Identidad Criptográfica: Comunicaciones Cifradas con PGP

Estantería: DevSecOps e Infraestructura

Subtema: Gobernanza

mercedev.es — 2026-05-21 | Epic 3 - Fase 3

El Desafío (Síntoma)

Exponer un formulario de contacto tradicional (PHP, Node) en una web estática rompe el paradigma de *Zero-Bloat* y *0 dependencias bloqueantes*. Los formularios requieren backend, validación de spam (reCAPTCHA) y bases de datos, abriendo la puerta a inyecciones SQL o Cross-Site Scripting (XSS). Además, los correos enviados en texto plano pueden ser interceptados por cualquier nodo intermedio. La necesidad era clara: permitir que clientes y auditores enviaran información confidencial sin vulnerar la integridad de la arquitectura estática.

La Maniobra (Lógica)

Se implementó un modelo de comunicación asimétrica utilizando el estándar PGP (Pretty Good Privacy) mediante la herramienta nativa GnuPG.

1. **Generación de Claves:** Se generó un par de claves criptográficas locales utilizando un algoritmo robusto (RSA de 4096 bits o curva elíptica Ed25519) protegiendo la clave privada con una frase de paso (Passphrase) fuerte.
2. **Exposición Estática:** En lugar de desplegar una API REST para procesar mensajes, se exportó la clave pública (`gpg --armor --export`) a un archivo ASCII de texto plano (`llave-publica.asc`). Este archivo se depositó en el directorio `/public/` para ser servido directamente desde el servidor web como un activo estático más.
3. **Identidad Visual:** En la página de contacto (`/contacto/index.html`), se publicó el enlace directo al archivo `.asc` junto con la Huella Digital (*Fingerprint*) criptográfica. Esto permite a los emisores verificar matemáticamente la autenticidad de la clave antes de cifrar su mensaje mediante su propio cliente de correo.

El Aprendizaje / Deuda Técnica

- **Seguridad por Diseño (Privacy by Design):** Servir un archivo de texto plano de apenas 3 KB con la clave pública es infinitamente más seguro, barato y rápido que mantener una API de correo electrónico. Delegar el cifrado (E2EE - End-to-End Encryption) al cliente empodera al usuario y garantiza que la infraestructura del servidor web jamás conozca el contenido del mensaje.
- **Autoridad Técnica:** Exponer una clave PGP no es solo una medida de seguridad; es una declaración de principios. Comunica a otros ingenieros que el proyecto comprende y aplica la seguridad en profundidad (Defense in Depth).

Resumiendo (Lenguaje no técnico)

En lugar de usar un formulario de contacto que puede ser atacado por piratas informáticos o llenarse de correo basura, hemos optado por algo mucho más seguro: ofrecer una "caja fuerte" pública. Cualquiera puede descargarse nuestra "llave pública" para cifrar un mensaje desde su propio ordenador. Ese mensaje viaja por internet como un código indescifrable que nadie puede leer, y solo nosotros podemos abrirlo al recibirlo. Garantizamos privacidad absoluta sin usar programas pesados.