TEMA 5. CRIPTOGRAFÍA

Levamos varios temas estudando seguridade e aínda case non vimosnada de algoritmos nin de métodos de cifrado, van sendo horas.

1. Principios de la criptografía

La criptografía (del griego "oculto" y "escribir", literalmente "escritura oculta") es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que solo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos. Otra aplicación frecuente es la de cifrar información contenida en soportes de almacenamiento para garantizar la privacidad y confidencialidad de la misma.

Con más precisión, cuando se habla de esta área de conocimiento como ciencia, se debería hablar de criptología, que a su vez engloba tanto las técnicas de cifrado, es decir, la criptografía propiamente dicha, como sus técnicas complementarias, entre las cuales se incluye el criptoanálisis, que estudia métodos empleados para romper textos cifrados con objeto de recuperar la información original en ausencia de las claves.

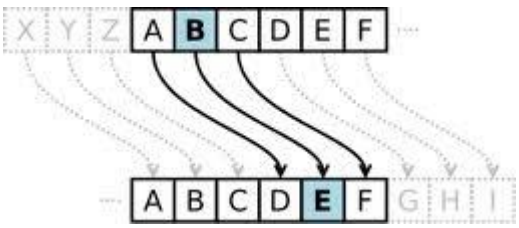
La criptografía se considera una rama de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas matemáticas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves.

En la terminología de criptografía, encontramos los siguientes aspectos:

- La **información original** que debe protegerse se denomina **texto en claro o texto plano**.
- El **cifrado** es el proceso de **convertir el texto plano en un texto ilegible**, denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado se basa en la existencia de una **clave** o información secreta que adapta el algoritmo de cifrado para cada uso distinto.
- Los algoritmos de cifrado se clasifican en dos grandes tipos:
  - **De cifrado en bloque**: dividen el texto origen en bloques de bits de un tamaño fijo y los cifran de manera independiente.
  - **De cifrado de flujo**: el cifrado se realiza bit a bit, byte a byte o carácter a carácter.
- Las dos técnicas más sencillas de cifrado, en la criptografía clásica, son:
  - **La sustitución:** supone el cambio de significado de los elementos básicos del mensaje, las letras, los dígitos o los símbolos.
  - **La transposición:** supone una reordenación de los mismos, pero los elementos básicos no se modifican en sí mismos.
- El **descifrado** es el proceso inverso que recupera el texto plano a partir del criptograma y la clave.

2. Tipos de algoritmos de cifrado

La historia de la criptografía es larga y abunda en anécdotas. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares, de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del enemigo. Posiblemente, el primer criptosistema que se conoce fuera documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como **César**, porque supuestamente Julio César lo empleó en sus campañas, uno de los más conocidos en la literatura.



César utilizó un esquema criptográfico simple pero efectivo para comunicarse con sus generales. El método de cifrado introducido por Julio César introduce el concepto de clave criptográfica. El desplazamiento de 3 letras es la clave que se utiliza por César para cifrar el mensaje, necesitándose la misma clave para descifrarlo. El ejemplo de César muestra un criptosistema de clave simétrica en el que se utiliza la misma clave para cifrar y descifrar el mensaje.

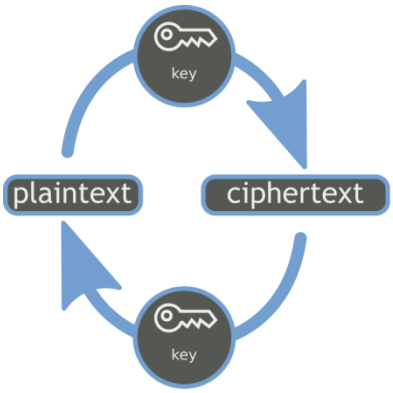
Existen dos grandes grupos de algoritmos de cifrado:

- **Simétricos o de clave simétrica o privada**: los algoritmos que usan una única clave tanto en el proceso de cifrado como en el de descifrado.
- **Asimétricos o de clave asimétrica o pública:** los que emplean una clave para cifrar mensajes y una clave distinta para descifrarlos. Estos forman el núcleo de las técnicas de cifrado modernas.

