



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

PLIEGO DE PRESCRIPCIONES TÉCNICAS

PARA LA CONTRATACIÓN DEL

**SERVICIO DE MANTENIMIENTO DE DRIVERS
Y HERRAMIENTAS PARA TARJETAS INTELIGENTES**



Índice

1	OBJETO	3
2	DESCRIPCIÓN	3
3	PROYECTOS INCLUIDOS EN EL MANTENIMIENTO.....	3
3.1	PROYECTO CSP PARA CNP	3
3.1.1	PROYECTO CSP DNie	3
3.1.2	PROYECTO CSP TIF.....	4
3.2	PROYECTO CSP PARA FNMT-RCM	5
3.2.1	PROYECTO CSP TC-FNMT/CERES.....	5
3.3	PROYECTO MULTIPKCS11.....	6
3.4	PROYECTO HERRAMIENTAS PROPIETARIAS PARA TARJETAS TC-FNMT/CERES - USUARIO FINAL	7
3.4.1	APLICACIÓN DE CAMBIO DE PIN	8
3.4.2	APLICACIÓN DE DESBLOQUEO DE TARJETA	8
3.4.3	APLICACIÓN PARA LA IMPORTACIÓN DE CERTIFICADOS	8
3.4.4	APLICACIÓN PARA LA GESTIÓN DE CERTIFICADOS	8
3.4.5	APLICACIÓN PARA ORDENAR LOS CERTIFICADOS.....	8
3.5	PROYECTO HERRAMIENTAS PROPIETARIAS PARA TARJETAS TC-FNMT/CERES - SOPORTE TÉCNICO	8
3.5.1	APLICACIÓN PARA ACTUALIZACIÓN DE CLAVES.....	9
3.5.2	APLICACIÓN PARA ACTUALIZACIÓN DE CERTIFICADOS	9
3.5.3	APLICACIÓN PARA FORMATEAR TARJETA.....	9
3.5.4	APLICACIÓN INFORME DE INSTALACIÓN Y TARJETA INTELIGENTE (SC_Report) ..	9
4	ALCANCE DEL SERVICIO	10
5	ENTREGA	10
6	GARANTÍAS.....	11
7	REQUISITOS DE LA EMPRESA ADJUDICATARIA DEL SERVICIO	11
7.1	REQUISITOS MÍNIMOS	11
7.2	ASPECTOS VALORABLES	11
8	OTRAS CUESTIONES.....	12

1 OBJETO

Este pliego tiene por objeto fijar las prescripciones técnicas para la solicitud de ofertas para la prestación del servicio de mantenimiento de drivers de usuario CSP y PKCS#11 para tarjetas DNIE/TIF/CERES/TC-FNMT y herramientas propietarias para tarjetas CERES/TC-FNMT por el periodo de un año.

A continuación se detalla en qué consiste el servicio:

2 DESCRIPCIÓN

El mantenimiento engloba principalmente resolución de incidencias y cambios funcionales. Además, se mantendrá la compatibilidad entre las diferentes plataformas y arquitecturas, haciendo que la gestión de los objetos de la tarjeta sea compatible entre CSP, CardModule, PKCS11 y multiPKCS11 propietarios de la FNMT.

3 PROYECTOS INCLUIDOS EN EL MANTENIMIENTO

Se incluyen definiciones de algunos términos para ayudar a una mejor comprensión del documento.

Sistema Operativo: Programa o conjunto de programas que efectúan la gestión de los procesos básicos de un sistema informático, y permite la normal ejecución del resto de las operaciones. Ejemplo: Microsoft Windows, GNU/Linux, Mac OS, etc.

Distribución: Variante de un sistema operativo que incorporan determinados paquetes para satisfacer las necesidades de un grupo específico de usuarios. Ejemplos: Ubuntu, Debian, SUSE, etc.

Versión: Número o nombre que indica el nivel de desarrollo de un sistema operativo. Ejemplo: Microsoft Windows 10, Ubuntu Xelial Xerus, Mac OS X Sierra, etc.

Arquitectura: La implementación del diseño de los diferentes componentes de la CPU. Ejemplo: Intel 32 y 64 bits

3.1 PROYECTO CSP PARA CNP

3.1.1 PROYECTO CSP DNIE

Este proyecto engloba un par de librerías de usuario para su implementación, además de una serie de utilidades para su correcta instalación y configuración:

- DNIECSP.dll

- DNleCertStore.dll

Este proyecto consta del mantenimiento de los drivers de la tarjeta DNle, que se trata de una tarjeta criptográfica de solo lectura que contiene dos certificados de usuario:

- Certificado de firma.
- Certificado de autenticación.

