Criptografía e Firma Dixital.

Modulo 2.
Usos Da Criptografía

Laboratorio de Seguridade da Información

Mediante o Cifrado de datos, o Hash o resumo de datos e as Firmas Dixitais, a criptografía participa directamente en ofrecer os seguintes servizos de seguridade:

- Autenticación de usuario ou autenticación de mensaxe ¿son o emisor ou o destinatario os que din realmente ser? ¿provén o mensaxe de quen di provir?
- Confidencialidade dunha mensaxe ¿puido alguén, non autorizado, ler ou acceder á mensaxe ou información?
- Integridade dunha mensaxe ¿recibiu o remitente realmente a información que lle enviou o seu emisor ou sería modificada?
- Non repudio dun mensaxe ¿poderá o remitente negar que enviou algo (ou o destinatario que o recibiu)?

Os clamados **Terceiros de Confianza** ou **Provedores de Servizos de Confianza**, a través do uso de Autoridades de Certificación (PKIs) e Certificados Electrónicos completan o marco para desenvolver múltiples tipos de usos de seguridade e criptografía.

Os Certificados Electrónicos:

- Son un documento, en formato electrónico.
- Asocia unha identidade (dunha persoa física, dunha persoa xurídica, dunha entidade, dun sistema, etc.) a unha clave pública.
- Unha Autoridade de Certificación avala esta asociación de datos xunto coa súa firma electrónica.
- Limita para que usos é válido (non todos os certificados se poden empregar para calquera cousa).
- Teñen caducidade. Despois haberá que renovalo.

As Autoridades de Certificación:

- Son entidades/organizacións independentes.
- Nos que depositamos a confianza sobre os certificados que emiten:
  - o a identidade que se mostra no certificado é auténtica e que eles se encargaron de verificalo.
  - o O usuario posúe a clave pública e a privada.
- O Ministerio de Industria, Enerxía e Turismo regula que Autoridades de Certificación están homologadas para emitir os chamados Certificados Recoñecidos. O resto emiten Certificados Non Recoñecidos.
- O uso de Certificados emitidos por Autoridades de Certificación Recoñecidas adoita estar orientado ó seu uso en procesos de autenticación e de firma electrónica con carácter público ou de recoñecemento xeral.
- O uso de Certificados emitidos por Autoridades de Certificación Non recoñecidas, adoita estar orientado a usos privados ou internos de Organizacións e compañías que non necesitan un recoñecemento xeral dos usuarios.

A criptografía, xunto cos certificados electrónicos e o papel das Autoridades de Certificación, son empregados en múltiples solucións, ferramentas e servizos que se ofrecen cara a todo tipo de usuarios e cidadáns así como cara organizacións, empresas e administración.

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