CONSEJERÍA DE TRANSPORTES, INFRAESTRUCTURAS Y VIVIENDA
Comunidad de Madrid

CONSORCIO TRANSPORTES MADRID

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO PARA LA "COORDINACIÓN DEL SISTEMA DE PROCESAMIENO AUTOMÁTICO DE LA INFORMACIÓN DEL BILLETAJE INTELIGENTE DEL TRANSPORTE (SPAI) PARA SU EVOLUCIÓN HACIA MECANISMOS FINANCIEROS"

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO PARA LA "*COORDINACIÓN DEL SISTEMA DE PROCESAMIENO AUTOMÁTICO DE LA INFORMACIÓN DEL BILLETAJE INTELIGENTE DEL TRANSPORTE PARA SU EVOLUCIÓN HACIA MECANISMOS FINANCIEROS*"

ÍNDICE

1 ANTECEDENTES

El Consorcio Regional de Transportes Públicos Regulares de Madrid (CRTM), en el ámbito del sistema BIT (sistema de Billetaje Inteligente en el Transporte) ha concluído 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, los títulos multiviajes, que entraron en funcionamiento en enero del 2018.

Actualmente el sistema cuenta con más de 4 millones de tarjetas personales y 12 de millones de anónimas. Este volumen, genera aproximadamente 150 millones de transacciones al mes, que el CRTM debe procesar constantemente por medio del *SPAI* (*Sistema de Procesamiento Automático de Información*), inicialmente concebido para el Proyecto BIT (Billetaje Inteligente en el Transporte) y para el PMI (Plan de Modernización de Interurbanos). Pero que hoy, 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

Los sistemas del CRTM están evolucionado en la optimización de la integridad de información entre ventas y facturas.

El objeto de este documento es desarrollar los procesos necesarios en torno al seguimiento de todas las actividades que son desplegadas desde el Consorcio Regional de Transporte Públicos Regulares de Madrid en relación a las actuaciones tecnológicas para la evolución del SPAI (sistema de procesamiento automático de información) del CRTM relacionadas con el sistema de Billetaje Electrónico, y muy en particular con las que se refieren al ámbito financiero, destacando las tareas de facturación, envío de datos tributarios por el sistema de Suministro Inmediato de Información del IVA (SII), inspección, y actividades deducidas de la utilización de la pasarela de pagos del Crtm.

Todas las actividades a desarrollar, detalladas en el epígrafe 5, son necesarias para alcanzar la integración con la parte financiera del SPAI. 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 COORDINACIÓN DEL SPAI PARA SU EVOLUCIÓN HACIA MECANISMOS FINANCIEROS; efectuando la implementación, ampliación y/o adaptación de los sistemas, subsistemas y aplicaciones afectados cuando se requiera, en fase de diseño e implantación, de los puntos objeto de este contrato.

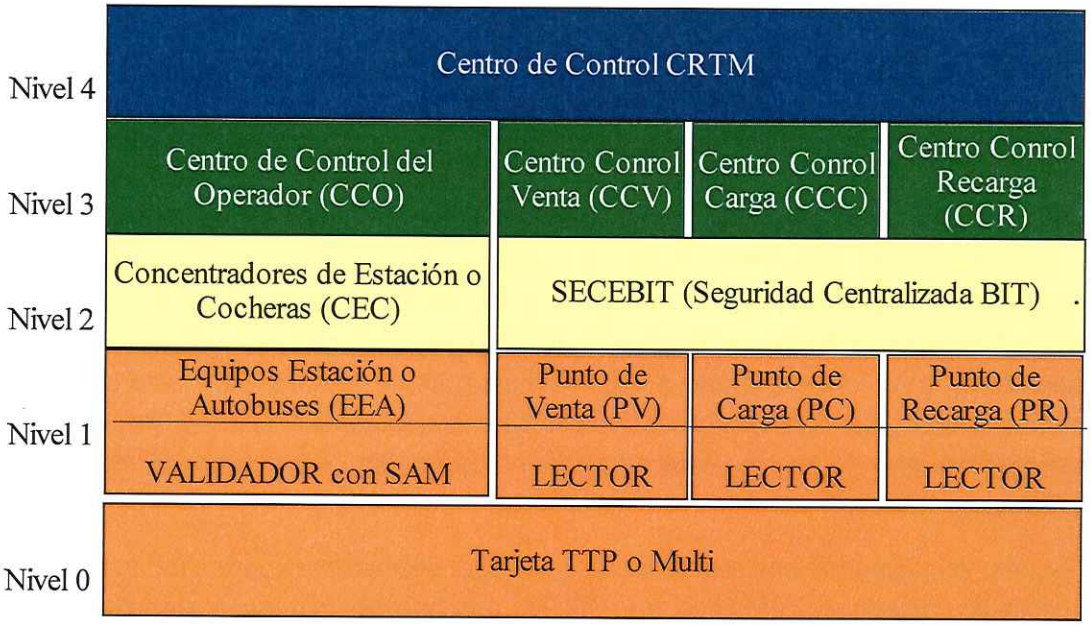
3 DESCRIPCIÓN GENERAL DEL SISTEMA BIT

El sistema BIT (Billetaje Inteligente del Transporte) es la evolución del sistema basado en

