

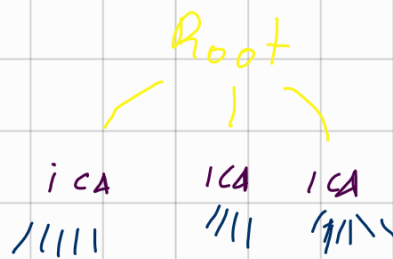
Entidad Certificadora (CA - Certificate Authority)

- GeoTrust - Let's Encrypt = Symantec

Tipos

Autoridad de Certificación Raíz: Es la entidad certificadora de nivel superior en una PKI. Emite y firma certificados para otras entidades certificadoras, creando una cadena de confianza.

Autoridad de Certificación Subordinada (intermediante CA): Emite certificados para usuarios finales, dispositivos y otros servicios dentro de una PKI.



Funciones

Emisión de certificados: Verifica la identidad y autenticidad de una entidad solicitante y emite un certificado digital que la identifica.

Firma de certificados: La CA utiliza su clave privada para firmar digitalmente los certificados emitidos.

Revocación de certificados: Si se detecta algún problema de seguridad o compromete la clave privada de una entidad certificada, la CA puede revocar el certificado.