

## MF0489\_3: Sistemas Seguros de Acceso y Transmisión de Datos.



## Índice

Capítulo 1 Criptografía .....	7
1. Introducción.....	7
2. Perspectiva histórica y objetivos de la criptografía.....	7
2.1.- Fundamentos de criptoanálisis.....	10
3. Teoría de la información.....	10
3.1.- Cantidad de información. Concepto de entropía .....	11
3.2.- Estableciendo la seguridad de un sistema.....	11
3.3.- Redundancia y compresión óptima de datos .....	12
4. Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía: confidencialidad, integridad, autenticidad, no repudio, imputabilidad y sellado de tiempos .....	13
4.1.- Confidencialidad .....	13
4.2.- Integridad.....	13
4.3.- Autenticidad .....	14
4.4.- No repudio .....	15
4.5.- Imputabilidad.....	16
4.6.- Sellado de tiempo .....	16
5. Elementos fundamentales de la criptografía de clave privada y de clave pública .....	16
5.1.- Elementos fundamentales de la criptografía de clave privada .....	17
5.2.- Elementos fundamentales de la criptografía de clave pública .....	27
5.3.- Criptografía de clave pública, curvas elípticas.....	31
6. Características y atributos de los certificados digitales.....	31
7. Identificación y descripción del funcionamiento de los protocolos de intercambio de claves usados más frecuentemente .....	32
7.1.- Protocolo Diffie-Hellman .....	32
8. Algoritmos criptográficos más frecuentemente utilizados .....	33
8.1.- Algoritmos de criptografía de clave secreta .....	33
8.2.- Algoritmos de criptografía de clave pública .....	37
8.3.- Algoritmos híbridos .....	38
8.4.- Robustez y eficiencia práctica de los algoritmos.....	39
9. Elementos de los certificados digitales, los formatos comúnmente aceptados y su utilización	41

9.1.- Certificados X.509 .....	41
9.2.- Certificados PGP .....	42
10. Elementos fundamentales de las funciones resumen y los criterios para su utilización .....	44
10.1.- Funciones resumen con clave.....	46
11. Requerimientos legales incluidos en la ley 59/2003, de 19 de diciembre, de firma electrónica.....	46
12. Elementos fundamentales de la firma digital, los distintos tipos de firma y los criterios para su utilización.....	48
12.1.- Elementos fundamentales. Esquema básico .....	48
12.2.- Tipos de firma y criterios de uso.....	49
13. Criterios para la utilización de técnicas de cifrado de flujo y de bloque .....	49
14. Protocolos de intercambio de claves .....	50
14.1.- Intercambio de claves secretas mediante criptografía simétrica .....	50
14.2.- Intercambio de claves secretas mediante criptografía asimétrica.....	51
14.3.- Intercambio de claves secretas mediante criptosistemas híbridos .....	52
14.4.- Intercambio de claves públicas.....	52
15. Uso de herramientas de cifrado tipo PGP, GPG o CryptoLoop.....	54
15.1.- Creación del certificado .....	55
15.2.- Uso del certificado para cifrar .....	58
15.3.- Descifrando un fichero recibido .....	60
16. Resumen.....	62
Capítulo 2 Aplicación de una infraestructura de clave pública (PKI) .....	63
1. Introducción.....	63
2. Identificación de los componentes de una PKI y su modelo de relaciones .....	63
2.1.- Entidades participantes .....	63
2.2.- Modelo de relaciones .....	65
2.3.- Arquitecturas de una PKI .....	67
3. Autoridad de certificación y sus elementos .....	70
3.1.- Funciones de gestión .....	70
3.2.- Validación de una cadena de certificación .....	71
3.3.- Aspectos prácticos: validación en los navegadores .....	72
4. Política de certificado y declaración de prácticas de certificación (CPS) .....	74

4.1.-	Política de certificación.....	74
4.2.-	Declaración de prácticas de certificación .....	75
4.3.-	Diferencias entre política de certificación y declaración de prácticas de certificación ..	76
4.4.-	Provisiones: política de certificación y declaración de prácticas de certificación .....	76
5.	Lista de certificados revocados (CRL) .....	77
5.1.-	Formato de una lista de revocación de certificados .....	78
5.2.-	Concepto de Delta CRL .....	79
5.3.-	Online Certificate Status Protocol (OCSP) .....	79
6.	Funcionamiento de las solicitudes de firma de certificados (CSR).....	80
7.	Infraestructura de gestión de privilegios (PMI).....	81
7.1.-	Entidades participantes .....	81
7.2.-	Aplicación de PMI para el control de acceso.....	83
7.3.-	Comparación con respecto a una PKI .....	84
8.	Campos de certificados de atributos, incluyen la descripción de sus usos habituales y la relación con los certificados digitales .....	85
8.1.-	Usos habituales de los certificados de atributos.....	86
8.2.-	Certificados digitales frente a certificados de atributos .....	87
9.	Aplicaciones que se apoyan en la existencia de una PKI.....	89
9.1.-	Uso de PKI para autenticación.....	89
9.2.-	Uso de PKI en firma .....	89
9.3.-	Uso de PKI para cifrado.....	93
10.	Resumen.....	93
	Capítulo 3 Comunicaciones seguras .....	94
1.	Introducción.....	94
2.	Definición, finalidad y funcionalidad de redes privadas virtuales.....	94
2.1.-	Conceptos previos. El modelo OSI .....	94
2.2.-	Descripción de las VPN .....	97
2.3.-	Ventajas y desventajas de las VPN .....	99
3.	Protocolo IPSec .....	99
3.1.-	Internet Key Exchange (IKE).....	100
3.2.-	Escenarios de uso .....	101

3.3.-	Encapsulating Security Payload (ESP) .....	102
4.	Protocolos SSL y SSH .....	103
4.1.-	Secure Sockets Layer (SSL) .....	103
4.2.-	Secure Shell (SSH) .....	106
5.	Sistemas SSL VPN .....	109
5.1.-	Tipos de SSL VPN .....	110
6.	Túneles cifrados .....	112
6.1.-	Point-to-Point Tunneling Protocol (PPTP) .....	112
6.2.-	Layer 2 Tunnelling Protocol (L2TP) .....	113
6.3.-	Datagram Transport Layer Security (DTLS) .....	114
7.	Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN	115
7.1.-	Pros y contras de IPSec VPN .....	115
7.2.-	Pros y contras de SSL VPN .....	116
7.3.-	Ánalisis de costes .....	116
8.	Resumen .....	116

## CAPÍTULO 1 CRIPTOGRAFÍA

### 1. INTRODUCCIÓN

Según la Real Academia Española, la criptografía es el "arte de escribir con clave secreta o de un modo enigmático". Tal y como muestra la definición, su existencia ha estado siempre ligada al mantenimiento de los secretos.

Desde la Antigüedad hasta nuestros días, numerosos protocolos y mecanismos criptográficos han ido desarrollándose. El avance de la tecnología y, particularmente, de los ordenadores, ha permitido que los algoritmos que se utilicen en la actualidad sean muy sofisticados y ofrezcan así una fuerte resistencia contra los atacantes.

En los últimos tiempos se han desarrollado, además, nuevos mecanismos que no pretenden mantener en secreto el mensaje, sino que se centran en dotarlo de autenticidad, identificar a quien lo envía, asegurar quién y cuándo lo recibe o verificar que no ha sido modificado.

Este capítulo comienza proporcionando una visión general de la Historia de la Criptografía. Posteriormente, se dan las nociones básicas relacionadas con esta disciplina y se describen las características principales de los procedimientos que permiten alcanzar los fines citados en el párrafo anterior. También se aborda el actual marco legal de la firma electrónica en España, con lo que se describen las condiciones para utilizarlo y las consecuencias asociadas.

### 2. PERSPECTIVA HISTÓRICA Y OBJETIVOS DE LA CRIPTOGRAFÍA

La criptografía es una parte de la disciplina encargada del estudio de la escritura secreta o criptología. La criptografía estudia las técnicas aplicadas a la protección de la información, evitando que pueda ser comprometida por un atacante. Desde la Antigüedad hasta nuestros días ha sufrido una extraordinaria evolución. En esta sección se efectúa un breve repaso de la historia, mostrando cómo ha sido la evolución de las propuestas a lo largo de los tiempos. En los siguientes capítulos se entra en mayor detalle sobre los sistemas más representativos.

Uno de los primeros ejemplos de mecanismo criptográfico fue la escíitala, que data del siglo IV antes de Cristo. Como muchos otros sistemas que posteriormente se desarrollarían, el objetivo de este sistema era cifrar la información, es decir, hacer incomprendible el contenido del mensaje a terceros no autorizados. Esencialmente, se trata de un bastón de madera con un diámetro concreto. Para cifrar un texto, bastaba con enrollar una tira a lo largo del bastón y escribir en ella el mensaje. Posteriormente, se desenrollaba la tira para transportarla a su destinatario. El mensaje resultaba ininteligible para cualquiera que no tuviese un bastón del mismo diámetro. La técnica subyacente a la escíitala es la transposición, que consiste en cambiar el orden en el que los caracteres aparecen en el texto.

#### Nota

Es preciso usar con cuidado el término "cifrar" y no confundirlo con "codificar". Esencialmente, siempre que se cifra se hace uso de una clave, al contrario que al codificar.

Aproximadamente tres siglos más tarde surge uno de los métodos de cifrado clásico más conocidos: el cifrado de César. En este sistema, cada una de las letras del mensaje era sustituida por la situada tres posiciones más adelante en el alfabeto. Así, la letra "C" del mensaje original era sustituida por la "F". Con él surge una completa familia de sistemas de cifrado denominados sistemas por sustitución monoalfabética. La característica de estos sistemas es que cada letra del mensaje original se sustituye siempre por una misma letra.

Uno de los mayores inconvenientes de los sistemas de sustitución monoalfabéticos es que la frecuencia de aparición de los caracteres no varía tras el cifrado. Siguiendo el ejemplo anterior, el texto 'CORRER' resultaría en 'FRUUHU~' Teniendo en cuenta que se conoce cuáles son las letras más y menos frecuentes para cada idioma, el criptoanálisis del texto (es decir, la obtención del mensaje original a partir del cifrado) resulta razonablemente sencillo.

Para evitar esta circunstancia, en el siglo XV después de Cristo se desarrollaron otros sistemas de cifrado: los cifradores por sustitución polialfabéticos. En ellos, cada letra no siempre se sustituye por otra fija, sino que la sustitución depende de la posición de la original en el texto. Uno de los más conocidos es el cifrado de Vigenere, en el que se utiliza una palabra como clave.

Cada letra del mensaje se suma a la que aparece en la posición correspondiente de la clave. Por ejemplo, las letras 'a' (posición 1 del alfabeto) y 'e' (posición 3) se sumarían resultando en la 'd' (posición 4). Si la clave es más corta que el mensaje a transmitir, la propuesta clásica de Vigenere especifica que la clave debe repetirse tantas veces como sea necesario.

#### Nota

Si la suma resulta en un valor mayor que el alfabeto, se comienza nuevamente por el principio. Así, si el alfabeto contiene 28 letras, 'y' (posición 27) + 'd' (posición 4) = 'e' (posición 31-28=3). A esta parte de la matemática se la conoce como aritmética modular.

Los siglos posteriores darían lugar a la creación de sofisticados sistemas de cifrado. Por su relevancia histórica, es necesario detenerse en el cifrado de la máquina Enigma, cuya invención data del año 1918. Esta máquina fue empleada por el ejército alemán en la Segunda Guerra Mundial. Se trata de una máquina compuesta por varios rotores (o ruedas dentadas), cada uno de los cuales dispone de 26 dientes. Cada diente representa la correspondencia entre el carácter de entrada y el de salida. Por cada letra del mensaje original que se cifrase, se giraba el rotor una posición. Cada vez que un rotor completaba una vuelta, el de su izquierda se movía una posición.

Este sistema es mucho más complejo que los anteriores, ya que las combinaciones posibles son muchas más.

Los sistemas descritos hasta el momento forman la familia de cifradores de clave privada. Esto es debido a que ambos comunicantes (emisor y receptor) debían disponer de la misma clave para acceder al contenido del mensaje. Por ello, se necesitaba un canal seguro por el que distribuir

previamente dicha clave. Para evitar esto, en 1976 los investigadores Whitfield Diffie y Martin Hellman propusieron un sistema para establecer una clave compartida a través de un canal inseguro.

Poco tiempo más tarde surgiría una aproximación completamente distinta a lo anterior: la criptografía de clave pública. En 1978, Ron Rivest, Adi Shamir y Leonard Adelman publicaron el sistema RSA. Dicho sistema, como cualquier otro de clave pública, asume que cada comunicante dispone de un par de claves. En dicho par, una es conocida por todos (pública) mientras que la contraria es privada y solo conocida por el poseedor. Para realizar una operación (ej. cifrado) y aquella que la revierte (ej. descifrado) se emplean claves distintas. Particularmente, para cifrar un mensaje se emplea la clave pública del receptor, mientras que el descifrado se realiza utilizando la privada.

En la actualidad se están desarrollando mecanismos basados en criptografía de curvas elípticas, cuya ventaja fundamental es su extrema rapidez. En lo referente al futuro próximo, la criptografía cuántica plantea un escenario totalmente revolucionario en el que los mensajes intercambiados se corresponderían con fotones (elemento constituyente de la luz), los cuales no pueden ser observados sin ser eliminados o modificados.

Además del objetivo de conseguir que el mensaje no sea conocido por terceras partes no autorizadas, los sistemas criptográficos han perseguido también otras metas. Entre ellas se destacan la identificación de las entidades participantes, el aseguramiento de que una cierta información es auténtica y no ha sido modificada y la prevención de que una entidad pueda negar que realizó una cierta acción.

Finalmente cabe destacar el uso de la esteganografía. A diferencia de la criptografía, el mensaje se oculta de modo que pase desapercibido para los usuarios que no sean los destinatarios del mismo. Un ejemplo sencillo es la construcción de un texto legible en el que, por ejemplo, uniendo la primera letra de cada palabra se transmita el mensaje deseado. Sin embargo, las técnicas son muy variadas. Por ejemplo, se puede hacer uso de tinta invisible para, únicamente aplicando calor o sustancias químicas, conseguir visualizar el texto o las marcas realizadas. Otro ejemplo es la realización de pequeños agujeros cerca de las letras escogidas, de modo que solo situando el documento enfrente de un foco de luz los agujeros puedan identificarse y con ello obtener el mensaje. En la actualidad, la esteganografía también puede aplicarse en todo tipo de documentos electrónicos. Uno de los ejemplos más comunes es la aplicación de la esteganografía en imágenes, basada en los cambios de tono. No todos los tonos de colores son perceptibles para el ojo humano. Debido a ello, es posible cambiar los tonos de algunos de los píxeles (es decir, partes mínimas que componen una imagen) sin que se note, y asociando un significado (partes del mensaje oculto) al nuevo color escogido. En relación con la criptografía, la esteganografía presenta múltiples inconvenientes. Por un lado, muchos esquemas son poco eficientes.

Por ejemplo, se necesitan muchas palabras para enviar un mensaje oculto largo utilizando el método de escoger la primera letra de las palabras. Además, cuando el sistema se descubre deja de ser útil. No obstante, si el mensaje que se oculta se cifra previamente, el atacante podrá detectar el mensaje pero éste estará cifrado. Por otro lado, la esteganografía presenta la gran ventaja de que el mensaje pasa desapercibido para el atacante. Debido a esta característica, un

atacante no solo necesita saber cuál es el mensaje en el que hay datos ocultos, sino también la técnica esteganográfica utilizada.

### 2.1.- Fundamentos de criptoanálisis

De acuerdo a la Real Academia Española, el criptoanálisis es el "arte de descifrar criptogramas". Esta definición afecta exclusivamente a los sistemas criptográficos centrados en el cifrado, aunque en la actualidad es común considerar que esta disciplina persigue frustrar el uso de cualquier mecanismo criptográfico.

El criptoanalista trata de adivinar el funcionamiento de un mecanismo criptográfico para poder predecir cuál será el resultado sobre cualquier mensaje. Por ello, para estudiar un sistema habitualmente lo considera como una caja negra que produce una salida a partir de una entrada.

La tarea del criptoanalista es distinta en función de los materiales de los que disponga. Así, la situación más desfavorable se produce cuando solo dispone de la salida del sistema, pero no de su entrada. Si conoce parte de la entrada (es decir, del texto en claro), se denomina "criptoanálisis de texto en claro conocido" y, si ha podido escoger dicha entrada, se conoce como "criptoanálisis de texto en claro escogido". Para los cifradores, también es posible realizar el criptoanálisis a la inversa, denominado "de texto cifrado escogido" en el que se escoge el resultado de cifrar y se conoce el descifrado correspondiente.

## 3. TEORÍA DE LA INFORMACIÓN

La Teoría de la información fue planteada por Claude E. Shannon en 1948. Dicha teoría se relaciona con los límites que se pueden alcanzar en la transmisión de datos sin errores y en la compresión de los mismos. El impacto de dicha teoría es evidente en el campo de la criptografía, donde la transmisión de mensajes entre dos o más entidades es la base de muchos algoritmos criptográficos. Con ello, es posible estimar la robustez y seguridad que ofrece un determinado mecanismo.

### Definición

#### Algoritmo

Una secuencia ordenada y finita de pasos u operaciones que contribuyen a resolver un problema.

Si un canal de comunicación (por ejemplo, Internet) tiene pérdidas de datos o no siempre llegan correctamente, parece claro que no es posible enviar cualquier cantidad de información a cualquier velocidad. En realidad, el canal presentará una máxima capacidad efectiva de transmisión de información, tal y como demostró el citado investigador.

Pero la capacidad del canal no es el único aspecto relevante de la teoría de la información.

También se aborda la cantidad de información que contiene un mensaje. En este apartado se presentan estos conceptos junto con las nociones básicas de probabilidad que se requieren para comprenderlos.

### 3.1.- Cantidad de información. Concepto de entropía

Véase la situación siguiente. Se está formando el coro de una clase de instituto, para el que se escogerán aleatoriamente cuatro alumnos de la misma. Dicha clase está compuesta por ocho alumnos y dos alumnas.

La primera persona escogida es una alumna. Intuitivamente, la información que se obtiene del suceso es que para las próximas selecciones solo queda una alumna frente a ocho alumnos.

Yendo más allá, si la siguiente persona elegida es la alumna restante, ya se sabe que los siguientes seleccionados serán alumnos. Parece claro que la incertidumbre asociada a cada uno de los eventos es extraordinariamente distinta. La entropía es, precisamente, una magnitud que permite medir esa incertidumbre (o aleatoriedad) y, con ello, la cantidad de información de un determinado mensaje.

#### Nota

Si se consultan otras fuentes de información, es posible que utilicen la notación  $H(X)$  para referirse a la entropía.

La entropía es mayor cuanto mayor sea el grado de incertidumbre. En el caso de la clase anterior, la probabilidad de ser chico es de 8 sobre 10, mientras que de ser chica es de 2 sobre 10. Sin embargo, si la clase tuviera nueve alumnos y una alumna, la entropía decaería notablemente al disminuirse el nivel de incertidumbre: intuitivamente, "casi todos son alumnos".

### 3.2.- Estableciendo la seguridad de un sistema

El concepto de entropía anterior mide la incertidumbre de un evento. Dando un paso más allá, otra cuestión que puede resultar de interés es medir la incertidumbre que el conocimiento de un evento aporta sobre otro. En el terreno de la criptografía, una aplicación clave de esta medida es en la seguridad de un sistema: conociendo la salida de una determinada función criptográfica, ¿qué información se puede deducir acerca de la entrada? Parece claro que la seguridad de un sistema criptográfico (por ejemplo, de cifrado), será mayor si la información que se deduce sobre la entrada a partir de la salida es pequeña o nula.

En el marco de la Teoría de la información, Shannon determinó que un sistema se considera incondicionalmente seguro si no se obtiene ninguna información sobre la entrada obtenida a

partir de la salida. En la práctica, se trata de una condición muy difícil de satisfacer y, de hecho, solo el cifrador de Vernam, que se verá más adelante, cumple esta condición.

**Nota**

Los sistemas incondicionalmente seguros, según la Teoría de la información de Shannon, también reciben el nombre de cripto-sistemas ideales. A pesar de su robustez teórica, su aplicación resulta impráctica.

Los sistemas incondicionalmente seguros, según la Teoría de la información de Shannon, también reciben el nombre de cripto-sistemas ideales. A pesar de su robustez teórica, su aplicación resulta impráctica.

### 3.3.- Redundancia y compresión óptima de datos

Tal y como se ha visto en los apartados anteriores, la Teoría de la información permite medir la cantidad de información que proporciona un determinado suceso. En base a estas mediciones y particularmente al concepto de entropía, esta teoría se aplica a dos cuestiones relacionadas con la calidad de la información: la redundancia (es decir, la repetición de ciertas partes del mensaje) y la compresión de los datos. Ambas serán clave para mejorar la eficiencia de la transmisión de información.

En lo referente a la **redundancia**, lo deseable sería eliminarla antes de la transmisión para que esta fuese más corta. Sin embargo, algunos canales de comunicación no están libres de errores y, por tanto, pueden producirse pérdidas o alteraciones de la información enviada.

Teniendo en cuenta lo anterior, es necesario establecer un equilibrio entre la eficiencia de la comunicación y la redundancia introducida. Con este fin se desarrollaron los Códigos de Redundancia Cíclica (CRC). Estos permiten añadir al mensaje una pequeña porción (idealmente mínima), asegurando que proporcionan una alta redundancia. Es importante tener en cuenta que los CRC no pueden utilizarse como mecanismo para comprobar si un mensaje ha sido manipulado. Dado que el cálculo del CRC es público y solo depende del mensaje, un atacante podría alterar el mismo y calcular el CRC correspondiente, con lo que no podría detectarse la modificación.

**Nota**

La cantidad de información redundante que debe añadirse depende en buena medida de la calidad del canal. Si la probabilidad de pérdida es mayor, se recomienda usar un CRC de mayor longitud.

La cantidad de información redundante que debe añadirse depende en buena medida de la calidad del canal. Si la probabilidad de pérdida es mayor, se recomienda usar un CRC de mayor longitud.

En lo referente a la compresión de datos, la información proporcionada por la entropía resulta de gran interés. Si, por ejemplo, la salida de un cifrador tiene una alta entropía, se puede decir que existe un gran grado de desorden o, lo que es lo mismo, que hay gran aleatoriedad entre los valores que puede tomar esa salida. Esta situación es la peor desde el punto de vista de la compresión, pues todos los datos son útiles o necesarios. Por el contrario, una baja entropía es indicativa de uniformidad y, por tanto, es posible que haya patrones de valores de la salida que se repitan a lo largo del tiempo.

#### **4. PROPIEDADES DE LA SEGURIDAD QUE SE PUEDEN CONTROLAR MEDIANTE LA APLICACIÓN DE LA CRIPTOGRAFÍA: CONFIDENCIALIDAD, INTEGRIDAD, AUTENTICIDAD, NO REPUDIO, IMPUTABILIDAD Y SELLADO DE TIEMPOS**

La seguridad de la información tiene como objetivo el establecimiento de medidas que controlen, mitiguen o prevengan distintos problemas de seguridad a los que un sistema puede enfrentarse, como pueden ser el acceso a datos no autorizados o la recepción de datos maliciosamente modificados. Por ello, se ha de estudiar cuáles son las propiedades objetivo de la criptografía, cuáles son las amenazas para cada una y los mecanismos que existen para paliarlas.

Estos aspectos se introducen a continuación.

##### **4.1.- Confidencialidad**

La información ha de permanecer secreta desde el origen hasta ser recibida por destinarios autorizados. Actualmente, dada la cantidad de información intercambiada digitalmente, la confidencialidad de los datos juega un papel fundamental. En este contexto, el cifrado es uno de los mecanismos de prevención más utilizados. Si los datos están cifrados desde el origen con una determinada clave, solo el que tenga disposición de la clave de descifrado podrá obtener la información, satisfaciéndose así esta propiedad.

Son muchas las amenazas que atentan contra la confidencialidad. Un ejemplo es el *software maligno* que se ejecute en el ordenador del emisor y cambie las claves de cifrado. Otro ejemplo es la ingeniería social, que se basa en engañar a los usuarios para conseguir información confidencial.

##### **4.2.- Integridad**

La información ha de permanecer inalterable desde el origen al destino, donde inalterable significa exacta y completa. De este modo, la integridad garantiza que los datos recibidos son exactamente los mismos que fueron enviados. Nuevamente la aplicación de técnicas criptográficas es uno de los

principales mecanismos de prevención de amenazas contra la integridad; en concreto, se aplican funciones resumen, que se explican más adelante.

Una de las amenazas más conocidas que atentan contra esta propiedad es la modificación de la información. Esta puede realizarse, por ejemplo, a través de un **ataque de hombre en el medio** (*man-in-the-middle*). Este ataque se basa en colocar a un atacante entre el origen y el destino al que se envía esta información, de modo que dicho atacante consiga, en este caso, modificar la información enviada.

#### 4.3.- Autenticidad

Esta propiedad afecta tanto al mensaje como a las entidades participantes. Autenticidad del mensaje se corresponde con recibir exactamente la misma información que fue enviada. Por otro lado, la autenticación de una entidad se corresponde con determinar que una entidad es quien dice ser.

Una de las técnicas utilizadas para satisfacer la autenticidad de los mensajes es la utilización de cifrado, códigos de autenticación de mensaje o funciones resumen. Por otro lado, una técnica muy utilizada para autenticar a las entidades es la firma, que se explica más adelante.

Hay distintos tipos de firmas y no todas ellas tienen la misma validez legal ni satisfacen las mismas propiedades. Sin embargo, la autenticidad sí es considerada en las formas más avanzadas y legalmente definidas. Dentro de las amenazas frente a la autenticación de entidades se puede subrayar la suplantación. En ella, un atacante consigue actuar en nombre de la entidad legítima (por ejemplo, tomando el control de su ordenador).

La autenticación de entidades puede basarse en distintos factores: en algo que se conoce, como son las contraseñas; algo que se tiene, como son las tarjetas electrónicas o los USB; algo que se es, es decir, rasgos biométricos como la huella dactilar o el iris de los ojos; o una combinación de cualquiera de las anteriores.

Según los estándares ITU-T X.509 e ISO/IEC 9594-8, la autenticación de entidades puede ser simple (basada en contraseñas), o fuerte (basada en la prueba de posesión de una clave privada tras establecer un algoritmo de cifrado y estar en posesión de las claves de cifrado/descifrado adecuadas). Suponiendo que una entidad A desea autenticarse ante una entidad B, se describen los modos de autenticación:

- **Autenticación simple:** A envía a B un mensaje con su identificación, una marca de tiempo, un número aleatorio y el resultado de aplicar una función de un único sentido (por ejemplo, las funciones resumen del Apartado 10) a dichos datos. Posteriormente, B envía un mensaje de confirmación o rechazo.

Definición: Función de único sentido: función con la propiedad de ser fácil de calcular un resultado Y para una entrada X pero difícil de obtener X a partir de Y.

- **Autenticación fuerte unidireccional:** se basa en el envío de un único mensaje entre A y B, de modo que la segunda autentique a la primera. A envía su identidad, la marca de tiempo, el número aleatorio, la identidad de B y la firma electrónica (que se verá más adelante) sobre estos datos.
- **Autenticación fuerte bidireccional:** se trata de una variante del anterior en la que cada entidad envía un mensaje firmado, de contenido similar al ya explicado. En este caso, se consigue que ambas entidades queden autenticadas frente a su interlocutor.
- **Autenticación fuerte de 3 sentidos:** esta variante añade un mensaje a la propuesta anterior. La ventaja de este método frente al anterior es que en este caso no es necesario hacer uso de marcas de tiempo, lo cual es conveniente para entornos en los que la sincronización del reloj no es posible.

#### 4.4.- No repudio

Se asegura que una determinada entidad no puede alegar que no ha realizado una acción.

Los servicios de no repudio permiten diseñar protocolos y aplicaciones donde las partes implicadas aseguran su participación. Según el estándar ISO/IEC DIS 13888-1, se distinguen los siguientes tipos:

- No repudio en creación: obtener una prueba que garantice que el emisor de un mensaje ha creado el contenido del mismo.
- No repudio en envío: el receptor obtiene una prueba garantizando que un determinado emisor ha realizado un envío.
- No repudio en origen: el receptor obtiene una prueba garantizando que un determinado emisor ha creado el contenido de un mensaje y lo ha enviado (incluye no repudio en creación y en envío).
- No repudio en recepción: el emisor obtiene una prueba garantizando que el receptor del mismo lo ha recibido.
- No repudio en conocimiento: obtener una prueba garantizando que el mensaje ha sido conocido por el destinatario.
- No repudio en entrega: el emisor obtiene una prueba garantizando que el mensaje ha sido recibido y conocido por el receptor (incluye no repudio en recepción y en conocimiento).
- No repudio en presentación: el emisor obtiene una prueba de que una autoridad de entrega ha aceptado la transmisión de un determinado mensaje.
- No repudio en transporte: el emisor obtiene una prueba que garantiza que una autoridad de entrega ha hecho llegar el mensaje al receptor.

El mecanismo más utilizado para satisfacer no repudio en emisión es la utilización de firmas. En el momento en el que el emisor firma el mensaje a enviar, este solo podrá ser verificado utilizando la clave pública del firmante, acreditándose así la autoría de la firma. No obstante, esta propiedad puede verse amenazada por situaciones tales como el robo de los elementos de firma (las claves), llegando a conseguirse repudiar información enviada. Para el resto de tipos de no repudio lo más

habitual es hacer uso de protocolos, como son los de intercambio justo, basados en garantizar que las partes involucradas obtienen lo deseado.

#### 4.5.- Imputabilidad

Se realiza un seguimiento de todas las acciones de los usuarios del sistema, de modo que todos ellos sean responsables de sus acciones. Parece claro que esta propiedad tiene una relación muy estrecha con la de no repudio. Para realizar el seguimiento de un usuario hay que conseguir el no repudio de las acciones realizadas. Por tanto, las firmas electrónicas vuelven a convertirse en un mecanismo que permite satisfacer esta propiedad, aunque debe acompañarse de otros procedimientos como son los ficheros de auditoría.

#### 4.6.- Sellado de tiempo

Se asegura que la información existió en un momento concreto y no ha sido modificada desde entonces. El sellado de tiempo está normalizado según las especificaciones del estándar RFC-3161, propuesto por el *Internet Engineering Task Force* (IETF).

Para realizar un sellado de tiempo se envía la información que se desea acreditar a una autoridad de sellado de tiempo. Esta entidad firmará la información recibida, así como una marca de tiempo adjunta (es decir, una indicación de la fecha y hora de realización de la firma).

Una de las cuestiones más importantes es la fiabilidad de la marca de tiempo. En otras palabras, ¿cómo garantizar que realmente era esa hora? Con este fin se necesita utilizar una fuente fiable de tiempo. Un ejemplo de fuente fiable es el Real Instituto y Observatorio de la Armada (ROA).

### 5. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA Y DE CLAVE PÚBLICA

"Solo el secreto de la clave proporciona un cifrado seguro" (Principio de Kerckhoff). Existen muchos algoritmos de cifrado pero todos ellos son bien conocidos y es en el secreto de las claves donde se encuentra la principal fortaleza. Por ello, los elementos fundamentales dentro de la criptografía son las claves y, junto con ello, los canales utilizados para su intercambio.

Se distinguen dos tipos de criptografía: la criptografía de clave privada y la criptografía de clave pública. En las siguientes secciones se detallan los elementos concretos que caracterizan cada una de ellas.

#### Nota

Los términos "criptografía de clave secreta": "de clave privada" y "criptografía simétrica" son sinónimos y se utilizan de manera indistinta. De igual forma, la "criptografía asimétrica" es también conocida y utilizada como "criptografía de clave pública".

### 5.1.- Elementos fundamentales de la criptografía de clave privada

La criptografía de clave privada considera que los mensajes intercambiados por los usuarios son cifrados y descifrados por una misma clave, secreta entre ambos. Por ello, la clave de cifrado es equivalente a la clave de descifrado o derivable de la misma y el canal utilizado para su intercambio ha de ser seguro, es decir, confidencial. El esquema general de un algoritmo simétrico se presenta en la siguiente imagen.



El hecho de disponer de una misma clave es una gran ventaja a la hora de gestionar grupos reducidos. Además, los algoritmos de cifrado y descifrado se caracterizan por su rapidez.

Sin embargo, la utilización de criptografía de clave secreta presenta serios problemas. Por un lado, cuando dos entidades se comunican, cada una no puede autenticar a la otra, es decir, asegurarse de su identidad. Como mucho, puede saber que es "una entidad que conoce la clave"; pero no determinar si es o no una persona concreta. Por otro lado, si varios usuarios se comunican entre sí, el número total de claves a gestionar es muy elevado: habrá tantas claves como pares de usuarios intercambiando información.

Según la cantidad de elementos que se vayan a cifrar, se distinguen dos familias de sistemas de clave privada: los cifradores de flujo y los de bloque.

#### Cifradores de flujo

Permiten el cifrado de uno o pocos símbolos. Por un lado, la información a cifrar se divide en caracteres o bits. Por otro lado, tanto el emisor como el receptor comparten una clave, denominada serie cifrante, que se corresponde con un conjunto de caracteres o bits aleatorios.

El cifrado consiste en realizar operaciones matemáticas con cada carácter/bit de la información y de la serie cifrante. Dentro de los cifradores de flujo, entre los que se pueden mencionar RC4, SEAL,

o eSTREAM, el más conocido es el cifrador de Vernam o One Time Pad. En él, la operación matemática es el OR-exclusivo (o XOR).

**Nota**

La operación XOR utiliza dos bits como entrada, y produce como salida un '1' si ambos bits son distintos.

El científico Shannon demostró que este es el cifrado perfecto siempre que la serie cifrante sea completamente aleatoria, solo se utilice una vez y su longitud sea mayor o igual a la de la información a cifrar. No obstante, estas condiciones son difíciles en la práctica.

**Sabía que ...**

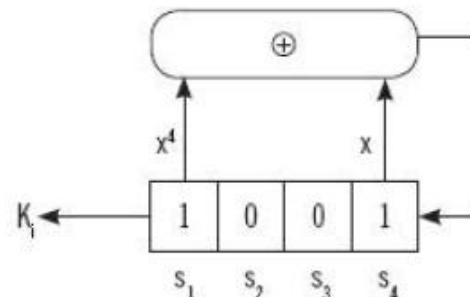
Los cifradores de flujo son muy habituales en escenarios donde la información se pueda dividir en pequeños trozos y procesar independientemente. En particular, se suele utilizar en entornos de streaming o difusión de flujos de datos (ej. vídeo) por internet.

Si bien la creación de series aleatorias es compleja, existen mecanismos para generar valores casi aleatorios (pseudoaleatorios). Entre ellos, los Linear Feedback Shift Register (LFSR) son uno de los mecanismos más utilizados. Los LFSR son registros de desplazamiento en los que la salida, correspondiente con un bit, proviene de aplicar una transformación lineal a un estado anterior. El periodo máximo (es decir, el tamaño de la secuencia de salida antes de que se vuelva a repetir) es  $2^n - 1$ , siendo n el número de bits de entrada. Los LFSR son utilizados porque son fáciles de programar en un circuito integrado (lo que hace que funcionen más rápidamente), pueden producir series cifrantes largas y con buenas propiedades estadísticas y pueden ser fácilmente analizados utilizando técnicas algebraicas. En concreto, los componentes más utilizados para construir estos registros de desplazamientos son las puertas XOR.

Por ejemplo, dado el LFSR mostrado en la imagen siguiente y el estado inicial  $s_1s_2s_3s_4 = 1001$ , la serie cifrante obtenida es K = 100100011110101. En este ejemplo, el bit que entra (flecha derecha) es el resultado de calcular el XOR entre el primer y el último bit del estado. Tras cada operación, todos los bits del estado inicial se mueven a la izquierda, produciendo en cada paso un bit de salida (representado como  $k_i$  en la figura). El conjunto de todos los bits de salida forman la serie cifrante.

