ANEXO

APLICACIÓN DE FIRMA

Como se ha comentado anteriormente, uno de los principales usos del DNI electrónico es la realización de firma electrónica. Para utilizar esta funcionalidad de firma, numerosas aplicaciones pueden ser empleadas, ya que éstas acceden a las capas o módulos intermedios de CSP y PKCS#11, que proporcionan un interfaz estándar de acceso a la tarjeta.

En el presente anexo se describe el manual de uso de una aplicación de firma que, si bien no es única y exclusiva para la operación con el DNIe, a la fecha es la referencia para la realización de firma electrónica con la tarjeta DNIe.

Las operaciones facilitadas por esta aplicación son:

- Firma: firma de un archivo, generando un nuevo fichero de firma.
- Firma documento adjunto: firma de un archivo, generando un nuevo fichero de firma, que contiene los datos firmados.
- Verificación off-line: comprobación de un archivo firmado con documento adjunto, en este tipo de verificación únicamente se comprueba si el certificado con el que ha firmado esta o no caducado, si el fichero firmado ha sido modificado y si el certificado de firma pertenece a una entidad de certificación de confianza.
- Verificación off-line sin documento adjunto: comprobación de un archivo firmado, en este tipo de verificación únicamente se comprueba si el certificado con el que ha firmado esta o no caducado y si el fichero firmado ha sido modificado, con respecto a un archivo facilitado por el usuario de la aplicación o mediante la inclusión de datos en un espacio facilitado por la aplicación.
- Verificación on-line: comprobación de un archivo firmado con documento adjunto. Comprende la verificación off-line y la comprobación del estado del certificado vía OCSP.
- Verificación on-line sin documento adjunto: comprobación de un archivo firmado. Comprende la verificación off-line sin documento adjunto y la comprobación del estado del certificado vía OCSP.

Todas y cada una de estas funciones soportarán firma múltiple.

Tanto los ficheros de firma resultantes como los de entrada a las operaciones de verificación seguirán el estándar CMS.

Hay que señalar que el usuario es el responsable final de utilizar la funcionalidad de firma en un sistema de creación de firma electrónica que garantice el cumplimiento de las garantías que exigen la Ley 59/2003 de firma electrónica y la directiva de firma electrónica (1999/93/CE), para su consideración como firma electrónica reconocida. Tales sistemas y aplicaciones son los homologados por la Dirección General de la Policía, con certificación del CCN.

Por otra parte, los sistemas y aplicaciones antes mencionados han de cumplir los siguientes requisitos:

- La aplicación de generación de firma electrónica debe realizar el hash de los datos a ser firmados por el DNIe utilizando el algoritmo SHA-1
- La aplicación de generación de firma debe iniciar las comunicaciones con la tarjeta DNIe, a tal objeto, bajo un canal seguro (se proporciona esta posibilidad) que proporcione integridad y confidencialidad de los datos enviados y recibidos entre este sistema y el DNIe

Contexto del sistema

La aplicación esta basada en:

- Módulos PKCS#11 (interfaz con dispositivo de firma) desarrollados por la FNMT-RCM.
- Herramientas software para la implementación de operaciones criptográficas.
- Servicio de verificación de certificados (OCSP) de la FNMT-RCM.

Para la ejecución del programa es necesario que el usuario tenga instalada la máquina virtual de java, en su versión 5 (JRE 1.5).

Acrónimos y abreviaturas

Acrónimo / Abreviatura	Termino expandido
PKCS#11	Public Key Certificate Standard Number 11
PKCS#7	Public Key Certificate Standard Number 7
CMS	Cryptographic Message Syntax
OCSP	Online Certificate Status Protocol
JCE	Java Cryptography Extensión

