DNIe

Bloque I. Tema 1

Gestión de Sistemas e Informática

Curso 2017 - 18

Juan José Aguado Gil

02 Agosto 2017

1. La Firma Electrónica. Conceptos Básicos

La *Firma Electrónica* es un sistema de acreditación que permite verificar le identidad de las personas con el mismo valor que la firma manuscrita, autentificando las comunicaciones generadas por el firmante.

La **Ley 59/2003 de Firma Electrónica**, distingue entre:

- **Firma Electrónica Avanzada**: aquella firma electrónica que permite establecer la identidad personal del suscriptor respecto de los datos firmados y comprobar la integridad de los mismos.
- **Firma Electrónica Reconocida**: aquella firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Tendrá respecto de los datos consignados de forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

2. Descripción Funcional del DNIe

2.1. Identificación

El DNIe permite, además de la capacidad de identificación física de su titular, la capacidad de identificación telemática.

Es un dispositivo con dos interfaces:

- Interfaz con contactos: permite el uso del DNIe mediante un lector de tarjetas inteligentes conectado a un puerto del ordenador.
- Interfaz sin contactos (*contacless*): permite el uso de dispositivos NFC (*Near Field Communications*), lo cuales permiten una comunicación mediante antena y sin contacto con el DNIe.

2.2. Vida Útil

- **Período de validez del DNIe**:
  - 2 años: si el titular < 5 años.
  - 5 años: si el titular ≥ 5 años y < 30 años.
  - 10 años: si el titular ≥ 30 años y < 70 años.
  - Permanente: si el titular ≥ 70 años.
- **Período de validez de los certificados**:
  - Real Decreto 1553/2005: 30 meses.
  - Real Decreto 414/2015 (modifica el RD 1553/2005, regula la expedición del DNI y sus certificados de firma electrónica): con independencia de lo que establece el artículo 6.1 sobre la validez del DNI, la vigencia de los certificados electrónicos reconocidos incorporados al mismo no podrá ser superior a **5 años**.

3. Descripción Física del DNIe

El propósito de la tarjeta soporte del DNIe es contener los datos de filiación del ciudadano, los datos biométricos (modelo dactilar, foto y firma manuscrita) y los dos pares de claves RSA con sus respectivos certificados (autenticación y firma).

La tarjeta física del DNIe sigue el estándar ISO-7816-1. Está fabricada en **policarbonato**, que es un material que permite su uso continuado y frecuente sin sufrir deterioro. La personalización de la tarjeta se realiza mediante la grabación con láser en el cuerpo de la tarjeta de los datos de filiación, fotografía y firma manuscrita.

3.1. Tarjeta DNIe

- Contiene:
  - Certificados X509v3 de ciudadano (autenticación y firma) y claves privadas asociadas, que se generan e insertan durante el proceso de expedición del DNIe.
  - Código CAN (Card Access Number): 6 dígitos usados en la comunicación del DNIe con un dispositivo lector NFC.

  - Antena NFC (Near Field Communication).
  - Otros ...
- NO Contiene: datos sanitarios, fiscales, de tráfico, etc.

3.2. Chip del DNIe

3.2.1. Características

- Chip SLE78CLFX408AP de Infineon Technologies.
- Sistema operativo DNIe v4.0 (versión comercial DNIe 3.0).
- 400KB memoria Flash (código + personalización).
- 8KB memoria RAM.
- Dual Interface (con contactos / sin contactos).
- Criptolibrería RSA.

3.2.2. Contenido del chip

- **Zona Pública**: accesible en lectura sin restricciones:
  - Certificado CA intermedia emisora.
  - Claves Diffie-Hellman.
  - Certificado x509 de componente.
  - Certificado de Autenticación.
  - Certificado de Firma.
- **Zona de Seguridad**: accesible en lectura por el ciudadano en los Puntos de Actualización del DNIe:
  - Datos de filiación del ciudadano contenidos en el soporte físico del DNI.
  - Imagen de la fotografía.
  - Imagen de la firma manuscrita.
  - Resumen criptográfico de la impresión dactilar.
- **Zona Privada**: ¡ojo! aplicable en versiones antiguas de DNIe. Accesible en lectura por el ciudadano, mediante la utilización de la Clave Personal de Acceso o PIN. Contenido:
  - Certificado de Autenticación.
  - Certificado de Firma.