billetes magnéticos hacia sistemas basados en tarjetas sin contacto, ya sean estas últimas, físicas o virtuales. Este aparente simple cambio de soporte, ha supuesto profundos cambios, tanto técnicos como funcionales, en todos los niveles del transporte público de la Comunidad de Madrid.

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

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



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

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

Para la transmisión de la información de validación entre el nivel 3 (CCO) y el nivel 4 (CRTM) se elegirá una ventana de tiempo que garantice la velocidad de transmisión de los procesos, normalmente en modo nocturno, aunque pueden darse comunicaciones diurnas. El canal entre el nivel 3 y 4, es seguro, pues se ha utilizado FTP sobre SSH. Por este canal, se transmitirán desde el nivel 3 al nivel 4 toda la información correspondiente a los registros de validación generados en los operadores de transporte a lo largo del día. Por otro lado, el CCO descargará del CRTM la información necesaria para actualizar su sistema. La información que genera el CRTM es de naturaleza muy diversa; tarifas, configuraciones, listas de tarjetas no permitidas, etc.

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

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

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

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

Las tarjetas TTP y Multi, se ha implementado sobre DESFire de NXP, este chip incorpora mecanismos de seguridad que se basa en tres pilares, estos son:

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

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

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

- Cuando una tarjeta TTP o Multi, entra en el campo magnético del lector, se le induce una corriente que activa la tarjeta y responde con su número de serie. El lector recibe este dato y se lo reenvía al dispositivo de seguridad. En este momento todos los dispositivos están preparados para trabajar con la tarjeta.

- El programa del lector necesita leer o escribir en un determinado fichero, pero lo único que conoce es el índice de la clave que utilizará, es decir, solo conoce la posición de las claves únicas que tiene cada tarjeta. El lector le comunica a la tarjeta y al dispositivo de seguridad algo del estilo "vamos a trabajar con la clave 5". En definitiva, el lector coordina el trabajo, pero no entra en los detalles.

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

El dispositivo de seguridad, internamente, descifra el dato al que aplica una serie de operaciones para generar un segundo dato y también otro nuevo número aleatorio. Finalmente se cifra la concatenación de ambos números con la clave que indica el índice y el resultado se envía al lector. El lector hace eco de esta información hacia la TTP o Multi. Ahora la tarjeta descifra la información y obtiene ambos números. Si la tarjeta TTP (o Multi)

comprueba que uno de ellos, después de deshacer las transformaciones necesarias, es el número original que envió, entonces significa que el otro extremo conoce su clave para trabajar. Este es el segundo paso.

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

El sistema BIT, es también, un generador de datos. Cada proceso asociado a la vida de las tarjetas del CRTM (prepersonalización, personalización, carga, validación e inspección) genera una o varias transacciones que se envían al SID (Servidor de Intercambio de Datos) y que es procesado mediante el SPAI (Sistema de Procesamiento Automático de Información). El gran volumen de datos recibido se ha formalizado en un enorme modelo de datos en BBDD relacional, que a su vez, en la actualidad, alimenta a GBIT, herramienta de Gestión integral de BIT compuesta por numerosos módulos: Permite resolver cualquier problema a los usuarios de la TTP y Multi, realizar pedidos de diferentes tipos de tarjetas a fabricantes, gestionar stocks de tarjetas y módulos SAM, facturación, etc. y que se utiliza tanto dentro del CRTM como en las Oficinas de Gestión de Tarjetas (OOGG) del CRTM.

4 DESCRIPCIÓN GENERAL DEL SPAI

El SPAI, o *Sistema de Procesamiento Automático de Información* de BIT, es el sistema encargado de procesar de forma automática y en régimen de 24x7x365, todas las transacciones generadas por todas las redes (de fabricación, 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.

