



GOBIERNO DEL
PRINCIPADO DE ASTURIAS



CONSORCIO TRANSPORTES ASTURIAS

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SERVICIO DE DISEÑO DE LA ESTRUCTURA DE DATOS Y SEGURIDAD DE LA NUEVA TARJETA DEL CTA Y DEL SUMINISTRO DE MÓDULOS SAM Y LAS HERRAMIENTAS NECESARIAS PARA LA GESTIÓN DE TODOS LOS COMPONENTES.

CO-9/2017





1. ANTECEDENTES

El Consorcio de Transportes de Asturias (CTA) es un ente público destinado a la promoción y desarrollo del transporte público en un contexto de movilidad sostenible.

CTA comercializa unos títulos de viaje englobados genéricamente bajo la denominación de Billete Único, que dan acceso a todos los autobuses interurbanos regionales, y a los sistemas ferroviarios de RENFE y FEVE en Asturias. Estos títulos se articulan mediante una tarjeta inteligente Mifare Classic 1K.

CTA ha decidido renovar su sistema tarifario y todo el sistema tecnológico que lo soporta mejorando aspectos claves en la seguridad y calidad de sus servicios. Una de las decisiones tomadas es modernizar el soporte de la tarjeta optando por la tecnología Mifare ® Desfire EV2 8K, considerada actualmente como una de las más avanzadas en aspectos de prestaciones y seguridad.

La nueva tarjeta deberá estar configurada de modo que permita cubrir las necesidades del modelo tarifario que se determine. Además y para garantizar la seguridad en su acceso desde todas las infraestructuras que permitan su tratamiento, se considera necesario el uso de módulos SAM que aseguren la confidencialidad de las transacciones entre los equipos implicados y las tarjetas.

2. OBJETO DEL CONTRATO

El objeto del contrato consistirá en la elaboración del diseño de las estructuras de datos de la nueva tarjeta del CTA, la definición de la seguridad y procedimientos relacionados, el suministro estimado de 2.000 módulos SAM para la gestión de la seguridad en las transacciones y las herramientas necesarias para la gestión de todos los componentes.

3. LUGAR DE ENTREGA DEL CONTRATO

El lugar de entrega será en las oficinas del CTA en la Avda. Julián Clavería, 11, 33006 Oviedo, Asturias, España.

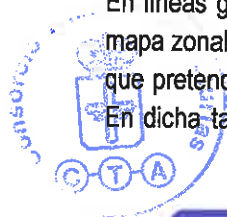
4. CONTENIDO DEL CONTRATO.

El contenido del contrato se compone de los trabajos y suministros que se relacionan a continuación. Como principio general el adjudicatario ejecutará los trabajos intentando maximizar el uso de las características funcionales de los elementos tecnológicos empleados en este contrato y si en algún caso existe incompatibilidad con las versiones actuales que no permita aprovecharlas, deberá en todo caso prever el posible uso futuro de las mismas.

4.1. Análisis de requisitos y funcional para la implantación de la nueva tarjeta del CTA.

El adjudicatario se encargará de definir requisitos y elaborar un documento de análisis funcional en base a las necesidades que el CTA especifique para los modelos de sistemas tarifarios que se desean aplicar en la nueva tarjeta.

En líneas generales se pone en conocimiento del licitante que, el CTA, dispone de un sistema zonal (ver mapa zonal en www.consortioasturias.com) con modalidades de viajes que pueden ir de una a ocho zonas y que pretende implantar una nueva tarjeta en soporte sin contacto con tecnología Mifare ® Desfire EV2 8K. En dicha tarjeta, se desea poder configurar al menos 5 tipos de títulos que podrán ser personalizados o





anónimos y cuya funcionalidad se determinará en esta fase de análisis. También se debe contemplar el uso delegado de la tarjeta a otras entidades para que puedan instalar sus propias aplicaciones bajo la supervisión del CTA, no siendo estos usos delegados objeto de este contrato.

Además, se debe tener en cuenta que la nueva tarjeta del CTA deberá cumplir con la definición de la especificación del Código Seguro Para Interoperabilidad en el Transporte – TESC (Tarjeta Española Sin Contacto) del Ministerio de Fomento por lo que se deberán contemplar las tareas necesarias para añadir este tipo de título.

El detalle completo del funcionamiento deberá concretarse durante esta fase de análisis.

4.2. Estructura de datos y diseño funcional de la tarjeta.

El adjudicatario se encargará de realizar el diseño de la nueva tarjeta Mifare ® Desfire EV2 8K en base al documento de análisis funcional elaborado previamente. Para ello el contratista deberá elaborar los documentos técnicos que se consideren necesarios detallando las estructuras de datos completas de la tarjeta y el diseño funcional que se derive del análisis anterior.

