La tarjeta de identidad española como método de autenticación en redes sociales

V. Gayoso Martínez, L. Hernández Encinas
y A. Martín Muñoz

Departamento Tratamiento de la Información y Criptografía (TIC)

Instituto de Tecnologías Físicas y de la Información (ITEFI),

Consejo Superior de Investigaciones Científicas (CSIC), Madrid

{victor.gayoso, luis, agustin}@iec.csic.es

29 de Octubre de 2013

Contenidos

Las escasas restricciones y la poca protección que los menores tienen para acceder a internet hace que éstos sean especialmente vulnerables (abusos, pedofilia, etc.).

La autenticación de ciudadanos se realiza mediante las tarjetas de identificación nacional. Si éstas incorporaran primitivas criptográficas, se podrían utilizar para permitir o rechazar el acceso a determinados servicios en la red.

En esta comunicación presentamos un protocolo criptográfico de autenticación, desarrollado en Java y basado en el Documento Nacional de Identidad electrónico (DNIe) español, que puede extenderse a tarjetas de identidad con características criptográficas similares.

Comentamos además la estructura lógica, el contenido y las diferencias existentes entre los DNIe emitidos para adultos y los emitidos para menores.

El DNIe es una tarjeta de policarbonato similar a las actuales tarjetas de crédito que incluye un chip con capacidades criptográficas. Los datos del ciudadano están impresos en el anverso y reverso de la tarjeta y el chip almacena los datos biométricos y criptográficos del ciudadano (firmados digitalmente por la DGP).

Información almacenada en el chip

Zona pública:

- Certificado X.509 de componente con clave RSA-1024.
- Certificado X.509 de componente de la AC intermedia con clave RSA-1024.
- Certificado X.509 de la AC intermedia de la DGP con clave RSA-2048 (el Certificado X.509 de la AC raíz de la DGP tiene una clave RSA-4096).

Zona privada (acceso con PIN):

- Certificado X.509 de usuario de autenticación con clave RSA-2048.
- Certificado X.509 de usuario de firma con clave RSA-2048.

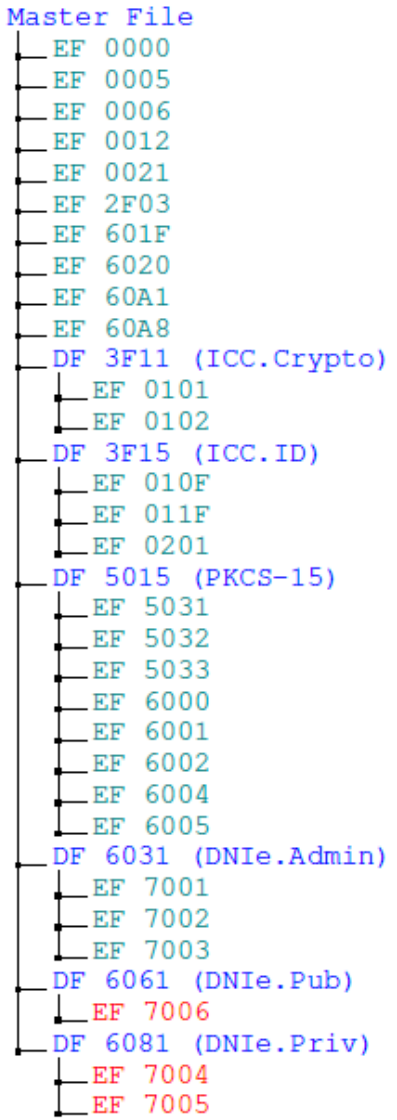
Zona de seguridad (autenticación biométrica):

- Datos de filiación del ciudadano (los mismos del soporte físico).
- Imagen escaneada de la fotografía.
- Imagen escaneada de la firma manuscrita.

El DNIe es compatible con el estándar PCKS #15 y su estructura de ficheros tiene dos tipos: directorios (DF, *Dedicated File*) y elementales (EF, *Elementary File*).

Los ficheros en rojo están en los DNIe de adultos y no en los de menores.

Un menor (en este trabajo) es un ciudadano de menos de 14 años. Los DNIe de los ciudadanos entre 14 y 18 años pueden contener los dos certificados, previa autorización de su tutor.



Determinadas acciones con el DNIe están sujetas a la existencia de un canal seguro de comunicación (envío de PIN).

Las cuatro fases que se deben seguir para establecer el canal seguro entre un terminal y el DNIe son las siguientes:

Fase 1. Verificación de certificados: al finalizar el intercambio de certificados, tanto el terminal como la tarjeta tendrán la clave pública y el certificado del otro.

