



CONSEJERÍA DE TRANSPORTES,
INFRAESTRUCTURAS Y VIVIENDA

Comunidad de Madrid



**PLIEGO DE CONDICIONES TÉCNICAS PARA LA
CONTRATACIÓN DEL SERVICIO DE “SUPERVISIÓN Y
COORDINACIÓN DE LA ADAPTACIÓN DEL SPAI A LOS
NUEVOS SOPORTES BIT”**





**PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL
SERVICIO DE “SUPERVISIÓN Y COORDINACIÓN DE LA ADAPTACIÓN
DEL SPAI A LOS NUEVOS SOPORTES BIT”**

ÍNDICE

1	ANTECEDENTES	4
2	OBJETO DEL CONTRATO	5
3	ACTIVIDADES A DESARROLLAR	6
3.1	Implantación de nuevas funciones y productos sobre la TTP	6
3.1.1	Tarjeta anónima. Adaptación del SATTP	7
3.1.2	Títulos multiviajes y sencillos. Adaptación del SATTP	7
3.1.3	Suplementos	7
3.1.4	Pago parcial	8
3.2	Coexistencia de títulos de transporte	8
3.2.1	Adaptaciones de modelo de datos y TLV para la correcta implementación de nuevas especificaciones de coexistencia de títulos.	9
3.2.2	Detección de irregularidades en la coexistencia de títulos y notificación automática en tiempo de procesamiento por parte del SPAI	9
3.3	Adaptaciones del backoffice para dar soporte a la nueva estructura del mapa de memoria.	10
3.3.1	Ampliación y adaptación del SATTP para dar soporte a los nuevos ficheros de elementales	10
3.3.2	Adaptación de modelos de datos, procesos y servicios para la nueva estructura (prepersonalización, personalización, carga/recarga, inspección y validación).	10
3.3.3	Implementación de tratamiento de nuevas TLV's en el SPAI:	10



3.3.4	Coordinación, supervisión y control de la ejecución de los procesos en backoffice CRTM:.....	11
3.4	Adaptaciones a la nueva tarjeta soporte.....	11
3.4.1	Identificar, diseñar y coordinar las adaptaciones en el backoffice para el nuevo soporte.....	11
3.4.2	Implementar en el SATTP los comandos abiertos de comunicación a bajo nivel entre “SAM/HSM” y “tarjeta sin contactos/software dispositivo”. 11	
3.4.3	Ampliación del XTTP para adaptarlo al nuevo soporte	13
3.5	Adaptación para la virtualización de la TTP del CRTM.....	13
3.5.1	Identificar y diseñar modificaciones en backoffice, servicios y procesos por las implicaciones de seguridad de la virtualización de la TTP.	
	13	
3.5.2	Coordinar la adaptación al nuevo modelo de negocio.	13
3.5.3	Coordinación en fase de implantación y despliegue.	13
3.5.4	Integración con subsistema VLAT.....	13
3.5.5	Evolución del subsistema SECU.....	14
3.5.6	Ampliación del SATTP para integrarlo con LAT/SECU/VLAT	14
3.6	Adaptación del SPAI al nuevo sistema de intercambio de información para las liquidaciones a redes de venta	15
3.6.1	Diseño y planificación de modificaciones a acometer en el SPAI	16
3.6.2	Validar la ejecución técnica de los desarrollos.....	17
3.6.3	Coordinar y supervisar la puesta en producción	17
4	EJECUCIÓN DE LOS TRABAJOS.....	17
5	PLAZO DE EJECUCIÓN DE LOS TRABAJOS	18
6	GLOSARIO DE TERMINOS.....	18





1 ANTECEDENTES

El Consorcio Regional de Transportes de Madrid, en el ámbito del sistema BIT (Billeteaje Inteligente en el Transporte) ha terminado la implantación de la tarjeta de transporte público para abonos personales, en toda la Comunidad de Madrid (zonas A, B y C) y área de influencia (zonas E), así como de otros servicios relacionados con la propia TTP, actualmente con más de 2,8 millones de tarjetas, o del Plan de Modernización de Interurbanos.

Durante el 2017 se realizará la implantación de títulos multiviajes, sencillos y otros tipos (turísticos, urbanos, etc.), que se estima, aproximadamente entre un 28% y un 29% (referencia 2014) del total de la demanda. Estos títulos podrán cargarse y recargarse en diferentes tipos de tarjetas comerciales (personales, anónimas, etc.).

