PROCESADOR:

Word 97

PUNTO DEL TEMARIO:

De “Oportunidades y desafíos”:
- Exigencias organizativas…..
- Administración electrónica…
- La Administración abierta 24….
- El marco regulatorio de la seguridad…

De “ Aspectos tecnológicos de la Administración…….”
- Infraestructura tecnológica en materia de…..

SOLUCIONES DE SEGURIDAD EN LAS COMUNICACIONES DE LA I.G.A.E.: CERES FICHERO Y SU APLICACIÓN EN TESEO

El área de Informática Presupuestaria de la I.G.A.E. lleva algún tiempo estudiando cómo dotar de las necesarias características de confidencialidad, integridad, no repudio y disponibilidad a los intercambios de información que se producen en los sistemas de su responsabilidad en los ámbitos de la Contabilidad Pública y del Control, con objeto de extender estas experiencias al resto de Sistemas de Información de la I.G.A.E.

Como es sabido la ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y de Orden Social encargaba a la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, F.N.M.T.-R.C.M., la implantación de un sistema de seguridad telemática para las relaciones entre particulares y la Administración y entre Organismos de la misma, lo que ha dado lugar al proyecto CERES.

El sistema elegido por la F.N.M.T.-R.C.M. se encuadra dentro de los denominados de clave pública. A grandes rasgos, y sin pretender dar nada más que una visión de conjunto de los procedimientos empleados, su funcionamiento es el siguiente:

Ambas partes, tanto el remitente del documento cifrado como el destinatario deben estar en posesión de certificados válidos emitidos por la F.N.M.T.-R.C.M.

El remitente del documento cifrado se autentica ante la F.N.M.T.-R.C.M. y descarga la clave pública del destinatario.

En el sistema del remitente se cifra el documento empleando una clave aleatoria y un algoritmo simétrico. La clave aleatoria, a su vez, se cifra usando la clave pública del destinatario y un algoritmo asimétrico. El documento cifrado y la clave cifrada constituyen el llamado sobre digital que se envía al destinatario.

La firma digital estriba en obtener un resumen tal que identifique al documento, y cifrarlo con la clave privada del remitente.

El destinatario descifra el mensaje haciendo uso de su clave privada.

Para la verificación descifrará la firma con la clave pública del remitente, obteniendo el resumen transmitido, resumen que comparará con el obtenido a partir del documento descifrado.

Aplicación a las necesidades de la I.G.A.E.: CERES Fichero.

Al analizar en la I.G.A.E. las prestaciones de los productos de la F.N.M.T.-R.C.M. se vio que para mejor adaptarse a las necesidades actuales sería conveniente desarrollar una ampliación que permitiese cifrar un fichero y guardarlo en ese estado, sin que la operación tuviera que estar ligada necesariamente al hecho de enviarlo por correo electrónico.

Desde el punto de vista de la I.G.A.E. había muchas ventajas, entre las que se pueden citar el independizarse del correo a usar, la flexibilidad a la hora de decidir el momento y el soporte para el envío de la información, la posibilidad de integrar tal función en las aplicaciones en curso o en las de nuevo diseño, el poder guardar la información cifrada en el propio disco del PC,.....

El resultado de tal ampliación ha sido una herramienta denominada CERES Fichero, desarrollada en colaboración con la F.N.M.T.-R.C.M., y que se distribuirá conjuntamente con el software de CERES. Nace con la ambición de ser el elemento básico para las funciones de seguridad de datos en la I.G.A.E. y aúna las funcionalidades que se han creído necesarias tras analizar las tendencias del mercado y los deseos de los usuarios.

CERES Fichero se compone de una interface en Visual Basic V. 5 y las llamadas a las librerías de cifrado y de firma digitales, y necesita para su funcionamiento la instalación básica y parte de las tool-kits de CERES. Está preparado para trabajar tanto con certificados en tarjeta - lo que permite la firma digital avanzada, según el Real Decreto Ley 14/1999 de 17 de septiembre de 1999 - como con certificados en software. Su funcionamiento se ha comprobado tanto en Windows 95 como en Windows NT, y en su diseño se han seguido las pautas de los estándares para microinformática de la I.G.A.E.

