seguro, pues se ha utilizado FTP sobre SSH. Por este canal, se transmitirán desde el nivel 3 al nivel 4 toda la información correspondiente a los registros de validación generados en los operadores de transporte a lo largo del día. Por otro lado, el

CCO descargará del CRTM la información necesaria para actualizar su sistema. La información que genera el CRTM es de naturaleza muy diversa; tarifas, configuraciones, listas de tarjetas no permitidas, etc...

Cuando el operador en conexión, comprueba que hay una nueva lista de tarjetas no permitidas procederá a descargarla; una vez recibido en su sistema verificará la firma electrónica de la lista para autentificarla e inmediatamente, el operador distribuirá la lista de tarjetas no permitida por su red, es decir, enviando cada fichero desde el nivel 3 al 1, por lo tanto, llegando hasta cada validador del operador. Así, por ejemplo, si el CRTM genera una lista en la que una nueva tarjeta sin contacto ha sido incluida, el operador detectará el cambio y actualizará su lista a nivel 3 para después transmitirla al nivel 2. Cada concentrador de estación (nivel 2) enviará la nueva lista a los distintos subconcentradores, transmitiendo esta información a todos los posibles equipos intermedios hasta que la reciban todos los validadores (nivel 1). De manera que, al día siguiente, cuando la tarjeta afectada intente entrar por cualquier operador de transportes se le denegará el acceso, ya que, el validador comprobará que la tarjeta está en lista no permitida informando de esta situación y bloqueando el paso.

Bloquear el acceso de una tarjeta a cualquier operador de transportes es una operación que prueba la capacidad defensiva del CRTM, mecanismo que se materializa en listas no permitidas de tarjetas. Esto es, una relación de tarjetas no admitidas.

Como se ha dicho, los operadores envían información de validaciones al CRTM, pero también lo hace los fabricantes de tarjetas, la red de ventas y también la red de carga/recarga. Todas estas fuentes de información alimentan a una base de datos (BBDD) donde se registra cada número de serie de cada tarjeta. Es decir, se dispone de una BBDD actualizada donde figuran todas las tarjetas que ha vendido el CRTM. De manera, que cualquier tarjeta que haya accedido a cualquier operador debe figurar en la BBDD del CRTM. En caso de que algún actor pusiera alguna tarjeta en circulación sin autorización del CRTM la tarjeta quedaría bloqueada en menos de 48 horas por el sistema.

Hablar de seguridad en el Sistema BIT implica hablar de la seguridad inherente a la tarjeta sin contactos TTP y/o Multi, de la seguridad en la custodia de las claves y de la seguridad de las comunicaciones e información de transacciones (como ya hemos explicado).

Todo el esquema de funcionamiento y seguridad de las tarjetas sin contacto (ya sean o Multi), se ha implementado sobre el modelo de chip DESFire (propiedad intelectual de la entidad NXP). Este chip incorpora mecanismos de seguridad que se basan en tres pilares, cuales son:

- Número de serie único (garantizado por el fabricante)
- Generador de números aleatorios FIPS 140-2
- Algoritmo criptográfico triple DES (3DES) y AES

Como norma general, cada vez que se accede a la TTP o Multi, ya sea para realizar una lectura o una escritura, es necesario un proceso de autenticación. El proceso de autenticación usado por las tarjetas del CRTM es el denominado como AUTENTIFICACIÓN MUTUA EN TRES PASOS que es el de mayor seguridad que soporta el DESFire. En el sistema BIT este modo se mejora con la seguridad añadida de dispositivos de seguridad como son SAM (Security Access Module) y/o HSM (Host Security Module). Estos módulos de seguridad son elementos de custodia de claves, que además incorporan comandos especiales de seguridad, con una propiedad tremendamente interesante, que es la de no permitir en ningún caso que las claves salgan del dispositivo, aunque internamente se opere con ellas para obtener la clave de sesión, que sí se entrega al lector, para acceder a un determinado fichero en un momento determinado.

Antes de comenzar el proceso de autenticación, hay que realizar algunas tareas previas:

- Cuando una tarjeta TTP o Multi, entra en el campo magnético del lector, se le induce una corriente que activa la tarjeta y responde con su número de serie. El lector recibe este dato y se lo reenvía al dispositivo de seguridad. En este momento todos los dispositivos están preparados para trabajar con la tarjeta.
- El programa del lector necesita leer o escribir en un determinado fichero, pero lo único que conoce es el índice de la clave que utilizará, es decir, solo conoce la posición de las claves únicas que tiene cada tarjeta. El lector le comunica a la tarjeta y al dispositivo de seguridad algo del estilo “vamos a trabajar con la clave 5”. En definitiva, el lector coordina el trabajo, pero no entra en los detalles.

Una vez establecido el índice de la clave con la que se va a trabajar, comentamos el proceso de autenticación que explicamos de forma general. La tarjeta TTP o Multi genera un número aleatorio (mediante FIPS 140-2) y lo cifra con el algoritmo 3DES utilizando el valor de la clave del índice, que conoce la tarjeta TTP o Multi. Todo esto, cifrado, se envía al programa del lector como primer paso. Pero el lector no conoce clave alguna y no entra en esos detalles (el CRTM no desea que los integradores conozcan las claves) y por esto se lo reenvía al dispositivo de seguridad; a un SAM o a un HSM.

El dispositivo de seguridad, internamente, descifra el dato al que aplica una serie de operaciones para generar un segundo dato y también otro nuevo número aleatorio.

Finalmente se cifra la concatenación de ambos números con la clave que indica el índice y el resultado se envía al lector. El lector hace eco de esta información hacia la TTP o Multi. Ahora la tarjeta descifra la información y obtiene ambos números. Si la tarjeta TTP (o Multi) comprueba que uno de ellos, después de deshacer las transformaciones necesarias, es el número original que envió, entonces significa que el otro extremo conoce su clave para trabajar. Este es el segundo paso.

Seguidamente la tarjeta TTP (o Multi) hace una serie de transformaciones al número que generó el dispositivo de seguridad y lo cifra con 3DES: este es el paso 3 y último. El dato cifrado se envía al lector que a su vez lo reenvía al dispositivo de seguridad. El dispositivo de seguridad comprueba si este número aleatorio es el número que él generó en el paso 1, pero previamente tiene que transformarlo. Si esto es así, queda autenticado el otro extremo también y el dispositivo de seguridad proporciona al lector la clave de sesión.

El sistema BIT es también un generador de datos. Cada proceso asociado a la vida de las tarjetas del CRTM (prepersonalización, personalización, carga, validación e inspección) genera una o varias transacciones que se envían al SID (Servidor de Intercambio de Datos) y que es procesado mediante el SPAI (Sistema de Procesamiento Automático de Información). El gran volumen de datos recibido se ha formalizado en un enorme modelo de datos en BBDD relacional, que a su vez, en la actualidad, alimenta a GBIT, herramienta que permite resolver cualquier problema a los usuarios de la TTP y Multi, y que se utiliza en la Oficinas de Gestión (OOGG) del CRTM.

4. DESCRIPCIÓN DE SECEBIT Y LAT-SECU

4.1. SECEBIT

En el año 2006, CRTM decidió la utilización de un sistema de seguridad centralizado para la gestión del sistema BIT (SECEBIT) con los niveles de seguridad que la tecnología a utilizar requería.

La implantación del sistema se configuró con una arquitectura distribuida de servidores criptográficos dotados de HSM (Hardware Security Modules) dedicado a la realización de procesos de gestión, almacenamiento de claves de seguridad, y operaciones de criptografía sobre determinados mensajes utilizados en el diálogo transaccional con las tarjetas sin contacto.

SECEBIT generara todos los TLVs (de todos los actores y de todos los procesos, excepto validación); estos TLV se envían al SID, donde el SPAI los procesa y comprueba que la firma digital de dichos TLVs es correcta.

Subsistemas de HSMs

El subsistema HSM se constituye en el elemento clave de seguridad para las operaciones de carga y recarga de la tarjeta de transportes de CRTM. Este subsistema va a disponer del conjunto de claves preciso para llevar a cabo, de forma segura, todas las operaciones de autenticación e intercambio, así como la firma de las operaciones.

Sobre la base de un HSM y con el fin de adaptarse a los requerimientos concretos de BIT, se ha creado una arquitectura software alrededor del HSM que se ha venido en denominar SECEBIT.

En concreto, los subsistemas HSM disponen de los siguientes niveles de software:

Software embebido en el dispositivo “tamper proof”. En este nivel se han creado un conjunto de comandos específicos. Estos comandos realizarán las operaciones seguras a bajo nivel del sistema.

El HSM usado en SECEBIT es enlazado por la aplicación usando un diálogo estandarizado PKCS#11, con la excepción de los comandos que, debido a su funcionalidad, requieren de un entorno de ejecución más seguro, condiciones que se cumplen en el interior del propio núcleo HSM. Este conjunto de comandos que han de ser embebidos dentro del propio HSM, son cargados en éste en forma de *FM*; un FM es un *Firmware Module*, es decir, un módulo binario que contiene código ejecutable, en este caso, los comandos concretos orientados al billeteaje del CRTM.

SECEBIT ofrece las siguientes prestaciones:

Todos los datos manipulados por los comandos permanecen completamente seguros, a diferencia de lo que ocurriría si se ejecutasen en el propio PC. El HSM cumple con el estándar FIPS 140-2 nivel 3.

El tiempo de ejecución disminuye sensiblemente, debido a que el número de llamadas al HSM es menor, todo el comando se resuelve en una única llamada.

- El HSM cuenta con medidas especiales de seguridad que evitan que el uso de un FM pueda presentar una brecha de seguridad, éstas son:
- Modo *Tamper Before Upgrade*, implica que cualquier intento de cargar un nuevo módulo con comandos o de actualizar el firmware del núcleo HSM, dará como resultado la reinicialización del mismo y con ello el borrado de todo el material criptográfico almacenado.