Por medio del *SPAI (Sistema de Procesamiento Automático de Información)*, inicialmente concebido para el Proyecto BIT (Billeteaje Inteligente en el Transporte) y para el PMI (Plan de Modernización de Interurbanos), se da soporte a todas las necesidades de intercambio y procesamiento automático de datos del CRTM. Este sistema se caracteriza por la alta carga transaccional por un lado, y la interoperabilidad entre sistemas y aplicaciones con datos muy heterogéneos por otro.





2 OBJETO DEL CONTRATO

El CRTM ha previsto evoluciones que aportan mayor flexibilidad en la definición de nuevos productos tarifarios y mejora en la explotación de datos, así como aumento en la seguridad pasiva de las tarjetas sin contacto.

Para ello se tienen que:

- A. Adaptar todos los subsistemas del *SPAI*
- B. Ampliar y adaptar modelos de datos, aplicaciones, procesos y servicios; así como de las infraestructuras necesarias en *backoffice*.
- C. Ampliación y adaptación del *SATTP*
- D. Diseño, coordinación e integración del *SPAI*, *SATTP* y *backoffice* en general, con los nuevos sistemas de seguridad.

Las aplicaciones, infraestructuras y subsistemas a los que se hace referencia son los siguientes:

- Arquitectura de servicios SOA integrada en el *SPAI*
- Sistemas de seguridad existentes (*SECEBIT*, *LATISECU*) o en fase de implantación (*VLAT*)
- Sistemas de balanceo de carga de todos los servicios BIT (seguridad y SOA)
- Bases de datos (*OLTP*) en cluster del *backoffice* BIT
- Infraestructura de *Big Data*.
- Servicio de Acceso a la TTP (*SATTP*)
- Sistema de reporte de incidencias centralizado
- Subsistemas de procesamiento de información recibida
- Subsistemas de procesamiento de información generada
- Subsistemas de registro, notificación y alarmas
- Subsistemas de transferencia de control de procesamiento



- PCyM (Panel de Control y Monitorización) del SPAI
- Subsistema de intercambio de información para las Liquidaciones a Redes de Venta

Dentro de este contexto, 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 supervisión y coordinación, en fase de diseño e implantación, de los puntos objeto de este contrato. También es objeto de este documento definir los procedimientos de ejecución y seguimiento de los trabajos contemplados.

3 ACTIVIDADES A DESARROLLAR

Los trabajos objeto de contratación se describen a continuación:

3.1 *Implantación de nuevas funciones y productos sobre la TTP*

Dentro del ámbito del *backoffice* del CRTM, el adjudicatario será responsable de:

- Coordinar a los diferentes equipos de trabajo cuyas tareas afecten al *backoffice* del CRTM.
- Verificar la adecuación de las soluciones propuestas a los requerimientos funcionales.
- Verificar la adecuación de las soluciones propuestas a los requisitos técnicos e infraestructuras software existentes en el CRTM, especialmente al SPAI y a la seguridad (sistemas SECEBIT/HSM/LAT/SECU).
- Determinar el impacto en el *backoffice*, especialmente en modelos de datos y capa de servicios.





- Validar la toma de requisitos y el análisis de necesidades de integración con el sistema existente.
- Colaborar y asesorar en los análisis funcionales a realizar por el CRTM.
- Verificar la correcta documentación de los equipos de trabajo y adecuación a las especificaciones técnicas.
- Validar las planificaciones de desarrollo y puesta en producción.
- Validar el alcance y adecuación de las matrices de pruebas.
- Coordinar la puesta en producción en el *backoffice* los nuevos productos y funcionalidades.

Estas nuevas funciones y productos (tarjetas, títulos y funcionalidades) son:

3.1.1 Tarjeta anónima. Adaptación del SATTP.

Debido a su pronta puesta en producción, el adjudicatario deberá acometer las modificaciones necesarias sobre los sistemas que lo requieran, en especial del SATTP, de forma que las nuevas tarjetas se puedan utilizar en las OGTP del CRTM. Así mismo, se deberán identificar los componentes del backoffice y procesos afectados, de forma que puedan tenerse en cuenta desde el origen en el resto de tareas necesarias para su puesta en marcha, y que serán acometidas por diferentes grupos de trabajo.

Esto implicará la implantación de la TLV CFh.