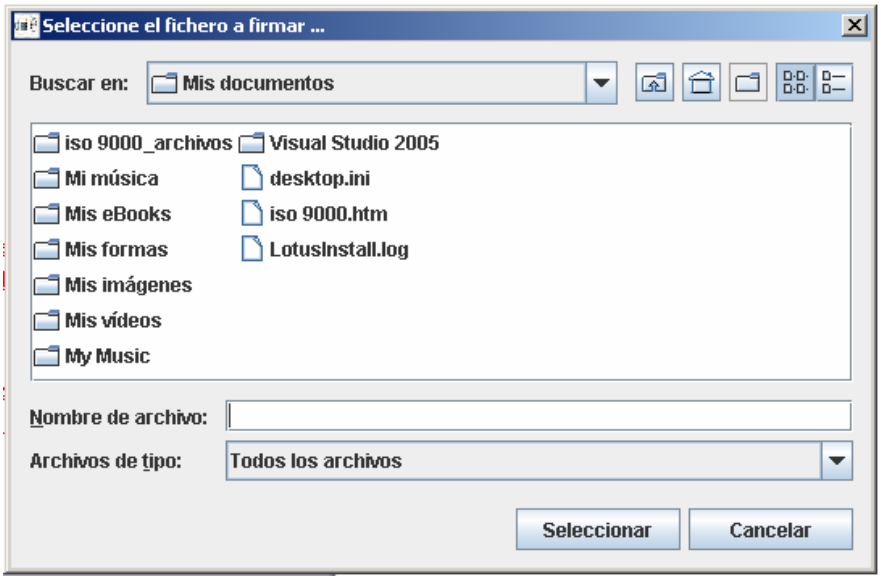
Interfaz general de usuario

Aquí se describe la interfaz de usuario donde encontraremos acceso a todas las funcionalidades de la aplicación.

Esta primera interfaz de usuario da acceso a todas las funcionalidades de la aplicación, en este caso a las de firmar, verificar, configurar y a la ayuda.

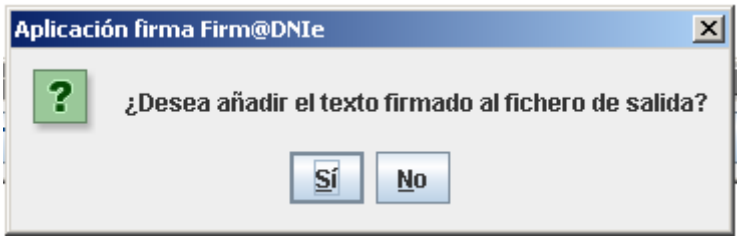
Firma

Cuando pulsemos en el botón de firmar, lo primero que se nos solicitará, es el fichero que deseamos firmar, para lo cual se nos muestra una pantalla como la siguiente:

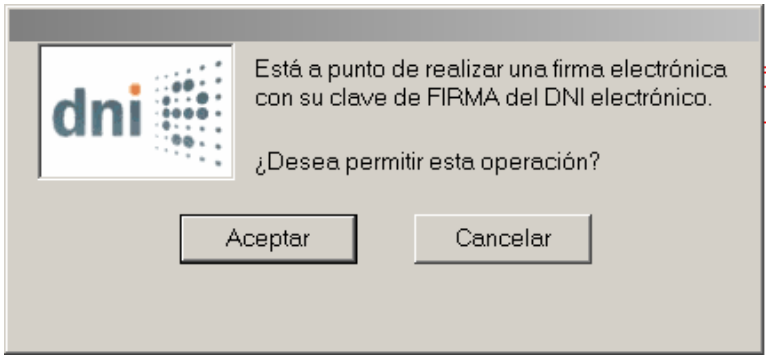


A continuación, tras seleccionar el fichero, se nos pide el código PIN

Si el código introducido es el correcto se nos pedirá una decisión para incluir o no lo firmado dentro de la propia firma generada, si es que sí, se generará un archivo que contiene lo firmado y la firma propiamente dicha



Posteriormente se nos pide autorización para realizar la operación



Finalmente se nos informa sobre el resultado de la operación

Y se nos pide el nombre del fichero en el que queremos almacenar el resultado

Se puede consultar una ayuda más detallada sobre este proceso en el menú de ayuda de la propia aplicación.

Verificación

En el proceso de verificación de un fichero firmado, mediante un cuadro de selección de ficheros, se nos solicitará la elección del mismo. Paso tras el cual se pedirá, si fuera necesario, el fichero original que se firmo. En este proceso no se requiere el código PIN del DNI electrónico, ya que la verificación se realiza mediante la clave pública del firmante del documento, no siendo necesario acceder en ningún caso a partes protegidas del DNI.

Pulsando el botón de “Verificar” se nos pide el fichero donde se encuentra la firma y en su caso los datos (si no estuviera en el mismo fichero, se nos solicitará el fichero de datos).

