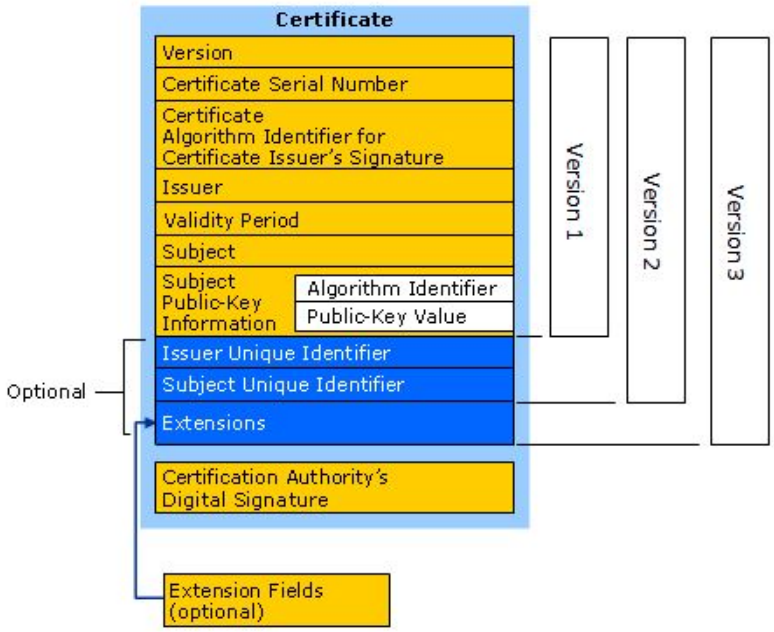
Las firmas digitales utilizan certificados basados en X.509

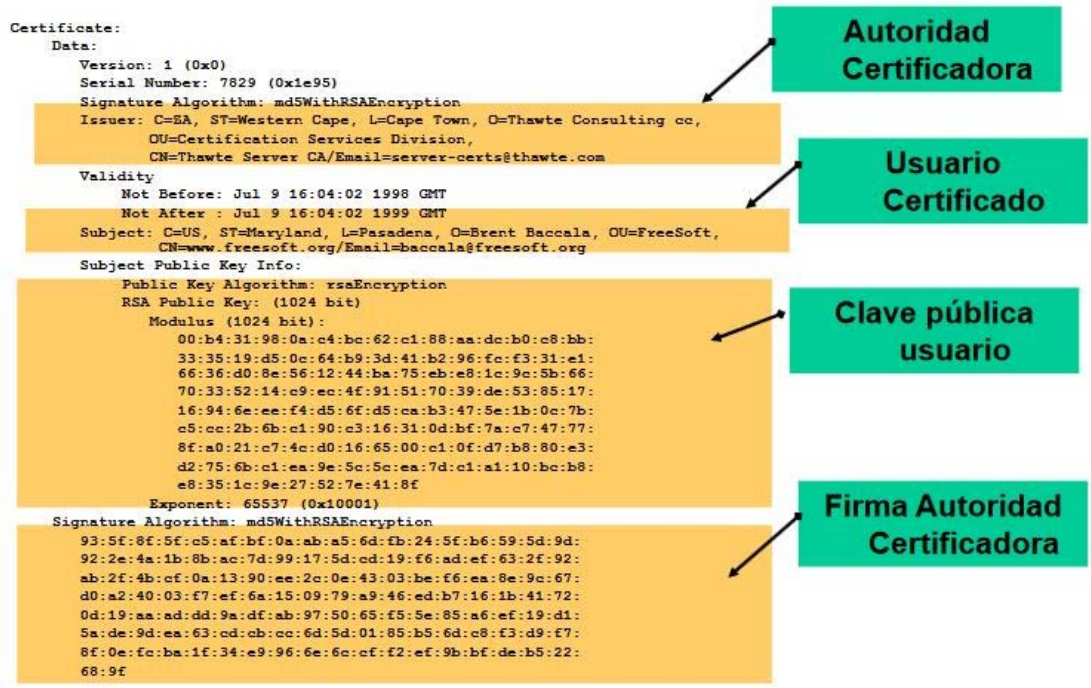
X.509 se trata de un estándar UIT-T aplicado en el marco del modelo PKI. Este estándar determina, entre otras cosas, un formato común para los certificados, las listas de revocación, atributos del certificado y algoritmos de validación de la ruta del certificado.

