AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación
Infraestructura de Clave Pública (PKI)

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-1020-110920*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*20/09/2011*
N° de Páginas	*1 de 16*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es proporcionar al personal técnico de la Junta de Andalucía información que le ayude a comprender el funcionamiento de una Infraestructura de Clave Pública o PKI (Public Key Infraestructure), las técnicas criptográficas que utiliza, los elementos que la componen, la interacción entre ellos y los riesgos más importantes que le pueden afectar.

3 ALCANCE

El documento va destinado al personal técnico de la Junta de Andalucía, técnicos de gestión de incidentes de AndalucíaCERT y público en general.

4 CONCEPTOS BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN

En este apartado se explicarán conceptos básicos relacionados con la seguridad de la información. Estos conceptos ayudarán a comprender los mecanismos descritos más adelante.

La seguridad de la información comprende aquellas medidas que permiten la protección de la información manteniendo su **confidencialidad**, **disponibilidad** e **integridad**.

Se utiliza la **criptografía** como herramienta para proteger las redes de comunicaciones, nos permite evitar que alguien intercepte, manipule o falsifique los datos transmitidos. Ésta estudia los métodos de protección de la información desde un punto de vista matemático.

Mediante el uso del **cifrado** se preserva la **confidencialidad**. Se aplica una transformación a los datos de manera que sólo el destinatario legítimo puede realizar la transformación inversa y obtener los datos originales.

Cifrar un mensaje consiste en aplicarle un algoritmo de cifrado. Este algoritmo transforma el mensaje o datos en otro mensaje al que llamaremos mensaje cifrado. Es necesario que exista un algoritmo de descifrado que permita obtener los datos originales a partir del mensaje cifrado.

La **integridad** de los datos es una propiedad cuyo objetivo es mantener los datos libres de modificaciones no autorizadas. Se suelen adjuntar otros datos junto con el mensaje original para comprobar que se mantiene la integridad del mismo, como por ejemplo la firma digital.

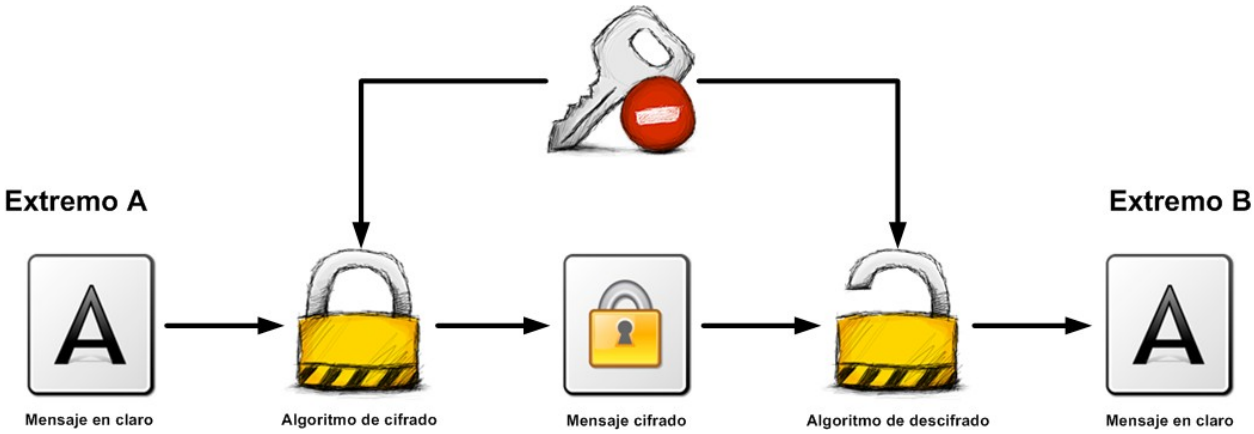
Por otra parte, la **autenticación** consiste en verificar o confirmar la procedencia de un objeto o la identidad de alguien.

Por último, la criptografía permite garantizar el **no repudio** o irrenunciabilidad, esto permite probar la participación de las partes en una comunicación.

5 CRIPTOGRAFÍA DE CLAVE SIMÉTRICA

La criptografía de clave simétrica se caracteriza por el hecho de que la clave utilizada para cifrar el mensaje es la misma que la que usa para descifrarlo. Es necesario mantener en secreto la clave para mantener seguro el sistema.

Si "A" quiere comunicarse con "B" por un canal inseguro mediante mensajes cifrados, en primer lugar ambos tienen que conocer la clave de cifrado/descifrado. Si "A" le envía la clave a "B" por el mismo canal que los datos cifrados es posible que un tercero intercepte la clave y descifre toda la comunicación.



Por este motivo sería conveniente que la clave viajara por un canal aparte y seguro, o que se pusieran de acuerdo de antemano sobre la clave a usar.

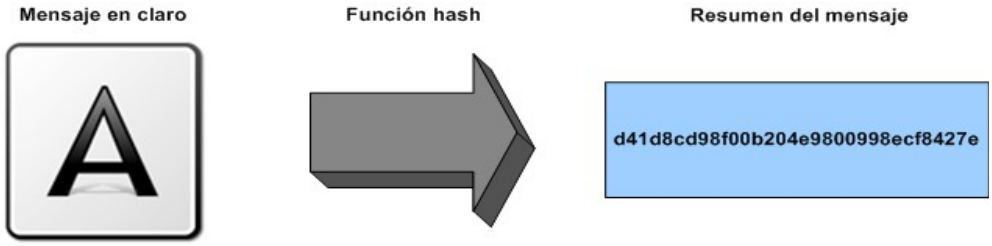
El canal seguro puede que no esté disponible o que resulte difícil enviar información por él, si no fuera así no habría problemas en mantener una comunicación desde el principio a través de él. Esto hace que cambiar la clave de cifrado y realizar un intercambio de claves sea un problema en la criptografía de clave simétrica.