4.3. Diseño de la seguridad de la tarjeta y de módulos SAM.

Con objeto de garantizar la seguridad en la gestión de las claves de las tarjetas y dispositivos utilizados como soporte de los títulos de transporte, y teniendo en cuenta que las transacciones a realizar tienen un valor económico que puede incitar a acciones fraudulentas, todos los equipos que gestionen tarjetas deberán contar con un módulo SAM (Security Access Module) que contendrá las claves necesarias para efectuar dicha gestión.

El adjudicatario se encargará de realizar el diseño de la seguridad de la tarjeta teniendo en cuenta el uso conjunto con módulos SAM. Definirá las estrategias que se deben aplicar tanto en la tarjeta como en los módulos SAM de modo que se maximice la seguridad en las transacciones que se puedan realizar con la tarjeta en todos los escenarios de su ciclo de vida. Se deberá prever, a modo de ejemplo, el uso de listas negras de SAM para poder bloquear las tarjetas recargadas con módulos de la lista.

Se deberán elaborar los documentos técnicos necesarios detallando el diseño de la seguridad y toda la información necesaria para configurar tanto la tarjeta como el módulo SAM (mapa de SAM) en base al diseño establecido.

Se debe tener en cuenta que los módulos SAM a instalar en todos los equipos que gestionen tarjetas sin contacto del CTA serán del tipo Mifare ® SAM NXP AV2 y que también son objeto del suministro de este contrato.

4.4. Definición de los procedimientos de uso de la tarjeta y protocolos de prueba.

Definición de las operativas del ciclo de vida de la tarjeta. El contratista, basándose en el análisis, diseño funcional y diseño de seguridad de la tarjeta elaborará toda la documentación necesaria para especificar en detalle los procedimientos necesarios así como sus correspondientes protocolos de prueba para las siguientes operaciones sobre la tarjeta con el uso conjunto del módulo SAM:

- Fabricación de la tarjeta.

- Emisión inicial.



- Personalización.
- Validación.
- Venta/Carga/Recarga.
- Recuperación.
- Inspección/Consulta.
- Aplicación de operaciones de Lista (blanca, negra, gris)

Se debe tener en cuenta que estos documentos podrán tener como destino la entrega a los diferentes proveedores, operadores e implantadores que se vayan a encargar de aplicar cada operativa por lo que deberán presentar un nivel de detalle técnico suficiente para poder realizar todas las tareas necesarias. Además y por razones de seguridad y confidencialidad, cada documento deberá restringir la información imprescindible para su aplicación al uso previsto.

4.5. Definición de datos en el Sistema de Información.

El adjudicatario deberá elaborar un documento donde se definan los datos de parametrización, configuración, etc. que se estime necesario almacenar en el Sistema de Información del CTA para garantizar la correcta operativa de las tarjetas según los diseños y procedimientos establecidos.

4.6. Suministros de módulos SAM.

El adjudicatario deberá suministrar una cantidad estimada de 2.000 unidades de módulos Mifare ® SAM NXP AV2.

Los módulos se entregarán en formato tarjeta SIM (ID-000) troquelado y embebido en tarjeta de plástico tamaño ID-1.

Los módulos vendrán rotulados con un número de serie que puede coincidir el número de chip (UID) o bien un número asignado a cada tarjeta comenzando por el 0001. En este último caso, el adjudicatario, proporcionará una relación entre el número de serie y el número de chip.

El CTA será el encargado de la emisión/grabación del mapa de los módulos SAM.

4.7. Suministro de herramientas software para la gestión de tarjetas y SAM.

Para que el CTA disponga del máximo control e independencia sobre la seguridad, el adjudicatario deberá suministrar el software que permita tanto gestionar las nuevas tarjetas como los módulos SAM.

4.7.1. Aplicación de gestión de tarjetas.

Se deberá suministrar una aplicación de escritorio con las siguientes funcionalidades mínimas:

- Cuentas de usuario con seguridad por contraseña encriptada AES-256.
- Perfiles de usuario permitiendo diferentes privilegios de acceso a las operaciones definidas.
- Lectura y grabación de la estructura de la tarjeta del CTA según los diseños de mapa realizados.
- Permitir la definición personalizada de diferentes operaciones de lectura/grabación sobre la tarjeta.
- Opción para la grabación masiva de la operación seleccionada sobre equipo dispensador de tarjetas.
- Uso de módulo SAM obligatorio para todas las operaciones.
- Auditoría de operaciones realizadas.



Requisitos técnicos:

- Windows 7 32/64 bits o superior.
- Desarrollo en .NET
- Almacenamiento de los datos en el SGBD Oracle 12c del CTA.

Se desarrollará para equipo de lectura/grabación de las características que se detallan en el Anexo 1.