En las explicaciones siguientes cifrar significará cualquiera de las operaciones de cifrado, de firma o de cifrado y firma, y descifrar se empleará - de igual modo - para referirnos a cualquiera de las operaciones de descifrado o de verificación de una firma. Con la aclaración de que, si bien el usuario puede elegir si desea cifrar, firmar o cifrar y firmar sus ficheros en el caso de operar sobre un fichero que ya esté cifrado o firmado el sistema hace todas las operaciones necesarias para ponerlo en claro y verificar la firma. Así hay un botón para cada operación de cifrado, de firma y de cifrado y firma, mientras que hay un único botón para el descifrado y verificación de firma.

Los ficheros conservan el nombre del original, sea éste un fichero en claro o uno cifrado. Al cifrar se añade la extensión atn, y al descifrar se elimina.

Funciones de CERES Fichero.

El modo de operación es el siguiente:

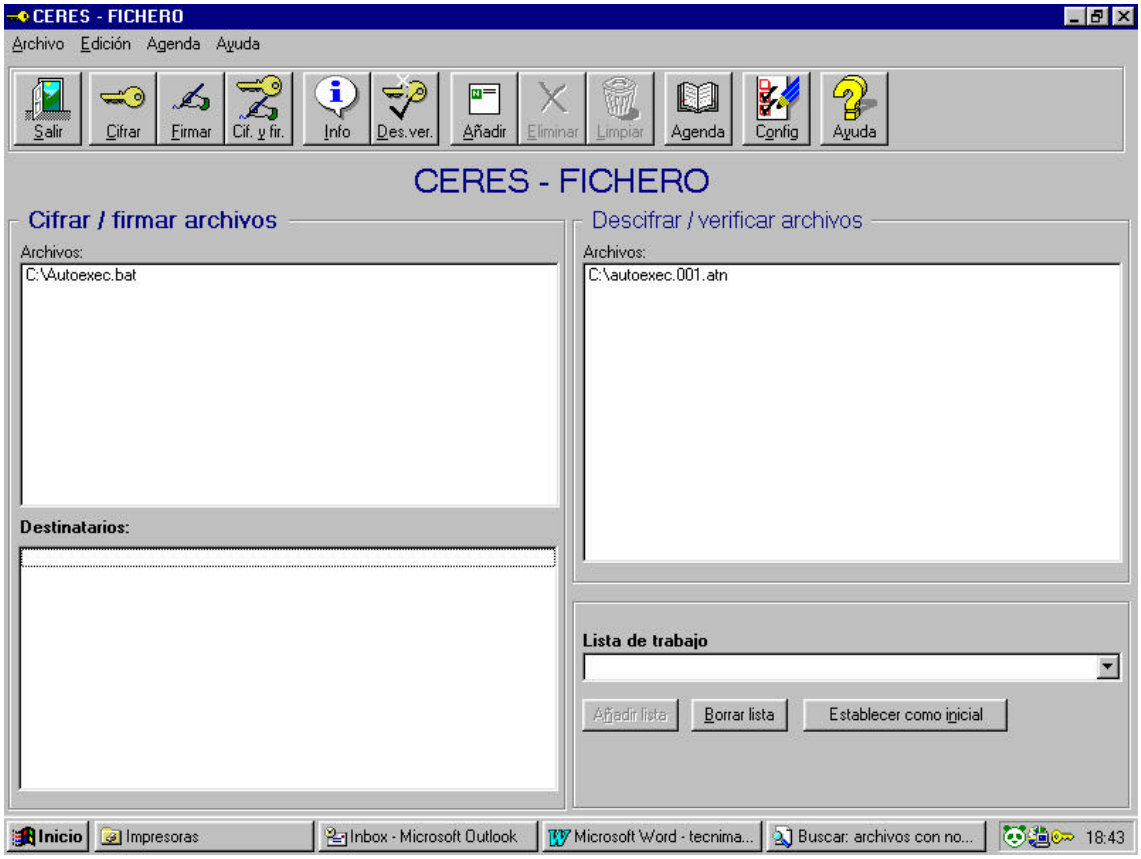
Para cifrar, firmar o cifrar/firmar se elige el fichero, o los ficheros, de entre las unidades accesibles al sistema, y se pulsa el botón de cifrar, o el de firmar, o el de cifrar y firmar. El sistema cifra para el conjunto de destinatarios que se haya elegido, y si tal lista está vacía entiende que debe cifrar para el propio usuario del sistema.

