



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



**PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN POR
PROCEDIMIENTO ABIERTO DEL “SECEBIT Y SISTEMAS ASOCIADOS, Fase II” DEL
CONSORCIO REGIONAL DE TRANSPORTES DE MADRID**





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



ÍNDICE

1	ANTECEDENTES	4
2	JUSTIFICACIÓN	4
3	DESCRIPCIÓN ACTUAL DE SECEBIT Y SISTEMAS ASOCIADOS.....	4
3.1	SECEBIT	4
3.1.1	Subsistemas de HSMs	4
3.1.2	Subsistemas de balanceo de carga y alta disponibilidad	8
3.1.3	Subsistemas de registro de operaciones de HSMs.....	9
3.2	Sistema LAT	11
3.3	Sistema SECU.....	15
4	OBJETO DEL DOCUMENTO	17
5	ALCANCE DEL CONTRATO.....	18
6	TRABAJOS A REALIZAR.....	18
6.1	SECEBIT	18
6.1.1	Proceso de particularización compatible con SAM tipo 4.....	18
6.1.2	Proceso de particularización on line	18
6.1.3	HSM26 compatible con SAM tipo 4	19
6.1.4	Rediseño de la arquitectura SECEBIT.....	21
6.2	LAT.....	22
6.2.1	Evolución funcional.....	22
6.2.2	Evolución tecnológica.....	23
6.3	SECU	24
6.3.1	Evolución de arquitectura	24
6.3.2	API SECU	24
6.4	Virtualización	24
6.5	Adaptación a los procedimientos del SII.	28
6.6	APP del CRTM.	29
6.7	Integración LAT con GBIT.....	30
6.8	Integración LAT con PASARELA DE PAGO.	31
6.9	Soporte medios de pago y pasarelas con la aplicación GBIT.....	31
6.10	Mantenimiento y soporte de los sistemas SECEBIT, LAT y SECU del CRTM..	31
6.11	Herramientas de test CDC.....	35
6.12	Pruebas.....	36
6.13	MiddleLAT.	36
7	DESARROLLO, PRUEBAS e INSTALACIÓN.....	36
8	ASEGURAMIENTO DE LA CALIDAD.....	37
9	CONDICIONES GENERALES.....	37





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



9.1	Introducción	37
9.2	Dirección del Proyecto	37
9.3	Seguimiento y control en la ejecución de trabajos	38
9.4	Entrega de los trabajos realizados	38
9.5	Entorno de trabajo	38
9.6	Transferencia de conocimiento	39
9.7	Reversión de servicio.....	39
9.7.1.	<i>Elaboración del plan de reversión del servicio</i>	<i>39</i>
9.7.2.	<i>Ejecución del plan de reversión del servicio</i>	<i>39</i>
10	PLAN DE TRABAJO.....	40
11	DOCUMENTACIÓN	40
ANEXO 1: GLOSARIO DE TERMINOS.....		41





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



1 ANTECEDENTES

En el ámbito del Sistema BIT (Billeteaje Inteligente del Transportes), el CRTM (Consorcio Regional de Transportes de Madrid), define y custodia, la seguridad de las tarjetas de transportes; TTP, Multi, o cualquier otro producto que surja en el futuro, como pueden ser las tarjetas virtuales. Para ello, se utilizan dos tipos de elementos custodios de claves, estos son: SAM y HSM

Los SAM están asociados a los procesos de validación e inspección, en cambio, los HSM están relacionados con la prepersonalización, personalización y carga (además de recarga). Estos últimos dispositivos, han dado lugar a los sistemas SECEBIT y LAT-SECU.

Tanto los SAM como los HSM deben ser compatibles y ofrecer operaciones equivalentes. Sin embargo, los SAM actuales (tipo 2), implantados en toda la red de Operadores de Transportes de la Comunidad de Madrid han llegado al final de su vida útil, y ya están siendo sustituidos por nuevos SAM (tipo 4), que además de ofrecer retrocompatibilidad con el tipo 2, aportan nuevos mecanismos de seguridad.

2 JUSTIFICACIÓN

Los sistemas SECEBIT y LAT-SECU requieren, por un lado, adaptarse a los SAM tipo 4, y por otro, incrementar sus funcionalidades para ofrecer al CRTM la capacidad que permita el tratamiento de tarjetas virtuales.

3 DESCRIPCIÓN ACTUAL DE SECEBIT Y SISTEMAS ASOCIADOS.

3.1 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.

3.1.1 Subsistemas de HSMs

El subsistema HSM se constituye en el elemento clave de seguridad para las operaciones de carga y recarga de la nueva tarjeta de transportes de CRTM. Este subsistema va a disponer del conjunto de claves preciso para llevar a cabo de una 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 ticketing, 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



Comunidad
de Madrid

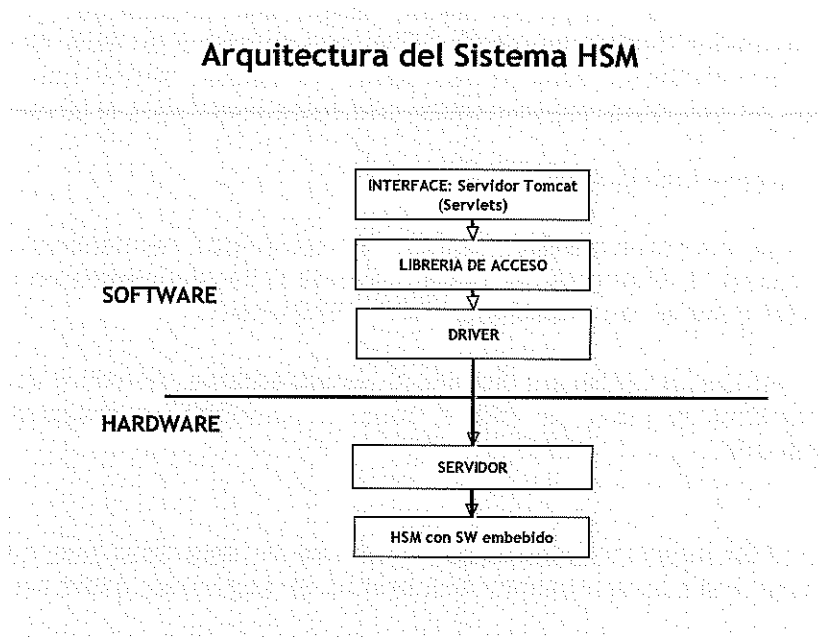
CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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 auditoria 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:



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





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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

Nivel implementacion	Comando	soportado desde
tomcat	InitOperation	HSM20

	Funcionalidades	soportado desde
	Control de comandos por IP	HSM21
	Modo degradado	HSM22
	limitación acceso a contadores	HSM22
	TransacCounter	HSM23
	Logs Claves diversificadas	HSM23
	externalizar contadores	HSM24
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:

Adicionalmente el subsistema HSM dispone de las siguientes facilidades para la gestión integral del sistema:

- Facilidades necesarias para su integración en un sistema de telediagnos 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.

2.1.2. 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.

2.1.3. 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.



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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				

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	-	-
CONOPERACION	NUMBER(20,0)	No	-	-
IDCOMANDO	CHAR(2)	No	-	-
TXIP	VARCHAR2(15)	No	-	-
TXIDPROCESO	VARCHAR2(20)	No	-	-
IDSERIEHSM	VARCHAR2(8)	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.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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 reintenta 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.

3.2 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

Conviene aclarar, que el sistema LAT es independiente de la tecnología de base utilizada en el título de transporte, Mifare-Desfire, Cipurse, De esta forma, si el CRTM decide añadir otro tipo de soporte, el LAT no habría que cambiarlo.

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



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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.

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
- ...