3.1.2 Títulos multivajes y sencillos. Adaptación del SATTP.

El adjudicatario deberá acometer las modificaciones necesarias sobre los sistemas que lo requieran, en especial del SATTP, de forma que en las nuevas tarjetas se puedan realizar operaciones de carga de sencillos y/o multivajes en las OGTP del CRTM.

3.1.3 Suplementos

Con la incorporación a la tarjeta sin contacto de los títulos sencillos, los multivajes y el suplemento del aeropuerto y la posibilidad de compra múltiple



de varios títulos en una sola operación por parte del usuario, se hace necesario modificar la transacción tradicional de venta de título y su transacción gemela de consulta de saldo.

Esto implicará la implantación de las TLV's: B9h, BAh, BBh, BCh, BDh, BEh y BEh.

3.1.4 Pago parcial

Se quiere implantar a la mayor brevedad posible la funcionalidad de Pago Parcial de Viajes, para lo que se han definido la TLV CDh, versiones v1.0, v2.0 y v3.0.

Al igual que en los puntos anteriores, es necesario identificar de forma temprana la interrelación con otros procesos y componentes del backoffice, para definir las necesidades que de estas se deriven.

Para la puesta en producción de estos puntos, es necesario que el adjudicatario identifique los procesos afectados y defina las tareas consolidación en *backoffice* que lleva a cabo el *SPAI*, de forma que quede integrada con las aplicaciones de negocio que lo requieran.

3.2 Coexistencia de títulos de transporte

La coexistencia de títulos de transportes consiste en la selección de los mismos adecuado en cada circunstancia, es decir, a la prioridad de elegir automáticamente un título frente a otro.

En el caso de la tarjeta de transportes del CRTM, puede albergar simultáneamente tres títulos de transportes diferentes, cada uno de los cuales, puede tener carga y recarga. Debido a la singular infraestructura de algunos operadores de transportes, como por ejemplo, compartir validadores para acceder a dos zonas tarifarias distintas, ejecutar una multivalidación cuando no lo es, etc...



Actualmente la correcta implementación de la coexistencia de títulos en la TTP, se traducirá en nuevas especificaciones BIT, tanto para la validación, como para las operaciones de carga/recarga, e inspección.

De esta forma el CRTM va a definir:

- Familias de títulos.
- Algoritmo de coexistencia de carga de títulos
- Algoritmo de prioridad en validación
- Algoritmo de inspección en base a la coexistencia.

Será tarea del adjudicatario:

- Identificar los componentes en *backoffice* afectados: modelos de datos, aplicaciones, procesos, servicios.
- Diseñar adaptaciones de *backoffice*
- Coordinar la implantación de las adaptaciones necesarias para asegurar la coexistencia según las especificaciones BIT.

, en especial:

3.2.1 Adaptaciones de modelo de datos y TLV para la correcta implementación de nuevas especificaciones de coexistencia de títulos.

3.2.2 Detección de irregularidades en la coexistencia de títulos y notificación automática en tiempo de procesamiento por parte del SPAI

Las modificaciones en las especificaciones de coexistencia de títulos implicarán una recodificación de los títulos actuales, proporcionando al mismo tiempo una agrupación en conjuntos (o familias) de títulos agrupados por características similares.

Debido a esto el adjudicatario será responsable de que la implantación no afecte al funcionamiento de la TTP en producción, es decir, a todos los procesos de



carga/recarga, validación e inspección.

3.3 Adaptaciones del backoffice para dar soporte a la nueva estructura del mapa de memoria.

La evolución y penetración de las nuevas tecnologías, tanto a nivel de los diferentes actores BIT como de los propios usuarios del transporte público, presentan un gran desafío para la tarjeta de transportes.

El elemento más condicionante que tiene el sistema BIT es el mapa de memoria que representa una tarjeta de transportes del CRTM.

Para ello, y fuera del alcance de este pliego, el CRTM está abordando la modificación de las especificaciones y aplicativos BIT.

Cambiar esto implica modificar no sólo el mapa de memoria de la actual TTP y de los aplicativos BIT, si no también gran parte del *backoffice* del CRTM, así como numerosos procesos y servicios afectados, además de a las propias transacciones BIT. Este cambio no sólo afectaría al CRTM, si no en mayor o menor medida, también a los *backoffice* de los diferentes actores BIT.