Una vez cifrados - o firmados, según qué operación se haya efectuado - el resultado queda almacenado en el propio directorio que alberga a los ficheros sin cifrar.

La elección de destinatarios se hace por referencia a una agenda que debe estar cargada previamente y a la que nos referiremos más adelante.

También es posible cifrar por listas de trabajo. Este procedimiento consiste en tener predeterminados - para cada lista de trabajo - unos nombres de ficheros y unos destinatarios, lo que puede ser especialmente adecuado para trabajos repetitivos y podría ser la base de futuros desarrollos en los que sea recomendable vetar el acceso a la agenda o a la lista de ficheros. Las listas de trabajo se almacenan en el sistema, y se puede elegir que una de ellas se cargue como inicial, con lo que al acceder a las pantallas de selección aparecerían los ficheros y destinatarios de tal lista.

Pantalla de cifrar, descifrar, establecer destinatarios y definir listas de trabajo



Para descifrar se procede de modo similar: se buscan los ficheros a descifrar de entre las unidades accesibles y se pulsa el botón de descifrar. Los ficheros descifrados quedarán almacenados en el mismo directorio de los ficheros originales.

Para esta operación se ha previsto una función de información acerca del remitente, operación que se ha preferido quede separada de modo que no modifique el fichero, una vez descifrado, en relación al fichero original. Esta función, además, nos da ciertos datos del certificado del remitente que pueden ser útiles a la hora de cargar la agenda que se ha mencionado más arriba.

Dentro de la idea de simplificar al máximo el uso de esta herramienta se han minimizado los ajustes iniciales. Con el botón de Configuración el usuario puede activar:

Aviso del sistema si ya existe un fichero con el mismo nombre que vaya a tener el fichero resultante de la operación de cifrado o de la de descifrado.

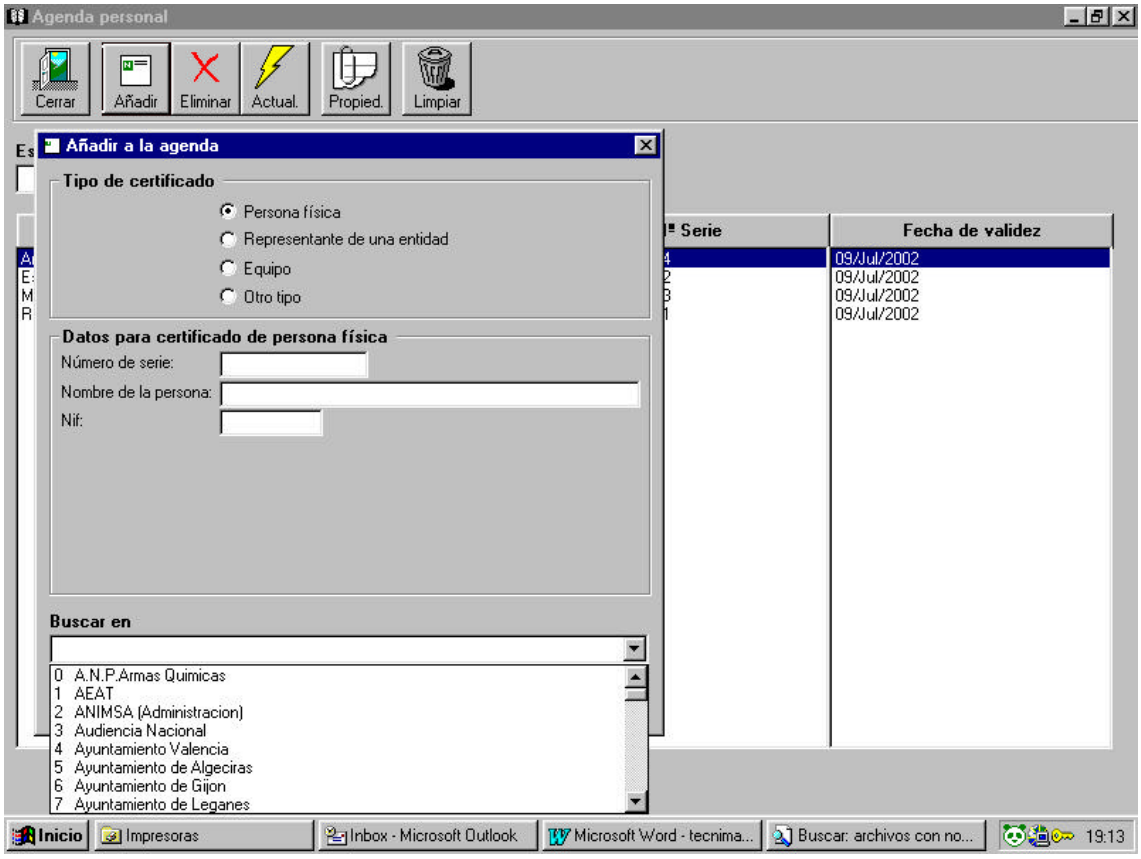
Borrado del fichero original.

