



Infraestructura de Clave Pública (PKI)

Implementación y Estándares



Universidad Central del Ecuador

Grupo: #1

Docente: Ing. Giovanny Moncayo



¿Qué es una Infraestructura de Clave Pública (PKI)?

Marco de Trabajo Integral

La PKI es un conjunto robusto de roles, políticas, hardware, software y procedimientos que establecen un ecosistema de confianza para la comunicación segura en redes.

Pilares de la Seguridad

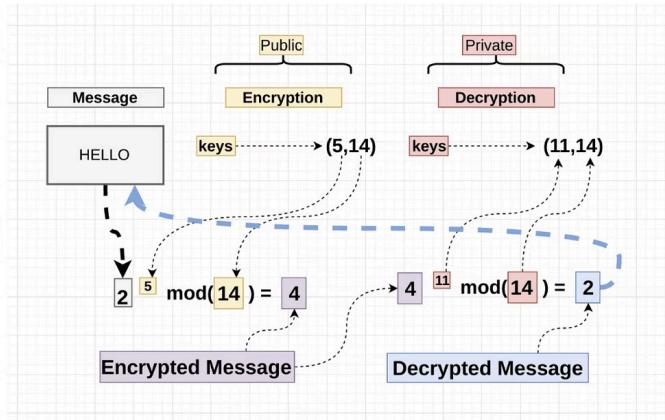
Su propósito fundamental es garantizar la autenticidad, integridad, confidencialidad y el no repudio de la información mediante el uso estratégico de pares de claves criptográficas.

Componentes Clave

- Autoridades de Certificación (CA)
- Autoridades de Registro (RA)
- Certificados Digitales X.509
- Almacenes de Certificados y Listas de Revocación

Tecnología y Algoritmos Fundamentales en PKI

La robustez de una PKI se cimenta en la elección y correcta implementación de algoritmos criptográficos probados.



Cifrado Asimétrico: RSA

El algoritmo RSA (Rivest-Shamir-Adleman) de 2048 bits es crucial para la generación de pares de claves y la creación/verificación de firmas digitales, basándose en la complejidad de la factorización de números grandes.



Función de Hashing: SHA-256

SHA-256 (Secure Hash Algorithm) produce un resumen único (digest) del mensaje o certificado, esencial para verificar la integridad de los datos, asegurando que no han sido alterados.

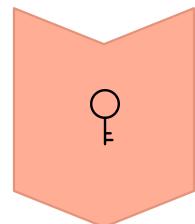


Estándar de Certificación: X.509 v3

El estándar internacional X.509 Versión 3 define la estructura de los certificados de clave pública, vinculando una identidad digital a una clave pública mediante la firma de una CA, y es la base para el protocolo TLS.

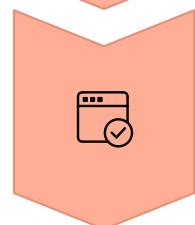
Flujo de Funcionamiento de una PKI

El proceso de una PKI es una secuencia lógica que garantiza la confianza y seguridad en las transacciones digitales.



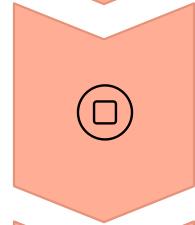
1. Generación de Claves

El usuario genera un par de claves (pública y privada) de forma segura.



2. Solicitud a la CA

Se envía una Solicitud de Firma de Certificado (CSR) a la Autoridad de Certificación (CA).



3. Emisión de Certificado

La CA verifica la identidad y firma digitalmente el certificado X.509 del usuario.