3.3 Sistema SECU

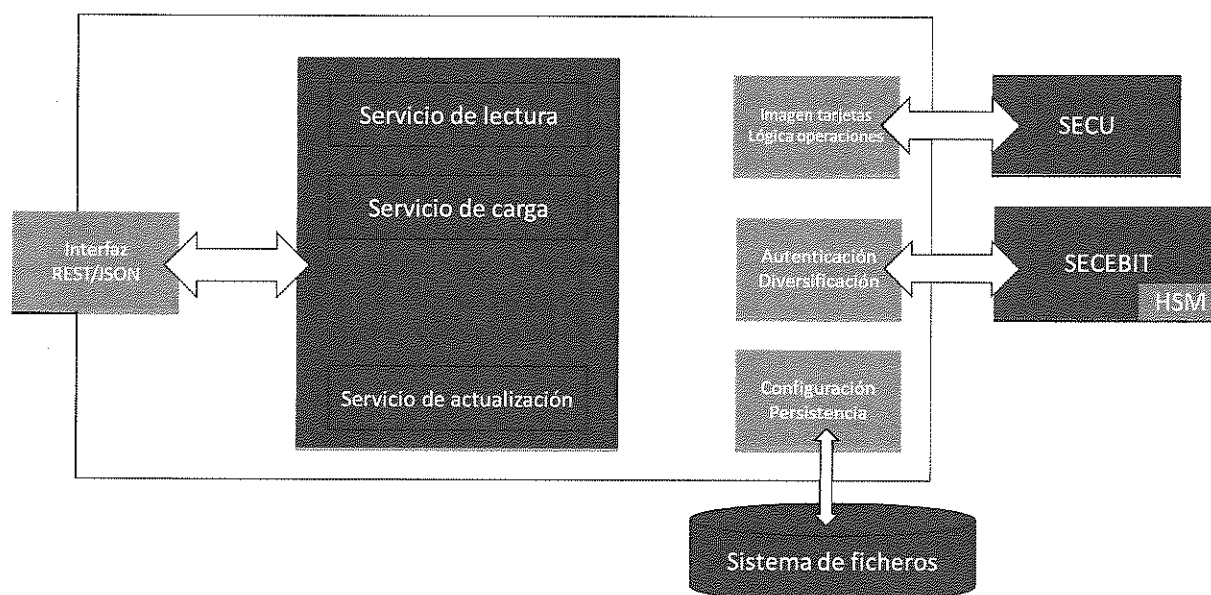
Si SECEBIT conoce como resolver la criptografía de la tarjeta, SECU conoce como se construyen los APDU's necesarios para leerla y escribirla, mientras que LAT conoce la estructura de los datos que contiene, lo que le permite interpretarla y operarla para realizar las operaciones que en cada caso apliquen,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



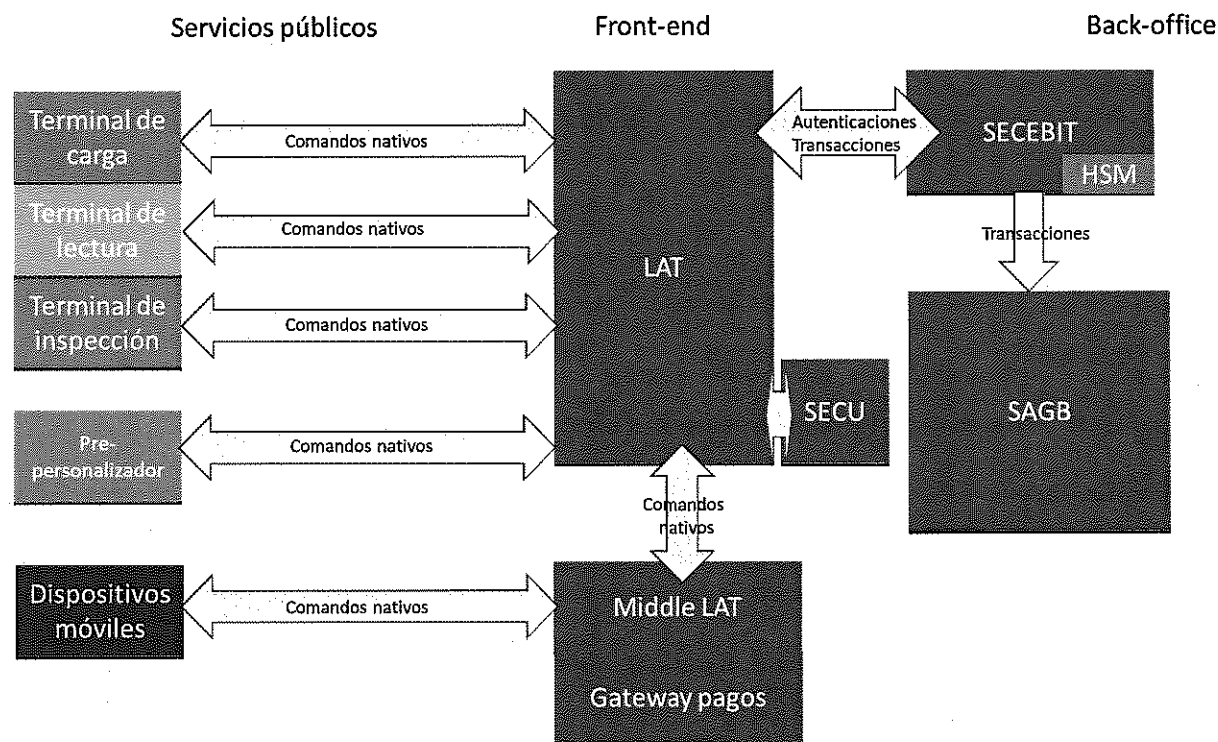
Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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:



4 OBJETO DEL DOCUMENTO

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 el mantenimiento, desarrollo e implantación de las aplicaciones software objeto de este contrato.

También es objeto de este documento definir los procedimientos de ejecución, seguimiento, control y validación de los trabajos contemplados en el alcance del proyecto, la responsabilidad, garantía y propiedad de los trabajos aquí definidos, así como toda la documentación técnica a presentar en cada caso.



5 ALCANCE DEL CONTRATO

Son objeto de este contrato las siguientes tareas:

- Mejoras de SECEBIT (6.1), LAT (6.2) y SECU (6.3).
- Virtualización (6.4)
- Adaptación al SII (6.5)
- App del CRTM (6.6)
- Integración LAT con GBIT (6.7) y con PASARELA DE PAGOS (6.8)
- Soporte de medios de pagos a GBIT (6.9) y soporte y mantenimiento a los sistemas SECEBIT, LAT y SECU (6.10)
- Herramientas de pruebas CDC (6.11) y pruebas del sistema (6.10)

6 TRABAJOS A REALIZAR

Los trabajos objeto de contratación se describen a continuación:

6.1 SECEBIT

6.1.1 Proceso de particularización compatible con SAM tipo 4

Los SAM de tipo 4 (en producción desde 2018), ofrecen retrocompatibilidad con los SAM actuales (compatible DesFire D40; SAM tipo 1, tipo 2 o tipo 3). Es decir, funcionan todos los comandos que tenían disponibles los anteriores SAM. Pero incorporaran nuevos comandos de autenticación FCI y AES, además de familias de claves maestras.

En consecuencia, los procesos de particularización para HSMs PL600 y PL1500 deberán evolucionar para soportar particularizar HSMs a partir de SAM tipo 4. Inyectando claves de cifrado y firma, también desde en SAM tipo 4, además de familias de claves organizadas a partir de diferentes AID, como, por ejemplo:

- Si es una tarjeta DESFire cuyo DF tiene como AID = 000001h, se ha de seleccionar el KeySet con Id=0001h
- Si es una tarjeta DESFire cuyo DF tiene como AID = DECADAh, se he de seleccionar el KeySet con Id=CADAh

6.1.2 Proceso de particularización on line

Se propone llevar a cabo una redefinición completa del actual proceso de particularización a fin 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.

En su lugar, se propone un sistema mucho más flexible en el cual el HSM es particularizado in situ en cada operador. 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.

Para ello, se requiere disponer de una solución basada en la utilización de mecanismos criptográficos de clave pública RSA y en la verificación de firmas en los mensajes de petición y respuesta entre el centro de gestión y cada uno de los componentes de seguridad del sistema desplegados en la red de CRTM.