### Ejemplo de generador LFSR

Bits K	Registro	Bits realimentación
	<u>1001</u>	$1 \oplus 1 = 0$
1	<u>0010</u>	$0 \oplus 0 = 0$
0	<u>0100</u>	$0 \oplus 0 = 0$
0	<u>1000</u>	$0 \oplus 1 = 1$
...	...	...
	1001	semilla

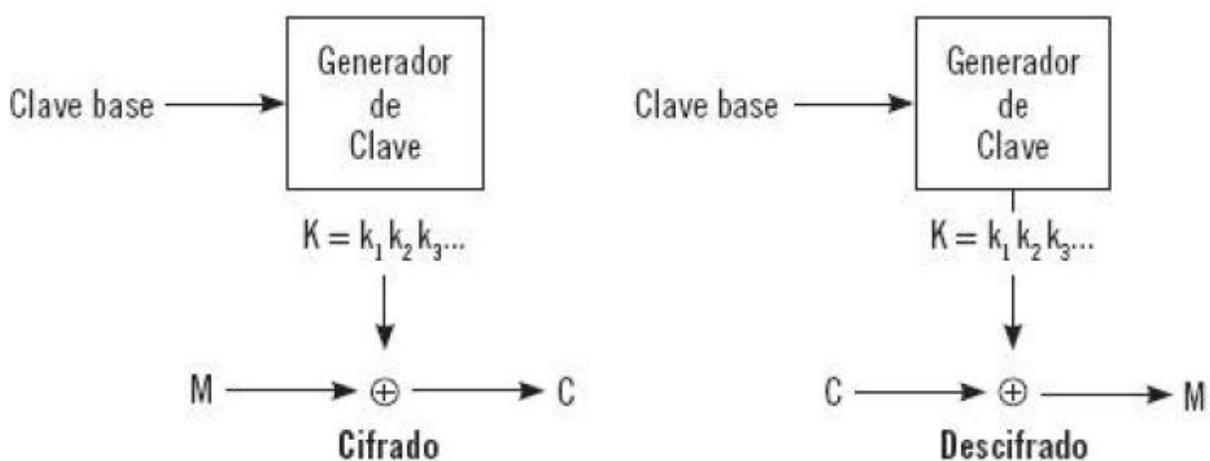


En general, los cifradores de flujo se diferencian entre cifradores síncronos y autosíncronos, según la forma en que se construya la serie cifrante.

#### ↳ Cifradores síncronos

Estos cifradores se caracterizan por que la generación de la serie cifrante (K), que se construye a partir de una clave base, es independiente del texto en claro (M) y del criptograma (C).

#### Cifrador síncrono



### Definición

#### Criptograma

Información cifrada cuyo significado resulta incomprensible.

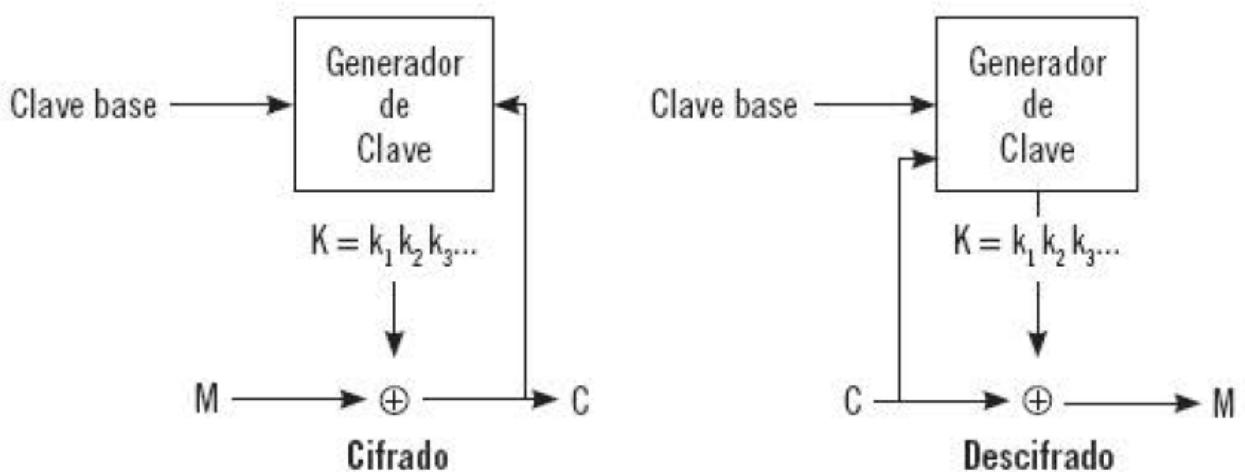
Los cifradores de flujo síncronos tienen las siguientes propiedades:

- **Sincronización entre emisor y receptor.** Los participantes involucrados en la transmisión han de estar sincronizados, ya que, de lo contrario, el descifrado sería incorrecto. De hecho, ante una pérdida de sincronización se requiere aplicar técnicas de re-sincronización, tales como la re-inicialización o la inclusión de caracteres especiales cada cierto tiempo.
- **Inexistencia de errores de propagación.** Si un bit/carácter es modificado durante la transmisión, pero no eliminado, solo dicho elemento será incorrecto al llegar al receptor. El error no afecta a otros bits.
- **Ataques activos.** Un ataque de borrado o inserción puede afectar a la sincronización, siendo posible que el receptor lo identifique. Asimismo, un ataque de modificación contra un conjunto de bits/caracteres provoca que partes del texto en claro no sean comprensibles, lo cual alertaría al receptor.

### Cifradores autosíncronos

Estos cifradores, también conocidos como asíncronos, se caracterizan por que la serie cifrante ( $K$ ) es generada en función de una clave base y de un conjunto fijo de caracteres previamente cifrados.

Cifrador autosíncrono



Los cifradores autosíncronos presentan las siguientes propiedades:

- **Sincronización automática de emisor y receptor.** El descifrado depende de un conjunto de caracteres que preceden al criptograma. Por este motivo, la sincronización se puede recuperar perdiendo únicamente un número fijo de caracteres.
- **Errores limitados de propagación.** Suponiendo que un cifrador autosíncrono depende de un número  $t$  de caracteres que preceden al criptograma, si un bit/carácter es modificado, solo se verán afectados un máximo de  $t$ .
- Ataques activos. Cualquier modificación, eliminación o inserción provoca que un conjunto de bits/caracteres no sean recibidos correctamente, de modo que hay muchas posibilidades de que un ataque pueda ser detectado. Sin embargo, en contraposición con los síncronos, la re-sincronización del emisor y el receptor hace más compleja la identificación de un ataque.
- Difusión estadística en el texto en claro. Dado que cada bit/carácter del texto en claro influye en el siguiente, las propiedades estadísticas están dispersas en el criptograma. Por ello, este tipo de cifradores son más resistentes que los síncronos a ataques basados en la redundancia del texto en claro.

### Cifradores de bloque

Permiten el cifrado de un gran conjunto de símbolos. La información a cifrar se divide en bloques de una determinada longitud (tamaños típicos 64, 128 y 256 bits) y cada uno de ellos se cifra con una misma clave.

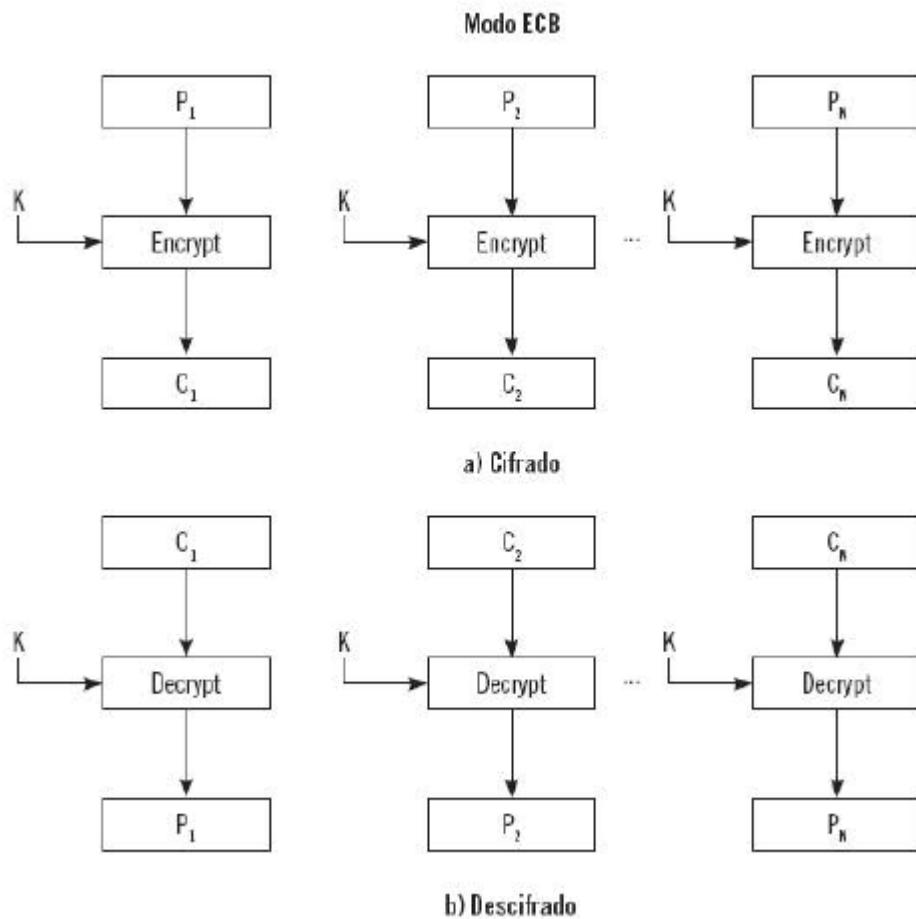
Uno de los métodos de cifrado de bloques más destacable es el cifrado de Feistel, el cual es utilizado por algunos de los algoritmos más conocidos, como es el Data Encryption Standard (DES), presentado más adelante. El método consiste en dividir cada bloque de entrada en dos partes. A una mitad se le aplica una función de transformación en la que interviene una subclave y a la salida de dicha función se le aplica una XOR con la otra mitad. Este proceso se repite un determinado número de veces y en la última de ellas se realiza una rotación entre las mitades del resultado. Una característica de este método es que el proceso de cifrado y descifrado es el mismo, excepto por el hecho de que las subclaves se aplican en el orden inverso.

Los cifradores de bloque pueden funcionar de formas distintas en función de cómo se divide la información en bloques. En general, se pueden distinguir muchos modos de operación, aunque aquí introduciremos solo cinco: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) y Counter Mode (CTR).

#### ↳ **Electronic Code Book (ECB)**

Un mismo bloque de entrada ( $P$ , en la figura) genera un mismo bloque de salida ( $C$ ). El proceso de cifrado y descifrado, mostrado en la siguiente imagen, es equivalente, a cada

bloque se le aplica una función de cifrado o de descifrado junto con una clave (K). Este modo destaca por no propagar errores de transmisión entre los distintos bloques. Sin embargo, al no producirse propagación es posible que un atacante elimine o modifique alguno de los bloques sin que el receptor pueda reconocerlo. Asimismo, dada la posibilidad de que existan bloques repetidos, es un modo susceptible a ataques (por ejemplo, basados en la estadística) que se basen en el reconocimiento de patrones.



(Fuente: Libro Cryptography and Network Security. W.Stallings)

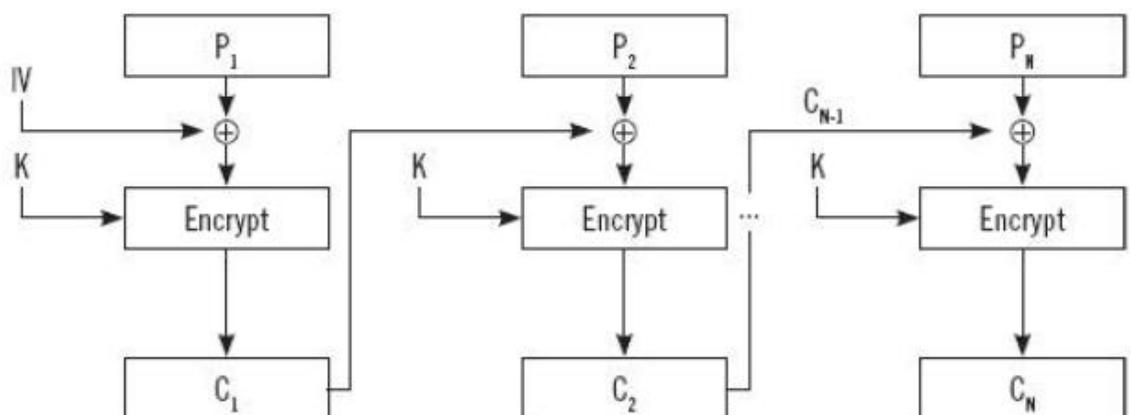
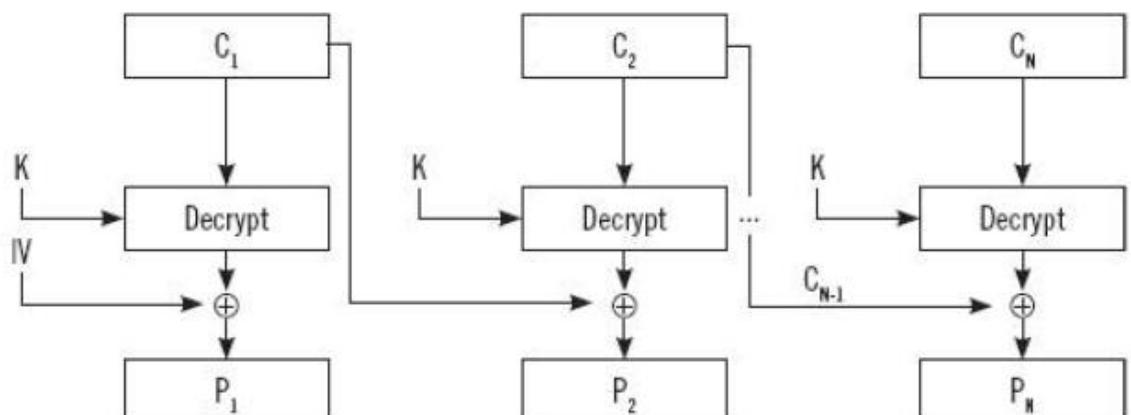
#### ↳ Cipher Block Chaining (CBC)

El cifrado y descifrado de un bloque depende de los anteriores, tal y como se presenta en la siguiente imagen. En el proceso de cifrado a cada bloque se le aplica una XOR con el bloque cifrado anterior y sobre el resultado se ejecuta una función de cifrado junto con una clave. De forma similar, al descifrar, tras aplicar a un bloque cifrado la función de descifrado, al resultado se le aplica una función XOR con el bloque cifrado anterior. Nótese que en el primer bloque, tanto para cifrar como para descifrar, el XOR se ejecuta sobre un vector de inicialización (IV, en la imagen).

Este modo soluciona los problemas de ECB. El cifrado/descifrado de un bloque depende tanto de la clave como del bloque anterior. Por tanto, si existe un error de transmisión, la propagación será de dos bloques. Por ejemplo, si un mensaje compuesto de 3 bloques ( $P$ ) es cifrado y se produce un error de transmisión del primer bloque cifrado  $C_1$ , en el proceso de descifrado los bloques  $P_1$  y  $P_2$  se verán afectados.

**Recuerde**

Los datos transmitidos a través de internet pueden ser manipulados (accidental o intencionadamente) durante la transmisión.

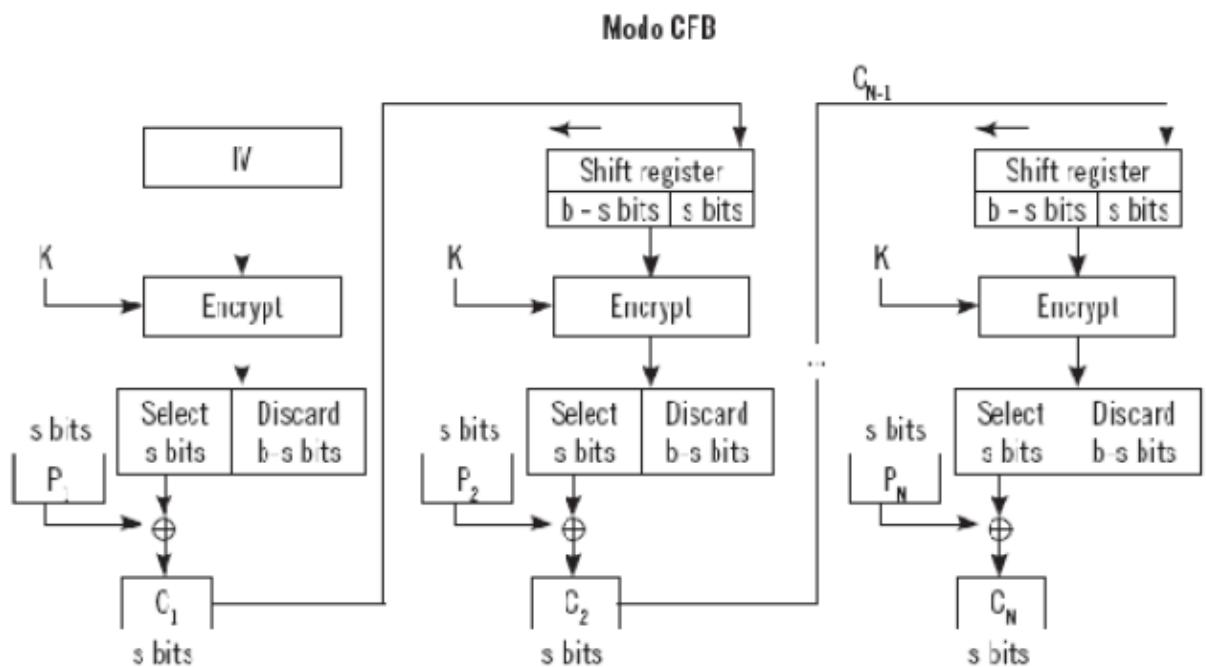
**Modo CBC**

**a) Cifrado**

**b) Descifrado**

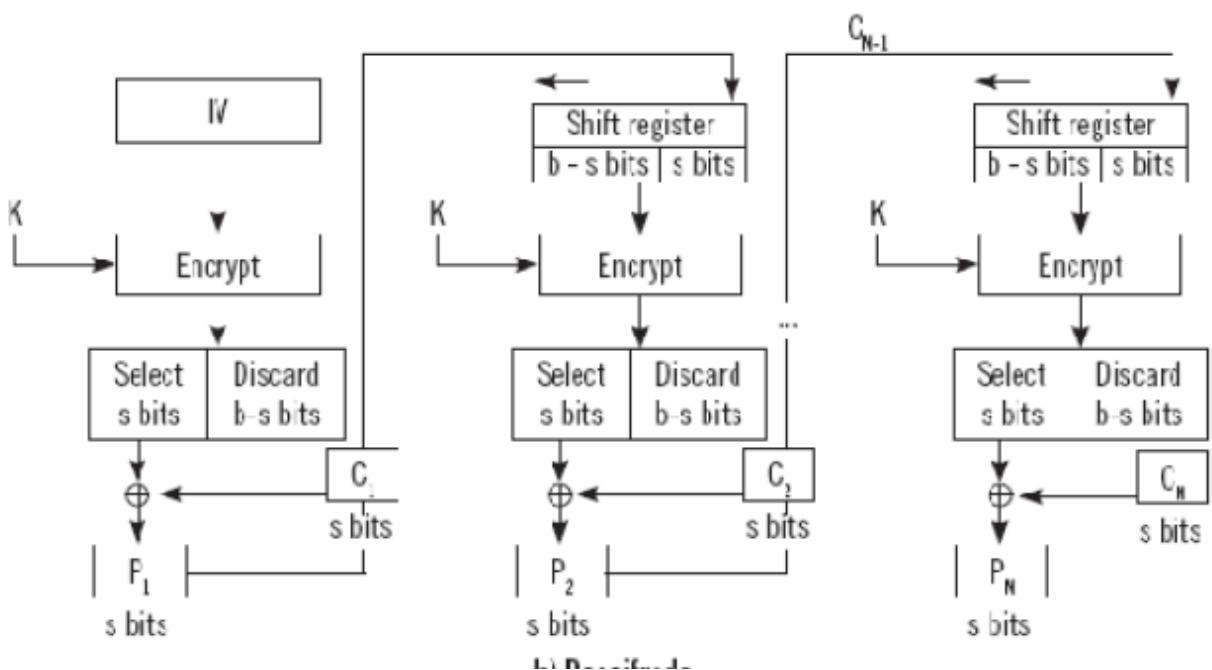
Fuente: Libro Cryptography and Network Security. WStallings

Edita

 Ciplizer Feedback (CFB)

Este modo, presentado en la imagen posterior, hace uso de registros de desplazamiento, operando sobre segmentos menores que un bloque. A grandes rasgos, el proceso de cifrado consiste en, primero, aplicar una función de cifrado sobre un bloque cifrado anteriormente ( $C_i$ ) y segundo, realizar una XOR del resultado con el siguiente bloque de texto en claro ( $P_{i+1}$ ). De forma similar, el descifrado consiste en aplicar la misma función de cifrado sobre un bloque cifrado anterior y, tras ello, ejecutar una XOR con el resultado de dicha operación y el bloque a descifrar. Al igual que en el modo CBC, se ha de utilizar un vector de iniciación (IV) en el primer bloque. Cabe destacar que, dado su funcionamiento, los errores de transmisión se propagan en dos bloques.

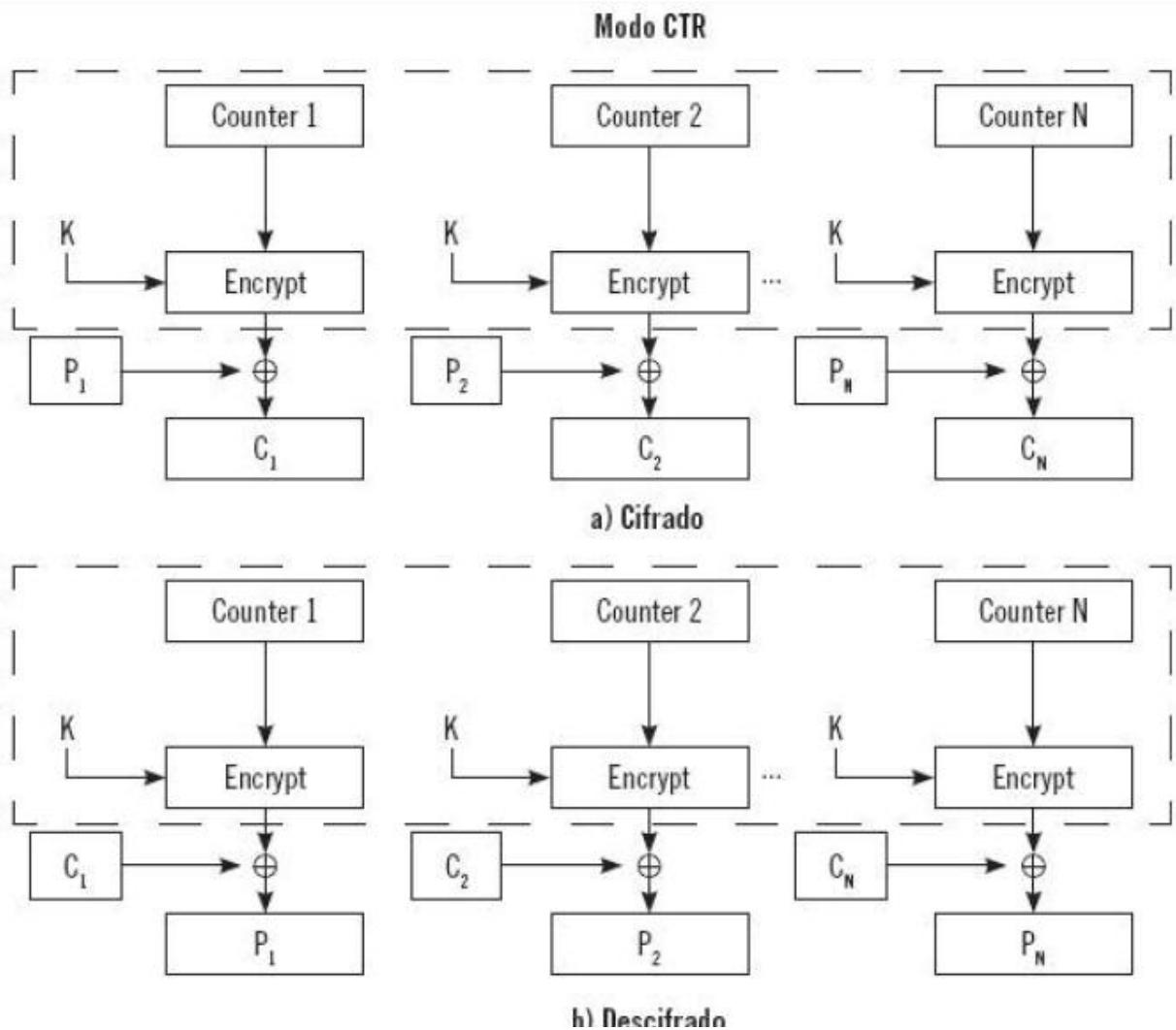




Fuente: Libro Cryptography and Network Security, W. Sallings

#### ↳ Output Feedback (OFB)

Los cifrados y descifrados son similares a CFB y se muestran en la siguiente imagen. La diferencia radica en que en ambas operaciones la entrada a la función de cifrado se corresponde con la salida de la función anterior. Tiene la ventaja de propagar errores de transmisión en un único bloque y, al igual que en el modo CFB, se requiere un vector de inicialización (IV) consistente en un nonce, es decir, un número aleatorio que se emplea una sola vez.



Fuente: Libro Cryptography and Network Security. WStallings

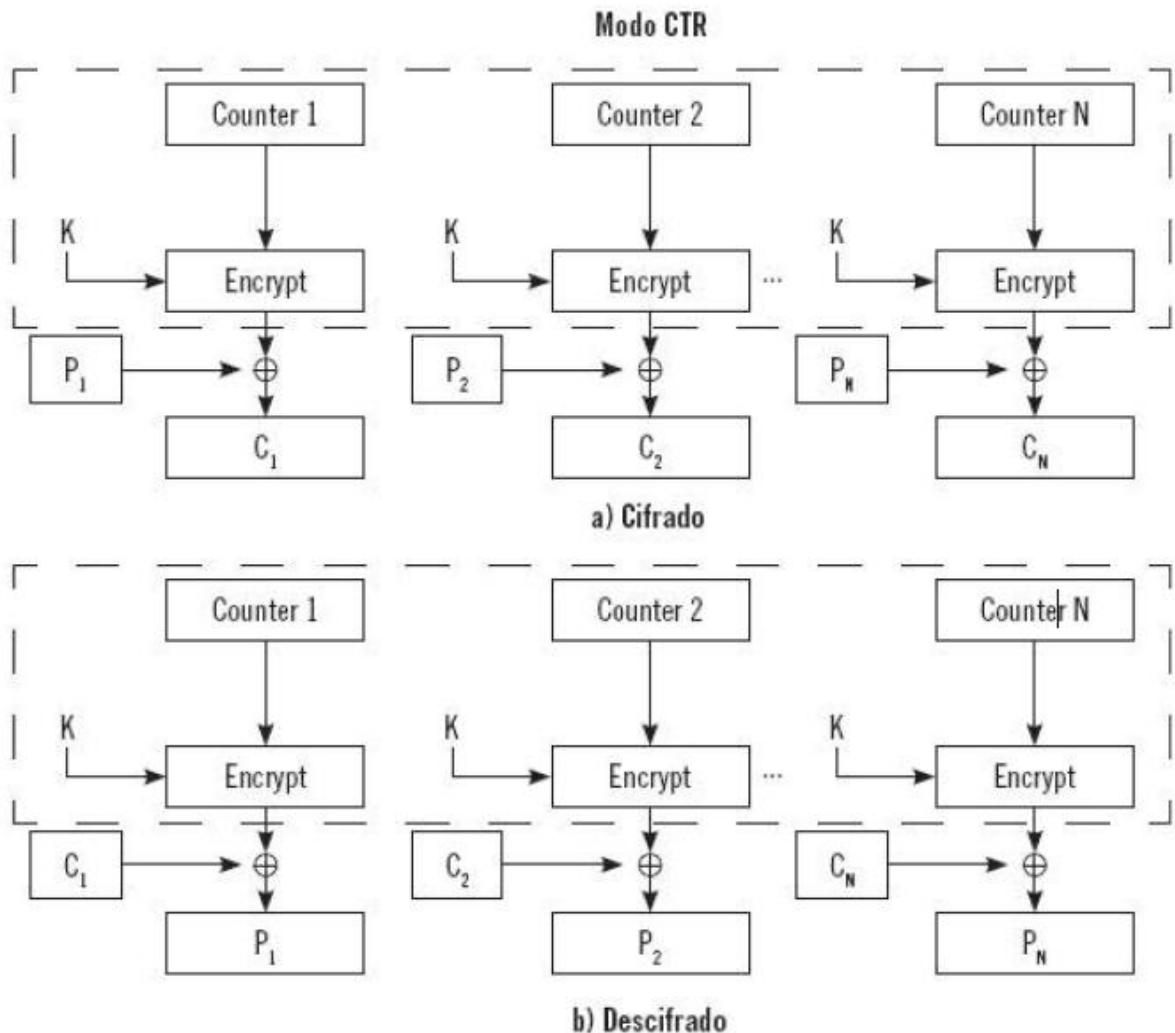
### ↳ Counter Mode (CTR)

Los procesos de cifrado y descifrado son análogos, tal y como se identifica en la imagen posterior. A cada bloque se le realiza una XOR con un nonce al que previamente se le aplica una función de cifrado (equivalente en cifrado y descifrado).

#### Recuerde

Un nonce es un número aleatorio que se utiliza una única vez.

Al nonce utilizado en el proceso de inicialización se le suma 1 en bloques consecutivos. Este modo destaca por ser uno de los más utilizados tanto por su simplicidad como por propagar los errores en un único bloque (en un bit) y por permitir acceso aleatorio.

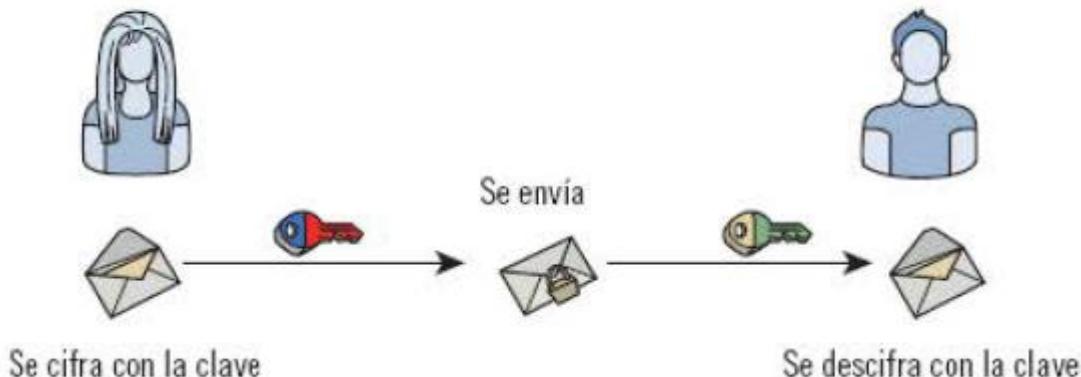


Fuente: Libro Cryptography and Network Security. WStallings

### 5.2.- Elementos fundamentales de la criptografía de clave pública

La criptografía de clave pública hace uso de claves distintas para el cifrado y el descifrado de los mensajes, de modo que cada usuario tiene un par de claves: una pública y una privada. En concreto, el usuario escoge una clave privada y, por medio de una relación matemática, se obtiene la clave pública, garantizándose la unicidad de dicha pareja de claves. El esquema general de un algoritmo asimétrico se presenta en la siguiente imagen.

### Uso de criptografía simétrica



En función de la relación matemática utilizada, se distinguen:

- **Reversibles:** las operaciones de cifrar y descifrar el mensaje se anulan entre sí, por lo que es posible obtener el mensaje en claro a partir del cifrado. El algoritmo reversible más popular es RSA (descrito más adelante).
- **Irreversibles:** no es posible obtener el texto en claro a partir del texto cifrado. Este tipo de algoritmos permiten verificar con la clave pública correspondiente que una determinada firma, realizada por la clave privada asociada, es correcta. Por este motivo, este tipo de algoritmos se conocen con el nombre de solo-firma (signature-only).

Uno de los algoritmos irreversibles más conocidos es El Gama (descrito más adelante).

La utilización de este tipo de criptografía presenta importantes fortalezas. Cada usuario únicamente necesita un par de claves, reduciéndose en gran medida la cantidad de claves a utilizar y la necesidad de gestión de las mismas. Las claves públicas no tienen por qué ser directamente transmitidas entre emisor y receptor, es decir, dada la naturaleza de las claves públicas, las cuales son públicamente conocidas, no se requiere un canal seguro para intercambiarlas.

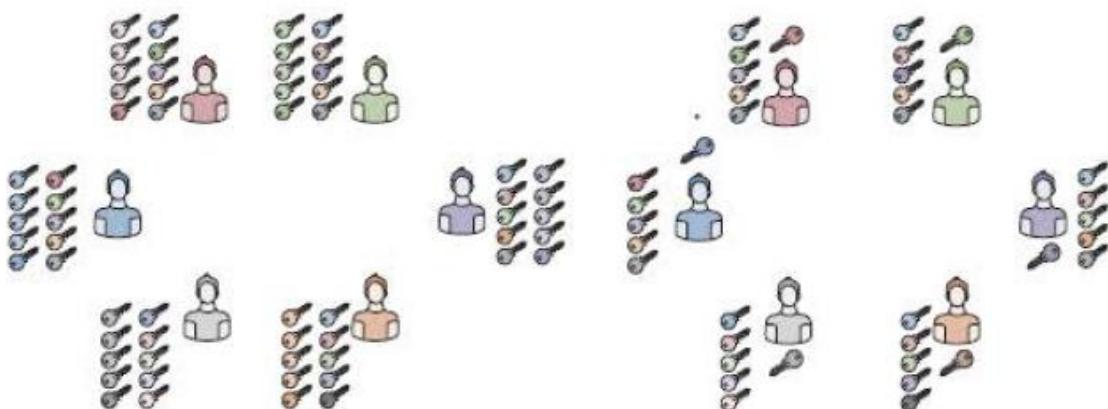
No obstante, a pesar del potencial que presenta este tipo de criptografía, el proceso de generación de claves es computacionalmente costoso, así como el proceso de cifrado y descifrado.

Por ello, este tipo de algoritmos no son eficientes si se aplican sobre datos de gran tamaño. Además, a diferencia de la criptografía de clave privada, estos algoritmos hacen uso de una clave de mayor longitud pero ofrecer un mismo nivel de seguridad.

#### Ejemplo

Suponiendo que un total de 6 personas quieren comunicarse entre todas ellas de modo que se mantenga la confidencialidad de los mensajes, en la siguiente imagen se muestran las claves necesarias al utilizar un algoritmo de clave pública y de clave privada.

### Gestión de claves



Se puede identificar la complejidad de gestión de claves al utilizar un algoritmo de clave privada, en el que se necesitarían un total de 15 claves. En concreto, cada usuario tendría que tener una clave distinta para intercambiar mensajes con cada uno de los usuarios.

Por el contrario, al utilizar un algoritmo de clave pública, cada usuario dispone de un par de claves y únicamente las claves públicas han de ser conocidas por todos los usuarios, necesitándose únicamente un total de 12 claves. Aunque la diferencia pueda parecer pequeña, el problema radica en que, al utilizar el algoritmo simétrico, las 15 claves han de ser intercambiadas, mientras que si se utiliza un algoritmo asimétrico solamente se comparten 6 claves públicas. Nótese que los protocolos para el intercambio de claves, presentados más adelante, son muy diversos y cada uno de ellos presenta ventajas y desventajas que han de estudiarse en cada caso.

Es importante considerar que los sistemas de clave pública han de basarse en problemas matemáticos (conocidos como problemas NP y NP-completos) que sean complejos de resolver con la ayuda de ordenadores. Los algoritmos más conocidos, descritos más adelante, son el algoritmo RSA, basado en el problema de la factorización, y el algoritmo El Gamal, basado en el problema del logaritmo discreto.