Algunos ejemplos de algoritmos de clave simétrica son: RC4 (Ron's Code 4), DES (Data Encryption Standard), 3DES (Triple DES), AES (Advanced Encryption Standard).

6 FUNCIONES HASH

Existen otros algoritmos cuyo objetivo es garantizar la integridad de los mensajes, las **funciones hash**. Estas funciones generan un resumen de longitud fija a partir de un mensaje de longitud arbitraria como entrada que identifica perfectamente el texto. Tienen la propiedad de que el mismo mensaje generará el mismo resumen. Si dos resultados de una misma función son diferentes los mensajes originales también lo son. Estas funciones se diseñaron para ser unidireccionales, es decir, que no fuera posible a partir del resumen obtener el mensaje original, y que fueran resistentes a colisiones, evitar que dos entradas distintas produzcan la misma salida.

Por ejemplo, MD5 genera un hash de 128 bits:



Aunque las funciones hash están diseñadas para funcionar en un único sentido, generar el resumen de datos o firma y no obtener el dato original a partir de ésta, existen técnicas para hackear o conseguir el mensaje o cadena original. Esto se puede conseguir generando claves mediante la combinación secuencial de caracteres hasta encontrar una cadena con un hash igual al que queremos descubrir. Esta es una técnica típica para obtener las contraseña del archivo SAM de Microsoft Windows © mediante las tablas Rainbow, romper los cifrados de los archivos shadow en Linux, Solaris y Unix o descubrir el usuario o password de un servicio remoto.

Sin embargo, un factor importante para poder obtener la cadena original es el tiempo que se necesita para lograrlo. No es lo mismo conseguir una clave en 30 minutos que en 2000 años. Los factores que influyen en el tiempo son los siguientes:

- **Se ha usado una clave o un cifrado fuerte.** El número de caracteres usados en la clave o el algoritmo utilizado para desordenar los datos influyen directamente en el tiempo que se necesita para averiguar la clave por fuerza bruta.
- **El charset o juego de caracteres utilizado.** Pueden ser números, letras, mayúsculas, caracteres especiales. A mayor variedad mayores combinaciones posibles aumentando la complejidad para sacar la clave.
- **Utilización de palabras predefinidas.** El usar palabras de diccionarios facilita la obtención de la clave, algunos diccionarios son: palabras del español e ingles, números, passwords por defecto, nombres de personas, diminutivos, nombres de trabajos, formatos de fechas.
- **Palabras híbridas.** Palabras terminadas por un número o unión de dos palabras son combinaciones sencillas que utilizan muchas herramientas de fuerza bruta de contraseñas.
- **Palabras relacionadas con un patrón.** No es recomendable usar palabras que sean fáciles de adivinar por estar relacionadas con nuestra persona o contexto como por ejemplo: nombre, dni, libros favoritos, nombres de parientes, mascotas, etc.

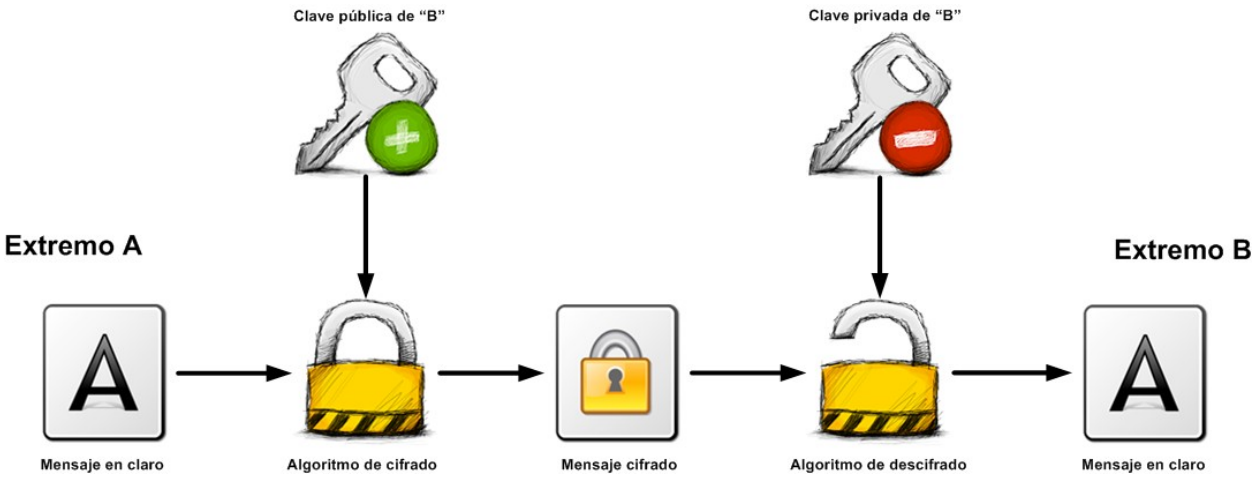
Los puntos anteriores deben tenerse en cuenta a la hora de elegir una clave para acceder a algún servicio.

Algunos ejemplos de funciones hash son: MD5 (Message Digest 5), SHA-1 (Secure Hash Algorithm-1).

