De coderingssleutel voor de naleving van IMiP coderen en decoderen

Inhoud

Inleiding

In dit document wordt beschreven hoe u de coderingssleutel die door IM&P is gegenereerd voor de gecodeerde configuratie kunt coderen en decoderen.

Voorwaarden

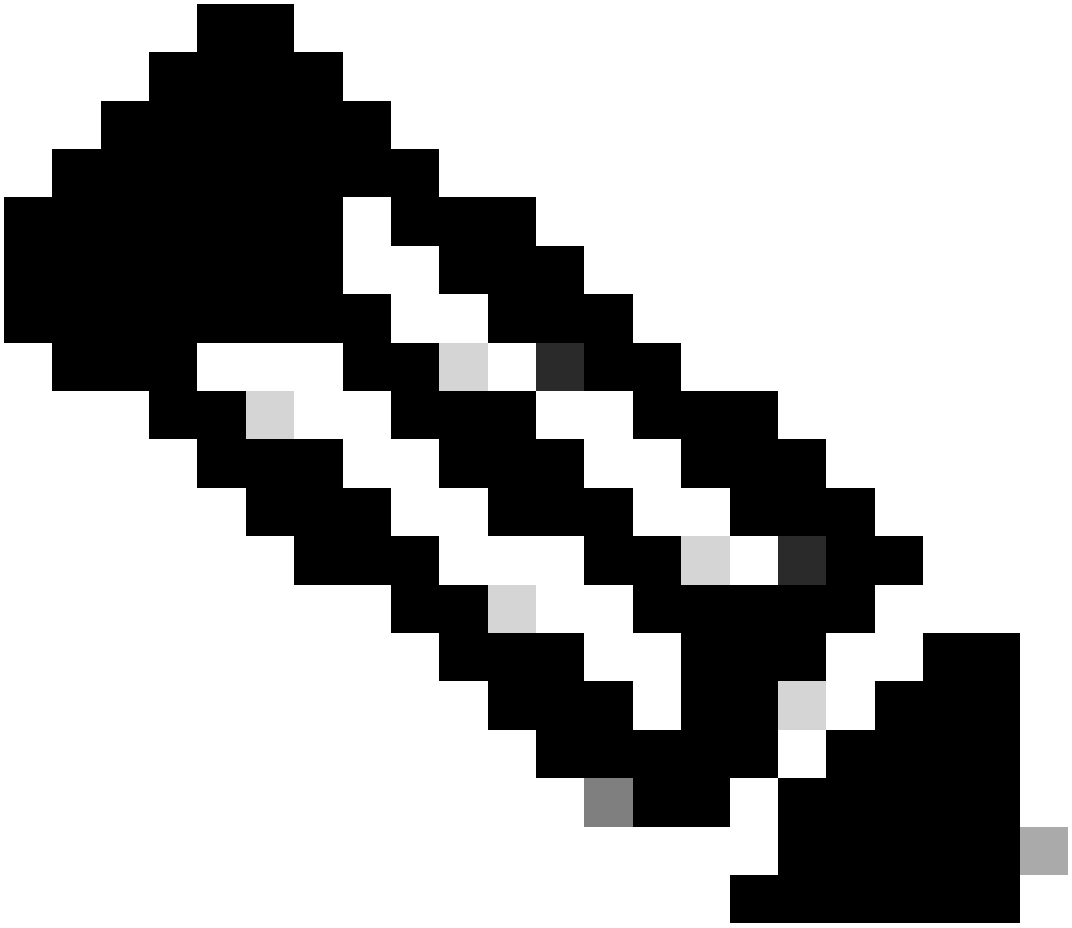
Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie berichtenarchief
- OpenSSL

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- MacOS 15,5
- IM en Presence(IM&P) versie 15su2
- OpenSSL 3.3.6



Opmerking: De opdrachten die in dit document worden weergegeven, kunnen variëren op basis van uw OpenSSL-versie of -platform. Het internet is een goede bron om mensen te vinden die bij uw omgeving passen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De functie Berichtenarchief biedt een eenvoudige oplossing voor IM-naleving. Met deze functie kan uw systeem voldoen aan voorschriften die vereisen dat al het instant messaging-verkeer in uw bedrijf wordt geregistreerd. Veel industrieën vereisen dat instant messages zich houden aan dezelfde richtlijnen voor naleving van de regelgeving als voor alle andere zakelijke records. Om aan deze voorschriften te voldoen, moet uw systeem alle zakelijke records registreren en

archiveren en moeten gearchiveerde records kunnen worden opgehaald.