El SPAI se compone de una serie subsistemas y módulos, y está basado en una serie de patrones y reglas que permiten el procesamiento/generación de numerosos tipos de información de forma automatizada, logra una infraestructura veloz, sólida y flexible, permitiendo cubrir las necesidades de intercambio y procesamiento de datos con más de 60 actores diferentes (fabricantes, operadores de transporte, redes de venta, aplicaciones externas, etc.), así como ofreciendo una capa de servicios SOA.

Se puede dividir en otros grandes subsistemas, entre los que destacan:

4.1 SID

El SID o *Servidor de Intercambio de Datos,* está basado en el intercambio de ficheros por SSH. Su finalidad es intercambiar información entre el CRTM y los demás actores de BIT, tanto de entrada (información recibida por el CRTM), como de salida (configuración de terminales de la red externa como validadores/torniquetes y máquinas de venta, pedidos de tarjetas, etc.)

Hace un uso extensivo de PKI para evitar el uso de contraseñas, y el módulo principal que lo compone es el denominado "Monitorizador del SID", que detecta la transferencia de ficheros en tiempo real y notifica por JMS al SAyP.

4.2 SAyP (SPAI-CORE)

El SAyP o *Servidor de Aplicaciones y Procesos*, también conocido como (SPAI-CORE) es la parte más compleja del SPAI, y consiste en un servidor JEE que contiene el núcleo del sistema de procesamiento de archivos recibidos por los actores externos, así como la generación de información por parte del CRTM, y que se intercambiará bien a través del SID o a través de servicios (SOA), ofrecidos por este mismo subsistema o bien a través del "SPAI-SERVICES".

Los módulos que lo componen son:

- MÓDULO DE TRANSFERENCIA Y CLASIFICACIÓN DE FICHEROS
- MÓDULO DE GENERACIÓN Y PUBLICACIÓN DE FICHEROS
- MÓDULO CRON
  Para la automatización de procesos y tareas de carga de de datos.
- MÓDULO DE CARGA DE FICHEROS TRANSACCIONALES
  Estos datos vienen dados por transacciones de tipo TLV (transacciones e imágenes de la memoria de la tarjeta, en hexadecimal).
- MÓDULO DE CARGA DE FICHEROS NO TRANSACCIONALES
- MÓDULO DE SERVICIOS
  Basado en Web Services, Servlet y EJB/RMI.
- MÓDULO DE GESTIÓN DE EVENTOS Y MOTOR DE REGLAS
  Interactúa con sistemas de notificación y toma decisiones respecto a la calidad de datos recibidos y su elevación hacia aplicaciones de negocio (mediante los denominados procesos de consolidación), en especial con GBIT.
- MÓDULO DE NOTIFICACIONES
- MÓDULO DE LOGGING DEL SISTEMA
- MÓDULO DE SEGURIDAD

Basado en PKI, comprueba la integridad y autenticidad de todos los datos intercambiados con los diferentes actores.
Interacciona con SECEBIT/HSM/VLAT, para operaciones criptográficas (comprobación de firmas digitales, negociado de claves, etc.)

- MODULO DE CONFIGURACIÓN
  Permite la definición declarativa de procesamiento de TLVs de tipo hexadecimal (descomposición de tramas, comprobación de firmas digitales, comprobación de coherencia de datos, interacción con SECEBIT/HSM, etc.)
- MÓDULO DE REPOSITORIOS Y CACHE
  Está ligado íntimamente al anterior, y permite entre otras cosas procesar grandes cantidades de información a gran velocidad, llegando a ser superior a 1.500 tx/s. Es un módulo muy eficiente, teniendo en cuenta que, por ejemplo, comprueba que exista el número de chip de la tarjeta indicado en cada transacción producida en la red de transporte, y que a día de hoy existen más de 16 millones de tarjetas, recibiéndose aproximadamente 5 millones de tx al día.
- MÓDULO DE EJECUCIÓN DE PROCEDIMIENTOS ADICIONALES (TRANSFERENCIA DE CONTROL)
  Se utiliza para transferir datos y ejecutar procesos en otros sistemas del CRTM.

4.3 SPAI-SERVICES

Es la capa de servicios adicional que ofrece el SPAI, y que está íntimamente relacionada con el SAyP, a través de la tenología EJB y JMS.

Este subsistema se ha separado de la capa de servicios original del SAyP para lograr un mayor desacoplamiento entre servicios de diferente naturaleza, siendo unos de tipo interno (orquestamiento de procesos internos del SPAI e integración con GBIT) y de tipo externo (interacción en tiempo real con redes de venta y otros actores externos, aplicaciones web externas, móviles, etc.)

4.4 PCyM

El PCyM, o *Panel de Control y Monitorización* del SPAI, consistente en una GUI de configuración, gestión y supervisión del SPAI.

