PKI の設定

この章では、Cisco NX-OS での公開キー インフラストラクチャ（PKI）のサポートについて説明します。PKI を使用すると、ネットワーク上で通信を安全に行うためのデジタル証明書をデバイスが入手して使用できるようになり、セキュア シェル（SSH）の管理性と拡張性も向上します。

この章は、次の項で構成されています。

- PKI の概要, on page 1
- PKI の注意事項と制約事項 （8 ページ）
- PKI のデフォルト設定, on page 9
- CA の設定とデジタル証明書, on page 9
- PKI の設定の確認, on page 30
- PKI の設定例, on page 30
- PKI に関する追加情報, on page 66
- Cisco SUDI 証明書チェーンを使用したデバイス構成証明 （66 ページ）

PKI の概要

ここでは、PKI について説明します。

CA とデジタル証明書

証明機関（CA）は証明書要求を管理して、ホスト、ネットワーク デバイス、ユーザなどの参加エンティティに証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

デジタル署名は、公開キー暗号法に基づいて、デバイスや個々のユーザをデジタル的に認証します。RSA 暗号化システムなどの公開キー暗号法では、各デバイスやユーザはキー ペアを持ち、これには秘密キーと公開キーが含まれています。秘密キーは秘密裡に保管し、これを知っているのは所有するデバイスまたはユーザだけです。一方、公開キーは誰もが知っているものです。これらのキーの一方で暗号化されたものは、他方のキーで復号化できます。署名は、送信者の秘密キーを使用してデータを暗号化したときに作成されます。受信側は、送信側の公開

キーを使用してメッセージを復号化することで、シグニチャを検証します。このプロセスは、受信者が送信者の公開キーのコピーを持っていて、これが本当に送信者のものであり、送信者を騙る他人のものではないことを高い確実性を持って知っていることを基盤としています。

デジタル証明書は、デジタル署名と送信者を結び付けるものです。デジタル証明書には、名前、シリアル番号、企業、部署または IP アドレスなど、ユーザまたはデバイスを特定する情報を含んでいます。また、エンティティの公開キーのコピーも含んでいます。証明書に署名する CA は、受信者が明示的に信頼する第三者機関であり、アイデンティティの正当性を立証し、デジタル証明書を作成します。

CA のシグニチャを検証するには、受信者は、CA の公開キーを認識している必要があります。一般的にはこのプロセスはアウトオブバンドか、インストール時に行われる操作によって処理されます。たとえば、通常の Web ブラウザでは、デフォルトで、複数の CA の公開キーが設定されています。

信頼モデル、トラストポイント、アイデンティティ CA

PKI の信頼モデルは、設定変更が可能な複数の信頼できる CA によって階層化されています。信頼できる CA のリストを使用して各参加デバイスを設定して、セキュリティプロトコルの交換の際に入手したピアの証明書がローカルに信頼できる CA のいずれかで発行されていた場合には、これを認証できるようにすることができます。Cisco NX-OS ソフトウェアでは、信頼できる CA の自己署名ルート証明書（または下位 CA の証明書チェーン）をローカルに保存しています。信頼できる CA のルート証明書（または下位 CA の場合には全体のチェーン）を安全に入手するプロセスを、*CA* 認証と呼びます。

信頼できる CA について設定された情報をトラストポイントと呼び、CA 自体もトラストポイント *CA* と呼びます。この情報は、CA 証明書（下位 CA の場合は証明書チェーン）と証明書取消確認情報で構成されています。

Cisco NX-OS デバイスは、トラストポイントに登録して、アイデンティティ証明書を入手し、キーペアと関連付けることができます。このトラストポイントをアイデンティティ *CA* と呼びます。

CA証明書の階層

セキュアサービスの場合、通常は複数の信頼できるCAがあります。CAは通常、すべてのホストにバンドルとしてインストールされます。NX-OS PKIインフラストラクチャは、証明書チェーンのインポートをサポートします。ただし、現在のCLIでは、一度に1つのチェーンをインストールできます。インストールするCAチェーンが複数ある場合、この手順は面倒です。これには、複数の中間CAとルートCAを含むCAバンドルをダウンロードする機能が必要です。

CA バンドルのインポート

crypto CA trustpointコマンドは、CA証明書、CRL、アイデンティティ証明書、およびキーペアを名前付きラベルにバインドします。これらの各エンティティに対応するすべてのファイルは、NX-OS certstoreディレクトリ（/ isan / etc / certstore）に保存され、トラストポイントラベルでタグ付けされます。

CA証明書にアクセスするには、SSLアプリケーションは標準のNX-OS証明書ストアをポイントし、SSL初期化中にCAパスとして指定するだけです。CAがインストールされているトラストポイントラベルを認識する必要はありません。

クライアントがアイデンティティ証明書にバインドする必要がある場合は、トラストポイントラベルをバインディングポイントとして使用する必要があります。

importpkcsコマンドは、トラストポイントラベルの下にCA証明書をインストールするように拡張されています。CAバンドルをインストールするようにさらに拡張できます。importコマンド構造が変更され、pkcs7形式のCAバンドルファイルを提供するために使用されるpkcs7オプションが追加されました。

Cisco NX-OS リリース 10.1(1) 以降、CA バンドルを解凍し、独自のラベルの下に各 CA チェーンをインストールするために、pkcs7 ファイル形式がサポートされています。ラベルは、メイントラストポイントラベルにインデックスを追加することによって形成されます。

一度インストールすると、バンドルへのすべてのCAチェーンの論理バインディングはありません。

PKCS7 形式での CA 証明書バンドルのインポート

複数の独立した証明書チェーンで構成される CA 証明書バンドルのインポートをサポートするために、 'pkcs7' のオプションが crypto import コマンドに導入されました。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**crypto ca import** <*baselabel*> **pksc7** <*uri0*> **force**	コマンドには2つの入力引数があります。Ca バンドルファイルであるソースファイルは、<*uri0*>、入力ファイルは pkcs7 形式である必要があります。これは cabundle ファイルであることを示します。 複数の証明書チェーンが cabundle から抽出されます。このコマンドは、CA証明書チェーンが接続された複数のトラストポイントを生成します。import コマンドは、グローバルCA バンドル構成と、生成された各トラストポイントごとの CA バンドル下位構成の、2 つの構成を生成します。

	コマンドまたはアクション	目的
		force オプションを指定すると、CA バンドルおよび関連するトラストポイント構成が削除され、同じバンドル名を持つ新しいCA バンドルがインポートされ、その CA バンドルに関連する新しいトラストポイント構成が生成されます。
ステップ 3	**crypto ca cabundle** <*bundle-name*>	bundle-name は、インポートの場合の baselabel と同じです。このコマンドの **no** 形式を使用すると、CA バンドル、トラストポイント、および関連する証明書チェーンを削除できます。 特定のベースラベル名で CA バンドルをインポートし、すべてのトラストポイントを生成した後、ユーザーが同じベースラベル名で import コマンドを再度実行しようとすると、CA バンドルがすでに存在するというエラーがスローされます。ユーザーは force オプションを使用して、既存の CA バンドルを変更できます。 サポートされる CA バンドルの最大数は 20 です。

ステップ 4	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	（任意） **show crypto ca certificates** 例： `switch# show crypto ca certificates`	CA 証明書を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

RSA のキー ペアとアイデンティティ証明書

アイデンティティ証明書を入手するには、1 つまたは複数の RSA キー ペアを作成し、各 RSA キー ペアと Cisco NX-OS デバイスが登録しようとしているトラストポイント CA を関連付けま

す。Cisco NX-OS デバイスは、CA ごとにアイデンティティを 1 つだけ必要とします。これは CA ごとに 1 つのキー ペアと 1 つのアイデンティティ証明書で構成されています。

Cisco NX-OS ソフトウェアでは、設定変更が可能なキーのサイズ（またはモジュラス）で RSA キー ペアを作成できます。デフォルトのキーのサイズは 512 です。また、RSA キー ペアのラベルも設定できます。デフォルトのキー ラベルは、デバイスの完全修飾ドメイン名（FQDN）です。

トラストポイント、RSA キー ペア、およびアイデンティティ証明書の関係を要約したものを次に示します。

- トラストポイントとは、Cisco NX-OS デバイスが、あらゆるアプリケーション（SSH など）のピア証明書用に信頼する特定の CA です。
- Cisco NX-OS デバイスでは、デバイス上に多くのトラストポイントを置くことができ、デバイス上のすべてのアプリケーションは、任意のトラストポイント CA によって発行されたピア証明書を信頼できます。
- トラストポイントは特定のアプリケーション用に限定されません。
- Cisco NX-OS デバイスは、トラストポイントに対応する CA に登録して、アイデンティティ証明書を入手します。デバイスは複数のトラストポイントに登録できます。これは、各トラストポイントから異なるアイデンティティ証明書を入手できることを意味します。アイデンティティ証明書は、発行する CA によって証明書に指定されている目的に応じてアプリケーションで使用します。証明書の目的は、証明書の拡張機能として証明書に保存されます。
- トラストポイントに登録するときには、証明を受ける RSA キー ペアを指定する必要があります。このキーペアは、登録要求を作成する前に作成されていて、トラストポイントに関連付けられている必要があります。トラストポイント、キーペア、およびアイデンティティ証明書との間のアソシエーション（関連付け）は、証明書、キーペア、またはトラストポイントが削除されて明示的になくなるまで有効です。
- アイデンティティ証明書のサブジェクト名は、Cisco NX-OS デバイスの完全修飾ドメイン名です。
- デバイス上には 1 つまたは複数の RSA キー ペアを作成でき、それぞれを 1 つまたは複数のトラストポイントに関連付けることができます。しかし、1 つのトラストポイントに関連付けられるキー ペアは 1 だけです。これは 1 つの CA からは 1 つのアイデンティティ証明書しか入手できないことを意味します。
- Cisco NX-OS デバイスが複数のアイデンティティ証明書を（それぞれ別の CA から）入手する場合は、アプリケーションがピアとのセキュリティ プロトコルの交換で使用する証明書は、アプリケーション固有のものになります。
- 1 つのアプリケーションに 1 つまたは複数のトラストポイントを指定する必要はありません。証明書の目的がアプリケーションの要件を満たしていれば、どのアプリケーションもあらゆるトラストポイントで発行されたあらゆる証明書を使用できます。
- あるトラストポイントから複数のアイデンティティ証明書を入手したり、あるトラストポイントに複数のキー ペアを関連付ける必要はありません。ある CA はあるアイデンティ

ティ（または名前）を1回だけ証明し、同じ名前で複数の証明書を発行することはありません。ある CA から複数のアイデンティティ証明書を入手する必要があり、またその CA が同じ名前で複数の証明書の発行を許可している場合は、同じ CA 用の別のトラストポイントを定義して、別のキー ペアを関連付け、証明を受ける必要があります。

複数の信頼できる CA のサポート

Cisco NX-OS デバイスは、複数のトラストポイントを設定して、それぞれを別の CA に関連付けることにより、複数の CA を信頼できるようになります。信頼できる CA が複数あると、ピアに証明書を発行した特定の CA にデバイスを登録する必要がなくなります。代わりに、ピアが信頼する複数の信頼できる CA をデバイスに設定できます。すると、Cisco NX-OS デバイスは設定されている信頼できる CA を使用して、ピアから受信した証明書で、ピア デバイスの ID で定義されている CA から発行されたものではないものを検証できるようになります。

PKI の登録のサポート

登録とは、SSH などのアプリケーションに使用するデバイス用のアイデンティティ証明書を入手するプロセスです。これは、証明書を要求するデバイスと、認証局の間で生じます。

Cisco NX-OS デバイスでは、PKI 登録プロセスを実行する際に、次の手順を取ります。

- デバイスで RSA の秘密キーと公開キーのペアを作成します。
- 標準の形式で証明書要求を作成し、CA に送ります。

Note 要求が CA で受信されたとき、CA サーバでは CA アドミニストレータが登録要求を手動で承認しなくてはならない場合があります。

- 発行された証明書を CA から受け取ります。これは CA の秘密キーで署名されています。
- デバイスの不揮発性のストレージ領域（ブートフラッシュ）に証明書を書き込みます。

カットアンドペーストによる手動での登録

Cisco NX-OS ソフトウェアでは、手動でのカットアンドペーストによる証明書の取得と登録をサポートしています。カットアンドペーストによる登録とは、証明書要求をカットアンドペーストして、デバイスと CA 間で認証を行うことを意味します。

手動による登録プロセスでカットアンドペーストを使用するには、次の手順を実行する必要があります。

- 証明書登録要求を作成します。これは Cisco NX-OS デバイスで base64 でエンコードされたテキスト形式として表示されます。

- エンコードされた証明書要求のテキストを E メールまたは Web フォームにカットアンドペーストし、CA に送ります。
- 発行された証明書（base64 でエンコードされたテキスト形式）を CA から E メールまたは Web ブラウザによるダウンロードで受け取ります。
- 証明書のインポート機能を使用して、発行された証明書をデバイスにカットアンドペーストします。

複数の RSA キー ペアとアイデンティティ CA のサポート

複数のアイデンティティ CA を使用すると、デバイスが複数のトラストポイントに登録できるようになり、その結果、別々の CA から複数のアイデンティティ証明書が発行されます。この機能によって、Cisco NX-OS デバイスは複数のピアを持つ SSH およびアプリケーションに、これらのピアに対応する CA から発行された証明書を使用して参加できるようになります。

また複数の RSA キー ペアの機能を使用すると、登録している各 CA ごとの別々のキー ペアをデバイスで持てるようになります。これは、他の CA で指定されているキーの長さなどの要件と競合することなく、各 CA のポリシー要件に適合させることができます。デバイスでは複数の RSA キー ペアを作成して、各キー ペアを別々のトラストポイントに関連付けることができます。したがって、トラストポイントに登録するときには、関連付けられたキーペアを証明書要求の作成に使用します。

ピア証明書の検証

PKI では、Cisco NX-OS デバイスでのピア証明書の検証機能をサポートしています。Cisco NX-OS では、SSH などのアプリケーションのためのセキュリティ交換の際にピアから受け取った証明書を検証します。アプリケーションはピア証明書の正当性を検証します。Cisco NX-OS ソフトウェアでは、ピア証明書の検証の際に次の手順を実行します。

- ピア証明書がローカルの信頼できる CA のいずれかから発行されていることを確認します。
- ピア証明書が現在時刻において有効であること（期限切れでない）ことを確認します。
- ピア証明書が、発行した CA によって取り消されていないことを確認します。

取消確認については、Cisco NX-OS ソフトウェアでは証明書失効リスト（CRL）をサポートしています。トラストポイント CA ではこの方法を使用して、ピア証明書が取り消されていないことを確認できます。

証明書の取消確認

Cisco NX-OS ソフトウェアでは、CA 証明書の取消のステータスを確認できます。アプリケーションでは、指定した順序に従って取消確認メカニズムを使用できます。CRL、NDcPP:OCSP for Syslog、なし、またはこれらの方式の組み合わせを指定できます。

CRL のサポート

CA では証明書失効リスト（CRL）を管理して、有効期限前に取り消された証明書についての情報を提供します。CA ではCRL をリポジトリで公開して、発行したすべての証明書の中にダウンロード用の公開 URL 情報を記載しています。ピア証明書を検証するクライアントは、発行した CA から最新の CRL を入手して、これを使用して証明書が取り消されていないかどうかを確認できます。クライアントは、自身の信頼できるCAのすべてまたは一部のCRLをローカルにキャッシュして、その CRL が期限切れになるまで必要に応じて使用することができます。

Cisco NX-OS ソフトウェアでは、先にダウンロードしたトラストポイントについての CRL を手動で設定して、これをデバイスのブートフラッシュ（cert-store）にキャッシュすることができます。ピア証明書の検証の際、Cisco NX-OS ソフトウェアは、CRL がすでにローカルにキャッシュされていて、取消確認でこの CRL を使用するよう設定されている場合にだけ、発行した CA からの CRL をチェックします。それ以外の場合、Cisco NX-OS ソフトウェアでは CRL チェックを実行せず、他の取消確認方式が設定されている場合を除き、証明書は取り消されていないと見なします。

NDcPP：syslog の OCSP

Online Certificate Status Protocol（OCSP）は、ピアがこの失効情報を取得し、それを検証して証明書失効ステータスを確認する必要がある場合に、証明書失効をチェックする方法です。この方式では、クラウドを介してOCSPレスポンダに到達するピアの機能、または証明書失効情報を取得する証明書送信者のパフォーマンスによって、証明書失効ステータスが制限されます。

リモート syslog サーバが OCSP レスポンダ URL を持つ証明書を共有すると、クライアントはサーバ証明書を外部OCSP レスポンダ（CA）サーバに送信します。CA サーバはこの証明書を検証し、有効な証明書か失効した証明書かを確認します。この場合、クライアントは失効した証明書リストをローカルに保持する必要はありません。

証明書と対応するキー ペアのインポートとエクスポート

CA 認証と登録のプロセスの一環として、下位 CA 証明書（または証明書チェーン）とアイデンティティ証明書を標準の PEM（base64）形式でインポートできます。

トラストポイントでのアイデンティティ情報全体を、パスワードで保護される PKCS#12 標準形式でファイルにエクスポートできます。このファイルは、後で同じデバイス（システム クラッシュの後など）や交換したデバイスににインポートすることができます。PKCS#12 ファイル内の情報は、RSA キー ペア、アイデンティティ証明書、および CA 証明書（またはチェーン）で構成されています。

PKI の注意事項と制約事項

PKI に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイスに設定できるキー ペアの最大数は 16 です。

- Cisco NX-OS デバイスで宣言できるトラスト ポイントの最大数は 16 です。
- Cisco NX-OS デバイスに設定できるアイデンティティ証明書の最大数は 16 です。
- CA 証明書チェーン内の証明書の最大数は 10 です。
- ある CA に対して認証できるトラストポイントの最大数は 10 です。
- 設定のロールバックでは PKI の設定はサポートしていません。
- Cisco NX-OS リリース 9.3 (5) 以降では、Cisco NX-OS ソフトウェアは NDcPP: OCSP for Syslog をサポートしています。
- Cisco NX-OS リリース 10.3(3)F 以降、Cisco Nexus スイッチで証明書を生成およびインポートするために、楕円曲線暗号（ECC）キー ペアのサポートが提供されます。

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

PKI のデフォルト設定

次の表に、PKI パラメータのデフォルト設定を示します。

***Table 1: PKI* パラメータのデフォルト値**

パラメータ	デフォルト
トラスト ポイント	なし
RSA キー ペア	なし
RSA キー ペアのラベル	デバイスの FQDN
RSA キー ペアのモジュール	512
RSA キー ペアのエクスポートの可否	イネーブル
取消確認方式	CRL

CA の設定とデジタル証明書

ここでは、Cisco NX-OS デバイス上で CA とデジタル証明書が相互に連携して動作するようにするために、実行が必要な作業について説明します。

ホスト名と IP ドメイン名の設定

デバイスのホスト名または IP ドメイン名をまだ設定していない場合は、設定する必要があります。これは、Cisco NX-OS ソフトウェアでは、アイデンティティ証明書のサブジェクトとして完全修飾ドメイン名（FQDN）を使用するためです。また、Cisco NX-OS ソフトウェアでは、キーの作成の際にラベルが指定されていないと、デバイスの FQDN をデフォルトのキー ラベルとして使用します。たとえば、DeviceA.example.com という名前の証明書は、DeviceA というデバイスのホスト名と example.com というデバイスの IP ドメイン名に基づいています。

Caution 証明書を作成した後にホスト名または IP ドメイン名を変更すると、証明書が無効になります。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**hostname** *hostname* **Example:** `switch(config)# hostname DeviceA`	デバイスのホスト名を設定します。
ステップ 3	**ip domain-name** *name* [**use-vrf** *vrf-name*] **Example:** `DeviceA(config)# ip domain-name example.com`	デバイスの IP ドメイン名を設定します。VRF 名が指定されていないと、このコマンドではデフォルトの VRF を使用します。