En el caso de haber elegido la opción anterior se ofrece la posibilidad de borrado seguro.

La agenda contiene la lista de posibles destinatarios y en el formato adecuado para poder encontrar en el directorio X-500 de la F.N.M.T.-R.C.M. de modo eficiente los certificados de aquellos para los que queramos cifrar. Para el caso de tener agendas muy extensas se ha incorporado el clásico sistema de búsqueda por las primeras letras del nombre.

El mantenimiento de la agenda se hace mediante una pantalla en la que se capturan los datos necesarios: nombre al que la F.N.M.T.-R.C.M. haya emitido el certificado, número de serie, NIF, organización a la que pertenece. Es exactamente así para el caso de personas físicas y muy parecido para el caso de representantes de entidades o para el caso de certificados de servidores. De cualquier modo, y por indicación de la Agencia de Protección de Datos, es necesario conocer con total precisión los datos del certificado cuya clave pública queremos incorporar a nuestro sistema, lo que claramente impide cualquier procedimiento de búsquedas masivas.

Pantalla de mantenimiento de la agenda



Este desarrollo se está utilizando ya en algunas aplicaciones de la I.G.A.E. relacionadas con el Control, como TESEO y AURIGA.

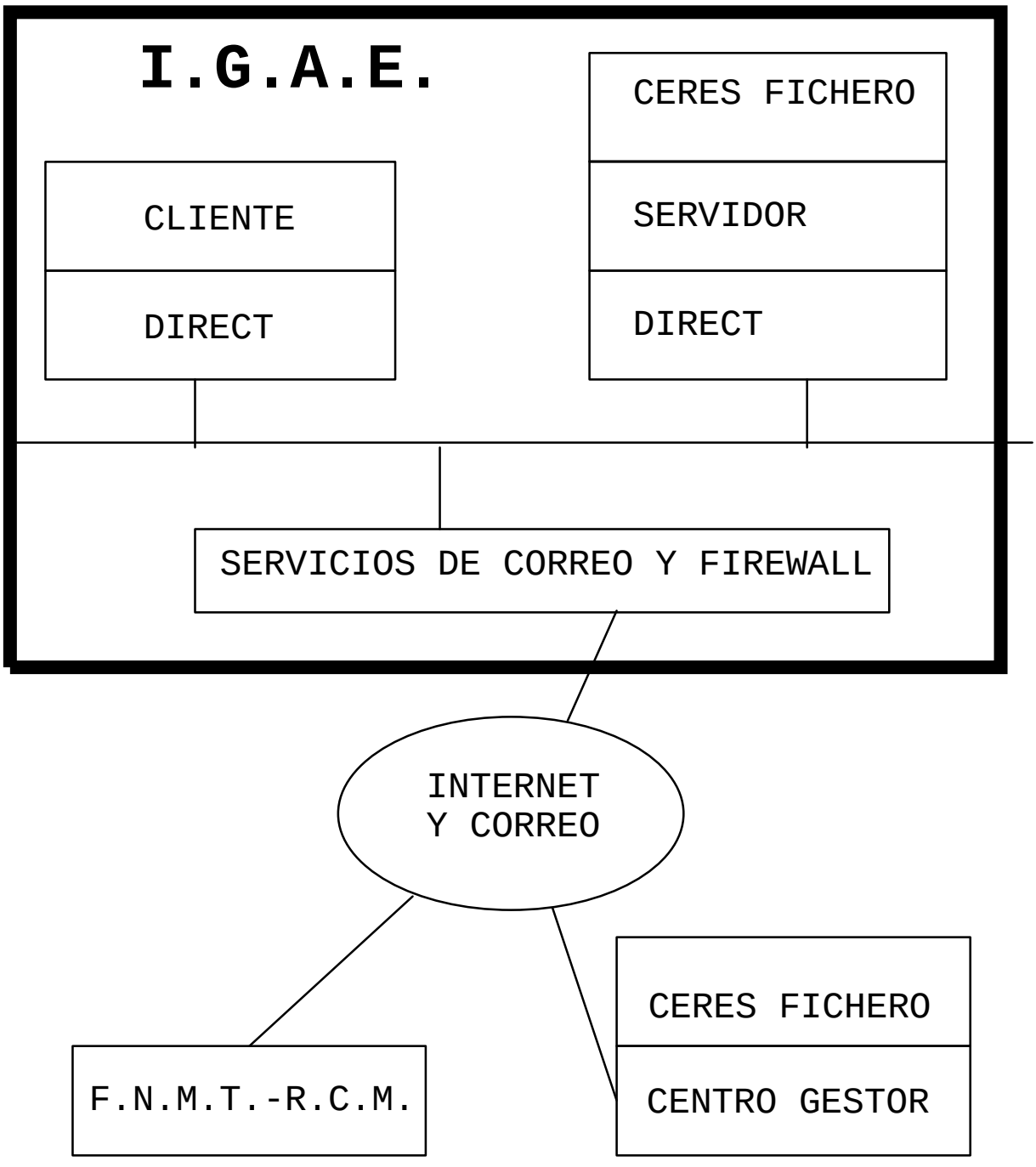
Aplicación a TESEO.

TESEO es un sistema de información para la creación y gestión de la Base de Datos Nacional de Perceptores de Subvenciones en el que se necesita transmitir datos entre la I.G.A.E. y los Centros gestores de las mismas, datos que por su carácter confidencial precisan de la máxima seguridad. En el esquema de funcionamiento que se ha definido la herramienta que proporciona las funciones de cifrado y de firma es CERES Fichero, con una particularidad sobre lo descrito anteriormente, y es que el equipo de la I.G.A.E. para el que cifran desde los Centros gestores es un servidor.

