PKI

PKI o Infraestructura de Clave Pública es una combinación de elementos que permiten cifrar, firmar y conseguir el no repudio de comunicaciones electrónicas

1.

ELEMENTOS FUNCIONALES

ELEMENTOS FUNCIONALES DE UNA PKI

- **Básicos**
  - Autoridad de certificación (CA)
  - Autoridad de registro (RA)
  - Almacén de certificados y claves

- **Opcionales**
  - Autoridad de sellado de tiempo (TSA)
  - Servidor de revocación

AUTORIDAD DE CERTIFICACIÓN (CA)

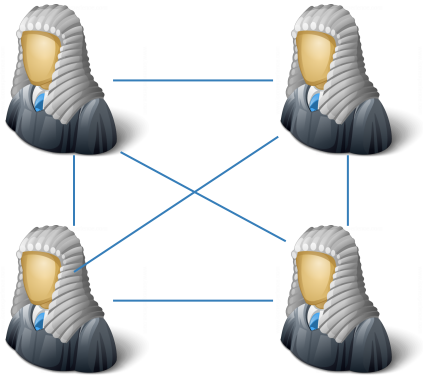
- **Tercero en quien se confía para:**
  - Firmar y publicar certificados
  - Revocar certificados y publicar la revocación
  - Recoge funciones de gestión y fechado

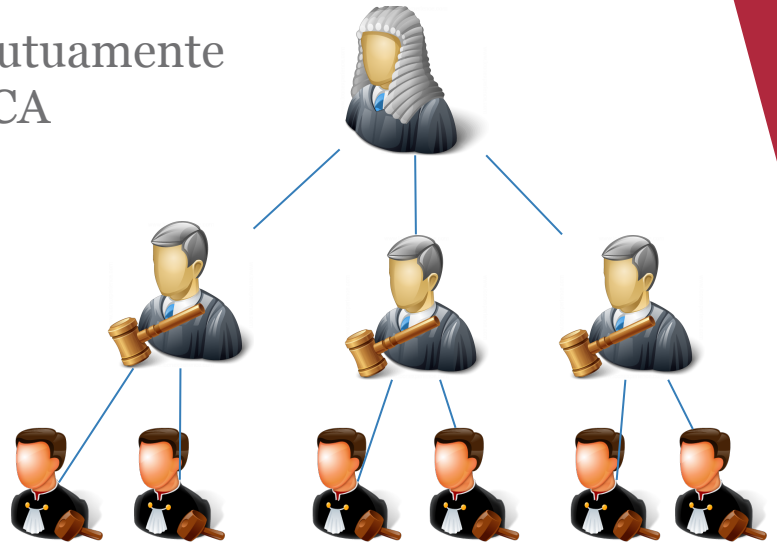
- **Pueden ser públicas, privadas o individuales**
  - Ejemplos: FNMT, GeoTrust, Camerfirma, Verisign

- **Firma los certificados su clave privada**
  - Para confiar en su pública se certifica a si misma o la certifica otra CA. Su clave pública viene preinstalada en el S.O o navegador en algunos casos o será necesario descargarla e instalarla manualmente.

ORGANIZACIÓN DE UNA CA

- **CA única**
  - Fácil de mantener pero punto vulnerable
- **Jerarquía de CA**
  - Árbol de confianza, cada CA certifica al nivel inferior
  - La CA raíz se certifica a si misma
- **Malla de CA**
  - Las CA se certifican mutuamente
  - El sujeto confía en su CA





AUTORIDAD DE REGISTRO (RA)

- **Autoridad delegada para algunas funciones:**
  - Recibir solicitudes de certificados
  - Generar las claves
  - Verificar la identidad del solicitante
  - Entregar el certificado al solicitante

ALMACÉN DE CERTIFICADOS Y CLAVES

- **Los certificados son públicos:**
  - Deben esta siempre disponibles y guardarse en histórico
- **Debe poderse comprobar que no están revocados**
- **Las claves privadas sí deben estar protegidas**
  - Si se comprometen se revocará el certificado

AUTORIDAD DE SELLADO DE TIEMPO

- **La TSA proporciona sellos de tiempo:**
  - Necesita que se registre el fechado
  - Documento que asocia la huella digital de un documento a una fecha y hora concreta
  - Permite el no repudio

SERVIDOR DE REVOCACIÓN

- **Lugar donde se almacena la CRL (Lista de Revocación de Certificados)**
  - Lista de números de serie que han sido revocados, ya no son válidos y en los que no debe confiar ningún usuario del sistema

2.