Fase 2. Autenticación interna: el terminal solicita a la tarjeta que se autentique.

Fase 3. Autenticación externa: la tarjeta solicita una autenticación al terminal.

Fase 4. Establecimiento de clave de sesión: después de la autenticación mutua, ambos determinan la clave de cifrado y la clave MAC.

- `Master File`
  - `EF 0000`: contiene el PIN del usuario.
  - `EF 0006`: contiene el número de soporte de la tarjeta.
  - `EF 2F03`: información sobre el sistema operativo del DNIe.
  - `EF 601F`: certificado de componente.
  - `EF 6020`: certificado de la AC intermedia de componente.
- `DF 5015 o PCKS-15`
  - `EF 6001`: metadatos sobre las claves privadas utilizadas.
  - `EF 6002`: metadatos sobre las claves públicas utilizadas.
  - `EF 6004`: información sobre certificados y datos personales.
- `DF 6031 o DNIe.Admin`
  - `EF 7001`: contiene los datos de filiación.
  - `EF 7002`: almacena la imagen facial escaneada.
  - `EF 7003`: imagen de la firma manuscrita escaneada.
- `DF 6061 o DNI.Pub`
  - `EF 7006`: certificado de la AC intermedia de la DGP.
- `DF 6081 o DNI.Priv`
  - `EF 7004`: certificado de firma del usuario.
  - `EF 7005`: certificado de autenticación del usuario.

- El ATR (*Answer To Reset*) enviado por los DNIe es una cadena de bytes que incluye el término "DNIe" (`0x444E4965`) por lo que se puede utilizar para determinar si una tarjeta inteligente es realmente un DNIe.
- En el DNIe de un menor existen los directorios `DNI.Pub` y `DNI.Priv`, pero están vacíos, no así para los adultos. Los ficheros `EF 7006`, `EF 7004` y `EF 7005` no se generan cuando se emite el DNIe de un menor.
- Los certificados `EF 601F`, `EF 6020` y `EF 7006` son accesibles sin el canal seguro y sin PIN. Por el contrario, los certificados `EF 7004` y `EF 7005` exigen el PIN, por lo que hace falta el canal seguro.
- Los certificados `EF 601F` y `EF 6020` están almacenados en la tarjeta sin comprimir. En cambio, los certificados `EF 7006`, `EF 7004` y `EF 7005` están almacenados en formato comprimido (*zlib*).

- Todos los DNIe tienen PIN, que se puede bloquear. En los DNIe de adultos, éste se puede desbloquear mediante autenticación biométrica; no así para los DNIe de menores.
- La información accesible sin PIN en un DNIe de adulto es: país, nombre, apellidos y Número de Identificación Fiscal (NIF). Todos ellos incluidos en el fichero `EF 6004` (así como en los certificados `EF 7004` y `EF 7005`).
  El fichero `EF 6004` del DNIe de un menor está vacío, por lo que imposible obtener estos datos.
- Por lo anterior es posible distinguir el DNIe de un adulto del de un menor a través del contenido del fichero `EF 6004`.
- La fecha de nacimiento de un adulto se puede leer de cualquiera de los dos certificados de usuario (accesible con PIN y, por tanto, a través de un canal seguro).

Las propiedades del DNIe nos han permitido desarrollar una aplicación Java con el fin de decidir si la tarjeta que se está leyendo es un DNIe y, en tal caso, leer todos los posibles ficheros que contiene (con o sin PIN) y decidir si el mismo es de un adulto o de un menor.

