Test Tema 81 #1

Actualizado el 13/04/2025

1. En relación a la afirmación de que la única empresa u organismo en España que proporciona certificados digitales es la FNMT (Fábrica Nacional de Moneda y Timbre) indique la alternativa correcta:

a) Es completamente falso.

b) Es completamente cierto.

c) Es cierto para certificados servidor.

d) Es cierto sólo para certificados de empleado público, sede electrónica y sello electrónico.

2. 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.

3. En relación con los prestadores de servicios electrónicos de confianza, señale la opción CORRECTA:

a) Sólo si son cualificados, notificarán al órgano supervisor cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado.

b) Registrarán la revocación de certificados en su base de datos y, en caso de ser cualificados, publicarán el estado de revocación en un plazo máximo de 48 horas.

c) No serán responsables por daños y perjuicios, en caso de negligencia por parte del titular del certificado en la conservación de sus datos de creación de firma, sello o autenticación de sitio web, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de estos o, en su caso, de los medios que den acceso a ellos.

d) El tiempo máximo de vigencia de un certificado cualificado son 4 años.

4. Con respecto a la seguridad en dispositivos y en el backend, indica cuál es la afirmación correcta

a) Tanto Oauth como OpenID Connect son soluciones para autenticación

b) Tanto Oauth como OpenID Connect son soluciones para autorización

c) Oauth es una solución para autenticación y OpenID Connect es una solución para autorización

d) Oauth es una solución para autorización y OpenID Connect es una solución para autenticación

5. La información contenida en el chip del DNI electrónico está contenida en tres zonas con diferentes niveles de acceso. Indique qué información está contenida en la Zona de seguridad:

a) Certificado de autenticación.

b) Datos de filiación del ciudadano.

c) Claves Diffie-Hellman.

d) Certificados X.509 de componente.

6. ¿De las siguientes APIs cual NO es un API de desarrollo de tarjetas inteligentes?

a) CryptoAPI

b) PKCS#7

c) PKCS#11

d) JCE/JCA

7. Señale cuál de las siguientes medidas de seguridad del DNI electrónico es falsa:

a) Tintas visibles con luz ultravioleta para evitar su falsificación

b) Chip RFID

c) Encriptación de los datos del chip

d) Acceso a la funcionalidad del DNI electrónico mediante clave personal de acceso (PIN)

8. Según la recomendación X.509 v3, las Listas de certificados revocados (CRL):

a) Permiten conocer el estado de un certificado en el instante de la consulta.

b) Para cada certificado revocado indican, entre otros, el nombre del titular del certificado y la correspondiente clave pública.

c) Pueden contener certificados revocados por diversas Autoridades de Certificación.

d) Las delta CRL son los subconjuntos en los que se divide una CRL y que instaladas en máquinas distintas facilitan su tratamiento.

9. Indique la afirmación correcta que aplica al DNI electrónico:

a) La PKI adoptada para el DNI electrónico asigna las funciones de Autoridad de Validación a las entidades Autoridad de Certificación, con objeto de tener conocimiento de la vigencia o caducidad de certificados de un determinado titular.

b) La clave personal de acceso (PIN) podrá contener signos de puntuación.

c) Todos los certificados emitidos por DNIe contienen la extensión 'Key Usage' con al menos los siguientes usos "contentCommitment", "Digital Signature" y "dataEncipherment".

d) El tamaño de las claves de los certificados de autenticación y firma contenidos en el DNIe, es de 4096 bits.

10. ¿Cuál de las siguientes no es un servicio ofrecido por el DNI electrónico?

a) Firma electrónica de documentos

b) Identificación en medios telemáticos

c) Acreditar la identidad física

d) Tarjeta sanitaria electrónica

11. Servicios de una Autoridad de Certificación esenciales son:

a) Generación y gestión de claves criptográficas

b) Servicios de directorio

c) Registro de usuarios mediante el que se acredita la identidad

d) Todas las respuestas anteriores son correctas

12. Guillermo es un PSG al que el Servicio Gallego de Salud ha contratado temporalmente. Para firmar el contrato generado por la dirección de RRHH del área sanitaria contratante en formato electrónico (PDF), usará su DNIe. Según esto, seleccione la respuesta correcta:

a) Guillermo firmará el contrato usando la clave pública del certificado de firma de su DNIe, generando una firma en formato XAdES.

b) Guillermo firmará el contrato usando la clave pública del certificado de autenticación de su DNIe, generando una firma en formato PAdES.

c) Guillermo firmará el contrato usando la clave privada de su DNIe, generando una firma en formato XCAdES.

d) Guillermo firmará el contrato usando la clave privada de su DNIe, generando una firma en formato PAdES.