ステップ 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 5	(Optional) **show hosts** **Example:** `switch# show hosts`	IP ドメイン名を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

RSA キー ペアの生成

RSA キーペアは、アプリケーション向けのセキュリティ プロトコルの交換時に、セキュリティ ペイロードの署名、暗号化、および復号化のために作成します。デバイスのための証明書を取得する前に、RSA キー ペアを作成する必要があります。

Cisco NX-OS リリース 9.3(3) 以降では、Cisco NX-OS デバイスをトラスト ポイント CA に関連付ける前に、明示的に RSA キー ペアを生成する必要があります。Cisco NX-OS リリース 9.3(3) よりも前では、使用できない場合、RSAキー ペアは自動生成されます。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**crypto key generate rsa** [**label** *label-string*] [**exportable**] [**modulus** *size*] **Example:** `switch(config)# crypto key generate rsa exportable`	RSA キー ペアを生成します。デバイスに設定できるキー ペアの最大数は 16 です。 ラベル文字列には、大文字と小文字を区別して、最大 64 文字の英数字で値を指定します。デフォルトのラベル文字列は、ピリオド文字（.）で区切ったホスト名と FQDN です。 有効なモジュラスの値は 512、768、1024、1536、2048、3072 および 4096 です。デフォルトのモジュラスのサイズは 512 です。 **Note** 適切なキーのモジュラスを決定する際には、Cisco NX-OS デバイスと CA（登録を計画している対象）のセキュリティ ポリシーを考慮する必要があります。 デフォルトでは、キーペアはエクスポートできません。エクスポート可能なキーペアだけ、PKCS#12 形式でエクスポートできます。 **Caution** キー ペアのエクスポートの可否は変更できません。

	Command or Action	Purpose

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	(Optional) **show crypto key mypubkey rsa** **Example:** `switch# show crypto key mypubkey rsa`	作成したキーを表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ECC キー ペアの生成

ECC キーペアは、アプリケーション向けのセキュリティプロトコルの交換時に、セキュリティペイロードの署名、暗号化、および復号化のために作成します。デバイスのための証明書を取得する前に、ECC キー ペアを作成する必要があります。ECC キーは、同じ長さの場合、RSA キーと比較して強力です。

Cisco NX-OS リリース 10.3(3)F リリース以降、ECC キー ペアを生成して、Cisco NX-OS デバイスをトラストポイント CA に関連付けることができます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto key generate ecc** [**label** *ecc-key-label*] [**exportable**] [**modulus** *size*] 例： `switch(config)# crypto key generate ecc exportable modulus 224`	ECC キーペアを生成します。デバイスに設定できるキー ペアの最大数は 16 です。 ラベル文字列には最大 64 文字の英数字で値を指定します。大文字と小文字は区別されます。デフォルトのラベル文字列は、ピリオド文字（.）で区切ったホスト名と FQDN です。

	コマンドまたはアクション	目的
		有効なモジュラス値は、224、384、および 521 です。デフォルトのモジュラスのサイズは 224 です。 （注） 適切なキーのモジュラスを決定する際には、Cisco NX-OS デバイスと CA（登録を計画している対象）のセキュリティポリシーを考慮する必要があります。 デフォルトでは、キーペアはエクスポートできません。エクスポート可能なキーペアだけ、PKCS#12 形式でエクスポートできます。 **注意** キー ペアのエクスポートの可否は変更できません。
ステップ 3	**no crypto key generate ecc** [**label** *ecc-key-label*] 例： `switch(config)# no crypto key generate ecc label label-name`	ECC キーを削除します。

ステップ 4	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	（任意） **show crypto key mypubkey ecc** 例： `switch# show crypto key mypubkey ecc`	作成した ECC キーを表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

トラストポイント CA のアソシエーションの作成

Cisco NX-OS デバイスとトラスト ポイント CA を関連付ける必要があります。

Before you begin

RSA キー ペアを作成します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**crypto ca trustpoint** *name*
	Example:
	`switch(config)# crypto ca trustpoint admin-ca`
	`switch(config-trustpoint)#`
		デバイスが信頼するトラストポイント CA を宣言し、トラストポイント コンフィギュレーション モードを開始します。
		Note
		設定できるトラストポイントの最大数は 50 です。

ステップ 3	**cabundle** *baselabel* **Example:** `switch(config-trustpoint)# cabundle test`	特定の CA バンドル下でトラストポイントをグループ化します。このコマンドの **No** 形式を使用すると、CA バンドルからトラストポイントが切り離されます。このコマンドは、トラストポイントを既存の CA バンドルに関連付けます。新しい CA バンドルは設定しません。
ステップ 4	**enrollment terminal** **Example:** `switch(config-trustpoint)# enrollment terminal`	手動でのカットアンドペーストによる証明書の登録をイネーブルにします。デフォルトではイネーブルになっています。 **Note** Cisco NX-OS ソフトウェアでは、手動でのカットアンドペースト方式による証明書の登録だけをサポートしています。
ステップ 5	**rsakeypair** *label* **Example:** `switch(config-trustpoint)# rsakeypair SwitchA`	RSA キー ペアのラベルを指定して、このトラストポイントを登録用に関連付けます。 **Note** CA ごとに 1 つの RSA キー ペアだけを指定できます。

	Command or Action	Purpose

ステップ 6	**exit**
	Example:
	`switch(config-trustpoint)# exit`
	`switch(config)#`
		トラストポイント コンフィギュレーション モードを終了します。

ステップ 7	(Optional) **show crypto ca trustpoints** **Example:** `switch(config)# show crypto ca trustpoints`	トラストポイントの情報を表示します。
ステップ 8	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

RSA キー ペアの生成 （11 ページ）

証明書マッピングのフィルタの設定

認証に使用される CA 証明書を検証するためのマッピングのフィルタを設定できます。マッピングのフィルタは、CA 証明書をユーザ名と照合するために使用されます。

Cisco NX-OS は次の証明書マッピングのフィルタをサポートします。

- %username%：ユーザのログイン名が代入されます。
- %hostname%：ピアのホスト名が代入されます。

始める前に

証明書認証の cert-store を設定します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto certificatemap mapname** *map-name* 例：	新しいフィルタ マップを作成します。

	コマンドまたはアクション	目的
	`switch(config)# crypto certificatemap mapname filtermap1`	

ステップ 3	**filter** [**subject-name** *subject-name* | **altname-email** *e-mail-ID* | **altname-upn** *user-principal-name*]
	例：
	`switch(config-certmap-filter)# filter altname-upn %username%@cisco.com`
		フィルタ マップ内で証明書マッピングのフィルタを 1 つまたは複数設定します。これらの証明書のフィールド属性は、フィルタでサポートされています。証明書は、マップで設定されたすべてのフィルタを通過した場合に検証にパスします。
		• subject-name：必要なサブジェクト名です。LDAP の認定者名（DN）文字列の形式で指定します。次に例を示します。
		`filter subject-name CN=%username%`
		または
		`filter subject-name /C=IN/ST=KA/L=BLR/O=CISCO/OU=ABC/CN=%username%`
		• altname-email：サブジェクト名の代わりに証明書に含まれている必要がある E メール アドレスです。次に例を示します。
		`filter altname-email %username%@cisco.com`
		• altname-upn：サブジェクト名の代わりに証明書に含まれている必要があるプリンシパル名です。次に例を示します。
		`filter altname-upn %username%@%hostname%`
		証明書は、マップで設定されたすべてのフィルタを通過した場合に検証にパスします。

ステップ 4	**exit** 例： `switch(config-certmap-filter)# exit switch(config)#`	証明書マッピングのフィルタ コンフィギュレーション モードを終了します。
ステップ 5	（任意） **crypto cert ssh-authorize** [**default** | *issuer-CAname*] [**map** *map-name1* [*map-name2*]]	セキュア シェル（SSH）プロトコル用の証明書マッピングのフィルタを設定します。SSH 認証用のデフォルトのフィ

	コマンドまたはアクション	目的
	例： `switch(config)# crypto cert ssh-authorize default map filtermap1`	ルタ マップを使用するか、CA 証明書の発行元を指定できます。デフォルトのマップを使用しない場合は、認証用のフィルタ マップを 1 つまたは 2 つ指定できます。 CA 証明書の発行元を指定した場合、ユーザ アカウントにバインドされた証明書が検証され、設定されたマップのいずれかを通過すると検証にパスします。
ステップ 6	（任意） **show crypto certificatemap** 例： `switch(config)# show crypto certificatemap`	証明書マッピングのフィルタを表示します。
ステップ 7	（任意） **show crypto ssh-auth-map** 例： `switch(config)# show crypto ssh-auth-map`	SSH 認証用に設定されたマッピングのフィルタを表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

CA の認証

CA が Cisco NX-OS デバイスに対して認証されると、CA を信頼するプロセスの設定が完了します。まず、PEM 形式の CA の自己署名証明書を入手し、Cisco NX-OS デバイスを CA に対して認証する必要があります。この証明書には、CA の公開キーが含まれています。この CA の証明書は自己署名（CA が自身の証明書に署名したもの）であるため、CA の公開キーは、CA アドミニストレータに連絡し、CA 証明書のフィンガープリントを比較して手動で認証する必要があります。

Note 認証する CA が他の CA の下位 CA である場合、認証する CA は自己署名 CA ではありません。その上位の CA がさらに別の CA の下位である場合もあります。最終的には自己署名 CA に到達します。このタイプの CA 証明書を、認証する CA の *CA* 証明書チェーンと呼びます。この場合は、CA 認証の際に、証明書チェーン内のすべての CA の CA 証明書の完全なリストを入力する必要があります。CA 証明書チェーン内の証明書の最大数は 10 です。

Before you begin

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**crypto ca authenticate** *name* **pemfile** *uri0*
	Example:
	`switch(config)# crypto ca authenticate admin-ca`
	`input (cut & paste) CA certificate (chain) in PEM format;`
	`end the input with a line containing only END OF INPUT :`
	`-----BEGIN CERTIFICATE-----`
	`MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB`
	`kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO`
	`MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE`
	`ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD`
	`QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN`
	`AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth`
	`cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG`
	`A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN`
	`AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI`
	`OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E`
	`BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ`
	`GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs`
	`L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv`
	`bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB`
	`BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea`
	`NBG7E0oN66zex0EOEfG1Vs6mXp1//w==`
	`-----END CERTIFICATE-----`
	`END OF INPUT`
	`Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12`
	`Do you accept this certificate? [yes/no]: yes`
		CA の証明書をカットアンドペーストするようプロンプトが表示されます。CA を宣言したときに使用した名前と同じ名前を使用します。
		また、CAチェーンを検証し、指定されたトラストポイントに直接接続します。
		ある CA に対して認証できるトラストポイントの最大数は 10 です。
		Note
		下位 CA の認証の場合、Cisco NX-OS ソフトウェアでは、自己署名 CA に到達する CA 証明書の完全なチェーンが必要になります。これは証明書の検証や PKCS#12 形式でのエクスポートに CA チェーンが必要になるためです。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	(Optional) **show crypto ca trustpoints** **Example:** `switch# show crypto ca trustpoints`	トラストポイント CA の情報を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

トラストポイント CA のアソシエーションの作成 （13 ページ）

証明書取消確認方法の設定

クライアント（SSH ユーザなど）とのセキュリティ交換の際に、Cisco NX-OS デバイスは、クライアントから送られたピア証明書の検証を実行します。検証プロセスには、証明書の取消状況の確認が含まれます。

CA からダウンロードした CRL を確認するよう、デバイスに設定できます。CRL のダウンロードとローカルでの確認では、ネットワーク上にトラフィックは発生しません。しかし、証明書がダウンロードとダウンロードの中間で取り消され、デバイス側ではその取り消しに気付かない場合も考えられます。

Before you begin

CA を認証します。

CRL チェックを使用する場合は、CRL が設定済みであることを確認します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**crypto ca trustpoint** *name*
	Example:
	`switch(config)# crypto ca trustpoint admin-ca`
	`switch(config-trustpoint)#`
		トラストポイント CA を指定し、トラストポイント コンフィギュレーション モードを開始します。

ステップ 3	**revocation-check** {**crl** [**none**] | **none**} **Example:** `switch(config-trustpoint)# revocation-check none`	証明書取消確認方法を設定します。デフォルトの方式は **crl**. です。 Cisco NX-OS ソフトウェアでは、指定した順序に従って証明書取消方式を使用します。

	Command or Action	Purpose

ステップ 4	**exit**
	Example:
	`switch(config-trustpoint)# exit`
	`switch(config)#`
		トラストポイント コンフィギュレーション モードを終了します。

ステップ 5	(Optional) **show crypto ca trustpoints** **Example:** `switch(config)# show crypto ca trustpoints`	トラストポイント CA の情報を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

CA の認証 （17 ページ）
CRL の設定 （26 ページ）

証明書要求の作成

使用する各デバイスの RSA キー ペア用に、対応するトラストポイント CA からアイデンティティ証明書を入手するために、要求を作成する必要があります。その後、表示された要求を CA 宛の E メールまたは Web サイトのフォームにカットアンドペーストします。

Before you begin

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**crypto ca enroll** *name* **Example:** `switch(config)# crypto ca enroll admin-ca`	認証した CA に対する証明書要求を作成します。 **Note**

	Command or Action	Purpose
	Create the certificate request .. Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password:nbv123 The subject name in the certificate will be: DeviceA.cisco.com Include the switch serial number in the subject name? [yes/no]: no Include an IP address in the subject name [yes/no]: yes ip address:172.22.31.162 The certificate request will be displayed... -----BEGIN CERTIFICATE REQUEST----- MIIBozCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY 0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8 8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0= -----END CERTIFICATE REQUEST-----	チャレンジ パスワードを記憶しておいてください。このパスワードは設定と一緒に保存されません。証明書を取り消す必要がある場合には、このパスワードを入力する必要があります。
ステップ 3	**exit** **Example:** switch(config-trustpoint)# exit switch(config)#	トラストポイントコンフィギュレーション モードを終了します。
ステップ 4	(Optional) **show crypto ca certificates** **Example:** switch(config)# show crypto ca certificates	CA 証明書を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

トラストポイント CA のアソシエーションの作成 （13 ページ）

アイデンティティ証明書のインストール

アイデンティティ証明書は、CA から E メールまたは Web ブラウザ経由で base64 でエンコードされたテキスト形式で受信できます。CAから入手したアイデンティティ証明書を、エンコードされたテキストをカットアンドペーストしてインストールする必要があります。

Before you begin

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**crypto ca import** *name* **certificate**
	
	Example:
	`switch(config)# crypto ca import admin-ca certificate`
	`input (cut & paste) certificate in PEM format:`
	`-----BEGIN CERTIFICATE-----`
	`MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G`
	`CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD`
	`VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz`
	`Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w`
	`NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu`
	`Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C`
	`dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UbiyeCYE8ylncWyw5E08rJ47`
	`glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb`
	`x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw`
	`GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR`
	`bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW`
	`pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE`
	`BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w`
	`DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh`
	`cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6`
	`Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6`
	`Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH`
	`AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl`
	`LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4`
	`XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF`
	`AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw`
	`E36cIZu4WsExREqxbTk8ycx7V5o=`
	`-----END CERTIFICATE-----`
		admin-ca という名前の CA に対するアイデンティティ証明書をカットアンドペーストするよう、プロンプトが表示されます。
		
		デバイスに設定できるアイデンティティ証明書の最大数は 16 です。

ステップ 3	**exit** **Example:**	設定モードを終了します。

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
ステップ 4	(Optional) **show crypto ca certificates** **Example:** `switch# show crypto ca certificates`	CA 証明書を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

トラストポイント CA のアソシエーションの作成 （13 ページ）

トラストポイントの設定がリブート後も維持されていることの確認

トラストポイントの設定が、Cisco NX-OS デバイスのリブート後も維持されていることを確認できます。

トラストポイントの設定は、通常の Cisco NX-OS デバイスの設定であり、スタートアップ コンフィギュレーションに確実にコピーした場合にだけ、システムのリブート後も維持されます。トラスト ポイント設定をスタートアップ コンフィギュレーションにコピーしておけば、トラスト ポイントに関連する証明書、キー ペア、および CRL が自動的に保持されます。逆に、トラスト ポイントがスタートアップ コンフィギュレーションにコピーされていないと、証明書、キー ペア、および関連 CRL は保持されません。リブート後に、対応するトラスト ポイント設定が必要になるからです。設定した証明書、キー ペア、および CRL を確実に保持するために、必ず、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてください。また、証明書またはキーペアを削除した後は実行コンフィギュレーションを保存して、削除が永続的に反映されるようにしてください。

トラストポイントに関連付けられた証明書と CRL は、そのトラストポイントがすでにスタートアップ コンフィギュレーションに保存されていれば、インポートした時点で（つまりスタートアップ コンフィギュレーションにコピーしなくても）維持されるようになります。

パスワードで保護したアイデンティティ証明書のバックアップを作成して、これを外部のサーバに保存することを推奨します。

Note コンフィギュレーションを外部サーバにコピーすると、証明書およびキー ペアも保存されます。

Related Topics

PKCS 12 形式でのアイデンティティ情報のエクスポート （24 ページ）

PKCS 12 形式でのアイデンティティ情報のエクスポート

アイデンティティ証明書を、トラストポイントの RSA キー ペアや CA 証明書（または下位 CA の場合はチェーン全体）と一緒に PKCS#12 ファイルにバックアップ目的でエクスポートすることができます。デバイスのシステム クラッシュからの復元の際や、スーパーバイザ モジュールの交換の際には、証明書や RSA キー ペアをインポートすることができます。

Note エクスポートの URL を指定するときに使用できるのは、bootflash:*filename* という形式だけです。

Before you begin

CA を認証します。

アイデンティティ証明書をインストールします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**crypto ca export** *name* **pkcs12** **bootflash:***filename password* **Example:** `switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123`	アイデンティティ証明書と、トラストポイント CA の対応するキー ペアと CA 証明書をエクスポートします。パスワードには、大文字と小文字を区別して、最大 128 文字の英数字で値を指定します。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**copy booflash:***filename scheme***://***server/* [*url /*]*filename* **Example:** `switch# copy bootflash:adminid.p12 tftp:adminid.p12`	PKCS#12 形式のファイルをリモート サーバにコピーします。 *scheme* 引数に対しては、**tftp:**、**ftp:**、**scp:**、または **sftp:** を入力できます。*server* 引数は、リモート サーバのアドレスまたは名前であり、*url* 引数はリモート サーバにあるソース ファイルへのパスです。

	Command or Action	Purpose
		server、*url*、および *filename* の各引数は、大文字小文字を区別して入力します。

Related Topics

RSA キー ペアの生成 （11 ページ）
CA の認証 （17 ページ）
アイデンティティ証明書のインストール （22 ページ）

PKCS 12または PKCS 7 フォーマットで ID 情報のインポート

デバイスのシステム クラッシュからの復元の際や、スーパーバイザ モジュールの交換の際には、証明書や RSA キー ペアをインポートすることができます。

Note インポートの URL を指定するときに使用できるのは、bbootflash:*filename* fという形式だけです。

Before you begin

CA 認証によってトラストポイントに関連付けられている RSA キー ペアがないこと、およびトラストポイントに関連付けられている CA がないことを確認して、トラストポイントが空であるようにします。

Procedure

	Command or Action	Purpose
ステップ 1	**copy** *scheme*:// *server*/[*url* /]*filename* **bootflash:***filename* **Example:** `switch# copy tftp:adminid.p12 bootflash:adminid.p12`	PKCS#12 形式のファイルをリモート サーバからコピーします。 *scheme* 引数に対しては、**tftp:**、**ftp:**、**scp:**、または **sftp:** を入力できます。*server* 引数は、リモート サーバのアドレスまたは名前であり、*url* 引数はリモート サーバにあるソース ファイルへのパスです。 *server*、*url*、および *filename* の各引数は、大文字小文字を区別して入力します。
ステップ 2	**configure terminal** **Example:**	グローバル コンフィギュレーション モードを開始します