Las tareas a realizar son las siguientes:

3.3.1 Ampliación y adaptación del SATTP para dar soporte a los nuevos ficheros de elementales.

3.3.2 Adaptación de modelos de datos, procesos y servicios para la nueva estructura (prepersonalización, personalización, carga/recarga, inspección y validación).

3.3.3 Implementación de tratamiento de nuevas TLV's en el SPAI:

- Recibidas en el SID





- Publicadas en el SID

3.3.4 Coordinación, supervisión y control de la ejecución de los procesos en backoffice CRTM:

3.3.4.1 *PREPERSO*

3.3.4.2 *PERSONALIZACIÓN, ya sea en diferido cómo en el acto*

3.3.4.3 *CARGA/RECARGA*

3.3.4.4 *VALIDACION (zonas A, B, C y E) en todos los OPERADORES de la Comunidad de Madrid*

3.3.4.5 *INSPECCIÓN*

3.4 Adaptaciones a la nueva tarjeta soporte.

El nuevo mapa de memoria, puede implantarse en el chip actual Mifare DesFire EV1 o en otro chip. Teniendo en cuenta el cambio profundo que supone modificar la estructura del mapa de memoria (como se detalla en el epígrafe anterior), el CRTM se plantea si es una oportunidad para buscar independencia en el soporte físico. Para lo cual, además de disponer de una estructura independiente, se requiere la implementación de comandos de comunicación no propietarios.

Las tareas que el adjudicatario consistirán en:

3.4.1 Identificar, diseñar y coordinar las adaptaciones en el backoffice para el nuevo soporte.

3.4.2 Implementar en el SATTP los comandos abiertos de comunicación a bajo nivel entre "SAM/HSM" y "tarjeta sin contactos/software dispositivo".





La lista siguiente, muestra el conjunto de comandos identificados actualmente, y que por lo tanto se deben implementar. No obstante, al estar todavía este apartado en proceso de análisis y definición (y que no es objeto de este pliego) es posible que se identifiquen más:

- SELECCION DE APLICACIÓN, mecanismo mediante el cual se identificará de manera inmediata la familia de claves maestras correspondientes.
- SELECCION DE FAMILIA DE CLAVES (cada familia de claves tendrá un conjunto de 7 claves maestras).
- SELECCION DE INDICE DE CLAVE, para posteriormente poder establecer claves de sesión.
- SELECCION DE FICHERO: Comando para elegir un fichero de la aplicación.
- LEER FICHERO
- ESCRIBIR FICHERO
- VERIFICAR PIN: En función del rol del módulo SAM/HSM será necesario la introducción de un PIN antes de poder ejecutar ningún comando.
- FORMATEAR TARJETA
- OBTENER RESPUESTA DE UN COMANDO EJECUTADO
- LEER CLAVE DIVERSIFICADA
- ESTABLECER CLAVE DE SESIÓN. Todos los datos enviados entre las partes se cifran en AES con la clave de sesión negociada.
- GENERADOR DE FIRMA DE UNA TRANSACCIÓN
- GENERADOR DE NÚMEROS ALEATORIOS
- OBTENER NÚMERO DE SERIE DEL SAM/HSM
- OBTENER FECHA DE FABRICACIÓN
- OBTENER EL VALOR DEL CONTADOR N
- CIFRADO/DESCIFRADO





3.4.3 Ampliación del XTTP para adaptarlo al nuevo soporte

Además de las modificaciones del SATTP, se debe realizar el diseño e implantación de una nueva versión del XTTP que englobe las necesidades del nuevo soporte y permita interactuar -a través del servicio- con todos los clientes del mismo, y ofreciendo toda la funcionalidad que ofrecerá dicho soporte.

3.5 Adaptación para la virtualización de la TTP del CRTM.

La virtualización de tarjetas físicas sin contactos embebidas en smartphone con NFC es cada vez un escenario más cercano y probable. Aunque, en el momento de la redacción de este pliego, hay todavía muchas cuestiones que resolver; tanto desde el punto de vista de modelo de negocio, como desde el punto de vista técnico.

En cualquier caso, se han establecido una serie de tareas, que el adjudicatario deberá efectuar:

3.5.1 Identificar y diseñar modificaciones en backoffice, servicios y procesos por las implicaciones de seguridad de la virtualización de la TTP.

