# La firma electrónica. Concepto, tecnología y aplicaciones

Javier Luque Ordóñez
javluqord@yahoo.es

## Introducción. La identidad personal

Según la Real Academia Española, la identidad se define como:

- Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás.
- Conciencia que una persona tiene de ser ella misma y distinta a las demás.

Por otro lado, tal y como se declara en el artículo 6 de la Declaración Universal de Derechos Humanos, "todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica".

Así pues, la identidad personal es un derecho de todo ciudadano, de manera que los estados tienen la obligación de establecer los mecanismos adecuados para facilitársela.

En el mundo físico, la forma más usual de comprobar la identidad es mediante tarjetas de identificación (DNI, pasaporte, permiso de conducir). Estas credenciales del ciudadano (que suelen incluir su fotografía y su firma manuscrita) están respaldadas por una tercera parte confiable (en este caso el Estado o Administración que ha expedido dicho documento) que acredita la veracidad de las mismas, y están diseñadas a prueba de alteraciones y falsificaciones para evitar que quien las porta pueda modificarlas.

La firma manuscrita (también conocida como autógrafa y hológrafa) ha sido desde hace siglos ampliamente utilizada en todos los ámbitos sociales como medio de acreditación de la identidad del signatario de un documento, e igualmente como método para expresar que se está de acuerdo con el contenido del documento firmado.

El concepto de identidad personal adquiere una nueva dimensión cuando se trata de establecerla para un uso no presencial en medios telemáticos. En plena sociedad de la información, y con el uso exten-

dido de ordenadores personales y el enorme crecimiento de Internet, deben existir por tanto mecanismos específicos y procedimientos electrónicos para otorgar y verificar la identidad en este nuevo ámbito.

## Técnicas de identificación digital

Existen actualmente diversas formas de identificar a los usuarios que acceden a un sistema informático:

### *Sistemas basados en claves de acceso (algo que se sabe)*

Son los más antiguos y los más usados en la actualidad, y están basados en un nombre de usuario (identificador) y una clave de acceso (contraseña). Son fáciles de usar y no requieren de hardware especial, pero su uso implica un conjunto de inconvenientes:

- El ordenador debe tener la clave de acceso archivada antes de comprobar la identidad.
- Si se intercepta la clave de acceso al enviarse al ordenador, es muy fácil la suplantación.
- Las personas pueden olvidar sus claves de acceso.
- Las personas eligen habitualmente claves fácilmente predecibles.
- Las personas confían sus claves a otras personas.

### *Prendas físicas (algo que se tiene)*

Se basa en la utilización de algún objeto físico que comprueba de alguna manera la identidad de quien lo posee y le proporciona el acceso al sistema. Las prendas más típicas actualmente son las tarjetas de acceso.

Entre los inconvenientes del uso de prendas para autenticación se encuentran:

- La prenda no prueba quién es la persona, cualquiera que la posea podrá entrar al sistema.
- Si una persona pierde su prenda, no podrá entrar al sistema aunque conserve su identidad.
- Existen prendas que son fácilmente copiables o falsificables.

Las prendas suelen utilizarse conjuntamente con los sistemas basados en claves de acceso. Por ejemplo, en un cajero automático es necesario utilizar una tarjeta para el acceso a la cuenta bancaria, pero se necesita teclear una clave de autorización.

### *Biométrica (algo que se es)*

Se basa en la medición física de algún rasgo de una persona viva, por ejemplo: imagen del rostro, huellas digitales, forma y tamaño de la mano, patrones de ADN, técnicas de caligrafía, formas de teclear, impresiones de voz, etc.

Entre los problemas que presenta la biometría se pueden citar los siguientes:

- La característica biométrica de la persona debe estar archivada en el banco de datos de un ordenador antes de ser identificada.
- La autenticación basada en biométrica requiere de equipos muy específicos y de alto coste.
- Los equipos de medición son vulnerables al sabotaje y al fraude.

Para evitar identificaciones falsas, la biométrica suele combinarse con claves de acceso o prendas.

### *Ubicación (algún lugar en el que se está)*

Se basa en la identificación del usuario según el lugar en el que se encuentren (por ejemplo, mediante sistemas basados en técnicas de GPS). Estos métodos deben ser acompañados de otros (prendas, claves) para evitar suplantaciones y falsificaciones.

### *Firma electrónica y certificado digital*

El correspondiente a la firma manuscrita en la sociedad de la información es la firma digital, también conocida en la Directiva Comunitaria 1999/93/CE y en la correspondiente ley española 59/2003 de 19 de diciembre como firma electrónica.

La firma electrónica posee dos diferencias fundamentales con respecto a la firma manuscrita:

- La firma electrónica debe ser función del documento al que acompaña, no puede ser constante (para evitar que por su naturaleza electrónica pueda ser cortada y pegada posteriormente en cualquier otro documento).
- La firma electrónica proporciona adicionalmente integridad, pudiendo verificarse si el documento al que acompaña ha sido modificado o no.

La firma electrónica, surgida como evolución de los sistemas criptográficos, proporciona una nueva dimensión al intercambio de información en el ciberespacio, presentándose como elemento imprescindible para autenticar de forma inequívoca al autor y garantizar la integridad del documento firmado. El certificado digital es un documento electrónico emitido por una tercera parte confiable que corrobora que la identidad del firmante es verdadera.

Este método puede utilizarse por sí mismo como medio de identificación digital, o para mejorar cualquiera de los métodos anteriores (por ejemplo, el DNI electrónico es una prenda que se posee, y que incluye una firma electrónica accesible mediante clave, para identificar digitalmente al usuario).

## Conceptos básicos de seguridad de la información

Desde hace miles de años, el ser humano se comunica con sus semejantes mediantes un lenguaje o sistema estructurado de signos. Mediante el lenguaje se componen mensajes (en diversos formatos; por ejemplo, mediante escritura o mediante voz), que contienen una determinada información que se quiere transmitir a un destinatario.

Dado que la información es poder, el ser humano ha intentado siempre elaborar mecanismos para proteger la información de aquellos que no son sus destinatarios. Es aquí donde surge la criptología (del griego '*kriptos*', oculto), que puede definirse como la disciplina que estudia los principios, métodos y medios para ocultar la información contenida en un mensaje.

Relacionados directamente con la criptología, que ha obtenido su mayor desarrollo con las dos guerras mundiales (aplicaciones diplomáticas y militares) y con la aparición de la informática y las redes de telecomunicaciones, están los conceptos de criptografía y criptoanálisis:

- Criptografía: conjunto de técnicas que permiten asegurar que un mensaje solo es entendible por aquel al que va dirigido, o protección de la información a través de su codificación mediante claves.
- Criptoanálisis: supresión de esa protección sin el conocimiento de las claves.

Asimismo, se define como cifrado a la transformación de un texto original (texto en claro) en otro, denominado criptograma. El descifrado es la operación inversa, es decir, la obtención del texto original a partir del criptograma. Existen de forma general dos métodos de cifrado:

- Algoritmo secreto:
  - La robustez del algoritmo se basa en el desconocimiento del mismo. Sólo utilizado en aplicaciones militares.
- Algoritmo público (y clave secreta). Mucho más utilizados, por diversos motivos:
  - Pueden fabricarse en cadena (más barato), en versiones tanto hardware como software.
  - Están más probados, ya que participa toda la comunidad científica.
  - Es más fácil y seguro transmitir una clave que todo el algoritmo.
  - Posee un nivel similar de seguridad al de los algoritmos secretos.

Los criptosistemas basados en algoritmos públicos deben cumplir dos requisitos principales:

- Las transformaciones para cifrado y descifrado no solo deben ser eficaces, sino también computacionalmente eficientes.
- La seguridad del sistema debe residir exclusivamente en el secreto de las claves, ya que los algoritmos de cifrado y descifrado son públicos.

Así pues, todo criptosistema tiene los siguientes elementos:

- Emisor: genera un mensaje, texto en claro.
- Cifrador: transforma el texto en claro en un mensaje ininteligible (criptograma). Es un dispositivo físico o programa que implementa el algoritmo de cifrado (que suele ser una función matemática que depende de un parámetro o clave).
- Canal inseguro.
- Descifrador: función inversa a la del cifrador.
- Receptor: recibe el mensaje generado por el emisor.
- Protocolo de intercambio de claves.