4. Firma Digital

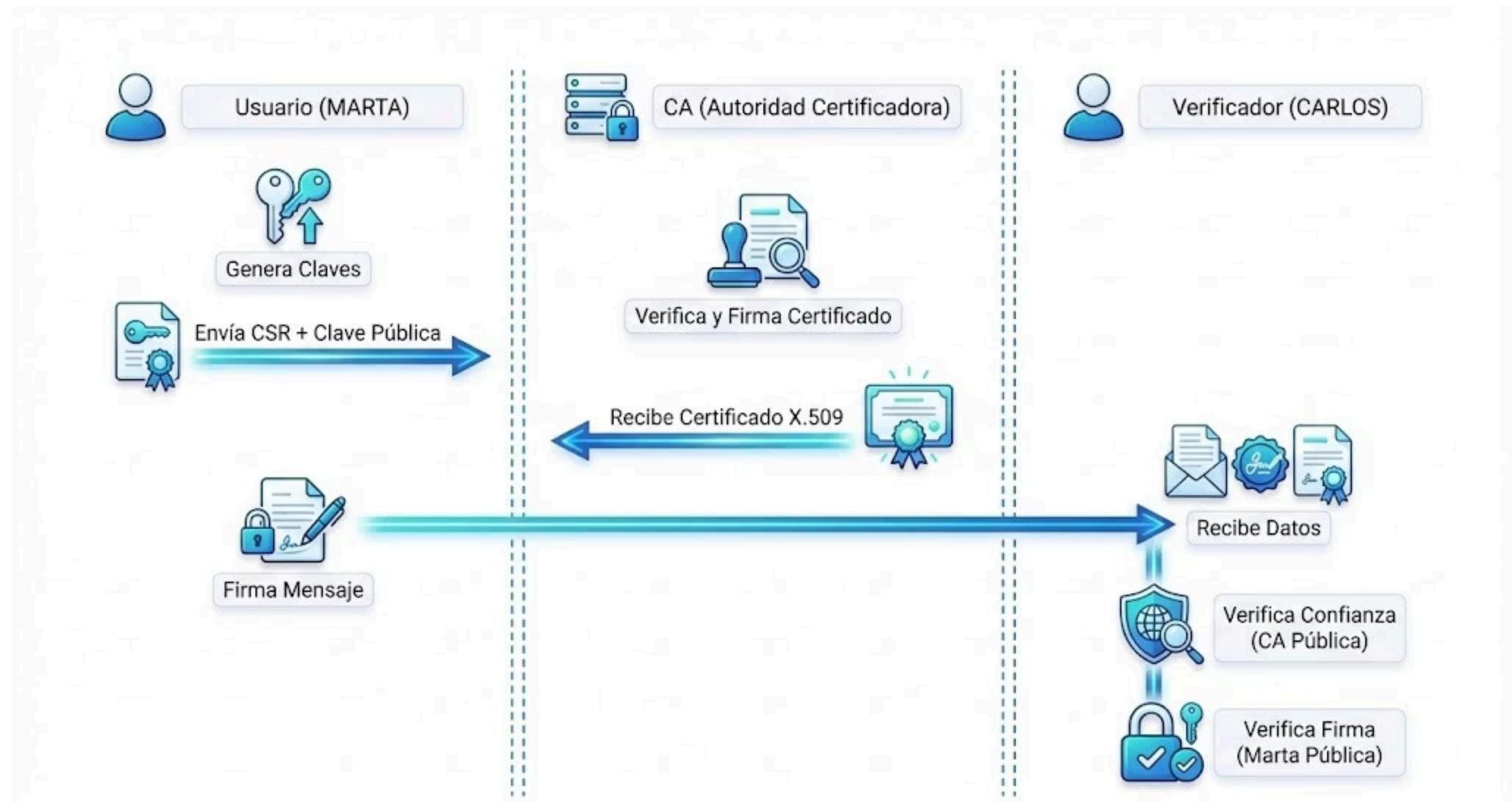
El usuario firma digitalmente mensajes o documentos utilizando su clave privada.



5. Verificación

Un tercero verifica la firma digital y la validez del certificado usando la clave pública y la de la CA.

Diseño esquemático de su funcionamiento:



Escenarios de Uso Frecuente de PKI en la Actualidad

La PKI es la columna vertebral de la seguridad digital en innumerables aplicaciones diarias.