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS

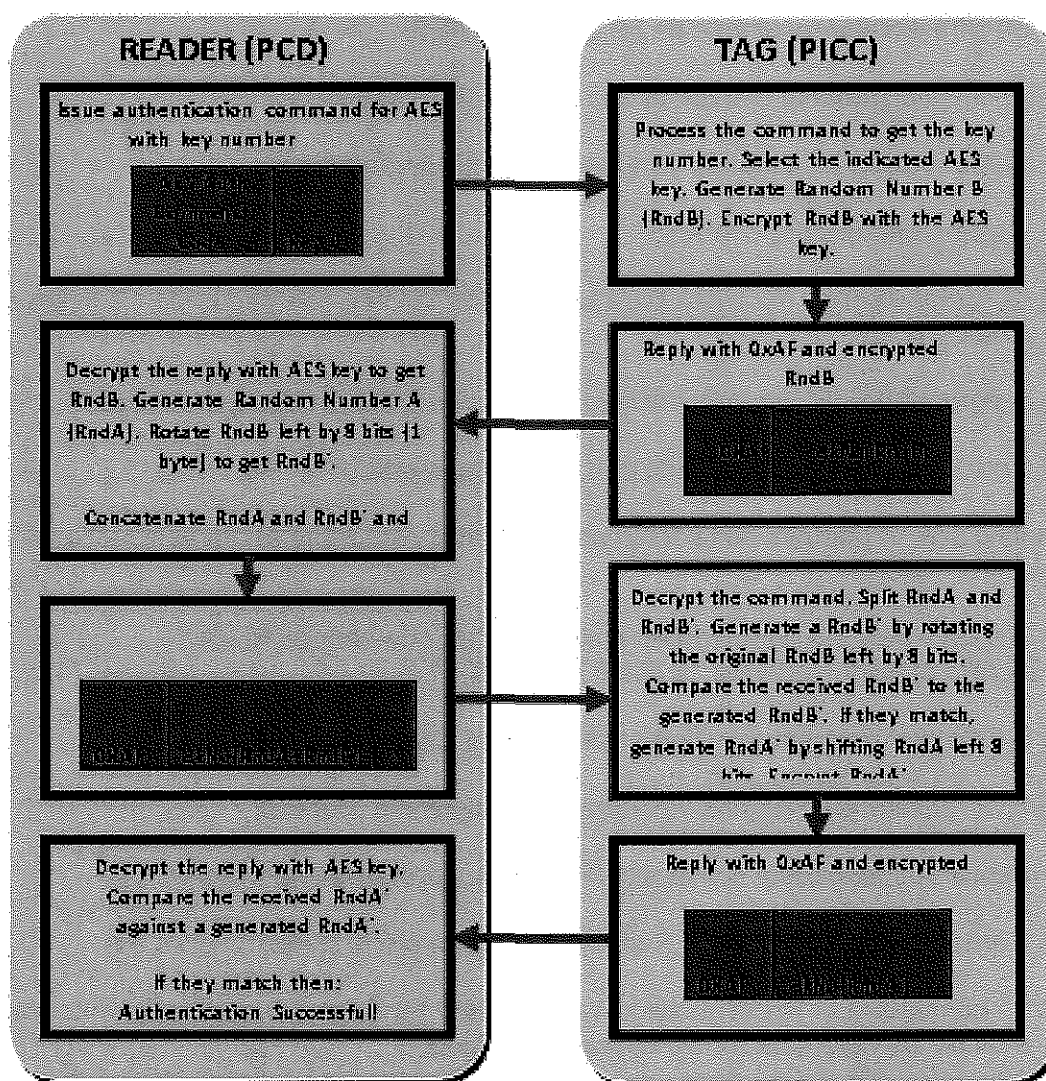


6.1.3 HSM26 compatible con SAM tipo 4

MIFARE DESFire EV1 o EV2, es el chip que utiliza el CRTM, basado en la norma RFID ISO14443A y una plataforma de etiquetas NFC tipo 4A que se utiliza en muchas aplicaciones de seguridad NFC y RFID debido a la capacidad que tiene para operar en forma clara u operar como un transpondedor seguro usando cualquiera de los tres diferentes tipos de encriptación: Single DES, Triple DES o AES.

En general, AES se considera el nivel de cifrado más seguro de los métodos enumerados anteriormente.

El proceso de autenticación AES es una secuencia de pasos múltiples en la que el lector NFC / RFID y la tarjeta del CRTM (TAG/PICC) intercambian datos encriptados para verificar que comparten la misma clave. Durante este proceso, se creará una clave de sesión que se utiliza para ciertos comandos, como el comando cambiar clave. La Figura siguiente muestra un resumen del proceso de autenticación AES.



Las tarjetas CRTM pueden tener varias claves diversificadas almacenadas dentro de ellas.



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



1. El lector emitirá el comando de autenticación AES junto con el identificador de clave.
2. La tarjeta seleccionará el identificador de clave AES y generará un número aleatorio B de 16 bytes (RndB) y encriptará RndB con AES. Luego responderá al comando transmitiendo el paquete de datos encriptados.
3. El lector recibirá la respuesta y pasará por el siguiente proceso:
 - (a) Desencrpte la respuesta con de AES, que le da al lector y recupera el numero aleatorio (RndB) que fue generado anteriormente.
 - (b) Genere un Número aleatorio A (RndA) de 16 bytes, o use un RndA pregenerado.
 - (c) Se gira RndB hacia la izquierda en 8 bits (1 byte), obteniendo RndB'.
 - (d) Se concatena RndA y RndB' para crear un nuevo valor de 32 bytes.
 - (e) Se cifra el valor resultante de 32 bytes con AES.
 - (f) Se envía el paquete resultante a la tarjeta DESFire EV2.
4. La tarjeta recibirá el comando y pasará por el siguiente proceso:
 - (a) Desencrpta el valor con AES.
 - (b) Divida el valor de 32 bytes para obtener los valores separados de 16 bytes para RndA y RndB '.
 - (c) A partir de RndB', girando hacia la derecha en 8 bits, se recupera RndB.
 - (d) Se compare el RndB' recibido con el RndB generado.

Si coinciden, el paquete se recibió correctamente y la tarjeta ahora tiene el RndA que generó el lector.
 - (e) Se gira RndA a la izquierda en 8 bits (1 byte), que obtiene RndA '.
 - (f) Se cifra el valor RndA 'de 16 bytes con AES.
 - (g) Se envía el paquete resultante nuevamente al lector.
5. El lector recibirá la respuesta y pasará por el siguiente proceso:
 - (a) Descifrá la respuesta con la tecla AES, recuperando el valor RndA'.
 - (b) Generará RndA' rotando el RndA que se generó a la izquierda en 8 bits.
 - (c) Se comparará el RndA' recibido con el RndA generado. Si coinciden, entonces el proceso de autenticación se considera exitoso.
 - (d) En este momento, se genera una clave de sesión AES de 16 bytes utilizando los bytes de RndA, RndA ', RndB y RndB':





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



AES Session Key = RndA_(byte 0-3) + RndB_(byte 0-3) + RndA_(byte 12-15) + RndB_(byte 12-15)

- Los comandos que deben incorporarse en el sistema para dar el soporte necesario a esta funcionalidad serían los siguientes;

Comando	soportado desde	Mejorado en
GetAllDiversifiedKey2TDEA	HSM26	
GetAllDiversifiedKeyEV2	HSM26	
GetAllDiversifiedKey	HSM20	HSM26
GetDiversifiedKey	HSM20	HSM26
GetDiversifiedKey2TDEA	HSM25	HSM26
InitSession	HSM25	HSM26
InitSession2TDEA	HSM26	
InitSessionEV2	HSM26	
GetInfo	HSM26	
GetAllCounters	HSM24	HSM26
Stop	HSM26	
listOperation	HSM26	
SelectFamilyKey	HSM26	
GetFamilyKey	HSM26	
Start	HSM26	

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

6.1.4 Rediseño de la arquitectura SECEBIT

La arquitectura actual del sistema SECEBIT responde al diseño realizado con antelación para dar respuesta a los mecanismos de seguridad del sistema de la tarjeta sin contactos del CRTM.

En el momento actual manteniendo estos mecanismos de seguridad y evolucionándolos como en el punto anterior se ha descrito, el objetivo del rediseño sería doble:

- Por un lado, conseguir que los elementos de seguridad, los HSM's, puedan ser considerados en el sistema como meros recursos de un servicio SECEBIT.

En tal sentido se busca que como recursos puedan ser añadidos de una forma "casi" automática al servicio SECEBIT. Para ello en la arquitectura descrita en el apartado de introducción deberán llevarse a cabo las modificaciones pertinentes.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



Este esquema daría lugar a un balanceo mucho más transparente que el actual, lo que unido al punto anterior daría como resultado una mayor flexibilidad en la gestión de las capacidades del sistema.

- Por otro lado, trasladar las operaciones lógicas relacionadas con los elementos de gestión y trazabilidad de operaciones que en la actualidad se efectúan en el propio recurso HSM a un entorno en el que por su carácter puedan realizarse de forma más efectiva y sin restar capacidades al elemento HSM.

Mover estos elementos y sus operaciones lógicas asociadas debe de proporcionar recursos adicionales a los HSMs de forma que se mejoren los tiempos por transacción en al menos un 20%.

Lógicamente y dado que los elementos en cuestión proveen la base de la gestión y trazabilidad a CRTM de las operaciones gestionadas por los diferentes SECEBIT desplegados en la red, dichos elementos deben ser dotados de funciones de seguridad que puedan ser robustas y almacenadas en los HSM's asociados.

En tal sentido puede plantearse;

- En primera fase un almacenamiento periódico del hash del conjunto de elementos en el HSM para poder ser verificado antes de dar comienzo al siguiente periodo de gestión. Esta aproximación puede ser complementada con eventos o interrupciones de servicio para el caso en que se detecte una modificación o alteración en los elementos en cuestión.
- En una fase posterior, podría utilizarse blockchain de CRTM para que el conjunto de redes y operadores consoliden los elementos de gestión con cada una de las operaciones gestionadas.

6.2 LAT.

De cara a la evolución del LAT, que es el elemento dedicado a la lógica del billeteaje, se plantea una evolución dual:

6.2.1 Evolución funcional

- Reparación automática de incidencias en soportes de la tarjeta sin contacto de CRTM.

