Cifrar y descifrar IM&P Compliance Encryption Key

Contenido

Introducción

Este documento describe cómo cifrar y descifrar la clave de cifrado generada por IM&P para la configuración cifrada de cumplimiento.

Prerequisites

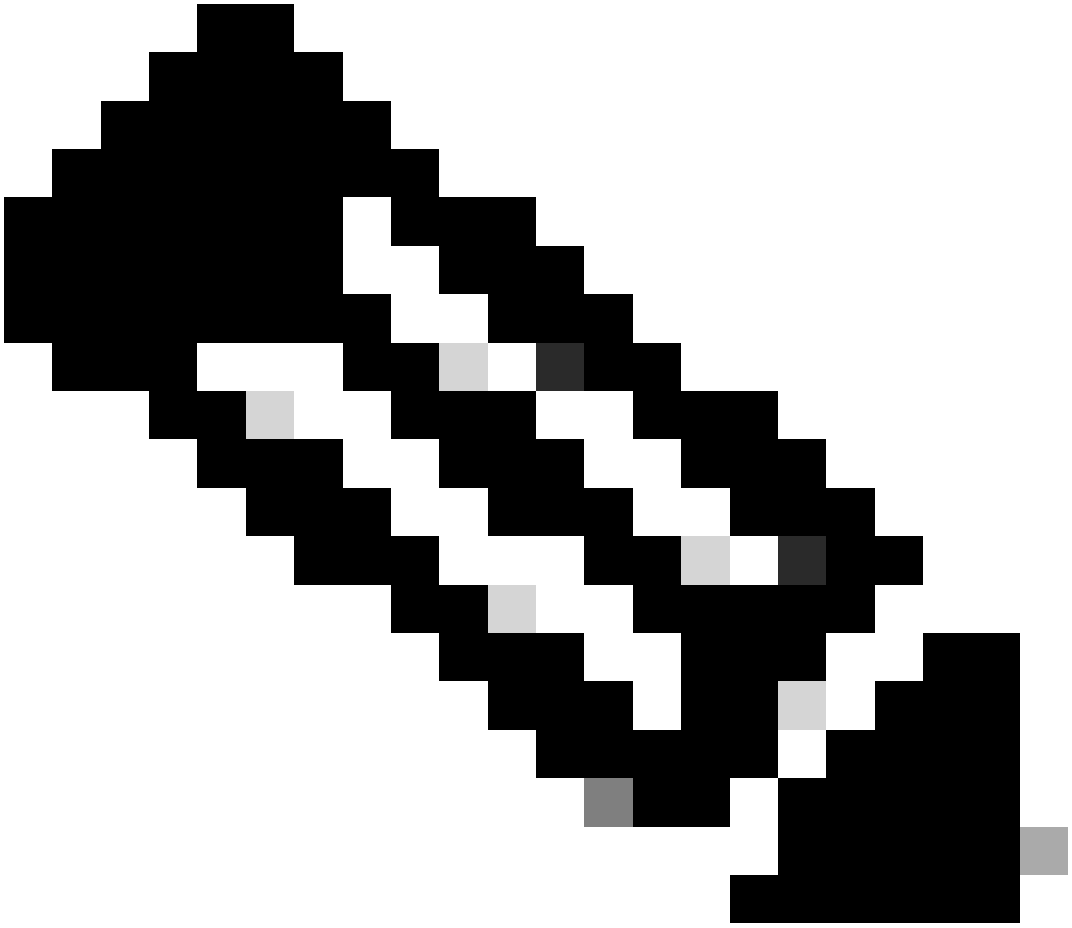
Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración del Archivador de Mensajes
- OpenSSL

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- MacOS 15.5
- IM and Presence (IM&P) versión 15su2
- OpenSSL 3.3.6



Nota: Los comandos que se muestran en este documento pueden variar según la versión o plataforma de OpenSSL. Internet es una buena fuente para encontrar a aquellos que se adaptan a su entorno.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La función Message Archiver proporciona una solución básica de conformidad con la mensajería instantánea. Esta función permite que el sistema cumpla las normativas que requieren el registro de todo el tráfico de mensajería instantánea de la empresa. Muchos sectores requieren que los mensajes instantáneos cumplan las mismas directrices de conformidad normativa que el resto de registros empresariales. Para cumplir estas normativas, el sistema debe registrar y archivar todos

los registros empresariales, y los registros archivados deben ser recuperables.

Para mayor seguridad, puede habilitar una base de datos cifrada para el Archivador de mensajes. Cuando esta opción está activada, el servicio de mensajería instantánea y presencia cifra los mensajes instantáneos antes de archivarlos en la base de datos externa. Con esta opción, todos los datos de la base de datos están cifrados y no se pueden leer los IM archivados, a menos que se posea la clave de cifrado.

La clave de cifrado se puede descargar del servicio de mensajería instantánea y presencia y se puede utilizar junto con cualquier herramienta que utilice para ver datos con el fin de descifrar los datos archivados.

Cifrar/descifrar

1. Abra su terminal OpenSSL.
2. Generar clave privada.

```
openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
```

3. Extraiga la clave pública de la clave privada.

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

4. En este punto, tenemos 2 archivos private_key.pem y public_key.pem.

- clave_privada.pem: Se utiliza para descifrar la clave cifrada desde IM&P.
- clave_pública.pem: Esta es la clave que comparte con el servidor de IM&P para permitirles cifrar la clave AES y IV.

Además, el servidor IM&P agrega la codificación Base64 a la clave de cifrado cifrada.

5. Descargue la clave de cifrado del servidor IM&P; consulte la sección Descargar clave de cifrado en la Guía de cumplimiento de mensajería instantánea para el servicio IM and Presence.
6. En este punto tiene 3 archivos private_key.pem, public_key.pem y encryp_key.pem.
7. En este caso, encryption_key.pem está codificado con Based64 para una transmisión segura.
8. Decodificar la clave cifrada codificada con Base64.

```
base64 -D -i encrypted_key.pem -o encrypted_key.bin
```

Esto elimina la codificación Base64 y produce un archivo de 256 bytes que se cifró originalmente con la clave RSA pública.

9. Descifre la clave cifrada con la clave privada RSA.

```
openssl pkeyutl -decrypt -inkey private_key.pem -in encrypted_key.bin -out decryptedkey.bin
```

Esto descifra la clave AES (K) e IV utilizada para el cifrado de mensajes IM&P.

Ejemplo de archivo descifrado:

clave = 0ec39f2a22abf63d4452b932f12de

iv = 6683bb3d7e59e82e3fa9f42

10. Descifrar los mensajes cifrados con AES.

```
openssl enc -aes-256-cbc -d -in encrypted.bin -out decrypted.txt -K <hex_key> -iv <hex_iv>
```

Troubleshoot

Un error común al intentar descifrar el archivo cifrado es:

```
Public Key operation error 60630000:error:0200006C:rsa routines:rsa_ossl_private_decrypt:data greater t
```

Este error se produce cuando intenta descifrar datos RSA que son demasiado grandes para el tamaño de su clave privada RSA. RSA sólo puede descifrar datos hasta el tamaño de su módulo. En nuestro caso, una clave RSA de 2048 bits sólo puede descifrar 256 bytes.

Si marca el archivo de clave encriptada generado por IM&P, es 344bytes. Solo puede descifrar 256 bytes con nuestra clave privada.

```
-rw-rw-rw-@ 1 testuser staff 344 Jun 5 13:10 encrypted_key.pem
```

Como se mencionó anteriormente en este documento, la clave cifrada está codificada en Base64 para una transmisión segura, lo que agrega bytes al tamaño del archivo.

Una vez que eliminamos la codificación Base64, tiene un archivo de 256 bytes, fácilmente

descifrable con nuestra clave privada.

```
-rw-r--r-- 1 testuser staff 256 Jun 12 09:16 encrypted_key.bin
```

Prácticas recomendadas de seguridad

- Almacene su clave privada (private_key.pem) de forma segura.
- No comparta su clave privada con otras personas ni la cargue en sistemas que no sean de confianza.
- Limpie los archivos temporales como decryptedkey.bin después del descifrado.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).