Según el principio de **Kerchohoff** la fortaleza de un sistema o algoritmo de cifrado debe recaer en la clave y no en el algoritmo, cuyos principios de funcionamiento son conocidos normalmente, en caso de no conocer la clave no podremos descifrar el mensaje.

Criptografía simétrica

La criptografía simétrica es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario y éste lo descifra con la misma.



Un buen sistema de cifrado pone toda la **seguridad en la clave** y ninguna en el algoritmo. Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio. Esto lo posibilita la longitud y el conjunto de caracteres que emplee. Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. Algunos ejemplos de algoritmos de cifrado simétrico son:

- El algoritmo de cifrado **DES** usa una clave de 56 bits, lo que significa que hay 256 = 72.057.594.037.927.936 claves posibles. Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días.
- Algoritmos de cifrado como **3DES**, **Blowfish** e **IDEA** usan claves de 128 bits, lo que significa que existen 2^{128} claves posibles. La mayoría de las tarjetas de crédito y otros medios de pago electrónicos tienen como estándar el algoritmo 3DES.
- Otros algoritmos de cifrado muy usados son **RC5** y **AES**, Advanced Encryption Standard, también conocido como **Rijndael**, estándar de cifrado por el gobierno de los Estados Unidos.

Los **principales problemas** de los sistemas de cifrado simétrico no son su seguridad sino:

- **El intercambio de claves**: una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero, ¿qué canal de comunicación seguro han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.
- **El número de claves que se necesitan**: si tenemos un número n de personas que necesitan comunicarse entre sí, se necesitan **n/2** claves diferentes para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Para solucionar estos problemas se mejora la seguridad de los sistemas, mediante la criptografía asimétrica y la criptografía híbrida.

Criptografía de clave asimétrica

En este caso, cada usuario del sistema criptográfico ha de poseer una pareja de claves:

- **Clave privada:** será custodiada por su propietario y no se dará a conocer a ningún otro.
- **Clave pública:** será conocida por todos los usuarios.

Esta pareja de claves es complementaria: **lo que cifra una solo lo puede descifrar la otra y viceversa**. Estas claves se obtienen mediante algoritmos y funciones matemáticas complejas de forma que por razones de tiempo de cómputo, es imposible conocer una clave a partir de la otra.

Los sistemas de cifrado de clave pública se basan en **funciones resumen o funciones hash de un solo sentido** que aprovechan propiedades particulares, por ejemplo de los números primos. Una función de un solo sentido es aquella cuya computación es fácil, mientras que su **inversión resulta extremadamente difícil**.

Por ejemplo, es fácil multiplicar dos números primos juntos para obtener uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos. Una función resumen o hash de un sentido es algo parecido, pero tiene una simplificación o atajo, si se conoce alguna parte de la información, sería fácil computar el inverso. Por ejemplo, si tenemos un número compuesto por dos factores primos y conocemos uno de los factores, es fácil computar el segundo.

Algunos de los algoritmos empleados como funciones resumen o hash son MD5 y SHA.

El **tamaño de la clave** es una medida de la seguridad del sistema, pero no se puede comparar el tamaño de la clave del cifrado simétrico con el del cifrado de clave pública para medir la seguridad.

En un ataque de fuerza bruta sobre un **cifrado simétrico** con una clave del tamaño de 80 bits, el atacante debe probar hasta 2^{80}-1 claves para encontrar la clave correcta.

En un ataque de fuerza bruta sobre **un cifrado de clave pública** con una clave del tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits. La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el **uso de claves públicas de 1024 bits** para la mayoría de los casos.

La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes **desventajas**:

- Para una **misma longitud de clave y mensaje se necesita mayor tiempo de proceso**.
- Las **claves deben ser de mayor tamaño** que las simétricas.
- El **mensaje cifrado ocupa más espacio que el original**.

Herramientas software como PGP o en comunicaciones TCP/IP, protocolos como SSH o la capa de seguridad TLS/SSL, utilizan un **cifrado híbrido** formado por la **criptografía asimétrica para intercambiar claves** de criptografía simétrica y la **criptografía simétrica para la transmisión de la información**.