13. Los certificados electrónicos contenidos en el DNI electrónico 3.0 tienen una vigencia de:

a) 30 meses.

b) 48 meses.

c) 60 meses.

d) 36 meses.

14. Indique la ventaja de los sistemas RFID (Radio Frecuency Identification) de baja frecuencia:

a) Soportan la lectura simultánea de varias etiquetas

b) El coste de las etiquetas es bajo debido al pequeño tamaño de su antena

c) Poseen alta tasas de transmisión

d) Su señal atraviesa materiales tales como el agua, la madera y el aluminio

15. ¿Cómo se conecta el DNI electrónico al ordenador personal del ciudadano?

a) Es necesario un lector de tarjetas específico diseñado por la Dirección General de la Policía, que se puede obtener en las comisarías

b) A través de un lector de tarjetas que cumpla el standard ISO-7816

c) Con un lector de tarjetas específico diseñado por la Dirección General de la Policía, que se puede obtener en establecimientos comerciales

d) No es posible conectarlo a ordenadores personales, sólo los especialmente habilitados para ello por la Dirección General de la Policía

16. Señalar cuál de los siguientes NO es un componente de una infraestructura de clave pública (PKI):

a) Autoridad de certificación.

b) Autoridad de gestión y control.

c) Autoridad de validación.

d) Autoridad de registro.

17. Respecto a la validez de los certificados del DNI electrónico, señale la falsa:

a) La pérdida de validez del DNI implica su pérdida de validez

b) La renovación implica la expedición de nuevos certificados

c) La expedición de duplicados implica la expedición de nuevos certificados

d) La caducidad de los certificados implica la renovación del DNI

18. PKCS#10 define:

a) Un formato portable para almacenar o transportar las claves privadas de un usuario

b) Sintaxis para las peticiones de certificados

c) El formato del sobre digital

d) La especificación de un interfaz de acceso a dispositivos que almacenan información

19. ¿Cuál es el estándar de la tarjeta física del DNI electrónico?

a) ISO-7816-1

b) PCKS#11

c) ISO-17789

d) ISO-7815-1

20. De entre los siguientes, ¿cuál no es uno de los servicios de certificación ofrecidos actualmente por la Fábrica Nacional de Moneda y Timbre?

a) Fechado digital.

b) Validación on-line de certificados.

c) Voto electrónico en Juntas Generales de Sociedades.

d) Login único en sistemas Windows, Linux y Unix.

21. ¿Está vigente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos?

a) Sí

b) Solo parcialmente

c) No

d) Sí, hasta el día 2 de abril de 2021

22. Si para un sistema de acceso basado en control biométrico, FAR = 0% y FRR=12%, puede afirmarse que...

a) Ningún acceso no autorizado ha sido denegado y un 12% de los accesos autorizados han sido denegados.

b) Ningún acceso no autorizado ha sido permitido y un 12% de los accesos autorizados han sido denegados.

c) Ningún acceso no autorizado ha sido permitido y un 88% de los accesos autorizados han sido denegados.

d) Ningún acceso no autorizado ha sido denegado y un 12% de los accesos autorizados han sido permitidos.

23. ¿Qué tipos de certificado están incluidos en el DNIe asociados a su titular?

a) Autenticación y firma.

b) Cifrado y firma.

c) Firma.

d) Cifrado, firma y autenticación.

24. ¿En qué 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.

25. ¿Qué versión del PKCS define una interfaz para el acceso a dispositivos que contienen información criptográfica como Tokens o Tarjetas?

a) PKCS 1

b) PKCS 7

c) PCKCS 9

d) PKCS 11

26. Dada una tarjeta con microprocesador utilizada en un sistema de control de acceso, ¿cuál de las siguientes afirmaciones es falsa?

a) Dispone de un sistema operativo con un juego de instrucciones grabado en memoria ROM

b) Permite realizar algoritmos complejos de cifrado con clave asimétrica

c) La lectura de su información se realiza mediante un diodo de láser

d) Incorpora un microprocesador con memoria

27. Los tipos de tarjetas inteligentes son:

a) de acoplamiento

b) de vecindad

c) de proximidad

d) todas las anteriores

28. Los certificados electrónicos reconocidos incorporados al DNI electrónico tendrán un período de vigencia de:

a) 24 meses.

b) 30 meses.

c) 5 años.

d) El período de validez del documento nacional de identidad.

29. ¿Cuál de estas opciones NO es una entidad certificadora?

a) GeoTrust

b) Ceres

c) WorldTrusted

d) Thawte

30. En una PKI:

a) Un certificado se añade a una CRL en cuanto se tiene conocimiento de que hay motivos para su revocación.

b) Las CRLs incluyen todos los certificados emitidos por una CA.

c) Un certificado revocado es eliminado de una CRL en cuanto se emite un nuevo certificado de las mismas características para el titular del certificado revocado.

d) No es obligatorio que una CA emita CRLs si proporciona otro mecanismo de consulta del estado de los certificados.