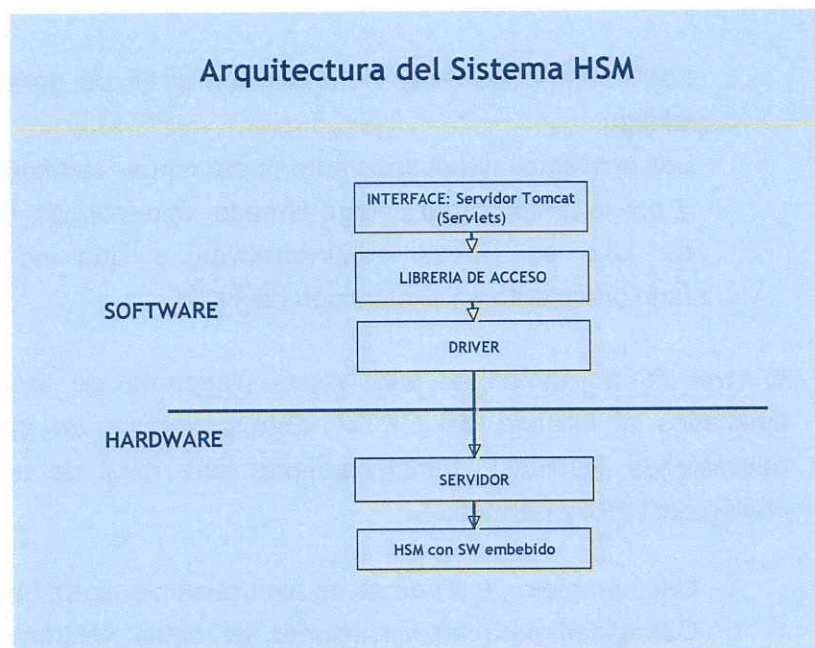
- Los FM's deben estar firmados con el fin de garantizar la autenticidad del código.
- Los privilegios necesarios para poder cargar certificados confiables en el HSM y por lo tanto cargar código firmado, depende del PIN del SO, PIN que sólo se usa en tareas administrativas y que no es requerido para el funcionamiento en explotación del HSM.
- A nivel de aplicación, el subsistema dispondrá de la aplicación de comandos asociados al billeteaje del CRTM. Esta aplicación se ejecuta en el servidor de aplicaciones TOMCAT. Funcionalmente este nivel de aplicación conecta con el núcleo del HSM y permite:
 - Uso completo de sistemas de almacenamiento de base de datos.
 - Capacidad para actualizaciones de datos síncronas y asíncronas. Permite trabajar regularmente con actualizaciones síncronas de datos, en caso de que se requiera disponer de datos en tiempo real. Mediante configuración puede disponerse las actualizaciones de los datos en segundo plano, que supone cierto retardo, pero asegura la máxima velocidad en la disposición de cargas/recargas.
 - Serialización de transacciones en disco, lo que permite almacenamiento y guardado en diferido de los datos sin interrupción del servicio.
 - Identificación de accesos. Es posible asignar un identificador a cada elemento que requiera conectarse con el sistema SECEBIT, para facilitar la auditoría del sistema.
 - Control de accesos por número IP.
 - Gestión de listas negras, configuradas en base de datos y cacheadas regularmente en memoria.

Gráficamente la arquitectura del subsistema es la siguiente:



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES,
MOVILIDAD E INFRAESTRUCTURAS



El detalle de comandos actualmente soportados es el siguiente;

COMANDO	parámetros	
	entrada	Salida
InitOperation	id	CodResponse
	rol	Jsessionid
		OperationNumber
		HsmSerial

Diversificación de una
clave de una tarjeta

COMANDO	parámetros	
	entrada	Salida
GetDiversifiedKey	SerialNumber	CodResponse
	KeyIndex	KeyDiversified

Diversificación de todas
las claves de una tarjeta

COMANDO	parámetros	
	entrada	Salida
GetAllDiversifiedKey	SerialNumber	CodResponse KeyDiversified0 KeyDiversified1 KeyDiversified2 KeyDiversified3 KeyDiversified4 KeyDiversified5 KeyDiversified6

Conceder clave de sesión DESFire. 1ª parte. Generar
claves

COMANDO	parámetros	
	entrada	Salida
InitSession	SerialNumber RndB KeyIndex	CodResponse RndABgCif SessionKeys VersionLNS

Conceder clave de sesión DESFire. 2ª parte. Autenticar clave

COMANDO	parámetros	
	entrada	Salida
InitSession	RndAprima	CodResponse

Transacción firmada

COMANDO	parámetros	
	entrada	Salida
DoMac	Data Tlv	CodResponse Mac OperationCounter TransacCounter TransaccControl CipherString

Recientemente y en sucesivas versiones del sistema se han actualizado comandos como muestra la siguiente tabla;

Nivel implementacion	Comando	soportado desde
tomcat	InitOperation	HSM20
nucleo	GetDiversifiedKey	HSM20
nucleo	GetAllDiversifiedKey	HSM20
nucleo	InitSession	HSM20
nucleo	DoMac	HSM20
nucleo	VerifyMac	HSM20
tomcat	VerifyAllMac	HSM21
nucleo	GetCupoValue	HSM20
tomcat	GetSubeTNumber	HSM20
tomcat	GetHSMNumber	HSM20
nucleo	DoDES	HSM20
tomcat	FinishOperation	HSM20
tomcat	GetAllCounters	HSM24

Además, se han incorporado las siguientes funcionalidades:

Funcionalidades	soportado desde	Adicio nalme nte el subsist ema HSM dispon e de las
Control de comandos por IP	HSM21	
Modo degradado	HSM22	
limitación acceso a contadores	HSM22	
TransacCounter	HSM23	
Logs Claves diversificadas	HSM23	
externalizar contadores	HSM24	

siguientes facilidades para la gestión integral del sistema:

- Facilidades necesarias para su integración en un sistema de telediagnóstico que permite una supervisión remota del estado de operación del subsistema.
- Facilidades para la telecarga segura desde un punto central.
- Facilidades para la telegestión del subsistema que permitan a CRTM disponer de información centralizada con información de operación, y estado de operación.
- Consolidación de información relativa a las operaciones gestionadas en un punto centralizado de la red de CRTM.

4.1.1 Subsistemas de balanceo de carga y alta disponibilidad

Con el fin de ofrecer un servicio de alta disponibilidad y balancear la carga entre los diferentes componentes, se ha diseñado desde su inicio un subsistema de reparto inteligente de carga que permite disponer de un entorno de reparto de carga en alta disponibilidad para el subsistema HSM en base a la carga real de cada HSM, esto es, el criterio de reparto de operaciones es la carga REAL de cada uno de los HSMs.

Este sistema incluye un software desarrollado sobre la base del Apache mod_jk, que permite la medida instantánea de la carga en cada uno de los módulos de seguridad adscritos al sistema. Estos módulos a partir de la información de carga real e instantánea permiten encaminar la operación hacia el módulo con menor nivel de carga.

SECEBIT se ha diseñado tomando en consideración el previsible crecimiento que a futuro experimentará como consecuencia de una más amplia difusión de la tarjeta sin contacto y tarjetas virtuales, así como de un mayor acceso a servicios de interés.

En este sentido si SECEBIT hubiera de incrementar su capacidad, su crecimiento puede gestionarse a través de diferentes alternativas;

- La primera de ellas es obviamente la de incrementar el número de sistemas SECEBIT.
- La segunda de ellas es mantener el número de sistemas SECEBIT e incrementar la capacidad de proceso criptográfico incrementando el número de HSM contenido en el subsistema HSM.
 - La posibilidad de crecimiento siguiendo esta estrategia es amplia, limitada únicamente por las capacidades del sistema de balanceo y con la particularidad de que el crecimiento en capacidad de procesamiento es lineal respecto al incremento de subsistemas HSM.
- La tercera de ellas es la de incorporar mayor número de núcleos HSM en cada uno de los HSM's. Es importante tomar en consideración que por defecto y en la configuración de partida cada HSM incorpora un solo núcleo HSM.
 - La posibilidad de crecimiento siguiendo esta estrategia es limitada en tanto que la forma de operar de los núcleos HSM hace que cuando trabajan en estas configuraciones sólo incrementen su rendimiento en aproximadamente un 10-20% por cada núcleo añadido al sistema y con la limitación de espacio en servidores se hace poco práctica.

4.1.2. Subsistemas de registro de operaciones de HSMs.

Con el fin de disponer de la información agregada de las operaciones gestionadas por cada uno de los sistemas SECEBIT se dispone de un subsistema centralizado de registro de transacciones. Es importante reseñar que este sub-sistema no forma parte intrínseca de SECEBIT, pero es también importante resaltar el hecho de que sin su participación la información generada puede no llegar a agregarse correctamente. La información que se agrega en este punto consta de la información de operaciones de carga / recarga, prepersonalización, personalización e inspección.

TABLA DE REGISTRO DE TRANSACCIONES FIRMADAS

Column Name	Data Type	Nullable	Default	Primary Key
IDLOGGENERAL	NUMBER(21,0)	No	-	1
CONTRANSACCION	NUMBER(20,0)	No	-	2
IDTLV	CHAR(2)	No	-	3
TXCABECERA	VARCHAR2(38)	No	-	-
TXCUERPO	VARCHAR2(500)	No	-	-
TXFIRMA	VARCHAR2(8)	No	-	-
1 - 6				



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES,
MOVILIDAD E INFRAESTRUCTURAS



TABLA DE LOG DE LLAMADAS USO GENERAL

Column Name	Data Type	Nullable	Default	Primary Key
IDLOGGENERAL	NUMBER(21,0)	No	-	1
CONTGENERAL	NUMBER(20,0)	No	-	-
CONTOPERACION	NUMBER(20,0)	No	-	-
IDCOMANDO	CHAR(2)	No	-	-
TXIP	VARCHAR2(15)	No	-	-
TXIDPROCESO	VARCHAR2(20)	No	-	-
IDSERIEHSM	VARCHAR2(6)	No	-	-
FXEJECUCION	TIMESTAMP(6)	No	-	-
1 - 8				

La recomendación para la configuración en el punto central pasa por disponer de al menos dos instancias de forma que un fallo en la instancia maestra permita ceder el control a la secundaria y hacerse con esta con la IP flotante para comenzar a dar servicio. Dado que la coherencia de los datos está garantizada, la recuperación del sistema es completa.

Respecto al dimensionamiento realizado para este punto de agregación cabe decir que los cálculos de tamaño por transacción almacenada son los siguientes:

- Para carga/recarga de títulos: se realizan 11 accesos a claves, que se traducen en 11 llamadas al comando HSM de autenticación. Esto supone 64 bytes en tablas de log de uso (por llamada) y 148 bytes en la tabla de transacciones. En total: 768 bytes en logs y alrededor de 148 bytes por carga / recarga en los registros de transacciones.

