

DESARROLLO E IMPLANTACIÓN DE SOFTWARE PARA VALIDACIÓN DE MUGI 2.0 EN SISTEMAS INDRA

PLIEGO DE PRESCRIPCIONES TÉCNICAS



ÍNDICE

1. OBJETO.....	1
2. RELACIONES ENTRE ETS Y EL CONTRATISTA. DEFINICIONES	1
3. ANTECEDENTES	2
4. DESARROLLO DE LOS TRABAJOS	3
4.1. INVENTARIO DEL EQUIPAMIENTO	3
4.2. ALCANCE DE LOS TRABAJOS	3
5. REQUERIMIENTOS DESARROLLO DE SOFTWARE	5
6. PLAZO DE EJECUCIÓN DE LOS TRABAJOS	9
7. JUSTIFICACIÓN DEL PRESUPUESTO	9

1. OBJETO

La presente especificación trata de establecer las bases para contratar los trabajos de desarrollo e implantación de software para la validación de MUGI Virtual con cuenta ABT y token identificador asociado (MUGI1.5) en equipos con Hardware MUGI 2.0, en los pasos de fabricación INDRA instalados en las estaciones de ETS.

Los trabajos de actualización tecnológica de los pasos automáticos y canceladoras existentes incluyen la integración DLL MUGI 1.5 para capturar el identificador de viaje Mugi Virtual, token (MUGI 1.5) a través del lector TSC, la integración de la librería ABT 2.0 a la que se enviará el token leído de la tarjeta o el QR para su procesamiento, la visualización del resultado al usuario y el envío de la transacción Mugi Virtual.

Una vez realizados los desarrollos de software se llevarán a cabo las pruebas e implantación y puesta en marcha en los equipos en servicio en las estaciones de ETS.

2. RELACIONES ENTRE ETS Y EL CONTRATISTA. DEFINICIONES

A los efectos de fijar las relaciones contractuales se definen las siguientes figuras jurídicas:

- PROPIEDAD - Euskal Trenbide Sarea, Ente Público del Gobierno Vasco
- RESPONSABLE DEL CONTRATO - Euskal Trenbide Sarea designará una persona Responsable del Contrato, bajo la supervisión de la Directora de Instalaciones y Mantenimiento de ETS. El Responsable del Contrato podrá rodearse del equipo técnico necesario que le asesorará y en su caso podrá actuar por delegación del mismo
- CONTRATISTA - Licitador Adjudicatario, persona natural o jurídica que adquirirá esa condición a la firma del Contrato

- DELEGADO DEL CONTRATISTA - Técnico designado por el Contratista para hacerse cargo de la coordinación técnica de los trabajos y representar a éste frente a ETS. Todo el equipo del Contratista dependerá del Delegado quien informará directamente y cuantas veces sea requerido al Responsable del Contrato.

3. ANTECEDENTES

Con fecha 20 de febrero de 2023 se publica Orden del Consejero de Planificación Territorial, Vivienda y Transportes, por la que se otorga una subvención nominativa por un importe máximo de UN MILLÓN DE EUROS (1.000.000,00 €) al ente público Red Ferroviaria Vasca - Euskal Trenbide sarea, destinada a la digitalización de los sistemas de cancelación en las estaciones ferroviarias adscritas a dicho ente público, en el marco del plan de recuperación, transformación y resiliencia – financiado por la Unión Europea – Next Generation EU.

Dentro de esta modernización y digitalización de los sistemas de cancelación se han contemplado los trabajos de desarrollo e implantación de software para la validación de MUGI Virtual con cuenta ABT y token identificador asociado (MUGI1.5) en equipos con Hardware MUGI 2.0 de tecnología INDRA instalados en las estaciones de ETS.

4. DESARROLLO DE LOS TRABAJOS

A continuación, se describen los trabajos a realizar para llevar a cabo las mejoras en los sistemas de cancelación de tecnología INDRA de ETS.

Las actuaciones para el desarrollo e implantación de software afectan a todos los pasos flap y canceladoras INDRA instalados en las estaciones de ETS.

4.1. INVENTARIO DEL EQUIPAMIENTO

Las actuaciones previstas afectan a estas series de equipos en operación actualmente en ETS:

- 22 unidades de Flap (Modelo 99/02).
- 37 unidades de Flap (Modelo 2004).
- 96 unidades de Flap (Modelo 2007)
- 102 unidades de Flap (Modelo L3).
- 40 unidades de Canceladoras (Modelo Mixta)
- 24 unidades de Canceladoras (Modelo Tótem)

4.2. ALCANCE DE LOS TRABAJOS

Se incluyen en las actuaciones a realizar los trabajos de diseño y desarrollos software necesarios, implantación y la puesta en marcha de la solución.