Debe tenerse en cuenta la convivencia con la librería PKCS11 específica de la tarjeta DNle y con otros drivers CSP/Cardmodule que pueda estar instalada en el mismo equipo.

Se garantizará su correcto funcionamiento en los siguientes ss.oo. sobre arquitectura 32 y 64 bits y en su último Service Pack:

- Windows Vista
- Windows Server 2003
- Windows Server 2008

Además, se garantizará su funcionamiento en las siguientes aplicaciones:

- Internet Explorer
- MS Office
- Logon en Windows
- Acrobat

3.1.2 PROYECTO CSP TIF

Este proyecto engloba un par de librerías de usuario para su implementación, además de una serie de utilidades para su correcta instalación y configuración:

- TIFeCSP.dll
- TIFCertStore.dll

Este proyecto consta del mantenimiento de los drivers de la tarjeta TIF, que se trata de una tarjeta criptográfica de solo lectura que contiene 3/4 certificados de usuario:

- Certificado de firma.
- Certificado de autenticación.
- Certificado de cifrado.
- Certificado de firma con pseudónimo.

Debe tenerse en cuenta la convivencia con la librería PKCS11 específica de la tarjeta TIF y con otros drivers CSP/Cardmodule que pueda estar instalada en el mismo equipo.

Se garantizará su correcto funcionamiento en los siguientes ss.oo. sobre arquitectura 32 y 64 bits y en su último Service Pack:

- Windows XP (aunque es un sistema obsoleto se mantiene por necesidad del cliente)
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008

Además, se garantizará su funcionamiento en las siguientes aplicaciones:

- Internet Explorer
- MS Office
- Logon en Windows
- Acrobat

3.2 PROYECTO CSP PARA FNMT-RCM

3.2.1 PROYECTO CSP TC-FNMT/CERES

Este proyecto engloba un par de librerías de usuario para su implementación, además de una serie de utilidades para su correcta instalación y configuración:

- CeresCSP.dll
- CeresCertStore.dll

Este proyecto consta del mantenimiento de los drivers de las tarjetas TC-FNMT y CERES, que son tarjetas criptográficas de lectura/escritura que pueden realizar las siguientes operaciones:

- Importación de certificados: usando Internet Explorer y la aplicación “Importador de Certificados”
- Generación de claves/certificados.
- Borrado de claves/certificados a través de la aplicación “Gestión de Certificados”.
- Firma

La principal diferencia entre la tarjeta CERES y la TC-FNMT, es que esta última usa canal de seguro según norma CWA 14890.

Debe tenerse en cuenta la convivencia con la librería PKCS11 específica de la tarjeta TCFNMT/CERES y con otros drivers CSP/Cardmodule que pueda estar instalada en el mismo equipo.

También se debe tener en cuenta el pack de herramientas desarrolladas para la gestión de las tarjetas por parte del “usuario final” y por parte de “soporte técnico”. Estas aplicaciones se detallan en los apartados PROYECTO HERRAMIENTAS PROPIETARIAS PARA TARJETAS TC-FNMT/CERES - USUARIO FINAL y PROYECTO HERRAMIENTAS PROPIETARIAS PARA TARJETAS TC-FNMT/CERES - SOPORTE TÉCNICO

Se garantizará su correcto funcionamiento en los siguientes SS.OO. sobre arquitectura 32 y 64 bits y en su último Service Pack:

- Windows XP (aunque es un sistema obsoleto se mantiene por necesidades de algunos clientes)
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008

Además, se garantizará su funcionamiento en las siguientes aplicaciones:

- Internet Explorer
- MS Office
- Logon en Windows
- Acrobat

3.3 PROYECTO MULTIPKCS11

Se trata de un desarrollo específico de la FNMT de un módulo PKCS#11 único para todas las tarjetas existentes (tarjeta TC-FNMT, CERES, DNle y TIF).

Este desarrollo está diseñado para operar con diferentes tarjetas dependiendo de opciones de compilación establecidas.

