Cisco Prime Prime Infrastructure でのサードパーティ証明書の証明書署名要求（CSR）の生成

このマニュアルでは、Cisco Prime Prime Infrastructure においてサードパーティ証明書を取得するために証明書署名要求（CSR）を生成する方法、および Prime Infrastructure に証明書をインポートする方法について説明します。この章の内容は、次のとおりです。

前提条件

この設定を行う前に、以下の要件を満たしていることを確認してください。

- 基本動作に対応するための Prime Infrastructure のインストールおよび設定方法の知識
- 自己署名およびデジタル証明書、公開キー インフラストラクチャ（PKI）に関連するその他のセキュリティ メカニズムの知識

使用されるコンポーネント

このマニュアルの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Prime Infrastructure Release 1.1.0.58

サポートされているハードウェアの詳細については、次の URL にある Prime Infrastructure のリリースノートを参照してください。

http://www.cisco.com/en/US/docs/wireless/ncs/1.1/release/notes/NCS_RN1.1.html

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

証明書署名要求（CSR）

証明書は、サーバ、企業などのエンティティを識別し、公開キーとそのアイデンティティを関連付けるために使用する電子ドキュメントです。

自己署名証明書は、その作成者自身によって署名されたアイデンティティ証明書です。つまり、証明書を作成した人もその正当性を認めています。

証明書は、自己署名により、または認証局（CA）からデジタル署名により証明されます。

CA は、アイデンティティを確認し、証明書を発行するエンティティです。CA によって発行された証明書により、その証明書を識別するエンティティ名（サーバ名またはデバイス名など）に特定の公開キーがバインドされます。証明書で認証する公開キーだけが、証明書で識別するエンティティが所有する対応した秘密キーと連動します。証明書により、偽装のための疑似公開キーの使用を防ぐことができます。

CSR は、申請者がデジタル アイデンティティ証明書を申請するために CA に送信するメッセージです。CSR を作成する前に、申請者は、最初に秘密キーを守るキー ペアを生成します。CSR には、申請者を識別する情報（X.509 証明書の場合はディレクトリ名など）、および申請者が選択した公開キーが含まれます。対応する秘密キーは CSR に含まれていませんが、要求全体に対するデジタル署名を行うために使用されます。

CSR には、認証局が要求するアイデンティティに対する他のクレデンシャルや証明情報を添付することができます。認証局は申請者と連絡を取ってさらに情報を求めることもできます。概して、Entrust や VeriSign など、サードパーティの CA 企業は、会社がデジタル証明書を作成する前に CSR を要求します。

CSR の生成は、外部証明書をインストールするデバイスに依存しません。したがって、CSR と秘密キー ファイルは、CSR の生成をサポートする任意のマシンで個々に生成できます。この場合、CSR の生成は、スイッチまたはアプライアンスにも依存しません。

このマニュアルでは、Cisco Prime Infrastructure を使用してサードパーティ証明書用の CSR を生成する方法について説明します。

証明書の生成

証明書を生成するには、次のコマンドを入力します。

ncs key genkey -newdn -csr *csrfilename* **repository** *repositoryname*

-newdn	ドメイン情報を使用して新しい RSA キーと自己署名証明書を生成します。
-csr	新しい CSR 証明書ファイルを生成します。
repository	リポジトリ コマンド。

csrfilename	CSR ファイル名。
repositoryname	ファイルをバックアップする場所。80 文字までの英数字で指定します。

これによって、新しいキー / 自己署名証明書のペアを生成し、指定したファイルに CSR を出力します。newdn フラグを使用すると、証明書の識別名フィールドに対して入力を求めるプロンプトが表示されます。ブラウザの警告を回避するために、DN の CN フィールドに Prime Infrastructure へのアクセスに使用する最終的なホスト名を指定することが重要です。

次に、Prime Infrastructure サーバの新しい RSA キーおよび証明書ファイルを生成する例を示します。

```
admin# ncs key genkey -newdn -csr csrfile.cert repository ncs-sftp-repo
Prime Infrastructure server is running
Changes will take affect on the next server restart
Enter the domain name of the server: <server name>
Enter the name of your organizational unit: <organizational unit>
Enter the name of your organization: <organization>
Enter the name of your city or locality: <city>
Enter the name of your state or province: <state>
Enter the two letter code for your country: <country code>
Generating RSA key
Writing certificate signing request to /opt/CSCOncs/migrate/restore/test
INFO: no staging url defined, using local space.        rval:2
```