- Algunos algoritmos de técnicas de clave asimétrica son:
  - Diffie-Hellman, RSA, DSA, ElGamal, criptografía de curva elíptica.
- Algunos protocolos y software que usan los algoritmos antes citados son:
  - DSS (Digital Signature Standard) con el algoritmo DSA (Digital Signature Algorithm). PGP y GPG, una implementación de OpenPGP SSH, SSL y TLS.

Criptografía híbrida

El uso de claves asimétricas ralentiza el proceso de cifrado. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es **utilizar un algoritmo de clave pública**, más seguro, tan solo empleado para el cifrado en el envío de una pequeña cantidad de información: por ejemplo **una clave simétrica**, junto a uno de clave simétrica, para el cifrado del mensaje, reduciendo de esta forma el coste computacional.

A modo de ejemplo describiremos un proceso de comunicación seguro:

Sonia y Diego tienen sus pares de claves respectivas.

- Sonia escribe un mensaje a Diego. Lo cifra con el sistema de criptografía de clave simétrica.

- La clave que utiliza se llama **clave de sesión** y se genera aleatoriamente. Para enviar la clave de sesión de forma segura, ésta **se cifra con la clave pública de Diego**, utilizando por lo tanto **criptografía de clave asimétrica**.
- Diego recibe el mensaje cifrado con la clave de sesión y ésta misma cifrada con su clave pública. Para realizar el proceso inverso, en primer lugar utiliza su **clave privada para descifrar la clave de sesión**.
- Una vez ha obtenida la clave de sesión, ya puede descifrar el mensaje.

Con este sistema conseguimos:

- **Confidencialidad**: solo podrá leer el mensaje el destinatario del mismo.
- **Integridad**: el mensaje no podrá ser modificado.

Pero todavía quedan sin resolver los problemas de **autenticación y de no repudio**.

Firma digital

Una de las principales ventajas de la criptografía de clave pública es que ofrece un **método para el desarrollo de firmas digitales**. La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación. De este modo, la firma digital ofrece el soporte para la **autenticación** e **integridad** de los datos así como para el **no repudio en origen**, ya que la persona que origina un mensaje firmado digitalmente no puede argumentar que no lo hizo.

Una firma digital está destinada al mismo propósito que una manuscrita. Sin embargo, una firma manuscrita es sencilla de falsificar mientras que la digital es imposible mientras no se descubra la clave privada del firmante.

La firma digital es un cifrado del mensaje que se está firmando pero utilizando la clave privada en lugar de la pública.

Sin embargo, ya se ha comentado el principal inconveniente de los algoritmos de clave pública: su lentitud que, además, crece con el tamaño del mensaje a cifrar. Para evitar este problema, la firma digital es el resultado de cifrar **con clave privada el resumen de los datos a firmar**, haciendo uso de funciones resumen o hash.

A modo de ejemplo: Cris y Jorge tienen sus pares de claves respectivas.

Cris escribe un mensaje a Jorge. Es necesario que Jorge pueda verificar que realmente es Cris quien ha enviado el mensaje, por lo tanto, Cris debe enviarlo firmado:

- Cris **resume el mensaje** o datos mediante una función hash.
- **Cifra el resultado de la función hash con su clave privada**. De esta forma obtiene su firma digital.
- **Envía a Jorge el mensaje original junto con la firma**.

Jorge recibe el mensaje junto a la firma digital. Deberá comprobar la validez de ésta para dar por bueno el mensaje y reconocer al autor del mismo (integridad y autenticación).