Los elementos del formato de un certificado X.509 son:

- **Versión**. El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
- **Número de serie del certificado**. Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
- **Identificador del algoritmo de firmado**. Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
- **Nombre del emisor**. Este campo identifica la CA que ha firmado y emitido el certificado.
- **Periodo de validez**. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
- **Nombre del sujeto**. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
- **Información de clave pública del sujeto**. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
- **Identificador único del emisor**. Este es un campo opcional que permite reutilizar nombres de emisor.
- **Identificador único del sujeto**. Este es un campo opcional que permite reutilizar nombres de sujeto.



Un ejemplo de un certificado X.509 es el que sigue:



PKI (Public Key Infraestructure) o Infraestructura de clave pública

PKI se define como el conjunto de herramientas, políticas, personas y recursos para permitir la puesta en marcha de un entorno de seguridad basado en sistemas criptográficos de clave pública, donde los usuarios pueden disponer de los servicios de autenticación, integridad y no repudio.

La PKI será la responsable de crear, distribuir, almacenar y revocar los certificados digitales necesarios. Para tal fin, dentro de los límites de PKI se establecen las llamadas CA (*Certificate authority, o Autoridades de Certificación*). Tanto el propietario del certificado (remitente) como el destinatario, que utilizará el certificado para verificar la validez de la clave pública del remitente, confían de forma implícita en la CA.

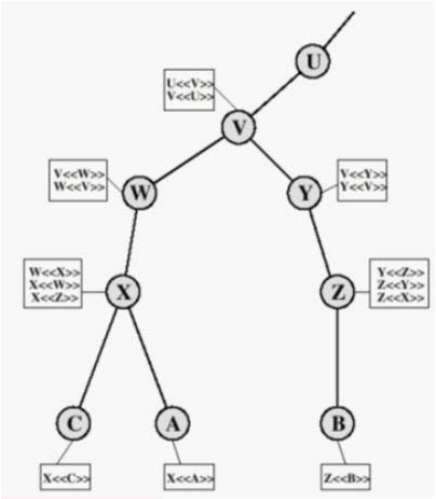
El flujo de comunicación se establece de la siguiente manera:

1. El remitente desea demostrar al destinatario que su identidad es real.
2. El remitente crea un certificado digital donde almacena la clave pública y los datos de identidad.
3. El remitente genera una solicitud de firma a una CA que contiene su certificado digital pendiente de confirmación.
4. La CA verifica la identidad del remitente y utilizando su clave privada firma el certificado digital del remitente.
5. A partir de este momento el remitente puede enviar el certificado al destinatario junto con las firmas creadas con la clave privada correspondiente.

El proceso de verificación de un certificado digital sigue estos pasos:

1. El destinatario recibe un mensaje firmado del remitente junto con el certificad digital de este firmado por la CA.
2. El destinatario contacta con la CA y solicita su clave pública para verificar la firma.
3. La CA envía al destinatario su clave pública en un certificado digital auto-firmado. Como el destinatario confía implícitamente en la CA es capaz de extraer la clave pública de la CA.
4. Utilizando la clave pública de la CA, el destinatario verifica la firma del certificado digital del remitente y es capaz de comprobar la integridad del mensaje.

El modelo PKI permite crear estructuras jerárquicas de CA, de tal forma que la Autoridad más importante se sitúa en la raíz del árbol. Esta entidad es auto-firma sus certificados ya que su validez es asumida por todos. Por debajo del nodo raíz se pueden definir tantas CA como se desee. La validez de estas autorizaciones no se asume y deben ser ratificadas por el nodo raíz. Esta ratificación se materializa cuando el nodo raíz firma los certificados emitidos por sus hijos inmediatos. En ese instante, estos nodos se convierten en distintos CA de pleno derecho, con la capacidad de ratificar otros nodos inferiores, y así sucesivamente.



Algunos de los CA más importantes en España son:

- Fábrica Nacional de Moneda y Timbre
- Ministro de Industria, Energía y Turismo
- Agencia Catalana de Certificación

A nivel mundial:

- Verisign
- Entrust
- GeoTrust
- Thawte