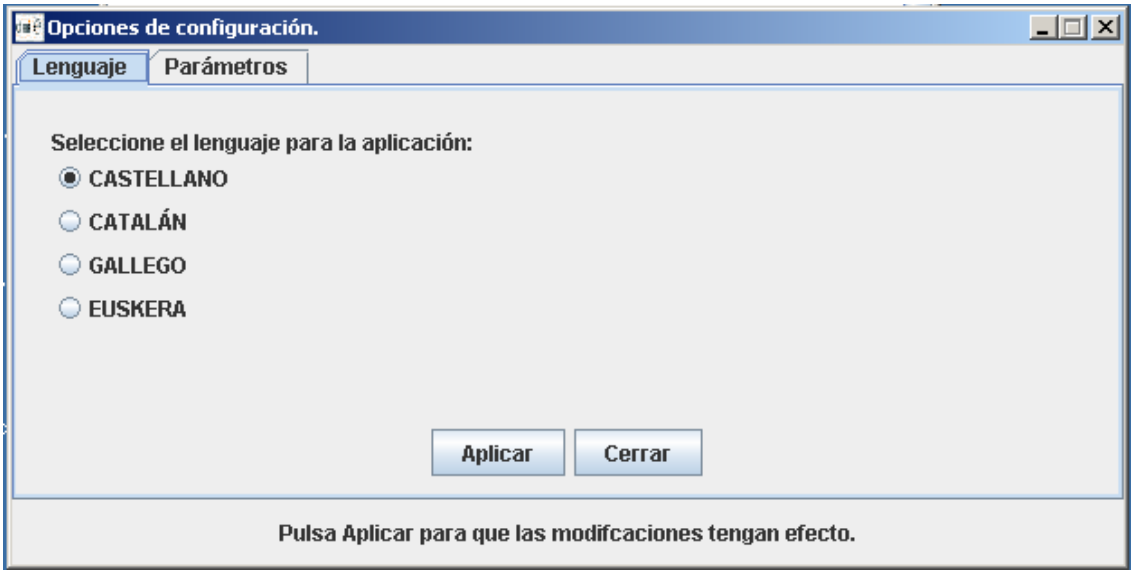
Una vez seleccionado el fichero, se nos muestra el resultado de la operación de forma gráfica y en la pantalla de resultados un detalle de la operación:

Puede encontrar más información sobre esta operación en la ayuda de la propia aplicación.

Configuración

La aplicación da la posibilidad de configurar una serie de parámetros como por ejemplo el lenguaje en el que se muestran los textos, etc.

El menú de configuración presenta el siguiente aspecto:



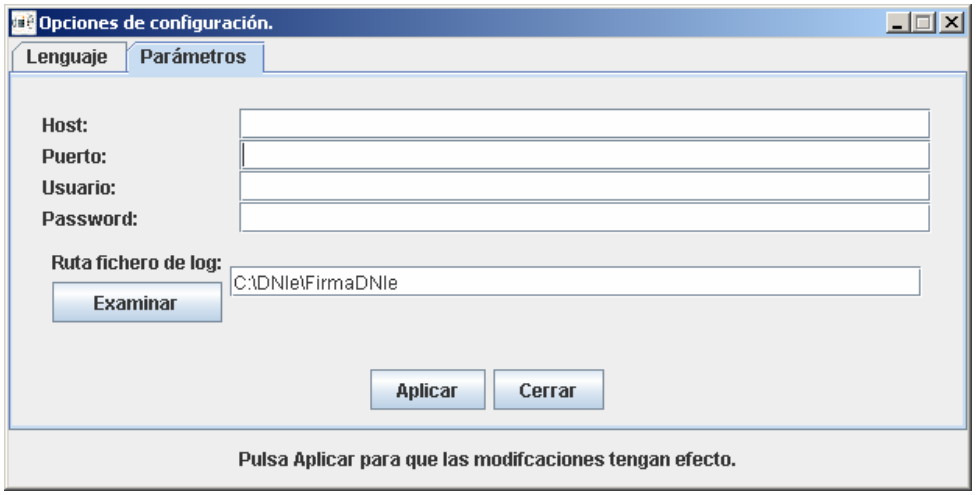
A través de las diferentes pestañas podremos ir accediendo a la configuración de los diferentes elementos que conforman la aplicación.

Es de especial interés la pestaña de parámetros en que se encuentran parámetros determinantes para el funcionamiento de la aplicación.

En primer lugar, si su ordenador tiene salida a la red pública a través de un Proxy que da servicio en un determinado puerto, ha de indicar su dirección y puerto en el campo “Host” y “Puerto” respectivamente

En el caso de que el proxy necesite autenticación con usuario y password se rellenarán los campos correspondientes.

Finalmente en el campo “Ruta de fichero de log” indicaremos el archivo donde queremos que la aplicación guarde un registro más detallado de su actividad.



Ayuda

La aplicación además ofrece una ayuda HTML que explica el funcionamiento del programa, y da una serie de nociones sobre criptografía.

La ayuda se presenta en el siguiente formato: