IEA での CSR の IEA 2048 ビット キー サポートの設定例

目次

概要

この資料に Cisco IronPort 暗号化アプライアンス (国際エネルギー機関) で証明書署名要求 (CSR) のための 2048 ビット キー サポートを生成する方法を記述されています。

設定

認証機関 (CA) のほとんどは長さ 2048 ビットのキーペアと生成されるすべての CSR があるために明示的 な 要求を示しました。 デフォルトで、国際エネルギー機関バージョン 6.5 はキーペア生成のために 1024 ビット 変調長さを使用します。 国際エネルギー機関に長さ 2048 のキーペアを生成させますここに記述されているように keytool コマンドを使用して下さい。

認証を生成して下さい

1. 国際エネルギー機関 CLI へのログイン
2. メインメニュー、型 **X** シェルに廃棄するため。
3. ルート ユーザに変更して下さい:
   ```
   $ su -
   ```
4. 新しい keystore を作成するために keytool を実行して下さい:
   ```
       # /usr/local/postx/server/jre/bin/keytool -genkey -alias <server alias>
   -keyalg RSA -keysize 2048 -keystore <name the new keystore>
          *alias should be what the server is known as externally when customers
   log into the device
          *When prompted for password use a easily remembered password
          *Enter in all requested information when prompted for the certificate
   request, make special note of the next question:
          --- What is your first and last name?
          [Unknown]: server1.example.com
   ```

```
                *For this question enter in the fully qualified domain name
of the system
       *The name of the newkeystore should be in the format <name>.keystore
where name should include the current date
           Example:  enterpriseks20130108.keystore
```

5. CSR ファイルを作成するために keytool を実行して下さい:
   # /usr/local/postx/server/jre/bin/keytool -certreq -keyalg RSA -alias <server alias> -file <servername>.csr -keystore <name of the new keystore>

6. に CSR ファイルを認証を生成するために認証局（CA）提供します。 Apache Web Server Certficate 署名要求として送信するをそれ確認して下さい。
7. CA から .cer ファイルを受け取った後、次 の ステップに進んで下さい。

証明書のインポート

注: CSR を生成するとき使用されるパスワードはこれらの手順がはたらくことができるように keystore パスワードとマッチする**必要があります**。 CSR が作成されたオフ ボックスだった場合、入力されるパスワードはこれらの手順がはたらくことができるように keystore パスワードとマッチする**必要があります**。

認証を正しく連鎖して下さい

1. 各 CA 認証は CA から届くおよび次にテキスト工ディタで一緒にマージされる CER ファイルから得る必要があります。

   注: Microsoft Windows マシンからされるこれは最も容易です。 他のオペレーティング システムはより得にくいですはたらきますが。
   認証はこの順序で連鎖する必要があります: 1.Domain 2.中間 3.Root

   証明書ファイル（.CER ファイル）を開くためにダブルクリックし次に**認証パス** タブをクリックして下さい:

   認証パスの中間レベルから開始し、**Details タブを**クリックし、**ファイルに**『Copy』 をクリック し、次にそれを **1.CER と**指名して下さい。

   X.509(.CER) を『Base 64 encoded』 を選択 して下さい。

   最高 レベル CA のために繰り返し、それを **2.CER と**指名して下さい。

サーバ証明のために繰り返し、**それを 3.CER と指名して下さい。**

3 つの **X.CER** ファイルをすべて開き、順序（1、および下部のの上の 3）で結合するためにテキストエディタ（**ない**テキストエディタ、notepad++ うまく作動を）使用して下さい:

注: 下部のに認証と空の行間に空の行はないはずです。

<servername>.CER として保存。

FTP または SCP の **/home/admin/ <servername.cer>** で国際エネルギー機関に **<servername>.CER** ファイルをアップロードして下さい。

/usr/local/postx/server/conf に /home/admin/ <servername.cer> をコピーして下さい:

2. 認証をインポートするために国際エネルギー機関 GUI を使用して下さい[キーおよび認証 | 設定される SSL]。

   注: Keystore = **[インストール ディレクトリ]** keystore ファイルの **/conf/enterprisenamestore.keystore か**現在の名前。

   認証 = **/usr/local/postx/server/conf/NEWCERT.CER**。

   信頼 CA 証明書をチェックして下さい。

   認証を『Import』 をクリック して下さい

3. （オプションの -- 新しい keystore が作成する必要があれば）。 国際エネルギー機関 GUI から、国際エネルギー機関を新しい keystore を使用するように言って下さい:

   『Configuration』 を選択 して下さい | Webサーバおよびプロキシ | Webサーバ | 接続リスナー | HTTPS

   新しい keystore ファイルにパスを打ち込んで下さい:

   例： ${postx.home}/conf/2013_5_13.keystore

4. 変更を展開し、SMTP アダプタを再起動して下さい。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。