



# Cisco 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

この付録では、Cisco Prime Infrastructure を使用してサードパーティの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 Cisco 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。ここで説明する内容は、次のとおりです。

- 「前提条件」(P.C-15)
- 「使用されるコンポーネント」(P.C-15)
- 「証明書署名要求 (CSR)」(P.C-15)
- 「トラブルシューティング」(P.C-16)

## 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、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。

サポートされているハードウェアの詳細情報については、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/products/ps12239/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps12239/prod_release_notes_list.html)

## 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、デジタル ID 証明書を申請するために申請者が 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。

表 C-1 に、CSR を生成、インポート、表示、および削除するコマンドのリストを示します。

表 C-1 CSR コマンド

コマンド	説明
ncs key genkey	サードパーティ証明書を生成します。
ncs key importcacert	Prime Infrastructure の信頼ストアに CA 証明書をインポートします。
ncs key importsigncert	Prime Infrastructure に RSA キーおよび署名付き証明書をインポートします。
ncs key listcacerts	Prime Infrastructure 信頼ストアにあるすべての CA 証明書を一覧表示します。
ncs key deletcacert	Prime Infrastructure 信頼ストアにあるすべての CA 証明書を削除します。

上記の表に記載されているコマンドの詳細情報については、次の URL を参照してください。

[http://www.cisco.com/en/US/docs/wireless/prime\\_infrastructure/1.2/command/reference/cli12\\_appendix\\_011.html](http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.2/command/reference/cli12_appendix_011.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。