3.2.3. Datos Criptográficos

- Claves RSA pública y privada de autenticación.
- Claves RSA pública y privada de firma.
- Clave pública de root CA.
- Claves Diffie-Hellman.
- Patrón de impresión dactilar.

3.3. Certificados del DNIe

- **Cerificado de Componente**: su propósito es la autenticación de la tarjeta DNIe mediante el protocolo de autenticación mutua definido en CWA 14890 (versión 2013). Permite el establecimiento de un canal cifrado y autenticado entre la tarjeta DNIe y los drivers de un lector de tarjetas.
- **Cerificado de Autenticación**: permite al ciudadano certificar su identidad frente a terceros.
- **Cerificado de Firma**: permite realizar y firmar acciones y asumir compromisos de forma electrónica, pudiéndose comprobar la integridad de los documentos firmados.

4. Tipos de Dispositivos, Sistemas Operativos y Estándares

Al ser el DNIe 3.0 un documento *Dual Interface*, es posible conectarse a la tarjeta de dos formas:

4.1. Mediante Contactos

- Elementos Hardware del PC.
  - Ordenador Personal.
  - Lector de tarjetas inteligentes que cumpla:
    - el estándar ISO-7816.
    - el estándar API PC/SC (Personal Computer/Smart Card).
- Elementos Software del PC.
  - Sistemas Operativos Windows 7 y superiores, GNU/Linux, Unix y Mac.
  - Navegadores Microsoft Internet Explorer, Chrome y Mozilla Firefox.
  - Controladores / Módulos criptográficos:
    - En Windows: drive Minidriver o CardModule y PKCS#11.
    - En Linux/Mac: PKCS#11.

4.2. Mediante Antena sin Contactos NFC

- Elementos Hardware: un dispositivo con NFC que cumpla el estándar ISO 14443 (este puede ser Smartphone, una tableta o un lector NFC).
- Elementos Software: APP que use el DNIe para identificarse y así acceder a un servicio específico o para realizar firmas de documentos.

5. Autoridades de Validación

La Autoridad de Validación es el componente que tiene como tarea suministrar información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación.

La información sobre los certificados electrónicos revocados (no vigentes) se almacena en las denominadas **Listas de Revocación de Certificados (CRL)** .

En la Infraestructura de Clave Pública adoptada para el DNI, se ha optado por asignar las funciones de Autoridad de Validación a entidades diferentes de la Autoridad de Certificación, a fin de aislar la comprobación de la vigencia de un certificado electrónico de los datos de identidad de su titular.

Así, la Autoridad de Certificación (Ministerio del Interior - Dirección General de la Policía) no tiene en modo alguno acceso a los datos de las transacciones que se realicen con los certificados que ella emite y las Autoridades de Validación no tiene acceso a la identidad de los titulares de los certificados electrónico que maneja, reforzando -aún más si cabe- la transparencia del sistema.

Para la validación del DNI se dispone de dos prestadores de Servicios de Validación:

- Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, que prestará sus servicios de validación con carácter universal: ciudadanos, empresas y Administraciones Públicas.
- Ministerio de Hacienda y Administraciones Públicas, que prestará los servicios de validación al conjunto de las Administraciones Públicas.

La prestación de estos servicios de validación se realiza en base a **Online Certificate Status Protocol (OCSP)**, lo que, en esencia, supone que un cliente OCSP envía una petición sobre el estado del certificado a la Autoridad de Validación, la cual, tras consultar su base de datos, ofrece vía http una respuesta sobre el estado del certificado.

6. Seguridad

6.1. Autenticación

La tarjeta DNIe dispone de distintos métodos de autenticación mediante los que una entidad externa demuestra su identidad.

