Gaytan Herrera Belen
Rojas Jimenez Claudia Alin

1. Descripción general del sistema

- ¿Qué problema resuelve su bóveda?
- ¿Cuáles son las características principales?
- ¿Qué está *explícitamente fuera del alcance* ?

La bóveda digital segura resuelve el problema de proteger documentos digitales contra acceso no autorizado, alteración y suplantación de identidad. Garantiza confidencialidad, autenticidad, integridad y no repudio mediante el uso correcto de criptografía moderna aplicada.

Características:

- Cifrado autenticado (AEAD) para proteger la confidencialidad e integridad de los archivos.
- Generación de una clave simétrica única por documento.
- Protección de la clave simétrica mediante cifrado híbrido usando la clave pública de cada destinatario.
- Firma digital del documento para garantizar autenticidad y no repudio.
- Verificación obligatoria de la firma antes de permitir el descifrado.
- Protección de llaves privadas usando una función de derivación de clave basada en contraseña (KDF).
- Soporte para compartir documentos con múltiples destinatarios.
- Mecanismo básico de respaldo y recuperación de llaves.

Queda fuera del alcance prevenir que un usuario comparta voluntariamente su clave privada, no se protege el documento si es exportado y compartido fuera del sistema y no se protege contra ataques físicos al dispositivo del usuario.

2. Diagrama de arquitectura (obligatorio)

Proporcione un diagrama claro que muestre:

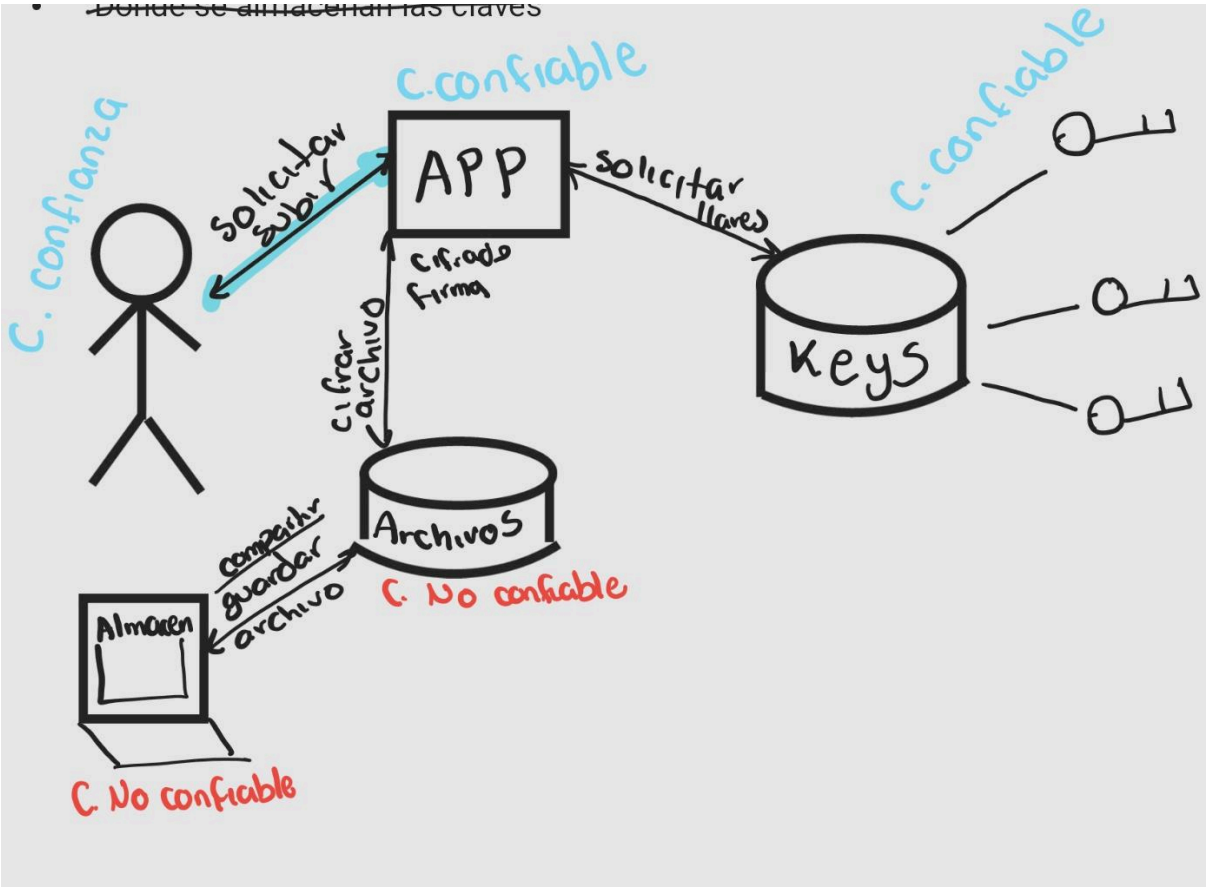
- Usuario
- Aplicación (Bóveda)
- Contenedor de archivos cifrados
- Almacén de claves
- Claves públicas/destinatarios
- Almacenamiento (local o remoto)