5 ACTIVIDADES A DESARROLLAR

Los trabajos objeto de contratación se describen a continuación:

5.1 Mejoras en los procesos de facturación de la TTP

El CRTM, tanto en sus OOGG (Oficinas de Gestión de Tarjetas) como a través de sus redes de venta (en especial las de venta de tarjetas y recarga de títulos, a través de sus diferentes

canales), ha puesto en marcha en 2019 un sistema de facturación que emite facturas simplificadas para el usuario en el propio momento de la venta. La casi totalidad de las facturas se emiten basándose en los propios HSM, a través de transacciones, y aprovechándose por lo tanto de los mecanismos de firma digital de las mismas.

Este sistema emite más de 5 millones de facturas mensualmente, y contempla una amplia y compleja casuística.

Se requiere el análisis, diseño e implentación de los mecanismos que doten al sistema de facturación de una mejor trazabilidad, detección y corrección de anomalías, y que cubran finalmente todos los posibles canales de emisión de facturas asociadas a la venta de tarjetas y recarga de títulos. Teniendo en cuenta las integraciones con el SII.

Debido a la complejidad del sistema de facturación, el adjudicatario deberá ejercer, en todo momento, las tareas de coordinación que se requieran entre los diferentes grupos de trabajo, bien del propio CRTM, como de las empresas implicadas (redes de venta externas) y los integradores de estas últimas.

Para ello, será tarea del adjudicatario:

5.1.1 Implementación en arquitectura SOA del tratamiento de facturas

Actualmente en sistema se basa en el procesamiento de transacciones hexadecimales empaquetadas en ficheros y procesadas por el SPAI, que a su vez se integra con GBIT mediante la consolidación de dichas transacciones (en adelante "*tx*") una vez cargadas.

Se pretende que se controle todo el ciclo de vida de las facturas mediante un sistema on-line mediante servicios (arquitectura SOAP), que amplíe y se integre con el ya existente y que está basado en tratamiento de ficheros.

Se han identificado las siguientes tareas:

5.1.1.1 *Procesamiento on-line de tx de facturas emitidas*

Se corresponden con los formatos de datos dados por las siguientes TLV's:

- TLV=(F4h; v1.0): Registro de tx de factura simplificada PRUEBAS/GRAL
- TLV=(F5h; v1.0): Registro de tx de factura rectificativa PRUEBAS/GRAL
- TLV=(F6h; v1.0): Registro de tx de factura simplificada PRUEBAS/TFM
- TLV=(F7h; v1.0): Registro de tx de factura rectificativa PRUEBAS/TFM
- TLV=(FAh; v1.0): Registro de tx de factura simplificada PROD/GRAL
- TLV=(FBh; v1.0): Registro de tx de factura rectificativa PROD/GRAL
- TLV=(FCh; v1.0): Registro de tx de factura simplificada PROD/TFM
- TLV=(FDh; v1.0): Registro de tx de factura rectificativa PROD/TFM

El modelado de eventos debe estar perfectamente integrado con el del SPAI, pues realmente son dos vías diferentes de suministro de información de facturas de facturas del CRTM asociadas a la venta de tarjetas y recarga de títulos, y en casos especiales, no asociados siquiera a la TTP (por ejemplo debido al acceso masivo y puntual de usuarios al Transporte Público de la CAM en eventos deportivos; así como a otros conocidos).

5.1.1.2 *Consulta de información on-line para redes de venta, internas o externas*

En función de la problemática conocida, pero también de la que pueda ir apareciendo durante la duración del contrato, se deberán identificar las características de dichos servicios, así como el modelado de procesos e interacciones entre los actores implicados, para permitir la identificación de problemas (falta de información, descuadres, errores o anomalías en los datos suministrados, etc.).

Será también tarea del adjudicatario el implementar dichos servicios, integrándolos con el backoffice del CRTM, y especialmente con el SPAI y GBIT.

5.1.1.3 *Servicios de resolución de problemas y/o modificación de información de facturación*

Muy relacionado con el punto anterior, y bajo las mismas premisas, el adjudicatario deberá de acometer las tareas necesarias para la resolución de las incidencias de facturación a través de servicios, lo cual permitirá a las propias redes de venta externas solventar de forma automatizada los problemas relacionados con las facturación.

5.1.2 Implementación de facturación en el Sistema de Acceso a la Tarjeta

Para dar respuesta a ciertas necesidades de negocio relacionadas con una mejor atención a los usuarios del transporte público, se ha incluido información del histórico de facturación en la propia memoria de la TTP.