3.5.2 Coordinar la adaptación al nuevo modelo de negocio.

3.5.3 Coordinación en fase de implantación y despliegue.

3.5.4 Integración con subsistema VLAT.

Las tarjetas virtuales necesitan un mecanismo o plataforma propia para el control del ciclo de "vida" de las tarjetas virtuales. El CRTM debe definir incluso los algoritmos para generar números de serie únicos.

El subsistema VLAT (Lógica de Aplicación de Transporte Virtualizada), gestionará las funciones de prepersonalización, personalización y carga/recarga, que se podrían realizar bien por la interfaz OTA o bien utilizando



el canal NFC. Hay que decir que este subsistema requiere conectarse al subsistema *SECU* para poder realizar procesos de autenticación. El CRTM tiene especificada al completo la lógica de la aplicación de transportes en sus distintos aplicativos y las reglas de negocio.

Será tarea del adjudicatario la integración de todos los componentes en *backoffice* que lo requieran, especialmente los de la capa SOA y el SATTP.

3.5.5 Evolución del subsistema SECU.

El *SECU* es la plataforma interna del CRTM que se ocupa de la lógica de seguridad, conectando, cuando es preciso, con el sistema SECEBIT. Dicho subsistema tiene que ir añadiendo varias funcionalidades en 2017.

El adjudicatario tendrá que identificar, coordinar y supervisar los cambios necesarios en los diferentes componentes del *backoffice* debido a esta evolución, garantizando que no se ven afectados los procesos y aplicaciones en producción.

3.5.6 Ampliación del SATTP para integrarlo con LAT/SECU/VLAT

Actualmente el SATTP interacciona directamente con SECEBIT/HSM.

Por motivos de seguridad y encapsulamiento de funcionalidad, se pretende integrar el servicio con los sistemas LAT/SECU/VLAT.

Será tarea del adjudicatario el diseño de la arquitectura que permita dicha integración, identificando los componentes de *backoffice*, aplicaciones y procesos afectados, y permitiendo una transición del actual sistema al nuevo sin interferir con el sistema en producción.



3.6 Adaptación del SPAI al nuevo sistema de intercambio de información para las liquidaciones a redes de venta

El CRTM está en proceso de definición e implantación de un nuevo sistema de intercambio de información para poder efectuar de forma precisa la liquidación a redes de venta.

El SPAI se basa en una serie de patrones y reglas que permiten el procesamiento de numerosos tipos de información de forma automatizada, aportando una infraestructura sólida y flexible, y que cuenta entre otras con:

- Módulo cron (automatización de tareas de procesado)
- Definición declarativa de procesamiento de TLV's (descomposición de tramas, comprobación de firmas digitales, interacción con SECEBIT/HSM,)
- Módulo de notificación
- Módulo de transferencia de control
- Subsistemas de consolidación de datos (con base de datos BIT, PMI y diferentes esquemas y bases de datos corporativas del CRTM)
- Motor de reglas, que interactúa con sistemas de notificación y toma decisiones respecto a la calidad de datos recibidos y su elevación hacia aplicaciones de negocio.
- Módulo de seguridad. Basado en PKI e integrado con SECEBIT/HSM.
- Capa de servicios (SOA)

En fase de análisis (ya realizada o en proceso, y que no es objeto de este contrato), se ha detectado la necesidad de modificar parte de la infraestructura que provee el SPAI, y al menos y más en concreto, la de tratar ciertos paquetes de información divididos en varios fragmentos, pero manteniendo la relación



entre los mismos de forma que los procesos de liquidación se puedan llevar a cabo de forma satisfactoria.

Esta tarea ampliará por tanto las capacidades del *SPAI*, y se pretende que se vaya implantando progresivamente en el tratamiento de otros tipos de datos, siempre del tipo “información recibida” a través del *SID*.

Será tarea del adjudicatario la validación, coordinación y supervisión de la correcta ejecución de estos trabajos, así como la planificación de la pronta puesta en marcha de esta nueva funcionalidad, ya que de lo contrario se vería seriamente afectada la puesta en marcha del nuevo sistema de liquidación.