A la hora de diseñar un cifrador existen dos principios básicos (que suelen usarse combinados):

- Confusión: establecimiento de una relación lo más compleja posible entre la clave y el texto cifrado.
- Difusión: distribución de las propiedades estadísticas del texto en claro sobre todo el criptograma.

De acuerdo a la forma de tratar el mensaje en claro, los cifradores pueden ser:

- De flujo: cifran carácter a carácter. Son muy rápidos pero no aportan difusión.
- De bloque: cifran descomponiendo el mensaje en claro en bloques. Son más lentos que los de flujo, pero aportan difusión.

Las posibilidades de éxito de un ataque a un criptosistema dependen en gran medida de las circunstancias que le rodean y de la información disponible. El criptoanálisis abarca diversas técnicas, existiendo dos mecanismos básicos de ataque:

- Realización de un análisis estadístico del mensaje. Busca relaciones existentes en el criptograma que puedan dar pistas sobre el mensaje en claro.
- Realización de una búsqueda exhaustiva (ataque de fuerza bruta). Se basa en probar exhaustivamente todas las claves del espacio de claves.

Asimismo todo criptosistema puede formalmente implementar dos tipos de secreto:

- Teórico o incondicional. Se basa en que la información disponible por el atacante no es suficiente para romper el sistema. Es seguro contra cualquier ataque aunque el atacante tenga recursos y tiempo ilimitados.
- Práctico. De acuerdo a la complejidad computacional del criptoanálisis, el criptosistema se considera seguro contra aquellos atacantes que dispongan de menos de una cantidad de tiempo y/o recursos determinada.

En la práctica no existen sistemas completamente seguros, por lo que en criptografía siempre se busca diseñar sistemas que cumplan al menos una de las siguientes condiciones:

- El precio para romperlo es superior al valor de la información que se quiere obtener.
- El tiempo necesario para romperlo es mayor que el tiempo de vida de la información.

Con la evolución de los sistemas criptográficos, las técnicas de criptografía actuales van más allá del cifrado y descifrado de los mensajes. Hoy día proporcionan al menos los siguientes servicios de seguridad de la información, claves para la aparición e implantación de la firma electrónica:

- Autenticación: confirmación de la identidad de las entidades comunicantes y protección frente a suplantaciones de identidad.
- Confidencialidad: protección frente a divulgación de los datos sin autorización y garantía de que la información sólo es entendible por su destinatario.
- Integridad: garantía de exactitud y veracidad de los datos y protección contra modificaciones, supresiones, creaciones y reactuaciones no autorizadas sobre los datos.
- No repudio: evitación de la negación sobre la realización de una acción y garantía de disponibilidad de las pruebas de autoría de una acción.

## Métodos criptográficos clásicos

Los métodos clásicos constituyen la base de los métodos actuales, y han sido los más utilizados hasta hace pocas décadas. Existen diversos tipos, basados en procesos de sustitución, transposición y operaciones matemáticas sencillas. Todos los sistemas actuales se basan en la aplicación en distintas iteraciones de una combinación de estas técnicas.

### *Métodos de sustitución*

Se sustituyen las unidades del texto original por otras. La forma más sencilla es la sustitución simple o monoalfabética, que se basa en el empleo de otras unidades del mismo alfabeto obtenidas tras un desplazamiento. Cuando cada letra se sustituye por su equivalente desplazada 3 lugares, el método se denomina César, por haberse utilizado en la época de Julio César.

La sustitución polialfabética utiliza varias sustituciones para cada letra del alfabeto, con desplazamientos diferentes, dependiendo por ejemplo de las letras de la palabra clave.

### *Métodos de transposición o permutación*

No se sustituyen las letras, sólo se cambia su posición dentro del mensaje. Por ello no rompen la frecuencia del mensaje, y son fácilmente destructibles. Ejemplos conocidos son la escitala (bastón de mando de los generales lacedomios; el diámetro del cilindro donde se enrolla una cinta de pergamino determina la clave), el posicionamiento en zigzag, la distribución en figuras geométricas o las funciones matemáticas de permutación.

### *Métodos basados en cálculos numéricos o lógicos*

Los métodos aritméticos destruyen la frecuencia del mensaje y son fáciles de implantar. Los caracteres del texto en claro y de la clave se codifican numéricamente. Se utilizan, entre otras, operaciones de suma y multiplicación, así como operaciones de cambio de base.

Las transformaciones lógicas booleanas son muy apropiadas para implantar en sistemas informáticos, y para permitir el descifrado deben utilizarse sólo aquellas operaciones que tengan inversa: negación, XOR, y equivalencia (no son válidos en este caso ni la suma ni el producto booleanos).

Las transformaciones matriciales son muy seguras (rompen la frecuencia del mensaje), pero muy laboriosas. Son posibles para cifrar y descifrar porque la suma y multiplicación de matrices poseen operaciones inversas bajo determinadas condiciones (para la suma, las matrices deben ser de las mismas dimensiones, y para el producto, tener una inversa única), permitiéndose el descifrado.

El cifrado producto es el método más usual para crear confusión y difusión, y consiste en la aplicación en cadena de diferentes cifradores, cada uno teniendo como entrada la salida del paso anterior. Un ejemplo clásico de cifrado producto es LUCIFER, que posteriormente evolucionó a DES, algoritmo muy extendido en el cifrado simétrico y basado en sucesivos cifrados de sustitución y transposición.

## Criptosistemas simétricos o de clave secreta

Los criptosistemas de clave secreta o simétricos se basan en el uso de una única clave para cifrado y descifrado. La conservación de dicha clave es responsabilidad del usuario. Se cifran bloques de texto, de tamaño constante o variable, y existen diversos modos de operar con dichos bloques, estando los más importantes estandarizadas por NIST (*National Institute of Standards and Technology*, instituto nacional americano de estándares y tecnología):

- ECB (*Electronic Code Book,* libro de código electrónico). Es el modo más simple, parte el mensaje en bloques y los cifra por separado. Como ventajas destacan la posibilidad de cifrado en paralelo y el acceso aleatorio a los bloques. Como desventajas, se posibilitan los ataques de diccionario y se pueden perder o interceptar bloques sin ser detectado.
- CBC (*Cipher Block Chainning*, encadenamiento de bloques de cifrado). Su utilizan funciones XOR para combinar el bloque ya cifrado con el bloque aún por cifrar, usando un vector de inicialización aleatorio para el primero. Añade más seguridad que ECB, pero no puede ser paralelizado y también permite ataque por sustitución de bloques
- CTR (*Counter Mode*, modo de conteo). Simula un cifrado de flujo, usando un cifrado de bloque para producir un flujo pseudoaleatorio (denominado *keystream*), generado a partir de la combinación de un contador con un número aleatorio. El flujo resultante se combina con el bloque actual en claro mediante XOR. Permite precalcular el flujo y trabajar en paralelo, pero no se deben reutilizar contadores con la misma clave y además es sencillo modificar bits en el mensaje original, por lo que se requiere de una verificación posterior de la integridad del mensaje.
- OFB (*Output FeedBack*, retroalimentación de salidas). Parecido a CTR, el flujo se genera cifrando el bloque anterior, y el primer bloque del flujo se crea con un vector de inicialización. Comparte desventajas con CTR, pero tiene menos ventajas que éste, por lo que es poco utilizado.
- CFB (*Cipher FeedBack*, retroalimentación de cifrado). Muy similar a OFB, para producir el flujo cifra el último bloque de cifrado en lugar del bloque anterior del flujo como en OFB. En este caso el descifrado puede ser paralelizado, pero sigue teniendo más ventajas el modo CTR.

Los algoritmos simétricos más utilizados son:

### *DES (Data Encryption Standard, estándar de cifrado de datos)*

Es el más utilizado históricamente y el más antiguo, y está sujeto a las leyes de seguridad de Estados Unidos, donde fue adoptado en 1977 como estándar de cifrado de todas las informaciones sensibles no clasificadas.