Por lo tanto esto implica implementar una nueva funcionalidad en el Sistema de Acceso a la Tarjeta, que hasta ahora no era requerida.

Se han identificado las siguientes tareas:

5.1.2.1 *Implementar el tratamiento del nuevo FEhf*

Este nuevo fichero elemental es el Histórico de Facturas (FEhf).
El Sistema de Acceso a la Tarjeta debe contemplar la lectura/escritura del mismo en la memoria de la TTP, conforme a las reglas de negocio establecidas por el CRTM.

5.1.2.2 *Ampliación del XTTP para soportar el FEhf*

El *XTTP* es un estándar de serialización de la información de la TTP definido por el CRTM para el proyecto BIT, en el que se pasa bidireccionalmente del binario (hexadecimal) de la memoria de la tarjeta a un formato de más alto nivel en XML.

El adjudicatario deberá de ampliarlo para soportar el nuevo FEhf, haciéndolo compatible con todos los sistemas que de él dependen, en especial con GBIT.

5.1.2.3 *Adaptación de modelos de datos, procesos y servicios afectados*

Cambiar esto implica no sólo el tratamiento que hará el Sistema de Acceso a la Tarjeta con el mapa de memoria y el XTTP, si no que también hay que adaptar GBIT para que finalmente se ofrezca la funcionalidad deseada en el servicio al usuario en las OOGG.

Será tarea del adjudicatario identificar los puntos afectados en el backoffice, y en especial de GBIT, para diseñar la interfaz de comunicación y modelado de procesos entre ambos sistemas (Sistema de Acceso a la Tarjeta y GBIT), acometiendo las implementaciones necesarias y coordinando los cambios necesarios por otros grupos de trabajo, para permitir la integración de los mismos.

En cualquier caso la funcionalidad ofrecida por este sistema debe permitir efectuar al menos los siguientes procesos de negocio:

- PREPERSO (sólo la capacidad relacionada con la resolución de incidencias en OOGG)
- PERSONALIZACIÓN
- CARGA/RECARGA
- CAMBIOS DE ZONA
- RESTAURACIÓN DE TARJETAS
- FACTURACIÓN
- INSPECCIÓN (sólo la capacidad relacionada con la resolución de incidencias en las OOGG)

5.2 Mejora de los procesos de Personalización Masiva

5.2.1 Personalización Masiva

Personalización masiva (PM) es el proceso industrial de personalización de una gran cantidad de tarjetas, que consiste en último término, en grabar en la memoria de la tarjeta sin contactos el fichero de "datos generales" y el fichero de "activación y perfiles" además de imprimir en las tarjetas (si se trata de tarjetas personales) determinada información, generalmente la foto, el nombre, apellidos y el número TTP.

La información almacenada en la tarjeta se notifica al CRTM mediante los TLVs correspondientes, y que se detallarán a continuación, indicando además cuales son objeto de los trabajos requeridos en este pliego.

5.2.1.1 *Tratamiento on-line de tx de personalización*

Siguiendo las mismas premisas que se han indicado en puntos anteriores para la capa servicios SOA y que se integrarán como parte del SPAI, el adjudicatario se encargará del diseño e implantación de los servicios que se requieran, con el objetivo final de la puesta en producción del tratamiento on-line de este tipo de transacciones.

El objetivo es mejorar la velocidad y eficiencia en la transmisión de la información al CRTM por parte de los fabricantes externos, permitiendo indentificar anomalías y problemas en tiempo real.

En concreto, será tarea del adjudicatario el tratamiento on-line de las tx (transacciones BIT), incluyendo imagenes de FE escritos en la tarjeta en el proceso de personalización, y que se corresponden con los formatos de datos dados por las siguientes TLVs:

- TLV=C4h: Registro de transacción de personalización de tarjetas (personalización) [PER]
- TLV=CAh: Registro de transacción de personalización para operadores de trenes (personalización) [PER]
- TLV=D4h: Imagen del FEdg: Registro de datos generales (personalización) [DGN]
- TLV=D5h: Imagen del FEdp: Registro de datos personales (personalización) [DPR]
- TLV=D6h: Imagen del FEap: Registro de activación y perfiles (personalización) [DAP]
- TLV=D9h: Imagen del REdp: Registro de datos personales de tutores (personalización) [DPR]. Estos datos viajan cifrados y se descifran por el SPAI, mediane SECEBIT/HSM.

Las tx que conllevan datos personales (registro REdp) están cifrados, para lo que es necesario integrarse con los sistemas SECEBIT/HSM para poder descifrarlos.