4.7.2. Aplicación para la configuración de los módulos SAM.

Deberá suministrarse una aplicación de escritorio que permita realizar las siguientes funciones mínimas sobre los módulos SAM:

- Cuentas de usuario con seguridad por contraseña encriptada AES-256.
- Configuración del SAM de acuerdo al diseño de seguridad previsto en la tarjeta sin contacto.
- Configuración de los perfiles previstos actuales y futuros del SAM para diferentes equipamientos.
- Dar soporte al proceso de generación de claves.
- Almacenamiento de la información de manera segura.
- Grabación y configuración SAM para los diferentes equipamientos extrayendo dicha información del lugar seguro donde está almacenada la configuración y las claves.
- Registro y control de los SAM generados.
- Importación de listados de SAM suministrados por el fabricante.

Requisitos técnicos:

- Windows 7 32/64 bits o superior.
- Desarrollo en .NET
- Almacenamiento de los datos en el SGBD Oracle 12c del CTA.

Se desarrollará para equipos de lectura/grabación de módulos SAM de las características que se detallan en el Anexo 2.

5. PLAN DE FORMACIÓN.

El adjudicatario está obligado a realizar la formación adecuada sobre la tecnología y los suministros realizados al personal del CTA que se designe.

La formación se impartirá como mínimo sobre las siguientes materias:

- Tecnología Mifare Desfire EV2.
- Módulos SAM. Tecnología.
- Diseño de la Tarjeta CTA, modelo de seguridad y procedimientos.
- Formación sobre los módulos SAM suministrados.
- Formación sobre las herramientas software suministradas.

El número mínimo de horas de formación será de 20 horas repartidas en un máximo de 4 horas diarias. El curso se impartirá en castellano, en las dependencias del cliente y al personal designado por el CTA.

Dicha formación deberá estar soportada por documentación que será entregada a CTA.

El adjudicatario entregará a los asistentes un certificado acreditativo de la formación impartida.





6. DOCUMENTACIÓN A ENTREGAR POR EL CTA.

El CTA trasladará al adjudicatario toda la documentación que se considere necesaria para la implementación de las funciones requeridas.

7. PRODUCTOS A ENTREGAR POR EL CONTRATISTA.

El adjudicatario entregará todos los documentos técnicos que se deben elaborar como exigencias de las sucesivas fases de la ejecución del contrato, siendo estos, al menos, los siguientes:

- Programa de trabajo, a presentar durante la primera semana del contrato.
- Análisis Funcional.
- Estructuras de datos de la tarjeta y Diseño Funcional.
- Definición y Gestión de seguridad (Tarjeta y SAM).
- Estudio claves, esquema de seguridad y tiempos de operación.
- Mapa del módulo SAM.
- Gestión general de flujos y procesos de la tarjeta.
- Procedimientos de uso y protocolos de prueba de la tarjeta.
- Definición de datos en el Sistema de Información del CTA.

El adjudicatario del concurso se compromete a entregar al CTA los programas fuente de todas las aplicaciones desarrolladas y de las sucesivas actualizaciones que durante el periodo de garantía realice y notificar al CTA todas las herramientas de desarrollo necesarias, que deberán ser accesibles y adquiribles en el mercado.

El software desarrollado se deberá suministrar al menos con la siguiente documentación:

- Manual de usuario, donde esté recogido el funcionamiento de cada uno de los módulos que integran los sistemas a desarrollar.
- Manual de instalación, donde se especificará el procedimiento de instalación así como los requisitos mínimos necesario.
- Modelos de datos, así como la descripción detallada de cada objeto.

Oviedo, 24 de noviembre de 2017.

LA DIRECTORA TÉCNICA,

Fdo. María Radisbunda López García



GOBIERNO DEL
PRINCIPADO DE ASTURIAS

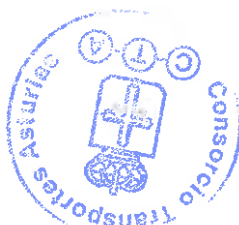


CONSORCIO TRANSPORTES ASTURIAS

ANEXO 1

Equipo de lectura y grabación de tarjetas TSC

- ISO14443 type A / B / C (TCL) and ISO18092 (NFC) Frecuencia de trabajo 13.56Mhz.
- 1 Zócalo para módulo SAM ID-000. ISO7816-3 T = 0 y T = 1
- Compatibilidad con Ultralight C (permitiendo la autenticación 3DES), Mifare Classic, EV1 y DESFire EV1 / EV2.
- Compatible mínimo Windows 7 32/64 bits o superior.



ANEXO 2

Equipos de lectura y grabación de módulos SAM

- Estándares: ISO/IEC 7816. Protocolo PPS y PTS T=0 y T=1.
- Tamaño de la tarjeta ID-1 (tamaño completo)
- Velocidad de interfaz de la tarjeta inteligente: 420 Kbps (cuando lo admita la tarjeta)
- Frecuencia del reloj de la tarjeta inteligente: Hasta 8 MHz.
- Tipos de tarjeta admitidos: Tarjetas inteligentes de 5 V, 3 V y 1.8 V, ISO 7816 Clase A, B y C.
- Detección automática de tipo de tarjeta inteligente.
- Compatible mínimo Windows 7 32/64 bits o superior

