

Test Tema 81 #2

Actualizado el 13/04/2025

1. Las tarjetas de proximidad se encuentran recogidas en el estándar:

- a) ISO 10536
- b) ISO 14443
- c) ISO 15693
- d) ISO 16949

2. Una CRL completa:

- a) Lista todos los certificados no expirados emitidos por la CA revocados por cualquier razón.
- b) Lista los certificados cuyo estado de revocación ha cambiado desde la anterior CRL completa.
- c) Se emite con la periodicidad definida en la política de actualizaciones, pero siempre que hayan transcurrido menos de 24 horas desde la última emisión.
- d) Lista todos los certificados no expirados revocados por los motivos de revocación dentro del alcance de la CRL.

3. En el ámbito de las tarjetas con chip integrado, ¿cuál es el apartado de la norma ISO 7816 que recoge las especificaciones eléctricas y los protocolos de comunicación?

- a) ISO 7816-1.
- b) ISO 7816-2.
- c) ISO 7816-3.
- d) ISO 7816-4.

4. Las dimensiones del DNI electrónico son:

- a) 85,60 mm de ancho X 53,98 mm de alto
- b) 8,6 mm de ancho X 5,9 mm de alto
- c) 60 mm de ancho X 58 mm de alto
- d) 85,60 mm de alto X 53,98 mm de ancho

5. En la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, se indica que la prestación de servicios electrónicos de confianza no cualificados:

- a) No está sujeta a autorización previa.
- b) Está sujeta a autorización previa por parte del organismo europeo de supervisión.
- c) Está sujeta a autorización previa por parte de la Secretaría de Estado de Digitalización e Inteligencia Artificial.
- d) Está sujeta a autorización previa por parte del Ministerio de Asuntos Económicos y Transformación Digital.

6. Según el estándar ISO 7816 sobre contactos del chip en las tarjetas inteligentes, ¿cuál de los siguientes contactos se utiliza para la señal de reloj?

- a) C2.
- b) C3.
- c) C5.
- d) C6.

7. La entidad que identifica de forma inequívoca al solicitante de un certificado electrónico es la:

- a) Autoridad de Registro
- b) Autoridad de Certificación
- c) Autoridad de Revocación
- d) Autoridad de Usurpación

8. El Documento Nacional de Identidad electrónico:

- a) Acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.
- b) Sólo se podrá utilizar para acreditar la identidad de su titular.
- c) Permitirá acreditar la identidad de las personas físicas o jurídicas.
- d) Puede almacenar información penal y sanitario del titular.

9. Si quiero cambiar el PIN del DNI electrónico:

- a) Sólo puedo hacerlo desde mi casa pero necesito un lector de huella dactilar
- b) Puedo hacerlo desde los dispositivos autorizados por la Dirección General de la Policía
- c) Puedo hacerlo sólo usando mi navegador web
- d) Sólo puedo hacerlo si tengo el PUK

10. ¿Qué disposición legal determina el procedimiento para la expedición del DNI electrónico y sus certificados de firma electrónica?

- a) Ley 40/2015, de 1 de octubre.
- b) RD 3/2010, de 8 de enero.
- c) RD 1553/2005, de 23 de diciembre.
- d) Ninguna de las anteriores

11. En una infraestructura PKI, la revocación de un certificado requiere la presencia del usuario en:

- a) El proveedor de servicios de certificación.
- b) En la Fábrica Nacional de Moneda y Timbre.
- c) No hace falta, se puede hacer desde Internet.
- d) En una oficina de registro.

12. Según la recomendación X.509 v3, en relación con las Listas de Certificados Revocados (CRL), ¿Cuál de las siguientes afirmaciones es correcta?

- a) Pueden contener certificados revocados por diversas Autoridades de Certificación.
- b) Para cada certificado revocado indican, entre otros, el nombre del titular del certificado y la correspondiente clave pública.
- c) Deben actualizarse al menos una vez a la semana.
- d) Permiten conocer el estado de un certificado en el instante de la consulta.

13. 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 de 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.

14. El estándar X.509 v3 define los distintos elementos que debe contener un certificado, entre los que destacan:

- a) Número de serie del certificado
- b) Nombre de la autoridad de certificación
- c) Firma digital de la autoridad certificadora
- d) Todas las respuestas anteriores son correctas

15. ¿Cuál de las siguientes características es propia de OCSP?

- a) Es un método de validación del estado de un certificado electrónico que emplea suplementariamente la descarga y consulta de CRLs.
- b) Permite la consulta off-line del estado de revocación de un certificado proporcionado por una autoridad de certificación.
- c) No permite implementar mecanismos de tarificación.
- d) Permite verificar el estado de los certificados mediante la consulta a una autoridad de validación.

16. ¿Cuál de los siguientes no es un sistema operativo utilizado en la arquitectura de un sistema de tarjeta inteligente?

- a) MultOS
- b) Jini
- c) Java Card
- d) Windows SC