31. El protocolo OCSP, se utiliza en…

a) la validación en tiempo real del certificado digital

b) comprobación de la validez de una trama

c) la comunicación entre sistemas abiertos

d) la validación de la dirección de origen de un equipo

32. Indique qué información NO se encuentra almacenada en la Zona de Seguridad del DNI-e 3.0:

a) Datos de filiación del ciudadano.

b) Imagen de la fotografía.

c) Imagen de la firma manuscrita.

d) Claves Diffie-Hellman.

33. Respecto al protocolo OCSP, es FALSO que:

a) Los mensajes OCSP son codificados en ASN.1.

b) Está definido en el RFC 2560.

c) Tanto la petición como la respuesta deben ir firmadas.

d) Puede usar SMTP como mecanismo de transporte.

34. Una de las zonas de datos que se encuentran dentro del chip criptográfico del DNI electrónico es la denominada zona de seguridad. Esta zona que almacena, entre otros, los datos biométricos, es accesible por:

a) El ciudadano

b) El ciudadano y la Dirección General de la Policía

c) La Dirección General de la Policía

d) Es una zona pública

35. Los certificados incluidos en el DNI electrónico tienen una validez máxima de

a) 30 meses.

b) La vigencia de los certificados electrónicos reconocidos incorporados al mismo no podrá ser superior a cinco años

c) 36 meses

d) 48 meses

36. Señale cuál de los siguientes datos no se almacena en la zona privada del chip criptográfico del DNI electrónico:

a) Claves privadas del ciudadano

b) Certificado de autenticación

c) Claves públicas del ciudadano

d) Certificado de firma

37. El elemento del DNI que no permite por si solo autenticar a una persona es:

a) El nombre

b) La foto

c) La firma

d) La huella dactilar

38. Respecto a las tarjetas de identificación con circuitos integrados, la norma ISO/IEC 7816-4:2020 NO especifica:

a) Las dimensiones y tolerancias de la tarjeta de identificación.

b) Métodos de acceso a los ficheros e información.

c) Métodos para la securización de los mensajes.

d) Métodos para la recuperación de información.

39. Dentro del chip criptográfico del DNI electrónico podemos encontrar tres zonas de datos diferenciadas. Señale cuál de las siguientes no es una de ellas:

a) Zona pública

b) Zona de seguridad

c) Zona privada

d) Zona confidencial

40. ¿Cuál de los siguientes no es un sistema operativo para tarjetas inteligentes?

a) Scfw

b) MultOs

c) Java Card

d) Open Card

41. El DNIe 4.0 fue elaborado para cumplir con la siguiente normativa europea:

a) Reglamento (UE) 2019/1571

b) Reglamento (UE) 2020/1157

c) Reglamento (UE) 2019/1157

d) Reglamento (UE) 2020/1571

42. Cuando se dispone de una tarjeta criptográfica para almacenar la clave privada, ¿Cuál es el procedimiento más usual para firmar un documento?

a) Se transfiere a la tarjeta un "hash" del documento a firmar y esta devuelve la firma.

b) Se transfiere a la tarjeta el documento a firmar y esta devuelve la firma.

c) El explorador de Internet calcula un "hash" del documento a firmar, obtiene la clave privada de la tarjeta y cifra el "hash" con ella.

d) El explorador de Internet obtiene la clave privada de la tarjeta, y firma el documento directamente.

43. Según la recomendación X.509 v3, las Listas de certificados revocados (CRL):

a) Permiten conocer el estado de un certificado en el instante de la consulta.

b) Para cada certificado revocado indican, entre otros, el nombre del titular del certificado y la correspondiente clave pública.

c) Deben ser expedidas por las mismas Autoridades que emiten los certificados revocados.

d) Pueden contener sólo certificados revocados desde la expedición de una CRL básica, en cuyo caso se denominan delta CRL.

44. La firma realizada a través del DNI electrónico:

a) Tiene valor jurídico, pero no equivale a la firma manuscrita

b) Tiene el mismo valor jurídico que la firma manuscrita

c) No tiene valor jurídico

d) Su valor jurídico queda a discreción de un juez

45. ¿A través de qué tecnología de conexión puede usarse el DNIe 3.0 en una aplicación de un teléfono móvil?:

a) Bluetooth.

b) Wi-Fi.

c) NFC.

d) Sólo puede usarse desde un teléfono móvil usando un lector de tarjetas.

