Criptografía y Firma Digital.

Modulo 2.
Usos De La Criptografía

Laboratorio de Seguridad de la Información

Mediante el Cifrado de datos, el Hash o resumen de datos y las Firmas Digitales, la criptografía participa directamente en ofrecer los siguientes servicios de seguridad:

- Autenticación de usuario o autenticación de mensaje ¿son el emisor o el destinatario quiénes dicen realmente ser? ¿proviene el mensaje de quién dice provenir?
- Confidencialidad de un mensaje ¿habrá podido alguien, no autorizado, leer o acceder el mensaje o información?
- Integridad de un mensaje ¿ha recibido el remitente realmente la información que le envió su emisor o habrá sido modificada?
- No repudio de un mensaje ¿podrá el remitente negar que ha enviado algo (o el destinatario que lo ha recibido)?

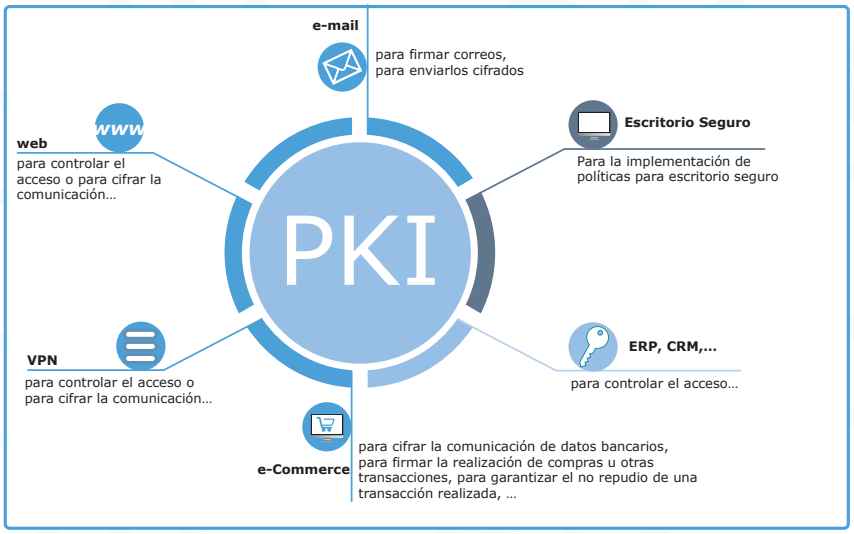
Los llamados Terceros de Confianza o Proveedores de Servicios de Confianza, a través del uso de Autoridades de Certificación (PKIs) y Certificados Electrónicos completan el marco para desarrollar múltiples tipos de usos de seguridad y criptografía.

Los Certificados Electrónicos:

- Son un documento, en formato electrónico.
- Asocia una identidad (de una persona física, de una persona jurídica, de una entidad, de un sistema, etc.) a una clave pública.
- Una Autoridad de Certificación respalda esta asociación de datos adjuntando su firma electrónica.
- Limita para qué usos es válido (no todos los certificados se pueden utilizar para cualquier cosa).
- Tiene caducidad. Después habrá que renovarlo.

Las Autoridades de Certificación:

- Son entidades/organizaciones independientes.
- En quienes depositamos la confianza sobre los certificados que emiten:
  - o la identidad que se muestra en el certificado es auténtica y ellos se encargaron de verificarlo.
  - o El usuario posee la clave pública y privada.
- El Ministerio de Industria, Energía y Turismo regula qué Autoridades de Certificación están homologadas para emitir los llamados Certificados Reconocidos. El resto emiten Certificados No Reconocidos.
- El uso de Certificados emitidos por Autoridades de Certificación Reconocidas suele estar orientado a su uso en procesos de autenticación y de firma electrónica con carácter público o de reconocimiento general.
- El uso de Certificados emitidos por Autoridades de Certificación No reconocidas, suele estar orientado a usos privados o internos de Organizaciones y compañías que no necesitan un reconocimiento general de los usuarios.



La criptografía, junto con los certificados electrónicos y el papel de las Autoridades de Certificación, son utilizados en múltiples soluciones, herramientas y servicios que se ofrecen hacia todo tipo de usuarios y ciudadanos así como hacia organizaciones, empresas y administraciones.

XUNTA DE GALICIA
CONSELLERÍA DE SANIDADE
SERVIZO GALEGO de SAÚDE
MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa