CONSEJERÍA DE TRANSPORTES, INFRAESTRUCTURAS Y VIVIENDA

Comunidad de Madrid

CONSORCIO TRANSPORTES MADRID

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE "SUPERVISIÓN Y COORDINACIÓN DE LA ADAPTACIÓN DEL SISTEMA BIT EN NUEVOS SOPORTES"

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE "SUPERVISIÓN Y COORDINACIÓN DE LA ADAPTACIÓN DEL SISTEMA BIT EN NUEVOS SOPORTES"

ÍNDICE

PLIEGO DE CONDICIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE "SUPERVISIÓN Y COORDINACIÓN DE LA ADAPTACIÓN DEL SISTEMA BIT EN NUEVOS SOPORTES"

1. ANTECEDENTES

El Consorcio Regional de Transportes de Madrid, en el ámbito del sistema BIT (Billetaje 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). Contando actualmente con más de 2,8 millones de tarjetas.

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...).

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. Cuya supervisión, coordinación, diseño y pruebas quedan en el ámbito de los objetivos de esta licitación, y que suponen cinco grandes líneas de actuación:

- Puesta en producción de títulos multiviajes y sencillos.
- Coexistencia de los diferentes títulos de transportes
- Nueva estructura en el mapa de memoria.

CONSORCIO REGIONAL DE TRANSPORTES MADRID

- Definición de la nueva tarjeta soporte físico del CRTM
- Definición de la virtualización de la nueva tarjeta soporte del CRTM

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, coordinación, diseño y pruebas 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 Coordinación en la implantación de la tarjeta anónima.

Anteriormente a esta licitación, el CRTM ha adaptado las especificaciones a un nuevo tipo de tarjeta, denominada anónima, donde es posible cargar títulos no personales, por ejemplo; títulos sencillos, multiviajes y otros tipos (turísticos, urbanos, etc...). Dicho soporte de tarjetas anónimas, se basa en el mismo chip que tiene la TTP (tarjeta de transporte público), que alberga títulos personales. El mapa de memoria de la tarjeta anónima garantiza la compatibilidad. Sin embargo, requieren procesos exclusivos como es la personalización ligera. En cualquier caso, el CRTM ya ha superado esta fase y durante el segundo semestre del 2016 se ha ejecutado un piloto.

No obstante, la puesta en producción requiere reconfiguraciones y un seguimiento con todos los operadores de transporte que el adjudicatario deberá supervisar y coordinar.

3.1.1.- Reconfiguración de ficheros de tarifas: Tarifas jerarquizadas, en función del título, perfil y colectivo. Tanto para redes de venta, como para redes de

validación.

3.1.2.- Reconfiguración de ficheros de propiedades: Propiedades de los títulos para redes de venta de títulos

3.1.3.- Supervisión de la extensión de TLVs en las redes de venta.

3.1.4.- Supervisión de la extensión de TLVs en los operadores de transportes.

3.1.5.- Pruebas en real.

.

3.2 Coexistencia de los diferentes títulos de transportes en todos los ámbitos de aplicaciones.

Se entiende, por coexistencia de títulos de transportes, el problema asociado a la selección de los mismos adecuado en cada circunstancia, es decir, a la prioridad de elegir automáticamente un título frente a otro.

Esta problemática aparece en primer lugar, debido a que la tarjeta de transportes del CRTM puede albergar simultáneamente tres títulos de transportes diferentes, cada uno de los cuales, puede tener carga y recarga. En segundo lugar, la situación se complica por 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...

Las especificaciones iniciales del sistema BIT definieron dos formas posibles de grupos de títulos; los títulos tipo abonos (todos, los mensuales y anuales) y los títulos de tipo multiviajes. También, se definió que en estas tarjetas sólo podría contener un único título de tipo abono y dos títulos excluyentes entre sí de tipo multiviaje. Estableciéndose siempre el abono como título prioritario frente a cualquier otro. Sin embargo, esta coexistencia es muy superficial y del todo insuficiente frente a la diversidad de tipos de títulos que posee el CRTM.

El adjudicatario deberá especificar los siguientes procesos:

3.2.1.- Familias de títulos.

Se requiere una recodificación de los títulos actuales sin que afecte a su funcionamiento en producción (es decir, en todos los procesos de carga/recarga, validación e inspección) proporcionando al mismo tiempo una agrupación en conjuntos (o familias) de títulos agrupados por características similares.

3.2.2.- Algoritmo de coexistencia de carga de títulos

3.2.3.- Algoritmo de prioridad en validación

3.2.4.- Algoritmo de inspección en base a la coexistencia.