- Autenticación de usuario (PIN). La tarjeta DNIe soporta verificación de usuario *CHV (Card Holder Verification)*. Esta operación se realiza comprobando el código facilitado por la entidad externa. Para la verificación del código PIN se estable un nuevo canal seguro entre el terminal y la tarjeta con objeto de que el código PIN que se transmite quede securizado.
- Autenticación de usuarios mediante datos biométricos. La tarjeta DNIe permite realizar una identificación biométrica del titular, si bien esta función sólo estará disponible en puntos de accesos controlados.
- Autenticación de aplicación.
- Autenticación mutua: permite que cada una de las partes (tarjeta y aplicación externa) confíe en la otra, mediante la presentación mutua de certificados y su verificación. El protocolo utilizado se basa en la especificación *CWA 14890-1 Application Interface for smart cards used as Secured Signature Creation Devices*.

6.2. Funcionalidad criptográfica

- Claves RSA. La tarjeta DNIe es capaz de generar y gestionar claves RSA. La generación de la pareja de claves RSA sigue el estándard PKCS#1 v1.5. Se usa el algoritmo de Miller-Rabin como test de primalidad.
- Hash. La tarjeta DNIe es capaz de realizar hash de datos con el algoritmo SHA-256. Después de finalizar cualquier operación de hash, el código resultante se almacena en la memoria de la tarjeta donde permanece hasta la siguiente operación.
- Firmas electrónicas. La tarjeta DNIe tiene capacidad para la realización de firmas electrónicas de dos modos diferentes: modo raw y modo relleno PKCS#1.

7. Ciclo de Vida de los Certificados

7.1. Generación de los Certificados

La DGP (Dirección General de la Policía) actúa como AC (Autoridad de Certificación) de los certificados contenidos en el DNIe, los cuales son generados en el momento de su expedición [3].

7.1.1. Tamaño de las Claves

- El tamaño de las claves de la AC Raíz es de 4096 bits.
- El tamaño de las claves de las AC Subordinadas es de 2048 bits.
- El tamaño de las claves de los certificados DNI y de firma centralizada es de 2048 bits.

7.2. Revocación de los Certificados [3]

Los certificados de identidad pública y firma electrónica, así como los certificados de firma centralizada pueden ser revocados por:

- Renuncia del ciudadano al sistema, excepto respecto del certificado de identidad.
- Sustracción, extravío, destrucción o deterioro del DNI soporte del certificado.
- Tras la renovación por variación de datos.
- Compromiso de las claves privadas del ciudadano.
- Compromiso de la clave privada de la Autoridad de Certificación de la Dirección General de la Policía emisora del certificado de ciudadano.
- Declaración de que el ciudadano no tiene capacidad de firma (pródigo).
- Otros ...

8. Preguntas de Exámenes

1. (2016.01). **El chip del DNI 3.0 en su zona de seguridad (accesible por el ciudadano en los puntos de actualización DNIe) contiene:**

   a) Certificado CA intermedia emisora.

   b) Datos de filiación del ciudadano.

   c) Claves Diffie-Hellman.

   d) Certificado x509 de componente.

2. (2016.03). **El lector NFC y el DNI 3.0 negocian y establecen un canal seguro de comunicación usando el código CAN (Card Access Number), éste es un código:**

   a) numérico de 9 dígitos que debe conocer sólo el ciudadano.

   b) de 6 dígitos y de un solo uso, es decir, sólo es válido para una única sesión de trabajo, terminada esta habría que solicitar otro.

   c) de 6 dígitos que aparce en el anverso del documento físico del DNI 3.0.

   d) accesible en la zona privada del del DNI 3.0 mediante la utilización de la clave personal de acceso o PIN.

3. (2016.04). **Según la Ley 59/2003 de firma electrónica, indique cuál es el tipo de firma electrónica que: "tendrá respecto de los datos consignados de forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel".**

   a) Firma electrónica avanzada.

   b) Firma electrónica intermedia.

   c) Firma electrónica reconocida.

   d) Firma electrónica final.

4. (2016.05). **Según se establece en el Real Decreto 414/2015 con independencia de lo que establece el artículo 6.1 sobre la validez del DNI, la vigencia de los certificados electrónicos reconocidos incorporados al mismo NO podrá ser superior a:**

   a) 2 años.

   b) 3 años.

   c) 4 años.

   d) 5 años.