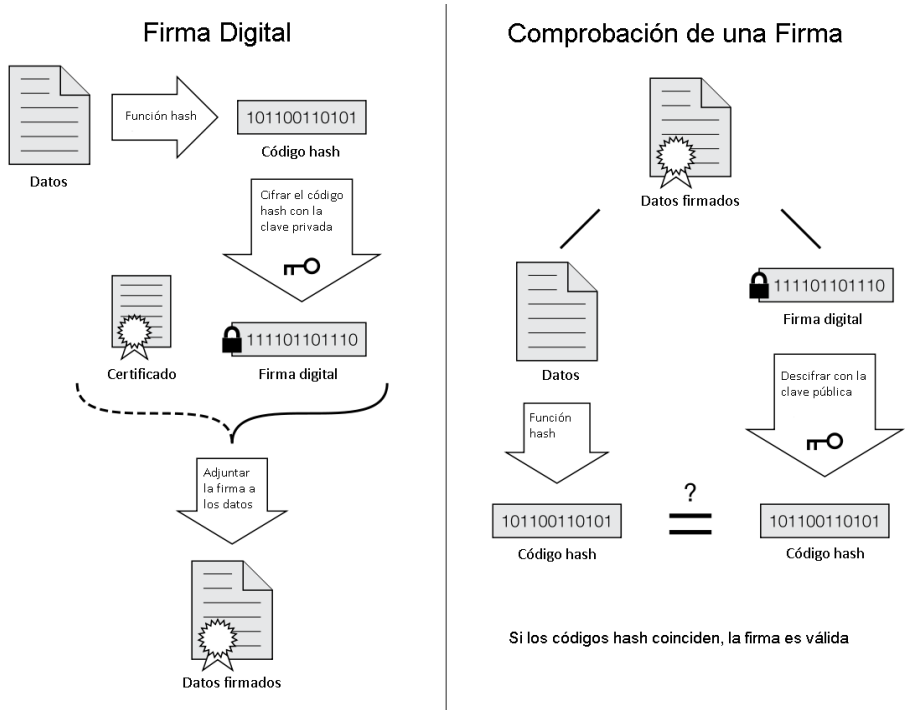
- **Descifra el resumen** del mensaje mediante la clave pública de Cris.
- Aplica al **mensaje la función hash** para obtener el resumen.

- Compara el resumen recibido descifrado, con el obtenido a partir de la función hash. Si son iguales, Jorge puede estar seguro de que quien ha enviado el mensaje es Cris y que éste no ha sido modificado.

Mecánica de la generación y comprobación de una firma digital.

Con este sistema conseguimos:

- **Autenticación:** la firma digital es equivalente a la firma física de un documento.
- **Integridad:** el mensaje no podrá ser modificado.
- **No repudio en origen:** el emisor no puede negar haber enviado el mensaje.



3. Certificados digitales

Según puede interpretarse de los apartados anteriores, la eficacia de las operaciones de cifrado y firma digital basadas en criptografía de clave pública solo está garantizada si se tiene la certeza de que la clave privada de los usuarios solo es conocida por dichos usuarios y que la pública puede ser dada a conocer a todos los demás usuarios con la seguridad de que no exista confusión entre las claves públicas de los distintos usuarios.

Para garantizar la **unicidad de las claves privadas** se suele recurrir a soportes físicos tales como tarjetas inteligentes (SmartCards) que garantizan **la imposibilidad de la duplicación de las claves**. Además, las tarjetas criptográficas suelen estar protegidas por un número personal o PIN solo conocido por su propietario que garantiza que, aunque se extravíe la tarjeta, **nadie que no**

conozca dicho número podrá hacer uso de ella. Como caso particular encontramos el DNI electrónico o DNIe.

Por otra parte, para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los certificados digitales o documento electrónico que asocia una clave pública con la identidad de su propietario.

En general un certificado digital es un archivo que puede emplear un software para firmar digitalmente archivos y mensajes, por ejemplo de correo electrónico, en los cuales puede verificarse la identidad del firmante.

Como ejemplo encontramos los certificados digitales que identifican a personas u organizaciones, y que contienen información sobre una persona o entidad, nombre, dirección, mail, el ámbito de utilización de la clave pública, las fechas de inicio y fin de la validez del certificado, etc., así como una clave pública y una firma digital de una autoridad certificadora u organismo de confianza, en España La Casa de la Moneda y Timbre. En el apartado siguiente veremos la importancia de las autoridades certificadoras.

El formato estándar de certificados digitales es X.509 y su distribución es posible realizarla:

- **Con clave privada** (suele tener extensión *.pfx o *.pl2) más seguro y destinado a un uso privado de exportación e importación posterior como método de copia de seguridad.
- **Solo con clave pública** (suele ser de extensión *.cer o *.crt), destinado a la distribución no segura, para que otras entidades o usuarios tan solo puedan verificar la identidad, en los archivos o mensajes firmados.