Con el fin de reducir las incidencias en tarjetas que por problemas en alguno de los procesos de carga, validación, etc. Pudieran quedar en un estado incorrecto impidiendo al usuario su acceso al operador de transporte y obligándole en la actualidad a acudir presencialmente a un punto de atención al usuario de CRTM, se permitirá disponer un botón multicanal (web, app) para ofrecerle al usuario la posibilidad de comprobar remotamente el problema acaecido en su tarjeta y tratar remotamente de solventarlo.

Esta operativa podría ofrecerse en una primera fase a los usuarios que dispusieran de un terminal con tecnología NFC para en una segunda fase poder hacerse accesible a través del conjunto de redes de ventas de CRTM.

La arquitectura técnica que permite dar soporte a esta nueva funcionalidad pasa por nuevos servicios en LAT acompañados por un motor-componente que permitiera "aprender" e ir incrementando progresivamente el tanto por ciento de resoluciones a distancia sin intervención.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



De esta forma puede conseguirse un sistema capaz de detectar desde el inicio de su despliegue incidencias básicas relacionadas con la estructura de ficheros de la tarjeta para llegar en un momento posterior a detectar no sólo este tipo de incidencias básicas sino y además cualquier tipo de inconsistencia en relación con los títulos de transportes.

- Soporte y gestión de apps CRTM.

El servidor LAT realiza todas las operaciones relacionadas con el ciclo de vida de la tarjeta que se han expuesto anteriormente en este documento. Hoy en día con la aparición de aplicaciones en móvil que permitan bien la virtualización de la tarjeta bien operaciones concretas sobre el soporte plástico de la tarjeta TTP o Multi, se hace necesario dotar al servidor LAT de una nueva funcionalidad que permita la gestión de estas apps, entendiendo que en el caso de la virtualización del título no dejan de ser nuevos soportes para los títulos de transporte de CRTM y que en este sentido requerirán de similares controles a los que hoy se realizan sobre los soportes en plástico, entendiendo por tales;

- Nº de apps distribuidas
- Apps en lista negra
- ...

6.2.2. Evolución tecnológica

Son varias las mejoras que entendemos pueden llevarse a cabo sobre el servidor LAT:

- Actualización tecnológica para dar soporte a nuevos estándares como JSON
En el desarrollo de LAT actual se utilizó XML como el soporte tecnológico para compartir datos. Ya que en el momento de dicho desarrollo no había otros formatos abiertos disponibles, por lo que XML fue considerado como la mejor solución para todos los problemas de intercambio de datos.

Hoy en día JSON ha superado en algunos aspectos a XML; si bien en términos de interoperabilidad, JSON y XML están parejos al igual que en la implementación de datos auto-descriptos e internacionalización (Unicode).

JSON es la mejor herramienta para compartir datos. Esto es porque los datos están almacenados en vectores y registros mientras que XML almacena los datos en árboles. Ambos tienen sus ventajas, pero las transferencias de datos son mucho más fáciles cuando los datos se almacenan en una estructura que está familiarizada a los lenguajes orientados a objetos. Esto hace que sea muy sencillo importar datos desde un fichero JSON a Perl, Ruby, Javascript, Python, y otros muchos lenguajes. Para hacer lo mismo con XML, necesitaría primero transformar los datos antes de que puedan ser importados.

- Mejora sustancial del rendimiento
Con objeto de dar una adecuada respuesta a procesos de billeteaje en la virtualización del soporte, el LAT debe mejorar su rendimiento.

En este sentido se plantea independizar por completo la gestión de las imágenes de la tarjeta de las operaciones ligadas al soporte, de esta forma, el sistema en su conjunto podría ser mucho más rápido en el ámbito de la virtualización, ya que en tal caso, no se requiere la parte SECU, y por consiguiente, podría dar respuestas en milisegundos.

Las firmas podrían encolarse con mecanismos de gestión de colas confiables. En concreto se propone emplear herramientas centradas en mensajería descentralizada.



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



Estas herramientas disponen de motores principales cuyo enfoque es construir y usar motores de mensajería distribuida. Estos varían en tamaño y capacidad y pueden ser ajustados a los tamaños de las firmas de operaciones. Los motores comparten una visión común y acuerdan protocolos (RFC) para conectarse entre sí e intercambiar mensajes. Los mensajes son blobs de datos útiles de cualquier tamaño.

- **API LAT**

Todas las funcionalidades del LAT, podrán ser utilizadas por otros sistemas mediante el uso de un API LAT. El cual dispondrá de versionado y documentación.

6.3 SECU

El servidor SECU en su actual versión es un componente embebido dentro del servidor LAT. Ambos sistemas se desarrollaron al mismo tiempo, por lo que es necesario abordar un rediseño.

Por lo tanto, SECU debe ser independizado del LAT, lo que requiere una evolución de arquitectura y tecnológica

6.3.1 Evolución de arquitectura

- La evolución de la arquitectura debe de permitir desacoplar completamente SECU de LAT para que ambos puedan considerarse piezas y elementos separados e individuales.

Adicionalmente esta evolución debe permitir futuras incorporaciones de nuevas tecnologías de tarjeta más allá de la actual Desfire.

6.3.2. API SECU

Todas las funcionalidades del SECU, podrán ser utilizadas por otros sistemas mediante el uso de un API SECU. El cual dispondrá de versionado y documentación.

6.4 Virtualización

Se requiere de un backoffice capaz de tratar la virtualización de las tarjetas sin contacto del CRTM (TTP y MULTI), basadas en el chip NFC Mifare Desfire.

El objetivo identificado es el de proporcionar, a los usuarios que dispongan de teléfonos compatibles con NFC la posibilidad de utilizar una app en su móvil en lugar de la tarjeta física para acceder al transporte.

Para conseguirlo, es preciso llevar a cabo el desarrollo de nuevos comandos y servicios necesarios que permitan el diálogo con las apps haciendo llegar a ellas de forma segura el título de transporte que solicite el usuario, almacenándose, también de forma segura, en el teléfono del usuario.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



Para ello va a resultar necesario incorporar los siguientes comandos:

Comandos LAT y NXP

Comando	Descripción
latNewCard	Crea una nueva tarjeta. Sirve tanto para una tarjeta nueva o migrada de una tarjeta física
latUpdateKey	Actualiza las claves diversificadas de una tarjeta
latUpdateMapCard	Actualiza el mapa de una tarjeta
getBalanceTitleList	Para tarjeta con títulos en uso
getGenericTitleList	Para tarjeta vacía

Comandos entre app y GOOGLE	
Comando	Descripción
getMetaData	Datos de la tarjeta virtual para lectura de saldo

A continuación, se indican los parámetros previstos inicialmente, tanto de entrada, como de salida, por cada uno de estos comandos.

COMANDO	parámetros	
	entrada	salida

latNewCard json_in json_out

json_in	descripción	obligatorio	tipo valor
ticketId	Es la referencia de un proceso iniciado desde un teléfono móvil	Si	String
tipoTarjeta	Código del tipo de tarjeta comercial; TTP, MULTI, etc...	No	hexadecimal
codigoTitulo	Código del título de transportes	No	hexadecimal
FCI- Info Byte	procedimiento usando el timestamp	Si	hexadecimal
FCI - Timestamp	procedimiento usando el timestamp	Si	hexadecimal

json_out	descripción	obligatorio	tipo valor
CodResponse	Código de respuesta. Valor 0 si no hay errores	Si	hexadecimal
serie	numero de serie de la tarjeta virtual	Si	hexadecimal
keys	claves diversificadas de la tarjeta virtual	Si	hexadecimal
map	estructura de la tarjeta con personalización, carga, o lo que corresponda.	Si	hexadecimal





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



COMANDO	parámetros	
	entrada	salida

latUpdateKey json_in json_out

json_in	descripción	obligatorio	tipo valor
ticketId	Es la referencia de un proceso iniciado desde un teléfono móvil.	Si	String
serie	número de serie de la tarjeta virtual	Si	hexadecimal
FCI- Info Byte	procedimiento usando el timestamp	Si	hexadecimal
FCI - Timestamp	procedimiento usando el timestamp	Si	hexadecimal

json_out	descripción	obligatorio	tipo valor
CodResponse	Código de respuesta. Valor 0 si no hay errores	Si	hexadecimal
serie	número de serie de la tarjeta virtual	Si	hexadecimal
key	clave diversificada asociada a timestamp	Si	hexadecimal

COMANDO	parámetros	
	entrada	salida

latUpdateMapCard json_in json_out

json_in	descripción	obligatorio	tipo valor
ticketId	Es la referencia de un proceso iniciado desde un teléfono móvil	Si	String
serie	número de serie de la tarjeta virtual	Si	hexadecimal
map	estructura de la tarjeta con personalización y carga incluida	Si	hexadecimal
codigoTitulo	Código del título de transportes	No	hexadecimal

json_out	descripción
CodResponse	Código de respuesta. Valor 0 si no hay errores
serie	número de serie de la tarjeta virtual
map	estructura de la tarjeta con personalización y carga incluida