Dado que es vital la recogida completa de todos los procesos de ventas en el sistema de almacenamiento centralizado, los sistemas SECEBIT incorporan capacidades de almacenamiento diferido a partir de la versión HSM20 del software.

Para paliar los problemas derivados de una falta de acceso a los sistemas de gestión de base de datos se ha diseñado un mecanismo de guardado de información que funciona desde el mismo momento en que la transacción es generada.

Si el sistema no es capaz de acceder al sistema de almacenamiento local, se genera la transacción en disco, y se reintentará el guardado periódicamente. De esta forma el sistema SECEBIT seguirá dando servicio ininterrumpidamente. Una vez recuperada la capacidad de almacenamiento, todas las transacciones en disco se almacenarán satisfactoriamente.

4.2. Sistema LAT

El sistema LAT es la capa de aplicación de transporte, orientada al billeteaje, incluye:

- Reglas operativas de billeteaje
- Perfiles de usuarios
- Tipos de títulos
- Combinaciones posibles perfiles de usuarios vs títulos
- Tarifas aplicables
- ...

Gestionando adicionalmente el ciclo de vida de la tarjeta sin contactos:

- Pre-personalizar tarjetas
- Personalizar
- Leer
- Cargar y recargar
- Realizar tareas de inspección

Técnicamente el servidor LAT está desarrollado de forma que expone un conjunto de servicios (APIs) a modo de invocaciones HTTP usando los métodos GET o POST, enviando las variables requeridas en cada servicio como `application/x-www-form-urlencoded` y recibándose igualmente las variables propias de cada servicio.

Esto es, lo que se intercambia en ambas direcciones es un conjunto de variables con sus respectivos valores. Ejemplo de petición GET al LAT:

Petición al LAT

GET /LAT2/Servicio?variable1=valor1&variable2=valor2

Respuesta del LAT

variable1=valor1\n variable2=valor2

La respuesta es servida usando `Content-Type: text/plain; charset=UTF-8` y dependiendo de la versión HTTP que emplee el cliente, el contenido de la respuesta anterior puede ser codificado como `Transfer-Encoding: chunked`.

Si el cliente lo permite, el servidor emplea Keep-Alive en las conexiones, esto es, no cierra el socket entre dos invocaciones, usándola para la siguiente conexión, lo que redundará en una mayor velocidad en el intercambio de datos.

El cliente debe soportar el uso de cookies en las comunicaciones, ya que, alguno de los servicios del LAT necesitan mantener una sesión HTTP.

Servicios expuestos por la plataforma LAT

Por defecto, los servicios expuestos por el servidor LAT, son en la actualidad los siguientes:

- Servicios para la lectura de una tarjeta.
- Servicios para la consulta de saldo.
- Servicio de listado de títulos, genérico y de tarjeta.
- Servicios para carga de títulos a partir del id del título.
- Servicios de actualización
- Servicios de gestión del LAT.

En todos estos servicios el LAT opera con una misma sesión que se establece en el primer comando de lectura de tarjeta.

Como ejemplo de Clientes que pueden hacer uso de estos servicios, están los terminales de lectura y las máquinas de venta de cualquiera de los operadores conectados a LAT:

Terminales de lectura:

- Primero invocan el servicio de lectura
- Finalmente, el servicio de consulta de saldo.

Terminales de venta:

- Primero invocan el servicio de lectura
- Seguidamente el servicio de actualización.
- Seguidamente el servicio de consulta de saldo
- Seguidamente el servicio de listado de títulos.
- Finalmente, el servicio de carga de título.

Lectura de la tarjeta

Es el servicio encargado de proveer los comandos necesarios para leer la tarjeta, debe ser siempre el primero de los servicios a usar, antes de poder realizar cualquier otro tipo de operación con la tarjeta.

Este servicio proporciona el conjunto de comandos que en función de la tecnología utilizada sean necesarios para hacer una lectura completa de una tarjeta TTP o Multi.

La obtención de comandos para la lectura requiere la URL:
/LAT2/GeneraComando

Consulta de Saldo

El servicio de consulta de saldo permite obtener para una determinada tarjeta, una interpretación del contenido de la misma, expresada en forma de un conjunto de variables y valores sobre distintos aspectos de la tarjeta.

La URL para la consulta de saldo es:
/LAT2/MuestraSaldo

Carga de títulos mediante prepago.

LAT permite operar un servicio de carga de títulos mediante prepago. Para ello dispone de un punto de servicio en el que se realiza una consulta al webservice de CTRM y obtiene una lista de los títulos disponibles.

Seleccionar un prepago y proceder con la carga del mismo. Inicia el diálogo entre la tarjeta y el LAT para realizar toda la lógica asociada a la carga de un título.

Carga de Títulos

Mediante esta operación se permite cargar un título en la tarjeta.

a.- Listado de títulos posibles a cargar en la tarjeta.

El LAT evalúa la tarjeta y en base a los posibles títulos que tiene configurados, genera una lista con los que pueden ser cargados.

b.- Carga de un título en la tarjeta.

Carga un título de la lista anterior en la tarjeta, el título es identificado por su código.

Servicio de listado de títulos

La URL de este servicio es
/LAT2/ListaTitulosCarga

Este servicio funciona de dos formas distintas dependiendo de la forma en la que sea invocado, el objetivo es proveer un listado genérico de títulos sin necesidad de operar sobre una imagen de tarjeta, es decir, sin necesidad de haber realizado una lectura previa de tarjeta alguna. Lógicamente los títulos devueltos en una consulta genérica están sujetos a los datos proporcionados en la invocación al servicio, no a los datos recuperados de una tarjeta específica tras su lectura, por lo que el resultado de una carga posterior no se puede garantizar.

Obtención de comandos para cargar un título

La URL del servicio es:
/LAT2/CompraTituloById

El servicio de carga de títulos opera de la misma forma que el servicio de lectura de la tarjeta, es decir se trata de recibir e inyectar a la tarjeta un conjunto de comandos, que se suceden hasta que el LAT indique que se ha concluido

Actualización de la tarjeta de transporte:

El servicio de actualización permite al LAT realizar cambios en caliente en una tarjeta o título de transporte. Un ejemplo puede ser un cambio del fichero de Personalización, FEap, debido a la entrada en vigor de nuevos títulos de viaje y hacerlo de forma transparente para el servicio.

La URL del servicio es:

/LAT2/Update

Este servicio debe usarse justo después de invocar al servicio de lectura.

El servicio funciona de la misma forma que la lectura de la tarjeta (/LAT2/GeneraComando) o la carga (/LAT2/CompraTituloByld). Es decir, se ha de invocar mientras el STATUS sea AF y debe terminar con un STATUS 00.

Gestión del LAT

El servicio de gestión del LAT se encarga de actualizar en memoria los ficheros que se hayan descargado del sistema de intercambio con operadores o manualmente y/o provee una forma de recargar todos los ficheros (incluyendo los XML de configuración) en caso de modificación, para ello provee el siguiente punto de servicio:

/LAT2/CargaInicial

Servicio de trazas

El servicio de trazas proporciona un punto único de recepción de alarmas para todos los terminales que se conectan con LAT. Estos terminales pueden ser atendidos o desatendidos, e ir orientados a servicios de lectura de saldo, personalización, servicios de carga/recarga o servicios de inspección.

Estas alarmas pueden ser recogidas por un sistema de monitorización (Nagios o similar) y pueden ser informadas de forma dinámica a una lista de distribución de eventos.

Servicio de Gestión de stock

Una de las funciones proporcionadas por el sistema, es la de controlar y gestionar los lotes de títulos o tarjetas que se asignan a cada operador y a cada punto de venta.

Mediante la administración Web se permite el alta de lotes de títulos-tarjetas y su asignación a operadores y/o terminales concretos.

La administración permite definir acciones automatizadas a partir de un umbral o del punto de ruptura definido para cada red u operador.

Servicio de gestión de redes de venta

La plataforma LAT permite gestionar y dar de alta redes de venta de títulos en el sistema. Cada una de las redes y cada uno de los puntos de venta en cada red puede disponer de un identificador de grupo o individualizado.

La variable con la que el sistema gestiona los puntos de venta (o grupos de puntos de venta) es;

TDSALEPOINT.

Identificador del punto de venta que realiza la llamada, este identificador es asignado por el administrador del sistema LAT y consta de 6 bytes ó 12 caracteres hexadecimales.

Devuelve como variables de salida:

STATUS. 00 indica que todo fue bien.

EXISTE. Indica con S ó N, si el punto de venta existe.

El resto de las variables dan información del punto de venta:

RED

ESTABLECIMIENTO - OPERADOR

TELEFONO

DIRECCION

NIF

WEB

HORARIO

RECIBO

Servicio de gestión de app's y terminales

Servicio de gestión de Pago

Como se puede observar en los parámetros necesarios para realizar una operación de carga, existe un argumento nombrado como OTP (One Time Password), su cometido es proteger este tipo de operaciones, evitando que estén disponibles de forma abierta para cualquiera que invoque el servicio LAT en operaciones de carga.



**Comunidad
de Madrid**

CONSEJERÍA DE TRANSPORTES,
MOVILIDAD E INFRAESTRUCTURAS



La obtención del OTP ha sido vinculada a la realización del pago, de esta forma se consigue independizar el proceso de pago, de lo que es puramente la lógica de carga de la tarjeta de transporte. Dado el carácter heterogéneo de los interfaces con los que opera cada servicio de pago, se ha optado por añadir un servicio de obtención de OTP, vinculado a cada uno de ellos. El cometido de cada uno de estos servicios de obtención de OTP, es comprobar las credenciales de la transacción de pago, preguntando directamente al servicio a través del cual se realiza el pago y generando el OTP. Dando la operación por buena, sólo cuando se tiene constancia de que el pago con las credenciales suministradas ha sido realizado y además el tiempo transcurrido entre el pago y la invocación a este servicio, no excede un tiempo configurado.

Todos ellos usan HTTP/HTTPS como medio para realizar la llamada y obtener el OTP, en concreto realizan un GET/POST de las variables necesarias, funcionando de la misma forma descrita para los servicios del LAT al comienzo de este documento. Lo mismo ocurre con la respuesta, la cual sigue el mismo esquema descrito para el LAT.