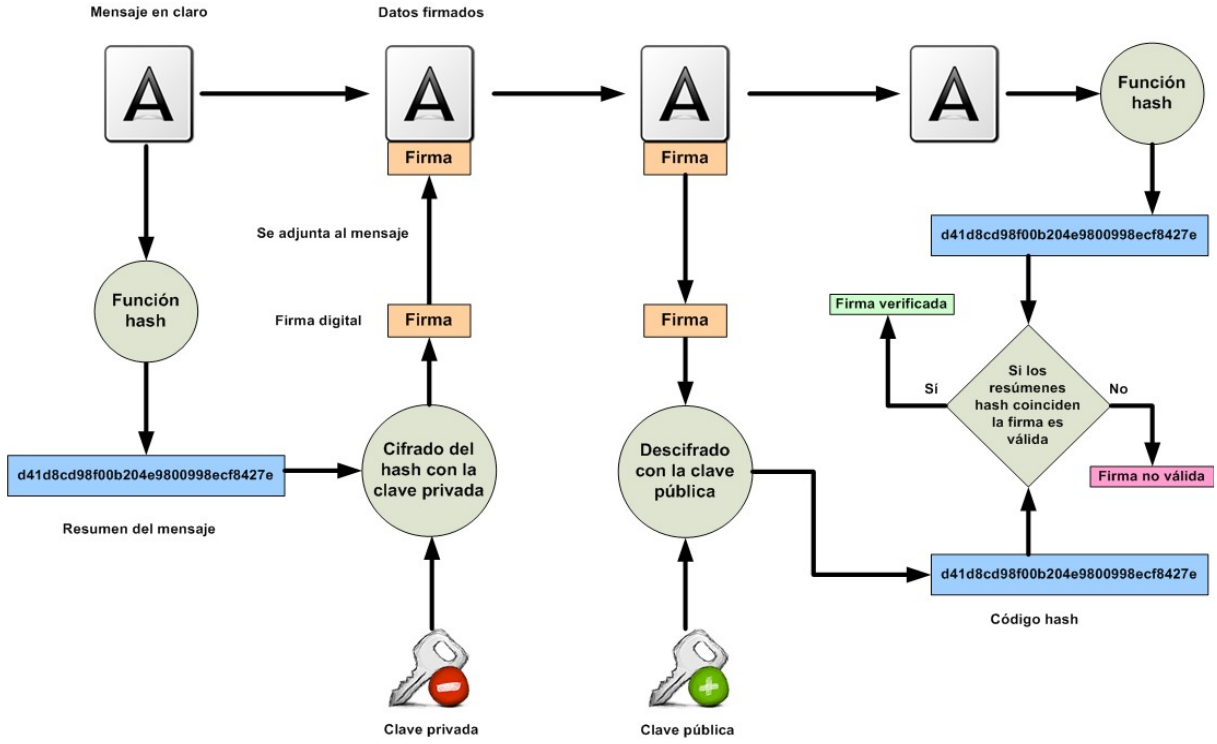
7 CRIPTOGRAFÍA DE CLAVE PÚBLICA

La criptografía de clave pública, también llamada de clave asimétrica, resuelve el problema de intercambio de claves que se presenta en la criptografía de clave simétrica. Un algoritmo de clave pública utiliza una clave para cifrar y otra distinta para descifrar datos. A una de ellas se le llama clave pública y a la otra clave privada. La clave pública se puede obtener fácilmente de la clave privada, mientras que la clave privada no se puede obtener a partir de la clave pública. Ambas claves son diferentes pero están matemáticamente asociadas. La clave privada debe permanecer en secreto y bajo el control del usuario. La clave pública podrá ser distribuida libremente.

Para cifrar la información y mantener la confidencialidad el emisor cifra un mensaje con la clave pública del receptor, el receptor lo descifra con su clave privada. Esto demuestra que la posee y se garantiza la autenticidad y confidencialidad. Aunque también hay algoritmos que cifran con la clave privada y descifran con la pública. Un inconveniente de este tipo de algoritmos es que son más lentos, necesitan mayor tiempo de proceso que los de clave simétrica por lo que se usan para aquellas situaciones en las que la clave simétrica presenta mayores problemas, como en el intercambio de claves y la autenticación con no repudio (firmas digitales).



También se usan los algoritmos de clave pública para comprobar la autenticación. "A" puede enviar un mensaje cifrado con su clave privada, los destinatarios al descifrarlo con la clave pública de "A" comprobarán que el mensaje lo ha generado "A" y no otra persona, pues él es el que posee su clave privada. Se comprueba además que el mensaje no ha sido manipulado en el camino, que mantiene su integridad, esto se realiza mediante las firmas digitales



Algunos ejemplos de algoritmos de clave pública son: Diffie-Hellman, RSA, DSA, ElGamal.
Como hemos podido ver, la criptografía de clave pública permite resolver los problemas derivados de la utilización de los algoritmos de cifrado de clave simétrica. A pesar de ello, surgen nuevos problemas que se deben resolver al utilizar la criptografía de clave pública:

- **Autenticidad de la clave:** cuando se recibe un mensaje de una persona, "A", afirmando ser "A", surge la necesidad de confirmar que efectivamente es quién dice ser y no una tercera persona que se haya generado un par de claves en nombre de "A" y se quiera hacer pasar por él, propio de ataques de tipo Man In The Middle y usurpación de identidad.
- **Revocación de claves:** si la clave privada de "A" fuera robada por un tercero, "C", este podría hacerse pasar por "A" y leer los mensajes cifrados con la clave pública de "A". Sería necesario un método que invalidara las claves robadas para que no pudieran ser utilizadas.
- **No repudio:** a la hora de firmar un documento, "A" guarda en secreto su clave privada. Podría afirmar que la clave con la que está firmado el documento no es suya. Haría falta un método para probar que la clave privada que generó la firma digital es realmente la de "A".
- **Necesidad de llevar a cabo políticas con las claves:** en una organización surge la necesidad de gestionar fácilmente las claves generadas, centralización de claves, homogeneización de parámetros al generar las claves, revocación de claves de forma automática, gestionar la caducidad de claves generadas, etc.