Debes etiquetar:

- Componentes de confianza
- Componentes que no son de confianza
- Flujos de datos

El diagrama debe mostrar:

- Dónde se realiza el cifrado
- Dónde se realiza la firma
- Dónde se almacenan las claves



3. Requisitos de seguridad

Enumere las propiedades de seguridad explícitas que su sistema debe proporcionar

- Si un atacante ve el contenido del archivo, mientras no se tenga la llave única y privada del autor, este no podrá acceder ni por aleatoriedad ni por fuerza bruta al contenido original del documento
- Cualquier modificación no autorizada del archivo cifrado o de su firma digital debe ser detectada antes del descifrado.
- El sistema debe permitir verificar criptográficamente que el documento fue firmado por el propietario legítimo de la clave privada correspondiente.
- Una vez firmado un documento, el autor no debe poder negar haberlo firmado, siempre que su clave privada no haya sido comprometida.
- Las claves privadas deben almacenarse cifradas utilizando una función segura de derivación de claves basada en contraseña (KDF), de modo que un atacante que obtenga el archivo de la clave no pueda utilizarla sin conocer la contraseña.
- Solo los destinatarios explícitamente autorizados deben poder descifrar la información del archivo mediante sus respectivas claves privadas.

4. Modelo de amenazas

Debe definir:

Activos

- Contenido del archivo original (antes del cifrado).
- Archivo cifrado almacenado o transmitido.
- Metadatos del archivo (identidad del autor, destinatarios, identificadores de claves).
- Claves privadas de los usuarios.
- Claves simétricas generadas por documento.
- Contraseñas utilizadas para proteger claves privadas.
- Validez e integridad de las firmas digitales.
- Copias de seguridad de claves privadas.

Adversarios

- ★ A. Atacante externo con acceso a contenedores almacenados
  - Puede obtener acceso a:
    - Archivos cifrados.
    - Metadatos.
    - Backups de claves.
  - Pero no posee claves privadas legítimas.
- ★ B. Atacante que intercepte comunicaciones (atacante pasivo)
  - Puede:
    - Observar tráfico.
    - Copiar archivos cifrados.
    - Capturar metadatos transmitidos.
  - No puede modificar el tráfico.
- ★ C. Atacante activo
  - Puede:
    - Modificar archivos cifrados.
    - Alterar metadatos.
    - Intentar reemplazar claves públicas.
    - Eliminar o modificar copias de seguridad.
    - Intentar ataques de fuerza bruta contra contraseñas débiles.
- ★ D. Destinatario malicioso
  - Un usuario autorizado que:
    - Puede descifrar el documento.
    - Puede intentar redistribuir el contenido fuera del sistema.
    - Puede intentar negar recepción o manipular evidencia.
- ★ E. Atacante con acceso temporal al dispositivo
  - Puede:
    - Acceder a archivos almacenados.
    - Intentar copiar claves privadas cifradas.