Servicio de liquidación y ficheros de intercambio

La plataforma LAT prepara un conjunto de ficheros (TLVs) de forma periódica que envía al SID (Servidor de Intercambio de Datos) para su procesado por el SPAI (Sistema automático de procesado de información).

Así mismo a través del SID el LAT es alimentado con ficheros que CRTM ha generado para mantener sus;

- Títulos
- Perfiles
- Tarifas
- Listas
- ...

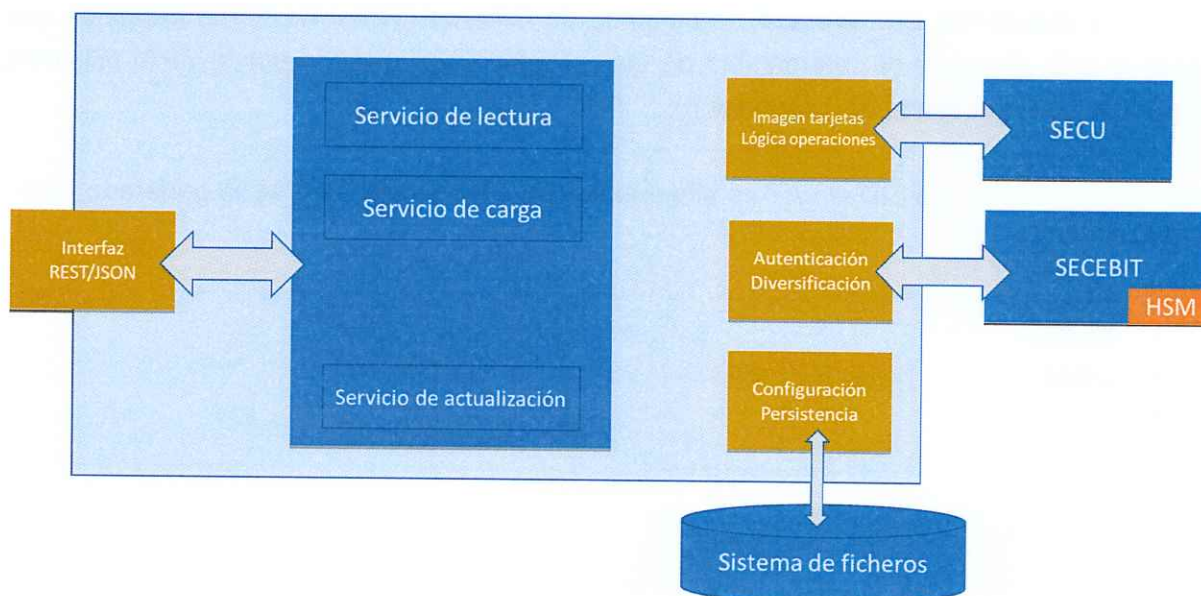
4.3. Sistema SECU

Si SECEBIT conoce como resolver la criptografía de la tarjeta, SECU conoce como se construyen los APDU's necesarios para leerla y escribirla, mientras que LAT conoce la estructura de los datos que contiene, lo que le permite interpretarla y operarla para realizar las operaciones que en cada caso apliquen, generalmente: pre-personalización, personalización, consulta de saldo, carga e inspección.

LAT-SECU está montado a partir de una aplicación Java 8, desplegada sobre un servidor de aplicaciones (Tomcat, Jboss, etc), cuenta como única dependencia su conexión con Cryptocard, la cual usa para poder resolver las autenticaciones que le permiten leer y escribir la tarjeta sin contacto y generar las transacciones que cada operación conlleva.

SECU Desfire. - permite construir los CAPDU's e interpretar los RAPDU's de la tarjeta sin contacto.

Una instancia típica del LAT podría ser:



En la figura anterior se muestra una instancia LAT + SECU genérica,

Por último, indicar que al igual que en el caso de SECEBIT y debido a lo crítico del servicio LAT, este se configura en los entornos de producción siguiendo un esquema de configuración igual al de aquel. Lo que aseguraría el balanceo de la carga y la alta disponibilidad. Ver figura con esta arquitectura para SECEBIT.

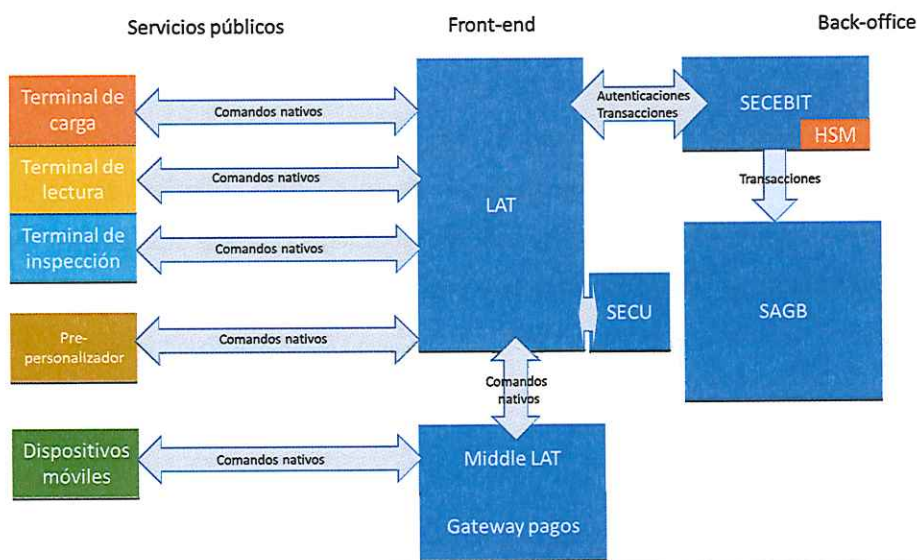
Configuración SECU

La lógica típica con la que opera suele definirse en base a ficheros de configuración en XML que permiten:

- Determinar los títulos con los que se puede operar y el conjunto de características que los definen.
- Determinar las tarifas aplicables a cada título en función del tipo de tarjeta, del colectivo y de los perfiles.
- Definir las aplicaciones activas en cada momento.
- Configurar listas negras por rangos de tarjetas.
- Configuración de distintas listas blancas, que permiten realizar acciones de mantenimiento e información sobre las tarjetas. Destinadas a aplicar actualizaciones sobre tarjetas que se encuentran en explotación y necesitan ser adaptadas, ya sea para corregir posibles problemas, para añadir nuevas funcionalidades o para informar al usuario sobre alguna cuestión.

Adicionalmente, LAT cuenta con herramientas de depuración tanto del propio LAT, como del sistema en su conjunto. Su activación permite tener un historial completo de las operaciones realizadas sobre una tarjeta, este historial se forma a partir de la imagen de la tarjeta antes y después de ser operada por el LAT, constituyendo una bitácora completa de la vida de la tarjeta.

Gráficamente el conjunto descrito se interrelaciona de acuerdo al siguiente esquema de operación:



5. ACTIVIDADES A DESARROLLAR

Los trabajos objeto de contratación se describen a continuación:

5.1. Generación automática de TLVs de configuración de tarifas sistema BIT.

La gestión de tarifas en el sistema BIT requiere la coordinación de TLVs en CARGA/RECARGA, VALIDACIÓN e INSPECCIÓN. De forma, que las fechas que establecen la entrada en vigor de las mismas en CARGA/RECARGA y los rangos de aceptación de tarifas en VALIDACIÓN e INSPECCIÓN deben ser coherentes. En caso contrario, las tarjetas son rechazadas.

La complejidad de la generación de tarifas se encuentra en que cada actor puede operar con un subconjunto de los títulos del CRTM sumado a títulos propios. Lo que implica, que cada actor tiene sus propios ficheros, y que todos los ficheros de todos los actores tienen que ser coherentes para que el sistema BIT funcione adecuadamente.

Se requiere que el adjudicatario implemente las siguientes funcionalidades, a nivel de comandos de órdenes en sistema operativo:

5.1.1 TLVs relacionados con carga/recarga

La venta de un título en carga/recarga necesita dos TLVs. El TLV B4 por actor del sistema BIT, es decir, por cada operador de transportes de la CCMM y redes de venta autorizados (ejemplo en el epígrafe ANEXO TLVs NECESARIOS) contiene las tarifas de cada título teniendo en cuenta los descuentos de perfil y colectivo, además de agrupación en familias.

Soporta tres cambios simultáneos.

El mapeo de fechas de etiquetas entre el XML del TLV B4h y el modelo de datos es el siguiente:



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES,
MOVILIDAD E INFRAESTRUCTURAS



ETIQUETA XML BBDD

<Fecha_Inicio_Venta> FECHA_INICIO_GARGA1
<Fecha_Cambio_Venta1> FECHA_CAMBIO_GARGA2
<Fecha_Cambio_Venta2> FECHA_CAMBIO_GARGA3
<Fecha_Fin_Venta> FECHA_FIN_ADMISION_VALIDA2

La interpretación de cuando aplicar una tarifa u otra es la siguiente:

ETIQUETA XML DESCRIPCION

<Tarifa_Venta_1> Entra en vigor cuando indica <Fecha_Inicio_Venta>
<Tarifa_Venta_2> Entra en vigor cuando indica <Fecha_Cambio_Venta1>
<Tarifa_Venta_3> Entra en vigor cuando indica <Fecha_Cambio_Venta2> y
finaliza <Fecha_Fin_Venta>

En el caso de que el CRTM no desee que el título se venda en la red pero si se quiera que se informe del SALDO, las fechas estarán caducadas.

Para su implementación se requiere modelado de datos e implementación (fuentes y ejecutables)

Para que los terminales de carga/recarga puedan incorporar en la tarjeta las propiedades de títulos hay que utilizar el TLV B5 (ejemplo en el epígrafe ANEXO TLVs NECESARIOS). Este fichero, es común para todos los actores del sistema BIT.

Esta tarea requiere un periodo **máximo de 45 días**

5.1.2 TLVs relacionados con validación e inspección.

La validación e inspección utilizan un TLV común. Se trata del TLV B3h por actor del sistema BIT, es decir, por cada operador de transportes de la CCMM (ejemplo en el epígrafe ANEXO TLVs NECESARIOS) que contiene las tarifas de cada título teniendo en cuenta los descuentos de perfil y colectivo. Soporta dos cambios tarifarios simultáneos y solapados.