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
ステップ 3	**crypto ca import** *name* **[pksc12 | pkcs7] bootflash:***filename* **Example:** `switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123`	アイデンティティ証明書と、トラストポイントCAの対応するキーペアとCA証明書をインポートします。

ステップ 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	(Optional) **show crypto ca certificates** **Example:** `switch# show crypto ca certificates`	CA 証明書を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

CRL の設定

トラストポイントからダウンロードしたCRLを手動で設定することができます。Cisco NX-OSソフトウェアでは、CRLをデバイスのブートフラッシュ（cert-store）にキャッシュします。ピア証明書の検証の際、Cisco NX-OSソフトウェアが発行したCAからのCRLをチェックするのは、CRLをデバイスにダウンロードしていて、このCRLを使用する証明書取消確認を設定している場合だけです。

Before you begin

証明書取消確認がイネーブルになっていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	**copy** *scheme*:[*//server/*[*url /*]]*filename* **bootflash:***filename* **Example:** `switch# copy tftp:adminca.crl bootflash:adminca.crl`	リモート サーバからCRLをダウンロードします。 *scheme* 引数に対しては、**tftp:**、**ftp:**、**scp:**、または **sftp:** を入力できます。*server* 引数は、リモート サーバのアドレ

	Command or Action	Purpose
		スまたは名前であり、*url* 引数はリモート サーバにあるソース ファイルへのパスです。 *server*、*url*、および *filename* の各引数は、大文字小文字を区別して入力します。

ステップ 2	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 3	**crypto ca crl request** *name* **bootflash:***filename* **Example:** `switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl`	ファイルで指定されている CRL を設定するか、現在の CRL と置き換えます。

ステップ 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 5	(Optional) **show crypto ca crl** *name* **Example:** `switch# show crypto ca crl admin-ca`	CA の CRL 情報を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

CA の設定からの証明書の削除

トラストポイントに設定されているアイデンティティ証明書やCA証明書を削除できます。最初にアイデンティティ証明書を削除し、その後で CA 証明書を削除します。アイデンティティ証明書を削除した後で、RSA キー ペアとトラストポイントの関連付けを解除できます。証明書の削除は、期限切れになった証明書や取り消された証明書、破損した（あるいは破損したと思われる）キー ペア、現在は信頼されていない CA を削除するために必要です。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**crypto ca trustpoint** *name*
	Example:
	`switch(config)# crypto ca trustpoint admin-ca`
	`switch(config-trustpoint)#`
		トラストポイントCAを指定し、トラストポイント コンフィギュレーション モードを開始します。

ステップ 3	**delete ca-certificate** **Example:** `switch(config-trustpoint)# delete ca-certificate`	CA 証明書または証明書チェーンを削除します。
ステップ 4	**delete certificate** [**force**] **Example:** `switch(config-trustpoint)# delete certificate`	アイデンティティ証明書を削除します。 削除しようとしているアイデンティティ証明書が証明書チェーン内の最後の証明書である場合や、デバイス内の唯一のアイデンティティ証明書である場合は、**force** オプションを使用する必要があります。この要件は、証明書チェーン内の最後の証明書や唯一のアイデンティティ証明書を誤って削除してしまい、アプリケーション（SSH など）で使用する証明書がなくなってしまうことを防ぐために設けられています。

ステップ 5	**exit**
	Example:
	`switch(config-trustpoint)# exit`
	`switch(config)#`
		トラストポイントコンフィギュレーション モードを終了します。

ステップ 6	(Optional) **show crypto ca certificates** [*name*] **Example:** `switch(config)# show crypto ca certificates admin-ca`	CA の証明書情報を表示します。

	Command or Action	Purpose
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco NX-OSデバイスからの RSA キー ペアの削除

RSAキーペアが何らかの理由で破損し、現在は使用されてないと見られるときには、そのRSAキー ペアを Cisco NX-OS デバイスから削除することができます。

Note デバイスからRSAキーペアを削除した後、CAアドミニストレータに、そのCAにあるこのデバイスの証明書を取り消すよう依頼します。その証明書を最初に要求したときに作成したチャレンジ パスワードを入力する必要があります。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**crypto key zeroize rsa** *label* **Example:** `switch(config)# crypto key zeroize rsa MyKey`	RSA キー ペアを削除します。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	(Optional) **show crypto key mypubkey rsa** **Example:** `switch# show crypto key mypubkey rsa`	RSA キー ペアの設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

証明書要求の作成 （20 ページ）

PKI の設定の確認

PKI 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show crypto key mypubkey rsa	Cisco NX-OS デバイスで作成された RSA 公開キーの情報を表示します。
show crypto ca certificates	CA とアイデンティティ証明書についての情報を表示します。
show crypto ca crl	CA の CRL についての情報を表示します。
show crypto ca trustpoints	CA トラストポイントについての情報を表示します。

PKI の設定例

ここでは、Microsoft Windows Certificate サーバを使用して Cisco NX-OS デバイスで証明書と CRL を設定する作業の例について説明します。

Note デジタル証明書の作成には、どのようなタイプのサーバでも使用できます。Microsoft Windows Certificate サーバに限られることはありません。

Cisco NX-OS デバイスでの証明書の設定

Cisco NX-OS デバイスで証明書を設定するには、次の手順に従ってください。

Procedure

ステップ 1 デバイスの FQDN を設定します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# hostname Device-1
```

```
Device-1(config)#
```

ステップ 2 デバイスの DNS ドメイン名を設定します。

```
Device-1(config)# ip domain-name cisco.com
```

ステップ 3 トラストポイントを作成します。

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key:
revokation methods:  crl
```

ステップ 4 このデバイス用の RSA キー ペアを作成します。

```
Device-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Device-1(config)# show crypto key mypubkey rsa
key label: myKey
key size: 1024
exportable: yes
```

ステップ 5 RSA キー ペアとトラストポイントを関連付けます。

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# rsakeypair myKey
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key: myKey
revokation methods:  crl
```

ステップ 6 Microsoft Certificate Service の Web インターフェイスから CA をダウンロードします。

ステップ 7 トラストポイントに登録する CA を認証します。

```
Device-1(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y
```

```
Device-1(config)# show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May  3 22:46:37 2005 GMT
notAfter=May  3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

ステップ 8 トラストポイントに登録するために使用する証明書要求を作成します。

```
Device-1(config)# crypto ca enroll myCA
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password: nbv123
 The subject name in the certificate will be: Device-1.cisco.com
 Include the switch serial number in the subject name? [yes/no]: no
 Include an IP address in the subject name [yes/no]: yes
ip address: 10.10.1.1
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

ステップ 9 Microsoft Certificate Service の Web インターフェイスからアイデンティティ証明書を要求します。

ステップ 10 アイデンティティ証明書をインポートします。