COMANDO	parámetros	
	entrada	salida

getBalanceTitleList json_in json_out





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



json_in	descripción	obligatorio	tipo valor
---------	-------------	-------------	------------

Meta-Datos	Meta-Datos extraídos de la imagen de la tarjeta en el dispositivo móvil.	Si	
------------	--	----	--

json_out	descripción	obligatorio	tipo valor
----------	-------------	-------------	------------

CodResponse	Código de respuesta. Valor 0 si no hay errores	Si	hexadecimal
-------------	--	----	-------------

saldo	Objeto con los campos que componen el saldo	Si	
-------	---	----	--

titulos	Lista de posibles títulos a ser cargados en la tarjeta.	Si	
---------	---	----	--

COMANDO	parámetros	
	entrada	salida

getGenericTitleList	json_in	json_out
---------------------	---------	----------

json_in	descripción	obligatorio	tipo valor
---------	-------------	-------------	------------

tipoTarjeta	Tipo de la tarjeta, 1 byte	Si	hexadecimal
-------------	----------------------------	----	-------------

tipoTarjeta	Código del tipo de tarjeta comercial; TTP, MULTI, etc...	Si	hexadecimal
-------------	--	----	-------------

colectivo	Código del colectivo de la tarjeta	No	hexadecimal
-----------	------------------------------------	----	-------------

perfil	Código del perfil de la tarjeta	Si	hexadecimal
--------	---------------------------------	----	-------------

json_out	descripción	obligatorio	tipo valor
----------	-------------	-------------	------------

CodResponse	Código de respuesta. Valor 0 si no hay errores	Si	hexadecimal
-------------	--	----	-------------

titulos	Lista de posibles títulos a ser cargados en la tarjeta.	Si	
---------	---	----	--

Definición de conceptos:

1.- App del CRTM: Se refiere a la app instalado en un teléfono, con NFC y compatible con el sistema del CRTM. Desarrollado por el adjudicatario de este contrato

2.- Wallet Server: Se trata del elemento que es capaz de acceder a la parte segura del teléfono NFC, para leer o escribir el mapa de memoria de la tarjeta virtual, así como lectura/escritura de las claves diversificadas. El adjudicatario de este contrato utilizará un API externo para esta integrar el LAT con el Wallet Server, siempre a través del Mifare Server. Aunque la app del CRTM podría solo acceder a información estadística directamente con el Wallet Server

3.- Mifare Server: Es un elemento intermedio entre el LAT del CRTM y el Wallet Server. Que requiere de una sesión para establecer la relación entre todas las partes, incluido la app del CRTM.

4.- Pasarela de Pago: La integración es desde el LAT, se utilizará mecanismo de OPT.



Teniendo en cuenta los conceptos anteriores, se definen los siguientes casos de uso, que tendrá que desarrollar el adjudicatario:

Caso de uso 1: Crear una nueva tarjeta virtual (incluir pago).

Caso de uso 2: Carga/recarga de títulos de transportes (incluir pago).

Caso de uso 3: Migrar una tarjeta física personal existente al entorno virtual.

Caso de uso 4: Resolver una incidencia de una tarjeta virtual

Con el fin de reducir las incidencias en tarjetas que por problemas en alguno de los procesos de carga / recarga, validación, etc. quedan en un estado incorrecto impidiendo al usuario su acceso al operador de transporte y obligándole en la actualidad a acudir presencialmente a un punto de atención al usuario de CRTM, se propone disponer un botón multicanal (web, app) para ofrecerle al usuario la posibilidad de comprobar remotamente el problema acaecido en su tarjeta y tratar, también remotamente, de solventarlo.

Esta operativa podría ofrecerse, en una primera fase, a los usuarios que dispusieran de un terminal con tecnología NFC para, en una segunda fase, poder hacerse accesible a través de la red de ventas de CRTM.

El motor en servidor podría y debería ir acompañado de un componente de IA que permitiera “aprender” e ir incrementando progresivamente el tanto por ciento de resoluciones a distancia sin intervención.

Para dar soporte a la web del CRTM, se propone la utilización de tecnología AMP (Accelerated Mobile Pages) que permite una mayor eficiencia en el tiempo de carga reduciendo a la vez el consumo de datos. Esta tecnología AMP, permite cuadruplicar la velocidad de carga y reducir significativamente el consumo de datos, haciendo en conjunto que el entorno gráfico sea más fluido y agradable de navegar.

6.5 Adaptación a los procedimientos del SII.

Los procesos de facturación se están adecuándose a la legislación vigente, serán coherentes con la arquitectura tecnológica del sistema BIT y cumplirán con los requisitos de información de los sistemas SII y NEXUS. Además, el CRTM pasará de realizar la declaración de IVA anual a mensual.

Este sistema permitirá emitir al usuario la factura simplificada en el mismo momento en que realiza la compra, en lugar, de entregarle el recibo de la operación. El sistema debe estar integrado con el sistema de facturación del CRTM, y debe generar las transacciones F0 de factura simplificada y F1 de factura rectificativa. El contenido de estas facturas está regulado en el art. 6 del RD 1619/2012 y la numeración de la factura se llevará de forma centralizada desde los HSMs teniendo un formato del tipo que se especifica a continuación.

Factura simplificada y factura rectificativa:

Tipo de contador tendrá dos valores 01 si es el contador de facturas simplificadas y 02 si es el contador de facturas rectificativas.



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



[CódigoActor, Número HSM, tipo contador, (ContadorFacturaHSM), Año]→ contador simplificada.

[1Byte, 3 Byte, 1 Byte, 8 Byte, 2 bytes] total 15 bytes

[CódigoActor, Número HSM, tipo contador, (ContadorFacturaHSM), Año]→ contador rectificativa.

El año se consigna en 2 bytes.

Los contadores del HSM tienen capacidad de 8 bytes por lo que se puede representar un numero entero de hasta 20 dígitos.

Las transacciones de facturación recogen todos los movimientos económicos de venta de tarjetas y/o títulos con especial atención en las redes externas al CRTM, operadores de transporte, red de cajeros 24 horas, red comercial atendida.

Las operaciones con cuantía económica de títulos y tarjetas en los ámbitos mencionados anteriormente son.

Operación económica	Operación sobre el título
Título	Función de compra de título (carga de título)
Título	Función de compra de título (recarga de título)
Título	Venta de suplemento
Cambio Tarifa	Función de cambio de tarifa
Cambio Zona	Función de canje venta
Operación sobre tarjeta	Motivo de la venta
Personalización completa	Emisión de nueva tarjeta

6.6 APP del CRTM.

Mediante el uso del API LAT y API SECU. El adjudicatario desarrollará una app o varias apps (tal y como indique el CRTM en su momento), basadas en tecnología NFC, que permitan que un usuario de la app del CRTM, pueda operar con cualquier tipo de tarjeta comercial existente (TTP, Multi, azul, infantil, etc...) o futura, ofreciendo las siguientes funcionalidades:

- a.- Obtener una tarjeta anónima virtual
- b.- Migrar una tarjeta TTP personal a una tarjeta TTP virtual
- c.- Soporte remoto: recuperar mapa de memoria (ya sea tarjeta física o virtual), modificar el mapa de memoria en backoffice y volver a actualizar la tarjeta de trasportes con el nuevo mapa de memoria.
- d.- Cargar o recargar la tarjeta, ya sean físicas o virtuales.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



e.- Obtención de nueva tarjeta personal virtual: Es la situación más avanzada. En este caso, si CRTM en el futuro dispusiera de licencias de un software externo especializado que cuente con un API de reconocimiento de DNI, fotos, etc... La app del CRTM deberá integrarse con ese API de reconocimiento que acredite, que un usuario, por ejemplo, es joven y además familia numerosa de forma automática. En esta situación el LAT tendría también que adaptarse a los TLVs específicos para esta funcionalidad.

f.- Obtener otro tipo de tarjeta comercial (virtual) que el CRTM especifique en el futuro.

6.7 Integración LAT con GBIT.

El adjudicatario tendrá que realizar todos los análisis y desarrollos correspondientes para que el LAT y/o SECU pueda integrarse con GBIT. Definiendo los comandos a los que accederá GBIT.

Está previsto abordar, al menos, las siguientes líneas de trabajo:

6.7.1. Solicitud de tarjeta TTP virtual desde GBIT procedente del canal Web.

El CRTM dispone de una Web, para que cualquier persona pueda solicitar una tarjeta de transportes público personal (TTP).

Esta Web envía la información de solicitud a GBIT, donde se comprueba toda la documentación necesaria, y se establece el perfil según la edad (infantil, joven, normal, tercera edad), pues todos los perfiles, excepto el normal tienen asociado bonificaciones, y además se verifica el colectivo al que pudiera pertenecer (familia numerosa general, familia numerosa especial, discapacidad, etc.), ya que añade adicionalmente otro descuento.