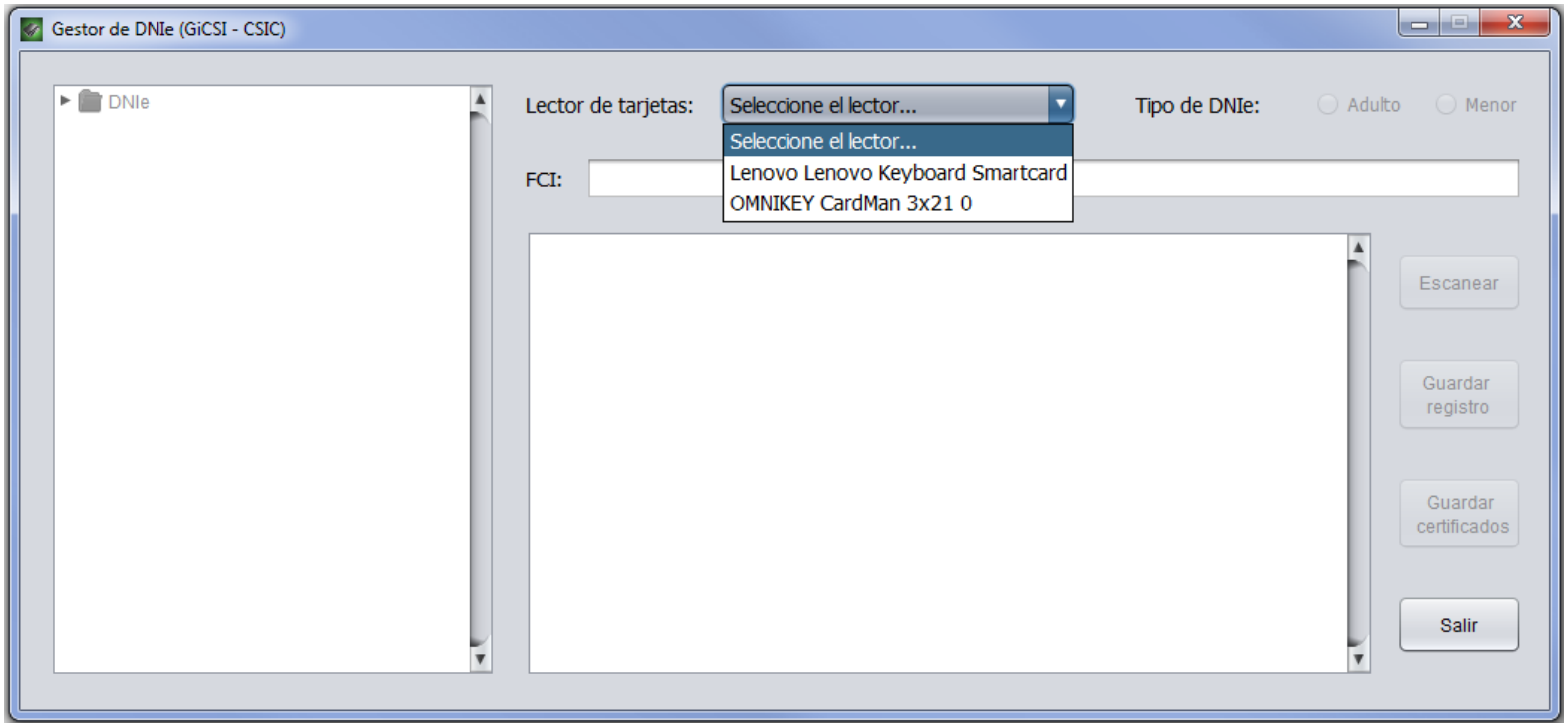
Esta discriminación permite (entre otras cosas):

- Impedir el registro y acceso de menores a páginas de adultos.
- Evitar que adultos se puedan hacer pasar por menores.
- Definir protocolos de autenticación de ciudadanos permitiendo su acceso a información a la que están suscrita.

Aplicación *Gestor de DNIe* (GDNIe)

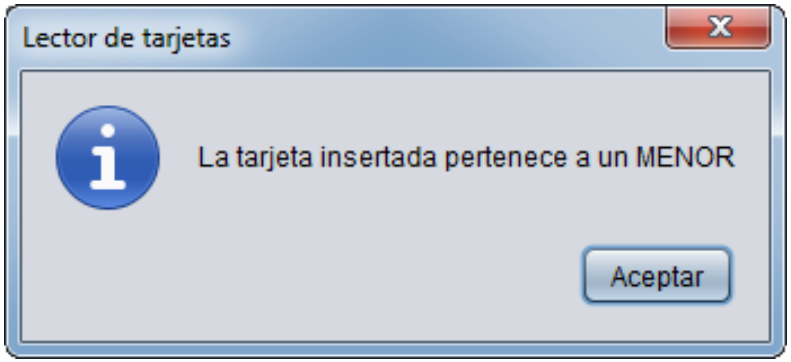
Una vez lanzada la aplicación, se selecciona el lector de tarjetas donde se insertará el DNIe. Hasta entonces, los botones de la aplicación estarán desactivados.

