# IM&の暗号化および復号化；Pコンプライアンス暗号化キー

## 内容


はじめに

前提条件

使用するコンポーネント

背景説明

暗号化/復号化

トラブルシュート

セキュリティのベストプラクティス


## はじめに

このドキュメントでは、コンプライアンス暗号化設定用にIM&Pによって生成された暗号化キーを暗号化および復号化する方法について説明します。

## 前提条件

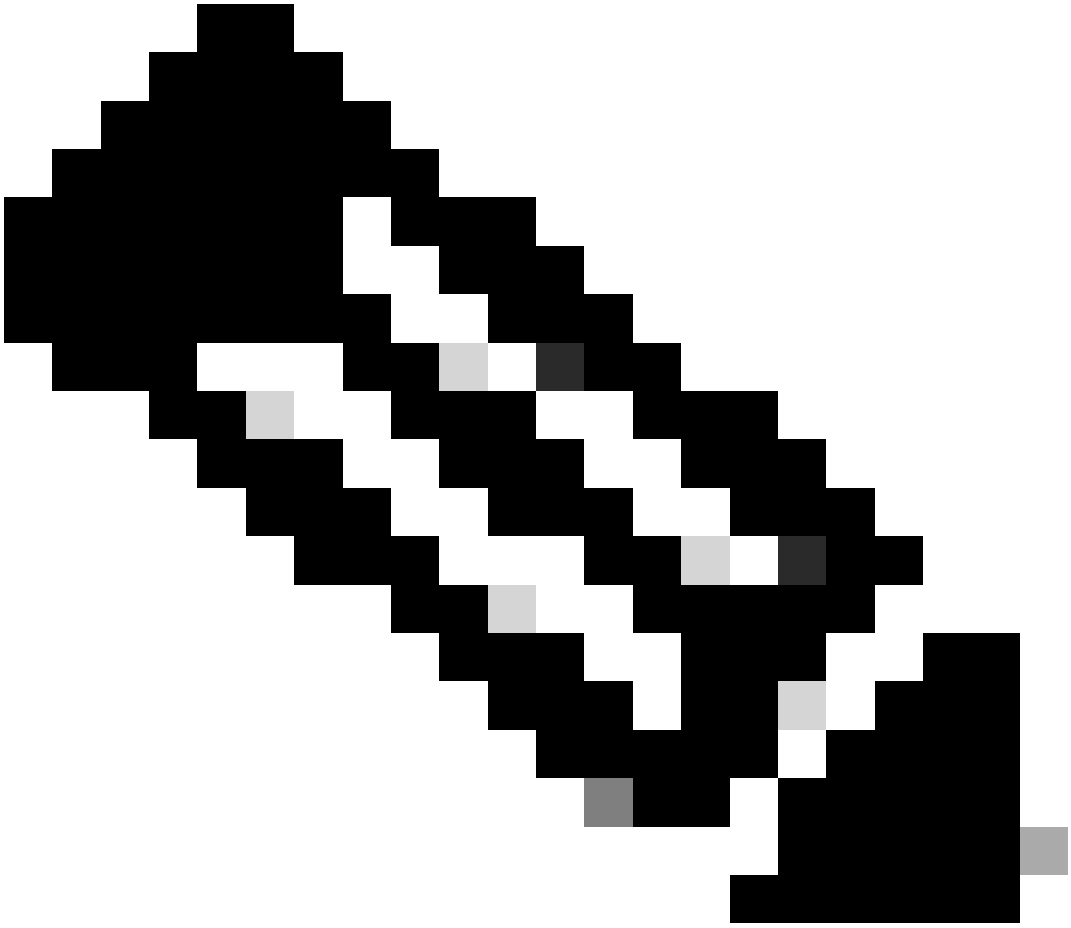
次の項目に関する知識があることが推奨されます。

- Message Archiverの設定
- OpenSSL

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- MacOS 15.5
- IM and Presence(IM&P)バージョン15su2
- OpenSSL 3.3.6



注：このドキュメントに記載されているコマンドは、OpenSSLのバージョンまたはプラットフォームによって異なる場合があります。インターネットは、自分の環境に適した人材を見つけるのに適した情報源です。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

Message Archiver機能は、基本的なIMコンプライアンスソリューションを提供します。この機能を使用すると、社内のすべてのインスタントメッセージングトラフィックのロギングを必要とする規制にシステムが準拠できるようになります。多くの業界では、インスタント・メッセージに関して、他のすべてのビジネス記録と同じ規制コンプライアンス・ガイドラインを遵守することが求められています。これらの規制に準拠するには、システムがすべてのビジネス記録を記録お

よびアーカイブし、アーカイブされた記録は取得可能である必要があります。

セキュリティを強化するために、Message Archiverの暗号化されたデータベースを有効にできます。このオプションを有効にすると、IM and PresenceサービスはIMを暗号化してから外部データベースにアーカイブします。このオプションを使用すると、データベース内のすべてのデータが暗号化され、暗号化キーを持っていない限り、アーカイブされたIMを読み取ることはできません。

暗号化キーはIM and Presenceサービスからダウンロードでき、アーカイブされたデータを復号化するためにデータを表示するために使用するツールと組み合わせて使用できます。

# 暗号化/復号化

1. OpenSSLターミナルを開きます。
2. 秘密キーを生成します。

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

3. 秘密キーから公開キーを抽出します。

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

4. この時点で、private_key.pemとpublic_key.pemの2つのファイルがあります。

- private_key.pem:IM&Pから暗号化されたキーを復号化するために使用されます。
- public_key.pem：これは、AESキーとIVを暗号化するためにIM&Pサーバと共有するキーです。

さらに、IM&Pサーバは暗号化された暗号キーにBase64エンコーディングを追加します。

5. IM&Pサーバから暗号キーをダウンロードします。IM and Presenceサービスのガイド『Instant Messaging Compliance Guide for the IM and Presence Service』の「Download Encryption Key」セクションを参照してください。
6. この時点で、private_key.pem、public_key.pem、encrypted_key.pemの3つのファイルがあります。
7. この場合、encrypted_key.pemは安全な転送のためにBased64でエンコードされています。
8. Base64エンコード暗号化キーをデコードします。

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

これにより、Base64エンコーディングが削除され、最初は公開RSAキーで暗号化された256バイトのファイルが作成されます。

9. RSA秘密キーを使用して暗号化キーを復号化します。

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

これにより、IM&Pメッセージの暗号化に使用されるAESキー(K)とIVが復号化されます。

復号化されたファイルの例：

キー= 0ec39f2a22abf63d4452b932f12de

iv = 6683bb3d7e59e82e3fa9f42

10. AES暗号化メッセージを復号化します。

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

# トラブルシュート

暗号化されたファイルの復号化を試みるときの一般的な工ラーは次のとおりです。

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

このエラーは、RSA秘密キーのサイズに対して大きすぎるデータをRSA復号しようとすると発生します。 RSAで復号化できるデータは、そのモジュラスのサイズまでです。この例では、2048ビットのRSAキーで復号化できるのは256バイトだけです。

IM&Pによって生成される暗号化されたキーファイルをチェックする場合、これは344バイトです。秘密キーを使用して256 バイトのみを復号化できます。

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

このドキュメントで前述したように、暗号化キーは安全な転送のためにBase64でエンコードされており、ファイルサイズにバイトが追加されます。

Base64エンコーディングを削除すると、256バイトのファイルが作成され、秘密キーで簡単に復

号できます。

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

# セキュリティのベストプラクティス

- 秘密キー(private_key.pem)を安全に保存します。
- 秘密キーを他のユーザーと共有したり、信頼されていないシステムにアップロードしたりしないでください。
- 復号後にdecryptedkey.binなどの一時ファイルをクリーンアップします。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。