Además, en INSPECCIÓN se dispone de otro TLV adicional. El TLV B2h que es común a todos los actores del sistema BIT (ejemplo en el epígrafe ANEXO TLVs NECESARIOS) permite conocer la descripción de un título a partir de su código hexadecimal. Este TLV es para que el terminal de inspección muestre al usuario inspector la descripción del título.

En Interurbanos se produce, además, la situación especial de “Prolongación de Recorrido”. Esto es básicamente la posibilidad que tiene un viajero de pagar un sencillo por el recorrido que exceda del título que porta. De manera, que el sistema requiere un TLV, que indique la diferencia que se debe cobrar al usuario (teniendo en cuenta el título validado de la tarjeta sin contactos) por prolongar el recorrido. El TLV que permite este cálculo es el TLV B7 que es común a todos los actores del sistema BIT (ejemplo en el epígrafe ANEXO TLVs NECESARIOS).

Esta tarea requiere un periodo **máximo de 30 días, respecto a la finalización del epígrafe 5.1.1.**

5.1.3 Puesta en producción.

El adjudicatario deberá proponer el conjunto de pruebas que deberá aceptar el CRTM para verificar el correcto funcionamiento.

Esta tarea requiere un periodo **máximo de 30 días, respecto a la finalización del epígrafe 5.1.2, teniendo en cuenta las correcciones necesarias que aparezcan durante la ejecución de la etapa de pruebas.**

5.2. Supervisión SECEBIT

Será necesario la supervisión en el desarrollo de los siguientes procesos:

5.2.1 Pruebas y control de calidad, sobre el software de particularización compatible SAM tipo 4

Este proceso requiere baterías de pruebas sobre la incorporación del SAM tipo 4 (retrocompatible con los SAM actuales: tipo 1, tipo 2 o tipo 3) como fuente origen del proceso, incluyendo las nuevas prestaciones, como, por ejemplo, familias de claves maestras. Este dispositivo afecta a la particularización de dispositivos PL600 y PL1500, ambos deberán evolucionar para soportar particularizar HSMs a partir de SAM tipo 4.

Se estima que esta tarea requiere un periodo aproximado de 30 días

5.2.2 Batería de pruebas sobre el aplicativo del Servidor Criptográfico

Se requiere la supervisión, y las pruebas, de una nueva versión del aplicativo del Servidor Criptográfico (SC) que se ejecuta sobre tomcat.

Los requisitos se resumen en la siguiente tabla:



**Comunidad
de Madrid**

CONSEJERÍA DE TRANSPORTES,
MOVILIDAD E INFRAESTRUCTURAS



Comando	soportado desde	Mejorado en	Descripción
GetAllDiversifiedKey2TDEA	HSM26		Obtiene todas las claves diversificadas de una tarjeta determinada usando 3DES y 2TDEA (timestamp) sólo para ReadTransKey. En base al SelectFamilyKey establecido
GetAllDiversifiedKeyEV2	HSM26		Obtiene todas las claves diversificadas de una tarjeta determinada usando AES. En base al SelectFamilyKey establecido
GetAllDiversifiedKey	HSM20	HSM26	se extiende la funcionalidad al SelectFamilyKey establecido
GetDiversifiedKey	HSM20	HSM26	se extiende la funcionalidad al SelectFamilyKey establecido
GetDiversifiedKey2TDEA	HSM25	HSM26	se extiende la funcionalidad al SelectFamilyKey establecido
InitSession	HSM25	HSM26	se extiende la funcionalidad al SelectFamilyKey establecido
InitSession2TDEA	HSM26		Conceder clave de sesión DESFire 2TDEA (timestamp), en tres partes. En base al SelectFamilyKey establecido controlando ROL INSPECCION
InitSessionEV2	HSM26		Conceder clave de sesión DESFire EV2 (AES), en tres partes. En base al SelectFamilyKey establecido controlando ROL INSPECCION
GetInfo	HSM26		Permite obtener la versión del software instalado y la versión del HSM
GetAllCounters	HSM24	HSM26	Mejorar la información solicitada, ordenado por IP- Contadores nucleo y fichero
Stop	HSM26		A partir de la ejecución de este comando el HSM no admite más InitOperation
listOperation	HSM26		Listar operaciones abiertas e Ips asociadas
SelectFamilyKey	HSM26		Selecciona el id de la familia de claves a utilizar
GetFamilyKey	HSM26		Permite conocer el identificador de la familia de claves que se está utilizando
Start	HSM26		Recarga cache y activa initOperation

Funcionalidades	soportado desde	Descripción
Versiones de TLVs	HSM26	
Servicio de recarga de cache	HSM26	para evitar reinicios, asociado al comando Start
familia de claves	HSM26	

Se estima que esta tarea requiere un periodo aproximado de **30 días**

5.2.3 Proceso de particularización on line

Hay que evolucionar el proceso de particularización, con el objetivo de evitar que el HSM deba ser enviado a CRTM para llevar a cabo la ceremonia de custodios y proceder a la carga de claves de producción. Este sistema será válido para sistemas HSM basados tanto en los ProtectServer PL600 de Safenet como en los ProtectServer PCIe de Gemalto (PL1500)

Esta evolución permitirá una gestión desde un panel central de control en CRTM del estatus de cada uno de los sistemas de seguridad desplegados en la red, así como de la versión de las claves disponibles en cada módulo de seguridad.

El adjudicatario deberá supervisar, tanto los desarrollos como las pruebas. Además de participar en las especificaciones

Se estima que esta tarea requiere un periodo aproximado de **45 días**

5.3. Supervisión evolución hacia la Virtualización

El adjudicatario deberá supervisar, pudiendo proponer mejoras, en las siguientes piezas de software: como es la virtualización del chip DesFire EV1 de NXP y la APP del CRTM de carga/recarga, teniendo en cuenta la PASARELA DE PAGO del CRTM.

El proyecto se separará en dos fases, que se ejecutaran tantas veces como versiones del producto:

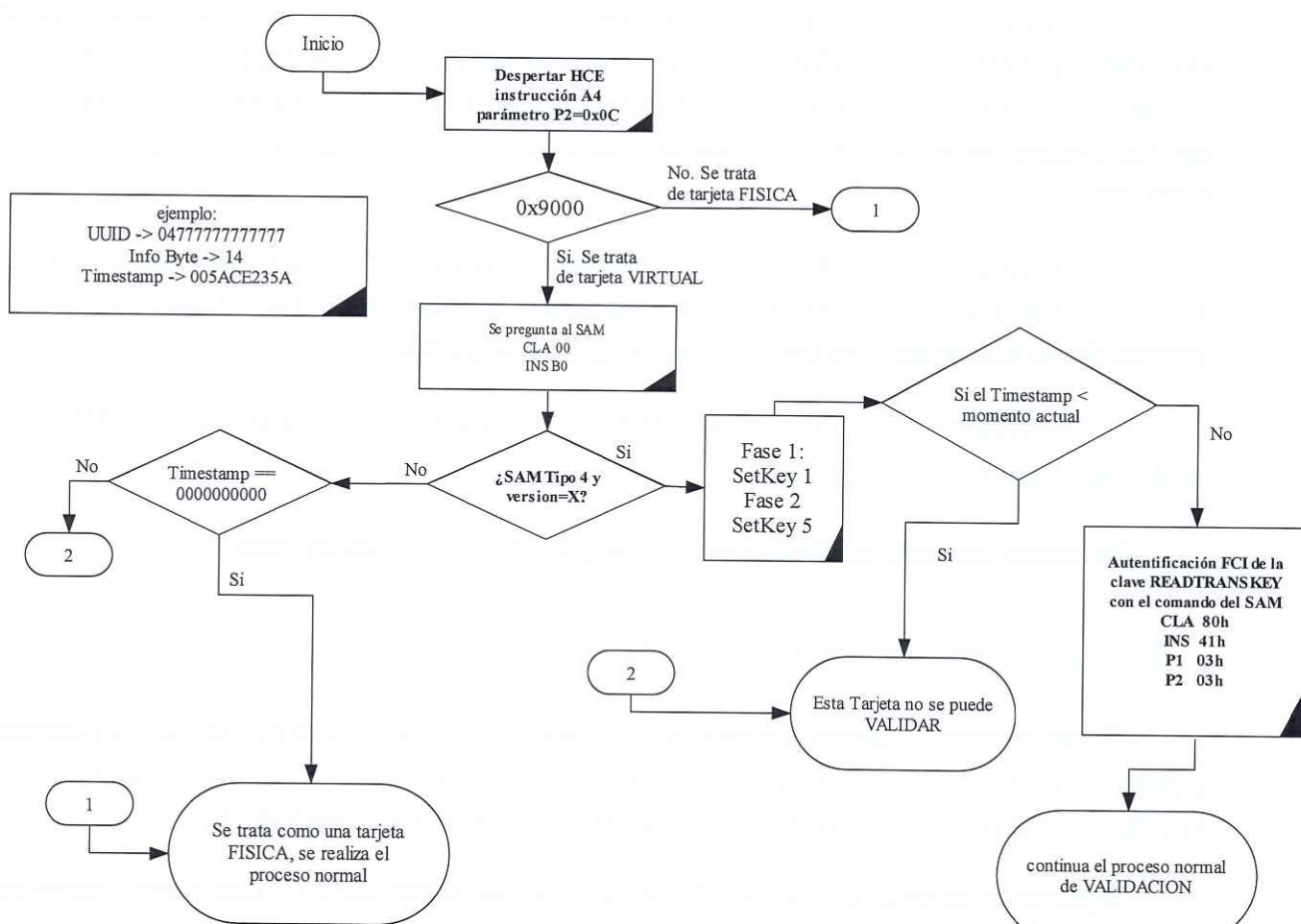
FASE 1

- A. Desarrollo producto: App piloto de tarjeta virtual
- B. Pruebas, si no cumple volver a A
- C. Puesta en producción

FASE 2

- A. Desarrollo producto: App tarjeta virtual
- B. Pruebas, si no cumple volver a A
- C. Puesta en producción

A.- Tanto el piloto (fase 1), como cualquier versión del producto final (fase 2), requerirá la implementación del siguiente flujo, por parte de los VALIDADORES/CANCELADORES.