Por normativa legal, la versión original solo puede ser implementada mediante un circuito integrado que no puede ser exportado a otros países sin un permiso especial; sin embargo, en 1981 ANSI (*American National Standard Institute*, organismo estadounidense de estandarización) adoptó el DES como norma para el sector privado y para el cifrado de redes, y esta versión de ANSI sí puede ser programada en un ordenador y utilizada fuera de Estados Unidos.

DES utiliza permutaciones y sustituciones, cifrando bloques de 64 bits con claves de 64 bits (56 de clave y

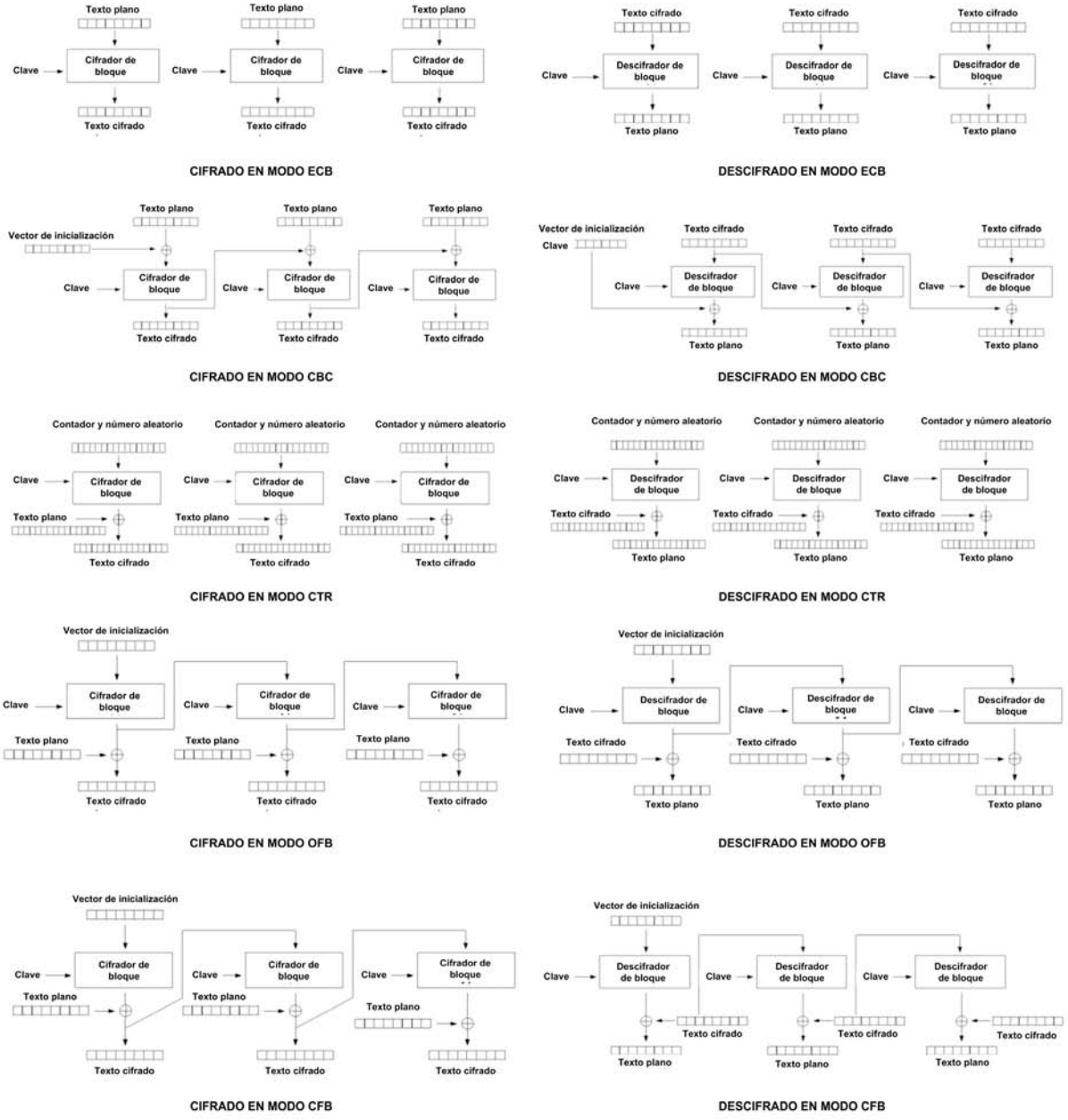


*Figura 1. Modos de cifrado y descifrado de bloques.*

8 de paridad). El cifrado son 19 etapas diferentes, con una transposición inicial y final, una penúltima etapa de intercambio, y 16 intermedias con 16 iteraciones en las que se dividen los bloques en dos mitades trabajando en cada vuelta de cifrado con una de ellas.

El descifrado consiste en la utilización del mismo algoritmo con las claves empleadas en orden inverso, no hay por tanto que invertir la función empleada, sólo repetirla.

Como ventaja principal del algoritmo es que es el más extendido en el mundo, siendo el más barato y el más probado (sobre todo en máquinas Unix). Además, nunca ha sido roto con un sistema práctico y es muy rápido y fácil de implementar. Como inconvenientes principales, la limitación de la versión hardware a Estados Unidos, y la longitud relativamente corta de la clave, que hace que pueda ser planteable un ataque de fuerza bruta. Hoy día se ha sustituido su uso por AES.

## *TDES (Triple DES)*

Es un algoritmo basado en el cifrado producto, mediante 3 iteraciones del algoritmo DES. Existen diversas variantes con varias claves diferentes, aunque una de las más extendidas emplea una clave de

128 bits (16 de paridad y 112 de clave), aplicando 64 bits a los dos DES (primer y tercer paso), y los otros 64 bits al DES inverso (segundo paso). Si las dos claves de 64 bits fueran iguales, el algoritmo equivaldría a un DES simple.

Para romper TDES por un ataque de fuerza bruta con la tecnología existente actualmente, se necesitarían más de 15.000 veces la edad actual del universo. Este algoritmo ha captado un gran número de adeptos, y se utiliza por ejemplo en las normas ANSI X9.17 e ISO 8732, o en productos comerciales como PEM (*Privacy Enhanced Mail*).

### *AES (Advanced Encryption Standard, estándar de cifrado avanzado)*

Desde NIST se convocó en 1996 un concurso de sistemas criptográficos simétricos para decidir cuál sería el nuevo estándar para los siguientes 20 años, denominado AES. En 1998 se aceptaron 15 candidatos, que se redujeron a 5 en 1999: MARS, RC6, Rijndael, Serpent y Twofish.

En octubre de 2000 se declaró ganador al algoritmo belga Rijndael, pasando a considerarse estándar en mayo de 2002. Desde 2006 es el algoritmo más popular usado en criptografía simétrica.

Al algoritmo ganador de AES se le pedía que al menos fuera tan seguro y rápido como TDES (es decir, que evitase al menos todos los ataques conocidos), y que pudiera ser implementado en una gran variedad de aplicaciones y formatos (incluyendo tarjetas de 8 Kbs de memoria). AES puede ser utilizado como cifrador de bloques o de flujos, como generador de funciones resumen o *hash*, y como generador de números aleatorios.

Rijndael fue desarrollado por dos criptólogos belgas, Joan Daemen y Vincent Rijmen, y se basa en una red de sustitución-permutación. Es rápido tanto en hardware como en software, es relativamente sencillo de implementar y requiere poca memoria. Cifra bloques fijos de 128 bits, con claves de 128, 192 o 256 bits, y opera en una matriz de 4x4 constando cada ronda del algoritmo de 4 pasos.

### *IDEA (International Data Encryption Algorithm, algoritmo internacional de cifrado de datos)*

Aparece en 1992, como evolución del algoritmo PEES (*Proposed European Encryption Standard*, propuesta de estándar europeo de cifrado). IDEA está libre de restricciones y permisos nacionales, y es de libre distribución en Internet. El texto en claro y el criptograma están compuestos por bloques de 64 bits, y la clave es de 128 bits.