Los trabajos de actualización tecnológica de los pasos automáticos y canceladoras existentes incluyen las siguientes tareas:

4.2.1. Integración DLL MUGI 1.5

En la aplicación de validación de los controles de acceso se integrará la DLL MUGI 1.5 que comprobará la firma digital del token grabado en la tarjeta y leerá los datos para su validación.

Los métodos a utilizar son los siguientes:

- Interfaz de inicialización: se le indica el tipo de hardware y callbacks a las funciones de las tarjetas.
- Callback para lectura de bloque: la DLL indicará mediante callback los bloques a leer de la tarjeta y guardará su contenido.
- Callback para escritura de bloque: la DLL indicará mediante callback cuando se requiera la escritura de un bloque de la tarjeta.
- Interfaz de identificación MUGI 1.5: se le pasará el uid de la tarjeta y devolverá si la tarjeta es Mugi 1.0 o 1.5.
- Interfaz para lectura del token: tras detectarse una tarjeta como Mugi 1.5, se utilizará este método para leer el token y devolverá el resultado de la lectura.
- Interfaz de versión de DLL: se utilizará para devolver la versión de la DLL y tener un control de la versión con la que se está trabajando.

4.2.2. Integración librería ABT 2.0

La librería ABT 2.0 se integrará en la aplicación de validación de los controles de acceso para comprobar la validez del token leído con la librería 1.5 y poder informar y permitir el paso del viajero.

Los métodos a utilizar son los siguientes:

- Inicialización: Se le pasará un identificador con las características del equipo, el contexto de la validación para trenes, la contraseña de autenticación y el path con la localización de los archivos utilizados por la librería.
- Resultado de validación MUGI 1.5: se le pasará el uid de la tarjeta, el token y el momento de la validación para obtener un resultado.
- Resultado de validación QR: se le pasará el payload del QR y el momento de la validación para obtener un resultado.
- Commit validation: si el resultado de la validación anterior es correcto y el usuario cruza el tornillo en el caso de los controles de peaje de puertas,



se utilizará este método para confirmar a la librería y que envíe los registros al ATTG.

- Reject validation: si el usuario no cruza en un control de acceso de peaje se utilizará este método para que la librería rechace la validación.
- Versión ABT 2.0: devolverá la versión de la librería con la que se está trabajando para poder mantener un control adecuado.

4.2.3. Visualización del resultado de la validación al usuario

Tras obtener el resultado de la validación de la librería ABT 2.0, ya sea una validación correcta o incorrecta se mostrarán los mensajes correspondientes en las pantallas del equipo tanto para validaciones de MUGI virtual en soporte TSC como QR.

4.2.4. Envío de la transacción Mugí Virtual

Después de obtener el resultado de la validación de la librería ABT 2.0 y conociendo si el usuario ha cruzado el paso en los equipos de control de acceso de puertas, se enviará la transacción al back office para recoger todos los movimientos de la MUGI virtual tanto en soporte TSC como QR.

5. REQUERIMIENTOS DESARROLLO DE SOFTWARE

El desarrollador deberá cumplir durante el desarrollo con los siguientes apartados de la Política de Seguridad de ETS:

- El desarrollador deberá utilizar entornos segregados para el desarrollo y producción, siendo recomendable la existencia de un entorno adicional de prueba.
- El desarrollador deberá llevar a cabo pasos de código y ejecutables entre los diferentes entornos segregados de forma controlada y únicamente con autorización explícita del responsable del contrato.

- El desarrollador deberá utilizar un sistema formal de control de cambios.
- El desarrollador deberá evitar el uso de librerías y código fuente con vulnerabilidades conocidas. En el caso en el que esto no sea posible el desarrollador deberá diseñar e implementar controles compensatorios que deberán ser aprobados explícitamente por ETS. Estos controles y las vulnerabilidades compensadas deben ser documentadas por el desarrollador.
- Las pruebas de aceptación del sistema incluirán una búsqueda de vulnerabilidades en el sistema que será llevada a cabo por el desarrollador. Dicha búsqueda deberá cubrir tanto vulnerabilidades de código como de configuración. Las vulnerabilidades descubiertas deberán ser parcheadas por el desarrollador o deberá diseñar, implementar y documentar controles compensatorios que tendrán que ser aprobados por ETS. El desarrollador deberá entregar un informe con los resultados de la búsqueda de vulnerabilidades.
- ETS se reserva el derecho de llevar a cabo por su cuenta una búsqueda de vulnerabilidades adicional. En el caso en que ETS encuentre vulnerabilidades adicionales procederá a comunicarlas al desarrollador, quien deberá tratarlas del mismo modo que si las hubiese descubierto en su propia búsqueda.
- En el caso en el que se deban utilizar controles criptográficos estos deberán cumplir con lo indicado en la última versión publicada del documento "SOGIS Agreed Cryptographic Mechanisms" disponible en <https://www.sogis.eu/>
- Se deberá llevar a cabo una clasificación conjunta entre ETS y el desarrollador del sistema a desarrollar siguiendo la legislación vigente, por ejemplo, el Esquema Nacional de Seguridad o la GDPR. El diseño de la aplicación deberá incluir las medidas de seguridad requeridas por la legislación aplicable.
- El desarrollador identificar los requisitos de seguridad a través del análisis de riesgos de la aplicación. Los requisitos de seguridad se añadirán al resto de los requisitos de la aplicación.