Voor extra beveiliging kunt u een gecodeerde database inschakelen voor de Berichtenarchief. Als deze optie is ingeschakeld, codeert de IM- en aanwezigheidsservice IM's voordat ze worden gearchiveerd in de externe database. Met deze optie worden alle gegevens in de database gecodeerd en kunt u geen gearchiveerde IM's lezen, tenzij u over de coderingssleutel beschikt.

De coderingssleutel kan worden gedownload van de IM- en aanwezigheidsservice en worden gebruikt in combinatie met welk hulpmiddel u ook gebruikt om gegevens te bekijken om gearchiveerde gegevens te decoderen.

Coderen/decoderen

1. Open uw OpenSSL terminal.
2. Genereer een privésleutel.

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

3. Haal de publieke sleutel uit de private sleutel.

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

4. Op dit moment hebben we 2 bestanden private_key.pem en public_key.pem.

- private_key.pem: Wordt gebruikt om de gecodeerde sleutel van IM&P te decoderen.
- public_key.pem: Dit is de sleutel die u deelt met de IM&P-server om hen in staat te stellen de AES-sleutel en IV te coderen.

Bovendien voegt de IM&P-server Base64-codering toe aan de gecodeerde coderingssleutel.

5. Download de coderingssleutel van de IM&P-server en raadpleeg het gedeelte Coderingssleutel downloaden in de gids Instant Messaging Compliance Guide voor de IM- en aanwezigheidsservice.
6. Op dit punt heb je 3 bestanden private_key.pem, public_key.pem en encrypted_key.pem.
7. In dit geval is encrypted_key.pem Based64-gecodeerd voor veilige verzending.
8. Decodeer de gecodeerde Base64-sleutel.

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

Dit verwijdert Base64-codering en produceert een bestand van 256 bytes dat oorspronkelijk was

gecodeerd met uw openbare RSA-sleutel.

9. Decodeer de gecodeerde sleutel met uw RSA-privésleutel.

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

Dit decodeert de AES-sleutel (K) en IV die worden gebruikt voor IM & P-berichtcodering.

Voorbeeld gedecodeerd bestand:

SLEUTEL = 0EC39F2A22ABF63D4452B932F12DE

IV = 6683BB3D7E59E82E3FA9F42

10. Decodeer de AES-gecodeerde berichten.

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

Problemen oplossen

Een veelvoorkomende fout bij het decoderen van het gecodeerde bestand is:

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

Deze fout treedt op wanneer u probeert RSA-gegevens te decoderen die te groot zijn voor de grootte van uw RSA-privésleutel. RSA kan alleen gegevens decoderen tot de grootte van de modulus. In ons geval kan een 2048-bits RSA-sleutel slechts 256 bytes decoderen.

Als u het gecodeerde sleutelbestand controleert dat door IM&P is gegenereerd, is het 344 bytes. U kunt alleen 256 bytes decoderen met onze privé sleutel.

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

Zoals eerder vermeld in dit document, is de gecodeerde sleutel Base64 gecodeerd voor veilige verzending, waardoor bytes aan de bestandsgrootte worden toegevoegd.

Zodra we de Base64-codering verwijderen, hebt u een bestand van 256 bytes, dat gemakkelijk kan worden gedecodeerd met onze privé sleutel.

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

Best practices voor beveiliging

- Sla uw persoonlijke sleutel (private_key.pem) veilig op.
- Deel uw persoonlijke sleutel niet met anderen of upload deze naar niet-vertrouwde systemen.
- Schoon tijdelijke bestanden zoals decryptedkey.bin na decryptie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.