IDEA opera mediante 8 vueltas de cifrado idénticas, más una transformación de salida. Se mezclan operaciones de 3 grupos aritméticos diferentes sobre subbloques de 16 bits (con subclaves diferentes): multiplicativo, aditivo, y aditivo bit a bit. Al ser de libre distribución, es un algoritmo muy popular, sobre todo fuera de Estados Unidos. Se utiliza por ejemplo en PGP (*Pretty Good Privacy*).

### *RC5*

RC5 (Rivest *Cipher* 5, cifrador de Rivest v5) es la evolución de RC2 y RC4, todos ellos de Ron Rivest. RC2 cifra bloques de 64 bits utilizando sustituciones y permutaciones, con claves de longitud variable entre 1 y 2048 bits (aunque las versiones exportadas están limitadas a 40 bits). El diseño de este cifrador es secreto.

RC4 es un cifrador de flujo, también de diseño secreto, y con clave variable entre 1 y 2048 bits (nuevamente 40 bits para la versión de exportación, y 128 bits para Estados Unidos). Dispone de muchos parámetros configurables, como el número de iteraciones, la longitud de la clave y el tamaño del bloque, entre otros.

RC5 es un cifrador de bloque, que opera con palabras de tamaño variable, número de vueltas variable, y clave secreta de longitud variable. Su diseño está optimizado para poder ser implementado tanto en hardware como por software. Se utiliza por ejemplo en Netscape.

## Criptosistemas asimétricos o de clave pública

La criptografía simétrica es de gran interés para garantizar la confidencialidad de la información. Sin embargo, es insuficiente para llevar a cabo comunicaciones seguras en redes abiertas, especialmente Internet, debido a la necesidad de compartir la clave de forma segura (esto es, se necesita un canal seguro –para compartir la clave– para poder crear otro canal seguro –para compartir el mensaje cifrado–).

Por otro lado, la posibilidad de ataques activos obliga a que la criptografía no solo garantice la confidencialidad de los datos, sino que aborde también la problemática de preservar la integridad del mensaje,

la actualidad de la información y la autenticidad de los actores.

Así, en el marco de la búsqueda de soluciones a los problemas planteados, Walter Diffie y Martin Hellman publicaron en 1976 el artículo *"New directions in cryptography"* (Nuevas tendencias en criptografía) en el que proponían un nuevo tipo de criptografía basado en utilizar claves diferentes para cifrar y descifrar. Era el nacimiento de los criptosistemas asimétricos.

Estos criptosistemas no precisan, previamente al establecimiento de una transmisión cifrada, la transferencia de una clave secreta entre emisor y receptor, evitando así los problemas inherentes a la búsqueda de canales seguros para tal transferencia.

Se utilizan dos claves por cada participante. Una de ellas, denominada clave pública, se hace de general conocimiento, y la otra, denominada clave privada, se mantiene en secreto. Cada par de claves, pública y privada, debe cumplir con las siguientes propiedades:

- Ambas claves no son independientes, pero del conocimiento de la pública no se infiera la privada, a no ser que se tenga algún dato adicional que también habrá de mantenerse en secreto o destruirse una vez generado el par de claves. De esta forma, dada la pública es computacionalmente imposible descubrir la clave privada.
- Cualquier información cifrada con una de las claves únicamente puede ser descifrada con la otra.

Estos principios han supuesto una auténtica revolución en la criptología, ya que los criptosistemas de clave pública se pueden utilizar para confidencialidad (como los criptosistemas asimétricos) y para autenticación. Para cada tipo de servicio se cifra de manera diferente:

- Confidencialidad: el emisor cifra el texto con la clave pública del receptor, y el receptor lo descifra con su propia clave privada. Cualquiera puede enviar un mensaje cifrado, pero sólo el receptor, que tiene la clave privada, y el emisor, creador del mensaje, pueden conocer su contenido.
- Autenticación: el emisor cifra el mensaje con su clave privada. Cualquiera puede comprobar su procedencia utilizando la clave pública del emisor. El mensaje es auténtico porque sólo el emisor verdadero puede cifrar con su clave privada.

Una variante del mecanismo de autenticación, aplicado sobre un resumen (mediante la aplicación de una función unidireccional, denominada función *hash*) del documento, ha dado lugar al concepto de firma electrónica, que además de proporcionar autenticación añade garantía de integridad.

Hay tres tipos de algoritmos de cifrado en criptosistemas asimétricos, según el problema matemático en el que se fundamenten:

- Factorización entera. Problema inverso a la multiplicación. Se trata de hallar los factores primos de un número muy grande.
- Logaritmo discreto. Se define sobre aritmética modular (operador resto de la división entera). Está directamente relacionado con el problema de factorización entera.
- Logaritmo discreto elíptico. Se trata de encontrar un número entero que relacione a dos puntos de una curva elíptica que cumple determinadas condiciones.

La fortaleza de estos algoritmos reside en la supuesta imposibilidad de resolver sus respectivos problemas de forma computacionalmente eficiente. No se ha podido hallar hasta el momento, ni se ha demostrado que exista, un algoritmo capaz de resolverlos.

El principal inconveniente de los criptosistemas asimétricos es su excesiva lentitud (los simétricos son mucho más rápidos –entre 100 y 10.000 veces–). Por ello, los criptosistemas asimétricos se utilizan sólo con mensajes pequeños, teniendo dos aplicaciones claramente establecidas:

- Intercambio seguro de clave de sesión. Se cifra con la clave pública del receptor una clave de sesión con la que realizar un cifrado simétrico del documento a enviar. Se utiliza por ejemplo en comunicaciones cifradas en Internet (VPNs, SSL, etc.).
- Firma electrónica. Se cifra con la clave privada del emisor el resumen del documento.

Lo habitual por tanto es encontrar criptosistemas mixtos, simétricos para confidencialidad y asimétricos para distribución de claves simétricas, autenticación y firma digital.

Los algoritmos más conocidos para cifrado asimétrico son:

- DH (Diffie-Hellman). Algoritmo propuesto en el artículo que dio origen a este tipo de criptosistemas, está basado en el logaritmo discreto, y se utiliza para la distribución de claves simétricas, pero no sirve para confidencialidad, autenticación o firma.

- DSA (*Digital Signature Algorithm*, algoritmo de firma digital). Basado en el logaritmo discreto, se utiliza únicamente para firma digital.
- DHE y DSAE. Variantes de DH y DSA basadas en el logaritmo discreto elíptico.
- RSA (Rivest, Shamir, Adleman). Desarrollado en 1977 en el MIT, popularizó los criptosistemas de clave pública. Está basado la factorización de números muy grandes, y es de libre distribución para claves de menos de 512 bits.

## Funciones *hash*

Una función *hash* acepta como entrada un mensaje M de longitud variable, y produce como salida un código de longitud fija, h=H(M), llamado resumen o huella digital. Este resumen es función de todos los bits del mensaje, y proporciona protección de errores, permitiendo asegurar que el mensaje no fue modificado y proporcionando por tanto garantía de integridad.

Una función *hash* debe tener las siguientes propiedades:

- Debe ser una función de un solo sentido: dado un documento es posible obtener siempre su resumen, pero dado un resumen, es prácticamente imposible deducir el documento original.
- Debe poder aplicarse a bloques de datos de cualquier tamaño.
- Debe producir una salida de longitud fija.
- Dos documentos electrónicos iguales producen la misma huella digital.
- Dos documentos parecidos producen huellas digitales completamente diferentes.
- Dos huellas digitales idénticas pueden ser el resultado de dos documentos electrónicos iguales o de dos documentos electrónicos completamente diferentes.
- Una función *hash* es irreversible, no se puede deshacer. Su comprobación se realiza aplicando la misma función *hash* al documento.
- H(x) debe ser fácil de calcular para cualquier x dado, de forma que tanto la implementación hardware como software sean prácticas.
- Para cualquier bloque "x", debe ser imposible computacionalmente encontrar un "y" tal que H(y)=H(x) (debe ser resistente a colisiones).
- Debe ser imposible computacionalmente encontrar un par (x,y) tal que H(x)=H(y). Conocido un mensaje y su función *hash*, debe ser imposible encontrar otro mensaje con la misma función *hash*. Esto debe cumplirse para evitar suplantaciones de identidad.