- El diseño de seguridad llevado a cabo por el desarrollador deberá enfocarse en la reducción de la superficie de ataque, el principio de least privilege y la defensa en profundidad.
- En el caso en el que la aplicación a desarrollar incluya diferentes niveles de privilegio entre sus usuarios, la aplicación deberá permitir gestionarlos siguiendo un modelo Role Based Access Control (RBAC), y como mínimo permitir segregar usuarios de administradores
- Como parte de los entregables del proyecto el desarrollador deberá entregar una memoria que refleje:
 - o Análisis del sistema a desarrollar y el catálogo de requisitos
 - o Diseño del sistema incluyendo los controles de seguridad incluidos en el diseño
 - o Construcción del sistema, incluyendo el plan de pruebas para validarlo y la interrelación entre requisitos y pruebas. Deberá quedar claramente reflejado como las pruebas evalúan el cumplimiento de los requisitos de seguridad.
- El diseño de la aplicación deberá verificar el correcto dimensionamiento de la aplicación para el uso que se plantea, y deberá tener en cuenta que exista la posibilidad de ampliar las capacidades de la misma.
- El desarrollador deberá aplicar las recomendaciones de guías de desarrollo seguras relevantes para los lenguajes de programación utilizados e indicárselos a ETS.

Se recomienda al desarrollador hacer uso de herramientas de análisis de código estático para asegurar que está cumpliendo con lo indicado por la(s) guía(s) de desarrollo seguro.

- El desarrollador no deberá utilizar funciones marcadas como deprecadas o inseguras. En el caso en el que no fuese posible evitar su uso, ETS deberá autorizar explícitamente el uso de las mismas.
- El desarrollador deberá hacer uso de una metodología de desarrollo formal y comunicar la misma a ETS. ETS utiliza preferentemente la metodología Métrica3
- Se considerará el código fuente utilizado en la aplicación como un dato a ser protegido que recibirá el tratamiento de información confidencial.

El desarrollador deberá tomar las medidas oportunas para evitar su divulgación y restringir su acceso al personal autorizado.

- El desarrollador deberá restringir el acceso a los diferentes entornos a fin de que únicamente el personal autorizado pueda acceder a los mismos.
- En los casos en que el código fuente vaya a ser propiedad de ETS, el desarrollador deberá documentar el desarrollo y deberá entregar dicha documentación a ETS como parte del proyecto. Debería indicar como realizar la compilación del código, y un manual de instalación de los binarios para cada entorno.
- En los casos en que el código fuente no vaya a ser propiedad de ETS, se requiere que el desarrollador entregue la documentación para permitir la instalación en cualquier entorno del entorno. Indicando la configuración. despliegue resultante de aplicar los pasos indicados en la documentación deberá representar una configuración segura de la aplicación. Esta documentación será considerada como un dato a ser protegido que recibirá el tratamiento de información confidencial. El desarrollador deberá tomar las medidas oportunas para evitar su divulgación.
- En todos los proyectos, el desarrollador deberá documentar los pasos necesarios para llevar a cabo las tareas habituales de la aplicación, o si es preciso actualizar la documentación ya existente.
- El desarrollador deberá, en colaboración con el personal de ETS, diseñar un plan de despliegue de la aplicación y los pasos necesarios para revertir el despliegue en caso necesario. Este plan deberá tener en cuenta las necesidades de confidencialidad, disponibilidad e integridad de los activos tecnológicos de ETS involucrados. ETS informará al desarrollador de las necesidades concretas de los activos involucrados.

6. PLAZO DE EJECUCIÓN DE LOS TRABAJOS

El plazo máximo para la realización de los trabajos es el incluido en el apartado 6 de la carátula.

7. JUSTIFICACIÓN DEL PRESUPUESTO

El presupuesto máximo de licitación es el indicado en el apartado 3 de la carátula.

Serán por cuenta del Adjudicatario los gastos de todo tipo que se originen en relación con los trabajos objeto de esta oferta, incluida la documentación de la instalación, formación e integración de los sistemas de gestión y explotación.

Estos precios serán de contrata, de modo que en ellos estén incluidos todos los beneficios, cargas sociales, gastos, impuestos, etc.