NOTA: La versión X representa el número de versión, a partir de la cual, el SAM soporta la autenticación FCI

La estructura de la tarjeta virtualizada es idéntica 100x100 a la tarjeta física.

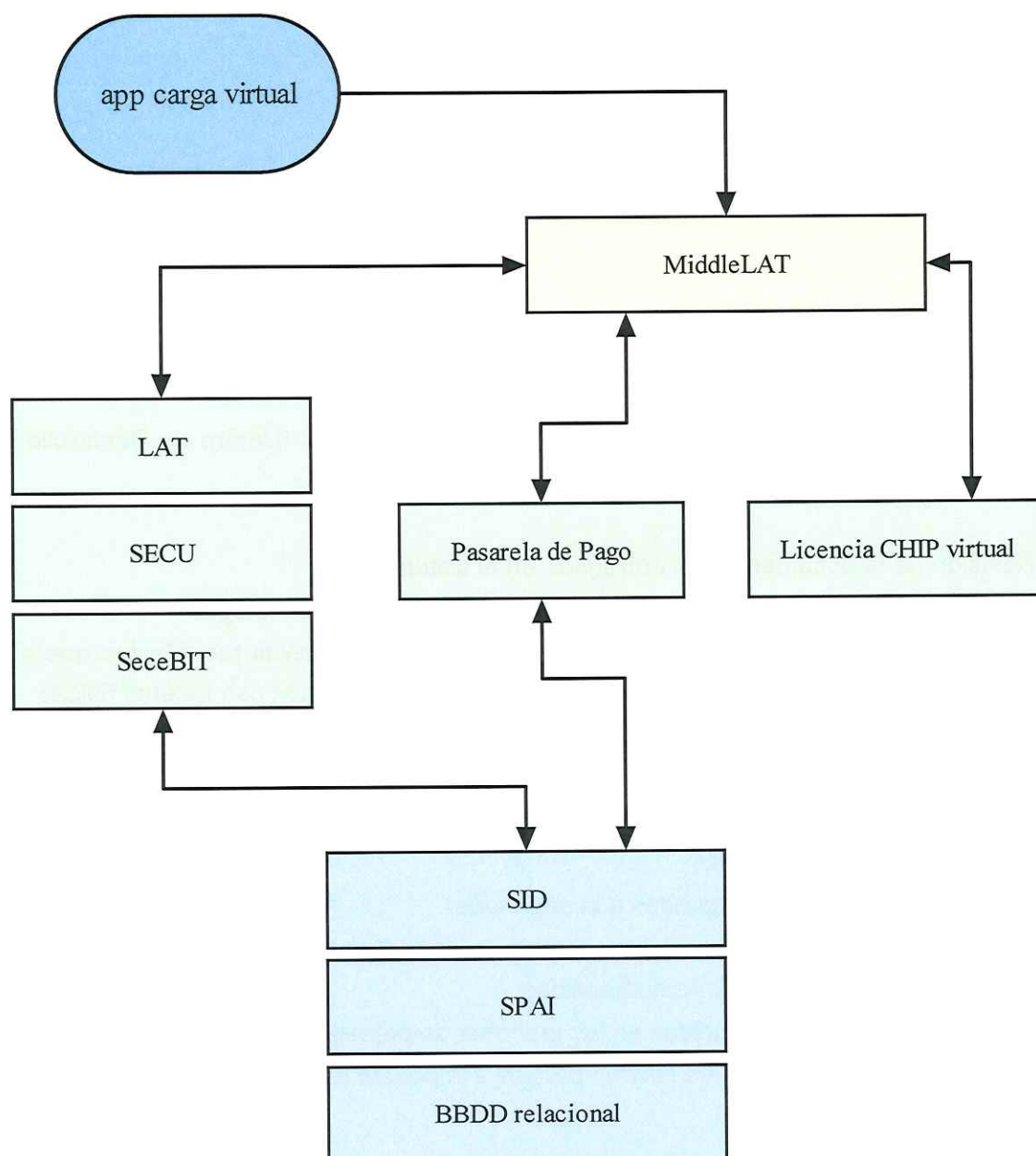
Los algoritmos utilizados en los distintos aplicativos (validación, inspección, carga/recarga) son idénticos a los definidos para las tarjetas físicas.

Las transacciones generadas son iguales en formato y contenido a las que se realizan con tarjetas físicas.

El número de serie de la tarjeta virtual se obtiene en el FCI

Se hace hincapié, en que para abordar la fase 2, es necesario disponer del setKey 5 en producción (tanto en SAM cómo en HSMs).

En cuanto a la arquitectura de la app de virtualización, requiere los siguientes bloques:



El MiddleLAT es un servicio que coordina todo el proceso de carga de un título, en la tarjeta virtual, de forma que tiene comunicación directa con todos los elementos que intervienen en el proceso, es decir con:

- LAT (que a su vez utilizará SECU y SECEBIT)
- Pasarela de pago
- Licencia CHIP Virtual
- App de carga en tarjeta virtual

El MiddleLAT permite gestionar con seguridad y garantías, las operaciones de devolución asociadas a problemas del proceso de carga.

B.- Las pruebas serán coordinadas por el adjudicatario, y abarcará, lo siguiente:

Para pruebas de los distintos industriales y actores BIT en el CDC (Centro de Desarrollo y Conformidad).

- Revisión de la documentación entregada en el sistema.
- Especificar las condiciones y entornos de pruebas de cada tecnología
- Definición de protocolos de pruebas funcionales de las nuevas tecnologías que se incorporen al sistema, usando el teléfono móvil en combinación con tarjetas físicas
- Supervisión, de la ejecución, de los protocolos de pruebas establecidos

En cuanto a los protocolos de pruebas integrados con el resto de tecnologías BIT.

- Pruebas extremo a extremo.
- Protocolos de pruebas orientados a la seguridad
- Protocolos de pruebas encaminados a verificar la fiabilidad de las tecnologías
- Protocolos de pruebas de interoperabilidad
- Análisis de los datos producidos en los entornos de pruebas
- Determinación de criterios de calidad previos a la puesta en producción.

En cuanto a los protocolos de pruebas de la app, se enfocarán con la batería de pruebas de la red de carga recarga, por tanto, se realizarán las siguientes pruebas:



**Comunidad
de Madrid**

CONSEJERÍA DE TRANSPORTES,
MOVILIDAD E INFRAESTRUCTURAS



- Interfaces de usuario
- Flujo de programa
- Consistencia de títulos
- Coexistencia de títulos
- Conformidad de valores dentro de rango
- Transacciones
- Formatos
- Integración con Pasarela de Pago
- Integración con BackOffice
- Interoperabilidad

C.- La puesta en producción será autorizada por el CRTM, una vez que el adjudicatario realice un informe/certificado positivo, por cada piloto o versión final del producto.

Se estima que esta tarea (epígrafe 5.3) requiere un periodo aproximado de 42 días, si bien los primeros 33 días se pueden ejecutar a la par que las tareas descritas en los puntos 5.2.1 a 5.2.3.

Aclaración sobre el versionado previsto.

Está previsto varias actualizaciones, en el producto final (fase 2).

App de la tarjeta virtual:

Ver 1: soporta sólo tarjeta Multi, con un solo título (multiviajes)

Ver 2: se añade a la Multi virtual el uso de sencillos

Ver 3: se añade a la migración de la TTP física a TTP virtual, quedando inactiva la TTP física.

Las tareas descritas en este punto alcanzan los 42 días. No obstante, en caso de prórroga del servicio, la misma alcanzaría a todas las horas/jornadas máximas previstas de trabajo durante toda la prórroga.

6.- Equipo técnico

Para la correcta consecución de los objetivos planteados, el adjudicatario deberá poner a disposición del proyecto, el siguiente perfil requerido:

- Titulado en ingeniería superior
- Experiencia (mínimo 3 años) demostrable en:
 - 1.- Proyectos de INNOVACIÓN TECNOLÓGICA
 - 2.- En dirección/coordiación de SISTEMAS DE BILLETAJE ELECTRÓNICO BASADOS EN "MIFARE DESFIRE - ISO 1444A"
 - 3.- DEFINICION DE ESPECIFICACIONES TECNICAS EN RELACIÓN A SISTEMAS DE BILLETAJE ELECTRÓNICO BASADOS EN MIFARE DESFIRE.
 - 4.- En COORDINACION DE PRUEBAS DE SISTEMAS BASADOS EN TARJETAS SIN CONTACTOS EN EL TRANSPORTE PÚBLICO (definición y puesta en marcha de protocolos de pruebas de billeteaje sin contactos en el ámbito del transporte público)
 - 5.- DISPOSITIVOS Y ALORITMOS DE SEGURIDAD ADECUADOS A LAS TARJETAS SIN CONTACTOS (SAM, HSM, SHA, MD5, DES, Triple DES (3DES), AES, RSA y SSLv3)

A tal efecto, y en plazo máximo de 15 días desde la formalización del contrato, el adjudicatario deberá aportar toda la documentación necesaria que justifique los mínimos exigidos en el equipo de trabajo.

7 CONDICIONES GENERALES

7.1 Introducción.

El adjudicatario realizará la totalidad de los trabajos especificados en el presente Pliego de Prescripciones Técnicas en cumplimiento del contrato que se establezca.

El adjudicatario será el único responsable de los desarrollos determinados en el contrato, limitándose el CRTM a controlar dichos desarrollos y, en general, a verificar y asegurar que estos se efectúan de acuerdo con lo que se establece en el presente pliego.

La Administración facilitará al adjudicatario cuanta información disponga relacionada con el objeto de este contrato, así como su acceso a la documentación existente que considerase de interés para el proyecto.

7.2 Dirección del proyecto.

La dirección del proyecto se llevará a cabo por parte del Consorcio de Transportes de Madrid. Por otro lado, el contratista determinará un Director Técnico que, salvo fuerza mayor, y previa justificación y aprobación ante el CRTM, será único a lo largo de la ejecución del proyecto.

Las funciones del Director de Proyecto del CRTM serán:

- Dirigir y supervisar la realización y desarrollo de los mismos.
- Facilitar la información necesaria para la ejecución de los trabajos descritos.
- Determinar y hacer cumplir las Normas de Procedimiento.
- Decidir la aceptación de las modificaciones propuestas por el Director Técnico en el desarrollo de los trabajos.
- Realizar las certificaciones parciales de servicios prestados.