No se procesarán on-line otros ficheros generados en este proceso y que serán subidos al SID y cargados por el SPAI. No obstante se indican en este pliego ya que deberán ser tenidos en cuenta para las tareas que se detallarán en el siguiente punto "*5.2.1.2. Servicios de consulta de estado de pedidos de personalización*".

Estos ficheros contienen fotos, solicitudes, escaneados, etc. y que vienen con los formatos definidos por:

- TLV=I0h: Corresponde a los ficheros de fotos recibidos [I0]

- TLV=DOCAZULh: Documentos adjuntos a la personalización de la tarjeta azul [DOCAZUL]
- TLV=DOCPERh: Documentos adjuntos a la personalización de la tarjeta TTP [DOCPER]
- TLV=DOCTTPh: Documentos adjuntos a la personalización de la tarjeta TTP [DOCTTP]

Finalizado el proceso, el fabricante envia al CRTM informes del resultado del proceso, que sirve además de para identificar las incidencias que hayan impedido llevar a cabo una personalización determinada, para asociar la tarjeta a la solicitud del usuario que pidió la misma:

- TLV=E2h: Informe de Personalización Masiva [IPM]

Asociada a la personalización de tarjetas se encuentra la solicitud, de donde se podrán extraer los datos personales del usuario para la generación de las tarjetas y de los TLV asociados. Existen una serie de formatos de ficheros XML para soportar esta información para un proceso industrial.

En el proceso de personalización masiva se distinguirán tanto la parte física del proceso, como la parte electrónica, debido a que a veces una puede ser correcta pero la otra no, dando como resultado una personalización fallida, y que habrá que subsanar consecuentemente.

El sistema soporta varios tipos de tarjetas comerciales, entre otros:

- Tarjetas personales (TTP normal)
- Tarjetas anónimas (MULTI, turísticas, eventos especiales, etc.)
- Tarjeta Azul (TAZ)
- Tarjeta Abono Anual (TAA)
- Tarjeta Infantil (INF)

En función del tipo de tarjeta comercial (que vendrá fijado del proceso de "prepersonalización"), se definen los posibles títulos y perfiles/colectivos que podrá alojar la tarjeta, y que se basan en mapas de memoria e instrucciones concretas para cada caso.

5.2.1.2 *Servicios de consulta de estado de pedidos de personalización*

Con el fin de mejorar los sistemas de seguimiento de pedidos de personalización masiva de tarjetas, resolución de incidencias e información al usuario, y con el objetivo final de reducir los tiempos de personalización efectiva y el impacto de la resolución de incidencias, será tarea del adjudicatario la identificación y modelado de procesos, e implementación de los servicios necesarios, y que se deberán ofrecer tanto a fabricantes externos como a GBIT y

los módulos de aplicaciones web del CRTM que lo requieran (por ejemplo las de información al usuario).

5.3 Personalización masiva extendida

La personalización masiva extendida (PME) es un tipo de personalización masiva a la que se le incorpora la carga de un titulo en el mismo proceso, generando las transacciones equivalentes a la personalización tal como se ha indicado en el punto "*5.2.1. Personalización Masiva*", y las transaciones de la carga de título.

En la personalización masiva/extendida, en el pedido a fabricantes se especificará el tipo de titulo que se cargará en la tarjeta así como el año a partir del cual el título se activa, y si fuera necesario, la zona límite.
Tanto las tarjetas personales como las anónimas podrán ser objeto de la personalización masiva extendida y con carácter general cualquier tipo de tarjeta comercial.

Los pedidos de tarjetas a los fabricantes externos se materializan mediante los siguientes formatos de datos:

- TLV=DBh: Solicitud de personalización masiva y extendida (Origen CRTM) [SPMIG]
- TLV=ITTPh: Fotos Personalización masiva y extendida de TTP [ITTP]

Además el propio CRTM puede ejercer de personalizador masivo, para lo cual se utiliza el formato:

- TLV=DAh: Solicitud de personalización masiva y extendida (Origen Red Externa) [SPM]

5.3.1 Tratamiento on-line de tx de carga de títulos asociados a la PME

Será tarea del adjudicatario poner en producción el tratamiento on-line de las tx e imágenes de FE escritos en la tarjeta de transportes, en el proceso de carga de títulos, y que se corresponden con los formatos de datos especificados por las siguientes TLVs:

- TLV=BCh: Registro de transacción de venta múltiple de títulos no-trenes (venta de títulos) [TTV]
- TLV=C9h: Registro de transacción de venta de títulos no de operadores de trenes (venta de títulos) [TTV]
- TLV=D3h: Imagen del FEdt (venta de títulos) [TTT]

5.3.2 Servicios de consulta de estado de pedidos de PME

Soportando todas las cuestiones definidas en el punto "*5.2.1.2. Servicios de consulta de estado de pedidos de personalización*", pero cubriendo además, la casuística derivada de la personalización masiva/extendida de tarjetas.