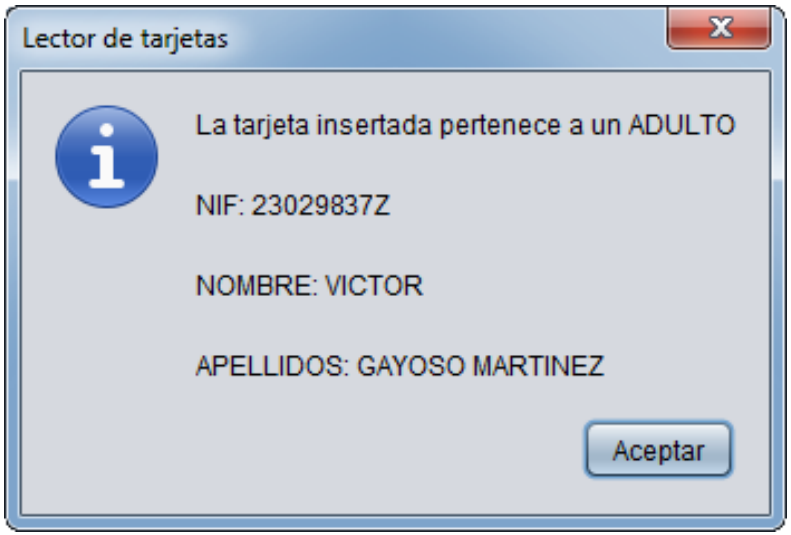
Si la tarjeta no es un DNIe, se avisa del error.



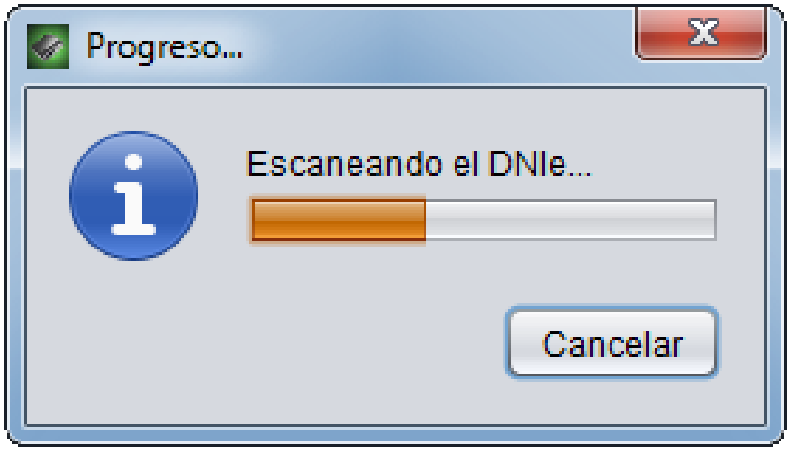
En el paso siguiente, la aplicación muestra el tipo de DNIe: de adulto o de menor.

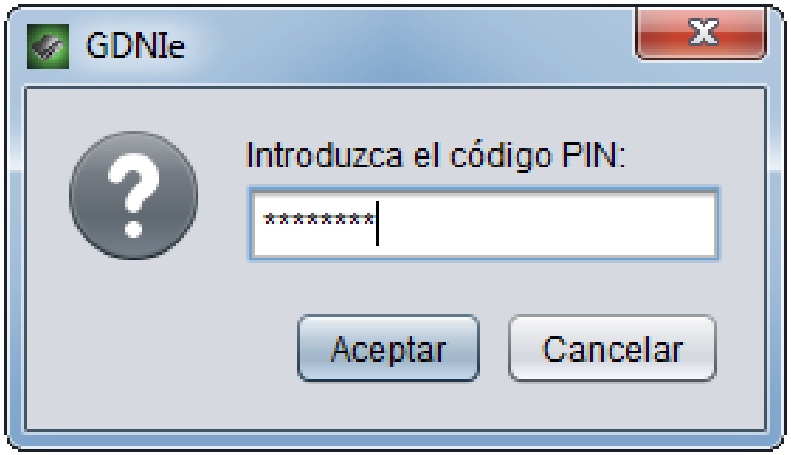
Si el DNIe es de un menor sólo se indica este hecho y si es de un adulto se muestran algunos de sus datos.





Eligiendo *Escanear*, se inicia el establecimiento de un canal seguro con la tarjeta, tras el que se procede al escaneado de los ficheros del DNIe.

