SSL 証明書が Cisco E メール セキュリティ アプライアンスに関連付けられたキーによって署名されていることを確認するにはどうしますか。

目次

質問

SSL 証明書が Cisco E メール セキュリティ アプライアンスに関連付けられたキーによって署名されていることを確認するにはどうしますか。

環境： Cisco E メール セキュリティ アプライアンス（ESA）、AsyncOS のすべてのバージョン

このナレッジ ベース記事では、シスコによる保守およびサポートの対象でないソフトウェアを参照しています。 情報は、利便性のために無償で提供されています。 さらにサポートが必要な場合は、ソフトウェア ベンダーに連絡してください。

SSL 証明書をインストールすることは TLS によって暗号化受信/配達への前提条件、および LDAP 安全なアクセスです。 証明書は CLI コマンド「certconfig」によってインストールされています。 インストールするように意図する証明書/キーペアは証明書に署名したキーで構成する必要があります。 これに従わないことは証明書/キーペアをインストールするために失敗に終わります。

次のステップは証明書が関連するキーによって署名したかどうか確かめるのを助けます。「server.key」および「server.cer」の証明書と呼ばれるファイルでプライベートキーがあると仮定して下さい。

1. 証明書およびキーの説明者フィールドが同じであることを確かめて下さい。 これが事実ではない場合、キーは署名者ではないです。 次のコマンド（openssl が付いているあらゆる標準 UNIXマシンの実行）はこれの確認を助けます。

   ```
   $ openssl x509 -noout -text -in server.crt
   $ openssl rsa -noout -text -in server.key
   ```

   証明書の説明者フィールドおよびキーが同じであることを確かめて下さい。 指数キーは 65537 と等しいはずです。

2. 証明書の係数の MD5 ハッシュを実行し、それらが同じであることを確認するためにキー入力して下さい。

```
$ openssl x509 -noout -modulus -in server.crt | openssl md5
$ openssl rsa -noout -modulus -in server.key | openssl md5
```

キーが証明書に署名した確実である場合もあれば MD5 がハッシュする 2 つが類似したである場合。

関連リンク

http://www.modssl.org/docs/2.8/ssl_faq.html