5.4 Adaptaciones derivadas de la puesta en marcha de la aplicación de inspección para operadores interurbanos

Las tareas consistirán en:

5.4.1 Identificar, diseñar y coordinar las adaptaciónes en el backoffice para la aplicación de inspección

5.4.2 Implementación de los servicios (SOA) que se requieran

Siguiendo las mismas premisas que se han indicado en puntos anteriores para la capa servicios SOA y que se integrarán como parte del SPAI, el adjudicatario se encargará del diseño e implantación de los servicios que se requieran.

En concreto:

5.4.2.1 *Tratamiento on-line de tx de inspección*

Se corresponden con los formatos de datos dados por las siguientes TLV's:

- TLV=(C5h; v1.0): Registro de tx de inspección [INS]
- TLV=(C7h; v1.0): Registro de tx de inspección de operadores de autobuses [INS]
- TLV=(D7h; v1.0): Registro de datos personales REdp [DPI]
- TLV=(90h; v1.0): Registro de tx de inspección de título mediante HSM [INSHSM]
- TLV=(91h; v1.0): Registro de observación de inspección de título mediante HSM [INSOBS]
- TLV=(DCh; v1.0): Registro de datos personales REdp (inspección) por HSM [INSDPI]

Las tx que conllevan datos personales (registro REdp) están cifrados, para lo que es necesario integrarse con los sistemas SECEBIT/HSM para poder descifrarlos.

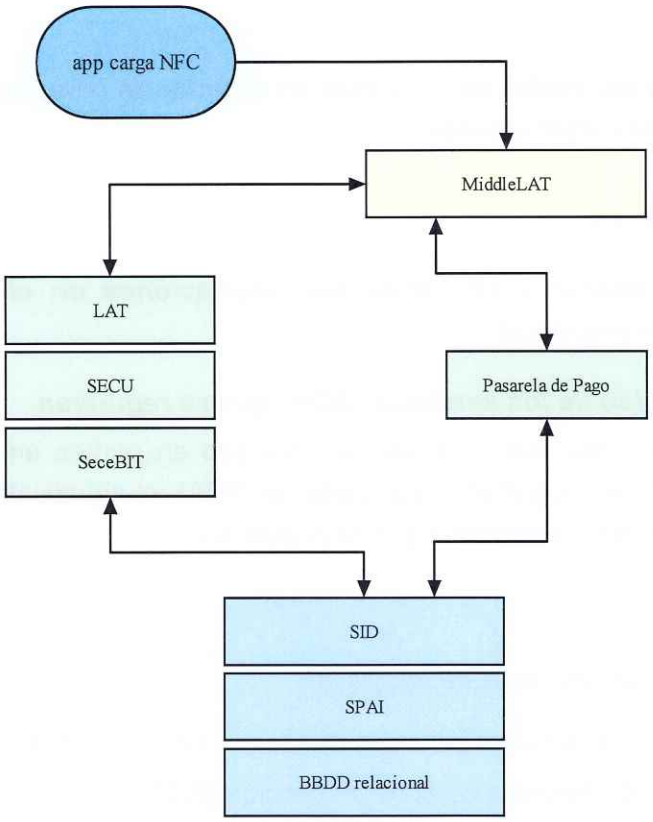
5.5 Integración entre SPAI y PASARELA DE PAGOS

El CRTM integrará con una pasarela de pago, sus 3 canales directos con los usuarios:

- Canal APP (aplicaciones móviles de venta de títulos en tarjetas físicas y emuladas).

- Canal Web para la solicitud de tarjetas y/o títulos.
- Red de oficinas de gestión del transporte publico.

Los canales, se integrarán con el SPAI/SID, siguiendo diferentes métodos. En el caso de la app, el flujo se muestra en el siguiente esquema:



El sistema BIT generará, fuera del ámbito de las pasarelas de pago, transacciones de todos los eventos que ocurren con las tarjetas de transporte. Las transacciones de venta de tarjeta y de título, y la correspondiente transacción de facturación deben ser conciliadas con la información recibida de la pasarela de pago en el SID.

El proceso de conciliación, que ejecuta el CRTM, responsabilidad del adjudicatario, debe verificar que los sucesos acontecidos en la plataforma de pago corresponden con sucesos en el sistema BIT y viceversa. Señalara los sucesos huérfanos de correspondencia en cualquiera de los ámbitos.