3.3 Nueva estructura del mapa de memoria.

Quizás el elemento más condicionante que tiene el sistema BIT es el mapa de memoria que representa una tarjeta de transportes del CRTM. Cambiar esto implica modificar todos los aplicativos además de transacciones, por lo que afectaría, posiblemente también a los backoffice de los diferentes actores, incluido el propio CRTM.

Este pliego aborda la parte de especificaciones y aplicativos, dejando la línea de backoffice para otra licitación.

Las tareas a tratar, en base a la zonificación, tipología de títulos y su comportamiento, y perfiles usuarios, son las siguientes:

3.3.1.- Definición de ficheros de elementales.

3.3.2.- Definición de especificaciones técnicas del sistema BIT con la nueva estructura (prepersonalización, personalización, carga/recarga, inspección y validación)

3.3.3.- Coordinación de los distintos industriales y actores BIT con el CDC (Centro de Desarrollo y Conformidad) para pruebas

•Revisión de la documentación entregada en el sistema.

•Especificar las condiciones y entornos de pruebas de cada tecnología

•Definición de protocolos de pruebas funcionales de las nuevas tecnologías que se incorporen al sistema.

•Definición y desarrollo de protocolos de pruebas adicionales de las nuevas tecnologías.

3.3.4.- Protocolos de pruebas integrados con el resto de tecnologías BIT.

•Pruebas extremo a extremo.

•Protocolos de pruebas orientados a la seguridad

•Protocolos de pruebas encaminados a verificar la fiabilidad de las tecnologías

•Protocolos de pruebas de interoperabilidad

•Análisis de los datos producidos en los entornos de pruebas

•Determinación de criterios de calidad previos a la puesta en producción.

•Definición y desarrollos de pruebas para la integración de SAE y sistemas BIT.

3.3.5.- Análisis y propuesta sobre las alternativas tecnológicas que los adjudicatarios planteen en la fase de ejecución.

3.3.6.- Análisis de discriminación del versionado del software de los distintos integradores.

3.3.7.- Coordinación, supervisión y control de la ejecución de los procesos de PREPERSO, (excepto backoffice CRTM)

3.3.8.- Coordinación, supervisión y control de la ejecución de los procesos de PERSONALIZACIÓN, ya sea en diferido cómo en el acto (excepto backoffice CRTM)

3.3.9.- Coordinación, supervisión y control de la ejecución de los procesos de CARGA/RECARGA. Actualización de TLVs concretos para envío al SID (excepto backoffice CRTM)

3.3.10.- Coordinación, supervisión y control de la ejecución de los procesos de VALIDACION (zonas A, B, C y E) en todos los OPERADORES de la Comunidad de Madrid (excepto backoffice CRTM)

3.3.11.- Coordinación, supervisión y control de la ejecución de los procesos de INSPECCIÓN (excepto backoffice CRTM).

3.4 Definición de la nueva tarjeta soporte del CRTM.

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 detalle 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.

La tarea que el adjudicario tendrá que realizar consiste en la identificación y definición de comandos abiertos en relación a la comunicación a bajo nivel entre "SAM/HSM" y "tarjeta sin contactos/software dispositivo". La lista siguiente, muestra un conjunto de comandos identificados (algunos son auto-explicativos), aunque en el proceso de análisis es posible que se identifiquen más:

- SELECCION DE APLICACIÓN: Identificador del aplicativo, debe ser un mecanismo eficiente para identificar de manera inmediata la familia de claves maestras correspondientes

- SELECCION DE FAMILIA DE CLAVES: Los dispositivos SAM y HSM están evolucionando con nuevas funcionalidades, una de las más importantes es la gestión de familias de claves maestras. Siendo una familia de claves un conjunto de 7 claves maestras.

- SELECCION DE INDICE DE CLAVE: Una vez establecida la aplicación y la familia de claves, hay que fijar el índice de las claves para el posterior proceso de autentificación que se tendrá en cuenta en el proceso de 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: Es un conjunto de comandos que sirven para que ambas partes puedan acreditar que conocen la familia de claves maestras y el índice en concreto sobre el que se desea realizar la autentificación. El resultado, del intercambio de estos comandos es obtener una clave de sesión válida hasta la próxima autentificación. 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

3.5 Coordinación y supervisión en el proceso de la virtualización de la nueva tarjeta sin contactos 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 supervisar y coordinar:

3.5.1. Elemento seguro frente a HCE: ventajas e inconvenientes.

Se requiere un estudio comparativo entre las diferentes formas de virtualizar una tarjeta sin contactos en un Smartphone (que tenga NFC). Considerando los siguientes aspectos:

