La Firma Electrónica: Conceptos Generales

QUÉ ES UNA PKI

PKI (Infraestructura de Clave Pública)

Una PKI (Public Key Infraestructure – Infraestructura de Clave Pública) es un conjunto de elementos hardware, software, personas, políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados basados en criptografía de clave pública.

Componentes PKI

1. Proveedores de servicios de certificación:
   - Autoridad de Certificación
   - Autoridad de Registro
2. Directorio de Certificados
3. Protocolos de certificación
4. Documentación de una PKI
   - Las “políticas” establecen requisitos que deben cumplir los certificados, las firmas electrónicas, los sellos de tiempo, etc
   - Las “declaraciones de prácticas” explican cómo se cumplen los requisitos establecidos en las políticas, de forma divulgativa
   - Los “documentos auxiliares” detallan los procedimientos concretos (confidenciales)
   - Los “instrumentos jurídicos”, como contratos, regulan las relaciones entre participantes

Procedimientos PKI

1. Solicitud de certificados:
   - Generación del par de claves
   - Protección de la clave privada
   - Envío de la solicitud de certificados
   - Validación de la solicitud
     - Aprobación
     - Rechazo
2. Aceptación de certificados
   - Manifestaciones del suscriptor en virtud de la aceptación
   - Deber del suscriptor de evitar la divulgación de la clave privada
3. Revocación de certificados
   - Causas generales de revocación
   - Revocación a instancia del emisor
   - Revocación a instancia del suscriptor
   - Revocación por error en la emisión
   - Aviso y confirmación de revocación
   - Efectos de la revocación

Autoridad de Certificación (CA)

- Tercera parte de confianza que acredita la conexión entre una determinada clave pública y su propietario
- La confianza en la autoridad de certificación supone la confianza en los certificados que emite.
- En ella confían uno más usuarios para la creación y firma de certificados.
- La AC firma digitalmente con su clave privada la información del certificado.
- La AC emite periódicamente listas de certificados revocados (CRLs).
- Un certificado puede ser revocado porque la información en el mismo ya no es válida, porque la clave privada asociada al mismo se ha perdido, o simplemente ha caducado su período de validez.

Autoridad de Certificación. Servicios prestados

1. Gestión del ciclo de vida de las claves
   - Generación
   - Custodia y desvelado
   - Recuperación
   - Renovación
2. Gestión del ciclo de vida de los certificados
   - Generación
   - Renovación
   - Revocación de certificados
   - Servicios de certificación cruzada
3. Publicación
   - Certificados
   - Políticas de certificación

Autoridad de Registro (RA)

- Entidad autorizada por al AC para registrar a los usuarios de la infraestructura asignándoles un identificador único de usuario.

- Funciones básicas
  - Identificar al usuario: Verificación de datos de registro (peticiones de certificado, revocación, suspensión y cambios)
    - Generar las claves
    - Gestionar de la petición y entrega: Verificación de la asociación de certificados y claves con su propietario (peticiones de certificado, revocación, suspensión y cambios)

Suscriptores

- Obligaciones habituales del suscriptor (DPCs y contratos de certificación)
  - Asunción de manifestaciones certificadas
  - Protección de la clave privada
  - Notificación del compromiso de la clave privada
  - Notificación de la aceptación y posesión del certificado
  - Vinculación a las firmas electrónicas verificadas mediante el certificado

PKI- Infraestructura de clave Pública

Certificado Raíz

Autoridad de Registro - AR

Certificación

Autoridad de Certificación AC

Registro

Emisión de Certificados

Publicación

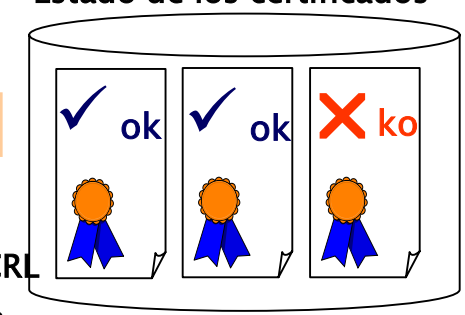
Estado de los certificados

Suscriptores

TERCEROS

Consulta

- Certificados
- Revocados - CRL
- Estado - OCSP



REPOSITORIO DE CERTIFICADOS