### Definición

#### Problema NP y NP-Completo

Un problema se considera de clase NP si puede ser resuelto en tiempo polinomial no determinista, donde no determinista significa que cada paso a realizar tiene muchas posibles opciones y la complejidad se calcula suponiendo que, en cada paso, se escoge la peor opción. Por otro lado, los problemas NP-Completos son los más complejos dentro de NP.

### Problema de la factorización

Calcular la descomposición de un número como producto de números primos elevados a potencias. Por ejemplo:

$$3630 = 10 \cdot 363 = 2 \cdot 3 \cdot 5 \cdot 121 = 2 \cdot 3 \cdot 5 \cdot 11^2$$

### Problema del logaritmo discreto

El logaritmo consiste en calcular la potencia  $x$ , a la que hay que elevar un número, utilizando como base  $a$ , para obtener otro número dado  $b$ ,  $\log_a b = x$ . Por ejemplo:

$$\ln 375 = 5,926926$$

$$\log_{10} 375 = 2,574031$$

$$\log_2 375 = 8,550747$$

En base a la definición de logaritmo, el problema del logaritmo discreto es equivalente pero restringiéndose a conjuntos finitos de números. Un ejemplo de dicho conjunto sería el que forman todos los números mayores que 0 y menores que un determinado número "n": es decir,  $\{0, 1, 2, \dots, n-1\}$ . Para conseguir operar dos elementos de ese conjunto y que el resultado siga perteneciendo a dicho conjunto, se define la aritmética modular. Así, la suma se representa como  $(a+b) \bmod (n)$  y se interpreta como el resto de dividir  $(a+b)$  entre  $n$ .

Empleando este concepto en el ámbito del logaritmo, el problema consiste en que dado  $b = a^x \bmod (p)$ , se debe hallar  $x = \log_a b \bmod (p)$ .

Por ejemplo, en  $Z_{11}$ :

$$\log_2 10 \cong 5 \bmod(11),$$

$$2^5 = 32 = 11 \cdot 2 + 10 \cong 10 \bmod (11)$$

### 5.3.- Criptografía de clave pública, curvas elípticas

La criptografía de curvas elípticas es una alternativa de la criptografía de clave pública cuya aparición está basada en la eficiencia de los algoritmos de curvas elípticas que estaban siendo desarrollados y en los progresos en la resolución de los cálculos relacionados con el problema del logaritmo discreto, puesto que algunos de los algoritmos de clave pública existentes se están consiguiendo romper (o criptoanalizar, tal y como se explicó anteriormente) y se hace indispensable el aumento del tamaño de las claves de cifrado.

Entre las ventajas principales de esta rama de la criptografía está la utilización de claves de menor tamaño que en criptosistemas de clave pública. Esto acelera el cálculo de las claves, disminuyendo la cantidad de memoria utilizada y reduciendo el coste de transferencia de datos.

En la actualidad, la criptografía de curvas elípticas es susceptible de ser utilizada en dispositivos móviles, tarjetas inteligentes o redes de sensores, entre otras aplicaciones.

## 6. CARACTERÍSTICAS Y ATRIBUTOS DE LOS CERTIFICADOS DIGITALES

Un certificado digital es un documento electrónico que vincula a una entidad (persona, servidor, etc.) con un par de claves que pueden utilizarse tanto para firmar digitalmente como para cifrar. La clave pública se almacena dentro del certificado mientras que la privada tendrá que ser almacenada y protegida por la entidad correspondiente.

Atendiendo a la definición de certificado, hay que subrayar la necesidad de tener control sobre nuestra clave privada, evitando posibles pérdidas, en cuyo caso sería necesario realizar la revocación del certificado asociado. Revocar un certificado consiste en invalidarlo, consiguiendo que posteriores usos de la clave privada no se consideren legítimos.

Los certificados son emitidos por distintas entidades dependiendo del tipo de certificado.

Así, pueden ser emitidos por Autoridades de Certificación (AC), las cuales se encargan de comprobar la identidad del solicitante, o bien puede ser el propio usuario quien lo emita (detalles más adelante). Por este motivo, excepto si los certificados son creados por el propio usuario, es indispensable la identificación del propietario del mismo previamente a que la AC realice la emisión del certificado.

Los certificados se pueden utilizar en distintas operaciones electrónicas. Por ejemplo: los correos electrónicos pueden firmarse o cifrarse haciendo uso de estos certificados o, en el caso de España, los trámites con la administración pública requieren o admiten también el uso de certificados digitales. Sin embargo, se necesitan distintos tipos de certificados en función de las operaciones a realizar. En base a las clases de certificados establecidas por VeriSign, se encuentran los certificados de:

- Clase 1, para los usuarios, especialmente para el correo.
- Clase 2, para las organizaciones, de modo que se pueda probar su identidad.
- Clase 3, para los servidores y las firmas de los programas.
- Clase 4, para trámites online entre empresas.
- Clase 5, para empresas privadas y de seguridad gubernamentales.

Hay que tener en cuenta la falta de estandarización de estas clases, de modo que es posible la existencia de otra clasificación en función del vendedor (AC) escogido.

## 7. IDENTIFICACIÓN Y DESCRIPCIÓN DEL FUNCIONAMIENTO DE LOS PROTOCOLOS DE INTERCAMBIO DE CLAVES USADOS MÁS FRECUENTEMENTE

Los protocolos de intercambio de claves son mecanismos por los que un par de entidades se comunican sobre un canal inseguro para generar una clave secreta común. Este tipo de protocolos son esenciales para transmitir datos sobre redes inseguras, de modo que los mensajes intercambiados no permiten conocer información sobre la clave secreta, la cual se utiliza para cifrar la información transmitida. Además, este tipo de protocolos son muy utilizados y se consideran una pieza clave en la construcción de canales seguros de comunicación.

El diseño y análisis de los protocolos de claves no es sencillo y hay numerosos modos de realizarlo. Se han de considerar las siguientes características:

- Naturaleza de la autenticación: determinar si las entidades que participan han de estar autenticadas, así como la clave. También se ha de valorar la necesidad de confirmar la recepción de la clave.
- Reciprocidad de la autenticación: la autenticación puede realizarse de forma unilateral o mutua.
- Frescura de la clave: la frescura se corresponde con el periodo de validez de una clave, es decir, la clave ha de permanecer fresca, evitando que pueda ser comprometida por un atacante.
- Control sobre la clave: en algunos protocolos una única entidad escoge una clave y se la envía a la otra parte. Sin embargo, otros protocolos permiten que ambas partes interactúen para establecer una clave derivada de la información proporcionada por ambas.
- Eficiencia: se ha de considerar el número de mensajes intercambiados, el ancho de banda (bits transmitidos) para la transmisión de los mensajes y la complejidad computacional de cada una de las entidades involucradas.
- Requisitos de tercera parte: ante la necesidad de involucrar a una tercera entidad en el protocolo, se ha de considerar si es on-line u off-line.
- Uso de certificados, en caso de utilizarse: en relación con la existencia de una tercera parte, si se requieren certificados se ha de valorar el modo de distribuirlos.

Más adelante se detallarán distintos protocolos de intercambio de claves privadas y públicas basados en criptografía simétrica o asimétrica. Sin embargo, dentro de los protocolos de intercambio de claves cabe destacar el protocolo Diffie-Hellman, que por su importancia se estudia a continuación.

### 7.1.- Protocolo Diffie-Hellman

Dentro de los protocolos de intercambio de claves más conocidos cabe destacar el protocolo de Diffie-Hellman, desarrollado en 1976. Está basado en las propiedades de los logaritmos discretos y

no proporciona ningún tipo de autenticación, permitiendo la existencia de un ataque de hombre en el medio.

Asumiendo la existencia de dos entidades, A y B, que desean establecer una clave en común, la cual es creada con información conjunta, el proceso es el siguiente:

1. A y B acuerdan dos números p, g. El número p es un número primo muy grande (ej. 300 dígitos decimales). Por su parte, g es un número que cumple que, si dividimos sus sucesivas potencias entre el número p, se obtienen todos los restos entre 1 y p-1.
2. A escoge un número aleatorio a y computa  $M_A = g^a \text{ mod } (p)$  y, enviando  $M_A$  a la entidad B. Recuérdese que la notación  $a \text{ mod } (b) = r$  se interpreta como el resto "r" de dividir "a" entre "b".
3. B escoge un número aleatorio b y calcula  $M_B = g^b \text{ mod } (p)$ , el cual envía a A.
4. B computa  $K_s = (M_A)^b \text{ mod } (p)$ .
5. A computa  $K_s = (M_B)^a \text{ mod } (p)$ .

## 8. ALGORITMOS CRIPTOGRÁFICOS MÁS FRECUENTEMENTE UTILIZADOS

Numerosos son los algoritmos existentes tanto en criptografía de clave privada como en criptografía de clave pública. De los primeros es posible destacar: DES, Triple DES, AES, IDEA y Blowfish. Por otro lado, entre los algoritmos de clave pública cabe destacar a RSA y El Gamal.

Sin embargo, dadas las debilidades y fortalezas de la criptografía pública y privada, otro tipo de algoritmos (conocidos como híbridos) son frecuentemente utilizados. Es preciso recordar que también existen algoritmos criptográficos para operaciones distintas del cifrado, tales como la generación de funciones resumen o firma electrónica. No obstante, estos se presentarán más adelante.

### 8.1.- Algoritmos de criptografía de clave secreta

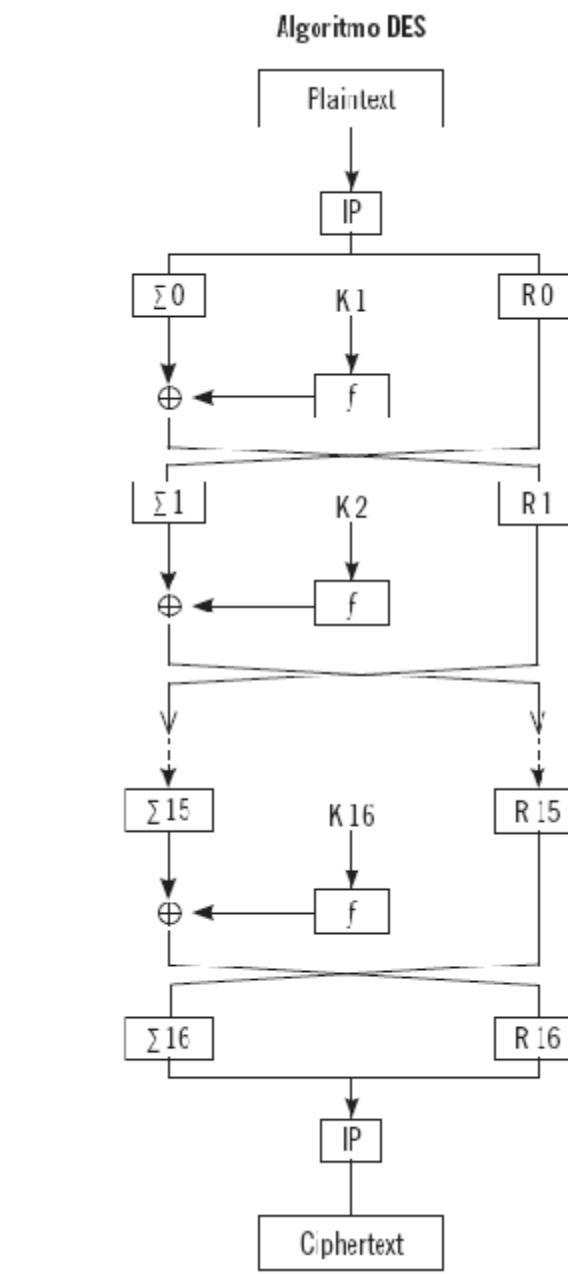
Dentro de los algoritmos más utilizados se encuentran DES, Triple DES, AES, IDEA y Blowfish.

#### Data Encryption Standard (DES)

Este algoritmo es uno de los más utilizados. Fue adoptado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) en 1977. Sin embargo, en 1998 DES fue atacado en 56 horas en un primer momento y en 22 horas posteriormente (DES cracker), surgiendo la necesidad de crear un algoritmo más robusto. En 2001 este algoritmo es sustituido por AES.

El algoritmo DES se basa en un cifrador de bloque en el que la clave es de 64 bits, dividiendo el mensaje en bloques de igual tamaño a la clave. Recuérdese que el bit es la unidad mínima de información y su valor puede ser '0' o '1'. Además, se hace uso de un total de 16 rondas, en las que se utilizan claves internas de 48 bits. En cuanto a la base matemática que lo soporta, esta consiste en sustituciones, lineales y no lineales, y en permutaciones. En concreto, el algoritmo, presentado en la siguiente imagen, se puede dividir en los siguientes pasos:

1. El mensaje a cifrar se divide en bloques.
2. Se selecciona un bloque y se descompone en 64 bits.
3. Sobre el bloque se realiza una permutación inicial (IP), la cual consiste en cambiar de orden todos los bits en base a unos criterios establecidos.
4. Por cada bloque permutado se producen un total de 16 rondas, en cada una de las cuales se realizan los siguientes pasos:
  - a. El bloque se divide en dos partes, izquierda ( $L_0$ ) y derecha ( $R_0$ ), cada una de ellas de 32 bits.
  - b. A  $R_0$  se le introduce en una Caja E, en donde se realiza una permutación y una expansión, obteniendo como resultado un bloque de 48 bits.
  - c. A la salida de la Caja E se le aplica una operación OR exclusivo (XOR) con una clave de ronda de 48 bits.
  - d. El resultado de la operación anterior se introduce en las Cajas S. Estas cajas, un total de ocho, se corresponden con un conjunto de ocho matrices, donde cada una de ellas toma como entrada un conjunto de seis bits consecutivos y produce 4 bits de salida.
  - e. Tras la salida de las Cajas S, a los 32 bits resultantes se les ejecuta una permutación final.
  - f. Para terminar, la ronda finaliza con un XOR entre los bits permutados y  $L_0$ , obteniendo  $R_1$  (es decir, el bloque derecho de la siguiente ronda) y considerando que en la siguiente ronda el bloque izquierdo ( $L_1$ ) será  $R_0$ .



### Triple DES

En 1999 se crea Triple DES, que consiste en el encadenamiento de tres funciones DES.

Particularmente, su forma más común está basada en el uso de dos claves, de forma que se cifra con la primera, el resultado se descifra con la segunda y a su vez el resultado se cifra con la primera.

**Sabía que ...**

El algoritmo Doble DES no fue utilizado de forma generalizada, dado que no aportaba un incremento de seguridad significativo y, por el contrario, implicaba la gestión de dos claves.

**International Data Encryption Algorithm (IDEA)**

IDEA, creado en 1991, tenía como objetivo reemplazar al algoritmo DES. Es un cifrador de bloque que opera sobre bloques de 64 bits, claves de 128 bits y un total de 8 rondas. Además, este algoritmo fue utilizado en las primeras versiones de PGP, uno de los programas de cifrado más comúnmente utilizados en los últimos tiempos.

El proceso de funcionamiento de IDEA se basa en ejecutar operaciones algebraicas no conmutativas de grupos algebraicos diferentes (XOR, sumas y multiplicaciones) sobre los bloques y las subclaves utilizadas.

**Blowfish**

Se desarrolló en 1993 con el objetivo de reemplazar al algoritmo DES o IDEA, pero no llegó a convertirse en estándar. Actualmente Blowfish es un algoritmo público que está a disposición de los usuarios.

Blowfish es un cifrador de bloque que opera sobre bloques de 64 bits con unos tamaños de claves desde 32 a 448 bits. Su funcionamiento consiste en la ejecución de 16 rondas, aplicando el cifrado de Feistel, en las que se hace uso de claves dependientes de las Cajas S (igual a DES).

**Advanced Encryption Standard (AES)**

Como mejora de DES y Triple DES se propone AES, basado en el algoritmo Rijndael. Este algoritmo fue escogido en 2001 por el NIST como el nuevo estándar para comunicaciones gubernamentales, transferencias de fondos bancarios, comunicaciones por satélite y software libre.

Es un cifrador de bloque que opera sobre bloques de 128 bits y claves de 128, 192 o 256 bits con subclaves de 128 bits. Este algoritmo es rápido tanto a nivel hardware como software, fácil de implementar y requiere poca memoria. Matemáticamente está basado en cuatro funciones invertibles que se aplican a los bytes de una matriz llamada Estado, durante un número determinado de rondas. A grandes rasgos, el algoritmo funciona del siguiente modo:

1. El mensaje a cifrar se divide en bloques.
2. La matriz Estado se carga inicialmente con el XOR de los bytes del bloque de entrada y la primera de las subclaves generadas.

3. Para cada bloque y por un conjunto N de rondas, a la matriz Estado se la pasa consecutivamente por las siguientes funciones:
- Sub Bytes: función no lineal realizada a través de una caja S (S-box).
  - ShiftRows: función que desplaza bloques de un byte hacia la izquierda módulo columna dentro de una fila. Por ejemplo, suponiendo una matriz 4x4, la fila 0 no se desplazaría, la fila 1 se desplazaría un byte, la fila 2 se desplaza 2 bytes y la fila 3 se desplaza 3 bytes:

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

- MixColumns: función matemática compleja. Simplificando su descripción, esta función multiplica columnas por un polinomio fijo.
- AddRoundKey: función que, en la primera ronda y al final de cada ronda, aplica un XOR entre el bloque implicado y la clave de ronda.

## 8.2.- Algoritmos de criptografía de clave pública

Los algoritmos más conocidos son el algoritmo RSA, basado en el problema de la factorización, y el algoritmo El Gama!, basado en el problema del logaritmo discreto.

### RSA

Este algoritmo fue creado en 1978 por Rivest, Shamir y Adleman, de donde proviene el nombre RSA, y destaca por ser el primer algoritmo efectivo de clave pública. Otros algoritmos fueron creados y todos ellos fueron rotos, permaneciendo este.

A diferencia de El Gamal!, RSA utiliza el mismo algoritmo tanto para el cifrado como para la firma electrónica (que se describe en profundidad más adelante). En ambos casos, el proceso utiliza la clave pública para una operación (envío de mensajes cifrados 1 verificación de la firma) y la privada para la contraria (descifrado de mensajes 1 realización de una firma).

Antes de explicar en detalle el funcionamiento del algoritmo, es preciso señalar los dos conceptos básicos sobre los que se desarrolla RSA. En primer lugar, la operación módulo (que aparece en la ya citada aritmética modular) que ya se introdujo anteriormente. El segundo concepto es el indicador de Euler para un determinado número n, que se representa como  $\phi(n)$ . Se define como la cantidad de números naturales menores o iguales a n cuyo máximo común divisor (m.c.d.) con n es exactamente 1. Los números que cumplen esta propiedad se denominan primos relativos.

Utilizando ambos conceptos es posible comprender el proceso seguido por RSA. Considérese el caso del cifrado de información. Suponiendo que A quiere mandar un mensaje cifrado a B, el proceso de ejecución es el siguiente:

1. A escoge dos números primos muy grandes y no públicos,  $p$  y  $q$ , de modo que obtiene  $n=p \cdot q$ .

A escoge un número entero  $e$  que sea primo relativo con  $\phi(n)$ .

A escoge un número  $d$  tal que  $e \cdot d = 1 \pmod{\phi(n)}$

La clave pública de A es  $(e, n)$ , mientras que la clave privada es  $(d, n)$ . A distribuye su clave pública utilizando cualquiera de los mecanismos de distribución de claves públicas.

2. B envía un mensaje cifrado (que llamaremos  $M$ ) a A,  $C = M^e \pmod{n}$ . Recuérdese que esta operación se realiza, primero, multiplicando el mensaje por sí mismo tantas veces como indique “ $e$ ” y, posteriormente, se obtiene el resto de dividir el resultado por el número “ $n$ ”. Es importante resaltar que el mensaje  $M$  tiene que ser numérico, por lo que si fuese un texto será necesario representarlo como número.
3. A descifra el mensaje haciendo uso de la clave privada,  $M = C^d \pmod{n}$

#### Nota

Para resolver ecuaciones en aritmética modular se utiliza el Algoritmo Extendido de Euclides o el Teorema de Euler.

#### El Gamal

Es un algoritmo basado en el protocolo de intercambio de claves Diffie-Hellman. Fue creado en 1984 y es utilizado en versiones recientes del programa de ordenador PGP.

El Gama! se basa en el problema del logaritmo discreto y puede utilizarse tanto para cifrar como para firmar, aunque los algoritmos son distintos. Por brevedad, solo se mostrará el algoritmo de firma (que se verá más adelante). La principal diferencia frente a RSA radica en que en El Gamal cada operación de cifrado sobre el mismo dato produce un resultado distinto, lo que complica el criptoanálisis.

#### **8.3.- Algoritmos híbridos**

Como se indica en secciones anteriores, la criptografía de clave secreta y pública tiene ventajas y desventajas opuestas. Es posible destacar que la criptografía de clave secreta, en contraposición con la de clave pública, es rápida pero necesita de la existencia de un canal seguro para los intercambios de las claves y, además, la gestión de un elevado número de claves es un proceso complejo. Por tanto, haciendo uso de las ventajas de la criptografía de clave pública y privada

simultáneamente, se desarrollan los criptosistemas híbridos. Estos algoritmos están basados en la aplicación de un algoritmo de clave pública y otro de clave privada.

Asumiendo que se desea enviar un mensaje desde A a B, el proceso de ejecución consiste en los siguientes pasos:

- a. A cifra un mensaje utilizando un algoritmo de cifrado de clave privada, como por ejemplo DES.
- b. La clave utilizada en el paso anterior (representada por  $K_s$ ) se cifra utilizando un algoritmo de clave pública (como RSA) usando la clave pública de B.
- c. A envía el resultado de ambas operaciones a B.
- d. B descifra primero la clave simétrica  $K_s$  haciendo uso de su clave privada.

Posteriormente, utiliza  $K_s$  para descifrar el mensaje.

#### 8.4.- Robustez y eficiencia práctica de los algoritmos

Los algoritmos descritos hasta el momento ofrecen alternativas distintas para la protección de la confidencialidad de la información. No obstante, tanto la seguridad que ofrecen como su eficiencia dependen de cómo estén programados. A continuación, se describen algunos aspectos importantes sobre esta cuestión.

##### Recuerde

El cifrador de Vernam es el único considerado incondicionalmente seguro de acuerdo a la Teoría de la Información de Shannon.

#### Vulnerabilidades del software

Uno de los principales problemas en la aplicación práctica de los algoritmos criptográficos reside en la calidad de su programación. No es extraño encontrar boletines de seguridad que describan la existencia de un error de programación o de configuración que da lugar a la creación de un procedimiento que pone en riesgo la seguridad del algoritmo.

Cuando esto sucede, se dice que esa implementación es vulnerable a uno o varios ataques, con lo que la seguridad efectiva que ofrece es inferior a la que teóricamente proporciona la especificación.

Para dar un nombre uniforme a los errores con independencia de quien lo descubra y permitir que se sepa si están o no resueltos, existen listas que les otorgan un código único. Entre ellas, una de las más conocidas es la Common Vulnerability Exposure (CVE), mantenida por la organización MITRE.

### Gestión de claves

Otra de las cuestiones que suelen provocar incidentes es la inadecuada gestión de las claves.

Particularmente, algunos algoritmos de cifrado simétrico no utilizan la clave proporcionada por el usuario. En su lugar, utilizan el resultado de aplicar sobre dicha clave algún proceso, que habitualmente es una función resumen. Gracias a ello, se hace más difícil que un atacante pueda adivinar la clave utilizada. Sin embargo, aparece un problema si dicho proceso es predecible.

Igualmente, algunos programas que hacen uso de cifrado incorporan la clave en su interior. De este modo, es posible que un atacante suficientemente preparado pueda extraer dicha clave del código del programa.

#### **Recuerde**

Las funciones resumen presentan una serie de propiedades interesantes desde el punto de vista criptográfico. Entre ellas, se trata de funciones criptográficas de un solo sentido, en tanto que no es computacionalmente posible obtener la entrada a partir de la salida. Esto, junto con el carácter aleatorio de su salida, las hace convenientes para la aplicación aquí descrita.

### Relevancia de la auditoría y certificación

Con el fin de garantizar que un determinado programa hace lo que debe hacer, en los últimos tiempos se está generalizando la realización de auditorías sobre el código del programa. Dado que una parte significativa de algoritmos criptográficos están descritos en sus respectivas normas (e.g. estándares ISO, FIPS, etc.) permite que se pueda realizar una verificación objetiva del funcionamiento.

Para dejar constancia de que se cumplen los requisitos impuestos, se han creado las certificaciones de programas y dispositivos. Por ejemplo, el National Institute of Standards and Technology de Estados Unidos (NIST) verifica el cumplimiento de la norma FIPS 140-1 relativa al funcionamiento de módulos criptográficos. Si la verificación es satisfactoria, se obtiene la certificación "FIPS 140-1 Validated". Como ejemplo en el ámbito español, el software del Documento Nacional de Identidad electrónico ha sido certificado por el Centro Criptológico Nacional con un nivel de evaluación EAIA+. Este nivel acredita que el elemento evaluado ha sido diseñado, probado y revisado de acuerdo a una metodología definida.

**Sabía que ...**

Existen normativas para la realización de verificaciones en productos y dispositivos relacionados con la seguridad. Uno de los más conocidos es el Common Criteria, que ha sido normalizado en la ISO/IEC 15408.

**Eficiencia práctica**

La utilización práctica de estos algoritmos está sujeta en buena medida a su eficiencia computacional. Así, debe consumir pocos recursos computacionales (memoria, procesador), ejecutarse en poco tiempo y, en dispositivos con batería reducida (e.j. teléfonos móviles), debe emplear una cantidad moderada de energía.

Para alcanzar estos objetivos y, de paso, garantizar una mayor disponibilidad, se puede recurrir a programarlos físicamente. En ellos, la secuencia de operaciones no está programada, sino definida en un circuito lógico. Con ello mejora la eficiencia de la ejecución al evitarse la sobrecarga de la propia ejecución del código.

Otra de las posibilidades es la utilización de co-procesadores criptográficos, es decir, procesadores especialmente optimizados para tareas lógicas. A diferencia de las implementaciones físicas, los co-procesadores no son específicos de un algoritmo concreto, sino que incluyen funciones que aceleran los cálculos habituales en los procesos criptográficos.

**9. ELEMENTOS DE LOS CERTIFICADOS DIGITALES, LOS FORMATOS COMÚNMENTE ACEPTADOS Y SU UTILIZACIÓN**

Existen distintos formatos de certificados, pudiendo destacar los certificados X.509 y PGP. Ambos tipos presentan importantes diferencias pero el contenido es similar. En líneas generales, los certificados contienen:

- Número de serie.
- Nombre de la entidad emisora.
- Periodo de validez.
- Nombre del sujeto propietario del certificado.
- Clave pública del sujeto propietario del certificado.

**9.1.- Certificados X.509**

Los certificados X.509 presentan 3 versiones, siendo la última versión la vigente en la actualidad. La primera versión apareció en 1988, X.509v1, utilizándose la Infraestructura de Clave Pública (PKI). Posteriormente, en 1993 apareció la segunda versión, X.509v2, en la que se añadieron campos para identificar únicamente al emisor (AC, de Autoridad de Certificación) y al

proprietario del certificado. Sin embargo, tras la aparición en ese mismo año de Internet Privacy Enhanced Mail (PEM), estándar para el intercambio seguro de correo electrónico, se detectó que la v2 no era suficiente y se requería una mayor cantidad de campos, surgiendo X.509v3. Esta nueva versión extendía las anteriores con un conjunto de campos adicionales que debían estar definidos en estándares o registrados por alguna comunidad u organización.

El principal contenido de los certificados x.509v3 es el siguiente:

- Versión: número de la versión del certificado, actualmente puede utilizarse 1, 2 o 3.
- Número de serie: número entero único asignado por la AC emisora.
- Identificador del algoritmo de firma: identificador de firma del certificado.
- Nombre del emisor: nombre de la AC que emite el certificado.
- Validez: fecha de inicio de validez de certificado y fecha de fin.
- Nombre del sujeto: nombre del usuario al que se le otorga el certificado.
- Se estructura de acuerdo al estándar X.500 y pretende ser [mico a través de Internet.
- Información de la clave pública del sujeto: clave pública del sujeto, parámetros asociados a la clave e identificador del algoritmo con el que ha de utilizarse la clave.
- Firma digital del emisor: firma de la AC emisora.
- Extensiones (opcional): proporcionan información adicional y pueden dividirse en tres categorías:
  - Información de la clave y la política: proporcionando información adicional sobre las claves del sujeto y de la AC emisora junto con indicadores de la política del certificado. Una política es un conjunto de reglas que indican la aplicabilidad del certificado en relación con una comunidad y/o los tipos de aplicación en base a una serie de requisitos de seguridad.
  - Atributos del sujeto y de la AC emisora: ofrece la posibilidad de establecer distintos nombres para ambas entidades en múltiples formatos, así como indicar información como el código postal, una imagen, etc.
  - Limitaciones del camino de los certificados: basado en el establecimiento de restricciones respecto a las AC que pueden participar en su creación (esto se explicará en profundidad más adelante).

Los usos de los certificados X.509 son muy diversos, destacando los trámites relacionados con la administración electrónica (en España), la transmisión segura de información entre servidores (uso del protocolo SSL, detallado más adelante), etc.

## 9.2.- Certificados PGP

Pretty Good Privacy (PGP) es un algoritmo desarrollado en 1991 por Phil Zimmermann con el propósito de transmitir información por Internet de forma segura, haciendo uso de la criptografía de clave pública. Actualmente PGP sigue el estándar de OpenPGP.

Al contrario que los certificados X.509 que son emitidos por AC, los certificados de PGP son habitualmente creados por los propios usuarios. Cada usuario crea un par de claves (pública-privada), almacenando la pública en un certificado PGP y haciendo uso de las mismas de igual

modo que con otros certificados. Sin embargo, puesto que no hay ninguna autoridad de confianza que certifique la posesión de unas claves por un determinado usuario, la confianza se establece en función de los usuarios que firmen el certificado PGP (la clave pública), introduciéndose así el concepto de anillo de confianza.

Cuando se hace uso de un certificado PGP, bien para firmar o para cifrar, el receptor tiene que verificar las firmas realizadas sobre este. Si las firmas realizadas sobre un certificado se verifican, entonces el certificado también será confiable y además, dicho receptor puede realizar una nueva firma sobre él para reflejar su confianza. Asimismo, como medida complementaria a la hora de establecer confianza, PGP proporciona un esquema de voto, de modo que cada usuario pueda establecer un nivel de confianza a cada una de las claves, inválida, válida o marginalmente válida (si una clave es marginalmente válida tendrá que firmarse dos veces por distintas entidades para considerarse válida). Por tanto, en PGP es remarcable la relevancia de depositar confianza automática en claves firmadas por terceros en los cuales confiamos.

#### Nota

La especificación actual del estándar OpenPGP permite la existencia de Autoridades de Certificación similares a las descritas para X.509. No obstante, el uso habitual es el aquí descrito, en el que esta tarea la pueden realizar los usuarios.

El contenido de los certificados PGP se puede resumir en:

- Número de versión: identifica el número de la versión de PGP utilizada para crear las claves asociadas al certificado.
- Clave pública: clave pública del propietario del certificado.
- Algoritmo de creación de claves: algoritmo empleado para la creación de las claves asociadas al certificado.
- Información del sujeto: datos del propietario del certificado como son su nombre, dirección de correo, etc.
- Firma digital del sujeto: se denomina auto-firma y se corresponde con la firma del certificado, haciendo uso de la clave privada asociada al mismo. De este modo, el certificado se considera auto-firmado.
- Periodo de validez: fecha de inicio y de fin de validez del certificado.
- Algoritmo simétrico preferido: elección del algoritmo de cifrado de clave privada que el propietario del usuario prefiere utilizar.

Finalmente, cabe señalar que la utilidad de estos certificados puede ser muy diversa. Sin embargo, la utilización de certificados PGP es especialmente frecuente en el envío de correos electrónicos.

## 10. ELEMENTOS FUNDAMENTALES DE LAS FUNCIONES RESUMEN Y LOS CRITERIOS PARA SU UTILIZACIÓN

En el ámbito de la criptografía, se denominan funciones resumen a aquellos procedimientos que, dado un mensaje de un tamaño cualquiera, producen una salida de un tamaño fijo. Como consecuencia de esta definición, el conjunto de mensajes de entrada es siempre mayor que el de las salidas. Por ello, parece claro que más de un mensaje de entrada ofrecerá la misma salida. A esta situación se le denomina colisión.

Las aplicaciones más extendidas de las funciones resumen son el control de integridad y la creación de firmas digitales. Gracias a las funciones resumen, ambas cuestiones se realizan de forma más eficiente. Considérese el caso del control de integridad para un determinado mensaje, que tiene por tamaño 1 Gigabyte. Comprobar que no ha sido modificado requeriría comprobar todos y cada uno de los bits que lo forman, comparándolos con los de una versión anterior del mismo mensaje. En contraposición, considérese que sobre ese mensaje se aplica una función resumen (por ejemplo, SHA-1), obteniendo una salida de 160 bits. Ahora, la tarea se reduciría a comprobar que esa salida (mucho más corta que el mensaje original) coincide con la que se obtuvo al aplicar esa función sobre una versión anterior del mensaje.

### Recuerde

El control de integridad se encarga de comprobar que un determinado elemento no ha variado.

La existencia de colisiones pone en peligro el uso descrito en el caso anterior. Si fuese posible encontrar otro mensaje que ofreciese la misma salida, el control de integridad no podría detectar que el mensaje original se ha alterado. Por este motivo, en la actualidad se emplean funciones resumen criptográficamente robustas. Dichas funciones deben satisfacer las tres propiedades siguientes:

- **Resistencia a la primera pre-imagen.** A partir de la salida de la función, debe ser computacionalmente imposible obtener el mensaje de entrada.
- **Resistencia a la segunda pre-imagen.** Dado un mensaje de entrada, debe ser computacionalmente imposible encontrar otro mensaje que produzca la misma salida de la función.
- **Resistencia a colisiones.** Es computacionalmente imposible encontrar dos mensajes de entrada que produzcan el mismo resumen.

Es importante destacar que las dos últimas propiedades son muy distintas entre sí. Considérese el caso de la fecha de nacimiento de dos personas: en un grupo, no es lo mismo la probabilidad de que otra persona nazca el mismo día que alguien concreto a la probabilidad de que dos personas al azar nazcan el mismo día.

A fin de satisfacer las propiedades anteriores, las funciones resumen se basan en el concepto efecto avalancha. Dicho efecto produce que un cambio en un bit de entrada produzca un cambio en la mitad de los bits de la salida. Con ello, la salida de la función resumen se comporta de una manera aleatoria, lo que dificulta la búsqueda de colisiones.

Por tanto, considerando todo lo anterior, se puede indicar que las funciones resumen tienen las propiedades de:

- Difusión, asociado con el efecto avalancha.
- Determinismo, la misma función sobre los mismos datos producen el mismo resultado.
- Eficiencia, rápidas tanto en hardware como en software.

En concreto, uno de los métodos más conocidos para la construcción de funciones resumen es la estructura de Ivlerkle-Damgard, que ha sido utilizada para crear algunas de las funciones resumen más conocidas, como son MDS, SHA-1 o SHA-2. Según esta estructura, el proceso de construcción consiste en ejecutar un algoritmo con iteraciones encadenadas:

1. El mensaje M se divide en bloques, B, de una determinada longitud. El último bloque se rellena con los bits adecuados para completar la longitud de un bloque.
2. Se aplica una función de compresión a la salida de una iteración anterior (vector de inicialización en el primer bloque) y a un nuevo bloque. Es importante tener en cuenta que, si la función de compresión es resistente a colisiones, la función resumen resultante también lo es. Por este motivo, el diseño de la función de compresión es el núcleo de la seguridad de la estructura de Ivlerkle-Damgard.

**Nota**

Al relleno de un bloque se le conoce con el nombre de padding y dificulta la búsqueda de colisiones.

En la actualidad, las funciones resumen que se consideran criptográficamente seguras son establecidas por diversos organismos internacionales. En particular, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) organiza periódicamente competiciones para que los participantes propongan funciones resumen. La especificación de cada propuesta es públicamente conocida, con lo que toda la comunidad científica puede contribuir a encontrar debilidades. Dichas debilidades se centran en encontrar colisiones o falta de aleatoriedad en la salida.