8 INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

Las necesidades planteadas en el punto anterior se satisfacen mediante el despliegue de una **infraestructura de clave pública** o Public Key Infraestructure (PKI) y el uso de los certificados digitales.

Una infraestructura de clave pública es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas. Estas garantías se basan en una autoridad de certificación (CA) en la cual se confía y nos asegura la vinculación o relación entre la identidad de un sujeto y su clave pública.

Los usuarios pueden utilizar la clave privada contenida en los certificados digitales para **firmar digitalmente mensajes**. Otros usuarios comprobarán la firma con la clave pública del usuario firmante contenida en el certificado emitido por la Autoridad Certificadora de PKI.

El **cifrado** de mensajes se realiza con la clave pública del destinatario. El destinatario es el único que puede descifrar el mensaje pues es el único que posee su clave privada, garantizando la confidencialidad del mensaje.

8.1 Funciones de una PKI

Las principales funciones de una Infraestructura de Clave Pública son:

- **Generación y registro de claves:** generación del par de claves del usuario y, opcionalmente, el almacenamiento de la clave privada para el caso de pérdida de la misma.
- **Identificación de los peticionarios de los certificados:** comprobación de la identidad de la persona que pide el certificado.
- **Emisión de los certificados:** una vez verificada la identidad del peticionario se procede a la emisión de su certificado.
- **Mantenimiento de la lista de certificados revocados:** en el caso de que un usuario crea que su clave privada ha podido ser obtenida por otra persona, debe comunicarlo a la Autoridad de Certificación la cuál lo incluirá en una lista "negra" de certificados que han perdido su validez, denominada lista de certificados revocados (CRL).
- **Publicación de los certificados:** es responsabilidad de la PKI que todos los certificados emitidos estén almacenados en un lugar público, para que estos puedan ser usados.

8.2 Elementos que forman una PKI

Se describen a continuación los elementos más comunes que forman una PKI:

- **Autoridad de Certificación (CA, Certificate Authority):** son entidades de confianza, responsables de emitir y revocar los certificados digitales. Básicamente se encargan de la gestión de los certificados firmados. Es un Prestador de Servicios de Certificación. Legitima ante terceros que confían en sus certificados la relación entre la identidad de un usuario y su clave pública. La confianza que los usuarios depositan en la CA es muy importante y es una de las bases del modelo de funcionamiento de una PKI. Se encargan de publicar y actualizar las listas de certificados revocados (CRL) y la renovación de certificados por caducidad o revocación. Esta lista se utiliza para publicar los certificados que dejan de ser válidos antes de su fecha de caducidad. Puede haber diversos motivos para revocarlos como que la clave privada del usuario haya sido robada o se haya emitido otro certificado que sustituya a éste. Por ello es importante que la CA mantenga actualizadas las listas de revocación.
- **Autoridad de Registro (RA, Registration Authority):** las Autoridades de Registro son las responsables de verificar la identidad del solicitante de un certificado y el enlace entre la clave pública y el certificado antes de su expedición. Estas entidades asumen tareas administrativas de la Autoridad de Certificación. Registran las peticiones de los solicitantes y una vez que identifican al solicitante realizan la petición de certificado a la CA. Este papel puede asumirlo también una Autoridad de Certificación que no disponga de una Autoridad de Registro.
- **Repositorios:** los repositorios contienen o almacenan la información relativa a una PKI. Los repositorios más importantes dentro de la infraestructura de una PKI son el repositorio de certificados y las listas de revocación de certificados o CRL. En estas listas se incluyen todos los certificados que se han invalidado antes de su fecha de caducidad.
- **Autoridad de Validación (VA, Validation Authority):** es la encargada de comprobar y proporcionar información sobre la validez de los certificados digitales que hayan sido registrados por una Autoridad de Registro y certificados por una Autoridad de Certificación.

  Estas funciones están separadas de la Autoridad de Certificación para separar la comprobación de la vigencia de un certificado de los datos de identidad de su titular. De esta manera la Autoridad de Certificación no tiene acceso a los datos de las transacciones que se realicen con los certificados que ella emite y las Autoridades de Validación no tienen acceso a la identidad de los titulares de los certificados electrónicos que maneja, reforzando la transparencia del sistema.

  Los datos de validación se ofrecen a través del protocolo Online Certificate Status Procol (OCSP). Un cliente OSCP envía una consulta sobre el estado de un certificado a la Autoridad de Validación, ésta tras consultar su base de datos ofrece vía http una repuesta sobre el estado del certificado.