Las labores de mantenimiento consisten en adaptar este desarrollo a diferentes sistemas basados en Unix (GNU/Linux, Mac OS X y Solaris) sobre arquitectura de 32 y 64 bits:

- GNU/Linux Ubuntu Desktop (Versión LTS y actual)
- GNU/Linux Debian (Versión actual)
- GNU/Linux Fedora (Versión actual)
- GNU/Linux OpenSUSE (Versión actual)
- Mac OS X (Versión actual y versión anterior)
- Solaris Intel/Sparc (Versión actual)

Y en garantizar su uso en las siguientes aplicaciones:

- Firefox
- Thunderbird

3.4 PROYECTO HERRAMIENTAS PROPIETARIAS PARA TARJETAS TC-FNMT/CERES - USUARIO FINAL

Se trata de un conjunto de herramientas destinadas a facilitar el uso de la tarjeta TC-FNMT/CERES al “usuario final”.

La lista de herramientas es:

- Cambio de código PIN.
- Desbloqueo de tarjeta mediante código PUK.
- Importar certificados.
- Gestión de certificados.
- Ordena certificados

El desarrollo es multiplataforma para garantizar su correcto funcionamiento en sistemas Windows, GNU/Linux y MacOS.

El propósito del desarrollo es generar una única implementación (por aplicación), y por lo tanto un único código fuente que se pueda desplegar y ejecutar en cada uno de los ss.oo. descritos arriba. De esta forma se obtienen ventajas significativas tanto a nivel de gestión (mantenimiento, documentación, etc), como de usabilidad para los usuarios que verán una interfaz homogénea y un desarrollo paralelo en las distintas plataformas.

Está desarrollado en Java y se generarán paquetes java (De esta forma cualquier equipo que cuente con la máquina virtual de java podrá lanzar la aplicación) y también los ficheros ejecutables.

Las aplicaciones son multilinguaje:

- Español

- Inglés
- Catalán
- Vasco

3.4.1 APLICACIÓN DE CAMBIO DE PIN

Esta aplicación permitirá al usuario cambiar el código PIN de su tarjeta TC-FNMT/CERES.

3.4.2 APLICACIÓN DE DESBLOQUEO DE TARJETA

Aplicación para desbloquear una tarjeta TC-FNMT/CERES que haya quedado bloqueada, para tal efecto se hará uso del código PUK de desbloqueo.

3.4.3 APLICACIÓN PARA LA IMPORTACIÓN DE CERTIFICADOS

Esta aplicación permite utilizar los certificados previamente almacenados en el ordenador (.pfx/.p12), para importarlos en la tarjeta criptográfica TC-FNMT/CERES.

3.4.4 APLICACIÓN PARA LA GESTIÓN DE CERTIFICADOS

Esta aplicación permite la gestión de los certificados de la tarjeta TC-FNMT/CERES. Muestra la lista de certificados almacenados y da la posibilidad de borrarlos.

3.4.5 APLICACIÓN PARA ORDENAR LOS CERTIFICADOS

Esta aplicación permite marcar por defecto uno de los certificados almacenados en la tarjeta TC-FNMT/CERES. El certificado marcado por defecto es el que se usará para hacer login.

3.5 PROYECTO HERRAMIENTAS PROPIETARIAS PARA TARJETAS TC-FNMT/CERES - SOPORTE TÉCNICO

Se trata de un conjunto de herramientas destinadas a facilitar el uso de la tarjeta TC-FNMT/CERES al “soporte técnico”.

El desarrollo es multiplataforma para garantizar su correcto funcionamiento en sistemas Windows, GNU/Linux y MacOS.

El propósito del desarrollo es generar una única implementación (por aplicación), y por lo tanto un único código fuente que se pueda desplegar y ejecutar en cada uno de los ss.oo. descritos arriba. De esta forma se obtienen ventajas significativas tanto a nivel de gestión (mantenimiento, documentación, etc), como de usabilidad para los usuarios que verán una interfaz homogénea y un desarrollo paralelo en las distintas plataformas.

Está desarrollado en Java y se generarán paquetes java (De esta forma cualquier equipo que cuente con la máquina virtual de java podrá lanzar la aplicación) y también los ficheros ejecutables.

La lista de herramientas es:

- Actualización de claves.
- Actualización de certificados
- Formatea tarjeta
- SC_Report

3.5.1 APLICACIÓN PARA ACTUALIZACIÓN DE CLAVES

Mediante el uso de esta aplicación se permite el borrado de las claves huérfanas de la tarjeta TC-FNMT/CERES.

3.5.2 APLICACIÓN PARA ACTUALIZACIÓN DE CERTIFICADOS

Mediante el uso de esta aplicación se permite el borrado de los certificados que no estén asociados a ninguna clave.

3.5.3 APLICACIÓN PARA FORMATEAR TARJETA

Se usará esta aplicación para poder realizar el reseteo de tarjetas CERES/TC-FNMT dejándolas en el estado inicial.