Las funciones *hash* se utilizan en los servicios de autenticación y firma digital para:

- No tener que cifrar todo el texto (el proceso de cifrado es más lento que en los algoritmos asimétricos, y el resumen también sirve para comprobar si la clave privada del emisor es auténtica).
- Comprobar automáticamente la autenticidad. Se compara el resumen realizado en el receptor con el resumen descifrado.
- Comprobar la integridad del texto. Si el texto ha sido alterado durante la transmisión, el resumen del texto recibido no coincidirá con el descifrado.

Las funciones *hash* más empleadas en criptografía son:

- MD5 (*Message Digest* 5, resumen del mensaje v5). Creado por Ron Rivest en 1992, genera un *hash* de 128 bits. Se ha utilizado en PGP, aunque hoy no se considera totalmente seguro.
- RIPEMD-160 (*RACE Integrity Primitives Evaluation-Message Digest*, evaluación de primitivas de integridad del proyecto RACE para MD). Es de los más rápidos, no está patentado y su código fuente es de libre acceso. Crea un resumen de 160 bits y por el momento está considerado como seguro.
- SHA-1 (*Secure Hash Algorithm*, algoritmo de *hash* seguro). Desarrollado en 1994 como parte del estándar de resumen seguro (SHS, *Secure Hash Standard*) y el estándar de cifrado digital (DSS, *Digital Signature Standard*), actualmente se le considera seguro. Es utilizado por PGP en sus claves DH/DSS (cifrado mediante Diffie Hellman y firmado mediante *hash* DSS).

## La firma electrónica

La firma electrónica se define, según ISO/IEC 7489/2, como los datos añadidos a un conjunto de datos, o transformación de éstos, que permiten al receptor probar el origen y la integridad de los datos recibidos, así como protegerlos contra falsificaciones.

Es por tanto un conjunto de datos asociados a un documento electrónico que permite garantizar la identi-

dad del firmante (autoría del documento) y la integridad del documento. Se emplean técnicas criptográficas basadas en criptosistemas asimétricos, tales que relacionan al documento firmado con información propia del firmante, permitiendo así que terceras partes puedan reconocer la identidad del firmante y asegurarse además de que los contenidos no han sido modificados.

Las firmas digitales pueden aportar por tanto 3 servicios de seguridad: autenticación, integridad (a diferencia de la manuscrita) y no repudio. Entre las características principales que debe cumplir la firma electrónica se encuentran:

- No ser falsificable.
- Ser capaz de verificar al autor.
- Ser capaz de autenticar los contenidos en el momento de la firma.
- Ser verificable por terceras partes, para resolver disputas.
- Ser un patrón de bits que dependa del mensaje completo a enviar. Nunca debe ser constante (para evitar ser cortada y pegada posteriormente en cualquier documento).
- Implicar la posesión por el emisor de alguna información exclusiva, para prevenir tanto la suplantación como el repudio.
- Ser relativamente sencillo producir la firma digital.
- Ser relativamente sencillo reconocer y verificar la firma digital.
- Ser imposible computacionalmente suplantar una firma digital, tanto por la construcción de mensajes nuevos a partir de una firma existente como por la construcción de una firma digital para un mensaje determinado.
- Ser posible y practicable el almacenamiento de una firma digital en un medio de almacenamiento.

La firma electrónica requiere de un conjunto de características técnicas (procedimientos técnicos de creación y verificación de firma) y normativas (existen documentos normativos que respaldan el valor legal de la firma).

Para firmar electrónicamente un documento, el firmante genera una huella digital del documento, y cifra la huella con su propia clave privada. El resultado, la huella digital firmada, es denominada firma digital o firma electrónica, y se envía adjunto al documento original, constituyendo una marca única para el documento y que sólo el firmante es capaz de producir.

Para la verificación de la firma, el receptor genera la huella digital del mensaje recibido aplicando la misma función *hash*. Por otro lado, descifra la firma digital del documento (que es el *hash* del documento, firmado con la clave privada del emisor) utilizando la clave pública del firmante, obteniendo la huella digital del documento original. Si coinciden ambas huellas digitales, el mensaje no fue alterado y el firmante es quien dice ser.

Por tanto, firmar un documento electrónicamente consiste en cifrar un resumen de dicho documento con la clave privada del remitente (ya sea persona o entidad). El destinatario verifica la firma utilizando la clave pública del remitente.

Como en todo criptosistema de clave pública, la vinculación entre las claves biunívoca: no hay dos claves privadas que se correspondan con una misma clave pública o viceversa. Tampoco pueden ser elegidas al azar, existiendo algoritmos para generar este par de claves. Asimismo, conociendo una de las claves, su algoritmo de generación, y/o documentos firmados con alguna de ellas, no es posible deducir la otra, e igualmente la información cifrada con una de las claves sólo puede ser descifrada con la otra.

La firma electrónica por sí misma no implica asegurar la confidencialidad del documento: un documento firmado electrónicamente puede ser visualizado por otras personas (al igual que ocurre con la firma manuscrita). Por ello, con frecuencia se emplea la firma electrónica en criptosistemas mixtos, generando lo que se denomina un sobre digital.

El sobre digital es la unión de un documento (o de manera más óptima, del documento con la firma electrónica asociada) cifrado simétricamente y una clave de sesión cifrada asimétricamente con la clave pública del receptor. El receptor descifra la clave sesión con su clave privada, y con la clave de sesión obtenida descifra el documento.

Así, mediante el sobre digital se aporta confidencialidad a todo el proceso, conjugando la velocidad y robustez de los criptosistemas simétricos con la facilidad de gestión de los sistemas asimétricos, y permitiendo además una gran versatilidad para los envíos multidestino (no es necesario cifrar *n* veces el documento original, solo cifrar *n* claves simétricas con la llave pública de cada destinatario).

La firma electrónica es regulada por primera vez en España en el RD Ley 14/1999 de 17 de septiembre sobre firma electrónica, hoy derogada y sustituida por Ley 59/2003 de 19 de diciembre. Se regula su efi-