Navegación Segura (HTTPS)

Protege las comunicaciones web, cifrando el tráfico entre navegadores y servidores, esencial para la protección de datos sensibles como información bancaria y credenciales.



Facturación Electrónica (SRI)

En Ecuador, el Servicio de Rentas Internas (SRI) utiliza firmas digitales basadas en PKI para garantizar la autenticidad e integridad de las facturas electrónicas, proporcionando validez legal.



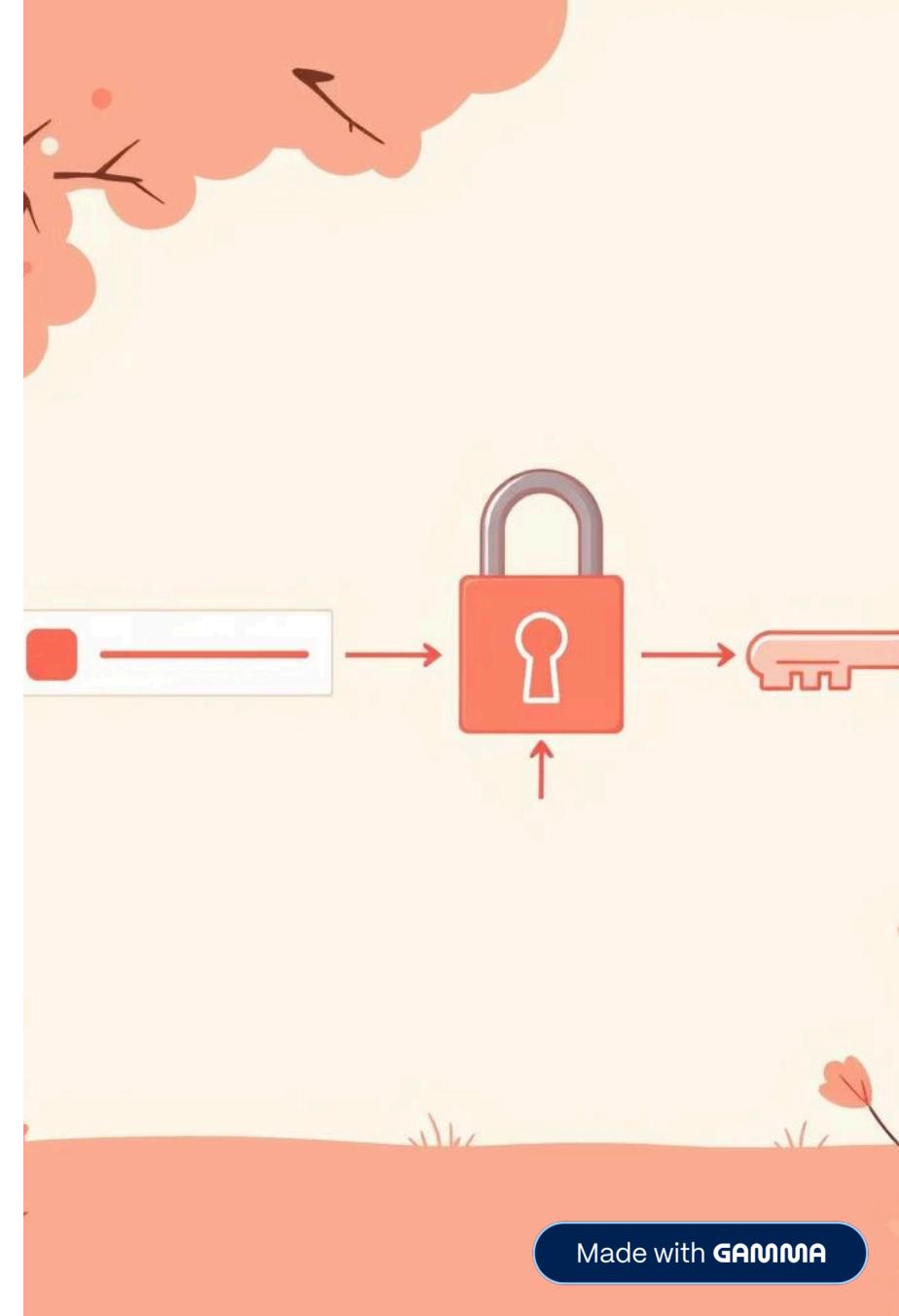
Identidad Digital (Cédula Electrónica)