46. PKCS#7 se centra en:

a) El formato del sobre digital

b) La especificación de un interfaz de acceso a dispositivos que almacenan información

c) Especificar un formato portable para almacenar o transportar las claves privadas de un usuario

d) Todas las respuestas anteriores son correctas

47. Una Autoridad de Validación (VA) puede realizar distintos tipos de servicios de validación:

a) Descarga de CRLs

b) Vía OCSP

c) A y B son correctas

d) A y B son incorrectas

48. Señale la opción verdadera en relación a las infraestructuras de clave pública…

a) Se ha de garantizar que ningún usuario, salvo aquel para quien se ha generado una pareja de claves de un certificado, pueda jamás llegar a disponer de ellas.

b) La utilización de hardware criptográfico (HSM) tiene sentido en las Autoridades de Certificación (CA) pero no así en las Autoridades de Registro (RA).

c) Es importante que la CA disponga de certificación FIPS 140-2.

d) EMV es un tipo de certificado que no responde al estándar X.509.

49. La Tercera Parte de Confianza (TPC) de un entorno de clave pública, que se encarga de legitimar la relación de una clave pública con la identidad de un usuario o servicio es:

a) Autoridad de Certificación (AC).

b) Autoridad de Validación (AV).

c) Autoridad de Registro (AR).

d) Autoridad de Revocación (AR).

50. Denominamos al conjunto de elementos software y hardware, procedimientos, políticas y personal; cuyo objetivo es crear, almacenar, distribuir y revocar certificados digitales de clave pública, como:

a) Autoridad de certificación (CA)

b) Autoridad de registro (RA)

c) Plataforma de servicios firma

d) Infraestructura de clave pública (PKI)

51. ¿Cuál de los siguientes no es un método de actualización de CRLs?

a) muestreo de CRLs

b) envío de CRL

c) anuncio de CRL

d) verificación en línea

52. La solicitud de certificación de una clave pública remitida a la autoridad de certificación correspondiente deberá ser generada en formato:

a) PKCS#10

b) PKCS#12

c) X.500

d) X.509

53. 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 en lectura 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.

54. En las tarjetas inteligentes sin contacto, la comunicación se realiza mediante tecnología de radio frecuencia, incorporando las tarjetas una antena de RF. En función de la distancia que permita la comunicación, ¿qué descripción corresponde a las tarjetas?

a) Requiere el contacto físico (<2mm) con el dispositivo de interfaz, aunque no su inserción, ni usa contactos eléctricos

b) Permite una distancia de 10 cm con el dispositivo de interfaz

c) No permite una distancia mayor de 5 cm con dispositivo de interfaz

d) Todas las tarjetas inteligentes sin contacto son de proximidad

55. Los certificados de identidad pública que están 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.

56. La Autoridad de Certificación de los certificados emitidos para el DNI electrónico es:

a) La Fábrica Nacional de Moneda y Timbre

b) El Ministerio de Hacienda y Función Pública

c) El CCN (Centro Criptológico Nacional)

d) El Ministerio del Interior - Dirección General de la Policía

57. ¿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.

58. PKCS#12:

a) Especifica un formato portable para almacenar o transportar las claves privadas de un usuario

b) Especifica una API, por la que los dispositivos que contienen información criptográfica realizan funciones criptográficas

c) El formato del sobre digital

d) La especificación de un interfaz de acceso a dispositivos que almacenan información

59. Si usamos el método de comprobación de la validez de un certificado mediante CRL en vez de OCSP puede ocurrir que (marcar la correcta respecto a CRL que no ocurriría usando OCSP)…

a) El certificado que estamos validando esté malformado

b) La autoridad de certificación que emitió el certificado sea incorrecta

c) El certificado haya sido revocado desde la anterior emisión de CRL pero la consulta lo dé por válido

d) El certificado haya expirado pero no se pueda verificar la fecha de fin de validez y la comprobación lo dé por válido cuando está expirado

60. Señale cuál de las siguientes afirmaciones sobre el DNI electrónico es CORRECTA:

a) Los certificados para los ciudadanos están firmados con SHA256, utilizan claves RSA 2048 y tienen una caducidad de 60 meses.

b) La validación del DNI electrónico se realiza en base a CRLs mediante dos prestadores de servicios de validación: "AV DNIE GOB" y "AV DNIE AEAT".

c) Las Autoridades de Certificación que componen la PKI del DNIe son "AC DGP" y "AC Oficina".

d) -

61. El DNIe 3.0:

a) Permite la lectura sin PIN del certificado de firma.

b) Incorpora tecnología de lectura sin contacto.

c) Reduce la vigencia de los certificados de identificación y firma a 5 años.

d) Todas las anteriores.

