Certificado digital

MOTIVAÇÃO

* assinatura digital com criptografia assimétrica nos dá a certeza que alguém, com acesso à chave privada assinou a mensagem. Contudo, não é possível afirmar que a assinatura foi feita p/ uma pessoa específica.

CERTIFICADO DIGITAL

→ associa dados de uma entidade a uma chave pública.
→ confiança no emissor do certificado.
→ possuem validade e podem ser revogados

AUTORIDADE CERTIFICADORA

→ terceira parte confiável
  ↳ CONFIANÇA COM BASE EM:
  I - reputação da AC
  II - políticas de emissão de certificados
  III - procedimentos de validação da identidade do solicitante
→ navegadores e SOs tem uma lista de ACs confiáveis.
  ↳ Let's Encrypt (ex)
→ tipos: X509

CERTIFICADOS AUTOASSINADOS

→ útimo para desenvolvimento
→ emitido e assinado pelo mesmo entidade
→ SOs e navegadores não confiam

INFRAESTRUTURA DE CHAVES PÚBLICAS (ICP)

↳ conjunto de entidades, procedimentos e tecnologias que viabilizam e gerenciam certificados digitais

→ HIERARQUIA: * autoridades certificadoras (AC) → emitir certificados
* " de registro (AR) → verificar identidade do solicitante do certificado
* " de carimbo de tempo (ACT) → atesta data e hora da assinatura
* lista de certificados revogados (CRL) → verifica se um certificado foi revogado

→ ICP PÚBLICA x ICP PRIVADA

↓ controlada por entidade pública ou privada
ex) Let's Encrypt e ICP Brasil

↳ controlada pela própria organização
↳ p/ dispositivos IOT e rede corporativa