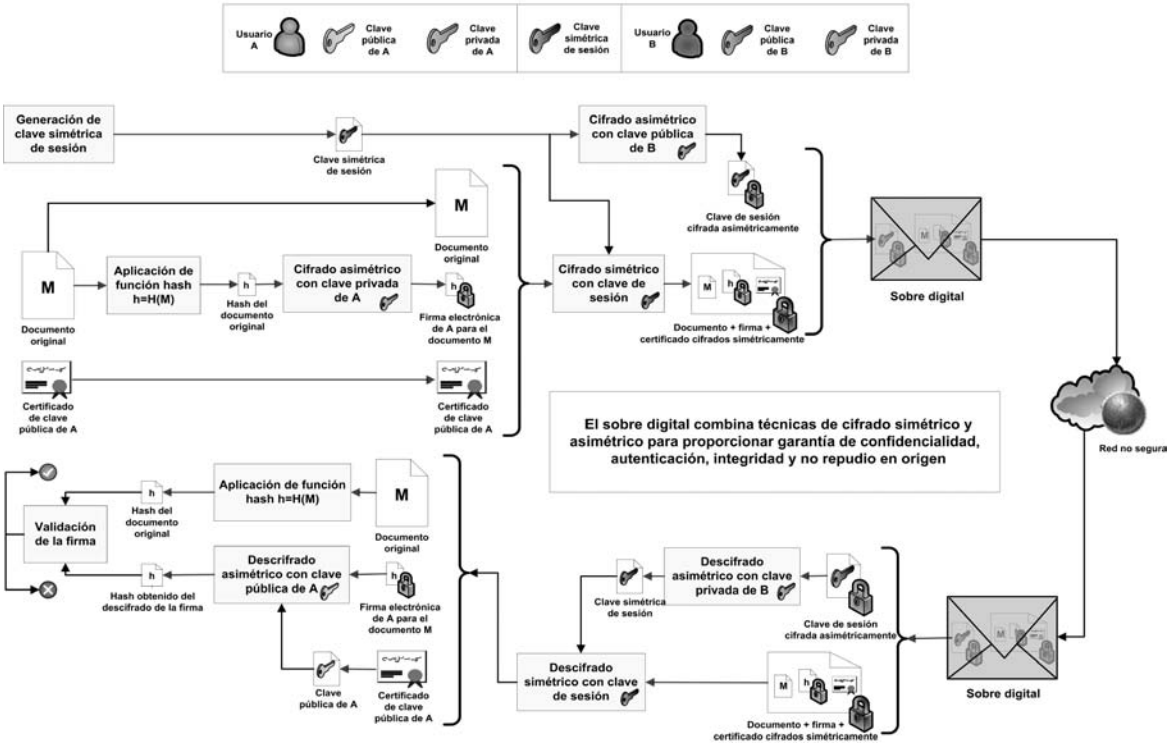


*Figura 2. Esquema completo de uso de la firma electrónica y el sobre digital.*

cacia jurídica y la prestación de servicios de certificación. Esta ley a su vez responde a la Directiva 1999/93/CE del Parlamento Europeo (13 de diciembre), marco comunitario para la firma electrónica. Dicha directiva otorga (cumpliendo unos requisitos mínimos en relación con los certificados, prestadores de servicios de certificación y dispositivos de creación de firma) eficacia jurídica equivalente a las firmas electrónica y manuscrita.

De acuerdo a la Ley 59/2003 existen 3 tipos de firma:

- Firma electrónica: conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
- Firma electrónica avanzada. Firma electrónica que además:
  - Permite detectar cualquier cambio ulterior de los datos firmados.
  - Está vinculada al firmante de manera única y a los datos a los que se refiere.
  - Ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- Firma electrónica reconocida. Firma electrónica avanzada que además:
  - Está basada en un certificado reconocido.
  - Ha sido generada mediante un dispositivo seguro de creación de firma.

La firma electrónica reconocida es la única que tiene respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita respecto de los datos consignados en papel.

Un dispositivo de creación de firma electrónica es un programa o sistema informático que sirve para aplicar los datos de creación de firma (por ejemplo, clave privada). Igualmente, un dispositivo de verificación de firma electrónica es un programa o sistema informático que sirve para aplicar los datos de verificación de firma (por ejemplo, clave pública).

## Certificados digitales. Infraestructuras de clave pública

La firma electrónica aporta importantes funcionalidades de autenticación, no repudio e integridad, pero por sí sola hay dos problemas que no es capaz de resolver:

- La firma digital permite comprobar la relación existente entre un mensaje y la clave secreta utilizada para realizar la firma, pero se necesita adicionalmente una garantía de la relación entre la clave utilizada y la identidad real del posee-

dor. Es decir, se necesita la seguridad de que la clave pública es propiedad realmente de quien dice poseerla.

- Debe poder accederse a todas las claves públicas necesarias para verificar cualquier mensaje.

Para solucionar estas cuestiones surgen las denominadas infraestructuras de clave pública (PKI, *Public Key Infrastructure*), y los certificados digitales como componente principal de las mismas.

Una PKI es el conjunto de aspectos técnicos (hardware, software, bases de datos) y normativos (leyes aplicables, estándares, procedimientos de seguridad) que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura utilizando criptosistemas de clave pública al realizar transacciones en redes (por ejemplo, Internet).

Los certificados digitales o certificados electrónicos son documentos electrónicos que dan fe de la vinculación entre una clave pública y un individuo o entidad, permitiendo verificar que una clave pública específica pertenece efectivamente a un individuo o entidad determinado.

De acuerdo a la Ley 59/2003, un certificado electrónico es un documento firmado electrónicamente (con su clave privada) por un prestador de servicios de certificación (entidad que hace las funciones de notario o tercera parte confiable) que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Los certificados, basados en su mayoría en el estándar ITU-T X.509v3, disponen de unos campos obligatorios y otros optativos. Entre los primeros se encuentran la versión, el número de serie del certificado (identificador único), el algoritmo identificador (algoritmo de firma, usualmente RSA o DSA), el emisor (nombre de la CA que crea y firma el certificado), el período de validez (fechas de inicio y fin de validez del certificado), el usuario (entidad propietaria de la clave certificada; suelen aparecer nombre, apellidos y DNI), la información de clave pública (clave pública del usuario) y la firma (código *hash* del resto de campos, cifrado con la clave privada de la CA).

Asimismo, un certificado reconocido es un certificado electrónico expedido por un prestador de servicios de certificación que cumpla los requisitos establecidos en Ley 59/2003 en cuanto a la comprobación de identidad y demás circunstancias de los solicitantes y en cuanto a la fiabilidad y las garantías de los servicios de certificación que presten. Deben incluir al menos la siguiente información:

- La indicación de que se expiden como tales.
- Código identificativo único del certificado.
- Identificación del prestador de servicios de certificación y su domicilio.
- Firma electrónica avanzada del prestador de servicios.
- Identificación del firmante mediante nombre, apellidos y DNI (si es persona física) o por razón social y CIF (si es entidad jurídica).
- Datos de verificación de firma que se correspondan a los datos de creación de firma que se encuentren bajo control del firmante.
- Comienzo y fin del período de validez del certificado.
- Límites de uso del certificado, si los hay.
- Cualquier otro atributo específico solicitado por el firmante.

Según su propósito, existen diversos tipos de certificado:

- Certificado personal, que acredita la identidad del titular.
- Certificado de pertenencia a empresa, que además de la identidad del titular acredita su vinculación con la entidad para la que trabaja.
- Certificado de representante, que además de la pertenencia a empresa acredita también los poderes de representación que el titular tiene sobre la misma.
- Certificado de persona jurídica, que identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones.
- Certificado de atributo, el cual permite identificar una cualidad, estado o situación (por ejemplo, la profesión del titular). Este tipo de certificado va asociado al certificado personal.
- Certificado de servidor seguro, utilizado en los servidores web que quieren proteger ante terceros el intercambio de información con los usuarios.
- Certificado de firma de código, para garantizar la autoría y la no modificación del código de aplicaciones informáticas.

Una autoridad de certificación (CA, *Certification Authority*, o prestador de servicios de certificación según Ley 59/2003) es por tanto una persona física o entidad jurídica pública o privada que expide certificados y actúa como tercera parte de confianza (TTP, *Trusted Third Party*) entre las personas u organizacio-

nes que intercambian mensajes utilizando la firma electrónica.

La clave pública de las CA más conocidas está incluida en los navegadores y en los sistemas operativos; en todo caso el usuario puede agregar manualmente las que necesite.

La CA efectúa labores de tutela y gestión permanente de los certificados electrónicos que expide, detalladas en la declaración de prácticas de certificación, donde se especifican condiciones aplicables a la solicitud, expedición, uso, suspensión, consulta de estado, y extinción de la vigencia de los certificados electrónicos. Emisor y receptor confían en los documentos firmados por la CA, en particular en los que identifican cada clave pública con su propietario correspondiente (certificado digital de clave pública).

Para ámbitos grandes, existe una jerarquía a nivel mundial de CA, de manera que se certifican unas a otras, existiendo en última instancia una CA raíz que es de confianza en todo el mundo. De esta manera se consigue una red de confianza en el uso por ejemplo de redes de ámbito global como Internet.

Una CA, además de emisión de certificados, presta servicios inherentes al propio certificado (revocación, suspensión en el caso de pérdida de clave, etc.) y complementarios (generación de claves, almacenamiento, servicio de sellado de tiempo o fechado electrónico, etc.).

La fecha electrónica o sellado de tiempo es el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en el que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.

Por su parte, la revocación de un certificado es la anulación de su validez antes de la fecha de caducidad que consta en el mismo. Tiene efectos a partir de la fecha efectiva de revocación que consta junto al número de serie del certificado revocado, en un documento firmado y publicado por la autoridad de certificación que se denomina lista de certificados revocados (CRL, *Certificates Revocation List*, idealmente, una CA emite a intervalos regulares una CRL firmada por ella misma). Firmas posteriores a esta fecha no tendrán validez.

Alternativamente a las CRL se utiliza la verificación en tiempo real mediante bases de datos en línea, mediente protocolos como OCSP (*Online Certificate Status Protocol,* protocolo de estado en línea del certificado) sobre HTTP.