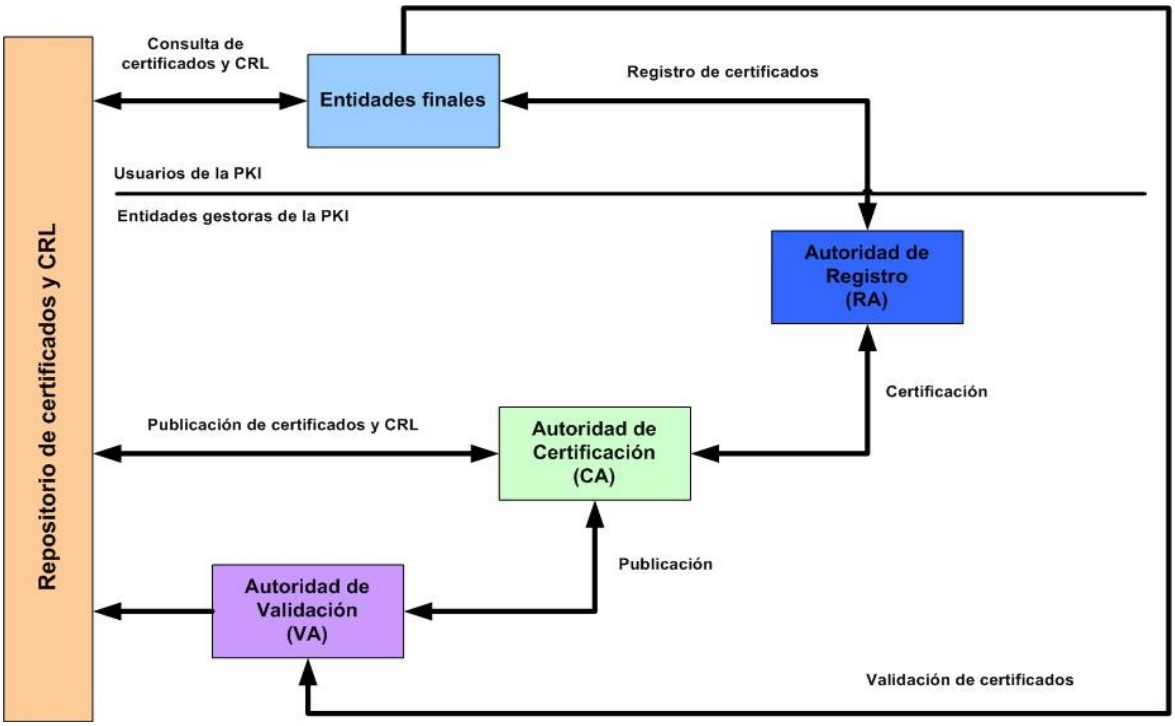
- **Autoridad de sellado de tiempo (TSA, TimeStamp Authority):** las Autoridades de sellado de tempo se encargan de firmar documentos electrónicos con la finalidad de demostrar que han existido y no han sido alterados desde un determinado instante de tiempo. La indicación temporal junto con el hash del documento se firma por la Autoridad de sellado de tiempo.

  Los sellos de tiempo garantizan que las transacciones en el comercio electrónico ocurren en un momento concreto y sus contenidos no han sido modificados desde entonces. Mediante la integración de un servicio de sellado de tiempo, se evita el fraude y la repudiación lo que aumenta la fiabilidad y la confianza. También puede usarse el sellado de tiempo para certificar la existencia de cualquier trabajo creativo desde un momento concreto. Esto impide infringir los derechos de la propiedad intelectual. Si se produce un plagio, la persona con el sello de tiempo más antiguo tendrá una prueba fehaciente para reclamar la propiedad del copyright de esa creación.

  En una PKI una firma digital indica quién ha firmado un documento electrónico. La firma puede aún ser repudiada si el documento no incluye una firma de tiempo fiable. El sello de tiempo sobre una firma digital proporciona tiempo preciso de una tercera parte confiable, mostrando cuándo el documento se ha firmado. En ese caso, el documento tiene la propiedad de no repudio.

- **Entidades finales:** aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmas digitales, cifrar documentos para otros usuarios, etc).

El gráfico siguiente muestra la interacción entre los elementos descritos anteriormente:



8.3 Certificados digitales

Un certificado digital es un documento digital que garantiza el vínculo entre la identidad de un sujeto y una clave pública. La garantía de este vínculo la proporciona una entidad en la que se confía, una Autoridad de Certificación. Esta entidad firma el certificado con su clave privada lo que asegura que la identidad y la clave corresponden al usuario o entidad que figura en el certificado. Existen varios formatos para los certificados digitales, aunque los más usados son los que se basan en el estándar X.509 en su versión 3. Estos emplean el lenguaje ASN.1 (Abstract Syntax One). Los formatos más comunes de codificación son DER (Distinguis Encoding Rules) o PEM (Privacy Enhanced Mail).
Un certificado X.509 contiene los siguientes campos:

- Certificado
  - Versión
  - Número de serie
  - ID del algoritmo
  - Emisor
  - Periodo de validez
    - No antes de
    - No después de
  - Nombre del sujeto
  - Información de clave pública del sujeto
    - Algoritmo de clave pública
    - Clave pública del sujeto
  - Identificador único de emisor (opcional)
  - Identificador único de sujeto (opcional)
  - Extensiones (opcional)
    - ...
- Algoritmo usado para firmar el certificado
- Firma digital del certificado

Se describen a continuación los tipos de ficheros de certificados más comunes:

- **.p12** : corresponde al estándar PKCS#12. Éste define un formato de fichero en el que se almacena tanto las claves privadas como el certificado de clave pública, protegido con una clave simétrica.
- **.pfx** : predecesor de PCKS#12.
- **.crt** : este formato almacena certificados X.509v3.
- **.pem** : Privacy Enhanced Mail Security Certifcate. Formato desarrollado para su uso en correo electrónico.
- **.cer** : usado para la distribución de certificados X.509.