        - Intentar ataques offline contra contraseñas.
    - No tiene acceso permanente ni control total del sistema operativo.

5. Supuestos de confianza

Indique explícitamente lo que su sistema asume.

- El generador de números aleatorios del sistema operativo proporciona entropía criptográficamente segura.
- El almacenamiento donde se guardan los archivos cifrados puede ser considerado no confiable.
- El canal de intercambio de claves públicas puede ser observado por terceros, pero no se asume seguro por defecto.
- Los usuarios protegen adecuadamente sus contraseñas.
- Los usuarios no comparten voluntariamente sus claves privadas.
- Los usuarios verifican la autenticidad de las claves públicas antes de utilizarlas.
- Las claves públicas utilizadas pertenecen realmente a las identidades que representan.
- Las claves privadas no han sido previamente comprometidas.
- El mecanismo de respaldo de claves es almacenado de manera segura por el usuario.

6. Revisión de la superficie de ataque

Enumere todos los puntos de entrada con los que los atacantes podrían interactuar:

Puntos	Que podría salir mal	Bienes en riesgo
Entrada de archivo (Encrypt/Upload)	Procesamiento de archivo malicioso, fuga de metadatos antes del cifrado, reutilización de nonce o clave	Contenido del archivo, clave simétrica, metadatos
Análisis y almacenamiento de metadatos	Alteración de identidad del autor/destinatarios, fuga de información sensible	Identidad del firmante, destinatarios, metadatos
Importación de claves públicas	Sustitución de clave pública (key substitution attack)	Confianza en identidad, clave simétrica del archivo
Exportación de claves privadas	Exportación sin cifrado fuerte, corrupción de archivo de clave	Claves privadas
Introducción de contraseña	Ataques de fuerza bruta offline, contraseña débil, exposición en memoria	Clave privada cifrada, backups
Flujo de compartición	Cifrado con clave pública	Clave simétrica del

(Sharing workflow)	incorrecta, manipulación del contenedor compartido	documento, archivo cifrado
Verificación de firma	Omisión de verificación antes del descifrado, validación con clave incorrecta	Validez de la firma, integridad del documento
Argumentos de la CLI	Inyección de rutas, sobrescritura accidental de archivos o claves	Claves privadas, archivos cifrados, backups
Generación de claves y nonces	Reutilización de nonce, generador de aleatoriedad débil, tamaño de clave incorrecto	Claves simétricas, seguridad global del sistema
Sistema de respaldo y recuperación	Backup sin cifrado adecuado, eliminación maliciosa, recuperación sin autenticación	Claves privadas, acceso histórico a documentos
Manejo de errores y logging	Filtración de información sensible en mensajes de error o logs	Metadatos, claves, información del sistema

7. Restricciones de diseño derivadas de los requisitos

Muestre cómo los requisitos se traducen en decisiones de arquitectura.

- Todos los archivos son cifrados utilizando cifrado autenticado (AEAD) antes de ser almacenados o compartidos.
- Se genera una clave simétrica única y aleatoria para cada documento.
- Se implementa cifrado híbrido, donde la clave simétrica del archivo se cifra individualmente con la clave pública de cada destinatario autorizado.
- Cada documento es firmado digitalmente con la clave privada del autor antes de su distribución.
- La firma digital debe verificarse obligatoriamente antes de cualquier operación de descifrado, y el cifrado autenticado detecta cualquier alteración del contenido.
- Las claves privadas se almacenan cifradas utilizando una clave derivada de contraseña mediante una función segura de derivación de claves (KDF).
- Se utiliza una KDF con sal y parámetros de endurecimiento (iteraciones elevadas o factores de costo) para dificultar ataques de diccionario.
- Se emplea cifrado autenticado (AEAD), que proporciona confidencialidad e integridad en una sola construcción criptográfica.
- El contenedor del documento incluye múltiples versiones cifradas de la clave simétrica, una por cada destinatario autorizado.