5. (2016.07). **En los entornos UNIX / Linux o MAC podemos utilizar el DNI 3.0 a través de un módulo criptográfico denominado:**

   a) PCKS#11.

   b) PKCS#10.

   c) PKCS#11.

   d) PSCK#12.

6. (2015.05). **¿Qué datos NO contiene el chip del nuevo DNIe 3.0?**

   a) Filiación.

   b) Firma digitalizada.

   c) Fiscal.

   d) Resumen criptográfico de la impresión dactilar.

7. (2015.20). **¿Qué permiten los certificados X.509 v3 de ciudadano del DNIe 3.0?**

   a) Firma y cifado.

   b) Autenticación y cifado.

   c) Autenticación y firma.

   d) Identificación y autenticación.

8. (2014.01). **¿En que zona del chip del DNI electrónico se encuentra el certificado x509 de componente?**

   a) Zona de seguridad.

   b) Zona autónoma.

   c) Zona privada.

   d) Zona pública.

9. (2014.05). **La prestación de servicios de validación del DNI electrónico se realiza en base a:**

   a) Online Certificate Status Protocol (OCSP).

   b) Online Services Protocol (OSP).

   c) Services Status Protocol (SSP).

   d) Online Status Services Certificate (OSSC).

10. (2013.04). **¿Qué certificados electrónicos incluye el chip de la tarjeta del DNI electrónico?**

    a) De autenticación y de firma.

b) De componente, de autenticación y de firma.

c) De cifrado y de firma.

d) De cifrado, de autenticación y de firma.

11. (2013.07). **¿De qué material está hecha la tarjeta física del DNI electrónico?**

a) Policloruro de vinilo.

b) Policarbonato.

c) Polietileno de alta densidad.

d) Fibra de vidrio.

12. (PI.2011.04, LI.2011.19). **El DNI electrónico es una tarjeta que cumple con la normativa Europea CWA-14890-1:2004, concretamente esta normativa define:**

a) El formato en el que se almacena el certificado reconocido de autenticación y firma.

b) Los ficheros que se generan al realizarse la firma electrónica.

c) Cómo realizar la comunicación entre una aplicación y un dispositivo seguro de creación de firma.

d) La normativa de accesibilidad para la firma electrónica para personas con capacidad reducida.

13. (PI.2011.08, LI.2011.04). **Los certificados de identidad pública contenidos en el DNI electrónico pueden ser revocados por:**

a) Compromiso de la clave pública de la Autoridad de Certificación de la Dirección General de la Policía.

b) Declaración de que el ciudadano no tiene capacidad de firma (pródigo).

c) Tras la renovación en todos los casos.

d) Compromiso de la clave pública del ciudadano.

14. (2010.03). **Elija la afirmación correcta, en relación con el contenido de la tarjeta chip del DNI electrónico:**

a) Se incluye un certificado electrónico único, personal e intransferible, con la doble funcionalidad de firma electrónica y de autenticación.

b) Se incluyen, entre otros, los datos de filiación del ciudadano (los mismos que están impresos en el soporte físico del DNI), junto con una imagen de la fotografía.

c) Los datos contenidos, en todo caso, sólo son accesibles por el ciudadano, mediante la utilización de la Clave Personal de Acceso o PIN, como garantía de confidencialidad.

d) No se incluye una imagen de la fotografía.

15. (2010.06). **La tarjeta DNIe tiene capacidad para la realización de firmas electrónicas en:**

    a) Modo raw y modo relleno PKCS#1.

    b) Únicamente en modo raw.

    c) Únicamente en modo relleno PKCS#11.

    d) Modo raw y en modo relleno PKCS#11.

16. (2008.01). **Señale cuál de las siguientes afirmaciones es FALSA respecto al DNI electrónico:**

    a) En el DNI electrónico se pueden almacenar otros certificados emitidos por otras entidades.

    b) El DNI electrónico contiene información biométrica del titular.

    c) La tarjeta DNI es capaz de generar y gestionar claves RSA.

    d) La tarjeta DNI es capaz de realizar hash de datos con el algoritmo SHA1.