En octubre de 2012 concluyó el concurso que resultó en el nombramiento de la que se conoce como SHA-3. Su diseño es más robusto que su antecesora, SHA-2, y ambas se consideran mucho más seguras que MDS. Se dice que MDS está rota en tanto que es posible encontrar una colisión en un tiempo moderado utilizando los actuales recursos computacionales.

### 10.1.-Funciones resumen con clave

Además de las anteriores funciones resumen, existe una variante conocida como funciones resumen con clave, comúnmente conocidas como HMAC. En este caso, la salida se calcula en función del mensaje de entrada y de la clave introducida. Dado que se emplea una clave durante el proceso, permite autenticar el origen del mensaje. Un caso de ejemplo sería un banco electrónico que quiere evitar transferencias no deseadas. Si cada cliente dispone de una clave compartida con el banco, se puede enviar junto con la orden de transferencia, el resultado de aplicar la función HMAC sobre este mensaje usando la citada clave. El banco puede estar seguro de que la orden ha sido efectuada por alguien que conocía la clave. Se debe presuponer que, salvo que el cliente haya denunciado el robo de la clave, él es el único conocedor de la misma.

A la vista de esta descripción, la finalidad de las funciones HMAC es muy similar a la de las firmas electrónicas.

## 11. REQUERIMIENTOS LEGALES INCLUIDOS EN LA LEY 59/2003, DE 19 DE DICIEMBRE, DE FIRMA ELECTRÓNICA

La Ley 59/2003 dota de marco legal a la utilización de la firma electrónica. La firma electrónica, de acuerdo a la definición prevista en la Ley, es "el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante". Así, la firma electrónica es un mecanismo que permite la autenticación del emisor.

#### Recuerde

La autenticación es la propiedad que garantiza que una entidad es la que dice ser.

Además de definir los requisitos necesarios que deben cumplir las distintas variantes de firma contempladas (detallados más adelante), esta Ley también establece que la firma electrónica se aplicará en las Administraciones Públicas, aunque en ese caso también se podrían imponer requisitos adicionales. Entre esos requisitos se menciona el fechado electrónico, que permite incluir una marca confiable de tiempo para acreditar el momento en que se realiza una determinada acción.

Con respecto a las entidades participantes en el proceso, la Ley introduce los denominados prestadores de servicios de certificación que operan en España. Se denomina así a cualquier persona física o jurídica que expida certificados electrónicos o, en general, preste cualquier servicio relacionado con la firma electrónica. Entre las obligaciones que se imponen a estas entidades está proteger los datos personales, no almacenar ni copiar los datos que sirven para crear una firma electrónica por parte del titular del certificado y proporcionar la información correspondiente sobre el proceso de certificación a la persona afectada. La declaración de

prácticas de certificación, la responsabilidad y las consecuencias del cese de actividad de un prestador de servicios de certificación quedan también descritas en esta Ley. Estos aspectos se abordarán en profundidad más adelante.

Entre los certificados electrónicos que pueden utilizarse para acreditar electrónicamente la identidad de un sujeto, la Ley introduce el concepto de certificado reconocido como aquel expedido por un prestador de servicios de certificación que cumpla una serie de condiciones.

Particularmente, deben comprobar la identidad del sujeto, verificar que la información contenida en el certificado es exacta y asegurarse de que el sujeto está en posesión de los datos de creación de firma. Además, si los datos de creación y verificación de la firma son calculados por el prestador, tendrá que asegurarse de que son correctos. De cara a demostrar el cumplimiento de estas condiciones, se establece la posibilidad de realizar un proceso de certificación de la tarea de expedición de certificados.

Con respecto al uso del Documento Nacional de Identidad electrónico (DNIE), el texto establece que es el documento que acredita la identidad del titular y que permite la firma de documentos. Se impone que la entidad encargada de emitirlo deberá cumplir las condiciones impuestas a los prestadores que emitan certificados reconocidos. De esta manera, los certificados que constan en el DNIE son reconocidos.

#### Sabía que ...

La expedición del DNI electrónico y sus certificados está regulada por el Reglamento aprobado en el Real decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

Dos de los elementos clave en el uso de la firma electrónica son los dispositivos de creación y verificación. El dispositivo de creación se define como el programa o sistema que se utiliza para aplicar los datos de creación de firma. Para considerarse seguro, se imponen cinco condiciones:

- Que los datos necesarios para firmar pueden generarse solo una vez y que, además, se mantienen en secreto con una protección razonable.
- Que se proporciona una seguridad razonable tal que no es posible derivar los datos de creación de firma a partir de la propia firma o de los datos de verificación.
- Que la firma esté protegida frente a falsificaciones, atendiendo a la tecnología disponible.
- Que el firmante pueda prevenir adecuadamente el uso de los datos de creación de firma por parte de terceros.
- Que no se altere la información que va a ser firmada y que esta se presente al firmante con anterioridad a la operación.

Al igual que sucede con los prestadores de servicios, los dispositivos de creación de firma pueden someterse a un proceso de certificación que determine si el producto evaluado cumple los requisitos definidos para considerarse seguro.

**Sabía que ...**

El chip del DNI electrónico es considerado un dispositivo seguro de creación de firma tras haber sido certificado por el Centro Criptológico Nacional (CCN).

En lo referente a los dispositivos de verificación, estos deben asegurar que el proceso, además de realizar la verificación (y mostrar el resultado) de forma fiable, cumple los siguientes aspectos:

- Que los datos utilizados para verificar la firma sean los mostrados a la persona que efectúa la verificación.
- Que la persona que verifica la firma pueda establecer si los datos han sido modificados.
- Que se muestren los datos de identidad del firmante y que se verifique su certificado electrónico.
- Que pueda detectarse cualquier cambio que afecte a la seguridad del proceso.

## 12. ELEMENTOS FUNDAMENTALES DE LA FIRMA DIGITAL, LOS DISTINTOS TIPOS DE FIRMA Y LOS CRITERIOS PARA SU UTILIZACIÓN

En este apartado se describen, en primer lugar, los elementos fundamentales de la firma, para posteriormente introducir los diferentes tipos de firma.

### 12.1.-Elementos fundamentales. Esquema básico

En un sistema de firma digital entran en juego, además del mensaje a firmar, cuatro elementos fundamentales: el algoritmo de firma, el material criptográfico del firmante, la identidad del mismo y el sistema sobre el que se realiza la firma.

La firma electrónica se asienta sobre los principios de la criptografía de clave pública. Así, el firmante debe disponer de un par de claves pública -privada, que se utilizarán durante el proceso. Para la realización de la firma se aplica un algoritmo criptográfico sobre el mensaje en juego, utilizando la clave privada del firmante. Dicho algoritmo puede ser el mismo que se emplea para realizar un cifrado (como en el caso de RSA) o puede ser distinto (como sucede con El Gama1).

A pesar de la descripción anterior, los algoritmos de clave pública no son especialmente rápidos. Por este motivo, en lugar de realizar la firma del mensaje completo, es habitual que la firma se realice sobre el resultado de aplicar una función resumen sobre el mensaje.

Una vez que se ha realizado la firma, esta se envía junto con el mensaje al receptor. Este, utilizando la clave pública del firmante, aplica el algoritmo de verificación correspondiente de acuerdo al algoritmo de firma escogido. La verificación será correcta si el resultado de este algoritmo es igual al mensaje recibido o, si se utilizó una función resumen, al resultado de dicha función.

Es importante destacar que la verificación descrita permite saber si el mensaje ha sido correctamente firmado (verificación de la firma) y no ha sido alterado (verificación del resumen).

Para completar el proceso, es imprescindible conocer si las claves pertenecen al supuesto firmante. Es en este punto en el que entra en juego la verificación del certificado de clave pública.

Este proceso conlleva, entre otras cuestiones, verificar la cadena de certificación.

### 12.2.-Tipos de firma y criterios de uso

La Ley define tres tipos de firmas, que se construyen de manera incremental. Así, basándose en la definición de firma electrónica, correspondiente con el primer tipo, se identifica la firma electrónica avanzada. Dicha firma permite no solo identificar al firmante, sino también detectar cualquier cambio que se realice sobre los datos firmados. Por este motivo, esta variante también permite verificar la integridad del mensaje. La firma electrónica avanzada, además, da un paso adelante en lo que se refiere al vínculo que debe existir entre el mensaje y quien lo firma. Así, se especifica que debe vincularse con el firmante y con los datos firmados de forma única. Además, se exige que haya sido creada utilizando medios que estén bajo el exclusivo control del firmante.

Con ello, se persigue que un documento firmado electrónicamente sea no repudiable: el firmante no podrá negar que realizó una determinada firma sobre el mensaje en cuestión.

La garantía de no repudio citada anteriormente podría ser cuestionada por un firmante que adujese que, aunque los medios estaban bajo su control, no realizaban adecuadamente la operación de firma. Con ello, podría eventualmente conseguir negar (repudiar) que realizará una determinada firma.

Para evitar la situación anterior, la Ley define la firma electrónica reconocida. Esta variante se construye sobre la avanzada pero exigiendo que se cumplan dos condiciones: que haga uso de un certificado reconocido y que sea creada utilizando un dispositivo seguro de creación de firma. Si se cumplen estas condiciones, el proceso de firma alcanza un elevado grado de seguridad. De hecho, la Ley equipara la firma electrónica reconocida con la firma manuscrita.

### 13. CRITERIOS PARA LA UTILIZACIÓN DE TÉCNICAS DE CIFRADO DE FLUJO Y DE BLOQUE

Una vez conocidos los cifradores de flujo y de bloque, hay que estudiar los criterios que ayuden a determinar qué cifrador es más apropiado en cada caso. Para ello, es necesario analizar las debilidades y fortalezas de ambas familias de cifradores.

Los cifradores de flujo presentan la gran ventaja de ser muy rápidos y sencillos. Además, evitan la propagación de errores en la transmisión y son capaces de descifrar sin necesidad de esperar a

que se reciba un bloque entero de datos. No obstante, requiere sincronización (si se cifra un bit, se ha de esperar por el siguiente). Sin embargo, también presenta dos inconvenientes principales. Por un lado, estos cifradores consiguen poca difusión en la información, es decir, cada símbolo en claro se corresponde con un único símbolo cifrado. Por otro lado, es difícil (computacionalmente imposible) conseguir una serie cifrante completamente aleatoria, así como no reutilizarla en numerosas ocasiones. Por estos motivos, la implementación adecuada de estos cifradores es compleja y la seguridad de los mismos se puede ver afectada.

Por otro lado, los cifradores de bloque también presentan pros y contras. En cuanto a las ventajas, estos destacan por conseguir una alta difusión de los elementos que forman el criptograma.

Sin embargo, presentan los inconvenientes de ser vulnerables a ataques si existen bloques repetidos, pueden ocurrir problemas de transmisión y es necesario que los bloques sean múltiplos del tamaño de bloque para evitar llenar el último bloque y facilitar el criptoanálisis del mismo. También se ha de tener en cuenta, al contrario que los de flujo, la necesidad de disponer de la memoria suficiente para almacenar y procesar cada uno de los bloques.

En base a todo lo comentado, es posible determinar que los cifradores de flujo son adecuados cuando los datos que van a cifrarse son continuos y no se conoce su tamaño, como por ejemplo, en el flujo de una red. En cambio, los cifradores de bloque son apropiados cuando la cantidad de datos a cifrar se conocen previamente, como por ejemplo en un fichero, siendo posible determinar la cantidad de bloques a procesar.

## 14. PROTOCOLOS DE INTERCAMBIO DE CLAVES

Los protocolos de intercambio de claves requieren, con frecuencia, el uso de claves maestras, utilizadas y válidas por un largo periodo de tiempo, y de claves de sesión, empleadas temporalmente entre dos entidades.

Estos tipos de protocolos se pueden clasificar según el tipo de claves intercambiadas, secretas o públicas. Asimismo, los intercambios de claves privadas se pueden realizar mediante criptografía simétrica o asimétrica.

### 14.1.-Intercambio de claves secretas mediante criptografía simétrica

Dos entidades han de intercambiar una clave, secreta entre ambos, la cual ha de ser protegida contra el acceso de la misma por un tercero. Dadas dos entidades, A y B, la distribución de una clave se podría realizar de los siguientes modos:

1. A genera la clave y se la entrega físicamente a B.
2. Una tercera parte puede elegir la clave y entregarla físicamente a A y B.
3. Si A y B se han comunicado previamente, pueden utilizar la clave anterior para cifrar la actual.
4. Si A y B tienen un enlace seguro con una tercera parte e, e puede generar y reenviar la clave a A y B.

En el caso de un enlace punto a punto (conexión directa entre los participantes), las opciones 1 y 2 se consideran aceptables. No obstante, en un enlace extremo-a-extremo sobre una red, el intercambio de claves sería muy costoso. Por ello, en un esquema distribuido las entidades (computadores, servidores, etc.) tendrían que hacerse intercambios cada cierto tiempo, necesitándose una entrega dinámica de las claves a cada una de las entidades.

En cuanto a la opción 3, hay que considerar que si la clave de cifrado es atacada, todas las claves intercambiadas desde ese momento pueden ser comprometidas.

La última opción puede presentar algunas variaciones. En este esquema un centro de distribución de claves (CDC) es el responsable de repartirlas según las necesidades. Para ello, cada entidad comparte una clave con el CDC para realizar la distribución. En particular, el CDC utiliza jerarquías de claves, basadas en claves de sesión y claves maestras (compartidas entre el CDC y una determinada entidad). Las primeras son utilizadas para realizar los intercambios de claves; y las segundas, para cifrar las claves de sesión intercambiadas.

A pesar de la simplicidad de este tipo de protocolos, el hecho de requerir el intercambio previo de una clave, bien físicamente o mediante una tercera parte, supone un gran problema que durante muchos años se pensó irresoluble. No obstante, esto cambió con Whitfield Diffie y Martín E. Hellman cuando, en 1976, surgió la criptografía de clave pública.

### **Controlando el uso de las claves**

El concepto de jerarquía de claves, junto con los procesos automáticos de distribución, simplifica la gestión de dichas claves. No obstante, también sería deseable controlar el uso de cada una de las claves. Un modo de conseguirlo es adjuntando a la clave una etiqueta, la cual se transmite cifrada y se corresponde con un conjunto de bits que determinan el uso de la misma.

Esta técnica tiene el inconveniente de que la longitud de la etiqueta es limitada. Debido a las limitaciones de este esquema, otra propuesta más flexible es la utilización de vectores de control, los cuales son un conjunto de campos que especifican el uso y las restricciones de la clave. Los vectores de control son generados conjuntamente con las claves en el centro de gestión de claves y presentan las ventajas de no tener limitación de tamaño y de ser distribuidos en claro.

### **14.2.-Intercambio de claves secretas mediante criptografía asimétrica**

Teniendo en cuenta las debilidades de la criptografía asimétrica (esencialmente la alta carga computacional), el uso más importante de este tipo de criptografía es el intercambio de claves. Las claves son intercambiadas entre dos entidades sin la necesidad de un canal seguro.

Dadas dos entidades, A y B, que desean establecer una clave secreta común, uno de los protocolos más simples consiste en los siguientes pasos. Nótese que la base sobre la que se sustentan los algoritmos de cifrado híbridos es equivalente a los pasos a y b del apartado 8.3.

1. A genera un par de claves público-privada y transmite a B su clave pública y su identificador.
2. B genera una clave secreta (K5), la cifra con la clave pública de A y se la envía.

3. A utiliza su clave privada para descifrar el mensaje recibido y obtener la clave secreta enviada por B, es decir, K5.

Sin embargo, este protocolo es susceptible a ataques de hombre en el medio. Un tercero se puede situar entre A y B creando un nuevo par de claves consiguiendo que A y B obtuviesen K5 a la vez que esta clave es conocida por dicho atacante. Por tanto, este protocolo solo es apropiado en escenarios donde la \mica amenaza posible sea la interceptación.

Los esquemas de clave pública sólo son seguros si se garantiza la autenticidad de la clave pública. En base a esto, el esquema anterior puede mejorarse utilizando un par de claves público-privadas una para cada una de las entidades participantes (A y B en este caso) y la inclusión de nonces (que denotaremos N1, N2,...) en los mensajes intercambiados. En concreto, el protocolo sería el siguiente:

1. A envía a B los datos  $N_1 + ID_A$  cifrados con la clave pública de B, a modo de identificación de la transacción.
2. B obtiene esos datos y envía  $N_2 + N_1$  a A, cifrado con su clave pública. Puesto que sólo B podría haber descifrado el mensaje enviado en 1, la presencia de  $N_1$  en este mensaje asegura a A que la entidad con la que se está comunicando es B.
3. A obtiene  $N_2 + N_1$  y envía a B  $N_2$  (con lo que demuestra a B que es realmente A) y una clave de sesión ( $K_S$  firmada).
4. B obtiene  $K_S$ . La firma garantiza que sólo A ha podido mandarlo y, al cifrarlo con la clave pública de B, se asegura de que sólo B puede recibirlo.

Por tanto, con este esquema se garantiza confidencialidad y autenticidad en los mensajes intercambiados.

#### 14.3.-Intercambio de claves secretas mediante criptosistemas híbridos

Las claves también pueden ser intercambiadas por criptosistemas híbridos, los cuales se sustentan bajo las características presentadas en el Apartado 8.3. La única diferencia es que, en este caso, la criptografía simétrica y asimétrica es conjuntamente útilizada para el intercambio de claves.

En concreto, un posible esquema se describe a continuación. El Centro de Distribución de Claves (CDC) distribuye claves maestras a cada usuario aplicando criptografía de clave pública y, posteriormente, distribuye claves de sesión cifrándolas con la maestra, es decir, aplicando criptografía de clave secreta. De este modo, se consigue una distribución eficiente de las claves de sesión, siendo posible que un único CDC pueda distribuir las claves entre un gran conjunto de usuarios.

#### 14.4.-Intercambio de claves públicas

Muchas han sido las técnicas propuestas para la distribución de claves públicas. Todas ellas se pueden agrupar en los protocolos de: anuncio público, directorio público, autoridad de clave pública y certificados de clave pública.

### Anuncio público

Dado que en la criptografía de clave pública todas las entidades disponibles de una clase que las demás pueden conocer, cualquier entidad puede mandar su clave pública a otra entidad o difundirla a un conjunto de entidades.

A pesar de la utilidad de esta propuesta, presenta el gran inconveniente de que cualquier entidad puede suplantar a otra. Si una entidad quiere suplantar a A, envía la clave pública a otras entidades y solo cuando A descubriese el problema, se alertaría de la situación.

### Directorio público

Es posible aumentar la seguridad haciendo uso de un directorio público en el que se encontrasen todas las claves públicas de las entidades participantes en intercambios de mensajes.

Para ello, una autoridad será la encargada de mantener el repositorio. Cada entidad puede depositar y actualizar su clave pública pero ambas operaciones se han de realizar físicamente o mediante algún tipo de comunicación autenticada.

Aunque este protocolo mejora la seguridad, es posible que un atacante consiga obtener o computar una clave privada asociada a una de las públicas almacenadas en el directorio, consiguiendo así poder suplantar a una determinada entidad, o alterar alguna de las claves almacenadas en el directorio.

### Autoridad de clave pública

Es necesario mejorar el control sobre la distribución de claves públicas. Al igual que en el protocolo anterior, se asume la existencia de un directorio y de una autoridad encargada de gestionarlo. Además, cada entidad tiene una clave privada y una pública, que deja en el directorio, de forma que la autoridad es la única que conoce la clave privada asociada a cada una de las públicas.

El protocolo presenta los siguientes pasos:

1. A envía un mensaje a la autoridad para conseguir la clave pública de B, incluyendo en dicho mensaje una marca de tiempo (T1).
2. La autoridad envía la clave de B firmada, y devuelve firmada tanto la solicitud como la marca de tiempo recibida. Posteriormente, A verifica la firma.
3. Posteriormente A envía a B un nance y su identificador cifrado con la clave pública de dicha entidad.
4. Los pasos 1-2 son repetidos por B para conseguir la clave pública de A.
5. B obtiene el nance enviado por A. Después, B crea otro nance, lo concatena con el recibido por A, lo cifra con la clave pública de A y se lo envía a dicha entidad.
6. A obtiene el nance creado por B y se lo devuelve cifrado con su clave pública.

Es importante considerar que los pasos 1, 2 y 5 han de ejecutarse periódicamente puesto que las claves públicas se pueden utilizar múltiples veces.

No obstante, las claves públicas han de actualizarse cada cierto tiempo para mantener la frescura de las mismas.

Al igual que en protocolos anteriores, a pesar de las mejoras introducidas, sigue presentando algunas debilidades. Por un lado, la autoridad podría suponer un cuello de botella por no ser capaz de satisfacer tantas peticiones como solicitudes se realicen. Por otro lado, atm sigue siendo posible la alteración del directorio.

### **Certificados de clave pública**

Como mejora del protocolo anterior se propone la utilización de certificados que permitan a los participantes intercambiar sus claves sin la necesidad de participación de ninguna autoridad.

Un certificado, como ya se ha comentado anteriormente, es un documento que vincula a una entidad con un par de claves (en el certificado sólo se almacena la pública). Por tanto, dado que las claves están vinculadas a un único usuario, este puede publicar su certificado sin miedo a ser suplantado.

#### **Sabía que ...**

El núcleo central del paquete es la carga útil, a la que es posible añadirle relleno, bien para dificultar la realización de ataques basados en el análisis de tráfico o bien conseguir paquetes de datos múltiplos de 32 bits.

## **15. USO DE HERRAMIENTAS DE CIFRADO TIPO PGP, GPG O CRYPTOLOOP**

En este apartado se describe el uso de una herramienta criptográfica, GPG, que es gratuita y de libre distribución. Se describirán los pasos fundamentales relacionados con la creación y uso de certificados, particularmente para el cifrado y descifrado de información. También se identificarán las opciones relacionadas con la firma. GPG constituye una alternativa de código libre a la herramienta PGP que, desde hace un tiempo, es comercializada por la empresa Symantec.

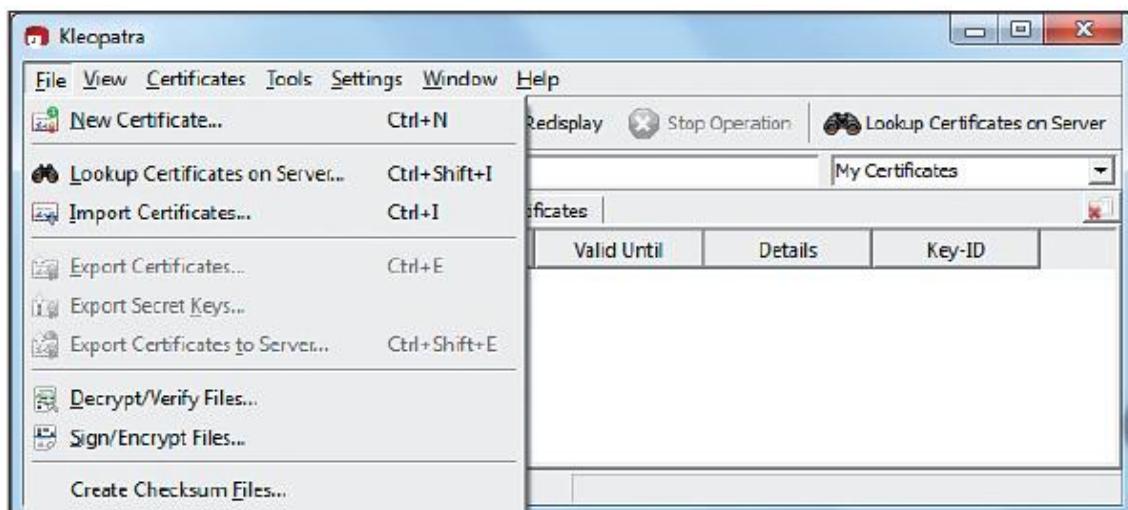
A pesar de que originalmente GPG estaba orientada a PGP, debe destacarse que también permite hacer uso de los certificados X.509.

La herramienta GPG permite cifrar y firmar documentos. Para la firma y, en general, para el cifrado de clave pública, es necesario disponer de un par de claves pública-privada junto con el certificado correspondiente. Para crear estos materiales, se hace uso de la utilidad Kleopatra, instalada junto con la herramienta.

### 15.1.-Creación del certificado

En lo referente a certificados, se permite la creación de certificados según el estándar openPGP o bien de acuerdo a la norma X.509. Las diferencias entre ambas cuestiones se han descrito anteriormente. En lo restante, se hará uso de un certificado openPGP.

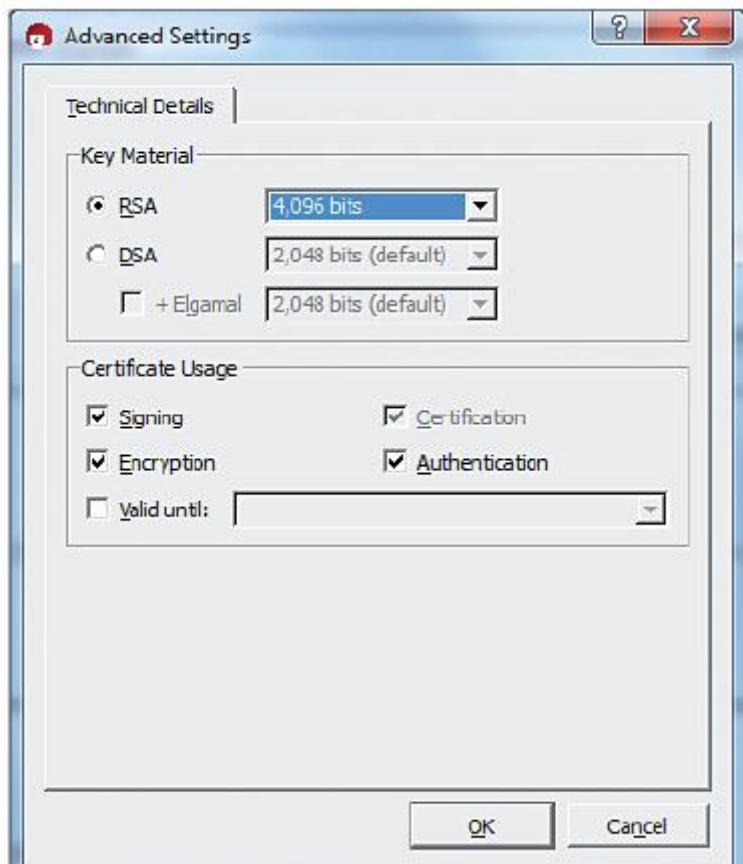
En el menú File --> New certificate, etc., Se introducen los datos identificativos y, en las propiedades avanzadas (Advanced settings), es recomendable establecer un tamaño de clave en función del uso previsto del sistema. La premisa es que cuanto mayor sea la longitud de la clave, mayor nivel teórico de seguridad ofrece el sistema.



Menú de creación de Nuevo certificado

En esta misma ventana se puede determinar para qué se quiere usar el certificado en cuestión.

Puede utilizarse para cifrar (Encryption), firmar (Signing), autenticarse electrónicamente (Authentication) y certificar a otras personas (Certification).



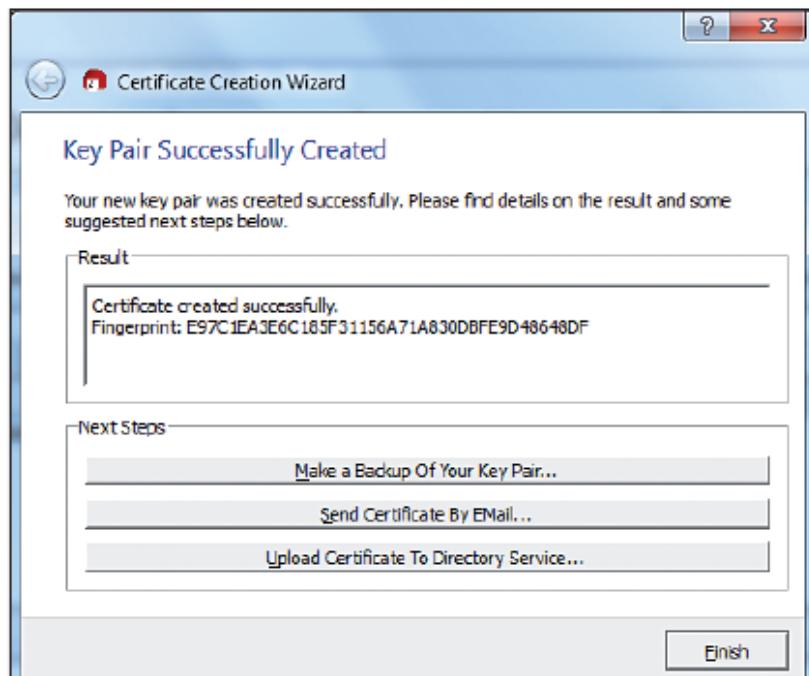
Propiedades avanzadas de creación de un certificado

**Recuerde**

**En el esquema PGP, cada uno de los participantes tiene la capacidad de certificar a los demás.**

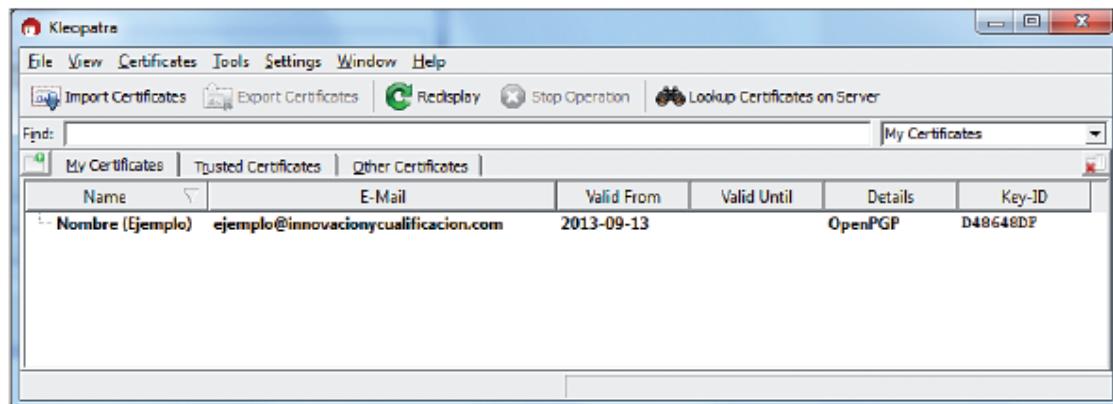
Durante el proceso de creación se pedirá una contraseña. Esta se utiliza para proteger el acceso a la clave privada. Una vez creado el certificado, es el momento de empezar a utilizarlo.

Es importante destacar que, para que otras personas sean capaces de enviar información cifrada utilizando la clave pública del portador del certificado, es imprescindible que conozcan dicha clave de antemano. Una de las formas más eficaces consiste en utilizar servicios de directorios, ya comentados anteriormente. Estos actúan a modo de páginas amarillas en tanto que almacenan el certificado de clave pública de una persona concreta.



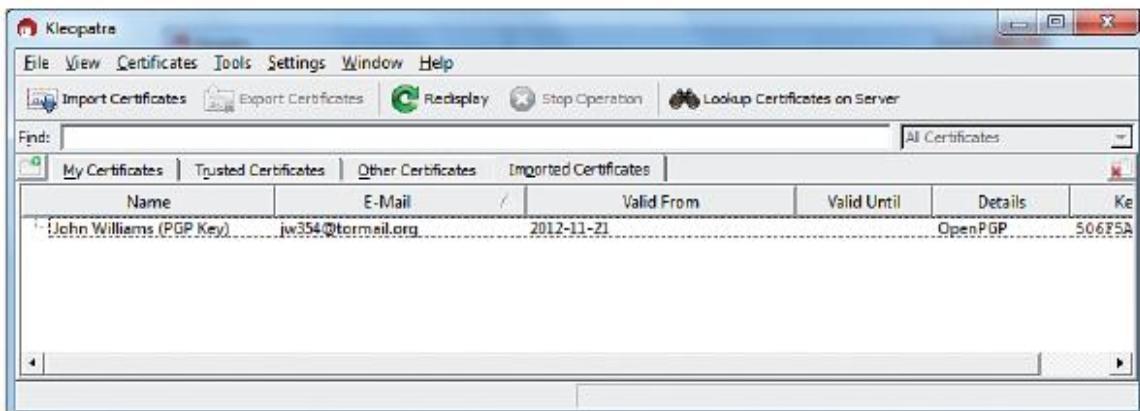
Ventana de confirmación de creación de certificado

Tras el proceso, se puede comprobar la correcta finalización del proceso en la pestaña principal de Kleopatra.



Resultado de la creación del certificado

Haciendo uso de la ventana Import certificates, es posible importar los certificados de otros usuarios en el propio sistema. Una vez realizada esta acción, dichos certificados aparecen en la pestaña Imported certificates:

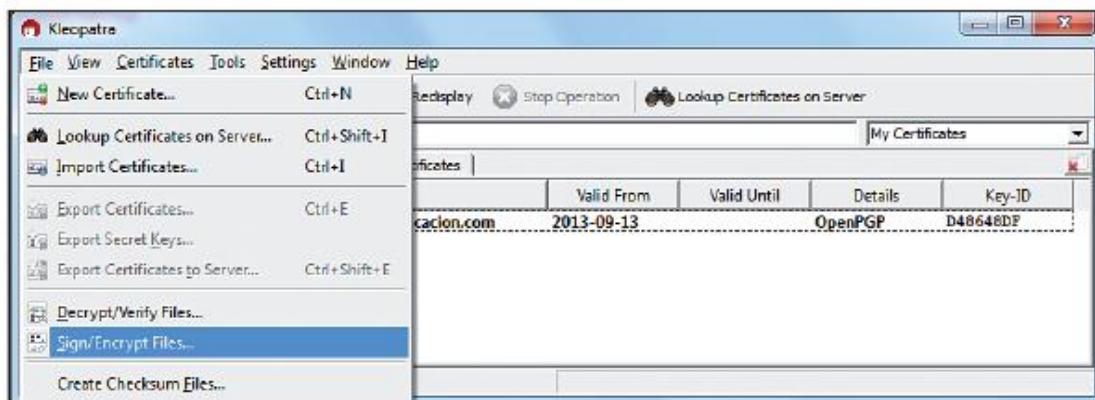


Pestaña de certificados importados

### 15.2.-Uso del certificado para cifrar

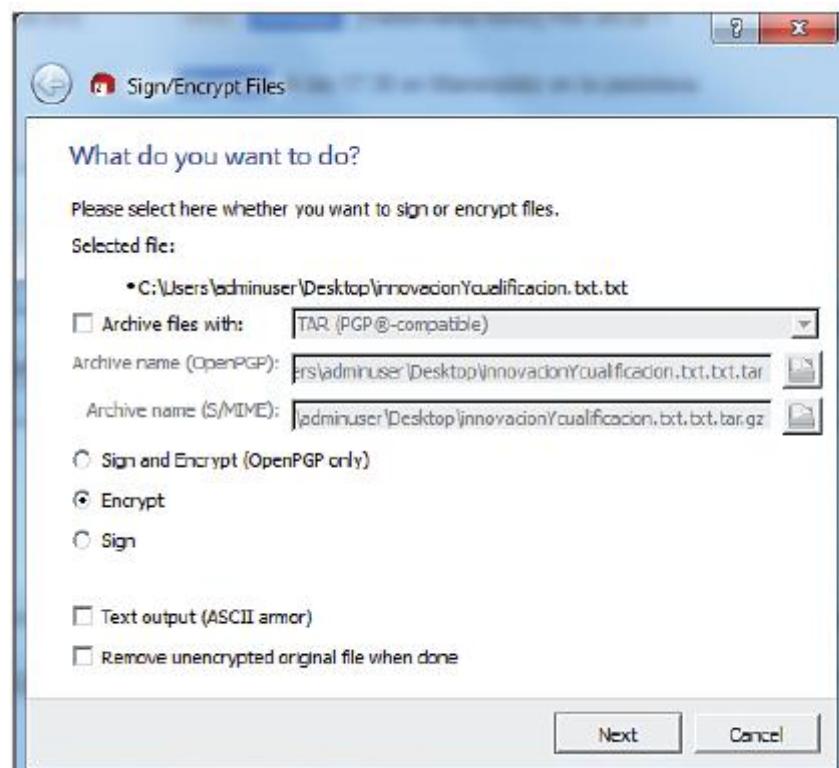
El primer paso para cifrar un fichero es seleccionar la opción de cifrar (Sign/encrypt files).

Tras esto, se escogen las opciones de solo cifrar (Encrypt) y se selecciona el destinatario deseado.

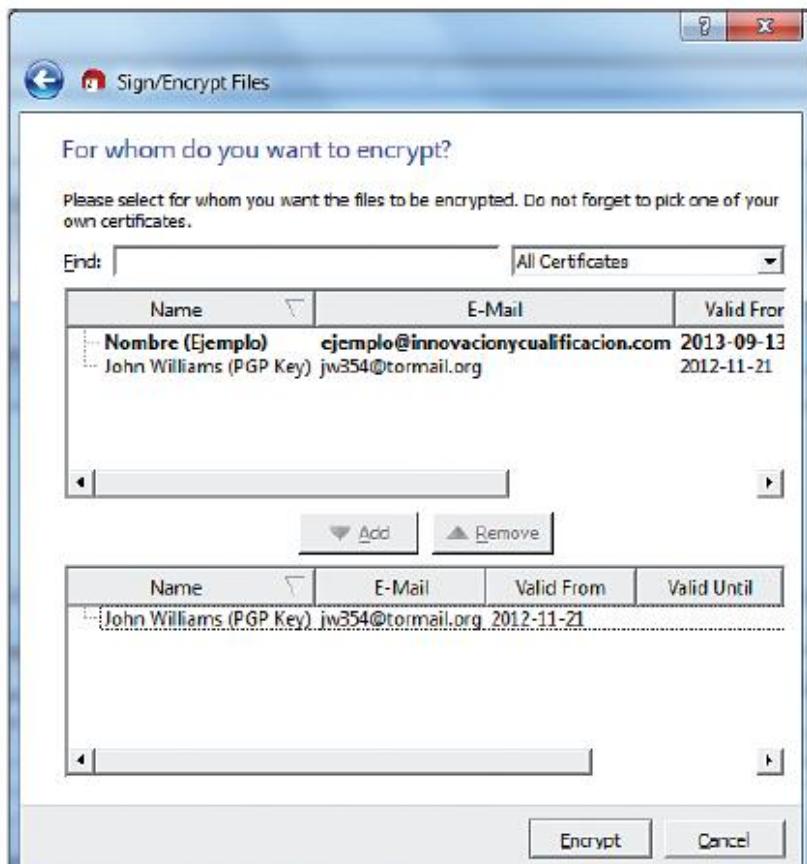


Cifrado de un fichero: selección de opción.

En la figura, el mensaje se cifra utilizando la clave pública contenida en el certificado de John Williams.



Cifrado de un fichero: selección de alternativas



Cifrado de un fichero: selección de destinatarios

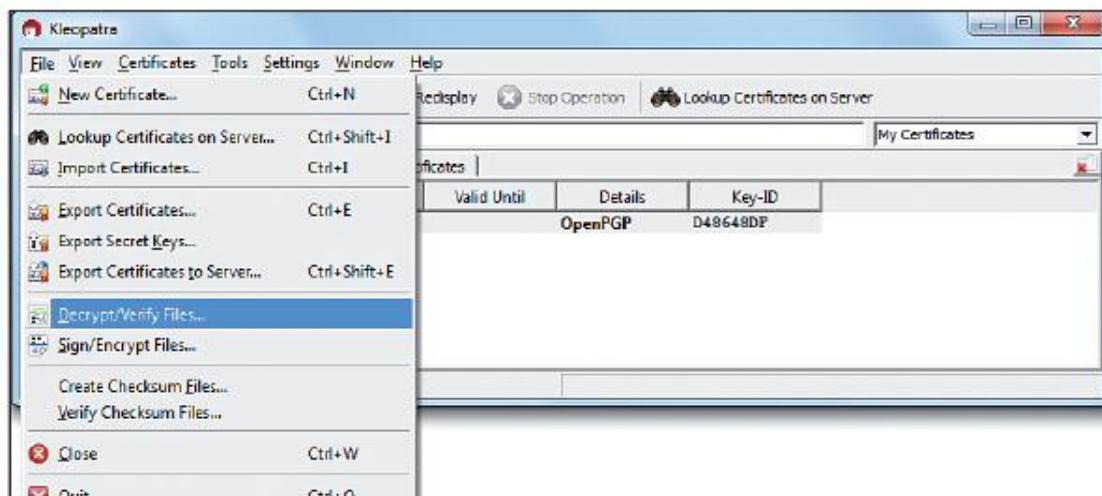
El proceso de firma es análogo al descrito hasta el momento, con la salvedad de que no se escogen certificados de terceros para realizar la operación, sino certificados propios.

#### Recuerde

Para la realización de una firma digital es necesario disponer de la clave privada del firmante. Por ello, la herramienta permite escoger cuál de los certificados de clave pública de los que tiene la clave privada quiere utilizar para realizar esta operación.

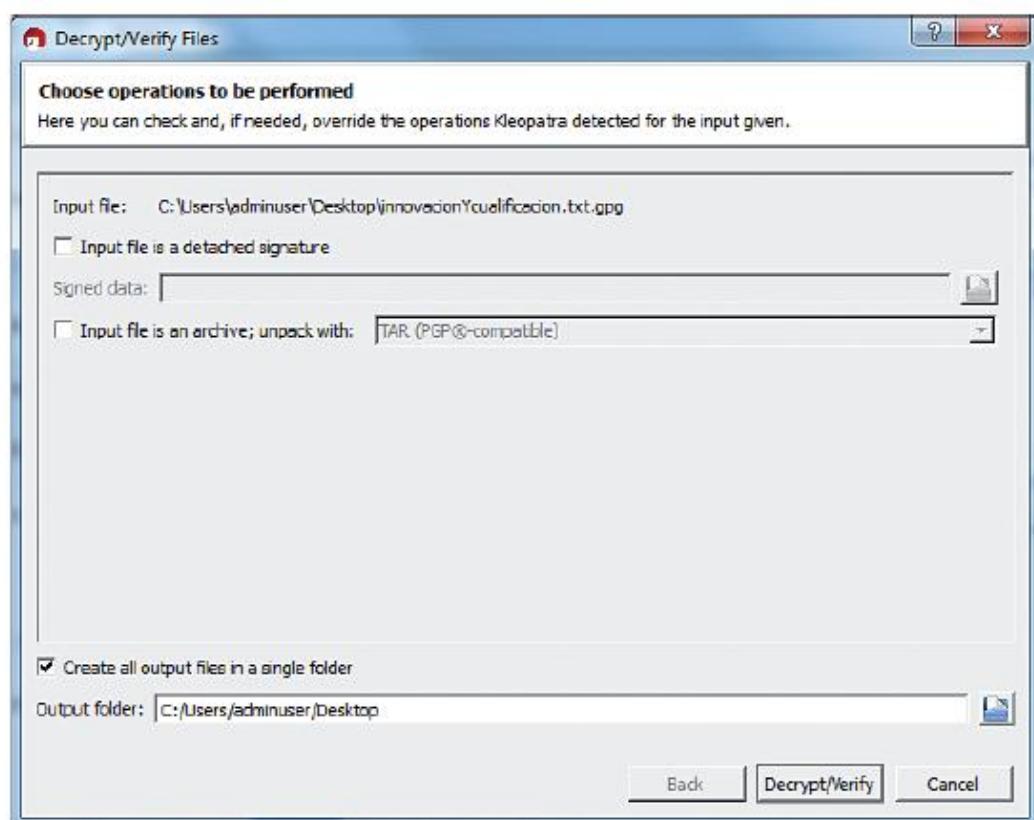
#### 15.3.-Descifrando un fichero recibido

Una vez que se ha recibido un fichero cifrado con la clave pública de quien lo recibe, la herramienta permite descifrarlo para obtener su contenido original. Para ello, es necesario utilizar la opción de descifrado y verificación de firma del menú principal.



Opción de descifrado de ficheros

Tras seleccionar el archivo (que tendrá extensión gpg), aparece la ventana de selección de opciones. Para realizar el descifrado, es suficiente con dejar todas las casillas desmarcadas.



Propiedades del descifrado de ficheros

Estas opciones vienen motivadas porque el menú de descifrado también sirve para verificar la firma sobre un fichero. Así, para realizar el descifrado bastará con dejar las casillas desmarcadas.

Si, por el contrario, se estuviese verificando una firma, la primera casilla permitiría determinar si el fichero seleccionado contiene solo la firma y, en dicho caso, habría que indicar en ese espacio cuál es el fichero que se firmó.

Tras confirmar las propiedades anteriores, la herramienta solicita la contraseña asociada a la clave privada del usuario. Como se dijo anteriormente, cualquier operación que involucre a la clave privada conlleva el uso de la contraseña para evitar usos malintencionados.

## 16. RESUMEN

La criptografía es una disciplina técnica fuertemente relacionada con la protección de la información. A lo largo de la Historia ha sufrido una extraordinaria evolución. Los sistemas de criptografía clásicos se pueden dividir en sistemas monoalfabéticos, como el de César, o los polialfabéticos, como el de Vigimere. Todos ellos compartían la misma propiedad: la clave de cifrado era la misma que la de descifrado. Por ello, se conocían como sistemas de clave secreta o simétrica. Fue en 1976 cuando surgió la criptografía de clave pública o asimétrica, pasando a utilizarse un par de claves: una pública y una privada.

Dependiendo de las necesidades, la criptografía permite satisfacer unas propiedades de seguridad u otras. La elección se realiza en base a los usuarios que están implicados en la comunicación (autenticidad), la prevención de accesos no autorizados (confidencialidad), la prevención de modificaciones del mensaje (integridad), la prevención de envíos no deseados (no repudio), el seguimiento de las acciones realizadas (imputabilidad) y el conocimiento de la fecha en la que se produce la comunicación (sellado de tiempo).

Sin embargo, la satisfacción de las propiedades de seguridad depende de la aplicación de numerosos mecanismos, como son el cifrado, la firma o la creación de resúmenes. La criptografía simétrica y asimétrica proporcionan las herramientas fundamentales para aplicar los mecanismos anteriores, siendo imprescindible escoger la más apropiada en cada caso. Por ejemplo, la criptografía simétrica se caracteriza por su rapidez, mientras que la asimétrica presenta la ventaja de no necesitar un canal seguro para intercambiar las claves de cifrado. Además, dado que en ambos tipos de criptografía los usuarios tienen que intercambiar claves, el protocolo a utilizar ha de considerarse. Hay que analizar, entre otras cosas, si el intercambio se realiza entre emisor y receptor o si es necesaria una entidad intermedia.

Una cuestión especialmente relacionada con los sistemas de clave pública es asegurar la identidad de su propietario. En este sentido surgen los certificados de clave pública.

## CAPÍTULO 2 APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

### 1. INTRODUCCIÓN

La aparición de la criptografía de clave pública en 1976 supuso el nacimiento de un nuevo paradigma en el aseguramiento de las comunicaciones. Ya no era necesario disponer de una clave compartida entre los comunicantes, sino que era suficiente con conocer la clave pública del otro interlocutor.

La pregunta que surgía a raíz de esta cuestión era: ¿cómo asegurar que la clave pública realmente pertenecía al otro interlocutor? Era necesario establecer un vínculo verificable de forma electrónica entre la identidad de la persona y su clave pública asociada.

En este contexto surgen las infraestructuras de clave pública (habitualmente referidas como PKI, del inglés *Public Key Infrastructure*), cuya misión es gestionar el ciclo de vida de los certificados de clave pública, que como se introdujo con anterioridad son documentos que vinculan una identidad y su clave pública.

En este capítulo se presentan en profundidad las infraestructuras de clave pública y sus certificados asociados. Dado que en el terreno electrónico no sólo es importante autenticar, sino también comprobar si se tienen privilegios suficientes para realizar una acción, en este capítulo se introducen también las infraestructuras de gestión de privilegios (o PMI, del inglés *Privilege Management Infrastructure*), que se encargan de instrumentar la concesión, verificación y revocación de privilegios a una entidad.

### 2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES

En una infraestructura de clave pública (en adelante, PKI) figuran todas las entidades que se relacionan, de alguna manera, con la gestión de certificados de clave pública. La norma que regula la existencia de estas entidades y su modelo de relaciones es la ITU-T X.509. Más allá del titular del certificado, existe un amplio conjunto de autoridades que participan en la emisión, renovación, verificación (uso) y revocación del mismo. En este apartado se presentan dichas entidades y posteriormente se introducirá su modelo de relaciones.

#### 2.1.- Entidades participantes

La entidad que emite un certificado de clave pública se denomina **Autoridad de Certificación** (en adelante CA, del inglés *Certification Authority*). Sus funciones son similares a las de un notario, en tanto que acredita o certifica la identidad de una determinada entidad. Esta cuestión es clave para la autenticación, la cual es fundamental para una parte importante de los intercambios de datos que se producen en Internet.

A pesar de que una CA puede estar formada por múltiples entidades internas (sistemas, departamentos, etc.), desde el punto de vista externo existen dos atributos que la identifican: su nombre y su clave pública.

Una CA realiza cuatro funciones fundamentales: emitir certificados, mantener información actualizada sobre el estado de los certificados y emitir listas de certificados revocados, hacer públicos estos datos para que los usuarios puedan emplearlos en sus servicios de seguridad y mantener un archivo histórico sobre el estado de aquellos certificados que ya están caducados.

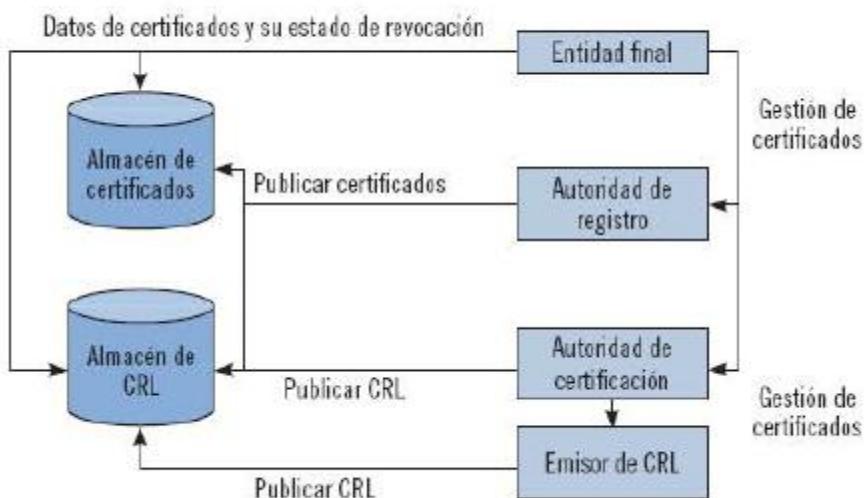
Una cuestión importante es que, dado que los certificados son firmados utilizando la clave privada de la CA, dicha clave es fundamental para garantizar la seguridad del proceso.

Sabía que ...

Si se compromete la clave privada de una CA, un atacante puede emitir certificados de forma fraudulenta. Esto puede dar lugar a ataques de suplantación, que son la base de otros conocidos como “phising”.

En el marco de una PKI, las CA se relacionan con otras muchas entidades, como muestra la figura siguiente.

Elementos de una infraestructura de clave pública (PKI) [Adaptado de RFC 5280]



Los certificados de clave pública (descritos en profundidad con anterioridad y referidos como PKC, del inglés *Public Key Certificate*) sirven para que la CA acredite que la entidad a la que se refiere el certificado conoce la clave privada asociada a la pública que figura en dicho documento.

Si la CA incluye información adicional en el PKC, también se acredita que dichos datos se relacionan con el sujeto del certificado. Los PKC se pueden emitir para un usuario final, o bien para otras CA. En este segundo caso, surgen las denominadas como cadenas de certificación, que se presentan en el siguiente epígrafe.

Para el proceso de emisión, las autoridades de certificación deben verificar la identidad de la entidad final. Por este motivo, las CA pueden delegar esta tarea (entre otras) a una Autoridad de Registro (AR). Es importante tener en cuenta que la AR debe verificar no solo la identidad, sino también los datos que figuren en el certificado. A diferencia de lo que sucede con las CA,

generalmente la gestión de una AR la realiza una única persona (como por ejemplo un funcionario que atiende en una determinada oficina). Para reflejar que la AR ha verificado los datos, habitualmente esta firma una constancia. La CA verifica dicha firma para tener constancia de este hecho. Así, al igual que ocurría en la CA, la custodia de la clave privada de la AR es fundamental para garantizar la seguridad.

Acerca de la revocación, se distingue por su importancia el emisor de listas de certificados revocados (*CRL issuer*), que se introducirá más adelante. Debe tenerse en cuenta que, tanto las tareas de la Autoridad de Registro como de la emisión de CRL, pueden ser realizadas por la propia CA.

Finalmente, para difundir los certificados de clave pública y las listas de certificados revocados, la norma X.509 identifica un repositorio dentro de la arquitectura. Debe notarse que este es solo uno de los mecanismos para la difusión de esta información, de acuerdo a lo ya expuesto anteriormente.

Una cuestión importante con respecto a los repositorios es que deben ser interoperables. De otra manera, una persona que reciba un certificado de una entidad certificada por una CA no sabría cómo obtener el estado de los certificados a menos que conociese previamente esa CA.

Gracias a la interoperabilidad, cualquier persona puede consultar los repositorios de cualquier CA, puesto que todas hacen uso de un protocolo de comunicación común.

Además de los repositorios, donde la información queda a disposición de los usuarios para que accedan a ella, habitualmente se distinguen en las PKI los archivos. Estos tienen como misión servir de almacén histórico confiable. Así, se encargan de garantizar la custodia de la información durante largo tiempo, asegurando que esta no ha sido modificada desde que se introdujo. Gracias a los archivos es posible conseguir una doble finalidad. Por un lado, se permite resolver disputas que tengan que ver con certificados que ya caducaron. Por otro, se hace posible verificar firmas realizadas en el pasado, como podría ser el caso de un testamento electrónico.

Gracias a la interoperabilidad, cualquier persona puede consultar los repositorios de cualquier CA, puesto que todas hacen uso de un protocolo de comunicación común.

Además de los repositorios, donde la información queda a disposición de los usuarios para que accedan a ella, habitualmente se distinguen en las PKI los archivos. Estos tienen como misión servir de almacén histórico confiable. Así, se encargan de garantizar la custodia de la información durante largo tiempo, asegurando que esta no ha sido modificada desde que se introdujo. Gracias a los archivos es posible conseguir una doble finalidad. Por un lado, se permite resolver disputas que tengan que ver con certificados que ya caducaron. Por otro, se hace posible verificar firmas realizadas en el pasado, como podría ser el caso de un testamento electrónico.

## 2.2.- Modelo de relaciones

Las autoridades en una PKI se relacionan habitualmente de manera jerárquica. No obstante, más adelante se presentarán otras alternativas.

En el modelo jerárquico, se establece una CA raíz en la que se deposita toda la confianza. Por debajo de esta CA pueden existir una o varias CA subordinadas, las cuales tienen la potestad de emitir y gestionar certificados digitales.

**Sabía que ...**

En Internet existen infinidad de Autoridades de Certificación que forman parte de una infraestructura de clave pública. No obstante, cualquier empresa puede hacer uso de programas de código abierto (como EJBCA) que permiten crear su propia infraestructura de clave pública para uso empresarial.

Es importante destacar que gracias a la existencia de CA intermedias aparece el concepto de cadenas de certificación. Así, el certificado de una entidad final (por ejemplo, un usuario) puede ser emitido por una CA intermedia (por ejemplo, CA2), que depende de otra CA intermedia (por ejemplo, CA1) que es subordinada a su vez de la CA raíz. La siguiente imagen representa esta situación a modo de ejemplo, en la que se observa que la Autoridad "Fraunhofer Service CA 2007" es subordinada de "Fraunhofer Root CA 2007" y esta, a su vez, de "Deutsche Telekom Root CA 2".

Las cadenas de certificación permiten llevar al mundo real las PKI, dado que la gestión de los certificados de una entidad puede ser distribuida entre varias CA intermedias o subordinadas.

Considérese, por ejemplo, la distribución territorial de un país como España: es más sencillo que exista una CA subordinada por cada Comunidad Autónoma (dependiendo todas ellas de una única CA regida por el Gobierno central) que si existiese una única CA raíz que gestionase todos los certificados de los ciudadanos.



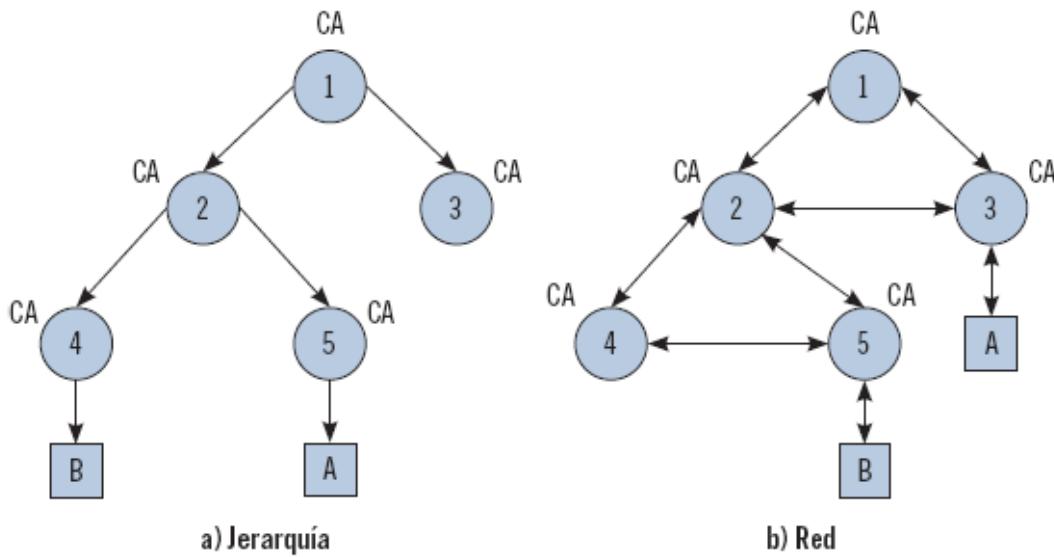
Ejemplo de cadena de certificación

### 2.3.- Arquitecturas de una PKI

Uno de los retos prácticos de las PKI es su aplicación en una empresa. Tradicionalmente se puede distinguir, además de la arquitectura jerárquica introducida anteriormente, la arquitectura en red (*mesh*). Además, para conseguir conectar dos PKI que están en distintas empresas entre las que se desea establecer un vínculo, se desarrolla la arquitectura de puente (*bridge*).

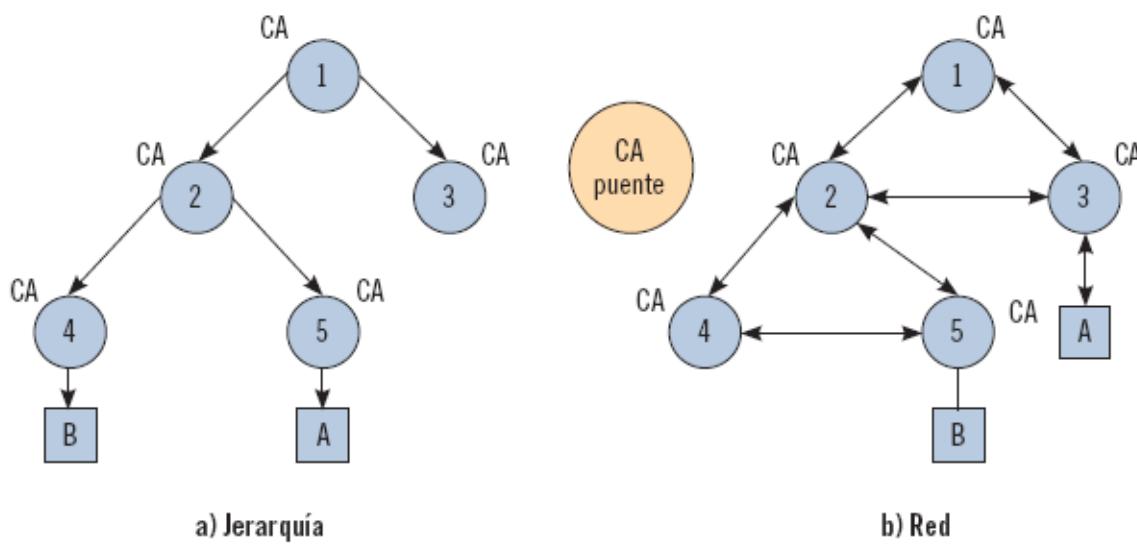
A continuación, se presentan ambas arquitecturas:

- **Red:** las CA se verifican independiente unas a otras, dando como resultado una red de confianza entre las CA cercanas. Una entidad final conoce la clave pública de la CA generalmente más cercana y verifica la cadena de certificación en base a las CA de confianza. Por ejemplo, en la imagen siguiente, suponiendo que la entidad A desea verificar el certificado de B y dado que A conoce la clave pública de CA3, la cadena de certificación más corta y la cual puede ser verificada por A es CA5, CA2 y CA3. A diferencia de este, la imagen muestra una arquitectura jerárquica en la que A, para verificar el certificado de B, ha de validar la cadena CA4, CA2 y CA1.

**PKI arquitecturas**


- Puente: este tipo fue diseñado para conectar las PKI de dos empresas con independencia del tipo de arquitectura (jerárquica o de red). Para ello, se introduce una nueva CA, denominada CA puente (*Bridge CA*), cuya función es establecer relaciones entre las PKI de las empresas correspondientes.

Una CA puente establece relaciones entre diferentes PKI. Estas relaciones pueden utilizarse para establecer un puente de confianza entre las entidades finales, (por ejemplo, usuarios), de las empresas asociadas. Si la arquitectura modo puente se construye sobre una arquitectura en jerarquía, la CA puente establecerá una relación con la CA raíz. Por el contrario, si la arquitectura es de red, la CA puente solo establecerá una relación con una de las CA de la red. La CA que establece relación con la CA puente recibe el nombre de CA principal. Un ejemplo de CA puente se muestra en la siguiente imagen.

**PKI arquitectura puente**


## Arquitectura física

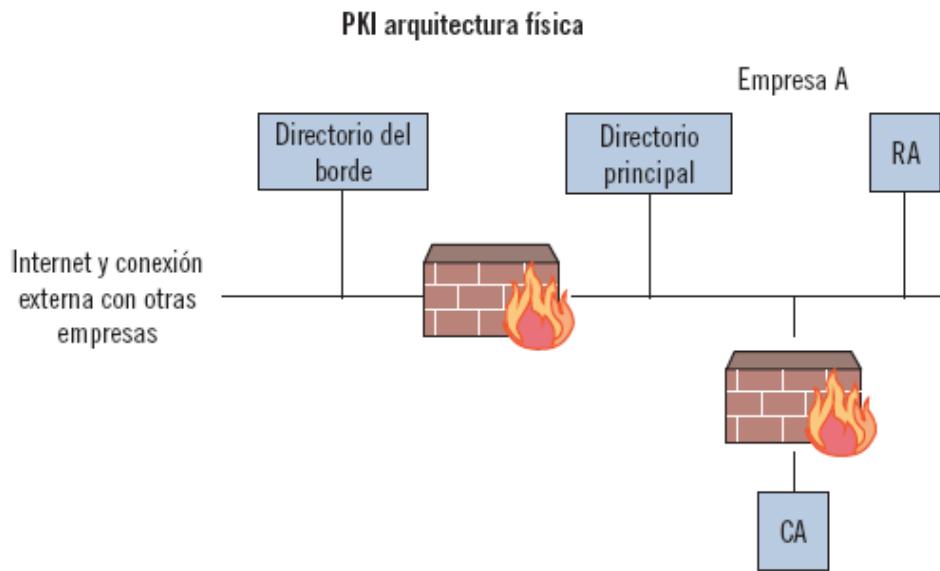
Hay múltiples formas de crear una arquitectura física de PKI, siendo recomendable que los componentes de la PKI se implanten en sistemas separados. Se aconseja pues que la CA, la RA y los repositorios se encuentren en sistemas independientes, consiguiendo que los datos sensibles se sitúen detrás del cortafuegos de la empresa. En concreto, la protección del sistema de las CA es muy importante porque si este resulta comprometido el sistema sería susceptible de ataques y habría que volver a crear todos los certificados afectados. Por ello, el sistema de CA ha de localizarse detrás del cortafuegos, el cual, además, ha de permitir la comunicación entre todos los sistemas que participen.

### Definición

#### Cortafuegos

En inglés conocido como firewall, es un sistema de seguridad (hardware o software), equiparable con una barrera, encargado de controlar el tráfico entrante y saliente a una red.

Una de las soluciones más comunes se basa en crear un directorio, en el que se almacenan las claves públicas, situado en el exterior del cortafuegos. A este directorio, dada su localización, se le conoce con el nombre de directorio de borde. Por otra parte, habría un directorio principal, dentro del cortafuegos, el cual actualizaría periódicamente el directorio de borde. Por este motivo, al directorio de borde accederían las entidades de las empresas externas y al directorio principal accederían las entidades de la propia empresa. Todo lo comentado se presenta en la siguiente imagen.



### 3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS

Tal y como se introdujo anteriormente, la CA se encarga de la gestión del ciclo de vida de los certificados que expide. Dentro de ese ciclo de vida se identifican una serie de funciones de gestión, que se introducen a continuación. Posteriormente, y dado que la CA puede formar parte de una cadena de certificación, se presenta el proceso de validar la misma.

#### 3.1.- Funciones de gestión

La norma X.509 establece 7 funciones de gestión que tienen lugar en las relaciones entre una entidad final (por ejemplo, un usuario) y la CA.

En primer lugar, se identifica el registro, que constituye el primer acercamiento de la entidad a la CA. Esencialmente, permite que esta se identifique frente a la CA. De acuerdo a la descripción presentada anteriormente, esto puede realizarse directamente o a través de una entidad intermedia, tal como la Autoridad de Registro (AR).

En segundo lugar, la operación de inicialización es fundamental para que la entidad final pueda ser capaz de verificar los certificados recibidos. En esta operación se envían a dicha entidad todos los materiales necesarios para hacer posible dicha verificación, lo cual incluye todas las claves públicas de las CA que participan en la PKI (tanto intermedias como raíz). En la inicialización, la entidad final también recibe típicamente su par de claves pública-privada.

Debe notarse que este par puede no ser único y que, de hecho, es habitual contar con más de un par (por ejemplo, uno para autenticación y otro para firma).

#### Sabía que ...

En el DNI electrónico se incluyen dos pares de claves, junto con sus certificados correspondientes, para distinguir las operaciones de autenticación electrónica y firma electrónica.

La tercera operación es la certificación propiamente dicha, en la que se emite el certificado de clave pública que acredita que la clave pública pertenece a la entidad correspondiente. Dicho certificado puede enviarse directamente a la entidad final interesada, o puede ponerse a disposición de los usuarios en el repositorio mencionado anteriormente.

Por otra parte, se identifican dos operaciones relacionadas con el mantenimiento del par de claves de la entidad final. Por un lado, como medida de precaución debe existir una función que permita realizar **una** copia de respaldo de dicho par, a fin de que el usuario pueda recuperarla en caso de

pérdida (por ejemplo, si se pierde un *pen-drive* en el que se había almacenado este material). Además, debe existir otra función que permita actualizar el par de claves. Esta función es conveniente por un doble motivo. El primero es dificultar los ataques que pretendan adivinar o averiguar la clave privada de la entidad en juego. El segundo es limitar el posible impacto que ese ataque pudiera tener: al renovar el par de claves, las operaciones siguientes harán uso de este nuevo par. De esta manera, una firma electrónica realizada con el par antiguo carecería de validez.

Precisamente, con la misión de reducir los efectos de un posible ataque o pérdida de una clave, surge la operación de revocación de la clave, de la que se hablará posteriormente.

La última función está relacionada con la certificación cruzada, es decir, con la posibilidad de que una CA pueda emitir un certificado para otra CA que le permita a la segunda emitir certificados que sean válidos también para la primera.

### 3.2.- Validación de una cadena de certificación

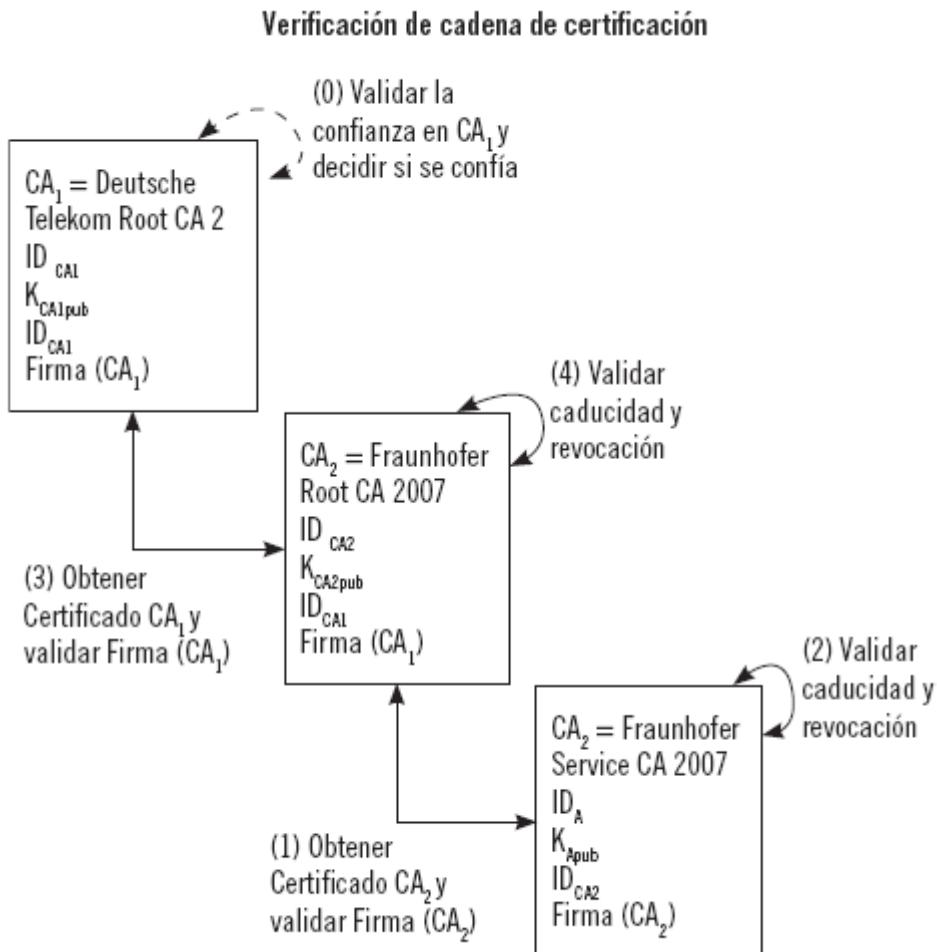
El proceso de validación de una cadena de certificación tiene por objetivo determinar si un certificado de una entidad final ha sido emitido, directa o indirectamente, por una CA de confianza. El proceso, por tanto, persigue comprobar que:

- El primer certificado de la cadena pertenece a una CA de confianza o ha sido emitido por ella. De acuerdo a la norma X. 509, este certificado es auto-firmado (es decir, se refiere a la misma entidad que lo firma).
- Para cada uno de los certificados intermedios, se cumple que:
  - La entidad que figura como sujeto de un certificado es la que emite el certificado siguiente.
  - Todos los certificados en juego eran válidos en el momento de su utilización.
- El último certificado de la cadena es el de la entidad final que participa en el proceso.
- A lo largo de la cadena no pueden producirse ciclos (un mismo certificado no puede aparecer más de una vez).

A lo largo de la comprobación se verifica la firma electrónica de cada uno de los certificados, utilizando el algoritmo especificado en el mismo.