- **.p7b** : formato de estructura de firma electrónica PKCS#7. Solamente contiene el certificado y/o la lista de certificados revocados.
- **.key** : formato para la distribución de claves privadas.

Ejemplo de certificado de una Autoridad de Certificación raíz:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=ES, O=Junta de Andalucia, OU=RCJA, CN=Autoridad de Certificacion Raiz de Telecomunicaciones/emailAddress=ac_rcja@juntadeandalucia.es
        Validity
            Not Before: Mar 30 15:29:56 2005 GMT
            Not After : Mar 23 15:29:56 2035 GMT
        Subject: C=ES, O=Junta de Andalucia, OU=RCJA, CN=Autoridad de Certificacion Raiz de Telecomunicaciones/emailAddress=ac_rcja@juntadeandalucia.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:c4:0a:3a:57:e7:b6:0a:27:be:8d:dd:e0:b7:41:
                    87:e5:22:2a:51:fa:99:f6:cd:86:b1:16:22:bb:df:
                    2c:a2:a7:8a:22:bf:63:54:82:f7:db:2e:56:d4:9e:
                    ae:64:c9:ab:8d:16:bf:47:95:4f:b4:ea:5d:62:e5:
                    98:9f:ea:22:be:24:d5:20:e9:49:72:6e:92:81:73:
                    35:fa:46:9d:76:e1:bd:3d:1b:3a:a9:64:a5:96:3f:
                    23:a7:83:4b:00:d7:2c:05:41:0b:8d:a0:20:de:2b:
                    5b:d1:f1:e0:6c:82:70:bf:fc:90:8c:0e:ec:8f:79:
                    e3:0a:1b:a3:e2:11:04:36:86:6e:a9:d0:40:df:56:
                    e3:f2:af:1f:5a:5b:80:03:ba:f4:27:9b:c0:d3:f5:
                    94:be:49:1f:db:1d:19:16:b7:3f:db:d0:49:ba:00:
                    6b:e9:d1:dd:64:12:74:fb:77:d2:db:e8:16:e2:6b:
                    7d:0d:86:ae:43:25:06:77:cc:59:71:f5:3a:d2:82:
                    f4:5c:35:73:ae:71:d9:5f:22:51:a8:28:d3:2e:32:
                    7b:49:cb:af:0e:02:03:91:c2:71:bf:17:b1:42:5c:
                    83:e3:0b:3b:64:ef:84:65:3f:57:2b:2b:3b:20:71:
                    5d:e0:a2:c6:c2:1a:26:be:18:e2:ba:f8:d5:64:23:
                    1d:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                55:24:17:49:2E:D3:7B:28:36:7A:2A:B4:51:7D:3A:51:1D:52:B0:A9
            X509v3 Authority Key Identifier:
                keyid:55:24:17:49:2E:D3:7B:28:36:7A:2A:B4:51:7D:3A:51:1D:52:B0:A9
                DirName:/C=ES/O=Junta de Andalucia/OU=RCJA/CN=Autoridad de Certificacion Raiz de
Telecomunicaciones/emailAddress=ac_rcja@juntadeandalucia.es
                serial:00

            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Certificate Sign, CRL Sign
            X509v3 Subject Alternative Name:
                email:ac_rcja@juntadeandalucia.es
            X509v3 Issuer Alternative Name:
                email:ac_rcja@juntadeandalucia.es
            Netscape Cert Type:
                SSL CA, S/MIME CA, Object Signing CA
            Netscape Comment:
                Certificado de la CA Raiz de Red Corporativa de la Junta de Andalucia
            X509v3 CRL Distribution Points:
                URI:http://crl.rcja.intranet.juntadeandalucia.es