```
Device-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
```

```
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZ1E9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRfbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRfbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
Device-1(config)# exit
Device-1#
```

ステップ 11 証明書の設定を確認します。

ステップ 12 証明書の設定をスタートアップ コンフィギュレーションに保存します。

Related Topics

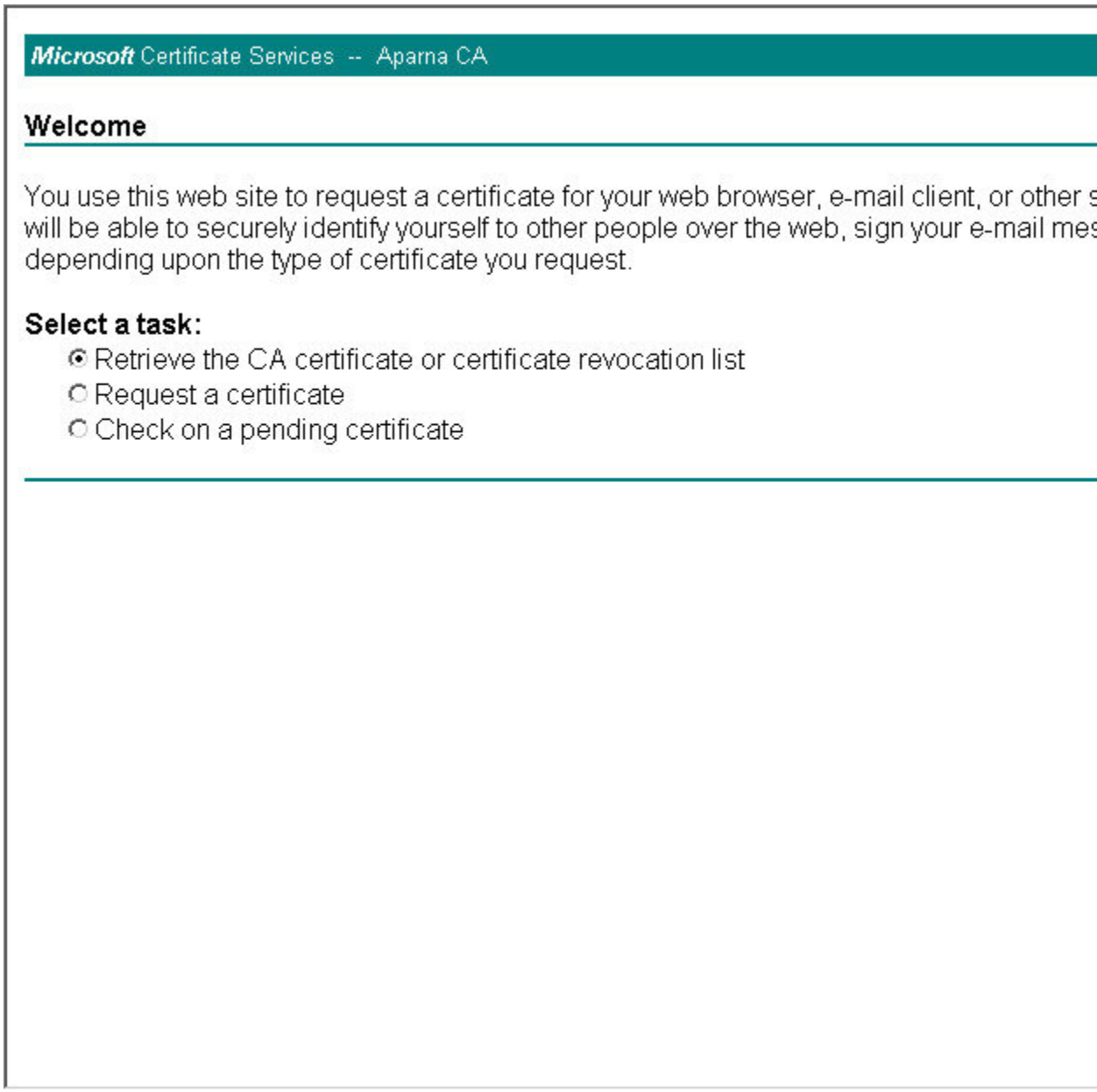
CA 証明書のダウンロード （33 ページ）
アイデンティティ証明書の要求 （39 ページ）

CA 証明書のダウンロード

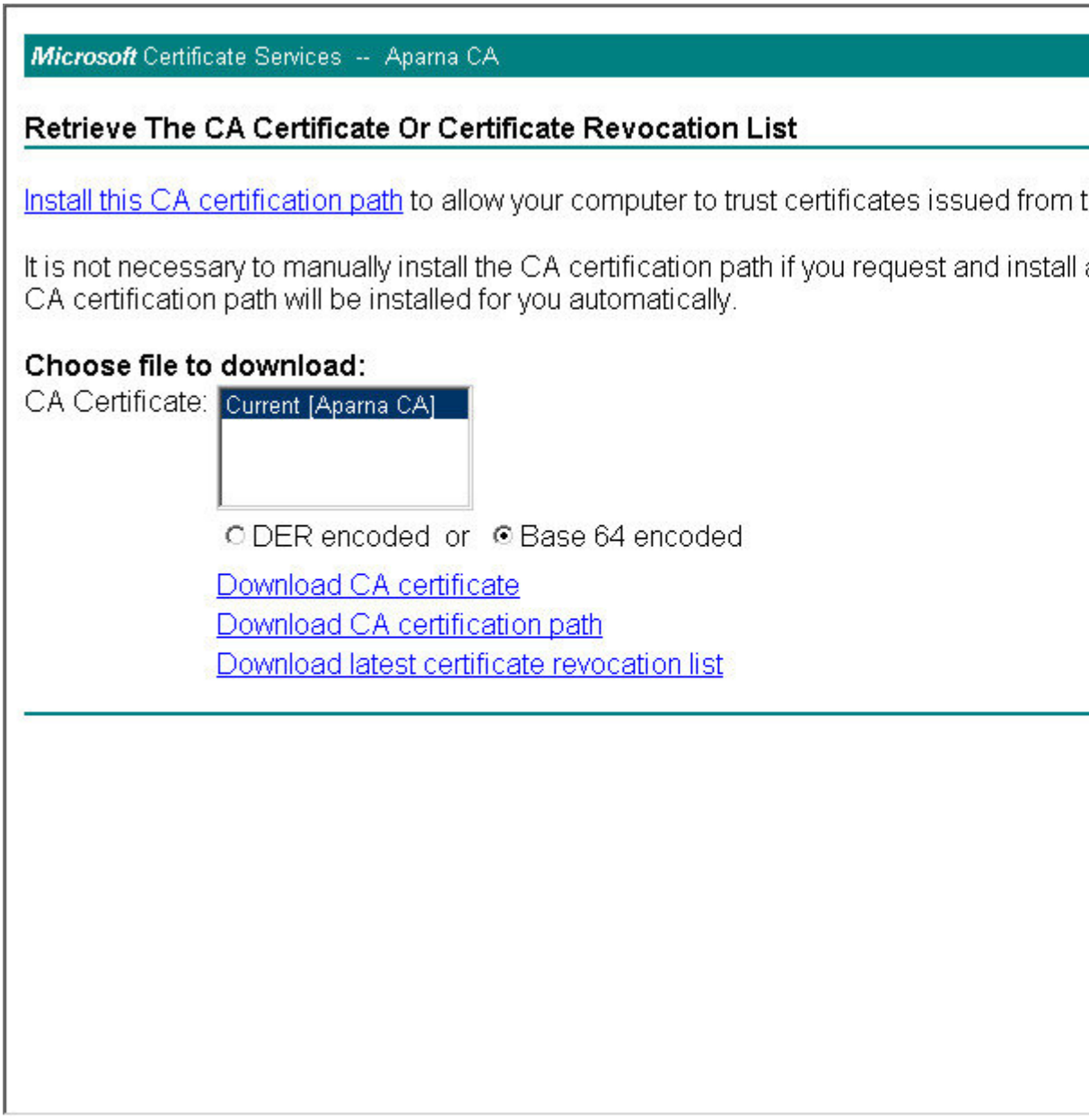
Microsoft Certificate Service の Web インターフェイスから CA 証明書をダウンロードする手順は、次のとおりです。

Procedure

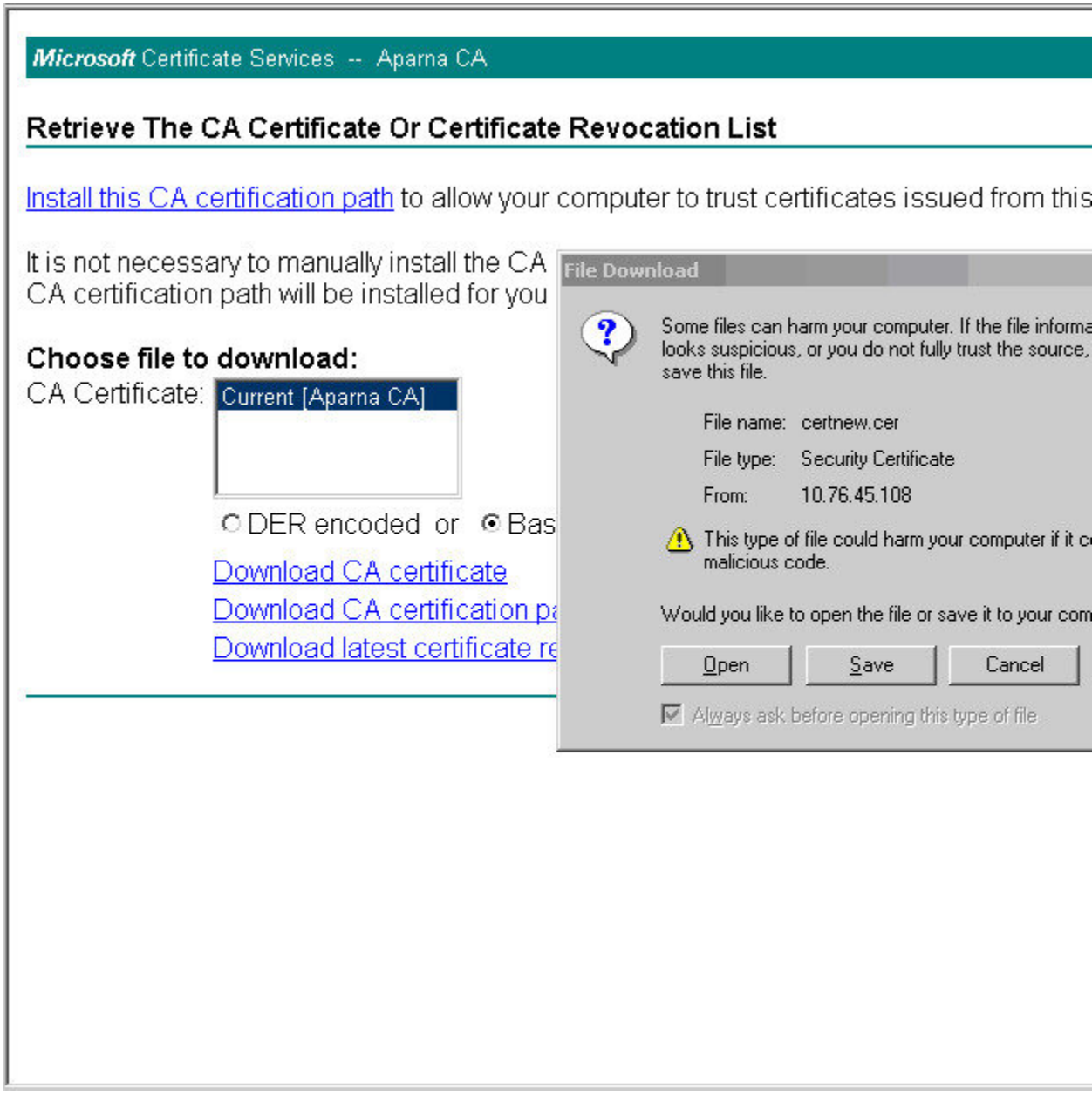
ステップ 1 Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation task] をクリックし、[Next] をクリックします。



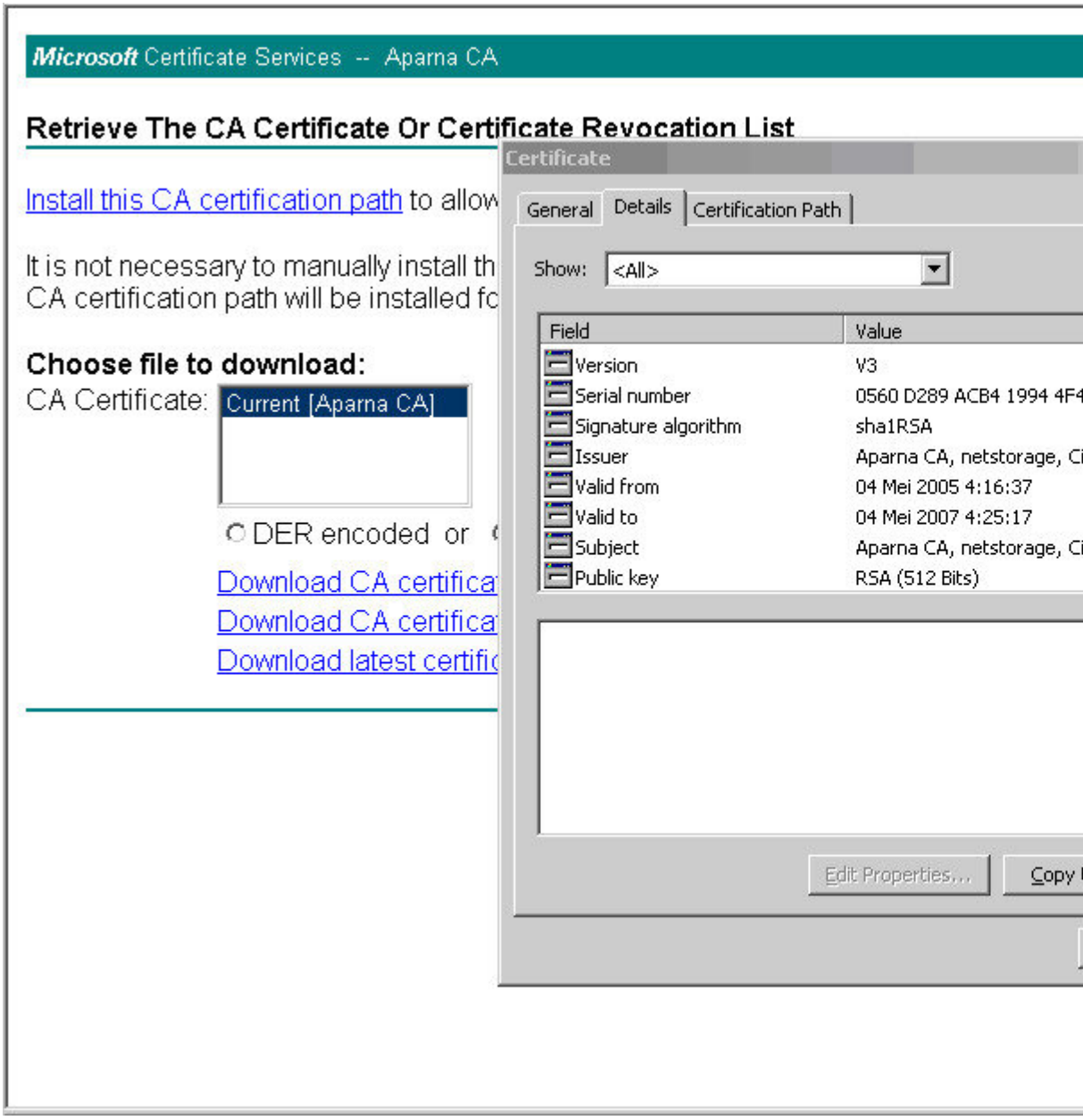
ステップ 2 表示されたリストから、ダウンロードする CA 証明書ファイルを選択します。[Base 64 encoded] をクリックし、[Download CA certificate] をクリックします。



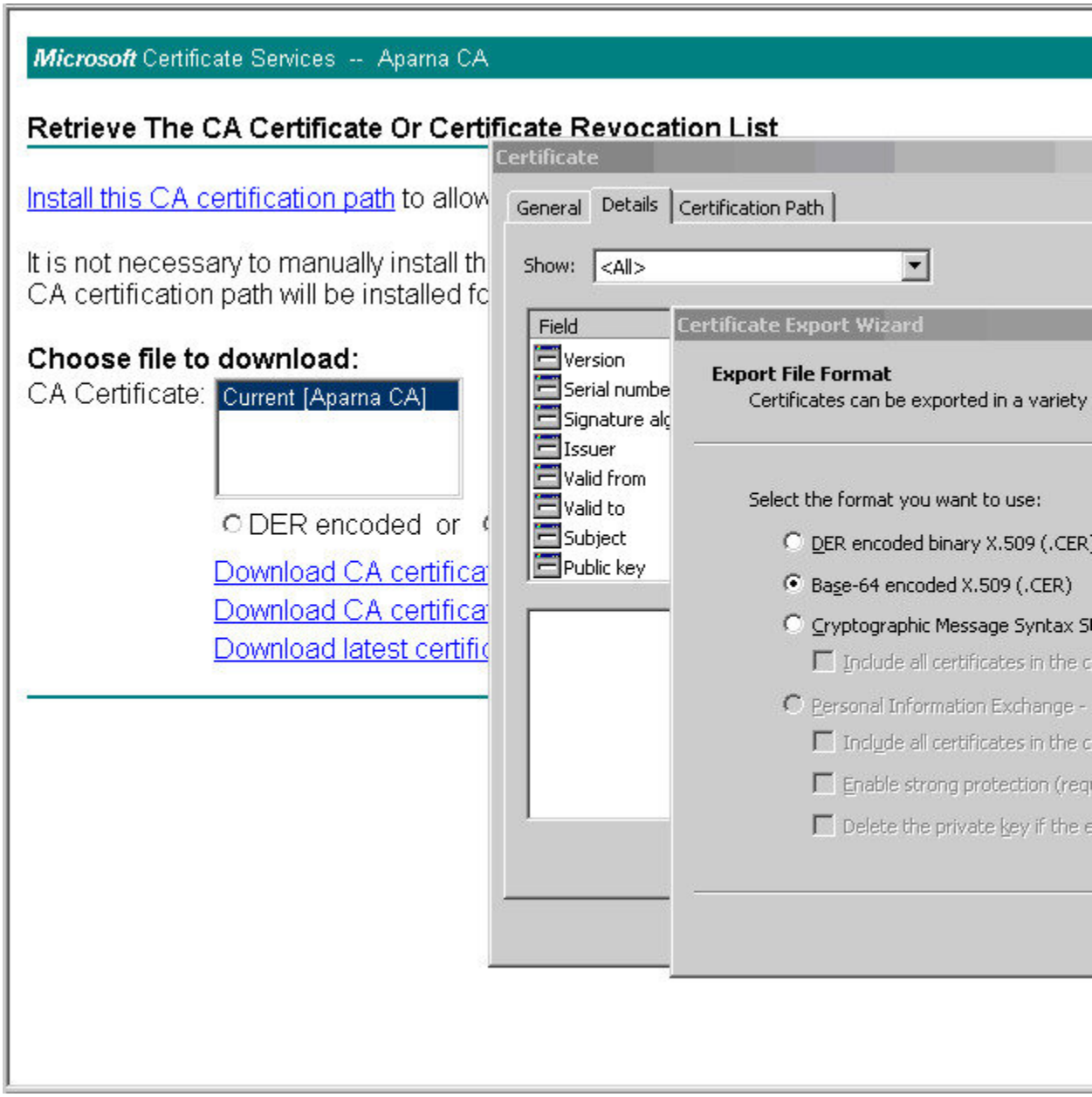
ステップ 3 [File Download] ダイアログボックスにある [Open] をクリックします。



ステップ 4 [Certificate] ダイアログボックスにある [Copy to File] をクリックし、[OK] をクリックします。



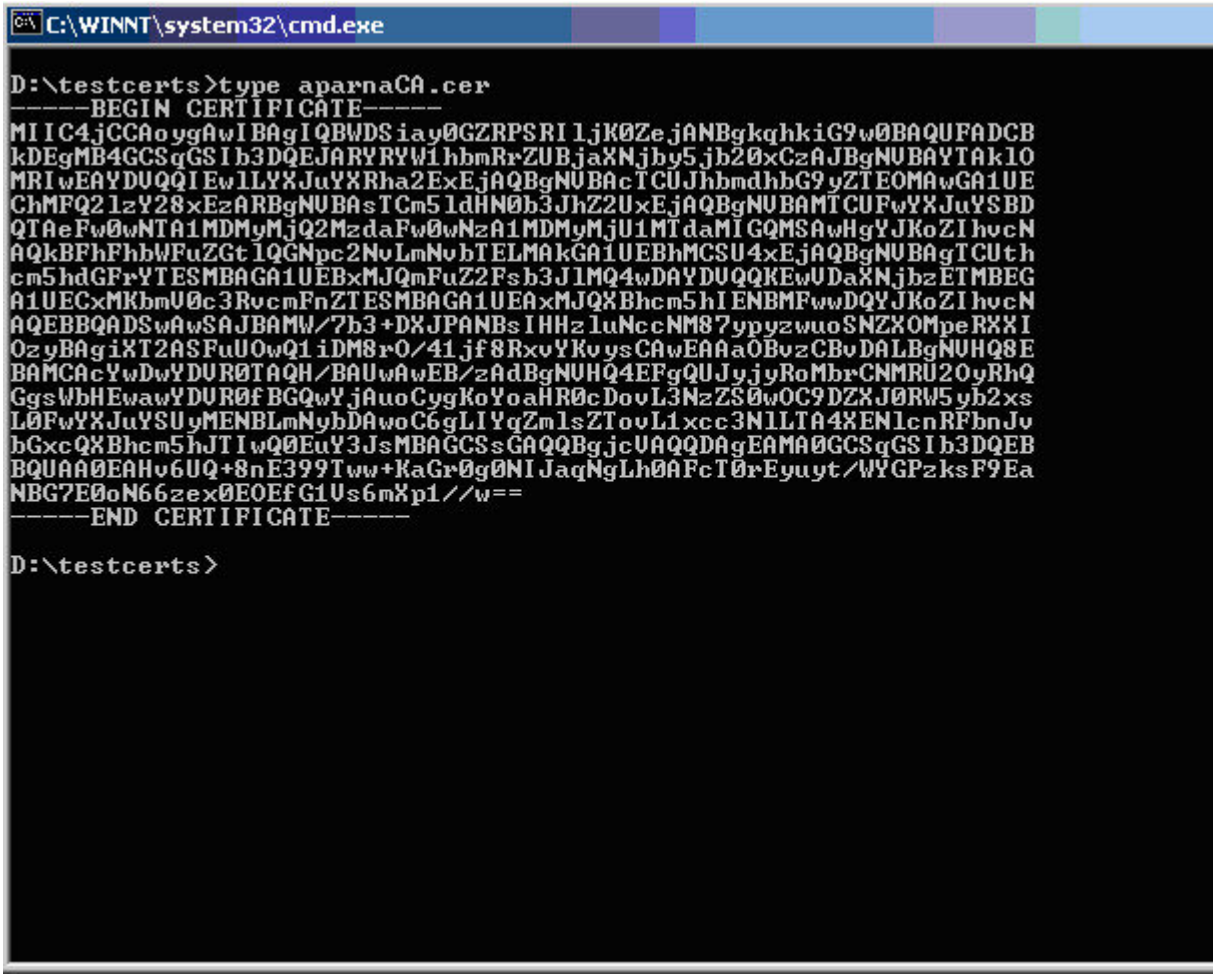