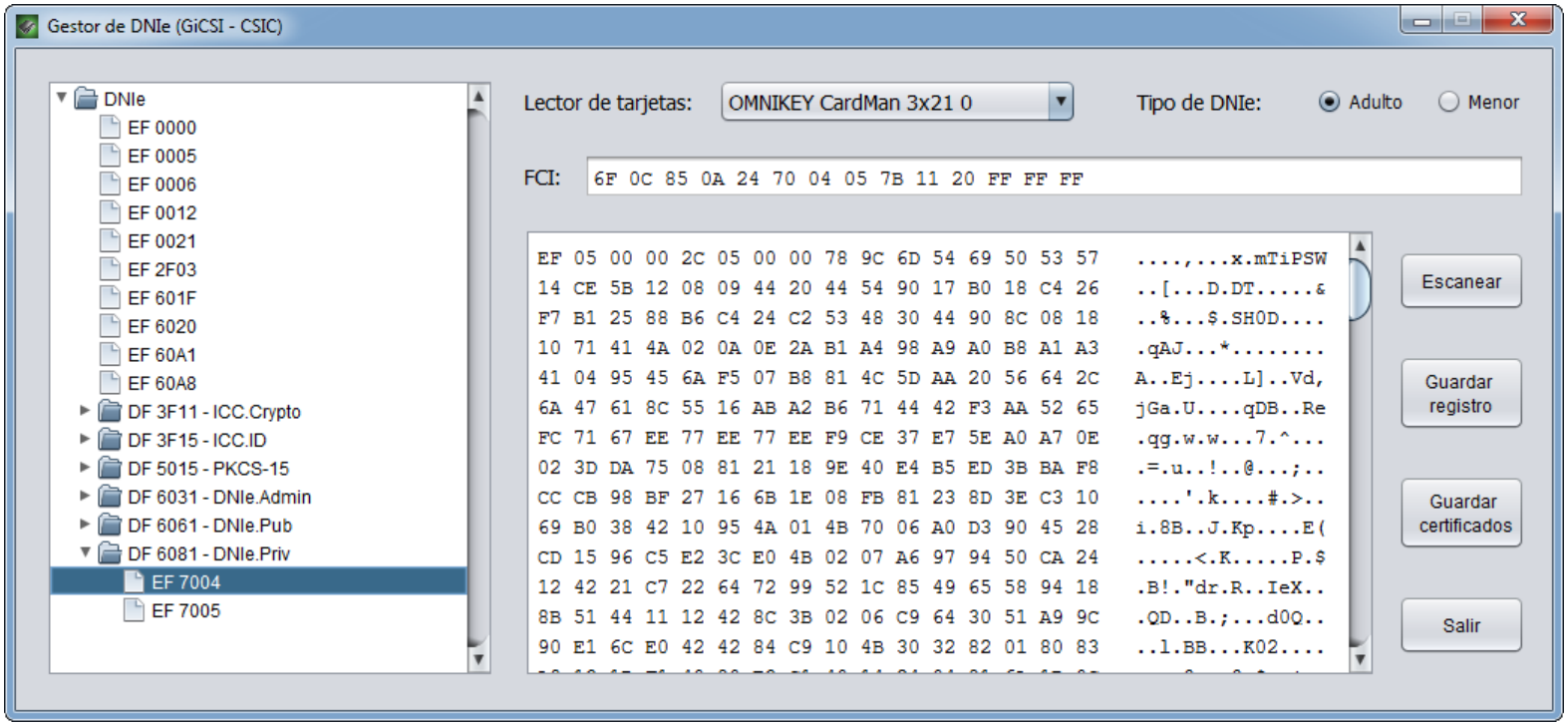




Si el DNIe es de un menor o si es de un adulto y no se introduce el PIN, el escaneado del DNIe continúa sin establecerse un canal seguro.

En este caso, no se mostrarán los certificados del usuario (o no existen o no se tiene acceso a ellos).

En la visualización y navegación por el árbol de directorios del DNIe, la información del fichero seleccionado se muestra en las cajas de texto correspondientes.



El usuario puede guardar la información asociada a todos los elementos del DNIe en un fichero de texto, denominado *registro*.

Para ello, se pulsa en *Guardar registro* y se almacena toda la secuencia de comandos y respuestas APDU intercambiadas entre la aplicación y el DNIe, así como el contenido de los ficheros que la aplicación haya podido leer.

Si el usuario ha escaneado el DNIe correspondiente a un adulto y ha verificado correctamente su código PIN, en caso de querer guardar sus dos certificados de usuario deberá pulsar en *Guardar certificados*.

Conclusiones

- Se ha presentado la estructura interna del Documento Nacional de Identidad electrónico de España y se ha detallado el contenido de sus ficheros más importantes.
- Se han mostrado las diferencias entre los DNIe de adultos y de menores, proponiendo su uso como método de autenticación en determinadas circunstancias (permitir o rechazar el registro de ciudadanos en determinadas redes atendiendo a su edad).
- Se ha presentado una implementación en Java que permite acceder al contenido del DNIe discerniendo entre adultos y menores, y sirviendo de ejemplo a las posibilidades que ofrece el DNIe como mecanismo de autenticación.
- En el futuro, un protocolo de autenticación similar al expuesto en esta contribución podría ser empleado en distintos países si sus tarjetas de identificación ofrecieran características similares.

Muchas gracias por su atención