Para ello debe acometer los siguientes trabajos:

3.6.1 *Diseño y planificación de modificaciones a acometer en el SPAI*

- Identificar módulos y subsistemas del *SPAI* que se verán afectados.
- Diseño técnico de nuevos módulos y modificación de los actuales.
- Modificaciones en la arquitectura actual del *SPAI* y el *backoffice* en general.
- Ampliación de la capa de servicios para ofrecer la funcionalidad necesaria a las redes externas (redes de venta en particular) para acometer el proceso de intercambio de datos en paquetes fragmentados, de forma que se pueda (1) determinar la ausencia o corrupción de paquete de datos completo y (2) permitir el reenvío de los mismos, manteniendo la coherencia de los datos a nivel de negocio en todo momento.
- Notificación automática de anomalías y gestión del ciclo de vida de los paquetes de datos descritos en el punto anterior.
- Plan de despliegue

Será de especial importancia asegurar la compatibilidad e integración con la arquitectura del *SPAI*, así como de los procesos de intercambio de datos, comunicaciones y firma con los diseños de *TLV's* definidos en las



estructuras de datos y procesos del sistema *BIT* implicados en el proceso de liquidación. Las *TLV's* con las que se debe asegurar la compatibilidad serán las siguientes: 0xCA, 0xC2, 0xC4, 0xC9.

3.6.2 Validar la ejecución técnica de los desarrollos

Conforme a los patrones de diseño y frameworks utilizados por el CRTM, y utilizando los mecanismos e infraestructuras de seguridad (JMS, firma digital del CRTM, RSA, PKI, SECEBIT/HSM) establecidos en las especificaciones BIT del CRTM.

3.6.3 Coordinar y supervisar la puesta en producción

Teniendo en cuenta que el SPAI está en producción y funciona en 24x7x365, el sistema en producción no debe verse afectado en ningún momento.

4 EJECUCIÓN DE LOS TRABAJOS

La entidad adjudicataria realizará íntegramente todos los trabajos descritos en el apartado 0. Para ello el adjudicatario relazará una propuesta de planificación.

Teniendo en cuenta el estado de implantación del sistema BIT y las expectativas de incorporación de nuevos títulos y las necesidades de ofrecer una solución más robusta y eficiente a los procesos de liquidación a redes de venta, se detallan los hitos urgentes, cuya falta de cumplimiento originará de forma cierta un retraso en la planificación de puesta en marcha de los proyectos afectados -especialmente el proyecto BIT- que no sólo puede afectar al CRTM, sino también a los operadores de transporte u otros actores externos implicados:

- **Hito I:** Deberá estar totalmente concluido en 20 días a contar desde la fecha de formalización del contrato, las tareas a llevar a cabo son:

3.1.1. *Tarjeta anónima. Adaptación del SATTP.*

3.1.2. *Títulos multiviajes y sencillos. Adaptación del SATTP.*



- **Hito II:** Deberá estar totalmente concluido en 30 días a contar desde la fecha de formalización del contrato la tarea a llevar a cabo es la siguiente:

3.1.3. Suplementos.

- **Hito III:** Deberá estar totalmente concluido en 40 días a contar desde la fecha de formalización del contrato la tarea a llevar a cabo es la siguiente:

3.6.1. Diseño y planificación de modificaciones a acometer en el SPAI

La penalización a la empresa adjudicataria por el incumplimiento de alguno de estos hitos será la rescisión del contrato.

5 PLAZO DE EJECUCIÓN DE LOS TRABAJOS

El plazo de ejecución será de 24 meses, prorrogables por un periodo igual, a contar, como muy pronto desde el 1 de diciembre del 2016. En el caso de que la formalización del contrato sea posterior a la mencionada fecha, se comenzará a contar con fecha de formalización del contrato.

6 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.

OGTTP

Oficina de gestión de tarjetas de transporte público

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.





SATTP

Servicio de acceso a bajo nivel de la TTP, en modo lectura y escritura.

Permite interactuar a los lectores sin contacto con la TTP, siendo imprescindible para que las aplicaciones de gestión BIT del CRTM puedan acceder y modificar el contenido de las tarjetas.

Interactúa con los servicios ofrecidos por SECEBIT/HSM, y representa el contenido de la TTP mediante los formatos RAW, XTTP y XTTP/R

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

XTTP

Formato propietario del CRTM de la representación de la TTP, según las especificaciones BIT.

XTTP/R

También conocido como XTTP/Relax, permite la relajación de ciertas normas de las especificaciones BIT, de forma que se pueden representar situaciones anómalas para solución e investigación de incidencias, creación de tarjetas de prueba, etc.

Madrid, 28 de septiembre de 2016

EL DIRECTOR GERENTE,

Juan Ignacio Merino de Mesa

CONFORME,

EL ADJUDICATARIO