62. Respecto a los certificados X.509 y las PKI, indique la respuesta correcta:

a) Exigen el uso de X.500 o LDAP para la distribución de certificados y CRLs.

b) Cuando el estado de revocación se proporciona mediante CRLs, la Autoridad de Certificación es también la emisora de las CRLs.

c) La emisión de CRLs es un mecanismo obligatorio de consulta de estado de los certificados.

d) Una CRL completa lista todos los certificados no expirados dentro su alcance revocados por los motivos de revocación dentro del alcance de la CRL.

63. Revocar un certificado electrónico significa:

a) Extender su validez más allá del tiempo límite inicialmente establecido

b) Anular su validez antes de la fecha de caducidad que consta en el mismo

c) Agotar su vida útil al haberse llegado al límite de vigencia del mismo

d) Desacoplar un certificado de la tarjeta criptográfica en la que reside

64. La información en el chip del DNI está distribuida en tres zonas, con diferentes niveles y condiciones de acceso. ¿Cuál no es una de ellas?

a) Zona privada

b) Zona de control

c) Zona de seguridad

d) Zona pública

65. En una infraestructura de clave pública PKI, indique cuál es el papel principal de la entidad de confianza denominada "Autoridad de Registro":

a) Se encarga de identificar de forma inequívoca al solicitante de un certificado a fin de que la Autoridad de Certificación emita el correspondiente certificado

b) Se encarga de publicar las listas de certificados revocados

c) Se encarga de registrar las peticiones de sellado de tiempo

d) Se encarga de comprobar la validez de un certificado digital ya emitido

66. Los algoritmos de autenticación y firma utilizados en el DNI se basan en:

a) Cuatro pares de claves RSA

b) Dos pares de claves DES

c) Dos pares de claves DSA

d) Dos pares de claves RSA

67. Acerca de las Autoridades de sellado de tiempo:

a) Para expedir su certificado precisan conocer en su integridad el documento.

b) En el modo de registros encadenados aplican iterativamente una función resumen (hash) a la concatenación del resumen del mensaje a sellar con el resultado de la iteración anterior.

c) En el modo de firma digital firman la concatenación de los mensajes a sellar con el tiempo.

d) Ninguna de las anteriores es correcta.

68. Con respecto al DNIe 3.0, señale la falsa:

a) Hace uso de la tecnología NFC.

b) Se basa en comandos ISO 7816.

c) No es posible utilizarlo con lectores de tarjetas inteligentes.

d) Incorpora un chip más rápido.

69. La entidad que realiza la identificación y autenticación de los solicitantes de certificados en nombre de la autoridad de certificación en una infraestructura típica de clave pública X.509 recibe el nombre de:

a) Autoridad de registro.

b) Oficina de reclutaniento.

c) Punto de venta autorizado.

d) Entidad de validación.

70. ¿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.

71. ¿Sobre qué versa el estándar PKCS#7 de criptografía?

a) Formato de certificado digital

b) Formato de sobre digital

c) Cifrado con clave privada

d) Sintaxis de la clave privada

72. Señale la opción correcta respecto a las smart cards o tarjetas inteligentes:

a) Requieren de una batería para conservar los datos almacenados.

b) Pueden ser de contacto, sin contacto, híbridas o duales.

c) Contienen memoria de sólo lectura y de almacenamiento, pero no pueden tener una CPU.

d) Las operaciones criptográficas se realizan mediante una aplicación específica en un equipo informático.

73. 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.

74. La definición de PKI, según IETF - PKIX es:

a) El conjunto de hardware, software, políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados basados en criptografía de clave pública

b) El conjunto de hardware, software, personal, políticas y procedimientos necesarios para crear, gestionar y almacenar certificados basados en criptografía de clave pública

c) El conjunto de hardware, software, personal, políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados basados en criptografía de clave pública

d) El conjunto de políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados basados en criptografía de clave pública

75. ¿Cuál es la vigencia de los certificados electrónicos incluidos en el DNI electrónico?

a) Dos años

b) Cuatro años

c) 30 meses

d) 60 meses

76. El certificado de firma del DNI electrónico es un certificado (según la normativa de firma electrónica):

a) Avanzado

b) Cualificado

c) Seguro

d) Reconocido

77. ¿Qué se entiende por autoridad de certificación (AC)?

a) Un juez

b) Una empresa que proporciona seguridad a los certificados, aunque en la actualidad sólo puede considerarse a Microsoft como tal.

c) Son órganos administrativos dependientes del Consejo Superior de Informática que dictan las normas de certificación digital, de acuerdo a las normas de la Unión Europea

d) Son entidades que expiden certificados digitales de manera que garantizan la correspondencia entre la identidad de un usuario y su par de claves

78. ¿Es capaz el DNI electrónico de identificar biométricamente al ciudadano?

a) Sí, a través del iris ocular

b) Sí, a través de la firma manuscrita

c) No, no dispone de esa capacidad

d) Sí, a través de la huella dactilar

79. En relación con los prestadores de servicios de confianza cualificados, la Autoridad de Validación:

a) Presta un servicio de comprobación de la vigencia de un determinado certificado.

b) Habitualmente coincide con la Autoridad de Certificación.

c) Es la encargada de revocar el certificado antes de su caducidad cuando deja de tener validez.

d) Es la encargada de verificar la identidad del titular de forma previa a la expedición del certificado.