PROCEDIMIENTOS

PROCEDIMIENTOS

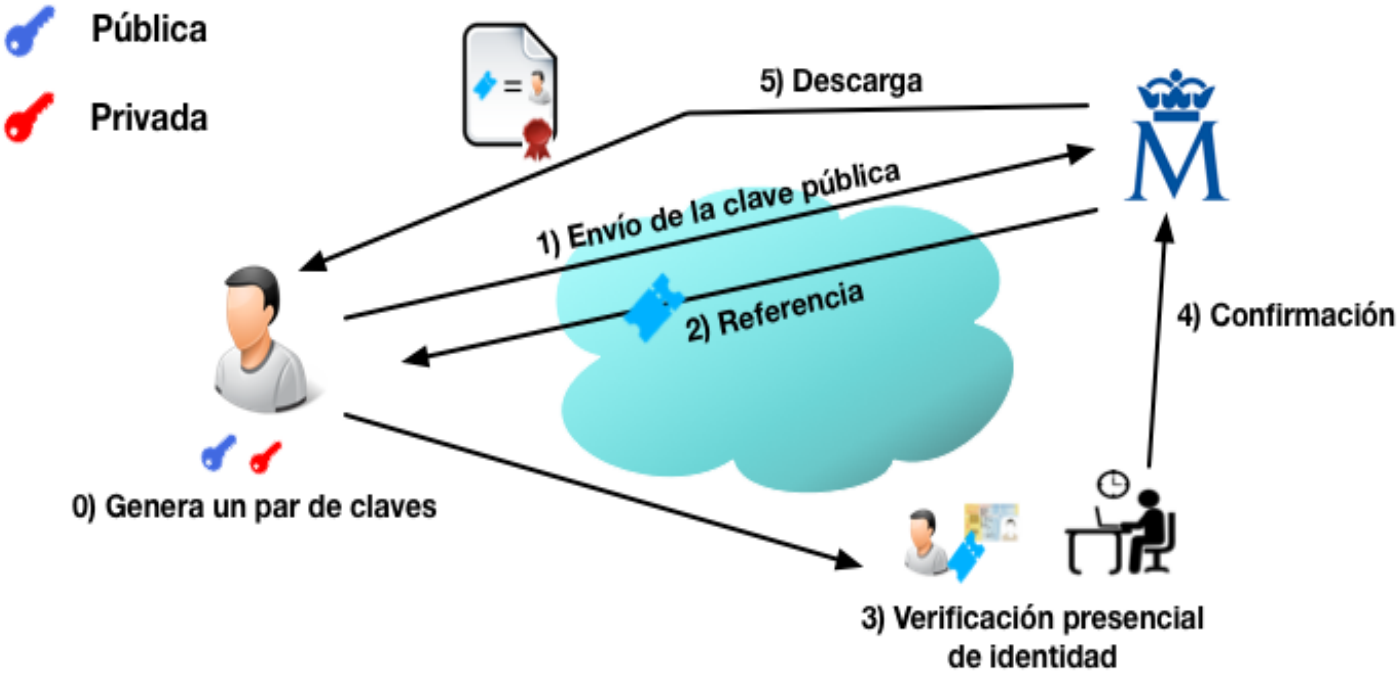
- **Básicos**
  - Emisión de certificado
  - Almacenamiento y uso de certificado
  - Renovación o expiración de certificado
  - Revocación de certificado

- **Opcionales**
  - Sellado de tiempo

EMISIÓN DEL CERTIFICADO

- **Pasos:**
  - *Solicitud en la RA*
  - *Generación del par de claves*, requiere un **muy buen** generador de números aleatorios.
  - *Verificación de identidad*, puede ser presencial o no presencial.
  - *Creación y entrega* del certificado, tarea exclusiva de la CA y la entrega depende del procedimiento de generación de clave y el nivel de seguridad del certificado.
  - *Publicación y respaldo* del certificado. Publicado por parte de la CA o del solicitante en almacenes públicos o diseminación con cada uso y copia de respaldo en el almacén.

EMISIÓN DEL CERTIFICADO FNMT CA2



ALMACENAMIENTO Y USO

- **Almacenamiento:**
  - Sólo la clave privada precisa protección
- **Uso: validación del certificado**
  - Debe estar vigente en plazo de validez sin estar revocado
  - La CA es de confianza para quien lo verifica
  - Las firmas son validas
  - Su uso consistente con su política

EXPIRACIÓN, RENOVACIÓN

- **Expiración:** se agota el plazo de validez, no requiere acción
- **Actualización:** Sólo de plazo de validez
- **Renovación:** También de claves

REVOCACIÓN

- **Solicitud a CA/RA:**
  - No es instantánea y tampoco se destruye

¿Clave privada comprometida? ¿Cambio del estado del sujeto?

- Se hace a través de una **Lista de Certificados Revocados (CRL)** o mediante **protocolos de comprobación (OCSP)** de vigencia o revocación.
  - *CRL completa*: solución lenta e inescalable.
  - *CRL incremental*: más escalable con respecto a la anterior.
  - *CRL combinada*: Mezcla CRL de varias CA.
  - *ARL*: CRL para las CA.