Las funciones del Director Técnico del contratista serán:

- Ser el único Interlocutor entre el grupo de trabajo del contratista y el CRTM.
- Organizar la ejecución de los trabajos y poner en práctica las órdenes de la dirección de los mismos.
- Ostentar la representación del equipo técnico contratado en sus relaciones con la Administración, en lo referente a la ejecución de los trabajos.
- Observar y hacer observar las Normas de Procedimiento.
- Proponer a la Dirección del Proyecto las modificaciones en el contenido y realización de los trabajos necesarios para el desarrollo de los mismos.
- Realizar el acta de todas y cada una de las reuniones de trabajo que se tengan.

Previamente al arranque del proyecto el contratista propondrá un Director Técnico al CRTM que deberá ser aprobado por éste.

7.3 Seguimiento y control en la ejecución de trabajos.

Corresponde a la Dirección del Proyecto, el control de la productividad y calidad de los trabajos ejecutados por el contratista, siendo potestad suya solicitar nuevamente la realización y/o el cambio de cualquiera de los desarrollos o servicios prestados.

Para realizar el seguimiento del proyecto, se mantendrán reuniones quincenales en las oficinas del CRTM el mismo día de la semana y hora que se acuerde al comienzo del proyecto. Según la evolución de los trabajos y si se considera necesario las reuniones pasarán de quincenales a semanales.

7.4 Carácter llave en mano.

El contratista deberá entregar los procedimientos, especificaciones o implementaciones desarrolladas durante la ejecución de este contrato al director nombrado por el CRTM, que será el encargado de validarlo, por tanto, el proyecto no se considerará finalizado hasta la aceptación por parte del director del proyecto nombrado por el CRTM.

8 GLOSARIO DE TERMINOS

AES

Advanced Encryption Standard (AES), también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques y es uno de los algoritmos más populares usados en criptografía simétrica.

Backoffice

Se refiere a los procesos informáticos internos que realiza el CRTM.

BIT o sistema BIT o proyecto BIT:

El BIT (Billete Inteligente del Transportes) es el núcleo de todo el cambio tecnológico que se está produciendo en el proceso de migrar la tecnología magnética de billete hacia la tecnología sin contactos. El BIT establece todas las reglas a todos los niveles, y esto, hace posible que dispongamos de la conocida TTP (tarjeta de transporte público). Es decir, la TTP es un producto del BIT.

HCE

Host card emulation. Término utilizado en el ámbito de emulación de tarjetas en teléfonos móviles.

HSM

Los Hardware Security Module (HSM) (Módulo de Seguridad Hardware) son los dispositivos garantes de la seguridad (con disponibilidad de 24x7x365). El CRTM se encarga de particularizar (preperso+perso) todos los HSM del sistema. Las tarjetas criptográficas utilizadas actualmente son PL600 y PSI-E2:PL1500. Estas tarjetas son capaces de embeber claves y comandos de forma segura (software de bajo nivel). Los HSMs incorporan un sistema antirrobo basado en la "tamperización", esto es un proceso autodestructivo por si se intenta abrir o quitar un dispositivo HSM.

Mapa de memoria

Se entiende por mapa de memoria a el conjunto de ficheros en hexadecimal que se requieren para representar todos los atributos descritos en las especificaciones del sistema BIT.

NFC

Near field communication (NFC, comunicación de campo cercano en español) es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos. Los estándares de NFC cubren protocolos de comunicación y formatos de intercambio de datos, y están basados en ISO 14443 (RFID, radio-frequency identification) y FeliCa.1 Los estándares incluyen ISO/IEC 180922 y los definidos por el NFC Forum.

OTA

Over the air programming. Término utilizado en comunicaciones inalámbricas para referirse al medio del canal.

SAE

Sistemas de Ayuda a la Explotación. En el ámbito del transporte público, cada operador de transportes requiere de un SAE para que el centro de control del operador de transportes pueda seguir, en tiempo real, la situación de cada autobús, su ocupación y el ajuste con respecto al horario programado. Estos sistemas están integrados con CRTM y representan la oferta.

SAM

Un módulo de acceso seguro (SAM) es un dispositivo de seguridad, que sirve para almacenar claves maestras y comandos de bajos nivel que permiten realizar operaciones seguras con el exterior, de forma muy rápida. Los módulos SAM permiten acceder al contenido de la Tarjeta de Transporte Público (TTP), tanto en validación como en inspección. Además, a través de estos dispositivos es posible particularizar los HSMs que se ocupan de los procesos de personalización y carga/recarga. El sistema de seguridad de

BIT, define comandos de bajo nivel específicos y mecanismos de seguridad propios del CRTM.

SECEBIT

SECEBIT (SEguridad CEntralizada para el sistema BIT) permite varios cientos de procesos concurrentes, se compone de al menos dos servidores criptográficos configurados en alta disponibilidad (balanceados), cada uno de los cuales incorpora al menos un módulo de hardware seguro (HSM) (tarjeta PCI), los HSMs son el núcleo del sistema SECEBIT, pero para que el servidor criptográfico pueda ofrecer el servicio del núcleo se precisa una capa software que establezca la comunicación entre el exterior y el núcleo. El CRTM dispone de este software (de alto nivel).

SID

Es el Servidor de Intercambio de Datos. La conexión es un canal seguro al que acceden todos los actores del sistema para subir las transacciones y descargar ficheros de configuración actualizados.

TLV

Son paquetes de datos (Tipo Longitud y Valor).

Las especificaciones BIT construyen los ficheros elementales incluidos en el mapa de memoria de la TTP como un conjunto de TLVs. También, por extensión, los TLVs se utilizan para nombrar los diferentes tipos de transacciones que se generan cada vez que la TTP interactúa con cualquier lector. Dichas transacciones, de tipo TLV se envían al CRTM mediante el SID.

TTP:

Es la tarjeta de transporte público (tecnología sin contactos, norma ISO 14443A). Dicha tarjeta sigue las especificaciones de tamaño de la norma ISO 7816 y dispone de un chip tipo NXP DesFire. La tarjeta TTP es pasiva y los lectores/validadores del sistema inducen la corriente suficiente para su funcionamiento

9 ANEXO: TLVs NECESARIOS

Ejemplos:

Estructura del TLV B2h:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<?xml-stylesheet type="text/xsl" href=".\\B2h_LTT_v1.0.xsl"?>
<listatitulos TipoTLV="B2h" Version="1.0" fecha="2019-05-10T14:14:52"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation=".\\B2h_LTT_v1.0.xsd">
  <names tipo="text" qty="239">
    <titulo codigo="1054h" nombre="TTP INFANTIL"/>
    <titulo codigo="1048h" nombre="ANUAL ZONA C2-E1"/>
    <titulo codigo="100Bh" nombre="ANUAL ZONA A"/>
    .....
    <titulo codigo="1020h" nombre="TURISTICO A 3 DIAS"/>
  </names>
</listatitulos>
```

Estructura del TLV B3h:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<?xml-stylesheet type="text/xsl" href=".\\B3h_TRF_v1.0.xsl"?>
<Informacion_Tarifas TipoTLV="B3h" Version="1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation=".\\B3h_TRF_v1.0.xsd">
  <Titulo Codigo="100Bh">
    <Empresa_Propietaria_Cod>01h</Empresa_Propietaria_Cod>
    <Perfil Codigo="01h">
      <Empresa_Propietaria_Perf>01h</Empresa_Propietaria_Perf>
    <Tarifa>
      <Tipo_Unidades>02h</Tipo_Unidades>
```



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES,
MOVILIDAD E INFRAESTRUCTURAS



<Unidades>54600</Unidades>
 <Fecha_Inicio_Admision>31/12/2015</Fecha_Inicio_Admision>
 <Fecha_Cambio_Tarifa>01/01/2020</Fecha_Cambio_Tarifa>
 <Fecha_Fin_Admision>01/02/2020</Fecha_Fin_Admision>
 </Tarifa>
 <Tarifa>
 <Tipo_Unidades>02h</Tipo_Unidades>
 <Unidades>54600</Unidades>
 <Fecha_Inicio_Admision>01/01/2020</Fecha_Inicio_Admision>
 <Fecha_Cambio_Tarifa>19/03/2020</Fecha_Cambio_Tarifa>
 <Fecha_Fin_Admision>20/03/2020</Fecha_Fin_Admision>
 </Tarifa>
 </Perfil>
 <PerfilCodigo="03h">
 <Empresa_Propietaria_Perf>01h</Empresa_Propietaria_Perf>
 <Tarifa>
 <Tipo_Unidades>02h</Tipo_Unidades>
 <Unidades>35000</Unidades>
 <Fecha_Inicio_Admision>31/12/2015</Fecha_Inicio_Admision>
 <Fecha_Cambio_Tarifa>01/01/2020</Fecha_Cambio_Tarifa>
 <Fecha_Fin_Admision>01/02/2020</Fecha_Fin_Admision>
 </Tarifa>
 <Tarifa>
 <Tipo_Unidades>02h</Tipo_Unidades>
 <Unidades>35000</Unidades>
 <Fecha_Inicio_Admision>01/01/2020</Fecha_Inicio_Admision>
 <Fecha_Cambio_Tarifa>19/03/2020</Fecha_Cambio_Tarifa>
 <Fecha_Fin_Admision>20/03/2020</Fecha_Fin_Admision>
 </Tarifa>
 </Perfil>
 </Titulo>

.....

```
<TituloCodigo="2532h">
  <Empresa_Propietaria_Cod>01h</Empresa_Propietaria_Cod>
  <PerfilCodigo="01h">
    <Empresa_Propietaria_Perf>01h</Empresa_Propietaria_Perf>
    <Tarifa>
      <Tipo_Unidades>02h</Tipo_Unidades>
      <Unidades>150</Unidades>
      <Fecha_Inicio_Admision>01/01/2017</Fecha_Inicio_Admision>
      <Fecha_Cambio_Tarifa>01/01/2020</Fecha_Cambio_Tarifa>
      <Fecha_Fin_Admision>01/02/2020</Fecha_Fin_Admision>
    </Tarifa>
    <Tarifa>
      <Tipo_Unidades>02h</Tipo_Unidades>
      <Unidades>150</Unidades>
      <Fecha_Inicio_Admision>01/01/2020</Fecha_Inicio_Admision>
      <Fecha_Cambio_Tarifa>19/03/2020</Fecha_Cambio_Tarifa>
      <Fecha_Fin_Admision>20/03/2020</Fecha_Fin_Admision>
    </Tarifa>
  </Perfil>
</Titulo>
</Informacion_Tarifas>
```