La cédula electrónica incorpora certificados digitales que permiten la autenticación segura en plataformas en línea y la firma de documentos con pleno valor legal, fortaleciendo la identidad digital ciudadana.



Pregunta de Control 1: Verdadero / Falso

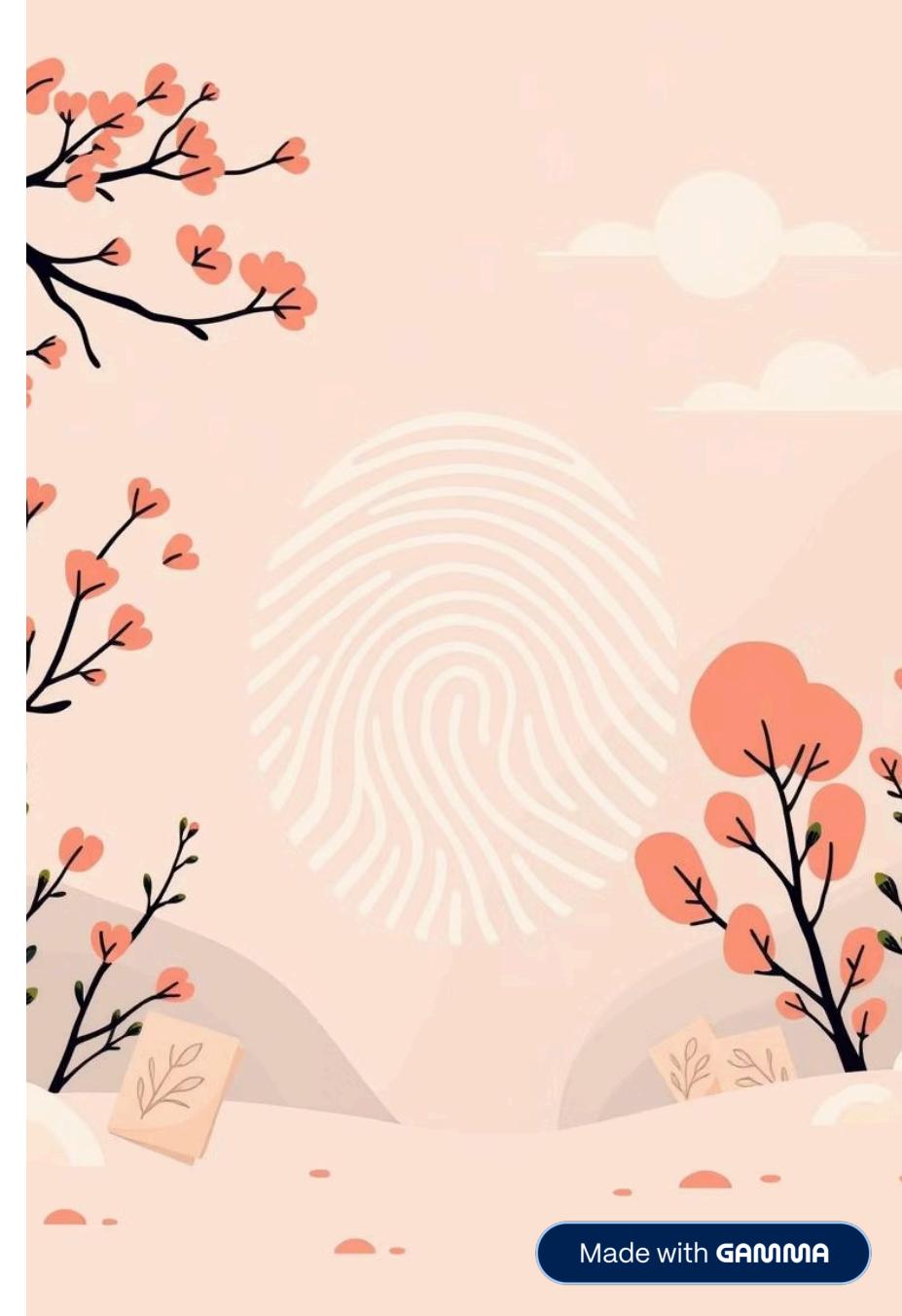
¿La PKI es un conjunto robusto de roles, políticas, hardware, software y procedimientos que establecen un ecosistema de confianza para la comunicación segura en redes?