Actualmente, cuando se comprueba que todo es correcto, se autoriza la personalización de la tarjeta física y posteriormente se envía por correo ordinario, la TTP, a la dirección postal del usuario.

Sin embargo, durante la ejecución de este contrato, el CRTM gestionará también TTP virtuales, por lo que, desde la Web del CRTM se posibilitará solicitarla también, llegando dicha solicitud a GBIT. Desde GBIT se realizarán las mismas comprobaciones que se hacen para una TTP física (descritas anteriormente). Una vez comprobada que toda la documentación es correcta, se envía la TTP virtual, mediante la integración entre GBIT y el LAT, al teléfono móvil NFC del usuario.

6.7.2. Soporte remoto al usuario desde GBIT.

Tanto si el usuario dispone de una tarjeta física como virtual, está previsto dar un soporte remoto, siempre y cuando, el usuario utilice un teléfono NFC que pueda soportar la app del CRTM, y en ese momento, disponga también de suficiente cobertura y conectividad de datos.

El proceso, en líneas generales, es el siguiente:

1.- El usuario tiene un problema con su tarjeta TTP y llama a un teléfono de soporte.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



- 2.- Desde soporte del CRTM le piden al usuario que compruebe en primer lugar que el móvil dispone de conectividad/cobertura, y si es así, que arranque la app del CRTM para activar la opción de "soporte remoto".
- 3.- La opción "soporte remoto" indicará al usuario los pasos para leer su TTP, ya sea físico o virtual. Recibiendo una copia del mapa de memoria en el LAT
- 4.- El LAT dispondrá de una serie de comandos para que desde GBIT se pueda acceder a esta información.
- 5.- Desde GBIT, el equipo de soporte arreglará el mapa de memoria de la TTP.

- 6.- Una vez resuelto el problema, desde GBIT, se envía el mapa modificado vía LAT a la app del usuario.
- 7.- La app del usuario indicará una serie de pasos para trasladar el nuevo mapa de memoria a la TTP (ya sea, físico o virtual)

6.8 Integración LAT con PASARELA DE PAGO.

El CRTM dispone por Concurso Público de una PASARELA DE PAGO, con la cual el LAT deberá integrarse.

6.9 Soporte medios de pago y pasarelas con la aplicación GBIT

Hasta el momento actual el soporte a los diferentes medios de pago y pasarelas desplegados en CRTM se ha llevado a cabo a través de un OTP.

Un OTP es genéricamente un código de un único uso que permite validar la "autenticidad" de un pago para proceder a una carga de un título. Este mecanismo se ha ido empleando con las diferentes pasarelas y procesadores de pago que se han incluido en el sistema.

La generalización del uso de estas u otras nuevas pasarelas hace que el mecanismo que hasta el momento se ha utilizado deba de ser revisado e incorpore mecanismos criptográficos que permitan funcionalmente asegurar no sólo la existencia de la operación de pago sino y adicionalmente autenticar el origen y el código en sí mismo.

En consecuencia, nos proponemos desplegar nuevos servicios de:

- Autorización y autenticación para los servicios de pago
- Encriptación -mecanismos de hashing- robustos y aceptados en la industria

6.10 Mantenimiento y soporte de los sistemas SECEBIT, LAT y SECU del CRTM.

El CRTM dispondrá de una veintena de HSMs, aproximadamente diez núcleos PL600 y otros diez núcleos PL1500.

Se requiere un servicio de mantenimiento para esta situación final, que permita monitorizar los sistemas en modo 24x7 y reducir al máximo los tiempos de respuesta ante cualquier incidencia en el sistema SECEBIT y sistemas asociados durante los 365 días del año.

Antes de proceder con el detalle de los servicios es importante tener una visión de la topología de la red de sistemas desplegada en CRTM.



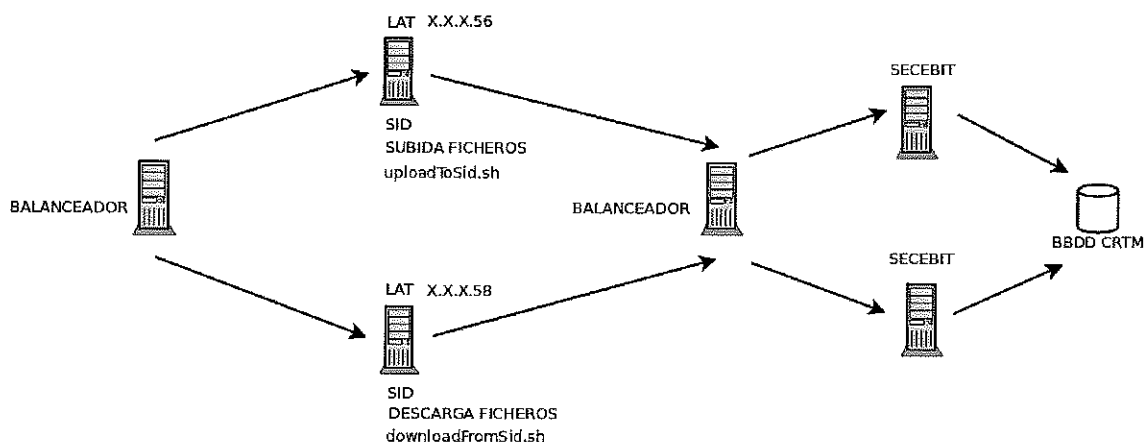


Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



Esquema SID



/etc/cron

la subida se hace cada hora

la descarga una vez al día

el programa que establece conexión con la BBDD (programa JAVA) es secebitsid, crea los ficheros en base a las transacciones que extrae de la BBDD

Los hosts monitorizados actualmente son 26, más 3 hosts Virtuales (Frontend de Balanceadores). Los equipos se han clasificado en categorías: TABLETS, SECEBIT, LAT-SECU, VENDING y MONITORIZACIÓN:

- TABLETS

crtm-tablet1
crtm-tablet2

- SISTEMA SECEBIT:

hsm-balanceo1
hsm-balanceo2
hsm-balanceo3
hsm-balanceo4
hsm-balanceo-flotante1
hsm-balanceo-flotante2
hsm1
hsm2
hsm3
hsm4
hsm5
hsm6
hsm7
hsm8
hsm9
hsm-desal
hsm-canal-ssh1
hsm-fortigate

- SISTEMA LAT-SECU

lat-proxy1





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



lat-proxy2
flotante-lacsecu
lat-secu1
lat-secu2

- NAGIOS:

hsm-monitor1

- Máquinas de VENDING:

indra-T1
indra-T4
vending1

En cuanto a servicios monitorizados, hay una serie de servicios genéricos que se debe comprobar en todos los equipos:

Current Load
Current Users
PING
SSH
Swap Usage
Total Processes
Zombie Processes
home Partition
opt Partition
raiz Partition
var Partition

Adicionalmente se dispone de servicios concretos dependiendo del sistema monitorizado, estos son algunos ejemplos:

Proceso Heartbeat
HSM
HSM Counter Material
HSM Key Material
Error_de_conexion_DB

Los servicios de mantenimiento operativo de la plataforma de CRTM debe constar de:

6.10.1. Servicio de mantenimiento hardware y software El alcance de este servicio tiene por objeto garantizar el adecuado funcionamiento de los sistemas SECEBIT, LAT y SECU. Este servicio abarca lo siguiente:

- **Software SECEBIT, LAT, SECU**, resolución de bugs, configuración y/o reconfiguración, actualización
- **Hardware SECEBIT**, reposición exclusivamente para el hardware en periodo de garantía.
- **Traslado y/o instalación y/o configuración y/o reconfiguración** de equipos entre los CPDs del CRTM (o Madrid Digital)





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



- **Servicio de soporte de monitorización**, este servicio de soporte se ofrece para el conjunto de servidores propios de CRTM más allá de los propios de los sistemas SECEBIT, LAT y SECU.
- **Mantenimiento preventivo** cuya finalidad es la de evitar errores y fallos en el sistema SECEBIT y resto de plataformas cubiertas por el servicio de monitorización a tal fin se dispone de un sistema de monitorización activo que reporta continuamente información del estado de cada uno de los sistemas y subsistemas involucrados en el servicio prestado. De esta forma cualquier desviación en los parámetros operativos genera una alerta que es capturada y tratada por el personal de mantenimiento con el fin de retornar el sistema a su normal operación antes de que se genera una incidencia en el servicio
- **Mantenimiento correctivo** que comprende la identificación de posibles incidencias y el asesoramiento sobre la más correcta utilización del sistema SECEBIT, y la corrección de los defectos de concepción, realización o fabricación que generen anomalías de funcionamiento en el mismo, lo que, como consecuencia de lo anterior, podrá implicar la obligación de poner a disposición de CRTM nuevas versiones corregidas del sistema SECEBIT o aquellas piezas hardware o recambios que fueren precisos para reemplazar elementos defectuosos.