Estructura del TLV B4h:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<?xml-stylesheet type="text/xsl" href=".\\B4h_TLP_v5.3.xsl"?>
<!-- La version XML 5.3 corresponde en especificaciones con TLV B4h=4.0 --
>

<!-- revisado 18 marzo 2019 -->
<Informacion_Tarifas_Titulos TipoTLV="B4h" VersionTLV="5.3"
VersionContenido="1.1" fecha="2019-05-13T07:49:50"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation=".\\B4h_TLP_v5.3.xsd">
  <Tipo_TarjetaCodigo="00h" Descripcion="Tarjeta TTP Personal">
    <Familia idfamilia="10" TipoTitulo="TITULO TEMPORAL 30 DIAS">
```




Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES,
MOVILIDAD E INFRAESTRUCTURAS



```
<TituloCodigo="1055h" Descripcion="30 DIAS JOVEN" Orden="1">
<Empresa_Propietaria_Cod>01h</Empresa_Propietaria_Cod>
<Fecha_Inicio_Venta>2016-01-01</Fecha_Inicio_Venta>

<Fecha_Cambio_Venta1>2020-01-01</Fecha_Cambio_Venta1>
<Fecha_Cambio_Venta2>2020-03-19</Fecha_Cambio_Venta2>
<Fecha_Fin_Venta>2020-03-20</Fecha_Fin_Venta>
<ColectivoCodigo="00h" Descripcion="Normal">
  <PerfilCodigo="03h">
    <Perfil_Nombre>JOVEN</Perfil_Nombre>
    <Empresa_Propietaria_Perfil>01h</Empresa_Propietaria_Perfil>
    <Tarifa_Venta_1>
      <Porcentaje_IVA>10</Porcentaje_IVA>
      <Tipo_BaselImponible>02h</Tipo_BaselImponible>
      <BaselImponible>1818</BaselImponible>
      <Tipo_UnidadIVA>02h</Tipo_UnidadIVA>
      <ImporteIVA>182</ImporteIVA>
      <Tipo_Unidades>02h</Tipo_Unidades>
      <Unidades>2000</Unidades>
      <crc>1</crc> <!-- 1 es correcto, 2 incorrecto -->
    </Tarifa_Venta_1>
    <Tarifa_Venta_2>
      <Porcentaje_IVA>10</Porcentaje_IVA>
      <Tipo_BaselImponible>02h</Tipo_BaselImponible>
      <BaselImponible>1818</BaselImponible>
      <Tipo_UnidadIVA>02h</Tipo_UnidadIVA>
      <ImporteIVA>182</ImporteIVA>
      <Tipo_Unidades>02h</Tipo_Unidades>
      <Unidades>2000</Unidades>
      <crc>1</crc> <!-- 1 es correcto, 2 incorrecto -->
    </Tarifa_Venta_2>
    <Tarifa_Venta_3>
      <Porcentaje_IVA>10</Porcentaje_IVA>
      <Tipo_BaselImponible>02h</Tipo_BaselImponible>
      <BaselImponible>1818</BaselImponible>
```

```
<Tipo_UnidadIVA>02h</Tipo_UnidadIVA>
  <ImporteIVA>182</ImporteIVA>
  <Tipo_Unidades>02h</Tipo_Unidades>
  <Unidades>2000</Unidades>
  <crc>1</crc> <!-- 1 es correcto, 2 incorrecto -->
```

```
</Tarifa_Venta_3>
</Perfil>
</Colectivo>
```

....

```
</Tipo_Tarjeta>
</Informacion_Tarifas_Titulos>
```

Estructura del TLV B5h:

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<?xml-stylesheet type="text/xsl" href=".\\B5h_PTL_v4.2.xsl"?>
<Propiedades_Titulos TipoTLV="B5h" VersionTLV="4.2"
VersionContenido="1.0" fecha="2019-05-13T07:55:12"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation=".\\B5h_PTL_v4.2.xsd">
  <!-- revisado 29 agosto 2016, 4 de oct 2017 -->
  <Titulo Codigo="1031h">
    <Empresa_Propietaria_Cod>01h</Empresa_Propietaria_Cod>
    <Trasbordos_Max>00h</Trasbordos_Max>
    <Viajeros_Max>01h</Viajeros_Max>
    <Viaje_Tiempo_Max>0000h</Viaje_Tiempo_Max>
    <Viajes_Dia_Max>00h</Viajes_Dia_Max>
    <Unidades_Aviso>03h</Unidades_Aviso>
    <Unidades_Dispatch>100000h</Unidades_Dispatch>
    <cmvc>0000h</cmvc> <!-- Cantidad Max. Viajes Compra -->
    <cmcc>0000h</cmcc> <!-- Cantidad Max. Compras Consecutivas -->
    <fraccion>00h</fraccion> <!-- Fraccion de titulo -->
    <antipasscontractMaxUserQty>00h</antipasscontractMaxUserQty> <!--
valor 0 no aplica, valor 1 indica que aplica -->
```

<suplemento>00h</suplemento> <!-- valor 0 no aplica, valor 1 indica que aplica -->

<Tiempo_Min_Borrado>000029h</Tiempo_Min_Borrado>
 <Nombre_Titulo>30 DIAS ZONA B1-E1</Nombre_Titulo>
 <Periodo_Validez>00001Eh</Periodo_Validez>
 <Periodo_Validez_Compra>00h</Periodo_Validez_Compra>
 <Periodo_Invalidez_Compra>000029h</Periodo_Invalidez_Compra>
 <Propiedades_Contrato>00h</Propiedades_Contrato>
 <Dias_Restriccion>0000h</Dias_Restriccion>
 <Fecha_Inicio_Restriccion>0000h</Fecha_Inicio_Restriccion>
 <Hora_Inicio_Restriccion>0000h</Hora_Inicio_Restriccion>
 <Fecha_Fin_Restriccion>0000h</Fecha_Fin_Restriccion>
 <Hora_Fin_Restriccion>0000h</Hora_Fin_Restriccion>
 <Operador Cantidad="04h">
 <Operador_Validez1>01h</Operador_Validez1>
 <Operador_Validez2>02h</Operador_Validez2>
 <Operador_Validez3>03h</Operador_Validez3>
 <Operador_Validez4>04h</Operador_Validez4>
 </Operador>
 <Zona_Validez>000000FCh</Zona_Validez>
 <Linea_Restriccion Cantidad="0000h"/>
 <Linea_Validez Cantidad="0004h">
 <Linea1>01F4h</Linea1>
 <Linea2>01F4h</Linea2>
 <Linea3>05DCh</Linea3>
 <Linea4>09C4h</Linea4>
 </Linea_Validez>
 <ContractInfo>00h</ContractInfo>

<Reserva_Uso_Futuro_2>06202020202020h</Reserva_Uso_Futuro_2>
 </Titulo>

.....

<Titulo Codigo="1059h">
 <Empresa_Propietaria_Cod>01h</Empresa_Propietaria_Cod>
 <Trasbordos_Max>00h</Trasbordos_Max>


```
<Viajeros_Max>01h</Viajeros_Max>
  <Viaje_Tiempo_Max>0000h</Viaje_Tiempo_Max>
  <Viajes_Dia_Max>00h</Viajes_Dia_Max>
  <Unidades_Aviso>01h</Unidades_Aviso>
  <Unidades_Dispatch>100000h</Unidades_Dispatch>
  <cmvc>0000h</cmvc> <!-- Cantidad Max. Viajes Compra -->
  <cmcc>0000h</cmcc> <!-- Cantidad Max. Compras Consecutivas -->

  <fraccion>00h</fraccion> <!-- Fraccion de titulo -->
  <antipasscontractMaxUserQty>00h</antipasscontractMaxUserQty> <!--
valor 0 no aplica, valor 1 indica que aplica -->
  <suplemento>00h</suplemento> <!-- valor 0 no aplica, valor 1 indica que
aplica -->
  <Tiempo_Min_Borrado>000029h</Tiempo_Min_Borrado>
  <Nombre_Titulo>TURISTICO T 4 DIAS</Nombre_Titulo>
  <Periodo_Validez>000004h</Periodo_Validez>
  <Periodo_Validez_Compra>00h</Periodo_Validez_Compra>
  <Periodo_Invalidez_Compra>000000h</Periodo_Invalidez_Compra>
  <Propiedades_Contrato>00h</Propiedades_Contrato>
  <Dias_Restriccion>0000h</Dias_Restriccion>
  <Fecha_Inicio_Restriccion>0000h</Fecha_Inicio_Restriccion>
  <Hora_Inicio_Restriccion>0000h</Hora_Inicio_Restriccion>
  <Fecha_Fin_Restriccion>0000h</Fecha_Fin_Restriccion>
  <Hora_Fin_Restriccion>0000h</Hora_Fin_Restriccion>
  <Operador Cantidad="04h">
    <Operador_Validez1>01h</Operador_Validez1>
    <Operador_Validez2>02h</Operador_Validez2>
    <Operador_Validez3>03h</Operador_Validez3>
    <Operador_Validez4>04h</Operador_Validez4>
  </Operador>
  <Zona_Validez>000001FFh</Zona_Validez>
  <Linea_Restriccion Cantidad="0000h"/>
  <Linea_Validez Cantidad="0004h">
    <Linea1>01F4h</Linea1>
    <Linea2>01F4h</Linea2>
```



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES,
MOVILIDAD E INFRAESTRUCTURAS



<Linea3>05DCh</Linea3>
 <Linea4>09C4h</Linea4>
 </Linea_Validez>
 <ContractInfo>00h</ContractInfo>
 <Reserva_Uso_Futuro_2>06202020202020h</Reserva_Uso_Futuro_2>
 </Titulo>
 </Propiedades_Titulos>

Madrid, 2 de octubre de 2019
LA DIRECTORA GERENTE

Silvia Roldán Fernández

CONFORME:
EL ADJUDICATARIO