Dentro de una PKI también es importante la misión de las autoridades de registro. Una autoridad de registro (RA, *Register Authority*) es una entidad autorizada por una CA cuya misión principal es identificar de forma inequívoca a los solicitantes de certificados, cumplimentar las solicitudes, y remitirlas a la CA para que proceda a la emisión de los mismos.

Existen 3 tipos de RA:

- Entidades colaboradoras: sirven de ayuda en la prestación de servicios de la CA.
- Entidades corporativas: solicitan un cierto número de certificados a la propia CA para ser utilizados dentro de su ámbito interno y con sus clientes.
- Entidades distribuidoras: empresas que distribuyen los certificados de las CA (por ejemplo, suministradores de tarjetas inteligentes que actúan de soporte físico del certificado).

En ocasiones, dentro de una PKI se considera como entidad independiente a la autoridad de validación (VA, *Validation* Authority), encargada de comprobar la validez de los certificados digitales. Igualmente, los servicios de sellado de tiempo pueden ser llevados a cabo por otra autoridad independiente denominada TSA (*Time Stamping Authority*). Aunque sí es frecuente encontrar RA como entidades independientes, es habitual no obstante que las CA se encarguen de estas tareas de validación y de sellado de tiempo.

Entre los datos que debe comunicar un prestador de servicios de certificación o CA se encuentran:

- Datos de identificación.
- Datos que permitan establecer comunicación con el prestador.
- Datos de atención al público.
- Características de los servicios que vayan a prestar.
- Certificaciones obtenidas para sus servicios.
- Certificaciones de los dispositivos que utilicen.
- Si son certificados reconocidos, además:
  - Protección de datos personales de los firmantes.
  - No deben almacenar ni copiar datos de creación de firma.
  - Información a los solicitantes: obligaciones del firmante, forma de custodia de datos de creación de firma, procedimiento de comunicación de incidencias, mecanismos para garantizar la fiabilidad de la firma en el tiempo, método para comprobar la identidad del

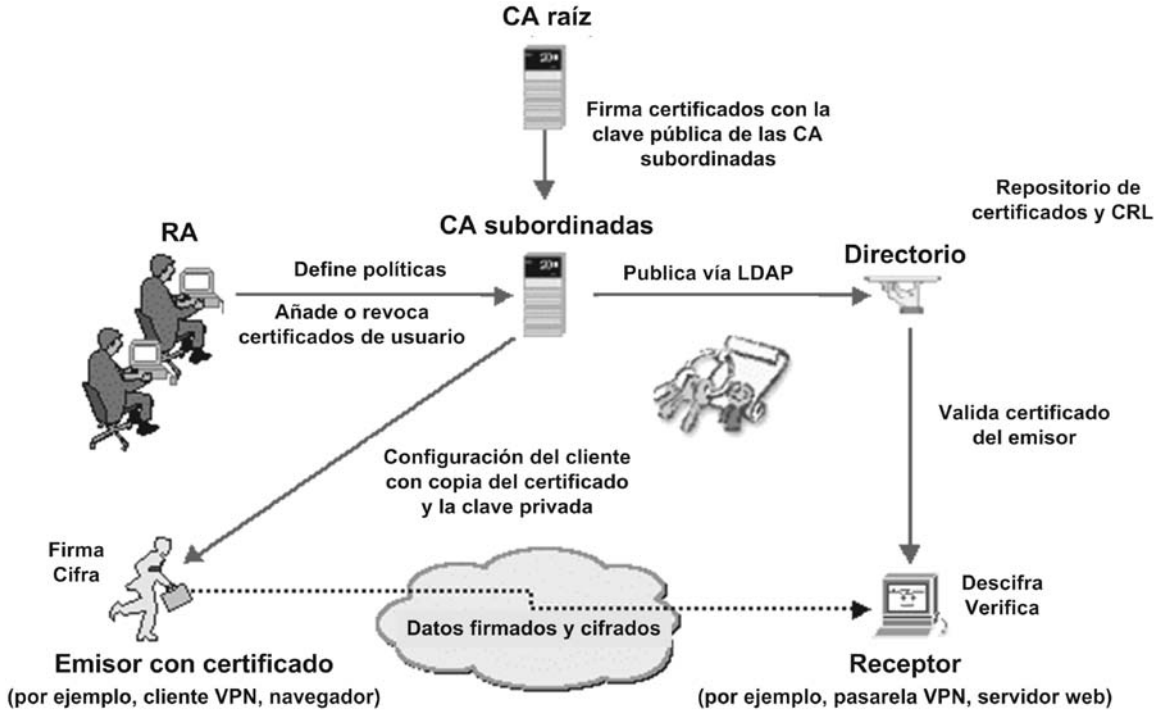


*Figura 3. Esquema general de funcionamiento de una PKI.*

firmante, condiciones de uso del certificado, certificaciones y procedimientos para resolución de conflictos, resto de información según declaración de prácticas.

- Deben mantener un directorio actualizado de certificados, indicando su vigencia.
- Deben disponer de un servicio de consulta.
- Deben disponer de una declaración de prácticas de certificación.

Por su parte, en la declaración de prácticas de certificación una CA debe incluir:

- Obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos.
- Condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados.
- Medidas de seguridad, técnicas y organizativas, perfiles y mecanismos de información sobre la vigencia de los certificados.
- Existencia en su caso de procedimientos de coordinación con registros públicos sobre la vigencia de los poderes indicados en los certificados.
- Requisitos exigidos por la Ley Orgánica de Protección de Datos.
- Si son certificados reconocidos:
  - Demostración de fiabilidad necesaria para prestación de servicios.
  - Empleo de personal cualificado.
  - Uso de sistemas y productos fiables que garanticen la seguridad técnica y criptográfica de los procesos de certificación.
  - Empleo de medidas contra la falsificación de certificados y garantía de confidencialidad de los datos de creación de firma.
  - Garantía de determinación con precisión de fecha y hora de expedición, extinción o suspensión de un certificado.
  - Registro en medio seguro de la información relativa a un certificado reconocido al menos durante 15 años desde expedición.
  - Uso de sistemas fiables para almacenar certificados reconocidos.
  - Seguro de responsabilidad civil.

En España, en la página web del MITYC puede encontrarse la relación de prestadores que han efectuado la comunicación prevista en el artículo 30.2 de Ley 59/2003:

PRESTADORES DE SERVICIOS DE CERTIFICACIÓN DE FIRMA ELECTRÓNICA

## Resultado de la Consulta

✓ **Servicios de certificación basados en certificados reconocidos**

| Prestadores |
|---|
| AC ABOGACÍA |
| ANCERT - Agencia Notarial de Certificación |
| ANF AC |
| Autoritat de Certificació de la Comunitat Valenciana - ACCV |
| BANESTO CA |
| CAMERFIRMA |
| CATCert |
| CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM) |
| CICCP |
| Dirección General de la Policía y de la Guardia Civil – Cuerpo Nacional de Policía |
| EDICOM |
| Firmaprofesional, S.A. |
| HEALTHSIGN, S.L. |
| Izenpe, S.A |
| Ministerio de Defensa de España |
| REGISTRADORES DE ESPAÑA |
| Santander |

✓ **Servicios de certificación basados en certificados no reconocidos**

| Prestadores |
|---|
| CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM) |
| Colegio Oficial de Arquitectos de Sevilla |
| ipsCA |
| Izenpe, S.A |
| Ministerio de Defensa de España |
| Servicio de Salud de Castilla-La Mancha (SESCAM) |
| Telefónica Empresas. |

✓ **Otros servicios en relación con la firma electrónica - Servicios de validación temporal**

| Prestadores |
|---|
| Autoritat de Certificació de la Comunitat Valenciana - ACCV |
| CAMERFIRMA |
| CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM) |
| EDICOM |
| Firmaprofesional, S.A. |
| Izenpe, S.A |
| Ministerio de Defensa de España |
| Tractis |

✓ **Otros servicios en relación con la firma electrónica - Servicios de validación de certificados**

| Prestadores |
|---|
| CertiVer |
| Tractis |

✓ **Otros servicios en relación con la firma electrónica - Servicios de custodia**

| Prestadores |
|---|
| CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM) |
| EDICOM |
| Tractis |

✓ **Otros servicios en relación con la firma electrónica - Otros servicios**

| Prestadores |
|---|
| CERES Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT-RCM) |
| EDICOM |
| Firmaprofesional, S.A. |

*Figura 4. Prestadores de servicios de certificación en España.*

## Aplicaciones de la firma electrónica

Las aplicaciones de la firma electrónica (y de los criptosistemas de clave pública en general) están directamente relacionadas con las funcionalidades criptográficas que proporciona su uso: identificación del firmante, integridad de los datos y no repudio en origen.

