IM and PresenceおよびECDSA証明書に関する質問と回答

内容

概要

このドキュメントでは、Cisco IM and Presence(IM&P)アプライアンスと連携する楕円曲線デジタル署名アルゴリズム(ECDSA)証明書に関する質問に回答します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Communications Manager（CUCM）

- Cisco IM and Presence(IMP)
- Session Initiation Protocol（SIP）
- コンピュータ/テレフォニー インテグレーション（CTI）
- Rivest-Shamir-Adleman(RSA)暗号化
- 楕円曲線デジタル署名アルゴリズム(ECDSA)
- eXtensible Messaging and Presence Protocol（XMPP）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IM and Presence 11.5.1

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、初期（デフォルト）設定の状態から起動しています。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。

ECDSAに関するIM&P製品チームのディスカッション

エンタープライズパラメータのTransport Layer Security(TLS)暗号を参照する場合、デフォルトの選択は**All Ciphers RSA Preferredです**。そのため、パラメータTLS暗号に関して、IM&Pエンジニアリングチームから次の質問がありました。

> **注**：すべての質問に回答し、IM&Pエンジニアリングチームが確認します。

このパラメータは、RSAとECDSAのどちらかを選択する必要がある場合にIM&PがRSAを選択するように指示しますか。

はい。このパラメータは、CUCM SIP/CTIインターフェイス専用です。 RSA暗号はECDSAよりも優先されます。

[All Ciphers RSA Preferred]が選択されていても、Cisco IM and PresenceがECDSAを送信できる条件はどれか？

これはRSA暗号を優先するためのものですが、ECDSA暗号も持っていますが、クライアントが接続を開始するとECDSAの上にRSA暗号を送信します。

ECDSAのプライオリティが高い場合は、[All Ciphers RSA Preferred]が選択されていても選択できますか。

はい。このパラメータは、CUCMがクライアントとして機能する場合にのみ画像に表示されます。クライアントが接続を開始する順序が優先されます。 クライアントが上部のECDSA暗号を使用して接続を開始すると、接続はECDSAで行われます。そうでない場合は、RSAが優先されます。

どの暗号が最も優先順位が高いかを明らかに選択できる。サードパーティのクライアントが暗号スイートを含むHelloメッセージを送信すると、Cisco IM and Presenceは、サーバとクライアントの両方がサポートするサードパーティクライアントのTLS Cipher Mappingページ上のこのリストから最も強力な暗号暗号を選択しますす。

はい。サーバがクライアントとして機能する場合、前の質問で述べた順序で暗号を送信します。

これらのことを明らかにする書類はありますか。

はい。サポートされている暗号のリストが記載されているエンタープライズパラメータのページでTLS Ciphersリンクを選択するとすぐにヘルプオプションがあります。

すべてのCiphers RSA Preferredパラメータは、CUCM/IMPがクライアントとして機能している場合にのみ重要ですか。

はい。

CUCM/IMP（クライアント）がRSA証明書とECDSA証明書の両方を送信するが、RSA証明書の優先順位を最も高くすることはできますか。

はい。

TLS暗号のヘルプページでは、暗号がこの順序に含まれていることを示しています。このオプションを選択すると、暗号がその順序で送信されるという意味ですか。

すべての暗号RSA推奨

次の順序で暗号を含みます。

TLS_ECDHE_RSA（AES256_GCM_SHA384を使用）

TLS_ECDHE_ECDSA（AES256_GCM_SHA384を使用）

TLS_ECDHE_RSA（AES128_GCM_SHA256を使用）

TLS_ECDHE_ECDSA（AES128_GCM_SHA256を使用）

AES_128_CBC_SHA1によるTLS_RSA

はい。

All Ciphers RSA Preferredパラメータは、CUCM/IMPがサーバとして機能する場合には関係ありません。この場合、CUCM/IMPは、クライアントのHelloメッセージで最も優先度の高い証明書タイプで応答しますか。

はい。

このパラメータがSIP/CTIのみを参照している場合、XMPPインターフェイスとのTLS接続に対応するパラメータはありますか。

いいえ。XMPPの機能拡張がありますが、まだ実装されていません。