17. (2008.10). **Señale qué contenido de los siguientes NO está almacenado en el CHIP del DNI electrónico:**

    a) El domicilio del titular.

    b) Datos de filiación del titular.

    c) Imagen digitalizada de la fotografía.

    d) Un certificado electrónico para autenticación y otro para firma.

18. (LI.2014.10). **Según se establece en la política de certificación de la DGP para el DNI electrónico (DNIe) en lo relativo a las autoridades de certificación (AC) raíz y subordinadas, ¿cuál es el tamaño de esas claves?:**

    a) El tamaño de las claves de la AC Raíz es de 2048 bits y el de las claves de las AC subordinadas será de 4096 bits.

    b) Las claves de la AC Raíz y de las AC subordinadas serán de 2048 bits.

    c) El tamaño de las claves es: 4096 para la AC Raíz y 2048 para las AC Subordinadas.

    d) El tamaño de las claves de la AC Raíz es 8192 bits para la raíz y 4096 para las AC subordinadas.

19. (LI.2013.09). **El uso conjunto de los certificados ubicados en el DNI electrónico proporcionan las siguientes garantías:**

    a) Disponibilidad, autenticidad de origen, confidencialidad y no repudio de origen.

    b) Disponibilidad, integridad, autenticidad de origen.

c) Integridad, autenticidad de origen y no repudio de origen.

d) Integridad, confidencialidad, autenticidad de origen y no repudio de destino.

20. (LI.2008.07). **Los Certificados de Identidad Pública, emitidos por la Dirección General de la Policía tendrán como finalidad:**

a) Garantizar electrónicamente la identidad del ciudadano y permitir la firma electrónica avanzada de documentos, pero no la firma electrónica reconocida de documentos.

b) Garantizar electrónicamente la identidad del ciudadano y permitir la firma electrónica reconocida de documentos.

c) Permitir el desplazamiento por la Unión Europea de los menores de edad.

d) Permitir a los ciudadanos tener un certificado electrónico de autenticación, pero no de firma electrónica.

21. (TAI.PI.2008.01). **Señale la afirmación correcta. Una persona física:**

a) Puede tener varios certificados de persona física expedidos por la Fábrica Nacional de Moneda y Timbre.

b) Puede tener varios certificados que corresponden a entidades de certificación distintas.

c) Si tiene DNI electrónico, no puede tener certificado de la Fábrica Nacional de Moneda y Timbre.

d) Si tiene el DNI electrónico obligatoriamente tendrá los certificados electrónicos de autenticación y firma electrónica.

22. (TAI.PI.2008.02). **Señale la respuesta correcta. ¿Con qué clave se genera la clave de sesión y cifrado de un canal privado y autenticado entre un ciudadano que utiliza el DNI electrónico en su relación con un organismo público?:**

a) Con la clave pública del DNI electrónico.

b) Con la clave privada del Organismo Público.

c) Con la clave privada del DNI electrónico.

d) Con la clave pública del Organismo Público.

23. (TAI.LI.2008.11). **De entre las siguientes opciones, ¿cuál no es posible realizar con el DNI electrónico?:**

a) Identificar electrónicamente a su titular.

b) Firmar electrónicamente trámites administrativos.

c) Integrar en la tarjeta el certificado X509 de autenticación y firma de su titular.

d) Garantizar la integridad durante su transmisión de los documentos firmados por medio del mismo.

24. (TAI.PI.2014.02). **En lo referente a los certificados de identidad pública contenidos en el Documento Nacional de Identidad (DNIe), señale la sentencia FALSA:**

    a) Son emitidos como certificados reconocidos.

    b) Vinculan una serie de datos personales del ciudadano a unas determinadas claves.

    c) Garantizan la autenticidad, integridad y no repudio.

    d) Pueden ser renovados por declaración de que el ciudadano no tiene capacidad de firma (pródigo).