3.5.4 APLICACIÓN INFORME DE INSTALACIÓN Y TARJETA INTELIGENTE (SC_Report)

La aplicación es compatible con sistemas Windows y con tarjetas DNle, CERES/TC-FNMT y TIF.

La aplicación genera un informe en formato pdf con tres grandes bloques de información:

Entorno: Se obtendrá, por un lado, la información del sistema operativo, los lectores conectados, navegadores instalados, versiones de software, y por otro lado la información de los servicios involucrados en la comunicación con la tarjeta.

Instalables: Se volcará la información de las entradas del registro asociadas a cada uno de los instalables propietarios de la RCM-FNMT y del sistema de archivos (drivers/librerías/herramientas propietarias) de los mismos.

Tarjeta: Información de la tarjeta que se encuentra insertada en el lector. Se incluirá también la información de los objetos PKCS11 y PKCS15.

Por su parte las tarjetas a tener en cuenta serán:

- Tarjeta DNle
- Tarjeta CERES/TC-FNMT
- Tarjeta TIF

Para mantener la misma línea de desarrollo utilizada en proyectos similares, y teniendo en cuenta las ventajas que ofrece, el desarrollo es JAVA, de esta forma podría adaptarse la aplicación para, no solo Windows, sino otros sistemas operativos compatibles con JAVA.

4 ALCANCE DEL SERVICIO

Lo que se pretende es dar continuidad al mantenimiento del software relacionado con las tarjetas inteligentes que se comercializan:

- Tarjetas DNle (todas sus versiones)
- Tarjetas TIF (todas sus versiones)
- Tarjetas CERES/TC-FNMT (todas sus versiones)

Incluyendo:

- Mantenimiento correctivo
- Resolución de incidencias
- Adaptación a los nuevos requisitos

El servicio engloba en su totalidad el mantenimiento de los siguientes proyectos:

1. Proyecto CSP para CNP
 - Proyecto CSP dnle
 - Proyecto CSP tif
2. Proyecto CSP para FNMT-RCM
3. Proyecto multiPKCS11
4. Proyecto herramientas propietarias para tarjetas TC-FNMT/CERES - usuario final
5. Proyecto herramientas propietarias para tarjetas TC-FNMT/CERES - soporte técnico

5 ENTREGA

Se realizará la entrega debidamente versionado de:

- Fuentes

- Binarios
- Manuales

De los proyectos arriba detallados.

Se debe mantener al día el empaquetado de los paquetes para las nuevas distribuciones GNU/Linux que vayan liberándose durante el transcurso del contrato.

6 GARANTÍAS

La empresa adjudicataria debe ofrecer una garantía de 12 meses, a partir de la fecha de aceptación de los desarrollos llevados a cabo durante el contrato de mantenimiento

Esta garantía cubrirá cualquier defecto de funcionamiento detectado en los entornos operativos anteriormente descritos, atribuible al propio software.

7 REQUISITOS DE LA EMPRESA ADJUDICATARIA DEL SERVICIO

7.1 REQUISITOS MÍNIMOS

La empresa adjudicataria deberá contar con la experiencia suficiente en desarrollo de software para tarjetas inteligentes, así como otras actividades relacionadas con la prestación del servicio objeto del presente pliego. Para ello, deberá acreditar su experiencia en desarrollo/mantenimiento/ingeniería de software para tarjetas inteligentes de al menos 3 años, inmediatamente anteriores a la solicitud de esta oferta.

7.2 ASPECTOS VALORABLES

Aparte del requisito mínimo anteriormente expresado, la empresa contratada deberá utilizar el personal con los conocimientos técnicos necesarios y los organizará de forma que sea posible conseguir los objetivos establecidos. La empresa adjudicataria deberá presentar una descripción de los perfiles profesionales de los recursos que se dedicarán al servicio objeto del presente pliego.

También se valorarán aquellas mejoras y condiciones adicionales de carácter económico-financiero y técnico que se presenten.

8 OTRAS CUESTIONES

Para llevar a cabo el correcto mantenimiento de los proyectos detallados, FNMT hará entrega de los diferentes tipos de tarjetas, sus manuales de comandos y las últimas versiones de los códigos fuentes.

Habrá una persona de contacto perteneciente al área de Documentación y Tarjetas de la Dirección Comercial con la que se llevará a cabo la gestión de las incidencias, desarrollo de los nuevos requisitos y resolución de dudas técnicas referentes a los productos de la RCM-FNMT