ステップ 5 [Certificate Export Wizard] ダイアログボックスから [Base-64 encoded X.509 (CER)] を選択し、[Next] をクリックします。



ステップ 6 [Certificate Export Wizard] ダイアログボックスにある [File name:] テキスト ボックスに保存するファイル名を入力し、[Next] をクリックします。

ステップ 7 [Certificate Export Wizard] ダイアログボックスで、[Finish] をクリックします。

ステップ 8 Microsoft Windows の type コマンドを入力して、Base-64（PEM）形式で保存されている CA 証明書を表示します。

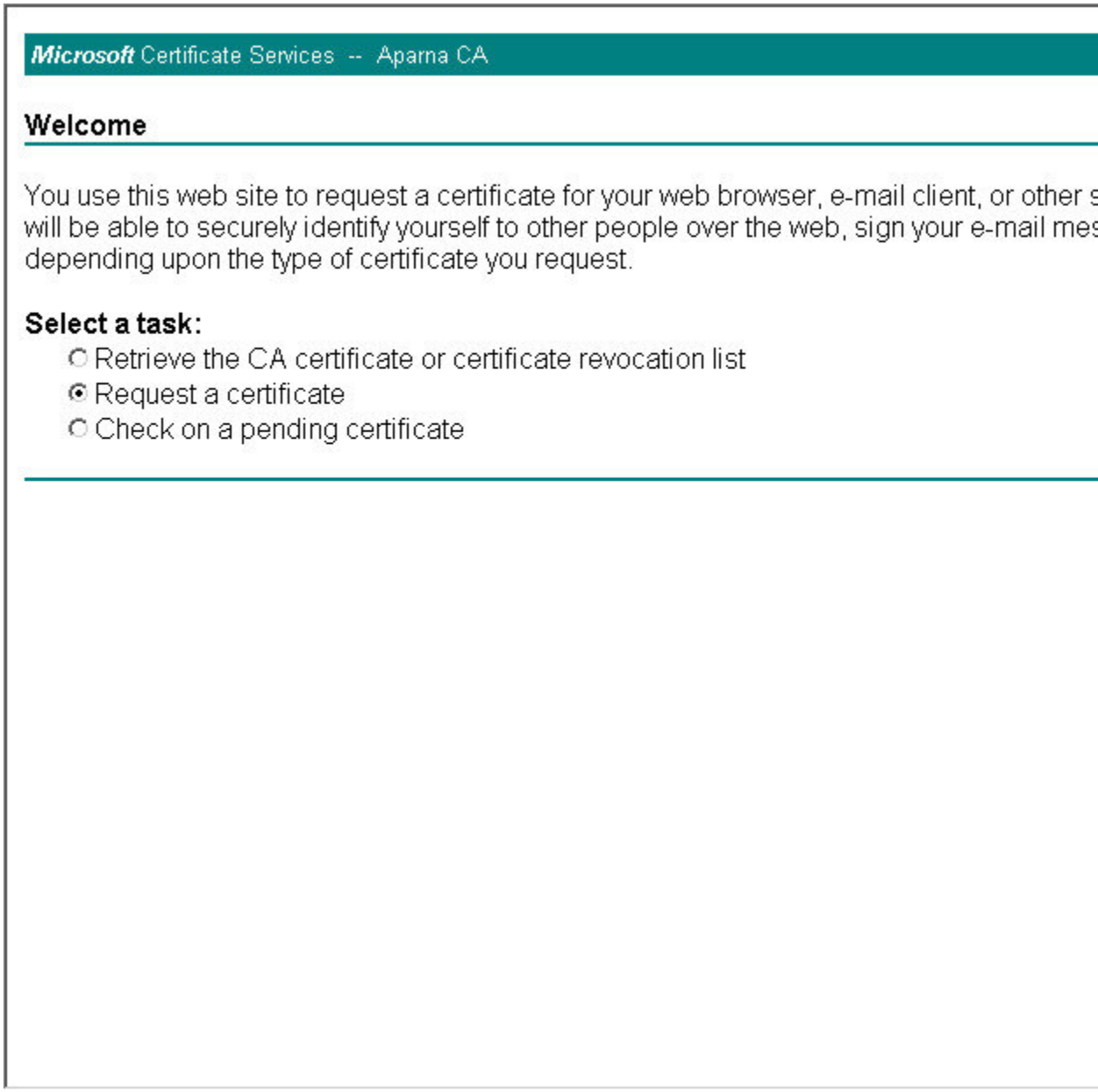


アイデンティティ証明書の要求

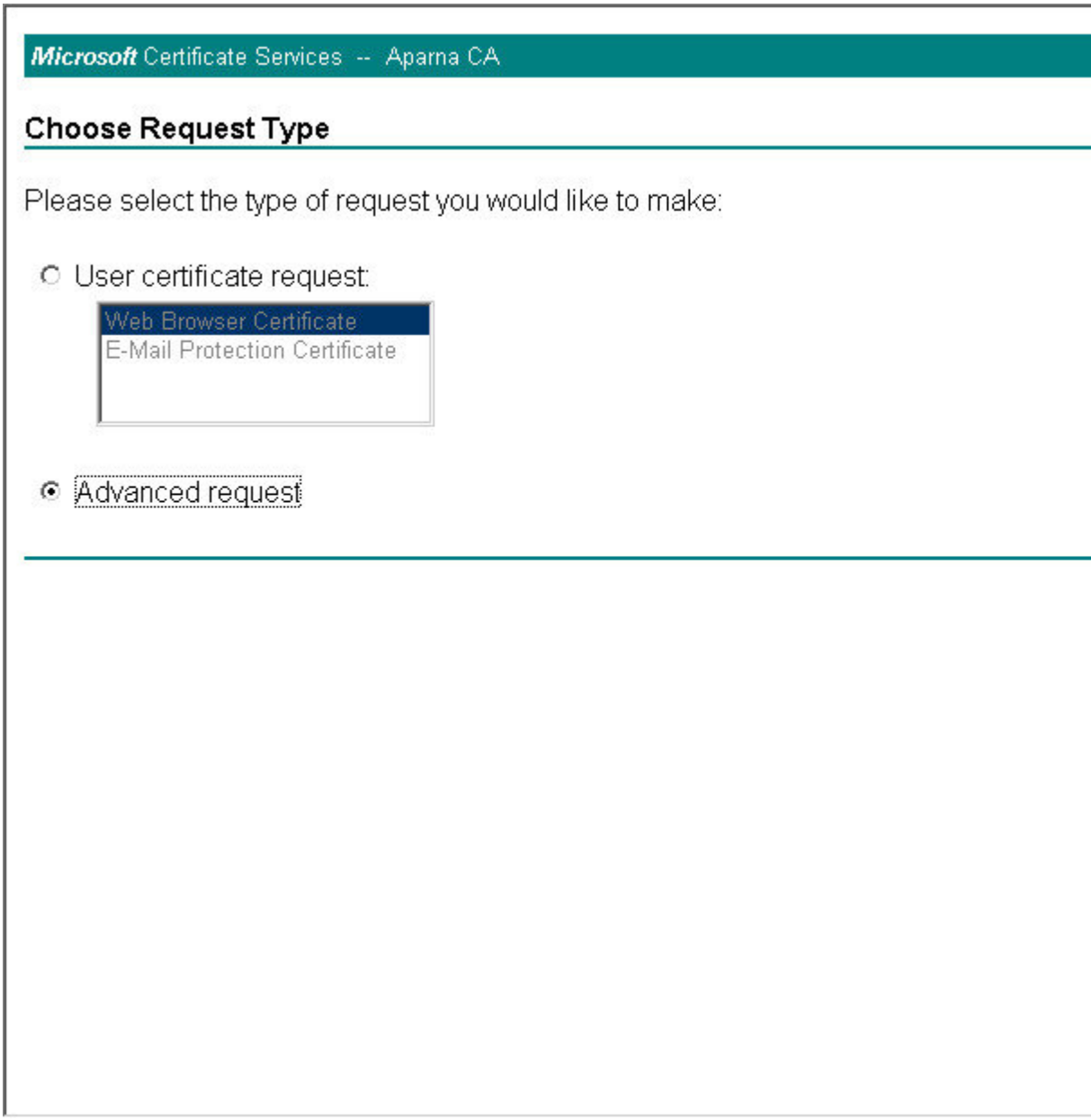
PKCS#12 証明書署名要求（CSR）を使用して Microsoft Certificate サーバにアイデンティティ証明書を要求するには、次の手順に従ってください。

Procedure

ステップ 1 Microsoft Certificate Services の Web インターフェイスから、**[証明書の要求（Request a certificate）]** をクリックし、**[次へ（Next）]** をクリックします。

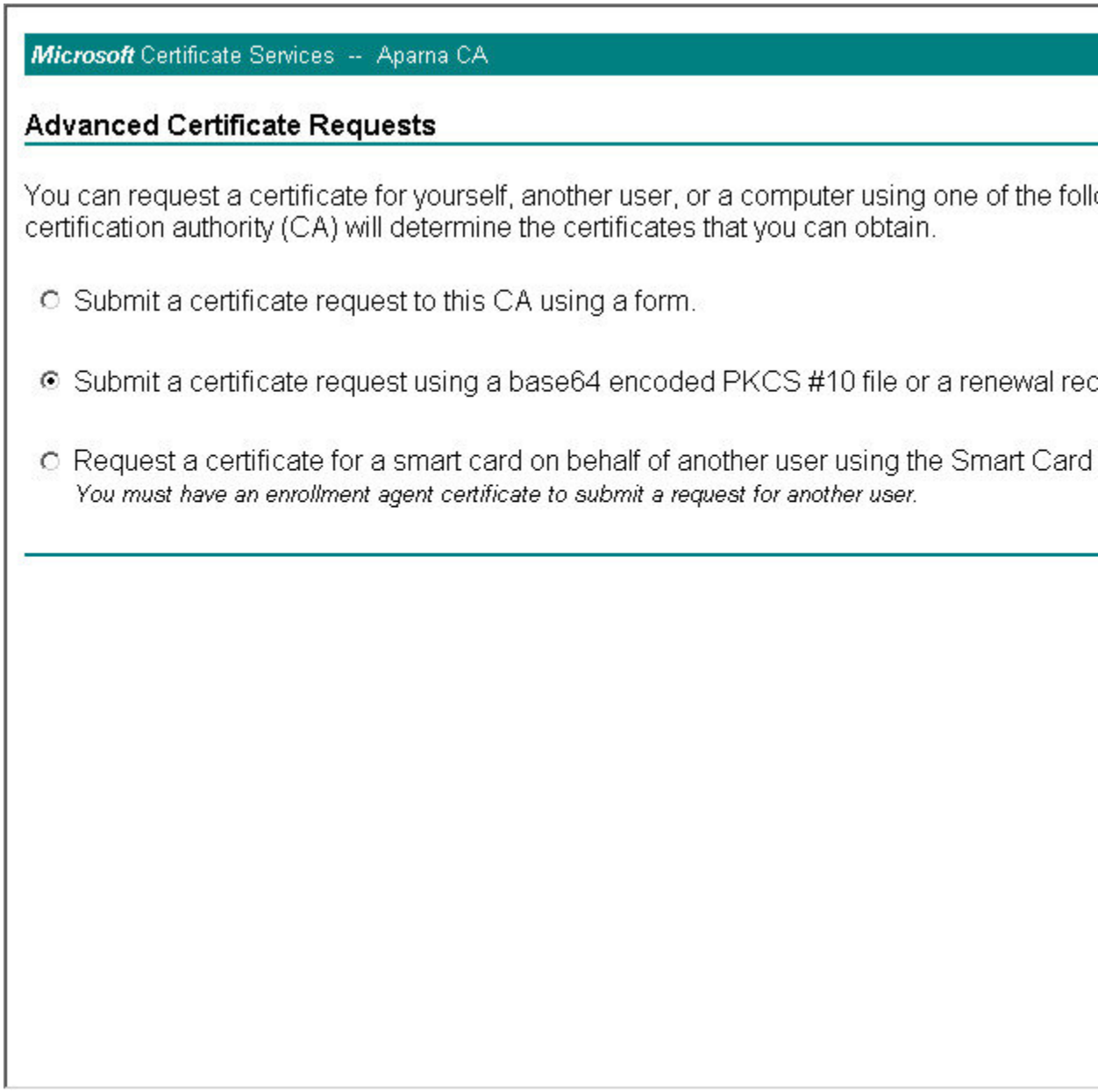


ステップ 2　**[詳細な要求（Advanced request）]** をクリックし、**[次へ（Next）]** をクリックします。



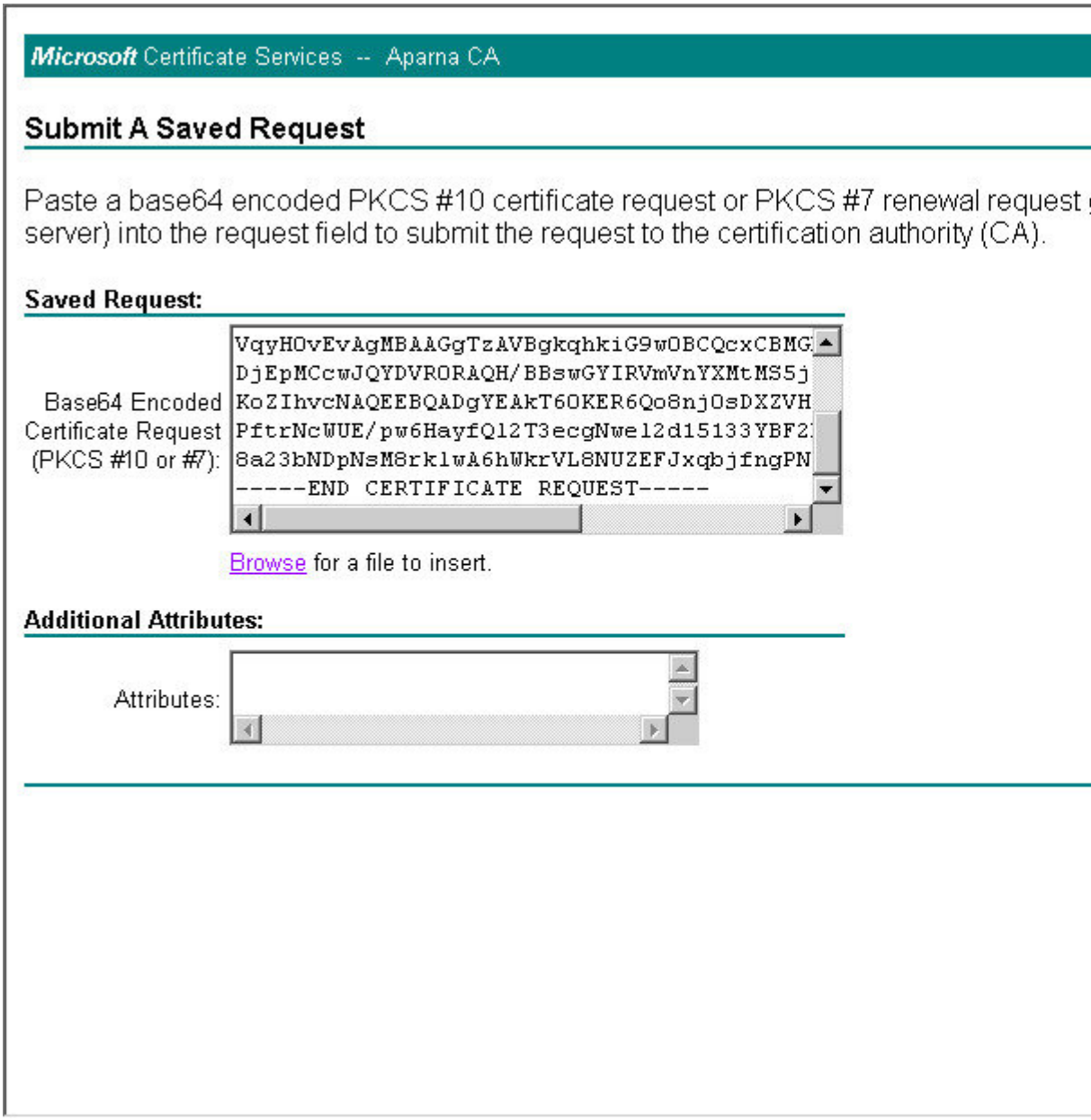
ステップ 3　**[Base64 エンコード済み PKCS#10 を使用する証明書要求または base64 エンコード済み PKCS#7 ファイルを使用する更新要求を送信する（Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file）]** をクリックし、**[次へ**

（**Next**）] をクリックします。

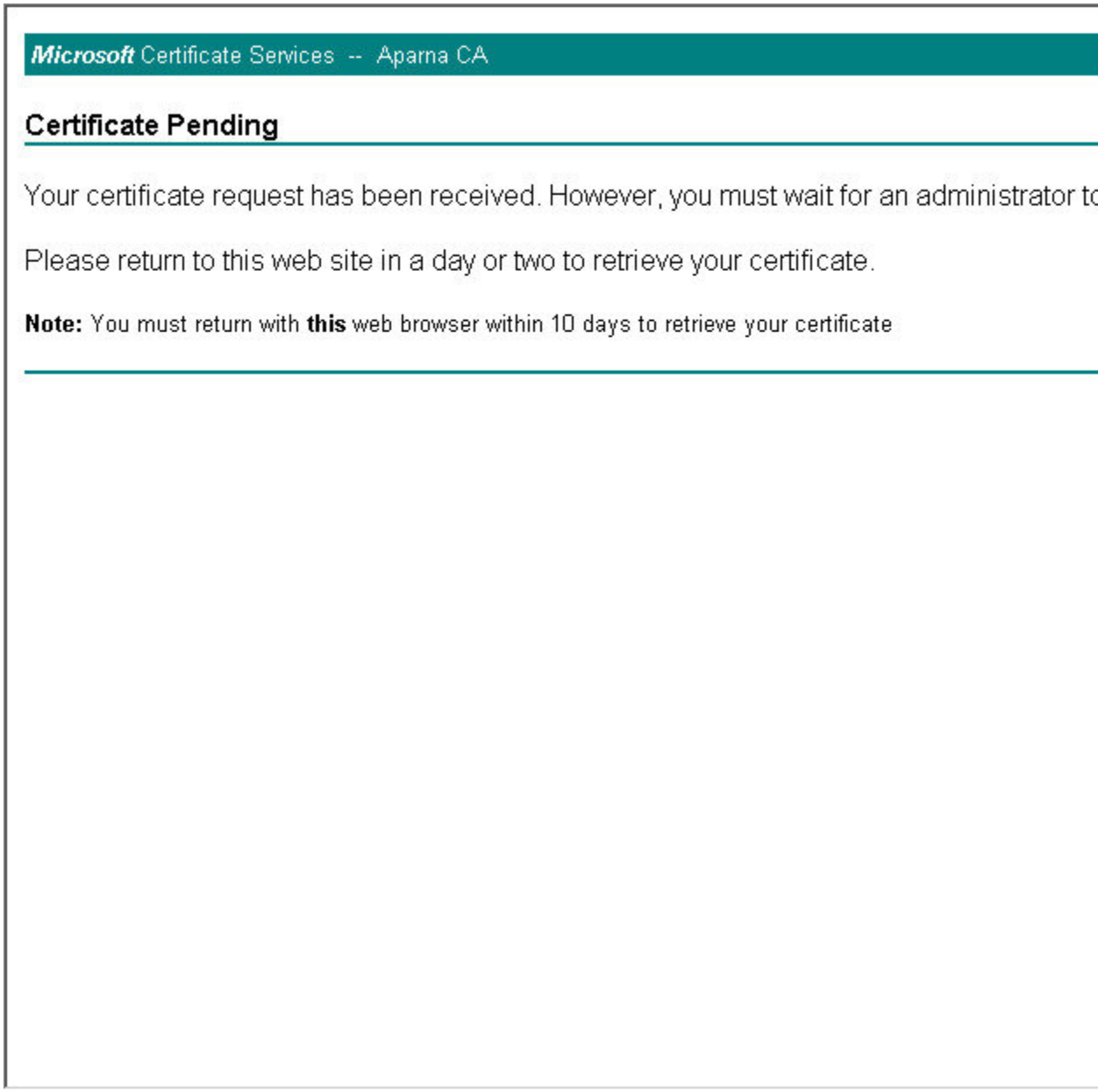


ステップ 4 [保存済みの要求（Saved Request）] テキスト ボックスに、base64 の PKCS#10 証明書要求をペーストし、**[次へ（Next）]** をクリックします。証明書要求が Cisco NX-OS デバイスのコンソール

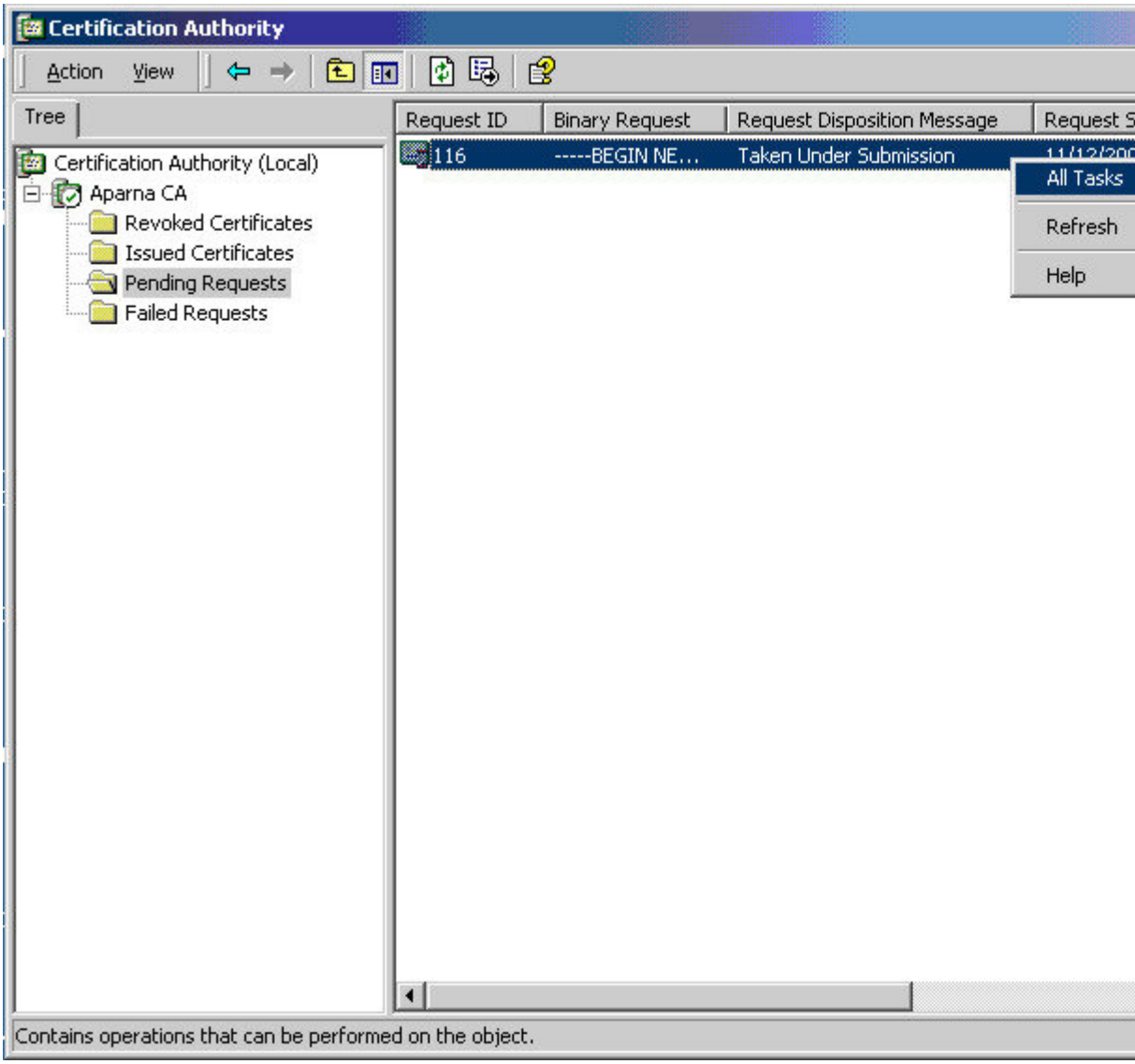
からコピーされます。