25. (TAI.PI.2014.03). **Según el Real Decreto 869/2013, que modifica el RD 1553/2005, ¿cuál de los siguientes periodos de validez del DNI electrónico es correcto?:**

    a) Diez años, cuando el titular haya cumplido los treinta y no haya alcanzado los sesenta.

    b) Permanente cuando el titular haya cumplido los sesenta años.

    c) Dos años cuando el solicitante no haya cumplido los cinco años de edad.

    d) Diez años, cuando el titular no haya cumplido los treinta al momento de la expedición o renovación.

26. (TAI.PI.2014.04). **¿Cuál de las siguientes claves NO está contemplada entre los datos criptográficos que almacena el DNI electrónico?:**

    a) Clave RSA privada de autenticación (Digital Signature).

    b) Clave RSA pública de autenticación (Digital Signature).

    c) Clave RSA privada de no repudio (ContentCommitment).

    d) Clave RSA privada de firma (ContentCommitment).

27. (TAI.LI.2016.15). **Con carácter general, el Documento Nacional de Identidad, tendrá un periodo de validez de:**

    a) 3 años cuando el solicitante no haya cumplido los 5 años de edad.

    b) 5 años cuando el titular no haya cumplido los 5 años de edad y no haya alcanzado los 25 al momento de la expedición o renovación.

    c) 10 años cuando el titular haya cumplido los 25 y no haya alcanzado la edad de validez permanente del DNI.

    d) Permanente cuando el titular haya alcanzado los 70 años.

28. (TAI.LI.2016.17, TAI.PI.2016.02). **Según el RD 414/2015, por el que se modifica el RD 1553/2005, por el que se regula la expedición del DNI y sus certificados de firma electrónica, en relación con la vigencia de los certificados electrónicos reconocidos, incorporados al DNI electrónico:**

a) Es de 30 meses.

b) No podrá ser superior a 4 años.

c) No podrá ser superior a 5 años.

d) Es de 2 años.

29. (SSTI.LI.2007.52, SSTI.LI.2013.74). **¿Cuál de las siguientes normas regula la expedición del DNI y sus certificados de firma electrónica? :**

a) RD 153/2005, de 14 de enero.

b) RD 1553/2005, de 23 de diciembre.

c) RD 1555/2003, de 29 de mayo.

d) RD 155/2003, de 15 de septiembre.

30. (SSTI.LI.2007.72). **¿Qué tipos de certificado están incluidos en el DNIe?:**

a) Autenticación y firma.

b) Cifrado y firma.

c) Firma.

d) Cifrado, firma y autenticación.

31. (SSTI.LI.2007.82). **¿En cuál de las siguientes zonas del chip del DNIe se almacenan los datos biométricos?:**

a) Zona pública.

b) Zona privada.

c) Zona de seguridad.

d) Zona compartida.

32. (SSTI.LI.2011.68). **Los certificados incorporados al DNI-e:**

a) Son dos: de autenticación y de firma del ciudadano.

b) Los usuarios finales pueden validarlos en la Dirección General de la Policía, que está constituida como Autoridad de Validación.

c) Están basados en la recomendación X.509 v.3 sin extensión alguna.

d) Están integrados en un chip certificado en el nivel de seguridad EAL4+ definido en la norma ISO/IEC 15408.

33. (SSTI.LI.2014.91). **Indique la respuesta FALSA respecto a las autoridades de validación del DNI electrónico:**

a) La prestación de estos servicios de validación se realiza en base a Online Certificate Status Protocol (OCSP).

b) Para la validación del DNI electrónico se dispone de dos prestadores de Servicios de Validación.

c) La información sobre los certificados electrónicos revocados se almacena en las denominadas listas de revocación de certificados (CRL).

d) En la Infraestructura de Clave Pública adoptada para el DNI electrónico, se ha optado por asignar a una misma entidad las funciones de Autoridad de Validación y Certificación.

34. (SSTI.LI.2015.51). **¿Cuál de las siguientes características del DNI electrónico es exclusiva del DNIe 3.0?:**

a) Cumple la norma ISO 7816 para tarjetas inteligentes..

b) Emplea la tecnología inalámbrica NFC.

c) Contiene certificados de componente, autenticación y firma.

d) Sus certificados cumplen la norma X509 v3.