Si además de estas características se le añade la confidencialidad (usándola en combinación con claves privadas de sesión, habituales en conexiones SSL, VPN, etc.), la firma electrónica se convierte en un elemento fundamental para realizar operaciones electrónicas por redes no seguras. Particularmente, permite realizar operaciones por Internet que en la vida cotidiana requieren de una firma manuscrita para validarlas.

Algunos ejemplos de uso de la firma electrónica son:

- Comercio electrónico.
- Administración electrónica.
- Firma de correos electrónicos.
- Firma de facturas electrónicas.

Un caso especial particularmente interesante es la firma electrónica de personas jurídicas (sin intervención directa de una persona física), susceptible de ser utilizada en procedimientos automatizados: realización de pedidos, emisión de facturas, etc.

Una factura es un documento que refleja la entrega de un producto o la provisión de servicios, junto a la fecha de devengo, además de indicar la cantidad a pagar como contraprestación. Es así un justificante fiscal que afecta al obligado tributario emisor (vendedor) y al obligado tributario receptor (comprador). El original debe ser custodiado por el receptor de la factura, y el emisor conserva una copia o la matriz en la que se registra su emisión.

La factura electrónica por su parte consiste en la transmisión de las facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados cualificados, con la misma validez legal que las facturas emitidas en papel. Múltiples formatos admitidos siempre que incluyan todos los campos que legalmente debe incluir una factura.

Mención especial merece la Administración electrónica, que está siendo potenciada en España mediante la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y el RD 1671/2009, de 6 de noviembre, que la desarrolla. Mediante la aplicación de esta normativa se pone a disposición de los ciudadanos la posibilidad de interactuar con la Administración por medios telemáticos, como alternativa a los cauces tradicionales. Casos típicos de uso de la firma electrónica para interactuar con la Administración son la declaración de la renta o la solicitud de prestaciones sociales, aunque existen otros muchos trámites operativos.

En esquemas de comercio electrónico, la firma electrónica ayuda a prevenir fraudes y a establecer confianza en la interacción entre las distintas partes, especialmente en la comunicación con las pasarelas de pago y en la transmisión de datos personales y económicos.

Para ello se utilizan arquitecturas seguras, basadas en cifrados tanto simétricos como asimétricos, y con certificados tanto de las personas como de los servidores involucrados. Protocolos típicos usados en este caso son SSL (para comunicaciones cifradas), SET (*Secure Electronic Transactions*, para pasarelas de pago seguras) y las distintas implementaciones de monederos electrónicos existentes.

En España también es fundamental mencionar el DNI electrónico, evolución del DNI tradicional que permite el empleo también de firma electrónica para su uso en medios telemáticos. Aparece con el RD 1553/2005 de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica. Usando un dispositivo seguro de creación de firma, la firma electrónica efectuada mediante DNI electrónico tiene el mismo efecto que una firma manuscrita.

La Dirección General de Policía del Ministerio del Interior es la emisora de los certificados del DNI electrónico, actuando por tanto como CA (y también como RA). Como autoridades de validación se encuentran la Fábrica Nacional de Moneda y Timbre y el Ministerio de la Presidencia. La activación de la utilidad informática es de carácter voluntario para el ciudadano, mediante clave personal secreta. El DNI electrónico no incluye sistemas de cifrado ni de sellado de tiempo, lo que implica la existencia de terceras empresas prestadoras de servicios de valor añadido sobre la firma electrónica del DNIe.

La tarjeta física está diseñada acorde a ISO 7816-1, en policarbonato y personalizada con los datos de filiación y biométricos grabados en la tarjeta. El chip del DNI electrónico incluye 3 zonas con diferentes niveles y condiciones de acceso:

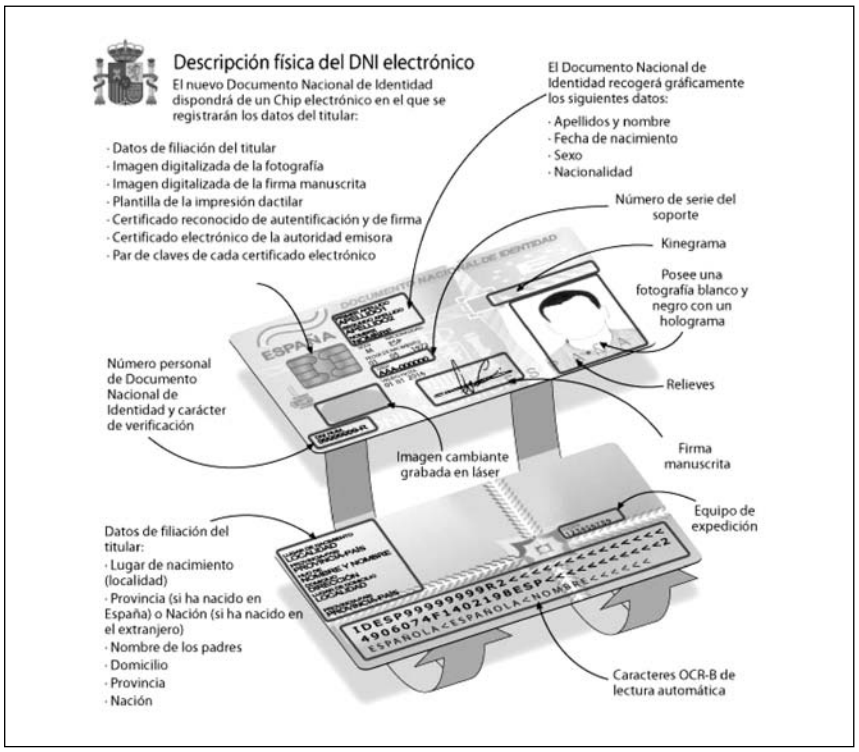


*Figura 5. Componentes del DNI electrónico.*

- Zona pública. Accesible en lectura sin restricciones:
  - Certificado CA intermedia emisora.
  - Claves Diffie-Hellman.
  - Certificado x509 de componente (para canal cifrado entre la tarjeta y los controladores del lector de DNIe).
- Zona privada. Accesible en lectura por el ciudadano, mediante la utilización de la clave personal de acceso o PIN:
  - Certificado de firma electrónica reconocida. Válido durante 30 meses. Permite realizar y firmar acciones y asumir compromisos de forma electrónica, pudiéndose comprobar la identidad de los documentos firmados por el ciudadano haciendo uso de los instrumentos de firma incluidos en él. Es equiparable a la firma manuscrita.
  - Certificado de autenticación. Válido durante 30 meses. El ciudadano podrá certificar su identidad frente a terceros, demostrando posesión y acceso a la clave privada asociada a dicho certificado y que acredita su identidad.
- Zona de seguridad. Accesible en lectura por el ciudadano, en los puntos de actualización del DNIe:
  - Datos de filiación del ciudadano (los mismos que están en el soporte físico).
  - Imagen de la fotografía.
  - Imagen de la firma manuscrita.
- Datos criptográficos. Claves de ciudadano (que se generan e insertan en el proceso de generación del DNI electrónico):
  - Clave RSA pública de autenticación.
  - Clave RSA pública de no repudio.
  - Clave RSA privada de autenticación.
  - Clave RSA privada de firma.
  - Patrón de impresión dactilar.
  - Clave pública de CA raíz.
  - Claves Diffie-Hellman.
- Datos de gestión:
  - Traza de fabricación.
  - Número de serie del soporte.