Esta condición añade la necesidad de que los usuarios de la I.G.A.E. que deban acceder al CERES Fichero del servidor han de estar autenticados ante éste de modo seguro.

La solución que se ha elegido en la I.G.A.E. pasa de nuevo por el uso de los certificados digitales emitidos por la F.N.M.T.-R.C.M.

En el esquema siguiente se expone el modelo de funcionamiento al completo, tanto en lo que concierne al cifrado entre el servidor de TESEO y los Centros gestores como la autenticación de los usuarios de la I.G.A.E. frente al servidor.



El cifrado se efectúa, según se ha descrito antes, con CERES Fichero.

La autenticación exige el uso de otro producto de la F.N.M.T.-R.C.M., el Direct, que actúa como proxy entre el cliente y el servidor, y que obtiene los datos para el reconocimiento mutuo de los certificados digitales. Si el resultado es satisfactorio la petición se dirige a la zona segura del servidor, y si no lo es se ignora.

A continuación, ya en la zona segura del servidor, una página web y un módulo CGI recogen las peticiones de los clientes, y el CGI devuelve un objeto manejable por las páginas ASP que se puede contrastar con una base de datos SQLServer en la que se han almacenado las operaciones y los accesos a los que tenga derecho cada usuario del sistema.

Las páginas ASP reciben el objeto desde el servidor y realizan la comparación indicada más arriba con la base de datos, y si ésta es correcta llaman al servicio de CERES Fichero y le pasan los parámetros deseados.

En el desarrollo de CERES Fichero han participado los componentes del Proyecto CERES de la F.N.M.T.-R.C.M. y un equipo de trabajo multidisciplinar por parte de la I.G.A.E.