35. (SSTI.LI.2016.70). **¿A través de qué tecnología de conexión puede usarse el DNIe 3.0 en una aplicación de un teléfono móvil?:**

a) Bluetooth.

b) NFC.

c) Wi-Fi.

d) El DNIe 3.0 sólo puede usarse desde un teléfono móvil usando un lector de tarjetas.

36. (BAQUEDANO.384). **La duración de la validez del DNI electrónico cuando el titular haya cumplido los setenta años es:**

a) por un período de 5 años.

b) por un período de 10 años.

c) permanente.

d) por un período de 3 años.

37. (BAQUEDANO.385). **Las características del chip del DNI electrónico incluyen:**

a) Sistema operativo DNIe v1.1 y capacidad de 32K.

b) Sistema Operativo micro-Android y capacidad de 1M.

c) chip SD32 con capacidad de 3K.

d) chip homologado con capacidad de 32T.

38. (BAQUEDANO.386). **La información en el chip del DNI electrónico está distribuida en tres zonas: pública, privada y de seguridad. Concretamente la zona pública contiene:**

a) Certificado de penales.

b) datos de filiación del ciudadano, imagen de la fotografía e imagen de la firma manuscrita.

c) certificado público del funcionario emisor del certificado.

d) certificado CA intermedia emisora.

39. (BAQUEDANO.387). **El certificado de Componente incluido en el chip del DNI electrónico tiene como propósito:**

a) la firma de documentos indexados.

b) garantizar electrónicamente la seguridad del ciudadano al realizar una transacción telemática.

c) la autenticación de la tarjeta del DNI electrónico mediante el protocolo de autenticación mutua.

d) identificación de un registro que permita expedición de certificados reconocidos por parte de entidades privadas.

40. (BAQUEDANO.388). **Un lector compatible con el DNI electrónico deberá soportar los siguientes estándares:**

a) API PC/SC (Personal Computer/Smart Card), CSP (Cryptographic Service Provider, Microsoft) y API PKCS#11.

b) API-II y SPS (Security Personal Software).

c) EAPI Simetric Encryption (DES, 3DES, IDEA, etc) y Microsoft Card Software.

d) X509 EncodedKeySpec Class y API Software.

41. (BAQUEDANO.389). **Para poder interaccionar adecuadamente con las tarjetas criptográficas en general y con el DNI electrónico en particular, el equipo ha de tener instalados:**

a) un módulo encriptado.

b) un servicio que se denomina "Cryptographic Service Provider" (CSP) o el servicio PKCS#11.

c) el driver del modelo de CHIP utilizado.

d) un módulo criptográfico que dependerá del sistema operativo del equipo y el driver correspondiente al modelo de lector.

9. Soluciones

1. B
2. C
3. C
4. D
5. C
6. C
7. C
8. D
9. A
10. B
11. B
12. C
13. B
14. B
15. A
16. A
17. Anulada
18. C
19. C
20. B
21. B
22. D
23. Anulada
24. D
25. C
26. C
27. D
28. C
29. B
30. A
31. C
32. D
33. D
34. B
35. B
36. C
37. A
38. D
39. C
40. A
41. D

Referencias

[1] https://www.dnielectronico.es/PDFs/Guia_de_referencia_basica_v1_5.pdf

[2] https://www.dnielectronico.es/PDFs/Guia_de_Referencia_DNIe_con_NFC.pdf

[3] https://www.dnielectronico.es/PDFs/Politicas_de_Certificacion_v2.1.pdf

[4] **RD 1553/2005. Regula el DNI y sus Certificados de Firma electrónica**. http://www.boe.es/boe/dias/2005/12/24/pdfs/A42090-42093.pdf

[5] **RD 1586/2009**: Modifica RD 1553/2005. http://www.boe.es/boe/dias/2009/11/03/pdfs/BOE-A-2009-17429.pdf

[6] **RD 869/2013**: Modifica RD 1553/2005. http://www.boe.es/boe/dias/2013/11/23/pdfs/BOE-A-2013-12320.pdf

[7] **RD 414/2015**: Modifica RD 1553/2005. http://www.boe.es/boe/dias/2015/05/30/pdfs/BOE-A-2015-5953.pdf