Para ello, el SPAI deberá procesar toda la información recibida y posteriormente activar los procesos de conciliación de GBIT

Desde el CRTM se cruzará por el número de serie de la tarjeta o por el número de solicitud, la información financiera recibida con la información de transportes del sistema BIT.

Una vez detectados los descuadres (para ello, el SPAI debera integrarse con los servicios web de la pasarela de pago que a su vez dará servicio a GBIT), se actuará de una de las siguiente forma:

1- Se intenta de nuevo el cobro no logrado (o como venta nueva), si se ha cargado el título de transporte

2- Reintentar cargar el titulo, si el cobro se ha realizado correctamente.

3- Poner la tarjeta de transporte en lista de tarjetas no permitidas.

4- Devolver el cobro al usuario.

Mediante orden a la pasarela de pago, a través del sistema del CRTM (GBIT) o mediante el portal de la propia pasarela.

6 Tiempos previstos en el desarrollo de las actividades a desarollar.

Por claridad, se muestra aquí una tabla estimada de los tiempos previstos:

	Tiempo medio estimado (en días)
5.1: Mejoras en los procesos de facturación de la TTP (total de todos los subapartados de este epígrafe del PPT)	**105**
Epígrafes del PPT 5.1.1.1 y 5.1.1.3 (valor medio)	25
Epígrafes del PPT 5.1.1.2	20
Epígrafes del PPT 5.1.2.1 y 5.1.2.2 (valor medio)	45
Epígrafes del PPT 5.1.1.3	15
5.2: Mejora de los procesos de Personalización Masiva (total de todos los subapartados de este epígrafe del PPT)	**30**
Epígrafes del PPT 5.2.1.1	15
Epígrafes del PPT 5.2.1.2 (valor medio)	15
5.3: Personalización masiva extendida (total de todos los subapartados de este epígrafe del PPT)	**35**
Epígrafes del PPT 5.3.1	15
Epígrafes del PPT 5.3.2 (valor medio)	20
5.4: Adaptaciones derivadas de la puesta en marcha de la aplicación de inspección para operadores interurbanos (total de todos los subapartados de este epígrafe del PPT)	**30**
Epígrafes del PPT 5.4.1	15
Epígrafes del PPT 5.4.2/5.4.2.1	15
D5: Integración entre SPAI y PASARELA DE PAGOS (incluye todos los subapartados de este epígrafe del PPT)	**52**

7 Equipo técnico

Para la correcta consecución de los objetivos planteados, el adjudicatario deberá poner a disposición del proyecto el equipo humano y técnico que fuere preciso, debiendo contar con al menos un profesional que reúna el siguiente perfil:

- Titulación en ingeniería superior.
- Experiencia (mínimo 3 años) demostrable en:
  1.- Direccion e implantación de proyectos de tecnologías de la información (ti) en el ámbito del transporte público
  2.- Implantación de sistemas de billetaje basado en "mifare desfire - iso 1444a" en el ámbito del transporte público
  3.- Administración e implantación de sistemas basados en linux y/o solaris
  4.- Administración e implantación de tecnologías xml, jee y oracle
  5.- Desarrollo de proyectos con c++ y en implantación/administración de oracle rac.

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

8 CONDICIONES GENERALES

8.1 Introducción.

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

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

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

8.2 Dirección del proyecto.

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

Las funciones del Director de Proyecto del CRTM serán:

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

Las funciones del Director Técnico del contratista serán:

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

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

8.3 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.

8.4 Carácter llave en mano.

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

9 GLOSARIO DE TERMINOS

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

BIT o sistema BIT o proyecto BIT:

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

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.

Sistema de Acceso a la Tarjeta

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.

RAW

El formato RAW representa los ficheros elementales (FE) de la memoria de la tarjeta y su contenido en hexadecimal.

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.

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.

Backoffice

Se refiere a los sistemas y procesos informáticos internos que realiza el CRTM, que dan servicio y soporte, entre otras, a las aplicaciones de gestión de la TTP/BIT.

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.

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 interactua con cualquier lector. Dichas transacciones, de tipo TLV se envían al CRTM mediante el SID.

SID

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.

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.

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.

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.

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.

HCE

Host Card Emulation.

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 HSM's 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).

Madrid, 14 de octubre de 2019

POR LA ADMINISTRACIÓN,

EL DIRECTOR GERENTE,

CONFORME:

EL ADJUDICATARIO

Luis Miguel Martínez Palencia