Documento Técnico
Arquitectura de Seguridad y Cifrado Adoxor

Fecha: Abril 2026
Confidencialidad: Público
Tecnología: Spring Boot, AES-GCM-256, Google Cloud KMS

---

1. Introducción al Cifrado en Adoxor

En Adoxor, la seguridad y privacidad de los datos no es una capa posterior añadida a la aplicación, sino la arquitectura fundamental. Nuestro sistema implementa un flujo criptográfico asimétrico conocido como Envelope Encryption (Cifrado de Sobre) que garantiza que cada documento, cada dato y cada identidad de los clientes permanezca de forma completamente ininteligibles(AES-256-GCM) para cualquier ente, incluyendo los administradores de la propia base de datos.

2. Niveles de Criptografía (Envelope Encryption)

Adoxor utiliza tres niveles jerárquicos de claves asimétricas para gestionar de forma eficiente el riesgo, rendimiento y capacidad de rotación, garantizando una protección de nivel gubernamental sin mermar la velocidad (Paginación a nivel SQL con tiempos de respuesta menores a 200ms).

2.1. KEK (Key Encryption Key):

Alojado exclusivamente en el hardware criptográfico de **Google Cloud KMS** (Key Management Service). Esta clave maestra jamás sale del KMS y su única función es cifrar y descifrar las claves de las organizaciones. Es el guardián de Nivel 1.

2.2. OEK (Organization Encryption Key):

Clave criptográfica temporal y única generada aleatoriamente en nuestros servidores (256 bits) para cada organización registrada. Una vez generada, se envía instantáneamente al KMS para que la firme con la KEK. La versión plana de la OEK se destruye y solo se almacena en la base de datos de Adoxor como `oekEncrypted` en Base64. (Tier 2).

2.3. DEK (Data Encryption Key):

Clave simétrica específica generada asíncronamente en milisegundos para *cada documento individual* o json de cliente subido. Se cifra utilizando la OEK descifrada en memoria RAM volátil. Es el último Tier 3 que garantiza el aislamiento unitario de los documentos.

3. Aislamiento Físico y Blind Indexing

Todos los campos relevantes para búsquedas como CIF, Nombres completos o DNI nunca se almacenan en texto plano en la plataforma.

Aún así, para dotar de una plataforma rápida a las organizaciones, Adoxor utiliza **Blind Indexing (Índices Ciegos)**. Cada campo susceptible de búsqueda sufre un proceso de ofuscación donde calculamos su `HMAC-SHA256(valor, BLIND_KEY_ORGANIZACION)`.

Cuando un usuario busca "Juan", el sistema genera el Hash ciego y busca en base de datos aquel valor coincidente. Logramos búsquedas exactas sobre datos criptográficos que nadie puede leer visualmente en el motor SQL de la BD (PostgreSQL).

4. Auditoría, Integridad y Aislamiento del Cliente

- **Aislamiento**: "1 DEK por Documento". Aunque un actor malicioso lograra por un error milagroso extraer la clave que protege el historial A de un Cliente, esta clave sería totalmente inútil para el historial B. No hay contigüidad criptográfica.
- **Rendimiento Seguro:** Toda la lógica ocurre instantáneamente gracias a implementaciones GCM en memoria.
- **Autenticación (JWT)**: Todo el flujo recae sobre la estricta capa de autenticación, validando los permisos mediante Roles inyectados dinámicamente dentro del payload cifrado del JSON Web Token validado mediante Spring Security HTTP.

Conclusión

Nuestros protocolos permiten a clínicas, hospitales, bufetes de abogados y gestorías transferir su responsabilidad a una estructura validada para el estricto cumplimiento RGPD dictado en la UE, asegurando su información con los mismos esquemas blindados siguiendo estándares ampliamente utilizados en la industria para sus transacciones internas de alto secreto.