Además de lo anterior, en el proceso se comprueba que la política de cada uno de los certificados es coherente con la de los demás y con el uso previsto en la acción que dio inicio al proceso de verificación. Debe notarse que, puesto que pueden existir diferentes certificados para una misma entidad, cada uno con una política distinta, el proceso de verificación puede requerir analizar más de una posible secuencia de certificados que lleven desde la entidad final a la CA raíz de confianza.

En relación con el ejemplo presentado anteriormente, en la siguiente imagen se muestra la cadena de certificación de la Autoridad “Fraunhofer Service CA 2007”, la cual es subordinada de “Fraunhofer Root CA 2007” y esta, a su vez, de “Deutsche Telekom Root CA 2”. Como se puede comprobar en la imagen, el proceso consiste, principalmente, en verificar la firma de cada uno de los certificados que aparecen en la cadena, así como la caducidad y revocación de los mismos.

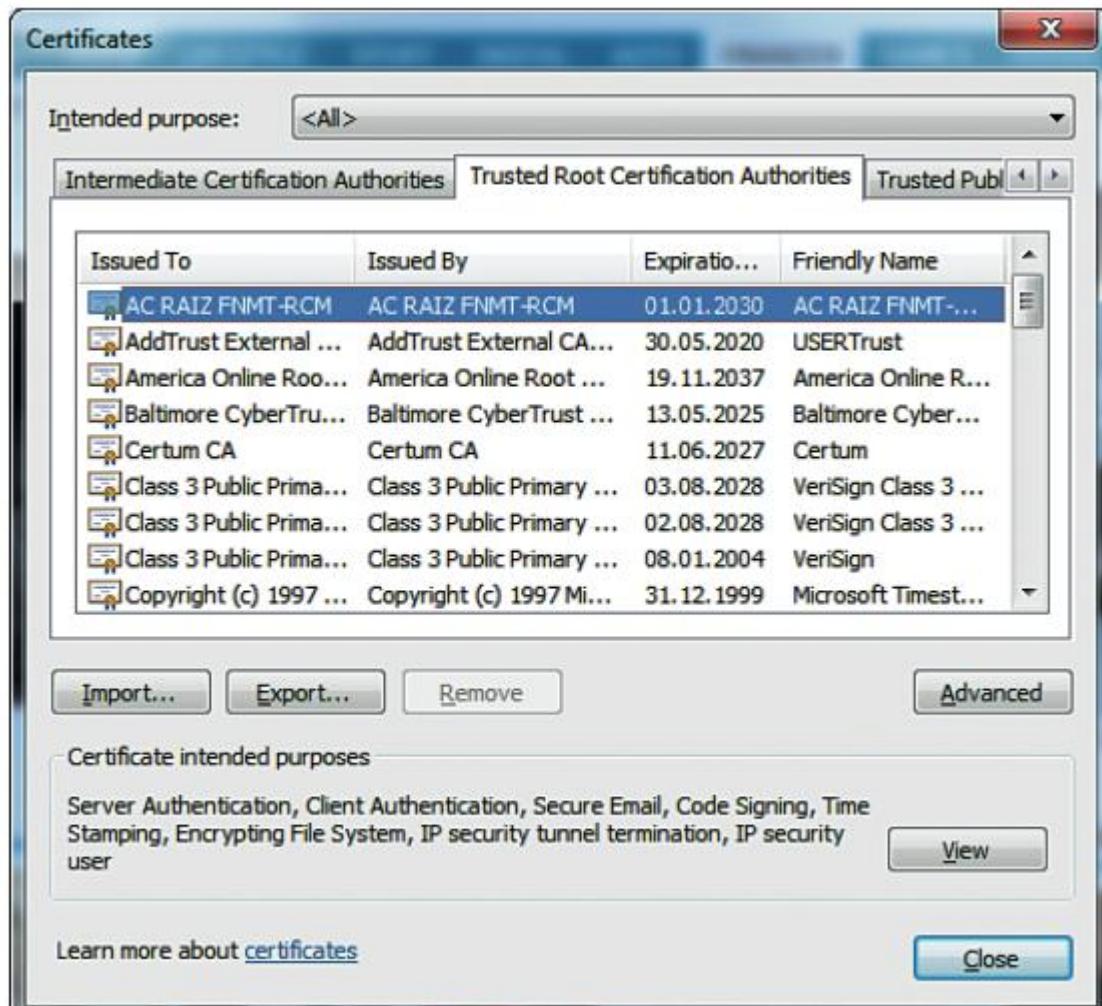


### 3.3.- Aspectos prácticos: validación en los navegadores

Como parte de la navegación por Internet, los navegadores realizan de manera automática la validación de los certificados. Esto ocurre, por ejemplo, cuando se ingresa en una página utilizando el protocolo SSL, que se presentará más adelante.

Gracias a esta validación, el usuario que navega puede tener la plena garantía de que se está conectando a la página legítima y no a una copia manipulada.

Para que esta validación se pueda realizar de manera automática, el navegador debe conocer cuáles son las CA raíz que son confiables. Para ello, los navegadores incorporan en su interior un gestor de certificados en el que vienen preinstalados los certificados de aquellas CA que se consideran confiables. La siguiente imagen muestra el gestor de certificados que puede visualizarse en Internet Explorer. Para mostrarlo, debe utilizar el menú Opciones de Internet y pulsar el botón Certificados dentro de la pestaña Contenido.



*Gestor de certificados*

En el caso de que una página utilice un certificado que no haya sido emitido por una CA raíz de confianza, el navegador mostrará un aviso al usuario, indicando que no se puede acreditar la identidad del sitio web al que se está accediendo.



*Aviso de seguridad del navegador Google Chrome por certificado no confiable*

Este tipo de avisos son fundamentales para evitar ataques tipo *phising*, tales como aquellos que replican la página de un banco y emplean ingeniería social para engañar al usuario. Por este motivo, las últimas versiones de los navegadores muestran mensajes sencillos de comprender pero transmitiendo la sensación de alerta al usuario.

Algo similar sucede cuando el certificado tiene problemas en cuanto a su validez. Si el certificado no es válido o ya ha expirado, el navegador también muestra habitualmente un mensaje sobre esta cuestión.



Aviso de seguridad del navegador Internet Explorer, por certificado caducado o no válido

#### 4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)

En base a la RFC 3647, de carácter informativo, se describen los conceptos de Política de Certificación (en adelante CP del inglés Certification Policy, CP) y Declaración de Prácticas de Certificación (del inglés Certification Practice Statement, CPS), presentándose en este apartado tanto la definición de cada uno de estos conceptos como las diferencias entre ambos.

##### 4.1.- Política de certificación

Considerando que un certificado es emitido por una determinada CA, vinculando a una entidad final (por ejemplo, un usuario) con un par de claves, hay que determinar el grado con el que el usuario puede confiar en el certificado obtenido.

##### Recuerde

En el certificado digital solo se almacena la clave pública, pues la privada debe ser solo conocida por su propietario.

Este proceso ha de ser realizado por el propio usuario o alguna entidad que controle el modo en el que los usuarios o sus aplicaciones hacen uso de los certificados. Muchos pueden ser los certificados utilizados, así como las aplicaciones y objetivos de cada uno de ellos.

En particular, en el estándar X.509 una CP se define como "un conjunto de reglas que indican la aplicación de un certificado en una comunidad y 1 o en un tipo de aplicación con objetivos comunes de seguridad". En base a esto, se distinguen un par de categorías: las CP que indican la aplicación de un certificado en una comunidad concreta, enfocadas a establecer los requisitos para el uso de los certificados y para los miembros de la comunidad que hace uso de ellos; y las CP que indican la aplicación de un certificado a un tipo de aplicación con unos objetivos comunes de seguridad, cuyo propósito es identificar el conjunto de aplicaciones y los usos de los certificados y establecer los niveles de seguridad en cada caso, los cuales se dividen en tipos o clases. Además, esta última categoría establece los requisitos que la PKI ha de cumplir en las aplicaciones y usos identificados.

Las CA se pueden asociar con una guía para ayudar a los usuarios a determinar si el certificado que van a utilizar es apropiado para el uso que una aplicación concreta va a hacer de él. Por ello, las CA son responsables de que los certificados que emitan estén conformes a la CP asociada.

Es posible cuestionarse la necesidad de las CP, pero la respuesta es sencilla. Los certificados proporcionados en una PKI tienen un propósito concreto, por estar vinculados a una determinada aplicación, y por ello es importante el establecimiento de una CP que indique los usos de los certificados expedidos.

Las CP se identifican con un Identificador de Objeto (*Object Identifier, OI*). Dicho identificador, o al menos sus primeros dígitos, puede ser registrado y asociado con una organización en concreto, siendo la entidad que realiza el registro la que puede publicar el texto de las CP. Cada certificado está asociado a una o múltiples CP, indicándose este hecho dentro de las extensiones de los certificados X.509, en concreto en el campo "Políticas del certificado".

Por otra parte, las CP también establecen las bases para las auditorías, las acreditaciones y otras cuestiones de evaluación de las CA. Cada CA puede evaluarse contra una o varias CP (o CPS). Además, cuando una CA emite un certificado para otra CA, la emisora debe evaluar todas las CP que hacen que pueda confiar en la CA sujeto, incluyendo dichas CP en el certificado ex-pedido.

#### 4.2.- Declaración de prácticas de certificación

El término CPS se define como "declaración de las prácticas que una CA ha de realizar a la hora de ex-pedir certificados". La CPS establece las prácticas en base al ciclo de vida de los servicios con los que se asocie. Asimismo, incluye la emisión, la revocación y la renovación de certificados. De forma más extensa, una CPS se puede definir como una declaración realizada por una determinada CA que indica la confianza del sistema asociado y los procedimientos utilizados en la ejecución de las operaciones realizadas. Por tanto, las entidades participantes en una PKI pueden hacer uso de las CPS para seleccionar a la CA entre todas las posibles, de modo que podamos depositar confianza en la CA escogida y se obtenga un certificado confiable.

En ocasiones es posible que las PKI no necesiten realizar una extensa CPS, siendo las propias CA las que conozcan los servicios a utilizar y confíen en ellos. En este caso, los certificados tendrían poco nivel de aseguramiento, siendo útiles en casos en los que las aplicaciones a las que afecten, aun comprometidas, no supusiesen un alto riesgo. Además, es ante esta situación cuando las PKI solo quieren tener CA asociadas mediante acuerdos entre los usuarios y las CA subscriptoras, de modo que dichos acuerdos se consideren como CPS.

Es posible que las CA solo dejen pública una parte de las CPS, es decir, un resumen de la misma. Una CPS establece los mecanismos utilizados en un determinado servicio, cuyo conocimiento puede ser utilizado por un atacante. Por ello, el resumen contiene las cláusulas que la CA correspondiente considere que son relevantes para todos los participantes de la PKI, como las responsabilidades de las partes o el ciclo de vida de los certificados. Sin embargo, hay que tener presente que una CPS no es un contrato. Sólo bajo la existencia de un documento independiente que establezca una relación contractual entre las partes implicadas y la CPS se podría indicar la existencia de un contrato.

Al igual que con las CP, es posible cuestionarse la utilidad de las CPS dentro de las PKI. Sin embargo, es necesario indicar unas reglas que determinen el modo de interacción de los usuarios con las CA, en base a emitir, revocar, distribuir y renovar los certificados.

#### 4.3.- Diferencias entre política de certificación y declaración de prácticas de certificación

Tanto las CP como las CPS estudian los mismos temas, en base al grado y propósito por el que los certificados de clave pública deberían ser confiables. En concreto, las diferencias se pueden resumir del siguiente modo:

- El objetivo de la CP es establecer qué deben hacer los participantes. En cambio, la CPS determina cómo una CA y sus participantes, en un determinado dominio, implementan los procedimientos y controles para satisfacer los requisitos establecidos por la CP.
- CP sirve para transmitir mínimas guías de operación a seguir por PKI que son compatibles (interoperables) entre sí. Por tanto, una CP es generalmente aplicable a múltiples CA, organizaciones o dominios. Por el contrario, una CPS es aplicable a una única CA u organización, la cual no es generalmente utilizada para facilitar interoperabilidad.
- Una CPS generalmente incluye más detalle que una CP y especifica cómo las CA han de satisfacer los requisitos establecidos en una o varias CP bajo los cuales emiten los certificados.

#### 4.4.- Provisiones: política de certificación y declaración de prácticas de certificación

Tanto los CP como los CPS se componen de un conjunto de provisiones, el cual se define como el conjunto de prácticas o declaraciones de políticas que abarcan los temas que las CP y las CPS han de contemplar.

En concreto un CP se puede expresar como un conjunto de provisiones, mientras que un CPS se expresa como un conjunto de provisiones con cada componente que satisface los requisitos

establecidos en una o varias CP o, alternativamente, un CPS se puede expresar como varios conjuntos de provisiones.

Es posible indicar, tal y como establece la norma RFC 3647, que el contenido de un conjunto de provisiones se corresponde con el siguiente marco compuesto por nueve componentes:

- Introducción.
- Publicación y repositorio.
- Identificación y autenticación.
- Ciclo de vida de los certificados, requisitos operaciones.
- Facilidades, gestión y controles de operación.
- Controles técnicos de seguridad.
- Perfiles de certificado, CRL y OCSP.
- Auditoría de cumplimiento.
- Otros asuntos legales y de negocio.

Sin embargo, esta especificación también puede ser útil para la realización de acuerdos entre las distintas partes involucradas en las PKI. Por ejemplo, un par de CA puede utilizar este marco para la creación de un acuerdo de interoperabilidad. De hecho, este sencillo marco puede ayudar en la creación de CP y CPS pero es extensible y puede ser ampliado, por ejemplo, es posible incluir subcomponentes. Además, es recomendable que todos los componentes estén completos, aunque alguno de ellos no incluya ningún requisito, puesto que esto indicará que todos los componentes se han considerado y ninguno de ellos ha pasado inadvertido.

## 5. LISTA DE CERTIFICADOS REVOCADOS (CRL)

Cuando el propietario de un certificado considera que este ya no es válido, puede llevar a cabo la revocación del mismo. Las razones de revocación de un certificado son numerosas y, en base al estándar X.509, estas pueden ser:

- Inespecífica, ninguna razón se señala.
- La clave privada asociada al certificado es comprometida.
- La clave privada de la CA que emitió certificados es comprometida.
- El propietario del certificado rompe el vínculo con el emisor del certificado y/o no tiene derecho de acceso al mismo o no lo necesita.
- Otro certificado reemplaza a uno existente.
- La CA que emitió un certificado deja de ser operable.
- Un certificado se mantiene a la espera de alguna acción. En este estado se considera revocado hasta el momento en que sea activado y nuevamente válido.

El uso de los certificados implica la verificación de los mismos, para lo cual, además de verificar su fecha de expiración, la firma de las CA correspondientes, etc., es imprescindible verificar si es o no un certificado revocado. La verificación se realiza verificando la existencia del certificado concreto en una lista, conocida como lista de certificados revocados (del inglés *Certificate Revocation List*, CRL) en la que, como su propio nombre indica, se almacenan todos los certificados que han sido revocados, identificados por su número de serie.

Las CA son las entidades responsables de indicar el estado de revocación de los certificados. Indicado por la RFC 5280, enfocada en X.509 PKI y CRL, la información de revocación puede obtenerse mediante *Online Certificate Status Protocol* (OCSP) (descrito más adelante), CRL o algún otro mecanismo.

En general, cuando se hace uso de las CRL, la CA es la autoridad que se encarga de firmar la lista. Sin embargo, la emisión de las CRL puede realizarse tanto por la CA como por otra entidad delegada. Concretamente, con cierta periodicidad una determinada CA o un emisor de CRL firma la CRL y la deja disponible en un repositorio público. Posteriormente, cuando un sistema hace uso de un certificado, en el proceso de verificación se garantiza que el número de serie del certificado a utilizar no se encuentra en la CRL. Las CRL se actualizan periódicamente (cada hora, día o semana), consiguiendo verificaciones sobre listas lo suficientemente actualizadas. Es importante considerar que en la CRL se mantendrá la identificación de los certificados revocados hasta que estos expiren.

Una ventaja de este proceso de distribución y utilización de CRL es que la distribución puede realizarse del mismo modo que ocurre con los certificados. Sin embargo, hay que destacar que la periodicidad de actualización de CRL es muy importante. De no ser muy frecuente es posible considerar válidos certificados que deberían ser revocados.

Finalmente, es importante mencionar que una extensión dentro de los certificados (en concreto "CRLDistributionPoint") permite indicar los puntos de distribución de CRL, aunque esta extensión no debe ser crítica. Así, es posible conocer dónde obtener la CRL que informa del estado de revocación del certificado asociado.

### 5.1.- Formato de una lista de revocación de certificados

Aunque una CRL se puede definir como una lista con los números de serie de los certificados revocados, la CRL X.509 está compuesta por los siguientes campos:

- Algoritmo de firma: algoritmo utilizado por la entidad correspondiente para firmar la lista.
- Valor de la firma: firma de la lista.
- Nombre emisor: nombre de la CA o de la entidad emisora de CRL encargada de emitir la CRL.
- Día de emisión: día en el que se realiza la emisión de la CRL.
- Día emisión nueva lista: día en el que se ha de realizar la emisión de la nueva CRL.
- Lista de certificados revocados: por cada certificado se ha de indicar su número de serie y el momento de la revocación.
- Extensiones: campos opcionales como el identificador de la clave utilizada para realizar la firma de la CRL, un nombre alternativo de la entidad emisora de la CRL, identificadores de Delta CRL (CRL que contienen actualizaciones sobre otras distribuidas previamente), etc.

### Sabía que ...

Gracias al formato estandarizado de las listas CRL, cualquier usuario puede comprender el contenido de la lista con independencia del país, lenguaje o política de certificación de la Autoridad que la gestione. Esto garantiza su fácil aplicación en un mundo globalizado como Internet.

### 5.2.- Concepto de Delta CRL

Tal y como se ha mencionado anteriormente, la CRL se publica periódicamente. Este modo de funcionamiento introduce un problema práctico de máxima importancia: cómo difundir, en el intervalo entre dos CRL, los certificados que quedan revocados. Considérese el caso de una Autoridad que emite sus CRL cada semana. Si a mediados de semana un certificado queda revocado los usuarios no serán conocedores de esta circunstancia hasta el principio de la semana siguiente.

Para paliar esta traumática situación se definieron las **Delta CRL** o, lo que es lo mismo, fragmentos reducidos de CRL que contienen los certificados revocados desde la última lista publicada.

Gracias a la Delta CRL el mecanismo adquiere cierto dinamismo, pues se reduce el periodo de incertidumbre. No obstante, debe tenerse en cuenta que esto introduce una mayor sobrecarga en la Autoridad, que ve así incrementada la frecuencia con la que publicar esta información.

Por tanto, se trata de un mecanismo que debe calibrarse adecuadamente para compensar los beneficios con el esfuerzo necesario.

Las Delta CRL suponen una reducción del problema planteado, pero no proporcionan una inmediatez completa. Por este motivo surgió el protocolo OCSP, que se introduce en el apartado siguiente.

### 5.3.- Online Certificate Status Protocol (OCSP)

OCSP, definido en la RFC 2560, es un protocolo también utilizado en la revocación de los certificados X.509, el cual se desarrolló como alternativa a las CRL. El propósito de OCSP es facilitar la verificación en línea de los certificados evitando posibles fallos en el proceso de revocación debido a CRL desactualizadas.

El protocolo OCSP especifica los datos que necesita intercambiar una aplicación con un servidor OCSP para conocer el estado de un determinado certificado. Es importante tener en cuenta que el servidor OCSP se corresponde con la CA emisora del certificado, un tercero de confianza acreditado por la CA emisora o un tercero de confianza para el cliente. La comunicación entre cliente y servidor se compone de un par de mensajes:

- **Solicitud:** se realiza desde un cliente OCSP a un servidor OCSP y contiene la versión del protocolo, el servicio solicitado, el identificador del certificado del cual se desea conocer el estado y, opcionalmente, extensiones.
- **Respuesta:** el servidor OCSP responde al cliente OCSP. Hay múltiples tipos de respuesta y no todas son soportadas por los servidores OCSP, aunque sí un tipo básico.

Todas las respuestas, con independencia del tipo, han de ser firmadas por el servidor OCSP.

Dentro de los tipos de respuesta, la básica contiene la versión de la sintaxis utilizada en la respuesta, el nombre del servidor OCSP, una respuesta para cada uno de los certificados, campos opcionales, el identificador del algoritmo de firma de la respuesta y la firma del *hash* de la respuesta. A su vez, la respuesta para cada uno de los certificados se corresponde con el identificador del certificado asociado a la respuesta, el estado del certificado, el periodo de validez de la respuesta y extensiones opcionales.

A raíz de la definición del protocolo OCSP es posible indicar que, a diferencia de las CRL, proporciona información reciente del estado de los certificados, puesto que se requiere conexión con el servidor OCSP, el cual dispone de información actualizada. Además, la utilización de OCSP elimina la necesidad de procesar CRL y, al contener menor información que una típica CRL, es posible hacer un uso más eficiente de los recursos tanto en cliente como en servidor.

Asimismo, en OCSP no se intercambia información considerada sensible, la cual sí se intercambia en las CRL.

#### Sabía que ...

La mejora de la conectividad de los dispositivos móviles está haciendo que el uso de OCSP sea cada vez más habitual en este tipo de dispositivos. Con ello se gana inmediatez en el proceso de verificación de los certificados.

## 6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)

La solicitud de firma de un certificado (del inglés *Certijicate Signing Request*, CSR), es un formato para realizar la solicitud de certificados, definidos en el estándar PKCS#10/RFC 2986.

Las CSR se utilizan para proporcionar a las CA toda la información necesaria para la emisión de certificados, evitando proporcionar la clave privada del solicitante. En el proceso de solicitud de un certificado se pueden distinguir las siguientes fases:

1. La entidad que solicita el certificado construye una solicitud del mismo, la cual está compuesta por tres grandes campos de información:
  - Información de solicitud del certificado. Esta información contiene:
    - Firma de la solicitud. Versión de la solicitud (debe ser 0 en la actualidad).

- Nombre del solicitante.
  - Clave pública del solicitante.
  - Otros atributos que proporcionan información adicional sobre el solicitante.
- Firma de la solicitud.
  - Algoritmo utilizado para realizar la firma.
2. El solicitante firma la solicitud (con su clave privada).
  3. La solicitud, la firma y el algoritmo de firma son enviados a la CA deseada o a una AR delegada, la cual completa la petición autenticando al solicitante y verificando la firma realizada. También comprueba que la solicitud se ajusta a la PC de la CA, tal y como se introdujo anteriormente. Así, por ejemplo, si la solicitud especifica que el certificado tenga una validez de 10 años, una CA cuyo plazo máximo de certificación sea 4 años impondrá esta duración en los certificados, ignorando la duración solicitada.
  4. Si la solicitud es válida y se puede ajustar a la CP establecida, se construye un certificado X.509 indicando el nombre del solicitante y su clave pública, el nombre de la CA emisora, el número de serie de la CA, el periodo de validez del certificado y el algoritmo de firma, es decir, se construye un certificado de clave pública con todos los campos indicados en el Capítulo 1.

## 7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)

Las infraestructuras de gestión de privilegios, habitualmente referidas por sus siglas en inglés PMI (de *Privilege Management Infrastructure*), permiten administrar de manera eficaz los permisos o acciones que una determinada entidad está autorizada a realizar. El mecanismo con el que se instrumenta la concesión de privilegios son los certificados de atributos, que se presentarán más adelante.

A continuación, se presentan las distintas entidades que participan en una PMI para, posteriormente, describir el proceso por el que se verifican los privilegios esgrimidos. En tercer lugar, se detalla cómo se aplica este concepto en el terreno del control de acceso y, finalmente, se señalan las diferencias entre esta infraestructura y una de clave pública (PKI).

### 7.1.- Entidades participantes

Una PMI se compone de diversas entidades, de acuerdo a la especificación prevista en la norma X.509. Debe tenerse en cuenta que existen diferentes fases dentro del ciclo de vida de un certificado de atributos: emisión, verificación y revocación. En cada una de ellas, un grupo distinto de entidades participan en diverso grado.

La emisión de los certificados corre a cargo de la Fuente de Autoridad (más conocida por su acrónimo en inglés *Source Of Authority*, SOA). Esta entidad emite los certificados especificando qué privilegio se concede al titular del mismo. Dicho privilegio o permiso se especifica a través de uno o varios atributos.

**Nota**

Habitualmente, pocas entidades ejercen el papel de SOA dentro de una organización. Por el contrario, cualquier entidad que pueda delegar privilegios ejerce el papel de AA. Por este motivo, es muy frecuente encontrar numerosas AA dentro de una organización.

El titular del certificado puede tener la capacidad para transferir el privilegio. En función de esto, surgen dos tipos de entidades que pueden ser titulares: Autoridad de Atributos (*Attribute Authority*, AA) y Propietario del Privilegio (habitualmente referido como *Privilege Holder*, PH). La AA puede transferir los privilegios, mientras que el PH no. Además de esta diferencia, se destaca también que, mientras que el PH puede ejercer siempre el privilegio, la AA no siempre puede hacerlo.

**Nota**

A modo de analogía con las PKI, las AA son similares a las Autoridades de Certificación intermedias en tanto que pueden emitir documentos que sean útiles para un usuario final (o PH, en la terminología de PMI).

La verificación del certificado tiene habitualmente lugar cuando el titular del privilegio desea ejercerlo. Es el caso, por ejemplo, del acceso a un recurso electrónico desde un equipo corporativo: el titular debe acreditar que está autorizado a consultar dicho recurso. En ese momento, el verificador (en inglés, *Privilege Verifier*) comprueba la validez y vigencia del certificado de atributos que refleja la existencia del privilegio.

La comprobación de la validez conlleva también la revisión del estado del certificado. Tal y como sucede con los certificados de clave pública, los certificados de atributos pueden ser válidos, estar caducados o ser revocados. Para hacer efectiva la revocación es necesaria la participación de la SOA, quien emite la correspondiente revocación. Esta queda incluida en la Lista de Certificados de Atributos Revocados (comúnmente ACRL, del inglés *Attribute Certificate Revocation List*).

### **Proceso de verificación de privilegios**

El proceso de verificación comprende las siguientes acciones:

1. El propietario del privilegio solicita realizar una determinada acción sobre un recurso.

2. El verificador comprueba que los atributos (privilegios) del solicitante se ajustan a los necesarios para realizar la acción. Para ello, toma en consideración los datos del certificado, el recurso solicitado y, eventualmente, otros parámetros del contexto (por ejemplo, la fecha y hora en que se produce la solicitud). En caso de que no se ajuste a lo establecido, deniega el permiso.
3. El verificador establece ahora la vigencia del certificado de atributos, para lo que efectúa dos acciones principales:
  - a. Comprobar la validez de la cadena de certificación, estableciendo si la firma del certificado de atributos es correcta y si corresponde a una autoridad correctamente autenticada y confiable. Nótese que puede existir una cadena de autoridades en el proceso (una o varias AA y una SOA), por lo que será necesario recorrer toda la cadena de certificación. Para la autenticación de estas entidades puede utilizarse, por ejemplo, un certificado de clave pública.
  - b. Comprobar si el certificado está revocado de acuerdo a la lista de certificados de atributos revocados publicada por la SOA.

## 7.2.- Aplicación de PMI para el control de acceso

Una de las aplicaciones más habituales de los PMI es en los sistemas de control de acceso. Dichos sistemas se encargan de controlar quién puede acceder a qué recursos y con qué fines.

Uno de los modelos clásicos de control de acceso es el modelo discrecional (DAC, del inglés *Discretionary Access Control*), en el que la asignación de privilegios a personas y recursos se hace de forma particularizada. Este modelo es típico de sistemas de información (por ejemplo, bases de datos o servidores), donde el administrador otorga permisos a determinados usuarios sobre ciertos recursos. Sería el caso, por ejemplo, del administrador de un portal web que permite que los empleados accedan a la intranet de la empresa.

Sabía que ...

El modelo discrecional recibe su nombre del hecho de que la entidad que dispone de un permiso puede delegarlo a discreción en un tercero. Este modelo se contrapone al MAC, del inglés Mandatory Access Control, en el que no existe esa posibilidad.

**Sabía que ...**

El modelo discrecional recibe su nombre del hecho de que la entidad que dispone de un permiso puede delegarlo a discreción en un tercero. Este modelo se contrapone al MAC, del inglés Mandatory Access Control, en el que no existe esa posibilidad.

La aplicación de una PMI a este esquema es directa, en tanto que cada certificado de atributos puede representar el permiso para operar sobre un determinado recurso. No obstante, este sistema plantea una elevada dificultad de gestión. Considérese la situación en que un determinado empleado es despedido de la empresa. Cuando este hecho se produce, es necesario eliminar todos los privilegios asociados, con lo que deben invalidarse (revocarse) todos los certificados correspondientes.

Otro modelo de control de acceso, más eficaz en su gestión que el DAC anteriormente introducido, es el sistema de acceso multinivel. Este tipo de sistemas son ampliamente utilizados en entornos donde existen diferentes niveles de confidencialidad de la información, como pueden ser los ámbitos de los cuerpos de seguridad. En estos sistemas se asocia a cada recurso con una etiqueta (por ejemplo, "confidencial"; "alto secreto"). Cada sujeto dispone de una lista de etiquetas sobre las que puede realizar diferentes acciones. La aplicación, en este caso, del concepto de PMI a este contexto es también directa: cada certificado de atributos representa la concesión de cierto privilegio (por ejemplo, lectura) sobre los recursos catalogados con una determinada etiqueta.

Finalmente, en los últimos tiempos se está generalizando el control de acceso basado en roles (o RBAC, de *Role-Based Access Control*). Gracias a los roles, es posible otorgar una serie de privilegios a todos los sujetos que dispongan de él. Una ventaja adicional es que existen variantes de RBAC en las que es posible construir jerarquías de roles, de forma que se facilite la gestión de los privilegios asociados. Así, el rol "director" dispone de todos los privilegios del rol "subdirector" y, además, otros propios y exclusivos de su función (como por ejemplo el acceso completo a los ficheros de nóminas). También existen variantes de RBAC que limitan los roles que puede tener un mismo sujeto al mismo tiempo. Con ello se impediría, por ejemplo, que la misma persona fuese quien autorizase un viaje y quien diese el visto bueno a la relación de gastos ocasionados. La aplicación de la PMI a los sistemas RBAC es sencilla, pues existen campos específicos para la determinación de roles.

### 7.3.- Comparación con respecto a una PKI

Teniendo en cuenta que tanto la PKI como la PMI están definidas dentro de la norma X.509, es razonable pensar que existen analogías sustanciales entre ambas estructuras.

En primer lugar, tanto PKI como PMI se centran en la gestión de certificados: mientras que los certificados de clave pública ligan a una entidad con dicha clave, los de atributos relacionan al titular con ciertas propiedades.

En segundo lugar, se observa el concepto de jerarquía de entidades. En una PKI, existe una autoridad raíz (CA) y una o varias autoridades subordinadas. En PMI, el SOA ejerce de autoridad raíz mientras que las AA pueden emitir certificados para delegar sus privilegios a un tercero.

Finalmente, en ambas estructuras existe un mecanismo similar para la gestión de la revocación. Si bien en una PKI los certificados se incluyen en una CRL, en la PMI lo hacen en una ACRL. El contenido de ambas listas es análogo en ambos casos.

## 8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES

Una vez conocido el concepto de CA, este apartado presenta los campos que contiene, así como sus usos más habituales y las diferencias con respecto a los certificados digitales.

### Nota

Los certificados de atributos pueden considerarse también certificados digitales. No obstante, en este manual, el uso de este término se reserva a los certificados de clave pública. 8.1. Campos de los certificados de atributos

En base al estándar X.509, los CA están compuestos por los siguientes campos:

- Versión: versión del certificado, la cual debe ser "v2". Nótese que "v2" no se aplica retroactivamente y, por tanto, no sería compatible con versiones anteriores.
- Propietario (*holder*): es una secuencia cuyo propósito es la identificación del propietario. Esta puede consistir en el identificador del certificado PKC asociado, el nombre de sujeto indicado en el PKC asociado o en el resultado de aplicar un resumen sobre un objeto (clave pública, certificado, etc.).
- Nombre del emisor: nombre de la SOA emisora de los certificados de atributos.
- Algoritmo de firma: algoritmo utilizado por la SOA para firmar el certificado.
- Firma: firma del certificado, la cual es realizada por la SOA emisora.
- Número de serie: número entero positivo, el cual se espera que sea largo debido a su unicidad y utilización en el tiempo.
- Periodo de validez: fecha de inicio de validez de certificado y fecha de fin.
- Atributos: proporcionan información sobre el propietario del certificado. Además, si el certificado se utiliza para autorización, este campo incluirá un conjunto de privilegios.

Este campo contiene una secuencia de atributos, cada uno de los cuales pueden tener un conjunto de valores. Sin embargo, solo se admite una única instancia de cada tipo de atributo en cada certificado. Asimismo, un certificado ha de contener un atributo como mínimo.

- Identificador único del emisor: identificador de la SOA emisora. Este campo solo ha de utilizarse si se hace uso de él en el PKC de la SOA emisora.
- Extensiones: proporcionan información adicional, como es el establecimiento de los objetivos de uso del certificado, el identificador de la clave de la SOA utilizada en la verificación de la firma del certificado o los puntos de distribución de CRL entre otros.

**Recuerde**

La SOA es la Source Of Authority y es la entidad encargada de emitir los certificados de atributos.

Dentro de los atributos que pueden utilizarse hay que destacar que un atributo, dependiendo del tipo, puede contener múltiples valores o un único valor. Es posible distinguir un total de seis tipos:

1. Servicio de autenticación de la información: este tipo de atributos proporcionan información que facilita la autenticación por una aplicación distinta al sistema para el que se desarrolló inicialmente. Este tipo de atributos será cifrado en el caso de contener información sensible, como son las contraseñas. Asimismo, este tipo puede contener múltiples valores.
2. Identidad de acceso: su utilización se basa en proporcionar información sobre el propietario del certificado. De este modo, una autoridad de verificación podrá autorizar, o no, las acciones solicitadas por un determinado usuario. Este tipo de atributos también acepta múltiples valores.
3. Identidad de cobro (*charging identity*): este campo es utilizado en servicios que implican un coste. Identifica al propietario del certificado para casos en los que sea necesario imputar un coste. Esta identidad es distinta del resto de identidades.
4. Grupo: proporciona información sobre el grupo al que pertenece el propietario.
5. Rol: informa de los roles asignados al propietario del certificado. Se permiten múltiples valores.
6. Autorización (*clearance*): indica información sobre la autorización de la que dispone el propietario del certificado. Dentro de este tipo se incluye la especificación de la política de seguridad asociada con la autorización. Además, las distintas organizaciones pueden crear sus propias políticas de seguridad. Se aceptan múltiples valores para este tipo de atributos.

### 8.1.- Usos habituales de los certificados de atributos

Los certificados de atributos se pueden utilizar en gran variedad de servicios, entre los que se incluyen el control de acceso, la autenticación en el origen y el no repudio.

**Recuerde**

Tal y como se describió anteriormente, la autenticación es el servicio de seguridad que garantiza que una entidad es la que dice ser. Por su parte, el no repudio impide que dicha entidad pueda negar haber realizado alguna acción.

En relación con el control de acceso, en muchos contextos, en lugar de utilizar una identidad que otorgue acceso basta con mostrar la pertenencia a un determinado rol o grupo. Estos esquemas de acceso se conocen con el nombre de control de acceso basado en roles.

Cuando se solicita acceso con un certificado de atributos, se ha de determinar que el propietario del certificado es el que ha realizado la solicitud. Un modo de realizarlo es incluyendo una referencia a un PKC contenido en el certificado de atributos, de modo que la autenticación se realice utilizando la clave privada que se incluye dentro de la solicitud de acceso.

En cuanto a la autenticación en origen y al no repudio, teniendo en cuenta la utilización de PKC en el certificado de atributos y recordando que la firma digital es uno de los mecanismos esenciales para autenticar a la entidad origen y evitar el no repudio en emisión, los atributos contenidos en el certificado proporcionan información adicional sobre la entidad que realiza la firma, es decir, el propietario del certificado. Por tanto, esta información puede ser utilizada para asegurar que el propietario puede realizar la firma de unos determinados datos. Sin embargo, hay que tener presente que este tipo de comprobaciones dependen del contexto o de los datos que tengan que firmarse digitalmente.