Microsoft Certificate Services -- Aparna CA
Submit A Saved Request
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request
server) into the request field to submit the request to the certification authority (CA).
Saved Request:
Base64 Encoded Certificate Request (PKCS #10 or #7):
VqyHOvEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMG
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5j
KoZIhvcNAQEEBQADgYEAkT6OKER6Qo8njOsDXZVH
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPN
-----END CERTIFICATE REQUEST-----
Browse for a file to insert.
Additional Attributes:
Attributes:

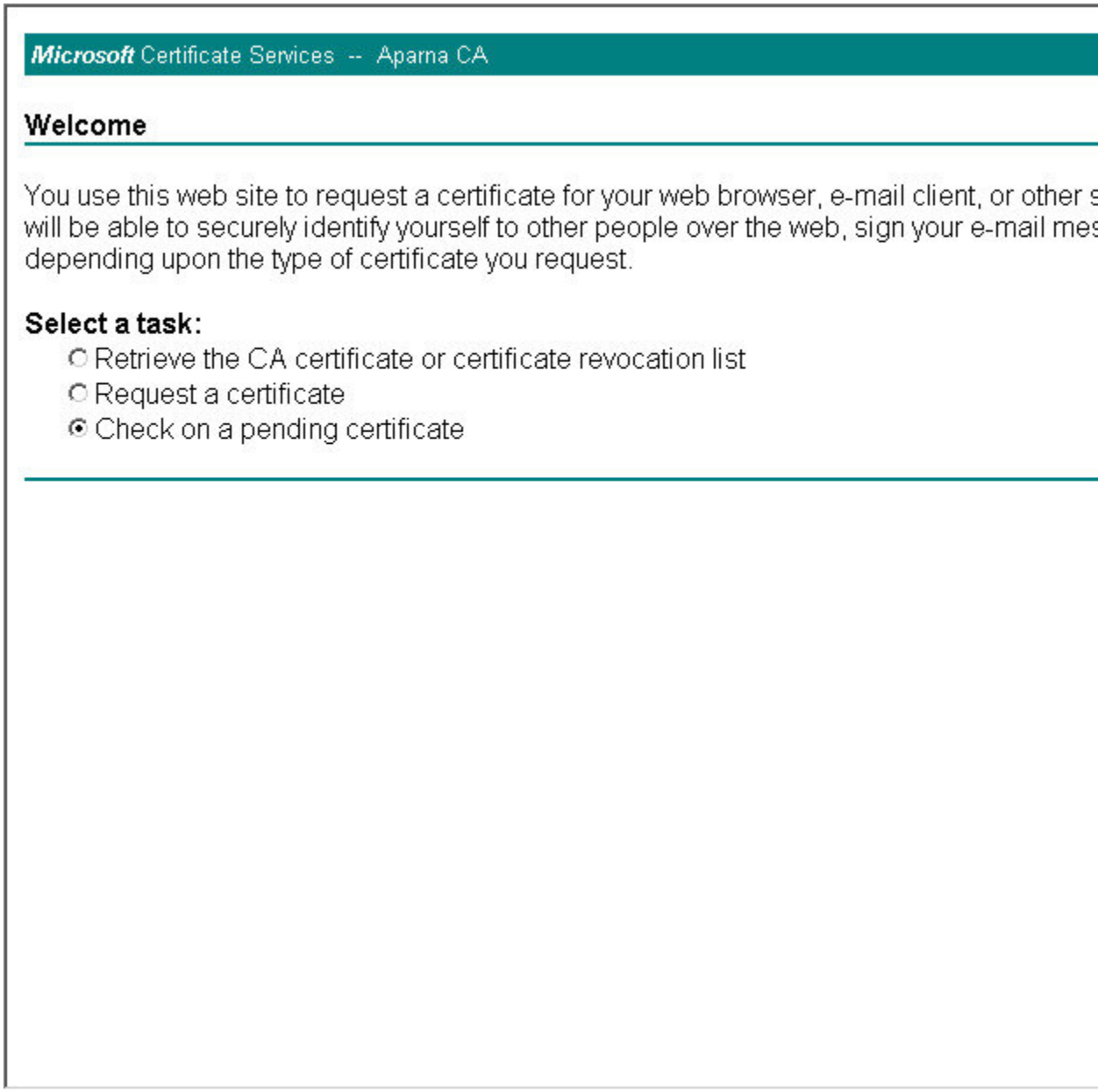
ステップ 5 CA アドミニストレータから証明書が発行されるまで、1 ～ 2 日間待ちます。



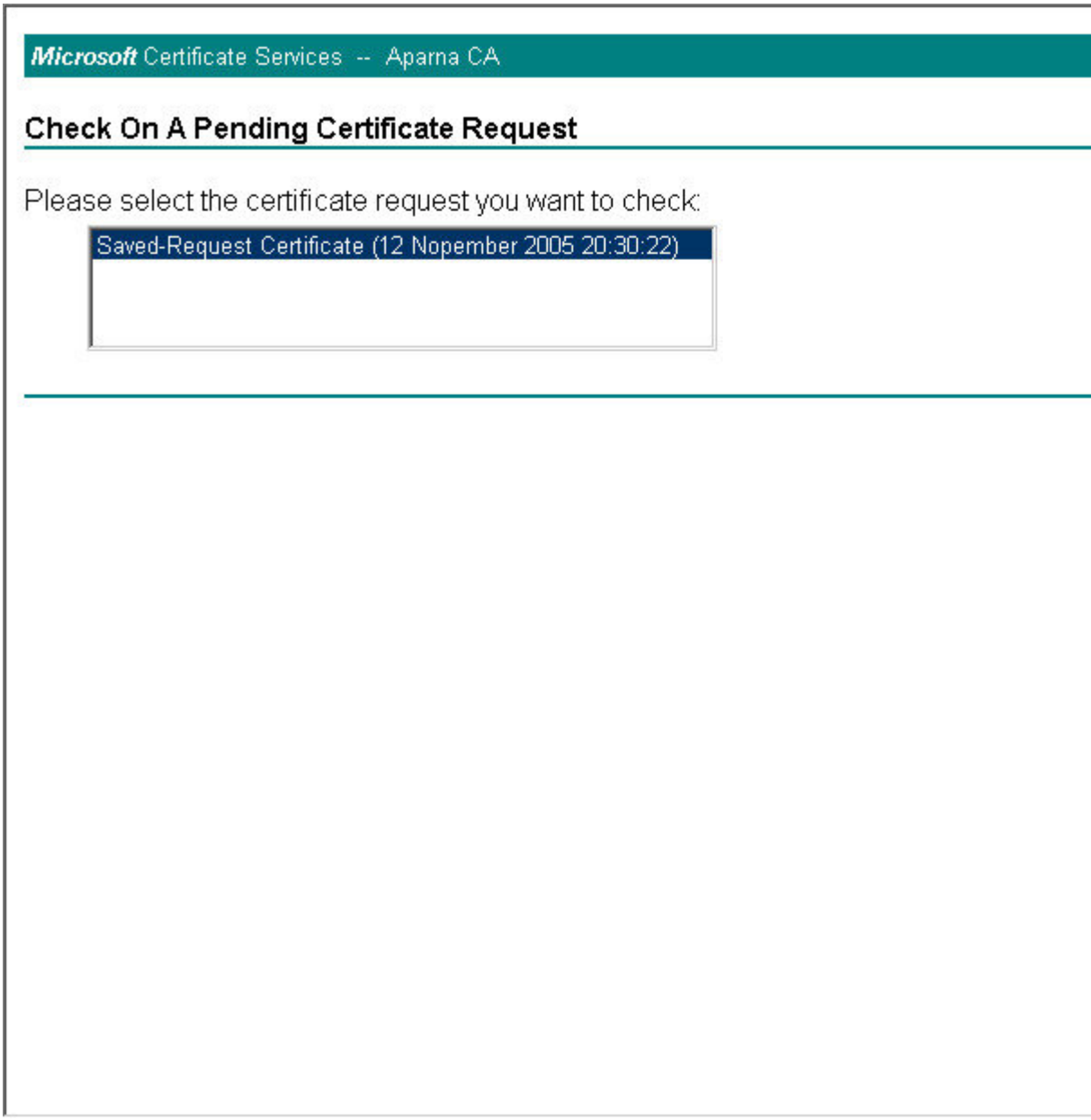
ステップ 6　CA アドミニストレータが証明書要求を承認するのを確認します。



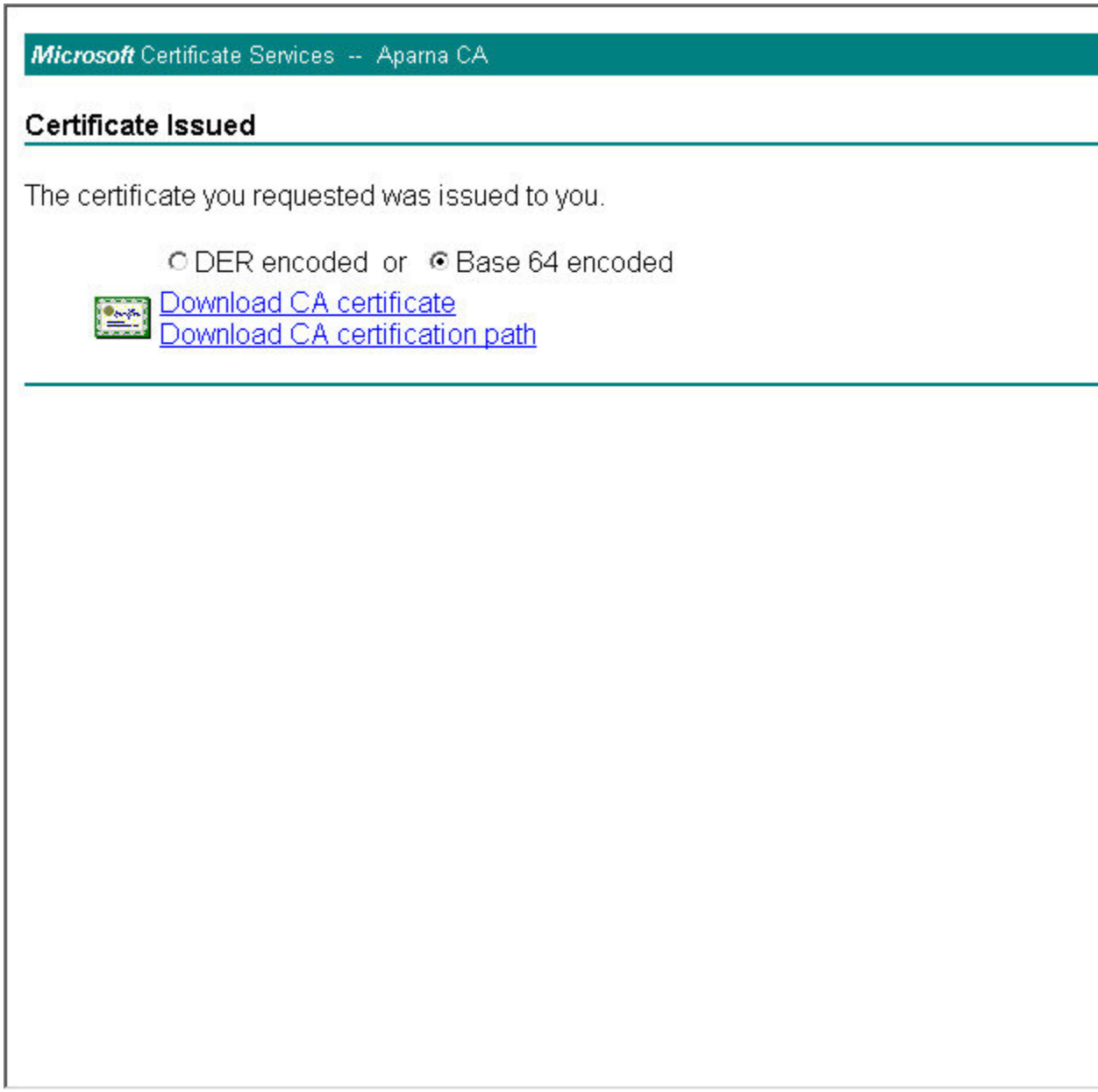
ステップ 7 Microsoft Certificate Services の Web インターフェイスから、**[保留中の証明書をチェックする（Check on a pending certificate）]** をクリックし、**[次へ（Next）]** をクリックします。



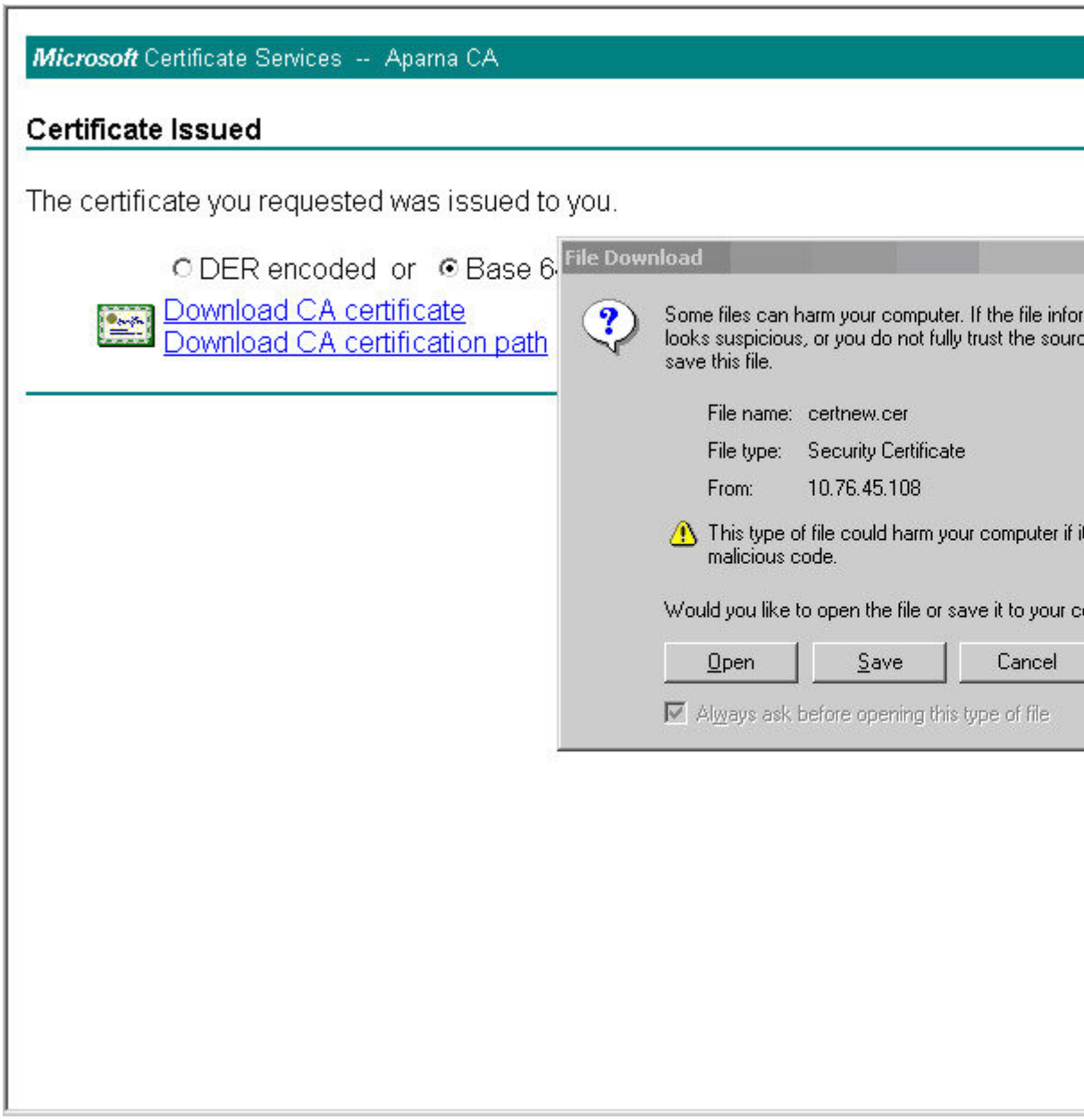
ステップ 8 チェックする証明書要求を選択して、**[次へ（Next）]** をクリックします。



ステップ 9　**[Base 64 エンコード済み（Base 64 encoded）]** をクリックして、**[CA 証明書のダウンロード（Download CA certificate）]** をクリックします。

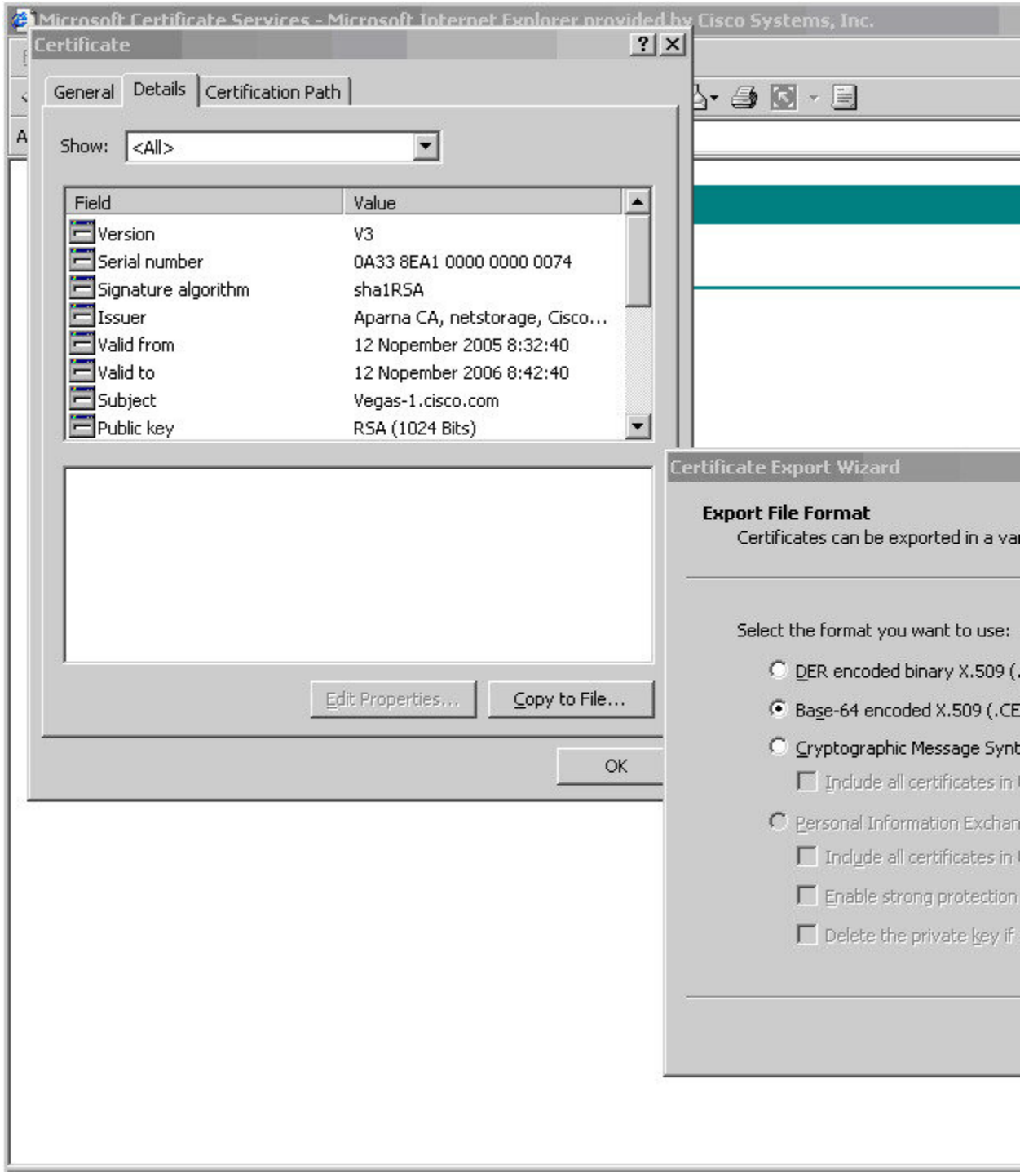