            Netscape CA Revocation Url:
                http://crl.rcja.intranet.juntadeandalucia.es
            Netscape Revocation Url:
                http://crl.rcja.intranet.juntadeandalucia.es
    Signature Algorithm: sha1WithRSAEncryption
        4e:d5:65:a1:7d:68:c4:69:59:db:97:aa:36:13:15:3d:c5:2f:
        e7:4d:fa:34:ce:d4:24:87:2b:28:b5:6e:80:dd:7b:c9:88:1b:
        c9:7b:0b:b0:94:3c:5e:ae:10:62:c1:a5:68:ab:a0:0f:1f:4d:
        12:3c:71:ac:e7:f2:e9:e2:3a:06:8a:24:ba:5b:7c:06:e2:bd:
        8a:2b:9d:db:ab:e9:5a:d5:3a:97:0e:79:0d:65:dc:b2:bb:d8:
        1a:54:b2:b0:f0:51:4e:f9:fb:9d:ac:04:b0:04:4d:0b:6a:98:
        7d:68:a8:22:df:0c:a5:ab:56:35:af:a5:eb:34:84:57:6b:08:
        fe:39:ff:e4:72:c6:6c:5a:3a:ee:ad:28:19:70:92:9b:72:21:
        70:d5:25:42:d9:84:a6:eb:61:ea:4d:f5:a7:b1:21:54:8c:1f:
        fc:40:1a:1a:4c:83:1c:24:b7:82:fb:59:4b:3e:82:f5:ce:87:
        03:14:27:57:97:45:6d:02:fa:35:cb:54:fe:63:f7:db:f8:09:
        f1:8d:72:67:3b:f7:bf:a8:29:b6:c7:6f:94:ef:ad:58:28:8a:
        6c:87:49:24:ec:fa:a8:e6:6d:d5:a2:a8:a7:1d:12:5e:c8:92:
        5b:96:ae:b3:b6:96:c7:c6:a1:d0:78:39:8e:69:2e:c0:a7:e6:
        d3:fc:19:9d
```

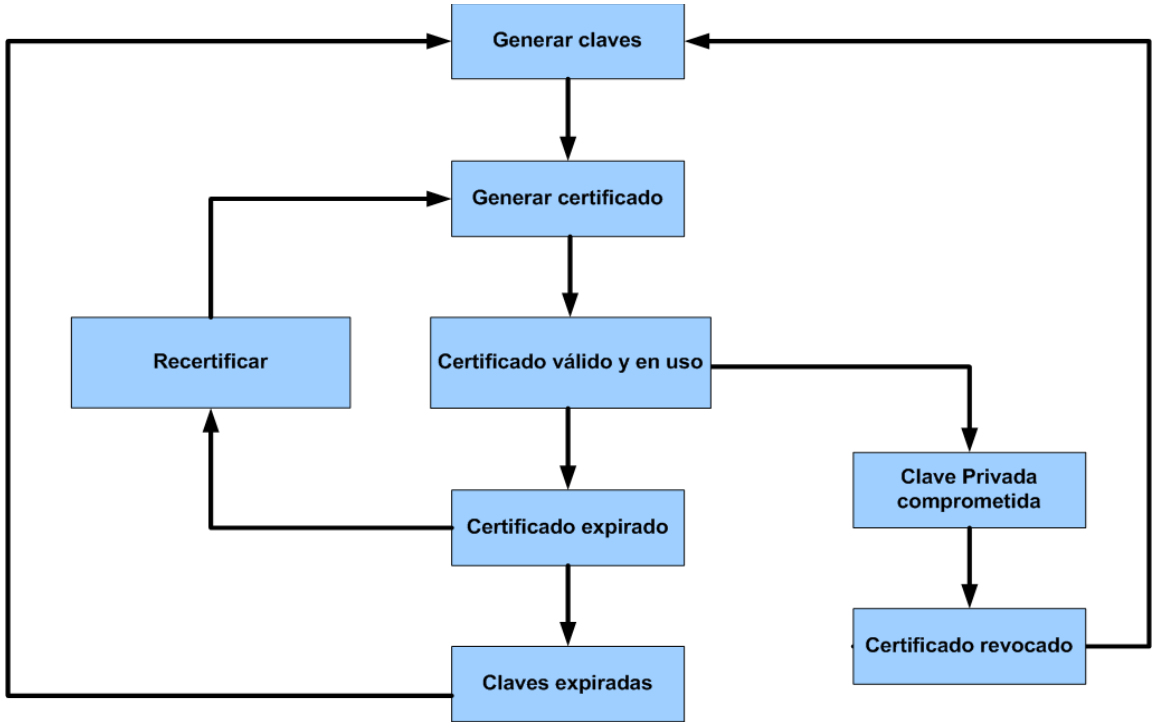
En el ejemplo anterior vemos que en el certificado de una CA raíz los campos emisor (issuer) y sujeto (subject) son la misma entidad. Esto es así porque las CA raíz usan certificados autofirmados por ellas mismas.

8.4 Ciclo de vida de un certificado

Los estados en los que puede permanecer un certificado digital son los siguientes:

- **Caducado**: cuando se ha superado el periodo de vigencia del certificado.
- **Revocado**: cuando se ha invalidado el certificado, ya sea por la CA que lo ha emitido o por el propio titular.
- **Suspendido**: cuando se invalida el certificado por un cierto periodo de tiempo. Se puede levantar la suspensión dentro del periodo de vigencia y pasarlo a estado válido.
- **Válido**: cuando es un certificado digital que no se encuentra en ninguno de los estado anteriores y puede usarse normalmente.

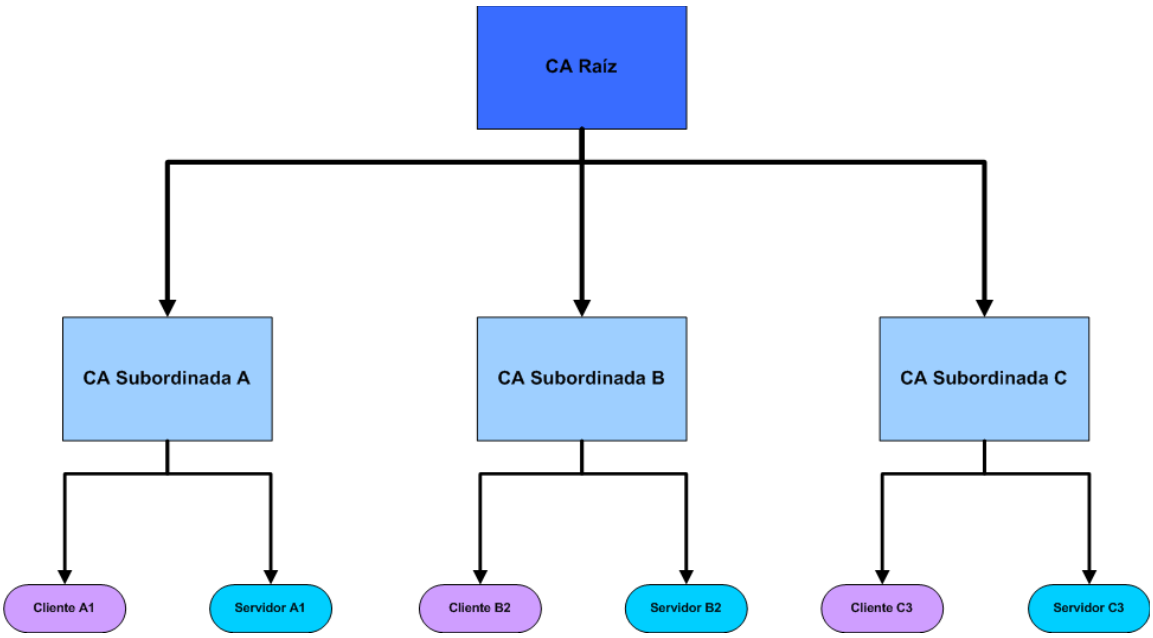
El diagrama siguiente muestra el ciclo de vida de los certificados digitales:



8.5 Jerarquía de la infraestructura de una PKI

El estándar X.509 se basa en un sistema jerárquico de autoridades de certificación para la emisión de certificados. Este sistema es diferente al usado en las claves PGP que usan un sistema en malla en el que no existen las autoridades de certificación raíz y cualquier nodo puede firmar claves públicas y avalar la validez de certificados de otros.

Cualquier persona o entidad puede generar un certificado digital, pero no se tendrá confianza en la vinculación entre los datos del sujeto y su clave pública si no está expedido por una Autoridad de Certificación reconocida. Para que sea aceptado por los navegadores es necesario que esté firmado por una CA reconocida. Si nos encontramos con un certificado de un usuario firmado por una CA que no conocemos, pudiera ser que este certificado esté firmado por otra que sí, u otra de nivel superior, y así sucesivamente. De esta manera se crea una jerarquía de autoridades de certificación en la que en el nivel más alto estarían las CA raíz con máxima autoridad que usarían certificados autofirmados, generados por ellas mismas, y éstas firmarían a otras CA. Las CA más bajas emiten los certificados de usuarios.