- Seguridad
- Rendimiento en cuanto a velocidad.
- Robustez: Frente a tener el teléfono móvil apagado, frente a tener el teléfono móvil sin la batería, frente a tener otra aplicación en primer plano, etc....
- Dependencia tecnológica
- Cobertura en terminales
- Implantación y despliegue. Facilidad para el usuario
- Modelo de negocio

3.5.2 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 autentificación. El CRTM tiene especificada al completo la lógica de la aplicación de transportes en sus distintos aplicativos y las reglas de negocio. Sin embargo, tendrá que ser adaptada por el adjudicatario, así como la coordinación y supervisión del subsistema descrito.

3.5.3. Evolución 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, coherentes con los comandos del epígrafe anterior (4.3) y que en resumen se traduce en nuevos algoritmos de diversificación, de autentificación y de cifrado; manteniendo, por supuesto, la retrocompatibilidad.

El adjudicatario tendrá que coordinar y supervisar los cambios de software de esta plataforma, comprobando que se ajustan a las especificaciones. Para ello, diseñará baterías completas de pruebas.

3.5.4. Pruebas integrales entre los subsistemas VLAT y SECU.

4. EJECUCIÓN DE LOS TRABAJOS

El adjudicatario realizará íntegramente todos los trabajos descritos en el epígrafe 3. Para ello, relazará una propuesta de planificación. Sin embargo, teniendo en cuenta el estado de implantación del sistema BIT, se detallan los hitos urgentes, cuya falta de cumplimiento originará de forma cierta un retraso en la planificación de este organismo.

HITOS URGENTES:

- Hito I: Deberá estar totalmente concluido en 20 días a contar desde la fecha de inicio de ejecución del contrato. La tarea a llevar a cabo es la siguiente:

Especificaciones para las familias de títulos. (apartado 3.2.1 de este documento)

- Hito II: Deberá estar totalmente concluido en 40 días a contar fecha de inicio de ejecución del contrato. La tarea a llevar a cabo es la siguiente:

Algoritmo de coexistencia de carga de títulos. (apartado 3.2.2 de este documento)

- Hito III: Deberá estar totalmente concluido en 60 días a contar fecha de inicio de ejecución del contrato. La tarea a llevar a cabo es la siguiente:

Algoritmo de prioridad en validación. (apartado 3.2.3 de este documento)

5 CONDICIONES GENERALES

5.1 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.

5.2 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.

CONSORCIO REGIONAL DE TRANSPORTES MADRID

5.3 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.

5.4 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.

6 PLAZO DE EJECUCIÓN DE LOS TRABAJOS

El plazo de ejecución del contrato será de 24 meses (prorrogables por 12 meses), a contar desde el 1 de diciembre de 2016 o, en caso de formalización del contrato en fecha posterior a la indicada, desde la fecha de esa formalización

7 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 (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.

HCE

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

HSM

Los Hardware Security Module (HSM) (Módulo de Seguridad Hardware) son los dispositivos garantes de la seguridad (con disponibilidad de 24x7x365). El CRTM se encarga de particularizar (preperso+perso) todos los HSM del sistema. Las

tarjetas criptográficas utilizadas actualmente son PL600 y PSI-E2:PL1500. Estas tarjetas son capaces de embeber claves y comandos de forma segura (software de bajo nivel). Los HSMs incorporan un sistema antirrobo basado en la "tamperización", esto es un proceso autodestructivo por si se intenta abrir o quitar un dispositivo HSM.

Mapa de memoria

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

NFC

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

OTA

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

SAE

Sistemas de Ayuda a la Explotación. En el ámbito del transporte público, cada operador de transportes requiere de un SAE para que el centro de control del operador de transportes pueda seguir, en tiempo real, la situación de cada autobús,

su ocupación y el ajuste con respecto al horario programado. Estos sistemas están integrados con CRTM y representan la oferta.

SAM

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

SECEBIT

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

SID

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

TLV

Son paquetes de datos (Tipo Longitud y Valor).

Las especificaciones BIT construyen los ficheros elementales incluidos en el mapa de memoria de la TTP como un conjunto de TLVs. También, por extensión, los TLVs se utilizan para nombrar los diferentes tipos de transacciones que se generan cada vez que la TTP interactua 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

Madrid, 28 de septiembre de 2016
EL DIRECTOR GERENTE,

Juan Ignacio Merino de Mesa

CONFORME,
EL ADJUDICATARIO

CONSORCIO REGIONAL DE TRANSPORTES MADRID