### 8.2.- Certificados digitales frente a certificados de atributos

En la siguiente imagen es posible identificar, a grandes rasgos, las diferencias entre un PKC y un certificado de atributos (en adelante AC, del inglés *Attribute Certificate*).

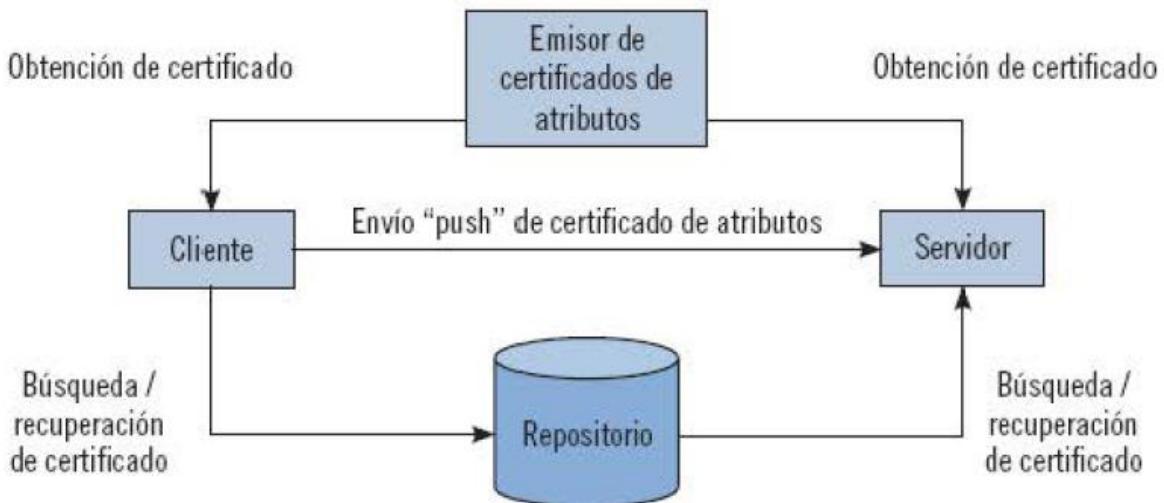
Los certificados digitales vinculan a un individuo (*Subject*) con una clave pública (*Subject Public Key Info*), manteniéndose en secreto la clave privada asociada. En cambio, los AC vinculan un conjunto de atributos (*Attributes*) bien con un individuo o con el identificador de un certificado digital (*Holder*), el cual es un PKC.

Public Key Certificate (PKC)		Attribute Certificate (AC)	
Signature	Version	Signature	Version
	Serial Number		Serial Number
	Signature ID		Signature ID
	Subject		Holder
	Issuer		Issuer
	Validity Period		Validity Period
	Subject Public Key Info		Attributes
	Extensions		Extensions

*PKC vs AC*

Además, los AC proporcionan ventajas respecto al proceso de revocación. Por un lado, si los atributos tienen una duración mayor que la clave pública incluida al PKC asociado, o únicamente

#### Intercambios de información relacionados con los certificados de atributos (adaptado de RFC 3281)



Ambos modelos presentan sus ventajas e inconvenientes, así como sus escenarios de aplicación ideales. El modelo *push* permite que al servidor se le presente toda la información que necesita conocer para tomar sus decisiones. Esto es especialmente adecuado cuando existe más de un dominio de seguridad, el cliente pertenece a uno distinto al del servicio al que se quiere acceder y

la asignación de privilegios se realiza en el entorno del cliente. Un ejemplo de esta situación sería un empleado de una empresa (dominio 1) que desea acceder a un periódico digital (dominio 2), al que solo pueden entrar los directores generales de dicha empresa (privilegio asignado en el dominio 1).

Por su parte, el modelo *pull* impone una sobrecarga en el servidor de autorización derivada de la búsqueda de los certificados. Sin embargo, es el modelo más adecuado cuando la asignación de privilegios se efectúa en el dominio del servidor. Siguiendo con el ejemplo anterior, el empleado de la empresa solo podría acceder al periódico si ha pagado la cuota de suscripción, lo cual es un atributo que se gestiona en el dominio del periódico. Como ventaja del modelo *pull* debe destacarse que permite que el protocolo de comunicación entre el cliente y el servidor no se vea afectado por el uso de certificados de atributos y, por tanto, pueda seguir siendo el mismo que cuando no se utilizaban.

## 9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

Las aplicaciones fundamentales de las PKI son la autenticación, la firma electrónica y el cifrado.

### 9.1.- Uso de PKI para autenticación

La autenticación se utiliza en muchos tipos de aplicaciones para tener constancia de quién es la entidad que está intentando hacer uso de ella. Con frecuencia, la autenticación está basada en nombres de usuarios y contraseñas, como en *Facebook* o *Gmail*. Sin embargo, la PKI es una alternativa más segura en la que la autenticación se produce probando la posesión de una clave privada en lugar de una contraseña, la cual puede verse comprometida con cierta facilidad, como por ejemplo, si la contraseña es una palabra del diccionario se podría conocer con mucha facilidad. Es cierto que la clave privada está protegida, se protege por medio de una contraseña, una característica biométrica, etc., pero su utilización es local y nunca llegan a ser conocidas por ninguna aplicación. Un ejemplo típico de autenticación es la utilización del protocolo SSL, el cual será estudiado más adelante.

### 9.2.- Uso de PKI en firma

La firma digital es otra de las aplicaciones más frecuentes de las PKI, las cuales se pueden definir como un esquema matemático que permite demostrar la autenticidad de un mensaje digital. En el mundo digital, la firma de documentos (especialmente XML) así como los correos electrónicos, constituyen claros ejemplos de esta aplicación.

### Recuerde

Como se indicó con anterioridad, la firma de un mensaje se realiza con la clave privada del emisor y la verificación con la pública. Además, si se hacen uso de resúmenes, lo cual es lo habitual, se facilita la verificación de la integridad del mensaje.

La utilización de firmas digitales en las transacciones entre dos entidades evita la necesidad de realizar trámites en papel, así como problemas a la hora de verificar firmas. Una firma manuscrita, aun dependiendo de la situación, podría llegar a ser copiada, pero una firma digital, sin conocer la clave privada utilizada en la firma, no puede ser realizada por un tercero. Algunos de los ejemplos más típicos de firma digital son la firma de documentos (utilizando programas como *Microsoft Office* o *Adobe Reader*), o la firma de formularios electrónicos (como los utilizados en la administración pública electrónica).

Una cuestión crítica en el ámbito de las firmas es asegurar su validez a lo largo del tiempo. Debe tenerse en cuenta que, para que una firma sea válida, es preciso:

1. Realizar la verificación criptográfica de la firma, de acuerdo al algoritmo seleccionado.
2. Verificar la cadena de certificación.

Tal y como se ha expuesto anteriormente, los certificados tienen dos fuentes principales para quedar invalidados: su caducidad o su revocación. Si el certificado del firmante o, en general, cualquiera de los certificados de la cadena de certificación, son inválidos cuando se verifica la firma, la firma no será válida. Considérese, por ejemplo, una factura electrónica que se firma utilizando la clave correspondiente del DNI electrónico. De acuerdo a la legislación vigente, dichos certificados caducan a los 30 meses. Si la factura se verifica tres años después (es decir, en 36 meses), el certificado del firmante habrá caducado y, por tanto, la factura no estará correctamente firmada.

### Sabía que ...

Muchos programas de ofimática usados frecuentemente (e.j. Microsoft Office, Adobe Acrobat) permiten agregar una firma a los documentos. Además, existen otras aplicaciones especializadas para la firma de documentos PDF, tales como Sinadura o ClickSign.

Esta cuestión refleja la relevancia de las PKI en los procesos de firma. Para dar respuesta a esta necesidad ha surgido el concepto de **firma longeva**. La firma longeva persigue mantener la validez de la firma a lo largo del tiempo. Con ello, se pretende contrarrestar, además, los efectos que el paso del tiempo puede tener en la seguridad de los algoritmos (en los que se pueden descubrir

vulnerabilidades) o en la disponibilidad de los materiales (podría perderse el certificado de clave pública asociado al firmante).

Además de la aplicación anterior, las PKI son también necesarias para la firma del código fuente de un programa. Gracias a estas firmas, es posible asegurar que el código del programa (por ejemplo, el descargado de una página web) cumple las dos propiedades siguientes:

- No ha sido manipulado desde que se creó.
- El código ha sido creado, supervisado o es responsabilidad de la entidad que lo firma.

Este tipo de firmas constituyen una barrera razonablemente eficaz contra la distribución de *software* malicioso o *malware*. Esto es debido a que los sistemas operativos permiten que el usuario conozca quién firma el programa para que, en su caso, autorice o deniegue la instalación.

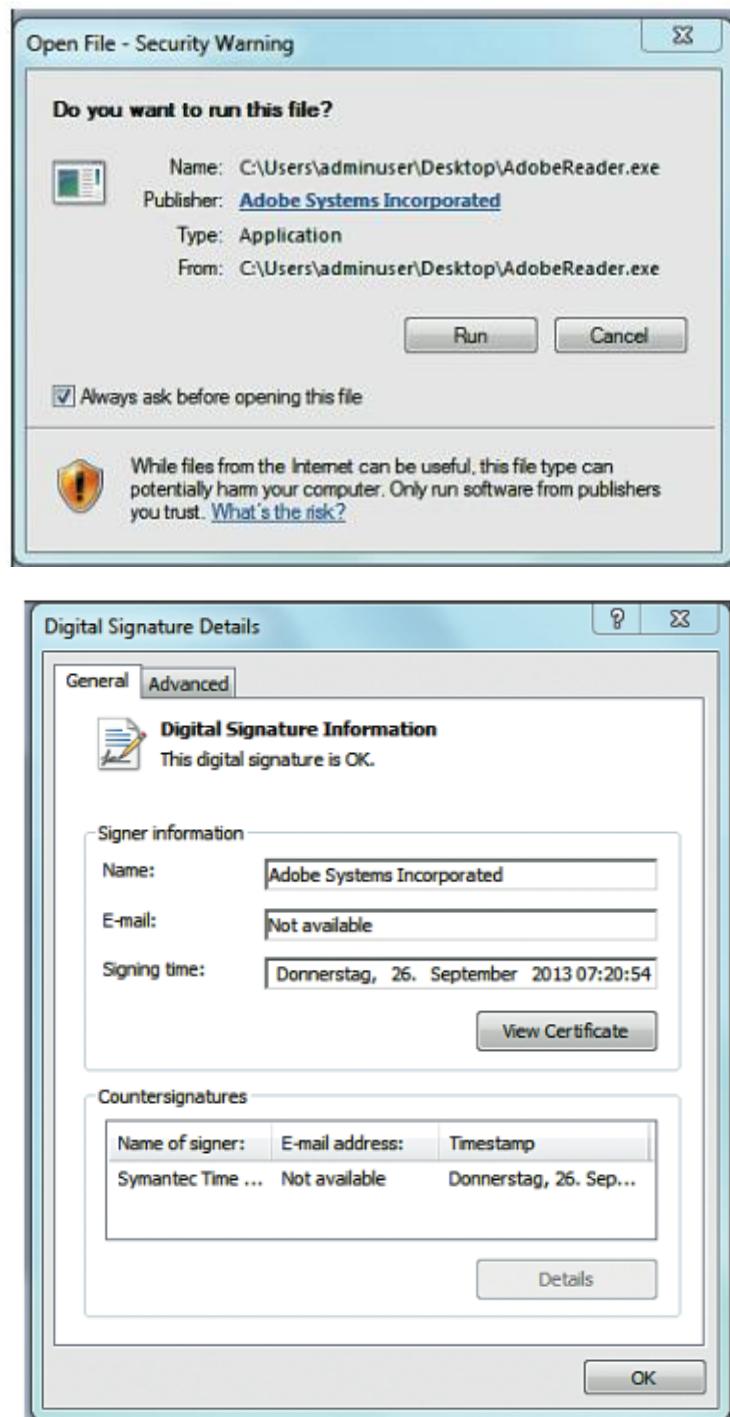
La imagen siguiente muestra una ventana de aviso sobre esta cuestión en *Microsoft Windows 7*.



Ventana de aviso por software no firmado

Por contraposición, cuando el programa está correctamente firmado, el sistema verifica la firma, incluyendo el estado de los certificados. Esta situación se refleja en la imagen siguiente.

No obstante, debe tenerse en cuenta que la firma electrónica no garantiza que el programa funcione correctamente: simplemente garantiza que fue creado por una determinada entidad.



*Proceso de instalación de software con programa correctamente firmado*

Es importante recalcar que las empresas que crean y distribuyen programas deben tener especial cuidado en la custodia de la clave privada empleada para firmarlo. No en vano, grandes

corporaciones (por ejemplo, *Microsoft*) han visto comprometida la seguridad de sus productos cuando un atacante ha conseguido acceder a dicha clave y firmar programas maliciosos.

### 9.3.- Uso de PKI para cifrado

Finalmente, la PKI es frecuentemente utilizada para el cifrado de datos. Cualquier usuario puede cifrar datos pero estos solo podrán ser descifrados por los usuarios que dispongan de las claves de descifrado. Por tanto, la privacidad se asegura siempre que la clave privada se mantenga secreta.

#### Recuerde

Al contrario que la firma, el cifrado de los datos se realiza utilizando la clave pública del destinatario y se descifra con la clave privada asociada.

El cifrado es comúnmente utilizado en tarjetas inteligentes para almacenar información sensible (ej. PIN de las tarjetas de crédito), en el envío de correos (ej. utilizando programas como *Thunderbird*) o en el almacenamiento de datos de carácter confidencial (ej. Utilizando programas como *GPG4Win*).

## 10. RESUMEN

Las infraestructuras de clave pública (PKI) constituyen el elemento fundamental que permite que los certificados digitales de clave pública puedan utilizarse de forma masiva en Internet. En una PKI participan una o varias autoridades de certificación, relacionadas en forma de jerarquía o de red. Para que los usuarios puedan disponer y utilizar sus certificados, es necesario solicitarlos a través de peticiones CSR. Dos aspectos clave en la gestión de certificados son la verificación del mismo (comprobando, entre otras cuestiones, la validez de la cadena de certificación) y la revocación (bien a través de listas CRL o utilizando el protocolo OCSP).

Asociadas a las PKI surgen las PMI, o infraestructuras de gestión de privilegios. Gracias a ellas es posible gestionar los certificados de atributos que permiten atestiguar que el propietario puede disfrutar de un determinado derecho. Los certificados de atributos son a los privilegios lo que los certificados de clave pública son a la identidad.

## CAPÍTULO 3 COMUNICACIONES SEGURAS

### 1. INTRODUCCIÓN

Una vez conocidos los algoritmos criptográficos, así como su funcionamiento, el siguiente paso es aplicarlos. Uno de los usos más importantes es el establecimiento de comunicaciones seguras.

Una de las cuestiones a resolver es conocer cómo se pueden conectar dos entidades de forma segura usando un canal de comunicación inseguro. Aquí surge el concepto de red privada virtual (VPN), la cual será definida indicando sus finalidades y sus funcionalidades.

Sin embargo, las VPN pueden establecerse haciendo uso de múltiples protocolos. En particular, en este capítulo se describen en profundidad los protocolos IPsec, SSL y SSH, junto con otros basados en el establecimiento de túneles cifrados.

Finalmente, dadas las diferencias de funcionamiento y utilización de los distintos protocolos, se presentan las ventajas e inconvenientes de utilizar distintas alternativas para la creación de VPN.

### 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

Las redes privadas virtuales, habitualmente llamadas VPN (del inglés *Virtual Private Network*), son un tipo de red de comunicaciones que se construye sobre otra ya existente. La característica fundamental es que pueden permitir que distintos equipos en diversas partes del mundo puedan comunicarse como si estuviesen en una red de área local. Esto tiene grandes ventajas, como se explica a continuación.

#### Ejemplo

Imaginemos un ejemplo de una familia (“Familia A”), compuesta por un padre, una madre y un hijo (Pepito). Un amigo de Pepito va a pasar un fin de semana con la Familia A, de modo que, por unos días, Pepito pasará a convertirse en miembro de la familia, aún sin serlo realmente.

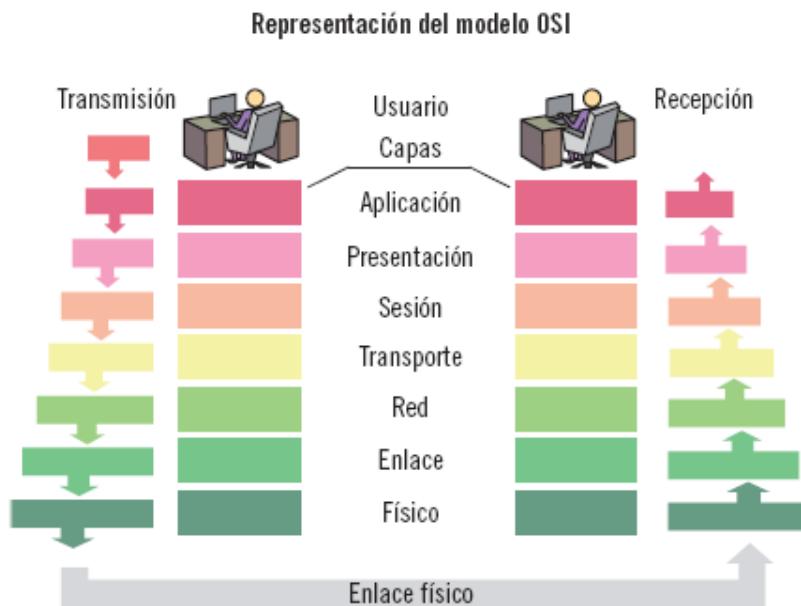
La analogía de las redes de ordenadores es evidente: una familia es una red local, donde cada uno de sus miembros son ordenadores de la misma. En la *red* privada virtual se permite justo lo anterior: que un equipo que no pertenece físicamente a una red se comporte como si estuviese en otra, es decir, que un amigo pueda comportarse como un miembro de la familia aun no siéndolo realmente. Las aplicaciones...

Para comprender cómo es esto posible es imprescindible introducir los conceptos más básicos de redes de ordenadores.

#### 2.1.- Conceptos previos. El modelo OSI

Dado que las VPN consiguen que redes distintas se comporten como una única, es necesario comprender cómo se establece una red y cómo es posible que las VPN puedan establecerse. La

comunicación entre distintos equipos puede plantearse como un conjunto de capas sucesivas entre las que se intercambian paquetes y cada una de las cuales tiene una misión particular. El modelo más comúnmente conocido es el modelo OSI, en el que las capas se interrelacionan de forma que aprovechan las capacidades de las capas inferiores y ofrecen servicios a las superiores.



### Definición

#### **Paquete**

Porción de datos compuesto, esencialmente, por CABECERA + CARGA ÚTIL. La cabecera suele contener los datos necesarios para mandar el paquete del emisor al receptor. En cambio, la carga útil (en inglés conocido como payload) se corresponde con los datos que se desean trasladar.

El modelo OSI se compone de siete capas, a saber:

- Nivel físico (capa 1). Se encarga de transmitir los datos físicamente por el canal de comunicación (el cable de red).
- Nivel de enlace (capa 2). Permite establecer el concepto de red local, es decir, qué equipos están directamente conectados entre sí. Para ello, se utilizan las direcciones MAC, que son las que los fabricantes proporcionan a las tarjetas de red.

Definición: una tarjeta de red es la parte del ordenador que se encarga de transmitir y recibir datos a una red de comunicaciones. Existen las tarjetas de red que se conectan a un cable y aquellas que se conectan de forma inalámbrica.

- Nivel de red (capa 3). Permite que equipos de distintas redes puedan comunicarse entre sí, gracias al establecimiento de una dirección de red. La dirección más habitual es la IP, cuya forma es X.Y.Z.W, siendo cada uno de esos fragmentos un valor entre 0 y 255. Por ejemplo, una dirección IP sería 81.33.11.53.
- Nivel de transporte (capa 4). Hace posible que el canal de comunicación pueda ser usado por distintos programas al mismo tiempo. Para ello, se introduce el concepto de puerto. Así, cuando un usuario navega a una página web, en realidad está enviando una solicitud al puerto 80 del servidor web. Además del concepto de puerto, algunos protocolos de esta capa ofrecen la posibilidad de gestionar la entrega de información haciendo frente a eventuales pérdidas de paquetes. A través de Internet, la información se divide en paquetes y estos se encaminan siguiendo diferentes rutas. Esto, junto con el hecho de que algunos se pueden perder, origina que la información pueda llegar en desorden o incluso no llegar. En esta capa, protocolos como TCP hacen frente a esta situación. No obstante, también existen otros (como UDP) que no ofrecen este servicio.
- Niveles de sesión (capa 5) y presentación (capa 6). La capa 5 crea el concepto de sesión entre dos aplicaciones (es decir, gestionan las diferentes fases por las que dos aplicaciones han decidido comunicarse). Por su parte, la capa 6 se encarga de asegurar que, aunque la representación de la información sea distinta entre dos ordenadores (por ejemplo, porque los bits se ordenan de forma distinta), esto no afecte al funcionamiento. Estas dos capas no son relevantes para lo que corresponde a las VPN, pero se incluyen por completitud.
- Nivel de aplicación (capa 7). Aquí se definen los protocolos que siguen los programas (por ejemplo, el protocolo HTTP sirve para la navegación web, FTP para la transferencia de ficheros, etc.). Un protocolo especifica qué datos se intercambian y cuándo se tiene que hacer.

La comunicación entre distintos ordenadores (o, mejor dicho, entre dos programas que están en distintos ordenadores) se hace de la siguiente manera. El programa emisor prepara el paquete que quiere mandar (capa 7) y lo manda a las capas inferiores. Dejando de lado las capas 6 y 5 (para no entrar en detalles), la capa 4 añade el puerto de origen (para identificar el programa emisor), así como el de destino. La capa 3 recibe toda esta información y añade la dirección IP de origen (para identificar el ordenador que envía el paquete) y la de destino. La capa 2 analiza: ¿está el destino dentro de la misma red?

- Si es así, se le puede enviar directamente, sin salir de la red local. La capa 2 añade la dirección MAC del ordenador destino.
- Si no es así, es necesario enviarlo fuera de la red para encaminarlo. La capa 2 añade la dirección MAC del encaminador o *router*, que se encargará de enviarlo a la red del destinatario.

Finalmente, toda la información de las capas anteriores se envía a través del medio de comunicación (el cable o el aire) gracias a la capa 1.

Cuando el receptor recibe el paquete (a través de su capa 1), la capa 2 confirma que la dirección MAC del destinatario es la suya y, en ese caso, se lo pasa a la 3. Esta comprueba que la IP del

destinatario es la suya y, como es así, se lo manda a la capa 4 para que esta decida a qué programa hay que entregárselo. Nuevamente obviando las capas 5 y 6, la capa 7 es la encargada de dárselo al programa que esperaba el paquete.

Tal cual se ha descrito hasta ahora, no hay forma de que dos ordenadores en distintas redes puedan alcanzarse directamente, sin ayuda de un encaminador.

### Definición

Un encaminador, o *router*, es un elemento por el cual dos redes locales pueden comunicarse entre sí.

Para conseguir que un equipo de una red se comporte como si fuese de otra, parece claro que es necesario introducir elementos en diferentes partes de este modelo. Particularmente, una de las técnicas más habituales es el encapsulado de protocolos.

### Ejemplo

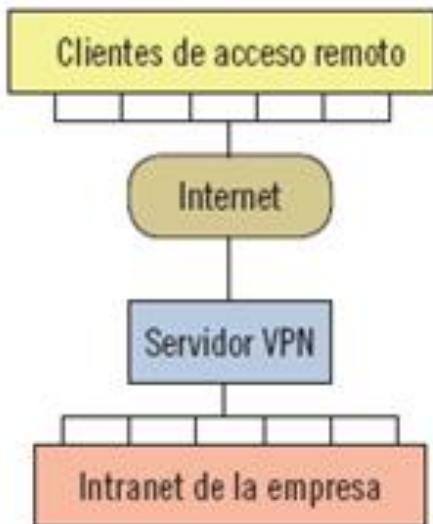
Una analogía para comprender este concepto sería el envío de correo postal entre dos casas situadas en distintas urbanizaciones. Si cada urbanización solo admitiese cartas enviadas por otros vecinos de la misma urbanización, no habría manera de conseguir el objetivo buscado. Sin embargo, si el conserje de la primera urbanización metiese la carta en un nuevo sobre, poniendo como remitente un vecino de la segunda, el envío podría realizarse. El conserje de la segunda observaría que el remitente pertenece a su urbanización y lo enviaría a su destinatario. Este, al recibirla, debería descartar el primer sobre y abrir el segundo para acceder a la carta.

El ejemplo anterior ilustra el funcionamiento de los túneles y los protocolos de encapsulación, que se estudiarán detenidamente a lo largo de este capítulo.

### 2.2.- Descripción de las VPN

Las VPN permiten que equipos físicamente distantes se comporten como si estuvieran dentro del mismo dominio de seguridad, es decir, en la misma red. Esto tiene especial relevancia de cara a permitir el acceso a determinados recursos, como un servidor de datos. Una adecuada política de seguridad debería establecer los mecanismos de protección que asegurasen que solo los equipos que están dentro de una determinada red (por ejemplo, la que agrupa a los ordenadores de la oficina) puedan tener acceso a dichos recursos. Las VPN permiten esto, pues los equipos conectados a ella se comportan como si estuviesen en dicha red: su configuración, incluyendo su dirección IP, hace que lógicamente pertenezca a esa red.

Diagrama de una red privada virtual (VPN)



Una de las cuestiones que las VPN garantizan es, precisamente, la confidencialidad de la información intercambiada. De esta manera, se puede decir que las VPN permiten crear una red privada a partir de una red pública típicamente insegura, como Internet. Esta circunstancia, junto con el hecho de que el usuario tenga la percepción de que puede emplear su equipo como si estuviese en su red habitual, da lugar a la denominación de red virtual (pues no existe físicamente) y privada.

**Recuerde**

La confidencialidad es la propiedad de seguridad que asegura que una información solo es conocida por las personas (o entidades) autorizadas.

Además de la confidencialidad, las VPN suelen proporcionar autenticación de origen (para evitar que terceros no autorizados entren en la red) e integridad de los datos (asegurando que estos no son alterados durante la comunicación).

Las VPN pueden servir para dos cuestiones distintas: por un lado, el hecho de que un empleado pueda acceder desde su domicilio a la red de la oficina. Este tipo de conexión sería ordenador-a-red. Por otro lado, puede posibilitar que dos o más edificios de una misma empresa se comporten como una \'mica red. Este sería el caso de las conexiones sitio-a-sitio.

Para poner en marcha una VPN se utilizan protocolos de tunelado (descritos más adelante).

Los principales protocolos a través de los cuales se puede establecer una VPN son los siguientes:

- IPSec (*Internet Protocol Security* ).
- SSL (*Secure Socket Layer*).
- SSH (*Secure Shell*).
- PPTP (*Point-to-Point Tunnelling Protocol*).
- L2TP (*Layer 2 Tunnelling Protocol*).
- DTLS (*Datagram Transport Layer Security*).

En la práctica, las dos opciones más extendidas son las basadas en SSL e IPSec, respectivamente.

### 2.3.- Ventajas y desventajas de las VPN

Las VPN ofrecen grandes ventajas, pero también tienen inconvenientes que hay que conocer con anterioridad a su uso.

En cuanto a las fortalezas de las VPN, se subrayan:

- Bajo coste de despliegue: redes físicamente separadas pueden conectarse sin la necesidad de establecer una red dedicada. Así, si una empresa crece y se crean distintas sedes, estas pueden comunicarse por Internet haciendo uso de VPN sin necesidad de tener una red de uso exclusivo propio.
- Transparencia de comunicación: los usuarios tienen la misma sensación de uso de la red que si estuvieran físicamente conectados a ella.
- Seguridad en los sistemas: permite crear una capa adicional de seguridad sobre información sensible a la que se tenga que proporcionar acceso.
- Simplicidad administrativa: las decisiones de a qué ordenadores se permite acceder a qué recursos son ahora más fáciles, pues todos pueden estar en una misma red.
- Por el contrario, la utilización de VPN también presenta numerosos inconvenientes:
- Fiabilidad de la red: las VPN se construyen sobre Internet que, como sabemos, no es completamente fiable y pueden producirse fallos que imposibiliten la comunicación.
- Velocidad de acceso: la velocidad de acceso es menor debido a las capas de seguridad que se aplican (ej. cifrado).
- Confianza de las entidades: si un equipo de la red es comprometido, los demás equipos conectados a la VPN podrían ser atacados a partir del primero.
- Incompatibilidad de las redes: cada fabricante de equipos de comunicación tiene su propia tecnología para crear la VPN. Esto hace que, en ocasiones, equipos de distintos fabricantes no puedan convivir en una misma VPN.

## 3. PROTOCOLO IPSEC

IPSec (*Internet Protocol Security*) es un conjunto de protocolos habitualmente usados para crear VPN. Siguiendo con el ejemplo del envío de correos entre urbanizaciones, planteado anteriormente, IPSec es el encargado de meter el primer sobre dentro del segundo (encapsulación) y, además, sellar los sobres (confidencialidad) y dar fe de que son verdaderos (autenticación).

Una característica importante de IPSec es que actúa en el nivel de red (nivel 3 del modelo OSI) a diferencia de otros mecanismos que, ofreciendo unos servicios de seguridad similares, actúan en capas superiores. Por ejemplo, SSL (presentado más adelante) actúa en la capa de transporte (nivel 4). Esta diferencia es importante, pues al estar situado en un nivel inferior, todos los programas y servicios que se sitúen por encima podrían hacer uso de IPSec.

Los protocolos que forman IPSec son esencialmente dos: *Internet Key Exchange* (IKE) y *Encapsulating Security Payload* (ESP). Generalmente, se apunta que existe un tercer protocolo (*Authenticated Header*, AH), pero, de acuerdo al investigador William Stallings, este protocolo ya no se usa, pues su principal objetivo de seguridad (proporcionar autenticación del mensaje) ya queda cubierto por ESP. De esta manera, aunque AH se mantiene por cuestiones de compatibilidad, se aconseja no utilizarlo en nuevas aplicaciones y servicios.

Teniendo en cuenta lo anterior, las dos secciones siguientes introducen IKE y ESP. Siguiendo la analogía del correo entre urbanizaciones, IKE se encarga de definir cómo se debe meter un sobre dentro de otro (aclarando cuestiones como el tamaño del sobre externo, si hay que preparar el sobre interno *de alguna manera*, etc.) y ESP realiza ese proceso de re-ensobrado según lo que se haya acordado en IKE.

### 3.1.- Internet Key Exchange (IKE)

Este protocolo permite establecer una asociación de seguridad entre dos partes comunicantes. La asociación de seguridad establece los parámetros que permitirán a las dos entidades comunicarse de forma segura. Así, se determina el algoritmo criptográfico a utilizar y su modo de operación junto con la clave de cifrado para los datos que se intercambien.

Gracias a la asociación de seguridad, las dos partes disponen de un esquema de funcionamiento acordado, que podrá ser utilizado en el protocolo ESP que se describe posteriormente.

En IKE, los intercambios de mensajes entre las partes se realizan por pares, de forma que a un envío ("pregunta") de una entidad le sigue otro ("respuesta") de su contraria. En el caso de que no se reciba respuesta, es responsabilidad del emisor repetir la pregunta o, en su caso, abandonar el protocolo.

En una ejecución del protocolo habitualmente se producen dos intercambios:

1. IKE\_SA\_INIT: este intercambio se produce antes que cualquiera de los demás y permite negociar algunos parámetros de la asociación de seguridad, intercambiar valores aleatorios y ejecutar el algoritmo Diffie-Hellman para establecer una clave compartida. Esta clave se toma como base (denominada semilla) para derivar de ella otras dos claves: una para cifrar y otra para autenticar los mensajes haciendo uso de funciones *flash* con clave.

Este intercambio es muy simple: el emisor propone una serie de algoritmos criptográficos y el receptor contesta escogiendo uno de ellos (o devolviendo un error, si ninguno de ellos es adecuado).

2. IKE\_AUTH: en esta fase se autentican mutuamente los comunicantes y se establece la asociación de seguridad que se utilizará en ESP.

**Nota**

Esta asociación será la primera que se utilice aunque podría no ser la única: los comunicantes pueden en cualquier momento negociar otra nueva a través de otro intercambio conocido como CREATE\_CHILD\_SA. Esto suele suceder dado que las claves deben utilizarse durante un periodo limitado de tiempo, lo que acota la duración de una asociación de seguridad.

Parte de los mensajes que se intercambian aquí están cifrados utilizando la clave negociada en el intercambio anterior. Por ejemplo, las identidades de los participantes se encuentran cifradas para evitar que sean conocidas por terceros no autorizados.

Para la autenticación se pueden utilizar los certificados de clave pública.

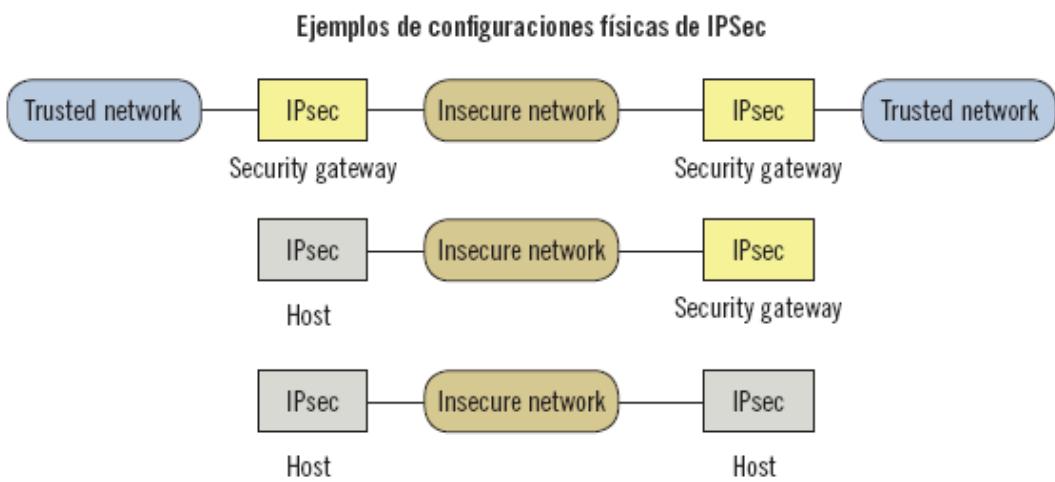
### 3.2.- Escenarios de uso

Según la configuración física o el tipo de protección que se aplique, es posible establecer las siguientes clasificaciones acerca de los escenarios de uso de IPSec.

#### Según la configuración física

La configuración física se refiere a si los participantes en IPSec son ordenadores de usuario (por ejemplo, el ordenador portátil de un empleado) o si son equipos intermedios que específicamente se dedican a establecer este tipo de conexiones. Se identifican tres escenarios posibles:

- Los equipos finales (es decir, los que se aprovecharán del protocolo IPSec cuando se establezca) se conectan a los citados equipos intermedios.
- Solo uno de los extremos es un equipo final, existiendo un intermediario en el otro extremo.
- Ambos equipos finales sí implementan IPSec, por lo que no existen intermediarios.



### Según el tipo de protección

Ve acuerdo al tipo de protección aplicada, se especifican dos posibles modos de uso:

- En el modo transporte, solo se protege la carga útil de cada uno de los paquetes que se envían. De esta manera, no se modifica la cabecera del paquete (que contiene, entre otras cosas, las direcciones origen y destino). Este modo de uso es adecuado para la configuración entre equipos finales.
- En el modo túnel, el paquete que contiene la información intercambiada se encapsula dentro de otro paquete. La principal ventaja es que de esta forma el original puede protegerse completamente, incluyendo su cabecera. Este modo es el idóneo cuando alguno de los comunicantes no es un equipo final, sino un intermediario.

### 3.3.- Encapsulating Security Payload (ESP)

El protocolo ESP se encarga de proporcionar confidencialidad, autenticación e integridad de la información en tránsito. Para ello, ESP introduce esa información en otro paquete, sobre el que se aplican los mecanismos de seguridad. Los mecanismos que se eligen y cómo se aplican se basan en la asociación de seguridad establecida tras IKE.