Para verificar la autenticidad de la clave pública de un usuario éste nos debe de enviar su certificado, más el certificado de la CA que lo ha emitido, más el certificado de la CA que ha emitido este último, así hasta llegar a la CA raíz que sería autofirmado. A esto se le llama **cadena de certificados**.

8.6 Riesgos de una PKI

Tomando como base el ensayo de Bruce Shneier y Carl Ellison, dos expertos de gran prestigio, se enumeran los riesgos más importantes de la Infraestructura de Clave Pública:

1. **¿En quién confiamos, y por qué?** Existen multitud de entidades de certificación pero, ¿quién te garantiza que los datos que certifican son correctos?. ¿Quién las ha situado en el contexto comercial en el que se encuentran?
2. **¿Quién tiene acceso a mi clave?** Hoy en día la clave privada no está segura. Normalmente se almacenan en ordenadores convencionales inseguros. Los sistemas operativos y navegadores adolecen de multitud de problemas de seguridad, además de existir virus y troyanos. Por tanto, no se puede garantizar que un documento firmado con una clave secreta constituya una firma confiable.
3. **¿Cómo de seguro es el ordenador verificador?** Como ocurre con el caso anterior, el ordenador que realiza la verificación del certificado puede haber sido manipulado.
4. **¿Cuál de los John Robinson es él?** Habitualmente los certificados se expiden a un nombre determinado,sin tener en cuenta que pueden existir diferentes personas con dicho nombre. En caso de disponer de información adicional, como su dirección de correo electrónico, tenemos que saber también si ésta es correcta o no, amén de vincular al usuario con datos que pueden quedar anticuados en un plazo breve.
5. **¿Es una CA una autoridad?** Por lo general, una entidad de certificación tradicional emite un certificado cubriendo datos sobre los que no tiene control. Por ejemplo, un certificado fusionando el nombre y la dirección de correo electrónico de un usuario no tiene en cuenta si el usuario se llama real y legalmente así, ni considera la posibilidad de que el email cambie o el ISP dé de baja la cuenta y la reasigne a otro usuario (o que todo el ISP desaparezca, por ejemplo).
6. **¿Es el usuario parte del diseño de la seguridad?** Son muy pocos los usuarios, por ejemplo, que verifican los certificados del servidor remoto cuando establecen una conexión SSL con su navegador.
7. **¿Autoridades de certificación o autoridades de certificación con autoridades de registro?** Se plantea que el modelo RA + CA puede ser menos seguro que un sistema con una CA en la autoridad de registro.
8. **¿Cómo identifica la autoridad de certificación al usuario?** Antes de emitir un certificado, la autoridad de certificación debe tener la certeza de que los datos que certifica son correctos.
9. **¿Son seguros los certificados?** El uso de certificados no garantiza la seguridad. Una cadena es tan fuerte como su eslabón más débil.
10. **¿Por qué existen entidades de certificación?** Existen otros métodos como el Single Sign-On que podrían ser más prácticos y seguros en algunas situaciones.

9 DOCUMENTACIÓN DE REFERENCIA

- Administrar una infraestructura de claves públicas de Windows Server 2003.
- Buenas prácticas para el uso de certificados (FNMT).
- Protocolos de gestión de certificados X.509.
- Políticas de certificado y el marco de prácticas de certificación.
- Certificados y perfiles de listas de revocación de certificados.
- Reglas genéricas de codificado de cadenas para tipos ASN.1.
- Ley 59/2003 de firma electrónica.
- Fábrica Nacional de Moneda y Timbre.
- Ten Risks of PKI: What You're Not Being Told About Public Key Infraestructure.