80. ¿Cómo se denomina el módulo criptográfico necesario para poder operar con el DNI electrónico en un entorno UNIX?

a) Cryptographic Service Provider (CSP).

b) PKCS#11.

c) PGP.

d) Smart Card Mini-Driver.

81. ¿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.

82. La tecnología utilizada para medir y analizar características del cuerpo humano con propósitos de autenticación se llama:

a) Huella

b) Biométrica

c) JBOD

d) Antropomorfismo

83. En el ámbito de los certificados X.509:

a) La CA de la PKI debe proporcional protocolos de gestión de certificados (registro, recuperación de claves, etc) disponibles online.

b) Una CRL es una lista de certificados revocados con un timestamp que determina su fecha de emisión y firmada en todo caso por la CA que emite los certificados.

c) Una CRL tiene un alcance que define el tipo de certificados que incluirá dicha lista.

d) Un certificado se añade a la CRL en la siguiente actualización según la política de actualizaciones definida.

84. El número máximo de certificados que se pueden almacenar en una tarjeta criptográfica CERES es:

a) 4

b) 5

c) 10

d) 7

85. Con independencia de lo establecido sobre la validez del documento nacional de identidad, la vigencia de los certificados electrónicos reconocidos incorporados al mismo no podrá ser superior a:

a) 2 años

b) 36 meses

c) 5 años

d) 12 meses

86. Dentro del chip criptográfico del DNI electrónico podemos encontrar tres zonas de datos diferenciadas. Una de las zonas sólo es accesible por la Dirección General de la Policía. Señale su nombre:

a) Zona pública

b) Zona de seguridad

c) Zona privada

d) Zona confidencial

87. De entre las siguientes opciones, indique qué atributo es más deseable con el fin de utilizar un rasgo biométrico en un sistema de control automático de accesos:

a) Que posea una alta variabilidad temporal.

b) Que posea una alta variabilidad inter-usuario.

c) Que posea una alta variabilidad intra-usuario.

d) Que posea una alta homogeneidad inter-usuario.

88. Según el Reglamento europeo 910/2014 relativo a la identificación electrónica y los servicios de confianza, ¿cuál de las siguientes modalidades de firma electrónica es equiparable, en cuanto a sus efectos jurídicos, a la firma manuscrita?

a) Firma electrónica autorizada.
b) Firma electrónica avanzada.
c) Firma electrónica homologada
d) Firma electrónica cualificada.

89. Con respecto al DNIe 4.0, señale la respuesta CORRECTA:

a) No presenta mejoras de rendimiento con respecto al DNIe 3.0
b) Utiliza la arquitectura basada en procesador ARM de 16 bits
c) Cuenta con algoritmos de curva elíptica de 384 bits
d) Todas las anteriores son falsas

90. 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 válido para una única sesión, terminada ésta habría que solicitar otro
c) de 6 dígitos que aparece en el anverso del documento físico del DNI 3.0
d) accesible en la zona privada del DNI 3.0 mediante la utilización de la clave personal de acceso o PIN

91. ¿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.

92. ¿Cuál de los siguientes NO es un procedimiento adecuado para la consulta de la validez de un certificado digital emitido por un prestador de servicios de confianza?

a) Declaración de prácticas de certificación.
b) Listas de certificados revocados.
c) LDAP.
d) OCSP.

93. Con respecto al DNIe 4.0, señale la respuesta FALSA:

a) Utiliza la arquitectura Cortex M basada en ARM de 32 bits
b) Contiene un total de 350Kb de memoria flash para almacenamiento de datos del ciudadano
c) Permite realizar la firma únicamente utilizando el algoritmo criptográfico RSA
d) Todas las anteriores son correctas

94. La prestación de los 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).

95. Se define Autoridad de certificación como aquella en la confían uno o más usuarios y cuya actividad principal es la certificación de la autenticidad de:

a) Los usuarios

b) Los datos

c) Los documentos

d) Los mensajes

96. ¿Cuál es la vigencia temporal de los certificados electrónicos contenidos en el DNIe?

a) Ilimitada.

b) No podrá ser superior a 5 años.

c) 30 meses.

d) El certificado de autenticidad 24 meses y el de firma 18.

