Codian MCU への HTTPS 接続を認証するにはどうすればよいですか。

目次

概要

この技術情報は Cisco TelePresence MCU 4203、Cisco TelePresence MCU MSE 8420、Cisco TelePresence MCU 4505、Cisco TelePresence MCU MSE 8510 および Cisco TelePresence によって進められるメディア ゲートウェイに 3610 の製品関連しています。

Q. Codian MCU への HTTPS 接続を認証するにはどうすればよいですか。

A. 前の Codian MCU バージョン 2.3 から、インストールされるセキュア マネージメント（HTTPS）または暗号化機能 キーがあれば MCU が Webインターフェイスのためのセキュア HTTP 接続（HTTPS）をサポートすれば。 これが暗号化されるべきユーザと MCU 間のすべてのトラフィックを割り当てる間、これを有効に して いる 管理者は専有物と MCU の識別が認証されるように供給された認証およびプライベートキーを取り替える必要があります。 MCU 毎に 1 つの認証があるただことができることに注目して下さい。

プライベートキーおよび認証を作成するために OpenSSL を使用して、組み合わせて下さい（たとえば）:

1. 必要ならばセキュア マネージメント（HTTPS）または暗号化機能 キーをインストールして下さい。
2. **ネットワーク > Services** に行き、ポートをオープンにして下さい。
3. 私達発行する temprary 認証を受け入れる HTTPS を使用して MCU に接続して下さい。
4. コンピュータ インストール OpenSSL*。 これは多くのでデフォルトで利用可能 Unix/Linuxシステムで、Windows のためにからダウンロードすることができます（書き込みの時に）: http://www.slproweb.com/products/Win32OpenSSL.html
5. コマンド ウィンドウで、たとえば C:\OpenSSL\bin は OpenSSL がインストールされたディレクトリに行きます。
6. 下記のコマンドを使用して RSA プライベートキーを生成して下さい。 このコマンドはプライベートキーである「privkey.pem」と呼ばれるファイルを生成します。 TANDBERG はこのキーをです長く少なくとも 2048 ビット推奨します。 このプライベートキーが MCU でから離れてどこでも保存されれば、パスフレーズによって保護する必要があります: このパスフレーズを二度入力するためにプロンプト表示されます。 > openssl genrsa -des3 -privkey.pem 2048
7. 下記のコマンドの 1 つを使用してこのプライベートキーに基づいて認証を作成して下さい。

テストおよび内部 使用の場合、この認証は自己署名である場合もあります最大のセキュリティのために認証局によって署名する必要があります。 自己署名証明書（cert.pem と呼ばれるファイル）使用を作成するため: > openssl req -新しい -x509 -キー privkey.pem - cert.pem -認証局 使用に送信 される 証明書要求のための幾日 1000 または: > openssl req - New 鍵 privkey.pem - cert.csr いくつかの属性のための両方のコマンド指示。 Common Name はインストールされる MCU のホスト名か IP アドレスを一致する必要があります。

8. 連鎖された認証を使用している場合、連鎖された認証は、pem 形式でユニットの認証の端に、追加 する必要があります。 これは 2 つの方法でするができます: テキストエディタでコピー アンド ペーストするか、または cat unix コマンド（例えば cat cert.pem authority.pem > chained.pem）のような何かを使用することによって。 それから作成済ファイルをアップロードして下さい。
9. MCU で**ネットワーク > SSL 認証**に行って下さい。
10. 認証に関しては、作成した認証を『Browse』 をクリック し、見つけて下さい（これは以前に使用した）ディレクトリにあります。 自己署名証明書を作成した場合、認証は cert.pem と呼ばれます。 認証局によって署名する 1 つのために彼らが供給した署名入り認証を選択して下さい。
11. プライベートキーに関しては、privkey.pem ファイルを選択して下さい。
12. プライベートキー暗号化 パスワードに関しては、プライベートキーを生成した場合使用されるパスフレーズを入力して下さい（もしあれば）。
13. **認証を**『Upload』 をクリック し、**キー入力して下さい**。 アップロードが成功である場合、ローカル証明書情報は新しい認証のそれにアップデートされ、MCU を再起動するためにプロンプト表示する警告は Webインターフェイスのヘッダでようです。
14. **設定に > シャットダウンされる**行き、MCU を再起動して下さい。
15. それが再起動した後、HTTPS を使用して Webインターフェイスに接続して下さい。 自己署名証明書を使用した場合、警告メッセージを無視して下さい。
16. 正しい認証が使用されていることを確認して下さい。 これを行うには、 - Firefox で…: ページの右クリックは、**ページ 情報を**『View』 を選択 します。 **Security タブを**クリックし、『View』 をクリック して下さい。 - Internet Explorer で…: ページの右クリックは、『Properties』 を選択 します。 **認証を**クリックして下さい。

* TANDBERG はサード パーティ Webサイトのコンテンツに責任がありません

関連情報

- テクニカルサポートとドキュメント - Cisco Systems