6.10.2. Servicio de mantenimiento avanzado

El servicio de mantenimiento avanzado tiene como finalidad detectar y corregir cualquier incidencia que pudiera producirse en los sistemas SECEBIT desplegados, así como sistemas asociados LAT y SECU. Este servicio se presta en combinación con el servicio anteriormente descrito, que tiene por objeto conservar el sistema SECEBIT, LAT y SECU en estado de adecuado funcionamiento.

A los efectos de una correcta interpretación del servicio es conveniente establecer las siguientes definiciones:

- Tiempo de Resolución:
 - Ante la detección y/o comunicación de errores o funcionamientos incorrectos, se entiende como tiempo de resolución el tiempo que transcurre desde su detección y reconocimiento o, en su caso, desde la petición de asistencia por parte de CRTM hasta que se aplica una solución definitiva.
- Incidencia/Repercusión de bloqueo:
 - Errores o funcionamientos incorrectos que tienen repercusión sobre el negocio. El sistema transaccional no opera. Requiere una actuación inmediata y continuada hasta su resolución.
- Incidencia/Repercusión grave:
 - Errores o funcionamientos incorrectos que no causan impacto inmediato en el negocio. El sistema transaccional opera parcialmente con limitaciones, aunque crea cierta sobrecarga.
- Incidencia de repercusión baja:
 - Errores o funcionamientos incorrectos que no causan impacto en el negocio. El sistema transaccional opera totalmente sin limitaciones.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



- Informe de resolución:
 - Informe de un determinado error o funcionamiento incorrecto en el que se reflejan todos los datos de su resolución (fecha de comunicación-petición de asistencia / resolución definitiva del problema detectado, descripción del problema, identificación del elemento o funcionalidad afectada, causa que ha motivado el problema, acciones o medidas se han tomado para su solución, si se precisa llevar a cabo acciones adicionales, documentación asociada, etc.).

A continuación, se detallan los parámetros de resolución:

Incidencia/Repercusión de bloqueo:

- El tiempo de resolución será inferior a cuatro (4) horas.

Incidencia/Repercusión grave:

- El tiempo de resolución será inferior a dieciocho (18) horas.

Incidencia/Repercusión baja:

- El tiempo de resolución será inferior a treinta y dos (32) horas.

Una vez resuelto el problema detectado, el adjudicatario elaborará y entregará a CRTM el informe de resolución del mismo.

6.11 Herramientas de test CDC.

Se requiere las siguientes herramientas de pruebas:

- Ciclo de vida de la tarjeta, que no están cubiertas en la actualidad.
 - El conjunto de herramientas debiera cubrir al menos las siguientes funciones y operaciones
 - Lectura en crudo de una tarjeta sin contacto empleando SECEBIT para resolver las autenticaciones.
 - Prepersonalización de una tarjeta sin contacto empleando SECEBIT para resolver las autenticaciones.
 - Cliente de lectura y consulta de saldo empleando el LAT.
 - Cliente de carga y recarga empleando el LAT.
 - Cliente de prepersonalización empleando el LAT.
 - Cliente de inspección empleando el LAT.
- Además, una herramienta con interfaz gráfico, destinada a poder operar el mapa de la memoria de la tarjeta a voluntad, gestionando a nivel de campos y tipos definidos, cada fichero. Dicha herramienta trabajará en modo crudo (RAW) con el LAT para leer y escribir la tarjeta sin contacto. Dicha herramienta debe convertirse en una herramienta que puedan ser empleada para la resolución de problemas reales en el backoffice de CRTM, por lo que será fundamental optimizar la usabilidad.
- Equipo de pruebas específico para alterar el tráfico entre el sistema HSM y elemento que se conecta con el HSM. La idea es que al probar, por ejemplo, un dispositivo de carga de TTP o Multi, se pueda simular, qué ocurre en caso que el dispositivo de carga no tenga conectividad o le falle un comando determinado del HSM.



6.12 Pruebas.

El adjudicatario, con la supervisión del CRTM, realizará el conjunto de pruebas establecidas, en dos niveles:

En las fases de pruebas se cumplimentarán los protocolos definidos por el CRTM. No podrá ponerse en producción un sistema o producto sin obtener previamente la VISA de APTO del CRTM. Cualquier modificación de software/hardware de la plataforma tiene que ser informada convenientemente al CRTM y obtener la VISA correspondiente.

NIVEL bajo: Pruebas concretas de cada comando, rendimiento de sistema, de configuración de la arquitectura, de robustez y fiabilidad y de rapidez.

NIVEL alto. Pruebas funcionales de lógica de negocio, de interfaces, de facturas simplificadas y pruebas transaccionales.

6.13 MiddleLAT.

Es una capa de software, a implementar, cuyo objetivo principal debe ser disminuir el número de devoluciones a efectuar en el proceso de carga/recarga de la tarjeta TTP mediante la aplicación móvil. Para ello, se concibe como un elemento que coordine todo el proceso, recibiendo información de las demás piezas software (app, LAT, PASARELA DE PAGOS, etc...)

El MiddleLAT también permitirá almacenar información en una BBDD donde se integre la información de carga/recarga con la información financiera.

Esta capa de software pueda evolucionar a gestionar, coordinar o integrarse con otros canales, como por ejemplo, OOGG (Oficinas de Gestión) y el canal Web.

7 DESARROLLO, PRUEBAS E INSTALACIÓN.

Las tareas de programación e instalación se realizarán en las dependencias del CRTM, ya que, es necesario acceder al núcleo del sistema (servidores y bases de datos de producción y desarrollo) de este organismo.

Las pruebas finales, antes de autorizar un cambio de entorno, serán realizadas por el adjudicatario en presencia de personal responsable del CRTM asignado. Se adjuntarán las librerías, scripts y demás componentes utilizados para realizar la implantación, con un documento detallado de todos los pasos y requerimientos para desarrollar esta tarea.

A continuación, se detallan los hitos cuya falta de cumplimiento originarían un retraso en la planificación del proyecto, y que no sólo puede afectar al CRTM, sino también a los operadores de transporte u otros actores externos implicados:

1. Hito I: Las tareas en relación con la particularización de HSMs en base a SAM tipo 4 (epígrafe 6.1.1) deberán estar totalmente concluidas en dos meses a contar desde la fecha de formalización del contrato.



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



2. Hito II: Las tareas en relación con los desarrollos del software HSM26 (epígrafe 6.1.2) deberán estar totalmente concluidas en seis meses a contar desde la fecha de formalización del contrato

La penalización a la empresa adjudicataria por el incumplimiento de cualquiera de estos hitos será la rescisión del contrato, ya que el incumplimiento de los mismos implicaría la imposibilidad de que el CRTM efectuó las tareas que tiene encomendadas según la planificación de implantación en relación al Proyecto BIT donde se enmarca este contrato

8 ASEGURAMIENTO DE LA CALIDAD

El oferente presentará un Plan de Aseguramiento de la Calidad del software (a partir de ahora QA) para las diferentes aplicaciones, que se realizará en el momento en que los productos estén desarrollados y antes de que lo recepcione definitivamente el CRTM.

Este plan de QA estará a su vez compuesto por planes de pruebas unitarias de cada una de las aplicaciones desarrolladas o implantadas y de un plan de pruebas de integración de todos y cada uno de los sistemas nuevos o existentes en el alcance del proyecto.

La estructura de estos planes incluirá, al menos, los siguientes aspectos:

- Planificación temporal y de dependencias de las pruebas a realizar.
- Casos de prueba basados en los casos de uso del sistema.
- Guiones de pruebas para cada uno de los casos anteriores.
- Registro de los resultados para cada uno de los guiones de prueba.

9 CONDICIONES GENERALES

9.1 Introducción

La realización de los trabajos se atenderá a las especificaciones al respecto contenidas en el Pliego de Cláusulas Administrativas Particulares que le es anejo al presente Pliego de Prescripciones Técnicas.

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.

9.2 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.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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.

9.3 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.

9.4 Entrega de los trabajos realizados

El adjudicatario, deberá entregar todos los programas (fuentes y ejecutables), librerías, scripts de compilación, especificaciones o cualquier otro componente que constituyan elementos del proyecto, embebido en una máquina virtual, o si lo decide el CRTM, en un repositorio subversión con toda la documentación técnica necesaria.

El adjudicatario no podrá hacer otras reproducciones, ni para uso propio ni para cesiones a terceros, no pudiendo quedarse con copia alguna de los mismos, debiendo contar con una autorización expresa y por escrito de la dirección del proyecto en el caso de que desee utilizarlos para alguna otra finalidad diferente de las derivadas del objeto del Contrato.