97. Una infraestructura de clave pública (PKI) es:

a) Un algoritmo de clave pública, cuya firma digital hace uso de funciones hash de 64 bits

b) El conjunto de certificado de autenticación y certificado de firma reconocida

c) Una tercera parte de confianza que se encarga de la firma digital de los certificados de usuarios de entorno de clave pública

d) Un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública

98. Señale cuál de los siguientes datos se encuentra en la zona pública del chip criptográfico del DNI electrónico:

a) Certificado de autenticación

b) Certificados de la autoridad de certificación

c) Datos biométricos

d) Claves privadas del ciudadano

99. OCSP es:

a) un protocolo de comprobación de estado de un certificado

b) un algoritmo de hash

c) un algoritmo de cifrado simétrico

d) un algoritmo de cifrado asimétrico

100. TTP hace referencia a:

a) La Top Testing Policy es una política que se implanta en organizaciones con un fuerte desarrollo de la calidad del software, para hacer de las pruebas algo fundamental.

b) Training To Practise es un tipo de trabajo en equipo que acelera el tiempo en que un empleado nuevo puede comenzar a desempeñar su función.

c) Una Trusted Third Party es una tercera parte de confianza, es decir una entidad en la que confiamos, y de la que aceptaremos todo lo que firme.

d) Todas son falsas.

101. NO es una autoridad de certificación electrónica en España:

a) IDCAT

b) CAMERFIRMA

c) CATCERT

d) IZENPE

102. ¿Cuál es el estándar de la ITU-T para infraestructuras de claves públicas?

a) X.500

b) X.509v3

c) X.CRL

d) OCSP

103. 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 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 bits para la AC Raíz y 2048 bits para las AC Subordinadas.

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

104. ¿Cuál es el período máximo de validez de los certificados del DNIe?

a) 24 meses.

b) 5 años.

c) 30 meses.

d) 4 años.

105. Señale donde se encuentran los datos biométricos y de identidad en el chip criptográfico del DNI electrónico:

a) Zona de seguridad

b) Zona pública

c) Zona privada

d) Zona confidencial

106. Los comandos y distribución de memoria de una tarjeta criptográfica se especifican en el estándar:

a) ISO 7816-2

b) ISO 7816-3

c) ISO 7816-4

d) ISO 7816-5

107. ¿Cuál de los siguientes apartados de la especificación 7816 de ISO/IEC (International Standards Organization/International Electrotechnical Commission) relativa a tarjetas inteligentes recoge sus especificaciones eléctricas y protocolos de comunicación?

a) 7816-2.

b) 7816-3.

c) 7816-4.

d) 7816-5.

108. ¿Cuál de los siguientes protocolos permite conocer en tiempo real si un certificado ha sido o no revocado?

a) OCSP

b) CRL

c) PKCS#10

d) HTTPS

109. ¿Cuál de las siguientes características del DNI electrónico se introdujo a partir 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.

110. ¿Cuáles de las siguientes opciones se corresponden con formatos de firma electrónica?

a) PNG, JPEG y TIFF.

b) XML, PHP y HTML.

c) X.509, ASN.1 y DER.

d) XAdES, CAdES y PadES.

111. El DNI digital permitirá:

a) Firmar y cifrar.

b) Solo firmar.

c) Solo cifrar.

d) Solo funciones 3DES.

112. El DNIe recoge los siguientes datos biométricos:

a) Huellas dactilares

b) Iris del ojo

c) Patrón facial

d) Ninguna de las anteriores

113. Es falso que las "Etiquetas RF/ID":

a) Permiten sólo lectura a una distancia de 1 metro. La escritura se debe hacer con contacto

b) Las etiquetas RF/ID pueden contener un bloque de memoria de usuario

c) Son etiquetas con una espiral en su interior de 5 x 5 cm

d) Su principal aplicación es inventario o seguridad

114. La estatura de una persona no puede emplearse en reconocimiento biométrico porque NO cumple el requisito de:

a) Universalidad

b) Distintividad

c) Evaluabilidad

d) Aceptabilidad

115. Denominamos al conjunto de elementos software y hardware, procedimientos, políticas y personal; cuyo objetivo es crear, almacenar, distribuir y revocar certificados digitales de clave pública, como:

a) Infraestructura de clave pública (PKI).

b) Autoridad de certificación (CA).

c) Autoridad de registro (RA).

d) Plataforma de servicios de firma.

116. Señalar cuál de las siguientes es un obligación impuesta a los prestadores cualificados de servicios de confianza:

a) Utilizar la etiqueta de confianza "UE" para indicar de manera simple, reconocible y clara los servicios de confianza cualificados que prestan.

b) Elegir en cada país al organismo de supervisión que garantice que se cumple con lo establecido en el Reglamento (UE) 910/2014, de 23 de julio de 2014.

c) Incluir atributos específicos adicionales en los certificados cualificados de firmas electrónicas.

d) Ser auditados, al menos cada 24 meses, corriendo con los gastos que ello genere, por un organismo de evaluación de la conformidad.