ステップ 10 [ファイルのダウンロード（File Download）] ダイアログ ボックスで、**[開く（Open）]** をクリックします。



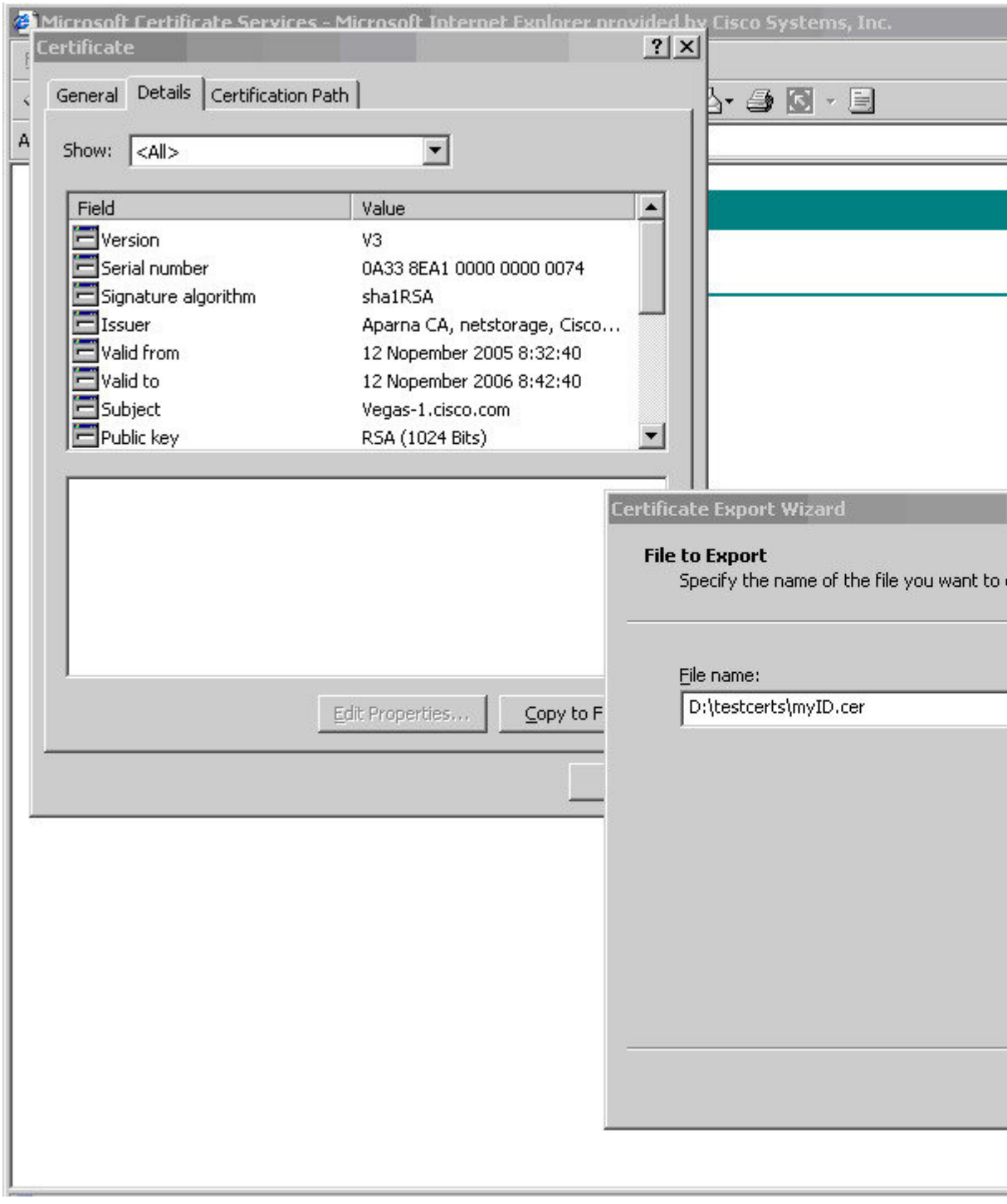
ステップ 11 [Certificate] ボックスで、**[Details]** タブをクリックし、**[Copy to File...]** をクリックします。. [証明書のエクスポート ダイアログ（Certificate Export Dialog）] ボックスで、**[Base-64 エンコード済み X.509 (.CER)（Base-64 encoded X.509 (.CER)）]** をクリックし、**[次へ（Next）]** をクリッ

クします。

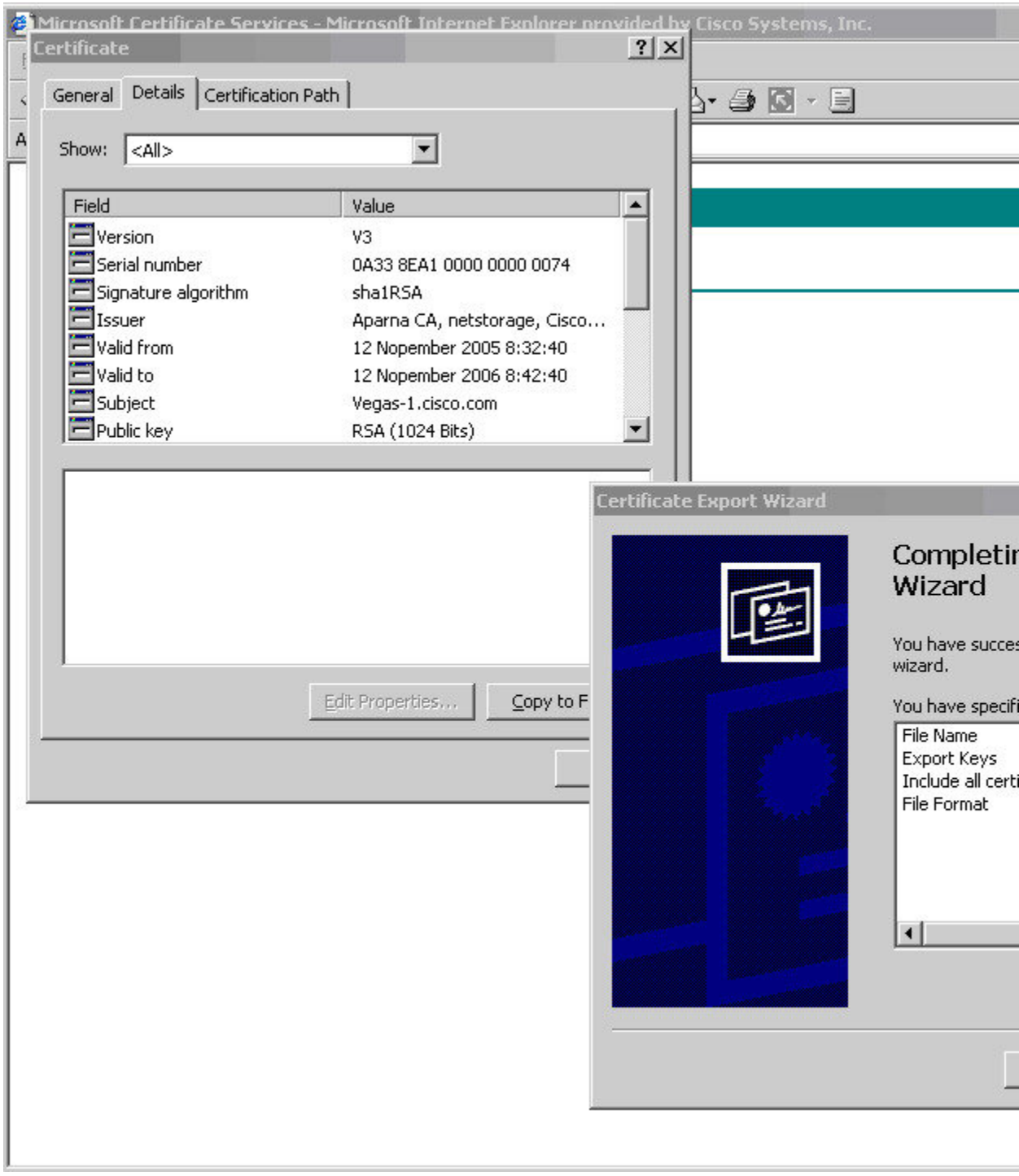


ステップ 12 [証明書エクスポート ウィザード（Certificate Export Wizard）] ダイアログ ボックスにある [ファイル名：（File name:）] テキスト ボックスに保存するファイル名を入力し、**[次へ（Next）]**を

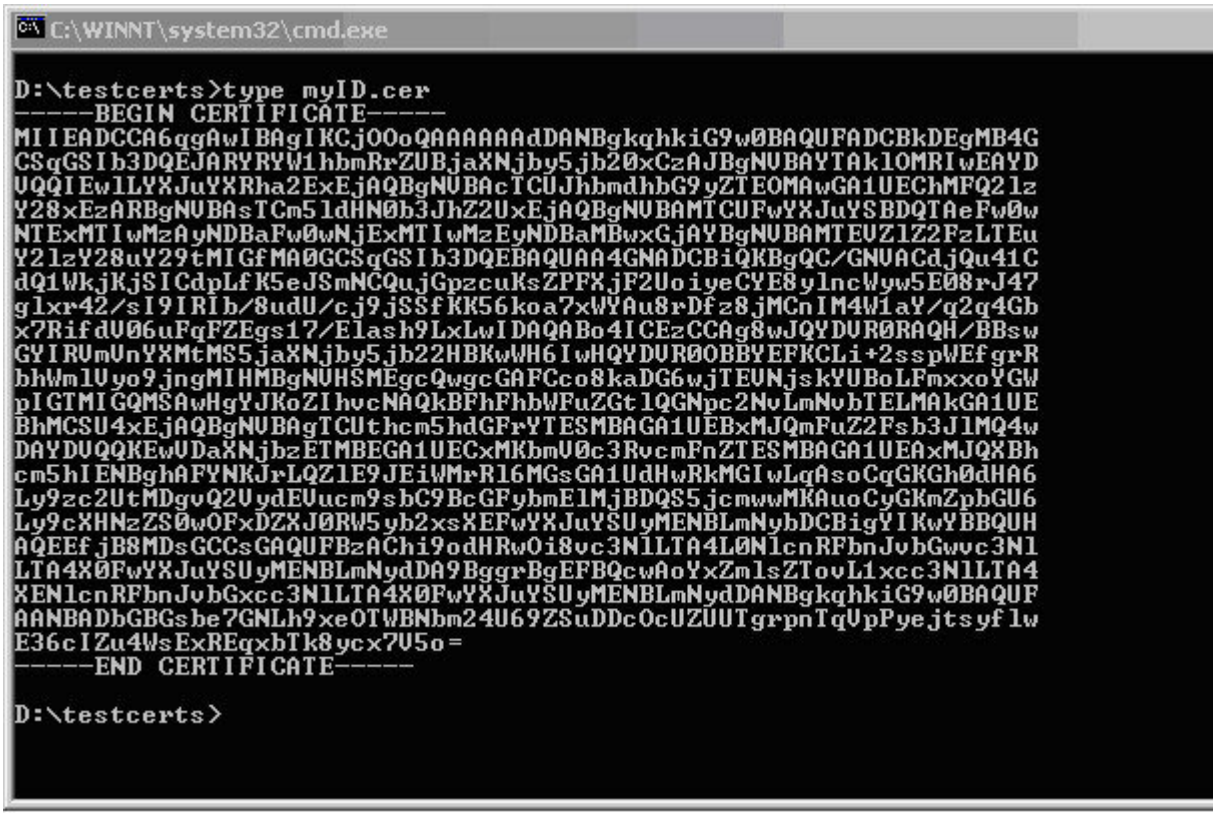
クリックします。


Microsoft Certificate Services - Microsoft Internet Explorer provided by Cisco Systems, Inc.
Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
0A33 8EA1 0000 0000 0074
Signature algorithm
sha1RSA
Issuer
Aparna CA, netstorage, Cisco...
Valid from
12 Nopember 2005 8:32:40
Valid to
12 Nopember 2006 8:42:40
Subject
Vegas-1.cisco.com
Public key
RSA (1024 Bits)
Edit Properties...
Copy to F
Certificate Export Wizard
File to Export
Specify the name of the file you want to
File name:
D:\testcerts\myID.cer

ステップ 13 [完了（Finish）] をクリックします。



ステップ 14 Microsoft Windows の **type** コマンドを入力して、アイデンティティ証明書を Base-64 でエンコードされた形式で表示します。