El adjudicatario no podrá utilizar para sí ni proporcionar a terceros, dato alguno de los trabajos contratados, ni publicar, total o parcialmente, el contenido de los mismos sin autorización escrita de este organismo. En todo caso el adjudicatario será responsable de los daños y perjuicios que se deriven del incumplimiento de esta obligación.

9.5 Entorno de trabajo

El trabajo se realizará en las oficinas del adjudicatario.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



9.6 Transferencia de conocimiento

El adjudicatario deberá establecer, conjuntamente con la dirección del proyecto del CRTM, un plan para la transferencia de conocimiento, teniendo en cuenta que ésta ha de realizarse en dos etapas:

- Transferencia de conocimiento constante: A lo largo del desarrollo del proyecto. Acompañando el desarrollo del mismo, se deberán establecer hitos en los que se muestre todo aquello que se va produciendo, tanto a los usuarios de negocio como a los usuarios que gestionarán y administrarán la plataforma tecnológica. Para ello, se actualizará la documentación técnica, por parte del adjudicatario, en la frecuencia establecida por el CRTM.
- Transferencia a la finalización del proyecto: El adjudicatario se compromete a transferir el conocimiento y colaborar a la finalización del contrato para la reversión del servicio tal y como se detalla en el apartado “reversión del servicio”.

9.7 Reversión de servicio

El adjudicatario deberá ejecutar la reversión del servicio de la siguiente forma:

9.7.1. *Elaboración del plan de reversión del servicio*

El contratista deberá facilitar a la Dirección del Proyecto antes de los seis últimos meses de ejecución del contrato un Plan de Reversión del servicio, que deberá ser aprobado por el Comité Técnico del proyecto y que recogerá la planificación y ejecución de las siguientes tareas:

- Elaboración de un plan de Traspaso de Conocimientos en el que se detalle la planificación temporal, los contenidos y la metodología que se utilizarán para traspasar los conocimientos del Sistema al nuevo adjudicatario y/o al personal del CRTM, o ambos.
- Documentación funcional y técnica sobre los sistemas de información, procesos, productos, licencias y componentes instalados en la plataforma.
- Documentación sobre los modelos de bases de datos y formatos de ficheros utilizados en la plataforma.
- Entrega de todo el software y aplicaciones desarrolladas en el ámbito de este contrato, incluido el código fuente y documentación técnica asociada.

9.7.2. *Ejecución del plan de reversión del servicio*

El adjudicatario está obligado a realizar el traspaso de los sistemas construidos al nuevo adjudicatario. Este traspaso se realizará antes de la finalización del presente contrato y una vez aprobado por el CRTM el “plan de reversión del servicio”.

El adjudicatario deberá ejecutar el plan de reversión del servicio anteriormente descrito, que tendrá en cuenta los siguientes aspectos:

- El adjudicatario designará un responsable que pueda realizar técnicamente el traspaso de los servicios, módulos y programas construidos, los responsables de su mantenimiento, a fin de explicar, aclarar o complementar la documentación entregada.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



- El traspaso se realizará en horario de oficina del CRTM y en las oficinas del CRTM.
- Todas las aplicaciones a traspasar deberán disponer de documentación actualizada.
- Durante la ejecución del plan de traspaso de conocimiento al futuro contratista deberá garantizarse la continuidad del servicio.

10 PLAN DE TRABAJO

Con carácter previo a la ejecución de los trabajos objeto de la contratación regida por el presente Pliego de Prescripciones Técnicas (PPT) la empresa adjudicataria deberá presentar un plan de trabajo para cada aplicativo, que se someterá a la dirección del proyecto, el cual deberá contener, como mínimo, los siguientes elementos:

- Metodología pormenorizada según la cual se propone el adjudicatario realizar los trabajos, desarrollada hasta los niveles operativos y acompañada de las justificaciones pertinentes.
- Cronograma de actividades (diagrama de Gantt), desagregado por fases y principales grupos de tareas.
- Relación de recursos humanos integrantes del equipo técnico asignados a cada tarea, según los currículos presentados.
- Recursos técnicos que se pondrán a disposición del trabajo.
- Información de partida que el equipo técnico contratado hubiera recopilado o se propusiera recopilar con vistas a la ejecución de los trabajos.
- Definición clara de los documentos que se generarán tanto de reporte y seguimiento, como entregables finales.
- Plazos de ejecución y duración total de los trabajos.

11 DOCUMENTACIÓN

Durante la ejecución de los trabajos, el contratista deberá elaborar y presentar al director del Proyecto del CRTM la documentación necesaria correspondiente a las diferentes fases de los trabajos que permitan a este realizar el control y seguimiento de los trabajos contratados. A la finalización del contrato el adjudicatario aportará los correspondientes manuales de usuario para su validación por parte del CRTM, siendo lo suficientemente exhaustivos y completos para el posterior mantenimiento de las aplicaciones objeto del contrato. Por lo tanto, será preciso elaborar al menos la siguiente documentación:

- Actas de cada una de las reuniones de proyecto mantenidas.
- Especificaciones técnicas de los módulos a desarrollar y/o adaptar.
- Diseño Técnico de los módulos a desarrollar y/o adaptar.
- Manuales de usuario.
- Manuales de Administración y mantenimiento.

El soporte de la documentación será papel impreso y DVD, y en un formato que permita su posterior edición e impresión en papel.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



ANEXO 1: GLOSARIO DE TÉRMINOS

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.

AMP

Accelerated Mobile Pages (AMP, literalmente, «Páginas Móviles Aceleradas») es una iniciativa de código abierto que busca mejorar la web para todos. El proyecto permite la creación de sitios web de alto rendimiento en dispositivos móviles y plataformas Web.

Apache mod_jk

Es un módulo de interconexión entre Apache y servidores de aplicaciones, como es el caso de Tomcat, usando el protocolo AJP. <http://tomcat.apache.org/connectors-doc/> ,

API

Es un interfaz de programación de aplicaciones (API), un conjunto de subrutinas, funciones y/o procedimientos que ofrece una biblioteca para ser utilizado por otro software como una capa de abstracción

Backoffice

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

Blockchain

Una cadena de bloques (blockchain) es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se le añade metainformación relativa a otro bloque de la cadena anterior en una línea temporal. Mediante mecanismos criptográficos la información contenida en un bloque sólo puede ser repudiada o editada modificando todos los bloques posteriores.

BIT o sistema BIT o proyecto BIT:

El BIT (Billeteaje Inteligente del Transportes) es el núcleo de todo el cambio tecnológico que se está produciendo en el proceso de migrar la tecnología magnética de billeteaje 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.

CDC

El Centro de Desarrollo y Conformidad (CDC) comenzó su andadura en el año 2006 y su objetivo fundamental es ser el centro de referencia tecnológico que garantiza la compatibilidad de todos los elementos, equipos y sistemas, tanto hardware como software, que constituyen o puedan constituir parte del Sistema de Billeteaje Inteligente de Transportes (BIT) de la Comunidad de Madrid.

FM

Es un **Firmware Module**. Un módulo binario que contiene código ejecutable. Se utiliza en el núcleo HSM

GBIT

Gestión para el Billeteaje Inteligente del Transporte (GBIT) es la herramienta utilizada en las Oficinas de Gestión del CRTM que permite atender y resolver cualquier incidencia a los usuarios de la tarjeta de transporte público.

GBIT comenzó a desarrollarse a principios del 2007 y ha continuado progresivamente evolucionando y adaptándose a la evolución de las prestaciones de la tarjeta de transporte público, primero con la TTP y actualmente con la TTP y Multi.





Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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.

IA

Es el acrónimo de Inteligencia Artificial.

JSON

Es un formato de texto ligero para el intercambio de datos, alternativo a XML. Una de las ventajas de JSON sobre XML como formato de intercambio de datos es que es mucho más sencillo escribir un analizador sintáctico (parser) de JSON.

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.

Multi

Es la tarjeta Multi (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 Multi es pasiva y los lectores/validadores del sistema inducen la corriente suficiente para su funcionamiento. La Multi es una tarjeta anónima de transportes para la Comunidad de Madrid

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.

OTP

One Time Password o contraseña de un solo uso.

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



Comunidad
de Madrid

CONSEJERÍA DE TRANSPORTES
VIVIENDA E INFRAESTRUCTURAS



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.

SPAI

Sistema de Procesamiento Automático de Información.

Sistema encargado de procesar de forma automática y en régimen de 24x7x365, todas las transacciones generadas por todas las redes (de prepersonalización, personalización, venta de títulos, validación e inspección).

Además, se encarga de generar la información de configuración de las redes externas, ejecutar tareas programadas, monitorizar y notificar en tiempo real de anomalías en el tránsito de datos.

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. La TTP es una tarjeta personal de transportes para la Comunidad de Madrid

En Madrid, 5 de diciembre de 2018

EL DIRECTOR GERENTE,

(Alfonso Sánchez Vicente)

CONFORME,
EL ADJUDICATARIO