Pregunta de Control 2: Opción múltiple (1 respuesta)

¿Qué algoritmo de función de hash en PKI es esencial para asegurar que los datos no han sido alterados (integridad)?

- A) RSA de 1024 bits
- B) AES-256
- C) SHA-256
- D) TLS 1.3



Pregunta de Control 3: Opción múltiple (N respuestas)

Selecciona los elementos que intervienen en un proceso típico de validación dentro de una PKI.

- a) Certificado digital del usuario
- b) Clave privada del verificador
- c) Autoridad Certificadora (CA)
- d) Lista de Revocación (CRL)
- e) Algoritmo AES





Pregunta de Control 4: Emparejamiento

Relaciona cada concepto con su definición correspondiente:

Concepto	Definición
1. CA	A. Entidad confiable que emite, valida y revoca certificados digitales dentro de una PKI.
2. Identidad Digital	B. Representación electrónica de un usuario, servidor o entidad asociada a una clave pública en un certificado.
3. RSA	C. Algoritmo de criptografía asimétrica utilizado comúnmente para intercambio de claves y firmas digitales en PKI.
4. HTTPS	D. Protocolo seguro que utiliza TLS y certificados digitales para proteger la comunicación entre cliente y servidor.



Pregunta de Control 5: Completar con una palabra

El estándar utilizado para definir la estructura de los certificados digitales en una PKI se denomina _____.

Referencias Bibliográficas

Public Key Infrastructure: A Survey

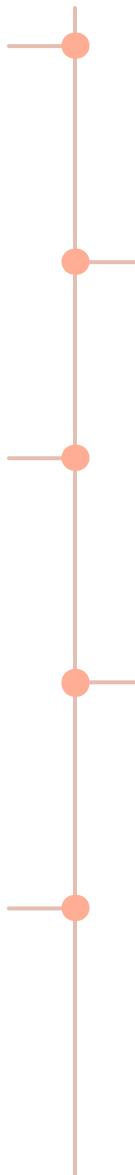
[1] A. Albarqi, E. Alzaid, F. Al-Ghamdi, S. Asiri, y J. Kar, "Public Key Infrastructure: A Survey," Journal of Information Security, vol. 6, no. 1, pp. 31–37, 2015. DOI: 10.4236/jis.2015.61004.

X.509 Certificate Frameworks

[3] ITU-T Recommendation X.509, "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks," Oct. 2019. URL: <https://handle.itu.int/11.1002/1000/14033>

Digital Signature Algorithms

[5] W. Stallings, "Digital signature algorithms," Cryptologia, vol. 37, no. 4, pp. 311–327, 2013. DOI: 10.1080/01611194.2013.797044.



Cryptographic Algorithms and Key Sizes

[2] H. Ferraiolo y A. Regenscheid, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification," NIST Special Publication 800-78-5, Jul. 2024. DOI: 10.6028/NIST.SP.800-78-5.

Analysis of Web-based PKI Failures

[4] H. Hadan, N. Serrano, y L. J. Camp, "A holistic analysis of web-based public key infrastructure failures," Journal of Cybersecurity, vol. 7, no. 1, 2021. DOI: 10.1093/cybsec/tyab025.