117. En una arquitectura PKI, la Autoridad de Validación:

a) Verifica la identidad del titular antes de la expedición del certificado.

b) Comprueba si un certificado ha sido revocado mediante servicios de directorio, CRL y OCSP.

c) Expide, gestiona y revoca certificados digitales.

d) Procesa solicitudes de revocación de certificados.

118. La tarjeta DNIe tiene capacidad para la realización de firmas electrónicas en:

a) Modo raw y modo relleno PKCS#11.
b) Únicamente en modo raw.
c) Únicamente en modo relleno PKCS#11.
d) Ninguna de las anteriores.

119. En un esquema de certificación y seguridad basado en clave pública (PKI), la 'tercera parte confiable' se denomina:

a) Autoridad de Certificación
b) Autoridad de Registro
c) Centro de Confianza
d) Autoridad de Revocación

120. Los certificados del DNI electrónico:

a) Se expiden voluntariamente a petición del ciudadano
b) Se expiden siempre y vienen activados
c) Sólo se expiden a quien autorice la Dirección General de la Policía
d) Se expiden siempre, pero se activan voluntariamente con el consentimiento del ciudadano

121. En relación al protocolo OCSP (Online Certificate Status Protocol):

a) Se utiliza para conocer el estado de revocación de un certificado X.509
b) Los mensajes enviados vía OCSP se codifican en ASN.1
c) Se define en el RFC 6960
d) Todas las anteriores respuestas son ciertas

122. El órgano competente para la expedición del DNIe es:

a) Ministerio de Defensa
b) Ministerio del Interior
c) Ministerio de Presidencia
d) Secretaria de Estado de Función Pública

123. Dentro del proyecto CERES, es posible disponer de tarjetas criptográficas para entregar a los ciudadanos ¿Qué funcionalidades proporcionan dichas tarjetas desde el punto de vista de la seguridad?

a) Autenticación e integridad, únicamente
b) Autenticación, integridad y confidencialidad, únicamente
c) Autenticación, integridad y confidencialidad y no repudio en origen
d) Autenticación, integridad y confidencialidad y no repudio en destino

124. ¿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.

125. ¿Quién expide los certificados del DNI electrónico?

a) El Ministerio de Hacienda y Función Pública
b) La plataforma @firma
c) La Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda
d) La Dirección General de la Policía

126. Cada vez que un ciudadano utilice su tarjeta criptográfica CERES para firmar documentos que debe entregar a la Administración, señale qué utilización estará haciendo de las claves sobre el resumen del documento:

a) Lo cifrará con su clave pública

b) Lo cifrará con la clave pública de la Administración

c) Lo cifrara con el certificado raíz de la FNMT

d) Lo cifrará con su clave privada

127. ¿Cuál de las opciones siguientes NO se corresponde con servicios ofrecidos por una PKI (Public Key Infrastructures)?

a) Registro de claves públicas: emisión de un nuevo certificado para una clave pública

b) Revocación de certificados: cancelación de un certificado previamente remitido

c) Evaluación de la confianza: determinación sobre si un certificado es válido y qué operaciones están permitidas para dicho certificado

d) Realización de trámites de forma segura con la Administración Pública a través de Internet

128. En un sistema de control de accesos, el EER (Equal Error Rate) se da cuando:

a) La tasa de falsos positivos es igual a la de falsos negativos (FAR = FRR).

b) La tasa de falsos positivos es mayor a la de falsos negativos (FAR > FRR).

c) La tasa de falsos positivos es menor a la de falsos negativos (FAR < FRR).

d) La tasa de falsos positivos es igual cero (FAR =0) y la tasa de falsos negativos es mayor que O y menor que 1 (0 < FRR <1).

129. Una infraestructura de clave pública:

a) Consiste en el acceso a soluciones de teletrabajo de las Administraciones Públicas.

b) Es el conjunto de servidores que realizan operaciones de cifrado en una autoridad de certificación.

c) Es la infraestructura capaz de soportar la gestión de claves públicas para los servicios de autenticación, criptación, integridad, o no repudio.

d) Es el conjunto de aplicaciones instaladas en ordenadores personales que permiten realizar operaciones de cifrado o de firma electrónica.

130. Dentro de los Estándares de Criptografía de Clave Pública (PKCS):

a) PKCS#1: Corresponde al algoritmo RSA

b) PKCS#3: Corresponde al algoritmo Diffie-Hellman

c) PKCS#8: Cifrado con clave privada

d) Todas las respuestas anteriores son correctas