Entre las aplicaciones de los certificados digitales y el DNIe encontramos, realizar compras y comunicaciones seguras, como trámites con la banca online, con la administración pública (hacienda, seguridad social, etc.) a través de Internet, etc.

Terceras partes de confianza

Una vez definido el concepto de certificado digital se plantea una duda: ¿cómo confiar si un determinado certificado es válido o si está falsificado? La validez de un certificado es la confianza en que la clave pública contenida en el certificado pertenece al usuario indicado en el certificado.

La manera en que se puede confiar en el certificado de un usuario con el que nunca hemos tenido ninguna relación previa es mediante la **confianza en terceras partes**.

La idea consiste en que dos usuarios puedan confiar directamente entre sí, si ambos tienen relación con una tercera parte y que ésta puede dar fe de la fiabilidad de los dos.

La necesidad de una **Tercera Parte Confiable** (TPC o TTP, Trusted Third Party) es fundamental en cualquier entorno de clave pública de tamaño considerable debido a que es impensable que los usuarios hayan tenido relaciones previas antes de intercambiar información cifrada o firmada. Además,

la mejor forma de permitir la distribución de las claves públicas (o certificad os digitales) de los distintos usuarios es que algún agente, en quien todos los usuarios confíen, se encargue de su publicación en algún repositorio al que todos los usuarios tengan acceso.

En conclusión, se podrá tener confianza en el certificado digital de un usuario al que previamente no conocemos si dicho **certificado está avalado por una tercera parte en la que sí confiamos**. La forma en que esa tercera parte avalará que el certificado es de fiar es mediante su **firma digital sobre el certificado**.

Por tanto, podremos confiar en cualquier certificado digital firmado por una tercera parte en la que confiamos. La TPC que se encarga de la firma digital de los certificados de los usuarios de un entorno de clave pública se conoce con el nombre de **Autoridad de Certificación** (AC).

El modelo de confianza basado en Terceras Partes Confiables es la base de la definición de las Infraestructuras de Clave Pública (ICP o PKI, Public Key Infrastructures), formado por:

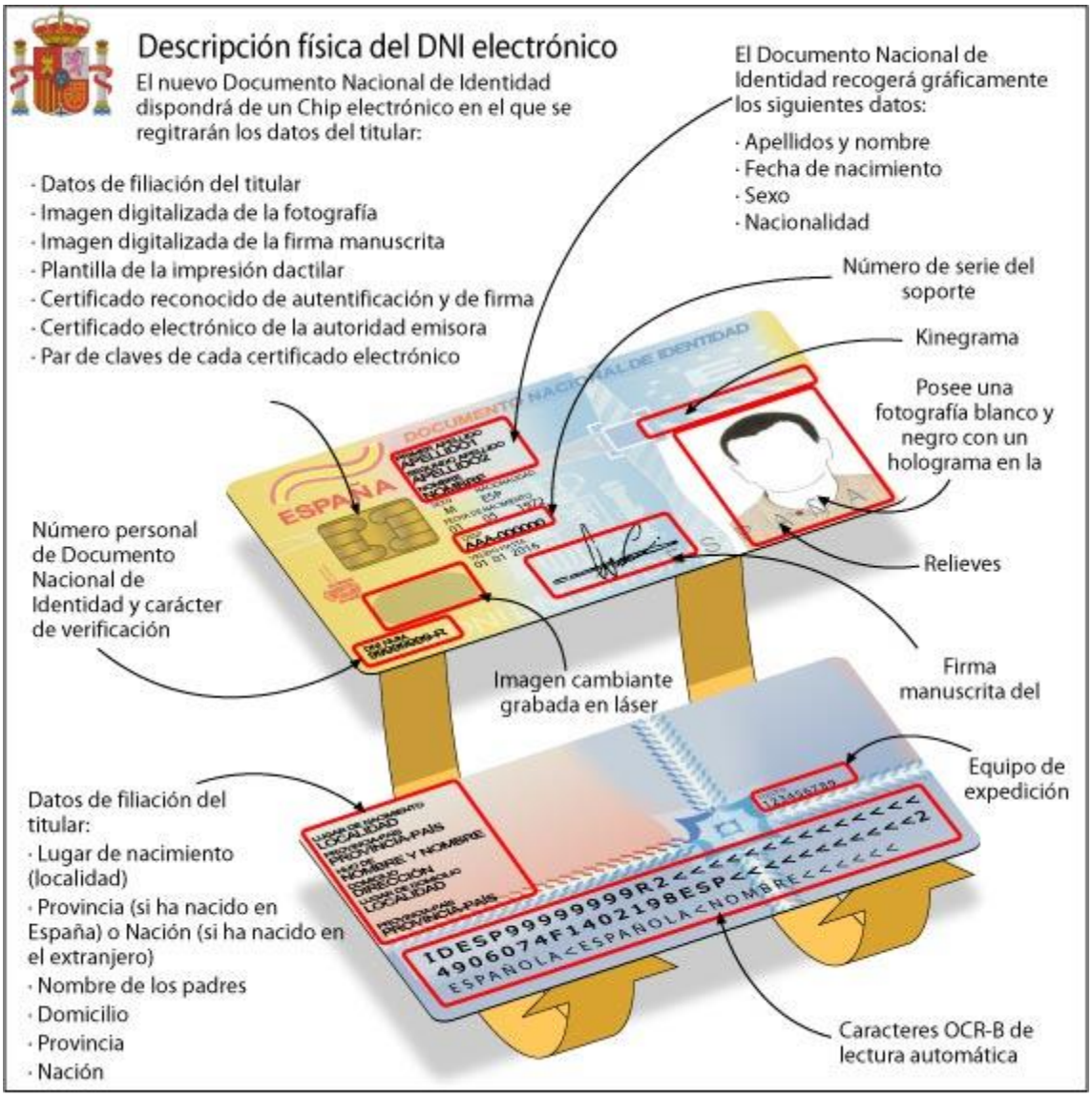
- **Autoridad de certificación** (CA): emite y elimina los certificados digitales.
- **Autoridad de registro** (RA): controla la generación de los certificados, procesa las peticiones y comprueba la identidad de los usuarios, mediante el requerimiento de documentación de identificación personal oportuna.
- **Autoridades de repositorio**: almacenan los certificados emitidos y eliminados.
- **Software para el empleo de certificados**.
- **Política de seguridad en las comunicaciones** relacionadas con gestiones de certificados.

Documento nacional de identidad electrónico (DNIE)

El Documento Nacional de Identidad (DNI), emitido por la Dirección General de la Policía (Ministerio del Interior), es el documento que acredita, desde hace más de 50 años, la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular.

Con la llegada de la Sociedad de la Información y la generalización del uso de Internet se hace necesario adecuar los mecanismos de acreditación de la personalidad a la nueva realidad y disponer de un instrumento eficaz que traslade al mundo digital las mismas certezas con las que operamos cada día en el mundo físico y que, esencialmente, son:

- **Acreditar** electrónicamente y sin posibilidad de duda, la **identidad de la persona**.
- **Firmar digitalmente** documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita.



Para responder a estas nuevas necesidades nace el Documento Nacional de Identidad electrónico (DNIe), similar al tradicional y cuya principal novedad es que incorpora un pequeño circuito integrado (chip), capaz de guardar de forma segura, mediante medidas específicas de seguridad para impedir su falsificación, información en formato digital como:

- **Un certificado electrónico** para **autenticar** la personalidad del ciudadano.
- Un certificado electrónico para **firmar electrónicamente**, con la misma validez jurídica que la firma manuscrita.
- **Certificado de la Autoridad de Certificación** emisora.
- **Claves** para su utilización.
- **La plantilla biométrica** de la impresión dactilar.

Para la utilización del DNI electrónico es necesario contar con determinados elementos:

- **Hardware específico**: lector de tarjetas inteligentes que cumpla el estándar ISO-7816. Existen distintas

implementaciones, bien integrados en el teclado, bien externos (conectados por ejemplo vía USB).

- **Software específico**: mediante controladores o módulos criptográficos que permitan el acceso al chip de la tarjeta y, por tanto la utilización de los certificados contenidos en él. En Windows es el servicio Cryptographic Service Provider (CSP), y en los entornos GNU/Linux o MAC el módulo criptográfico se denomina PKCS#11.

0. Índice