証明書のインポート

Prime Infrastructure の信頼ストアに CA 証明書をインポートするには、Prime Infrastructure の **key importcacert** コマンドを使用します。

ncs key importcacert *aliasname ca-cert-filename* **repository** *repositoryname*

aliasname	この CA 証明書用に指定された短い名前。
ca-cert-filename	CA 証明書のファイル名。
repositoryname	ca-cert-filename がホストされている Prime Infrastructure で設定されたリポジトリ名。

次に、Prime Infrastructure サーバの信頼ストアに CA 証明書ファイルを適用する例を示します。

```
admin# ncs key importcacert alias1 cacertfile repository ncs-sftp-repo
```

（注）　このコマンドの適用後に、変更を有効にするために、**ncs stop** および **ncs start** コマンドを入力して、Prime Infrastructure サーバを再起動します。

証明書とキーのインポート

Prime Infrastructure に RSA キーと署名付き証明書をインポートするには、Prime Infrastructure の **key importkey** コマンドを使用します。

ncs key importkey *key-filename cert-filename* **repository** *repositoryname*

key-filename	RSA 秘密キーのファイル名。
cert-filename	証明書のファイル名。
repositoryname	key-file および cert-file がホストされている Prime Infrastructure で設定されたリポジトリ名。

次に、Prime Infrastructure サーバに新しい RSA キーおよび証明書ファイルを適用する例を示します。

```
admin# ncs key importkey keyfile certfile repository ncs-sftp-repo
```

（注）　このコマンドの適用後に、変更を有効にするために、**ncs stop** および **ncs start** コマンドを入力して、Prime Infrastructure サーバを再起動します。

署名付き証明書のインポート

Prime Infrastructure に RSA キーと署名付き証明書を適用するには、Prime Infrastructure の key importsignedcert コマンドを使用します。

ncs key importsignedcert *signed-cert-filename* **repository** *repositoryname*

次に、Prime Infrastructure サーバに署名付き証明書ファイルを適用する例を示します。

```
admin# ncs key importsingedcert signed-certfile repository ncs-sftp-repo
```

（注）　このコマンドの適用後に、変更を有効にするために、**ncs stop** および **ncs start** コマンドを入力して、Prime Infrastructure サーバを再起動します。

証明書のリストの表示

Prime Infrastructure 信頼ストアにあるすべての CA 証明書を表示するには、Prime Infrastructure の **key listcacerts** コマンドを使用します。

ncs key listcacerts

次に、Prime Infrastructure 信頼ストアにあるすべての CA 証明書をリストする例を示します。

```
admin# ncs key listcacerts

Certificate utnuserfirsthardwareca from CN=UTN-USERFirst-Hardware,
OU=http://www.example.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
Certificate gtecybertrust5ca from CN=GTE CyberTrust Root 5, OU="GTE CyberTrust Solutions,
Inc.", O=GTE Corporation, C=US
Certificate equifaxsecureebusinessca1 from CN=Equifax Secure eBusiness CA-1, O=Equifax
Secure Inc., C=US
Certificate thawtepersonalfreemailca from EMAILADDRESS=email@example.com, CN=Thawte
Personal Freemail CA, OU=Certification Services Division, O=Thawte Consulting, L=Cape
Town, ST=Western Cape, C=ZA
```

```
Certificate addtrustclass1ca from CN=AddTrust Class 1 CA Root, OU=AddTrust TTP Network,
O=AddTrust AB, C=SE
Certificate aolrootca1 from CN=America Online Root Certification Authority 1, O=America
Online Inc., C=US
Certificate geotrustuniversalca from CN=GeoTrust Universal CA, O=GeoTrust Inc., C=US
Certificate digicertglobalrootca from CN=DigiCert Global Root CA, OU=www.example.com,
O=DigiCert Inc, C=US
Certificate certumtrustednetworkca from CN=Certum Trusted Network CA, OU=Certum
Certification Authority, O=Unizeto Technologies S.A., C=PL
Certificate swisssignsilverg2ca from CN=SwissSign Silver CA - G2, O=SwissSign AG, C=CH
```

証明書の削除

Prime Infrastructure 信頼ストアにある CA 証明書を削除するには、Prime Infrastructure の key deletecacert コマンドを使用します。

ncs key deletecacert *aliasname*

次に、Prime Infrastructure 信頼ストアにある CA 証明書を削除する例を示します。

```
admin# ncs key deletecacert certumtrustednetworkca
Deleting certificate from trust store
```

関連資料

Prime Infrastructure コマンドの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/wireless/ncs/1.1/command/reference/cli11.html

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。