En el nuevo paquete hay varios trozos especialmente interesantes. Por un lado, una parte se reserva para el identificador de la asociación de seguridad. De otra manera, los participantes no sabrían cómo se tiene que interpretar el resto del paquete. Otra parte se reserva para el número de secuencia, que permite al receptor reordenar los paquetes.

**Recuerde**

En Internet la información puede llegar al destino en orden distinto al que se envió. Esto se debe a que los datos se dividen en partes (paquetes) y cada uno puede seguir un camino distinto.

Una cuestión importante es que si el número de secuencia alcanza su máximo valor, se considera que la asociación de seguridad ha caducado y debe negociarse otra.

Si el algoritmo de cifrado utilizado requiere de un vector de inicialización (esto sucedía en algunos modos de operación), esta información también se indica en el nuevo paquete.

El núcleo central del paquete es la carga útil a la que es posible añadirle relleno, bien para dificultar la realización de ataques basados en el análisis de tráfico o bien conseguir paquetes de datos múltiples de 32 bits.

Lógicamente, como el relleno es inútil para el receptor, el paquete indica la longitud del relleno, de forma que este puede identificarlo y descartarlo adecuadamente.

Finalmente, el nuevo paquete tiene un espacio para el control de integridad. Lógicamente, solo se utiliza si este mecanismo quedó acordado en la asociación de seguridad.

#### 4. PROTOCOLOS SSL Y SSH

Los protocolos SSH y SSL permiten construir un túnel confidencial por el que enviar los datos de forma segura, además de verificar la integridad de los datos transmitidos. Sin embargo, hay diferencias entre ambos, entre las que es posible destacar que en SSH lo más habitual es que la autenticación se realice utilizando usuario y contraseña y en SSL se utilicen certificados. Además, SSL es utilizado frecuentemente en aplicaciones en las que se hace uso de datos sensibles, por ejemplo, en aplicaciones bancarias, mientras que SSH es utilizado habitualmente para enviar órdenes o comandos a otro ordenador a través de Internet.

A continuación, se describen ambos protocolos de forma separada.

##### 4.1.- Secure Sockets Layer (SSL)

El protocolo SSL fue diseñado originalmente por *Netscape*. La primera versión nunca llegó a entregarse, en la segunda se detectaron errores de seguridad importantes y no fue hasta 1996 cuando se presentó la versión SSL 3.0, la cual recibió revisiones y comentarios públicos y opiniones del mundo empresarial. Cuando se llegó a un consenso sobre su especificación, se publicó bajo el nombre de TLS (del inglés *Transport Security Layer*), lo que se puede considerar como la tercera versión de SSL.

El protocolo SSL trabaja por encima del nivel de transporte (nivel 4 del modelo OSI), proporcionando seguridad a cualquier servicio a nivel de aplicación (nivel S de dicho modelo).

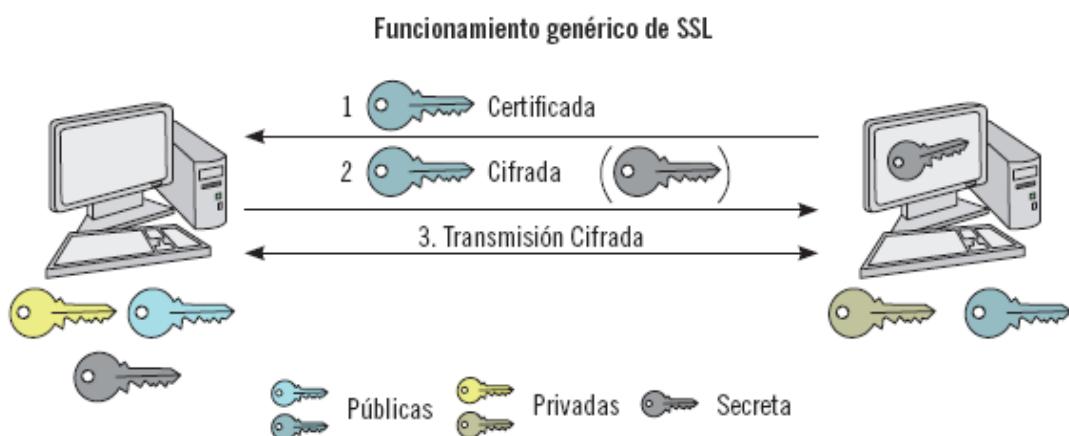
**Sabía que ...**

La utilización de SSL es muy habitual en aplicaciones en las que se hace uso de datos sensibles y se indica en el navegador con las siglas https. Por ejemplo, en la página del Banco Popular (al igual que otros), en el apartado de particulares, la dirección es: <https://www2.bancopopular.es/particularesN>.

Este protocolo se caracteriza por soportar compresión (aunque es opcional), hacer uso de certificados X.509 v3 y proporcionar los servicios de seguridad de autenticación en servidor (obligatoria), autenticación en cliente (opcional), integridad, confidencialidad y no repudio del cliente (opcional).

Para comprender con simplicidad y de forma general en qué consiste SSL, el funcionamiento del protocolo se presenta en la siguiente figura. Cada extremo de la comunicación posee un par de claves (junto con el certificado asociado y considerando que en el cliente es opcional).

Suponiendo que un cliente A quiere establecer comunicación con un servidor B, 1) B envía su clave pública certificada a A. Posteriormente A, tras crear una clave secreta, 2) se la envía a B y finalmente, 3) la transmisión de información puede comenzar, considerando que la información se transmitirá cifrada mediante la clave secreta intercambiada.



SSL está formado por varios subprotocolos, que se describen brevemente a continuación:

- Protocolo de salutación. Se ejecuta antes de transmitir los datos de la aplicación. En este protocolo el cliente y el servidor acuerdan los algoritmos que usarán para cifrar y aplicar control de integridad sobre los datos que se intercambien. Para ello, el cliente ofrece las opciones disponibles y el servidor selecciona aquella que más le conviene. En

este protocolo el servidor se autentica frente al cliente (enviándole su certificado de clave pública). Opcionalmente, también el cliente se puede autenticar.

- Protocolo de registro. Este protocolo utiliza los algoritmos definidos por el de salutación para cifrar y aplicar el control de integridad sobre los datos. También comprime los datos, haciendo que la transmisión sea más ligera.
- Protocolo de cambio de especificación de cifrado. Se emplea para que una de las partes anuncie a la otra que quiere cambiar la manera de cifrar la información. Solo consiste en un mensaje, que una parte envía a otra en el momento oportuno. De hecho, el protocolo de salutación siempre finaliza con ese mensaje. De esta manera, los acuerdos de ese protocolo empiezan a utilizarse.
- Protocolo *de aviso*. Este protocolo tiene como función avisar a cualquiera de los participantes de algún tipo de incidencia ocurrida. Puede ser debida a un error fatal o una advertencia. Si el nivel es fatal (por ejemplo, si no hay acuerdo en el protocolo de salutación) la conexión SSL asociada se finaliza. Entre las advertencias se pueden destacar la recepción de un certificado expirado o el hecho de que una de las entidades no deseé mandar más mensajes en una determinada conexión.

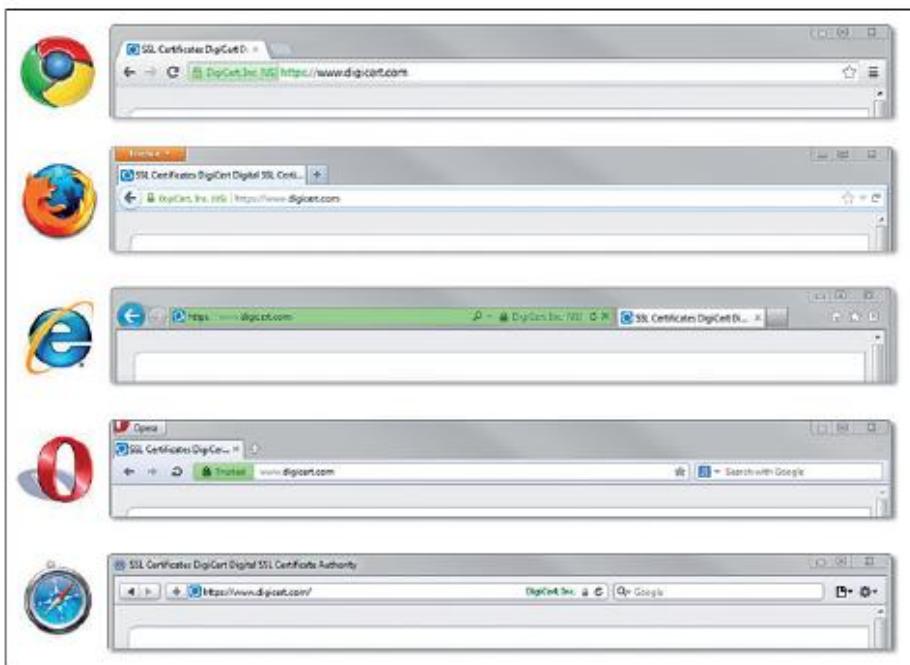
### Variante de SSL. SSL Extended Validation (EV-SSL)

Tal y como se ha podido comprobar en la descripción de SSL, uno de los aspectos clave es que el servidor envía un certificado de clave pública para autenticarse frente al cliente. Así, la capacidad para que el usuario sepa si, por ejemplo, se está conectando a la página de su banco, reside en que el certificado digital se valide correctamente.

Dada la importancia de que los certificados sean auténticos, en los últimos tiempos se ha extendido una variante de SSL, conocida como *SSL Extended Validation* (EV-SSL). EV-SSL es exactamente igual a SSL en sus fases y funcionamiento, pero impone restricciones adicionales sobre los certificados. Particularmente, se destacan las siguientes:

- Las Autoridades de Certificación están obligadas a pasar una auditoría periódica, que verifique el rigor del proceso de emisión de certificados.
- Para los certificados que se emiten a páginas web, solo se emiten si lo solicita la persona responsable del dominio o con control exclusivo sobre él.
- Las Autoridades de Certificación deben implementar el protocolo OCSP, de forma que el navegador pueda comprobar inmediatamente la vigencia del certificado.
- Los certificados se emiten con una política de certificación distinta que permite a los navegadores reconocer este tipo de certificados.

A efectos prácticos, los usuarios pueden saber que están actuando mediante EV-SSL porque el navegador suele introducir elementos visuales que así lo representan. Dichos elementos quedan reflejados en la siguiente figura.



*Representación en los navegadores de SSL Extended Validation (EV-SSL)*

#### Sabía que ...

Si se intenta conectar mediante el navegador a una página sin un certificado válido, el usuario recibirá un mensaje que indica que la web no es de confianza. Este es el motivo por el que en una web de un negocio, muchos posibles compradores abandonan la página y se pierde la venta que se iba a concretar.

#### 4.2.- Secure Shell (SSH)

*Secure Shell (SSH)* es un protocolo diseñado con los propósitos de ser simple y fácil de programar. La versión inicial estaba pensada para permitir que una persona pudiese abrir una sesión en un ordenador remoto. El propósito era reemplazar al popular protocolo TELNET y a otros esquemas que no proporcionaban seguridad.

SSH puede ser utilizado no solo para el propósito anterior, sino también para funciones como transferencias de ficheros o envíos de correos. La versión SSH2 ha supuesto una mejora respecto a la anterior y está documentada como propuesta de estándar.

Este protocolo es utilizado por múltiples aplicaciones cliente-servidor y está disponible en la mayoría de los sistemas operativos. De hecho, se ha convertido en el método habitual para realizar inicio de sesión remota y establecimiento de túneles.

SSH se compone de tres tipos de protocolos: el Protocolo de la capa de transporte, el Protocolo de autenticación de usuarios y el Protocolo de conexión. A continuación, se presentan los aspectos fundamentales de cada uno de ellos.

### **Protocolo de la capa de transporte**

Este protocolo proporciona autenticación de las entidades y de los mensajes, confidencialidad e integridad de los datos. Como su propio nombre indica, se ejecuta en la capa de transporte (nivel 4 del Modelo OSI).

Dentro de este protocolo se establecen las claves de *los Host*. La autenticación del servidor se realizará en base al par o pares de claves (público-privada) que dicho servidor posee.

#### **Nota**

El término "host" se utiliza de forma genérica para referirse a un equipo informático. En este contexto, se refiere tanto al cliente como al servidor de la comunicación.

Para autenticar al servidor, el cliente dispone de dos opciones de acuerdo a la especificación de la RFC 4251:

1. El cliente puede mantener localmente una base de datos que asocie cada nombre de host con su clave pública. Esta técnica evita la necesidad de una administración centralizada, así como el uso de un tercero de confianza para realizar la coordinación. No obstante, el mantenimiento puede ser costoso.
2. La asociación nombre de host-clave pública es certificada por una autoridad. Por tanto, el cliente puede verificar la validez de las claves proporcionadas por determinadas autoridades, utilizando la clave de la autoridad raíz. La ventaja de esta alternativa es que se disminuyen los problemas de gestión porque el cliente solo ha de almacenar de forma segura la clave de una autoridad. Sin embargo, todas las claves de los host tienen que ser certificadas por una autoridad.

Tras esta autenticación, se procede a realizar los Intercambios de paquetes. Para ello, el cliente y el servidor establecen una conexión (la cual no es parte del protocolo) y una vez establecida, comienza el intercambio de datos. Estos paquetes contienen la carga útil (es decir, lo que se quería intercambiar entre los comunicantes), a la que se aplica compresión, cifrado y control de integridad utilizando un código MAC. Al igual que sucedía en SSL, los algoritmos de cifrado, control de integridad y compresión son negociados en este protocolo, antes de que se produzca el intercambio.

Como dato interesante, el cifrado se realiza usando criptografía simétrica. Para ello se pueden utilizar distintos métodos de intercambio de clave aunque actualmente solo se han especificado

dos versiones de Diffie-Hellman. Además, el servidor es autenticado por el cliente al firmar su parte en el intercambio de Diffie-Hellman.

El intercambio de paquetes concluye con la solicitud del servicio, por el que el cliente solicita el Protocolo de autenticación de usuarios o el Protocolo de conexión.

### **Protocolo de autenticación de usuarios**

Este protocolo autentica a los usuarios frente al servidor y está pensado para ejecutarse sobre protocolos que proporcionen confidencialidad e integridad

En cuanto a los métodos de autenticación, es posible indicar el método de clave pública, en el que el cliente envía al servidor su clave pública firmada para que la verifique; el método de contraseña, en el que el cliente envía una contraseña al servidor; y el método *hostbased*, en el que el cliente envía una firma al servidor haciendo uso de la clave de su *host*, consiguiendo que el servidor confíe en el *host* cuando éste indique que el usuario se ha autenticado.

### **Protocolo de conexión**

Funciona sobre el Protocolo de la capa de transporte y permite que una misma conexión pueda ser utilizada a la vez para distintos propósitos, conocidos como canales. Un canal puede servir, por ejemplo, para ejecutar órdenes en un ordenador remoto (canal de sesión) o para usar en remoto sus programas que utilizan representación gráfica (por ejemplo, ventanas en un sistema *Windows*) (canal x11).

Un canal pasa por tres estados distintos en función del momento de transmisión de datos:

- Apertura del canal, indicando esencialmente el tipo de canal, el tamaño de datos a enviar y el tamaño máximo de los paquetes.
- Transmisión de los datos, es decir, el uso propiamente dicho del canal.
- Cierre del canal, para concluir la comunicación por parte de cualquiera de los participantes.

Finalmente, una característica muy importante de SSH es la posibilidad de realizar redirección de puertos, tanto del cliente como del servidor. Esto permite establecer la conexión SSH usando unos puertos y que cada uno de los extremos lo reenvíe a otro de sus puertos. Esto es especialmente útil cuando existen mecanismos de protección (como los llamados cortafuegos), que impiden que ciertos puertos puedan ser usados para recibir datos desde otros ordenadores.

Gracias a la redirección, se pueden recibir datos por un puerto (permitido por el cortafuegos) y reenviarlos a otro donde realmente esté esperando el programa que maneja la conexión SSH.

Un ejemplo de uso es el deseo de conectarse desde un ordenador personal al servidor de la empresa en la que se trabaja, puesto que el servidor de la empresa está tras un cortafuegos y no acepta el tráfico desde un ordenador personal.

**Recuerde**

Un cortafuegos es un dispositivo de seguridad software o hardware que permite o impide la comunicación por un determinado puerto, protocolo o aplicación.

## 5. SISTEMAS SSL VPN

SSL VPN es una forma de utilizar VPN en la que se utiliza el navegador web para establecer la conexión entre dos extremos. Una de las características más relevantes es que en SSL VPN no se requiere instalación de ningún cliente en el ordenador del usuario final. Por tanto, la utilización de este tipo de SSL se puede considerar muy sencilla para los usuarios. Un ejemplo de su utilización es la conexión desde el navegador de un ordenador personal al ordenador corporativo de la empresa, de modo que una vez establecida la VPN se consiga la misma seguridad que estando físicamente en el equipo.

A grandes rasgos, una SSL VPN se puede definir como uno o varios dispositivos VPN a los que el usuario se conecta por medio del navegador, de modo que el tráfico se cifra haciendo uso del protocolo SSL. Además de las ventajas de las VPN, los administradores pueden establecer un control de acceso más preciso, indicando tanto los usuarios que tienen acceso a una determinada aplicación como a los servicios u operaciones que estas proporcionan.

Por el contrario, las SSL VPN presentan posibles riesgos contra la seguridad de los sistemas:

- SSL VPN no requiere la instalación de ningún *software* en el cliente. Dado que habitualmente se utiliza el navegador, éste puede estar infectado con algún tipo de programa maligno, de forma que dicho programa podría infectar a la entidad donde se conecta (por ejemplo, su empresa).

Para resolver este problema, las entidades con las que se establece la VPN fuerzan la verificación de integridad en el cliente, rechazando las conexiones en caso de no disponer de ciertas medidas de seguridad establecidas en una política, por ejemplo, instalación de antivirus o de un cortafuegos.

Sin embargo, también existen otras medidas de seguridad, como el establecimiento de tecnologías que formen un perímetro de defensa, incorporando controles no en el cliente sino en el extremo opuesto con el que se establece la comunicación. Esta solución es más sencilla puesto que no se requiere ninguna acción en el cliente.

- Otro de los riesgos se asocia con la información almacenada en los historiales. Cuando se realiza una conexión con un navegador, se dejan rastros indicando dónde y para qué fueron utilizados (*cookies*, historial de URL, etc.). El problema se agrava si la comunicación se establece desde un ordenador público, ya que la información almacenada puede quedar a disposición de terceros no autorizados (por ejemplo, otros usuarios de un ciber-

café). Por ello, el extremo al que se establece la conexión VPN SSL suele incluir funciones para eliminar la información creada en cada sesión.

- Como no se requiere la instalación de ningún *software* en el cliente, cualquier usuario con acceso a la web puede acceder a una VPN SSL. Por tanto, esto facilita la existencia de ataques remotos de descubrimiento de contraseñas. Un modo de solucionarlo sería utilizar métodos robustos de autenticación, como es la autenticación de dos factores.

### Recuerde

La autenticación puede basarse en distintos factores, algo que se conoce, que se tiene o que se es. Por tanto, la autenticación de dos factores hará uso de técnicas que utilicen dos de los factores mencionados, por ejemplo, algo que se conoce y algo que se es, tal y como una contraseña y la huella dactilar.

## 5.1.- Tipos de SSL VPN

Se pueden distinguir un par de tipos de redes privadas virtuales basadas en SSL. Estos tipos son soportados por la mayoría de los sistemas y su utilización puede pasar desapercibida para los usuarios.

### VPN SSL portal

Permiten a los usuarios establecer una única conexión SSL con un sitio web para poder acceder remotamente y de forma segura a distintos servicios de red. El funcionamiento es muy sencillo: el usuario accede a una página web, la cual es una puerta de entrada a los servicios, de ahí el nombre de **portal**. Posteriormente, tras el acceso se produce la autenticación y, tras ello, dicha página web presenta los servicios a los que el usuario tiene acceso.

Muchas de las SSL VPN se basan en la re-escritura de las URL al vuelo. Esto se debe a que los servicios a los que se puede acceder a través de esa página web pueden estar situados en direcciones de Internet distintas. Así, aunque el usuario perciba que puede acceder a todos los servicios desde un punto único, en realidad es necesario que, cuando se acceda a un servicio, se le remita a la dirección (URL) donde éste se encuentra. Por ejemplo, la página <http://curso.example.com/clase> se puede convertir en "<https://proxySalida.example.com/clase>". Esta característica puede poner en riesgo la seguridad de los usuarios por dos motivos. Por un lado, si la re-escritura no se hace con cuidado, se puede enviar al usuario a una dirección no adecuada.

En otras palabras, si el sistema que hace la re-escritura es comprometido, puede poner en riesgo al usuario (al llevarle a páginas peligrosas) y al servidor completo (al permitir el acceso a zonas

restringidas). Por otro, esta re-escritura se hace habitualmente mediante lenguajes como Javascript, Flash o Java, que en ocasiones entrañan problemas de seguridad.

Otra cuestión que afecta a la seguridad es que muchas SSL VPN almacenan en caché o mantienen en memoria durante un periodo de tiempo, la información de autenticación de los usuarios para evitar que los clientes tengan que autenticarse frecuentemente en todos los servidores web utilizados. De nuevo, mantener almacenada la información de autenticación pone en riesgo la seguridad de los usuarios, puesto que podría permitir múltiples ataques como el de suplantación de identidad.

### Definición

#### Caché

Es un tipo de memoria volátil y de pequeño tamaño, que se caracteriza por ser de rápido acceso.

### SSL VPN túnel

Permite a los usuarios usar un navegador web para acceder de forma remota y segura a múltiples servicios web utilizando un túnel que hace uso de SSL. En este caso, se necesita que el navegador soporte, entre otros, el uso de Java, JavaScript, ActiveX, aplicaciones Flash o *plugins*.

### Definición

#### Plugin

Pequeño programa adicional que se instala en otro (por ejemplo, un navegador) para incorporarle alguna funcionalidad adicional.

Este tipo de VPN también presenta algunos inconvenientes. Por un lado está el uso de los puertos. Como se introdujo en el Modelo OSI, para establecer una conexión es necesario saber la dirección a la que conectarse y, además, el puerto al que se debe hacer. Esto permite al ordenador que recibe la conexión saber a cuál de los programas que están esperando datos debe enviarse lo que se reciba en esta conexión. En las VPN creadas con SSL no existe ningún estándar para la utilización de los puertos en los túneles. Esto exige conocer con antelación qué puertos hay que usar para la conexión. Por otro lado, los programas y funciones que se utilizan no siempre son

iguales en todos los navegadores. Esto fuerza a utilizar un determinado navegador (por ejemplo, *Microsoft Internet Explorer*) para utilizar esta tecnología.

## 6. TÚNELES CIFRADOS

Un túnel se define como la encapsulación de un protocolo de red en otro, de modo que las solicitudes puedan llegar de un origen a un destino. De esta forma, se permite la utilización de un protocolo en un entorno de red que no lo permitiría. Recordando la analogía del correo entre urbanizaciones, para comunicar ambas urbanizaciones fue necesario meter el sobre en otro. De lo contrario, una carta de una urbanización a otra jamás habría podido enviarse por las restricciones de seguridad (que, en ese caso, solo permitían el envío de correo entre vecinos de una misma urbanización). Ese es un ejemplo gráfico del uso de túneles.

Los túneles se pueden considerar como la base sobre la que se asientan las VPN. Para construirlos se utilizan los protocolos de tunelado. Dentro de estos, se destacan por su importancia aquellos que no solo incluyen la información en su interior, sino que además la cifran. A continuación, se revisan los protocolos más habituales que cumplen con este objetivo, además de SSL, IPSec y SSH, descritos anteriormente.

Debe destacarse que existen otros protocolos para la construcción de túneles, pero no siempre incluyen la característica de cifrado. Por ejemplo, el protocolo *Generic Routing Encapsulation* (GRE) establece una forma genérica de encapsular un protocolo en otro, lo cual constituye una base importante para establecer túneles. Esto es especialmente útil cuando se utilizan diferentes tecnologías de red en los distintos tramos. Sería el caso de una red interna que utiliza IP en su versión 6, mientras que la conexión a través de Internet usa IP en su versión 4: es necesario un protocolo de encapsulado (como GRE) que proporcione un mecanismo para encapsular el paquete de la versión 6 en uno transportable a través de dicha red. Nuevamente en la analogía del correo: gracias a GRE los conserjes de las urbanizaciones serían capaces de enviar el sobre a otra urbanización utilizando distintos tipos de sobres (acolchados, certificados, paquete postal, etc.). Esto hace que el envío pueda hacerse no solo a través de una única vía (el servicio público de Correos), sino de varias (por ejemplo, una empresa de mensajería que solo se hace cargo de paquetes postales).

A continuación, se presentan tres protocolos de tunelado relevantes: PPTP, L2TP y DTLS.

### 6.1.- Point-to-Point Tunneling Protocol (PPTP)

*Point-to-Point Tunneling Protocol* (PPTP) fue un protocolo desarrollado por Microsoft y normalizado por la IETF (RFC 2637). PPTP hace uso de la seguridad de otro protocolo, llamado *Point-to-Point* (PPP), para realizar la comunicación en el túnel. Así, se proporcionan los servicios de autenticación y confidencialidad haciendo uso de PPP.

Respecto a la autenticación, es posible hacer uso de protocolos como:

- *Password Authentication Protocol* (PAP). Este es un protocolo considerado inseguro, pues la contraseña se envía en claro (es decir, sin cifrar).

- *Shiva Password Authentication Protocol* (SPAP) es un protocolo sencillo en el que la contraseña se manda cifrada al servidor de acceso remoto *Shiva*, el cual la descifra y envía un mensaje de confirmación.
- *Challenge Handshake Authentication Protocol* (CHAP) es un protocolo que evita el envío de contraseñas. Está basado en un reto-respuesta de modo que el servidor envía un reto al cliente y éste responde haciendo uso de la función resumen MDS para poder autenticarse.
- Microsoft CHAP vi (MS-CHAP vi). Es un protocolo similar a CHAP pero, por el contrario, hace uso de MD4, proporciona un mecanismo controlado de cambio de contraseñas, incluye un mecanismo de control de reintentos al introducir contraseñas y especifica diferentes códigos de errores.
- MS-CHAP v2. Es la versión revisada del protocolo anterior. A pesar de mejorar la seguridad, sigue señalándose como inseguro.

**Sabía que ...**

MS-CHAP v2 ha sido criptoanalizado por autores como Bruce Schneier o Eisinger.

En relación con la confidencialidad, se hace uso del protocolo *Microsoft Point-to-Point Encryption* (MPPE) para cifrar los mensajes. El cifrado se realiza a través del algoritmo de cifrado de flujo RC4. La clave de cifrado se construye a partir de la contraseña especificada por el usuario y la información generada en el proceso de autenticación con MS-CHAP. Esta clave cambia periódicamente para dificultar la labor de un posible atacante. No obstante, debe tenerse en cuenta que el cambio de clave es un proceso que consume algunos recursos, por lo que el periodo no debe ser ni muy grande (pues disminuiría la seguridad) ni muy pequeño (pues sería muy costoso).

Finalmente, en cuanto a la comunicación por PPTP se pueden distinguir dos tipos: de control y de datos. La comunicación de control se basa en controlar y gestionar la información que pasa por el canal. Por otro lado, la comunicación de datos consiste en realizar el encapsulado y transmisión de datos mediante el protocolo GRE, presentado anteriormente.

## 6.2.- Layer 2 Tunelling Protocol (L2TP)

El protocolo L2TP permite esencialmente construir túneles para que dos equipos o subredes puedan conectarse a través del protocolo PPP.

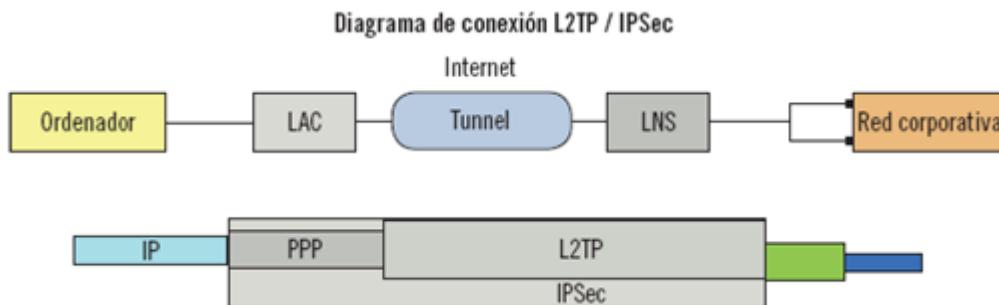
Para conseguirlo, la arquitectura de L2TP se compone de:

- Un equipo (o subred) origen.
- Un punto de acceso (denominado LAC).

- Un terminador del túnel (denominado LNS).
- Y una red (o un equipo) destino.

La relación entre los cuatro componentes es la siguiente: el equipo origen establece la conexión PPP con el LAC, y es éste el encargado de establecer el túnel L2TP propiamente dicho con el LNS. De esta manera, el equipo origen consigue conectarse mediante PPP a la red destino, a\m en presencia de diversas tecnologías de red.

Una cuestión importante es que L2TP no proporciona como tal cifrado de las comunicaciones. Por este motivo, se suele combinar con otras tecnologías que sí lo proporcionen. Una de las combinaciones más habituales es la utilización de IPSec. En este caso, una vez que el túnel se ha establecido entre el LAC y el LNS, el equipo origen se conecta por IPSec con el LNS.



Al igual que sucede en PPTP, para ofrecer un mejor nivel de servicio el protocolo L2TP no solo se dedica a transmitir paquetes con información útil, sino que también incluye mensajes de control. Estos sirven para mantener las conexiones activas, restablecerlas o finalizarlas cuando proceda. De hecho, en la puesta en marcha de un túnel L2TP se suceden dos pasos: primero se establece la conexión de control y, posteriormente, se inicia una sesión para la transmisión de información útil.

Dada la importancia de la conexión de control, L2TP incluye mecanismos para asegurar la entrega de los mensajes involucrados en ella. También incluye mecanismos opcionales para asegurar la autenticidad y la integridad de dichos mensajes. Si esta opción quiere activarse, los comunicantes deberán haber compartido previamente una contraseña común. Debe notarse que, a diferencia de la conexión de control, la transmisión de información útil en L2TP no garantiza ni la entrega ni la integridad de los paquetes intercambiados. Estos servicios deben ser proporcionados, por tanto, por el protocolo encapsulado en L2TP.

### 6.3.- Datagram Transport Layer Security (DTLS)

*Datagram Transport Layer Security (DTLS)* es un protocolo basado en TLS que proporciona comunicaciones seguras para la transmisión de datagramas.

**Definición****Datagrama**

Un datagrama es una unidad mínima de transferencia en la que no se garantiza el tiempo de entrega y llegada ni el orden de entrega.

Su utilización es adecuada para asegurar programas que sean sensibles a los retardos en la información (por ejemplo, escuchar música a través de Internet). Permite prevenir posibles escuchas, manipulaciones y falsificación de mensajes.

Dado que en DTLS se intercambian datagramas, incluye mecanismos para gestionar la pérdida y el reordenamiento de paquetes, junto con la detección de reenvíos.

En general, se pueden mencionar un par de ventajas de DTLS. Por un lado, dada la similitud de DTLS con TLS, la mayor parte de los medios que se emplean para utilizar TLS pueden ser reaprovechados. Por otro lado, DTLS tiene aspectos muy genéricos y flexibles, por lo que es fácil adaptar protocolos para que hagan uso de él.

## 7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

Las dos alternativas que más se emplean en la actualidad para la implementación de VPN son los sistemas basados en IPSec y aquellos basados en SSL. A continuación, se estudian por separado las ventajas e inconvenientes de cada uno.

### 7.1.- Pros y contras de IPSec VPN

La tecnología IPSec está especialmente diseñada para aquellas situaciones en las que se quiere realizar una red privada estable a lo largo del tiempo. Además, permite ofrecer un servicio de comunicaciones cifradas a diversas aplicaciones, ya que se sitúa en la capa de red (es decir, por debajo de las aplicaciones).

Entre las principales desventajas de IPSec, destaca la complejidad de su administración y configuración. Esta situación es particularmente desaconsejable cuando se trata de permitir, por ejemplo, que los empleados accedan desde los ordenadores de sus hogares a la red de la empresa. Para utilizar IPSec es necesario instalar en dichos equipos un programa que aplique la configuración necesaria. Esto dificulta el mantenimiento por parte del personal de Tecnologías de la Información de la empresa.

## 7.2.- Pros y contras de SSL VPN

La utilización del protocolo SSL para establecer una red privada virtual constituye una alternativa sencilla. Esto es importante para los escenarios en los que se persigue que un equipo se conecte a una determinada red empresarial: no es necesario que en dicho equipo se instale ningún programa especialmente complejo. Esto simplifica su puesta en marcha y disminuye la necesidad de mantenimiento, lo que en la práctica se traduce en una reducción de costes.

Entre los aspectos menos favorables, esta tecnología es más adecuada cuando las aplicaciones se ejecutan en el navegador web, algo que no siempre ocurre. Además, dado que SSL se sitúa en el nivel de transporte del Modelo OSI, no permite que todas las aplicaciones se aprovechen de la existencia de la red privada virtual. Por otro lado, es necesario tener en cuenta que SSL permite que los algoritmos criptográficos se negocien en cada una de las sesiones. Esto puede dar lugar a la elección de algoritmos o claves que sean poco robustos, lo que puede comprometer la seguridad de la comunicación.

## 7.3.- Análisis de costes

Además del análisis anterior, es necesario estudiar cada una de las fuentes de coste que originan estas soluciones.

Con respecto al equipamiento necesario para incorporar estas tecnologías, ambas necesitan algún equipamiento de red que permita utilizarlo en el entorno corporativo. En el caso de IPSec, esto suele ser un dispositivo de red (como un encaminador o *router*), mientras que en SSL se emplea un servidor especialmente dedicado. Estos servidores suelen ser mucho más caros que los encaminadores. Además de lo anterior, los equipos finales que acceden utilizando IPSec necesitan un componente (denominado habitualmente **cliente VPN**) que puede presentarse en forma de programa informático o dispositivo físico. En este último caso, debe tenerse en cuenta el coste, que contrasta con las necesidades que plantea SSL: no requiere ningún programa ni dispositivo específico.

La otra fuente de coste que debe considerarse es la relativa a la puesta en funcionamiento de todos los programas que deben poder ejecutarse a través de la VPN. En el caso de IPSec, una vez que se ha establecido la conexión todos los programas pueden emplearla. Por el contrario, cada uno de los programas necesita un soporte específico si la tecnología seleccionada es SSL.

## 8. RESUMEN

El establecimiento de canales seguros de comunicación es fundamental para el intercambio de datos. En base a ello, las redes privadas virtuales (VPN) y los túneles de cifrado son elementos esenciales. Gracias a ellos es posible establecer comunicaciones seguras entre dos entidades o usuarios, eliminando la necesidad de tener que estar físicamente en la misma red. Y no solo eso: permiten crear una comunicación segura utilizando un canal inseguro, como puede ser Internet. Hay múltiples protocolos que permiten su establecimiento. Entre ellos cabe destacar IPSec, SSL y SSH.

IPSec es un protocolo que actúa en la capa de red y está compuesto esencialmente de los protocolos de *Internet Key Exchange* (IKE) y *Encapsulating Security Payload* (ESP). SSL, en cambio, actúa en una capa superior, en la capa de transporte, y se compone de los protocolos de Registro, Salutación, Cambio de especificación de cifrado y Aviso. También ejecutándose en la capa de transporte, SSH es un protocolo de autenticación remota compuesto por los protocolos de Capa de transporte, Autenticación de usuarios y Conexión.

Finalmente, cabe destacar dos de las alternativas de VPN más extendidas: VPN SSL y VPN IPSec. La elección entre una u otra tecnología para implementar una VPN debe partir, necesariamente, del estudio detallado del contexto y de las necesidades de los usuarios. Las VPN SSL son interesantes porque pasan desapercibidas para los usuarios y se basan en utilizar el navegador web para establecer una comunicación entre dos extremos.