Related Topics

証明書要求の作成 （20 ページ）
Cisco NX-OS デバイスでの証明書の設定 （30 ページ）

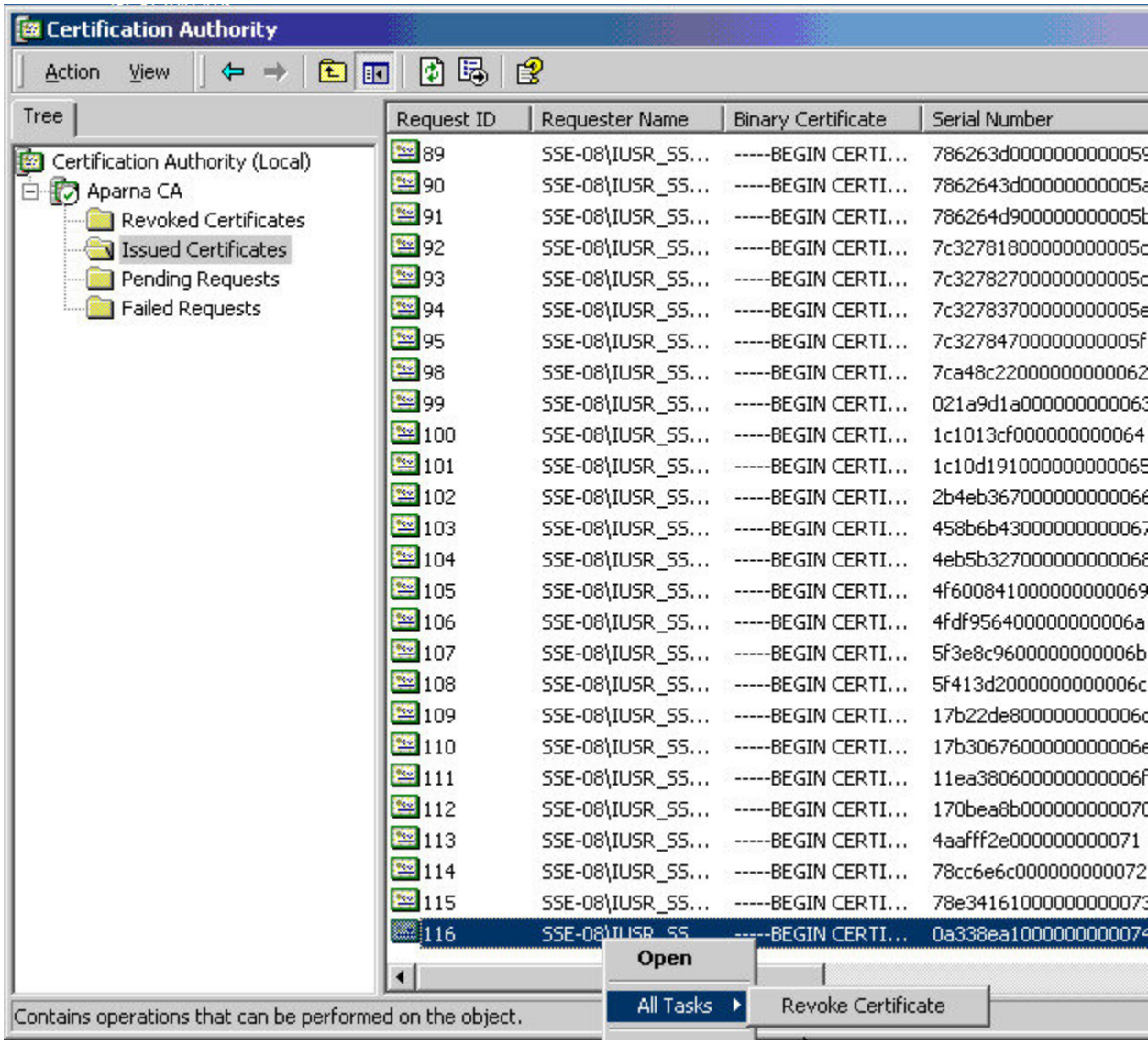
証明書の取り消し

Microsoft CA 管理者プログラムを使用して証明書を取り消す手順は、次のとおりです。

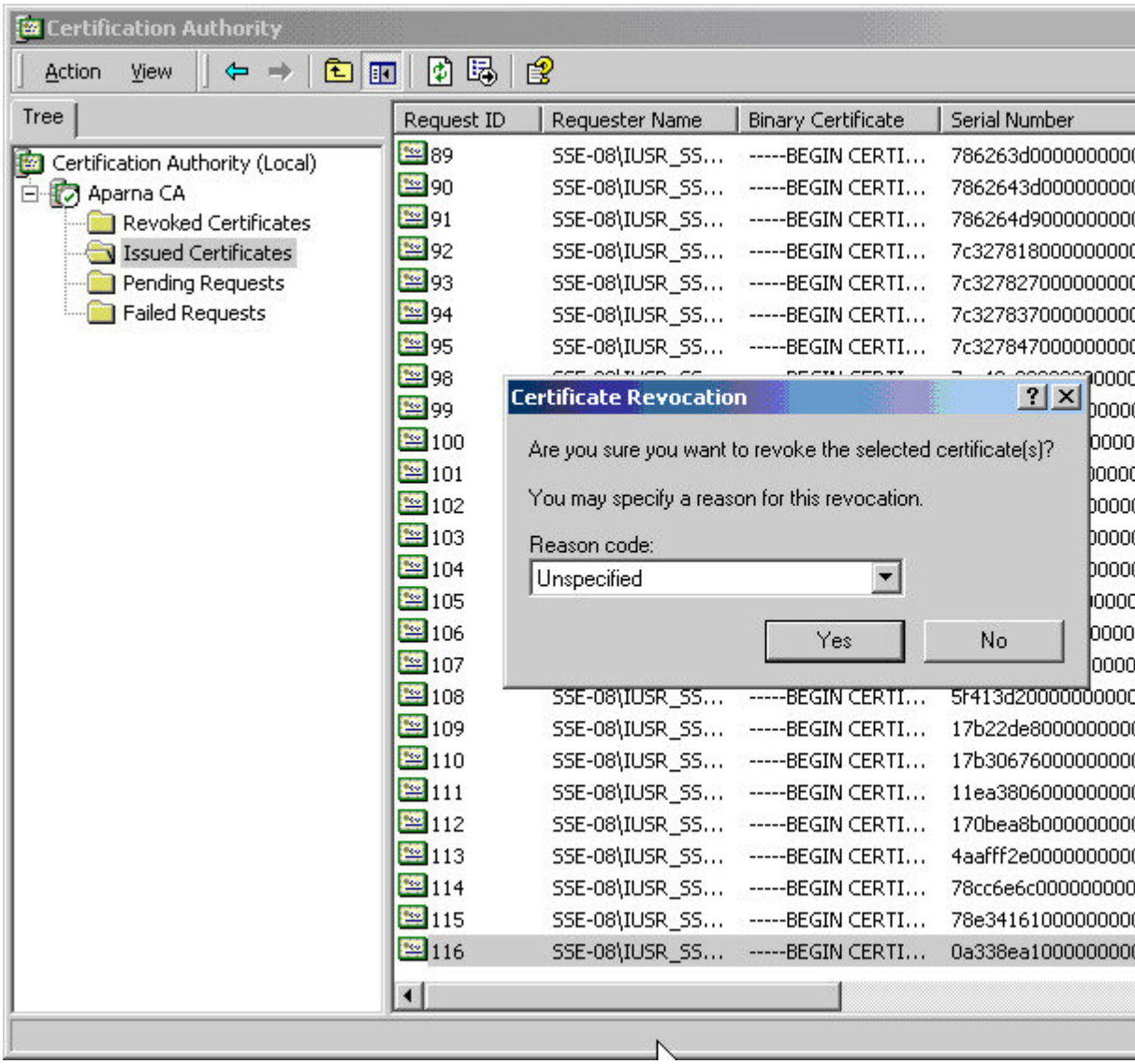
Procedure

ステップ 1 [Certification Authority] ツリーから、[Issued Certificates] フォルダをクリックします。リストから、取り消す証明書を右クリックします。

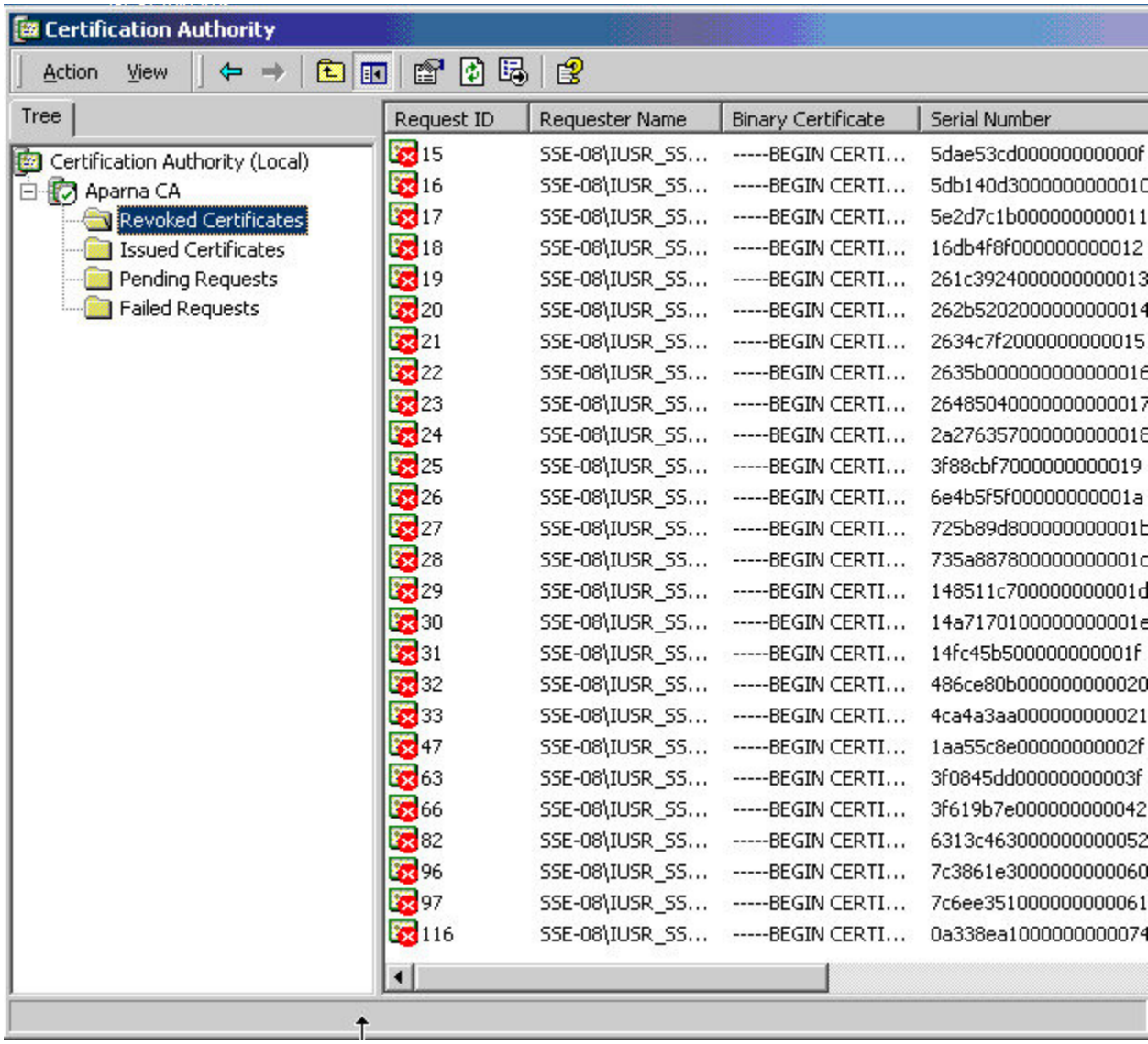
ステップ 2 [All Tasks] > [Revoke Certificate] の順に選択します。



ステップ 3 [Reason code] ドロップダウン リストから取り消しの理由を選択し、[Yes] をクリックします。



ステップ 4 [Revoked Certificates] フォルダをクリックして、証明書の取り消しを表示および確認します。

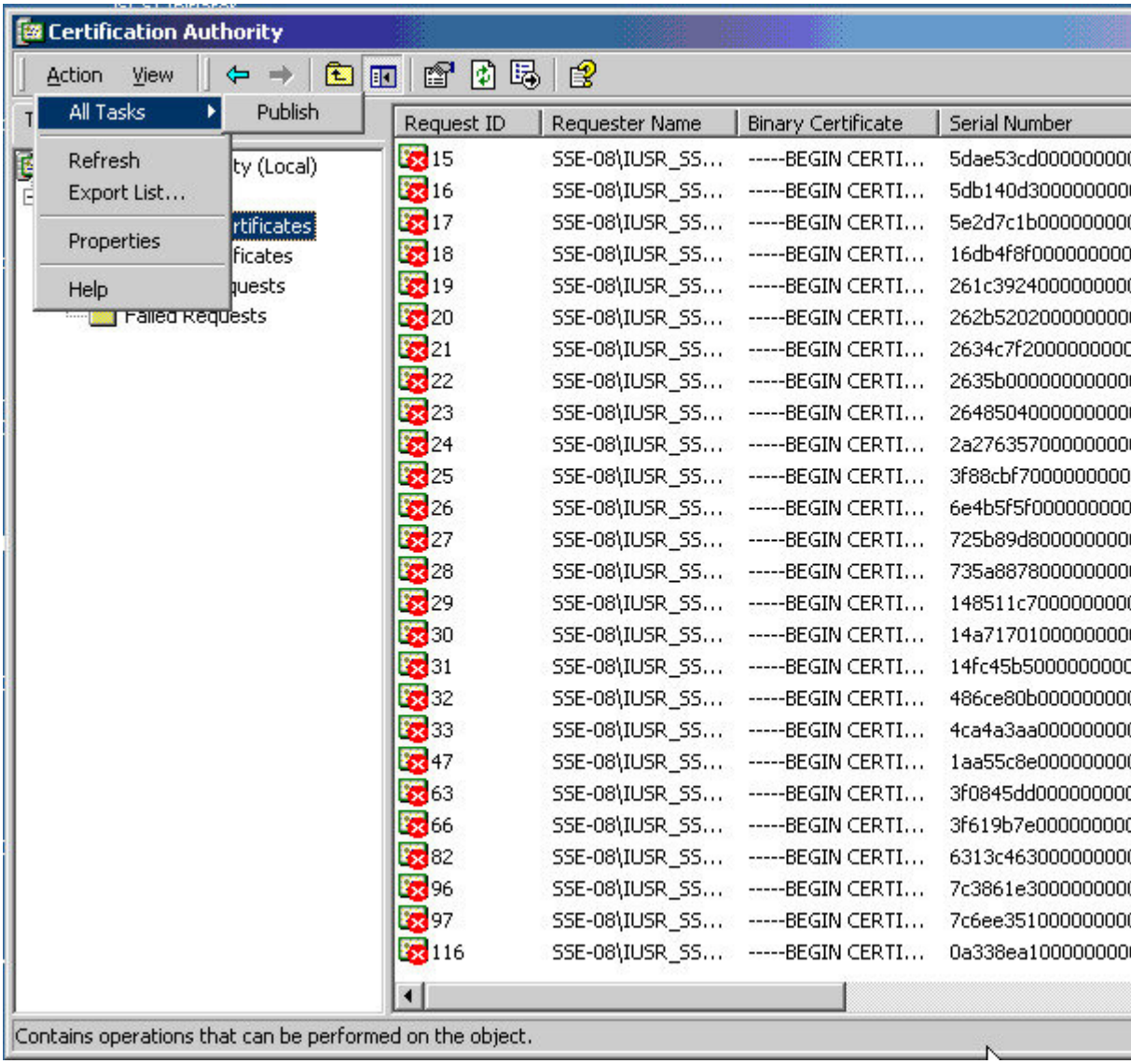


CRL の作成と公開

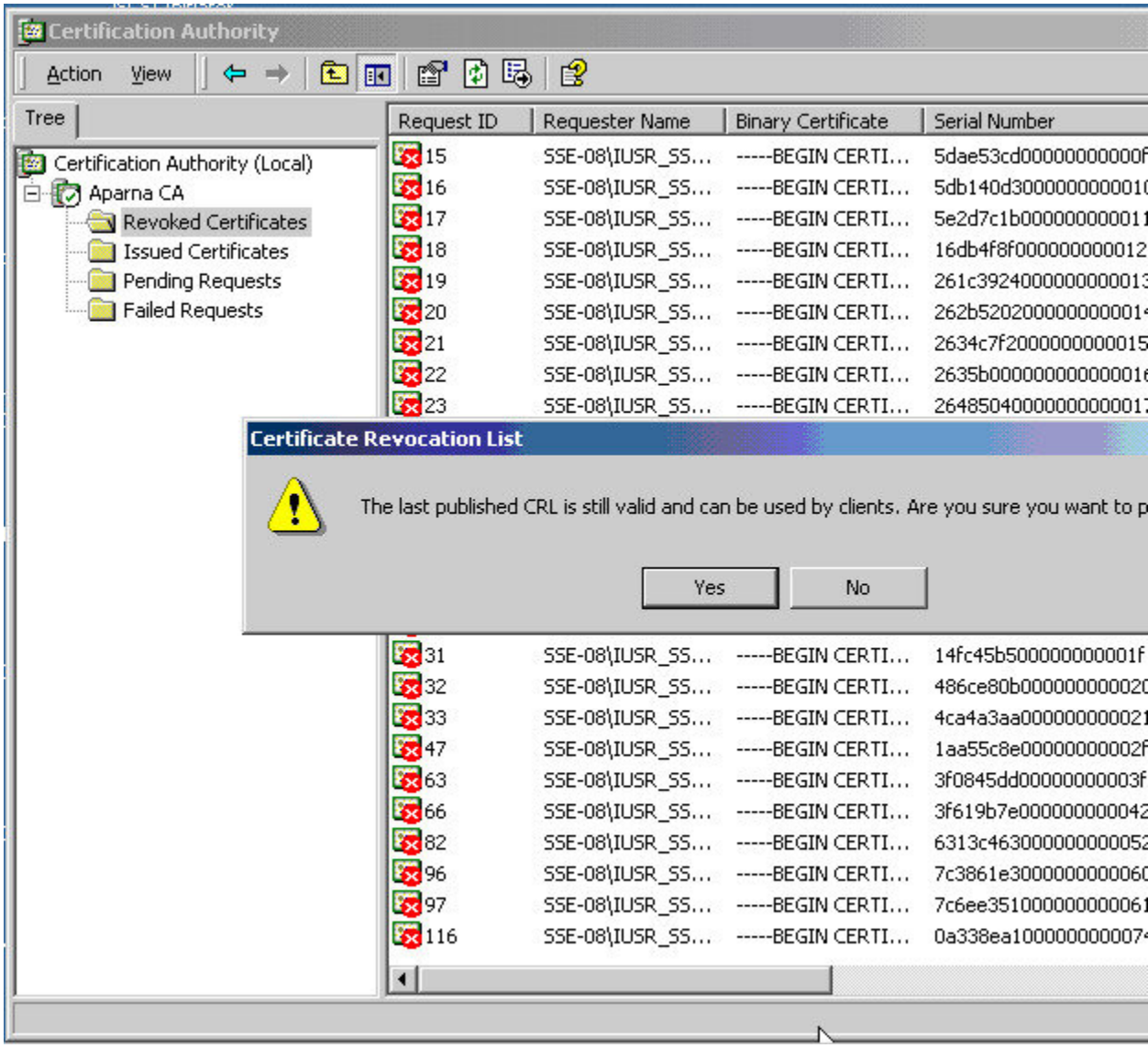
Microsoft CA 管理者プログラムを使用して CRL を作成および公開する手順は、次のとおりです。

Procedure

ステップ 1 [Certification Authority] の画面から、[Action] > [All Tasks] > [Publish] の順に選択します。



ステップ 2 [Certificate Revocation List] ダイアログボックスで、[Yes] をクリックして最新の CRL を公開します。

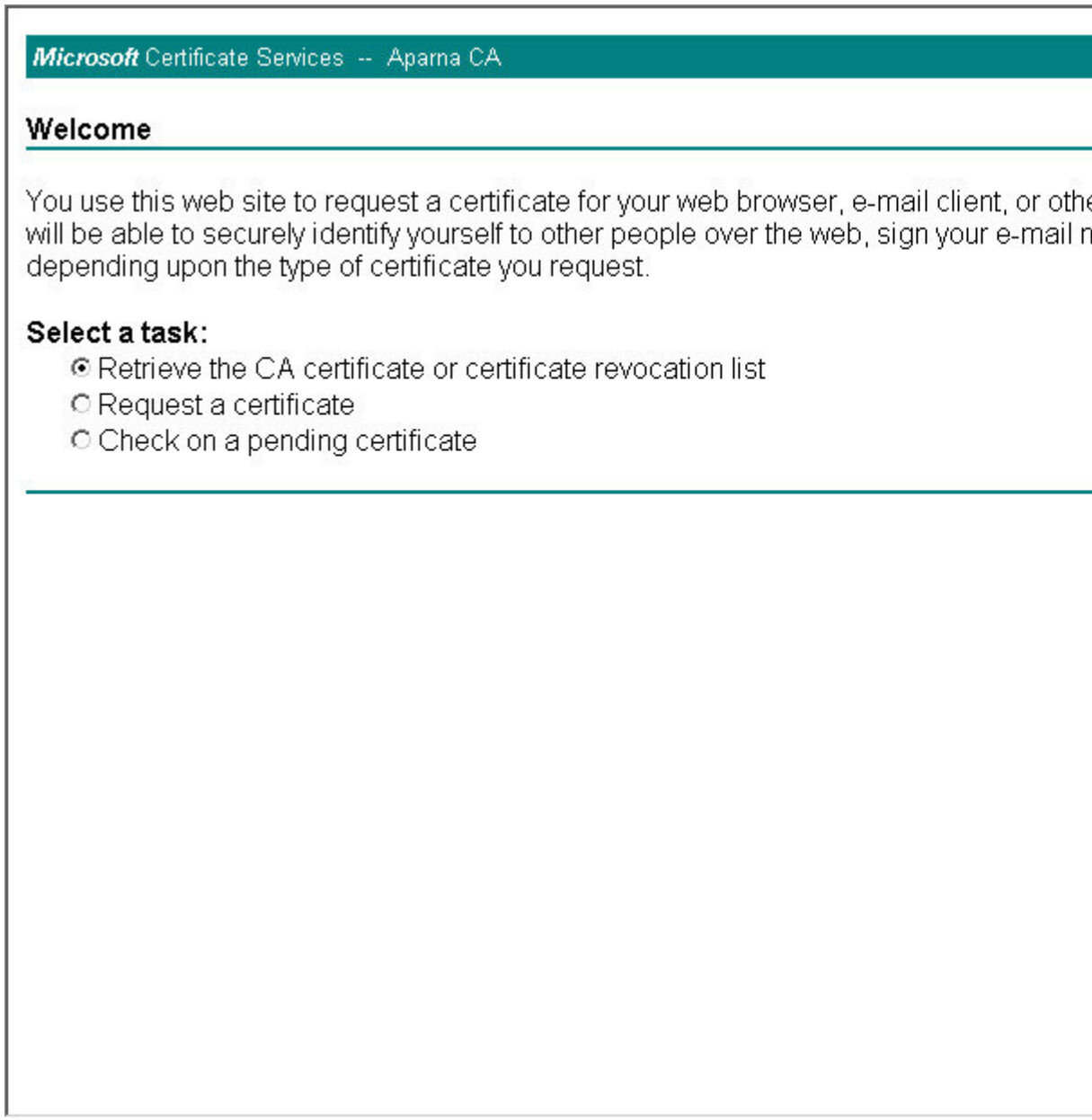


CRL のダウンロード

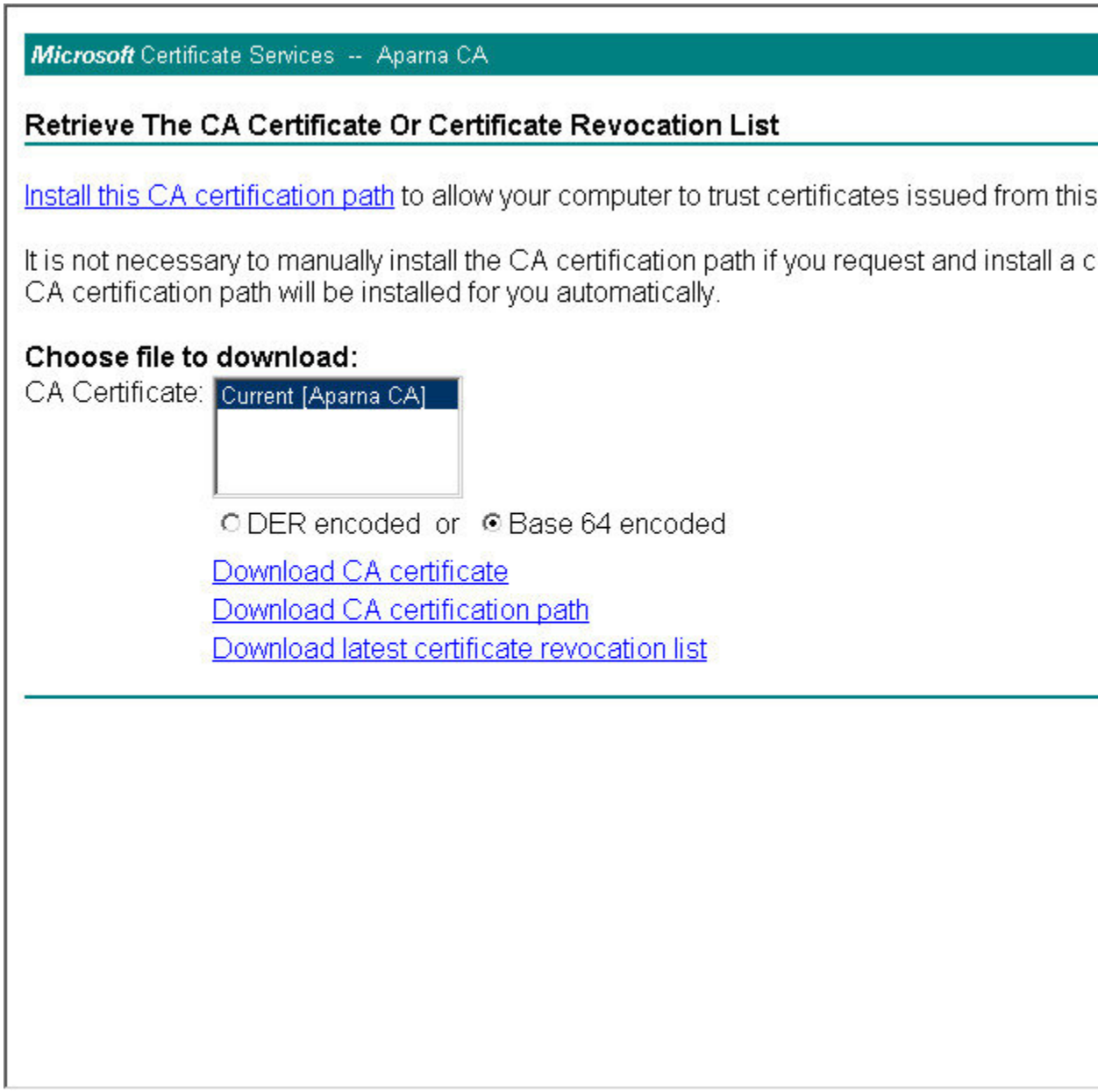
Microsoft 社の CA の Web サイトから CRL をダウンロードする手順は、次のとおりです。

Procedure

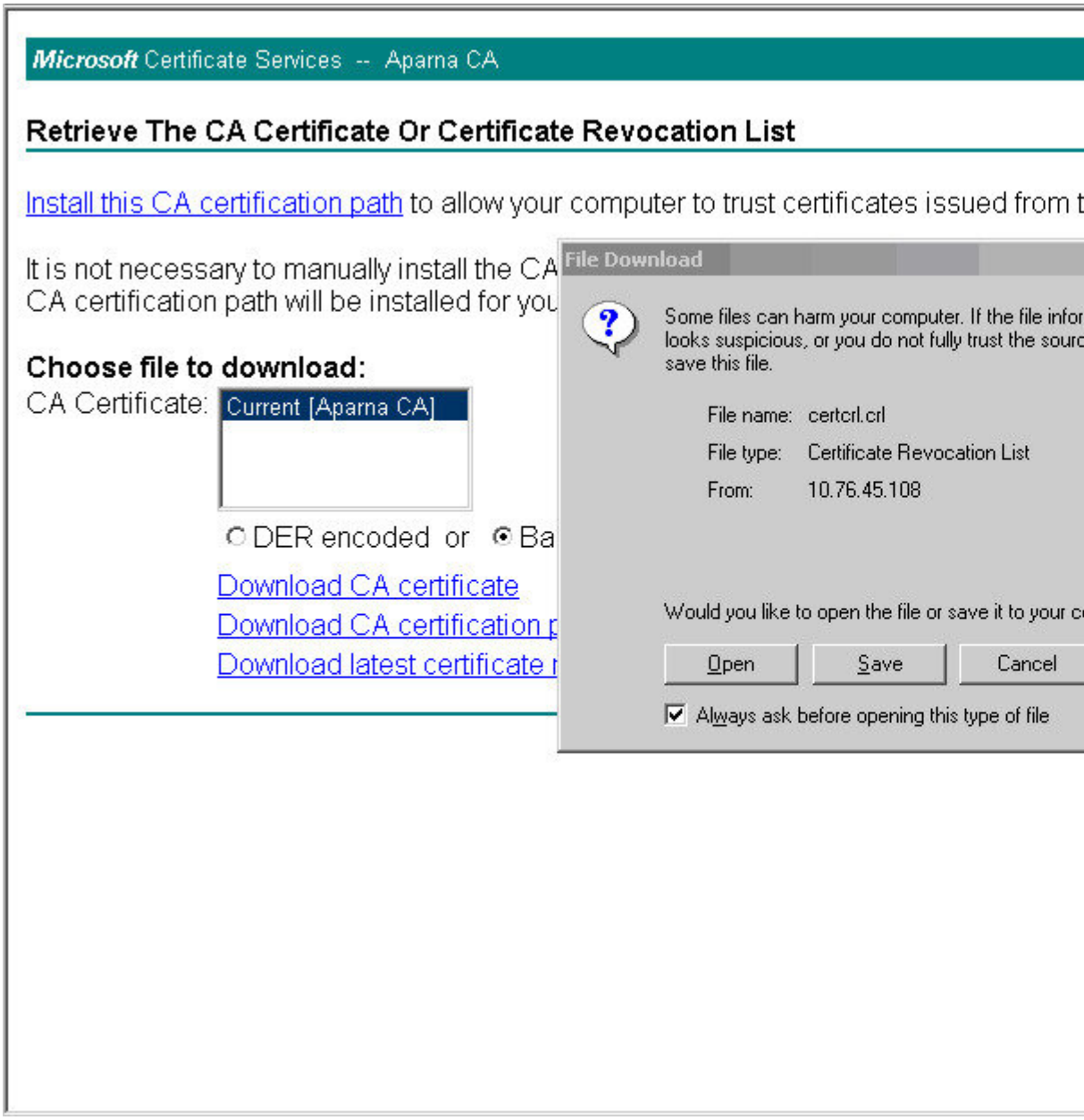
ステップ 1 Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation list] をクリックし、[Next] をクリックします。



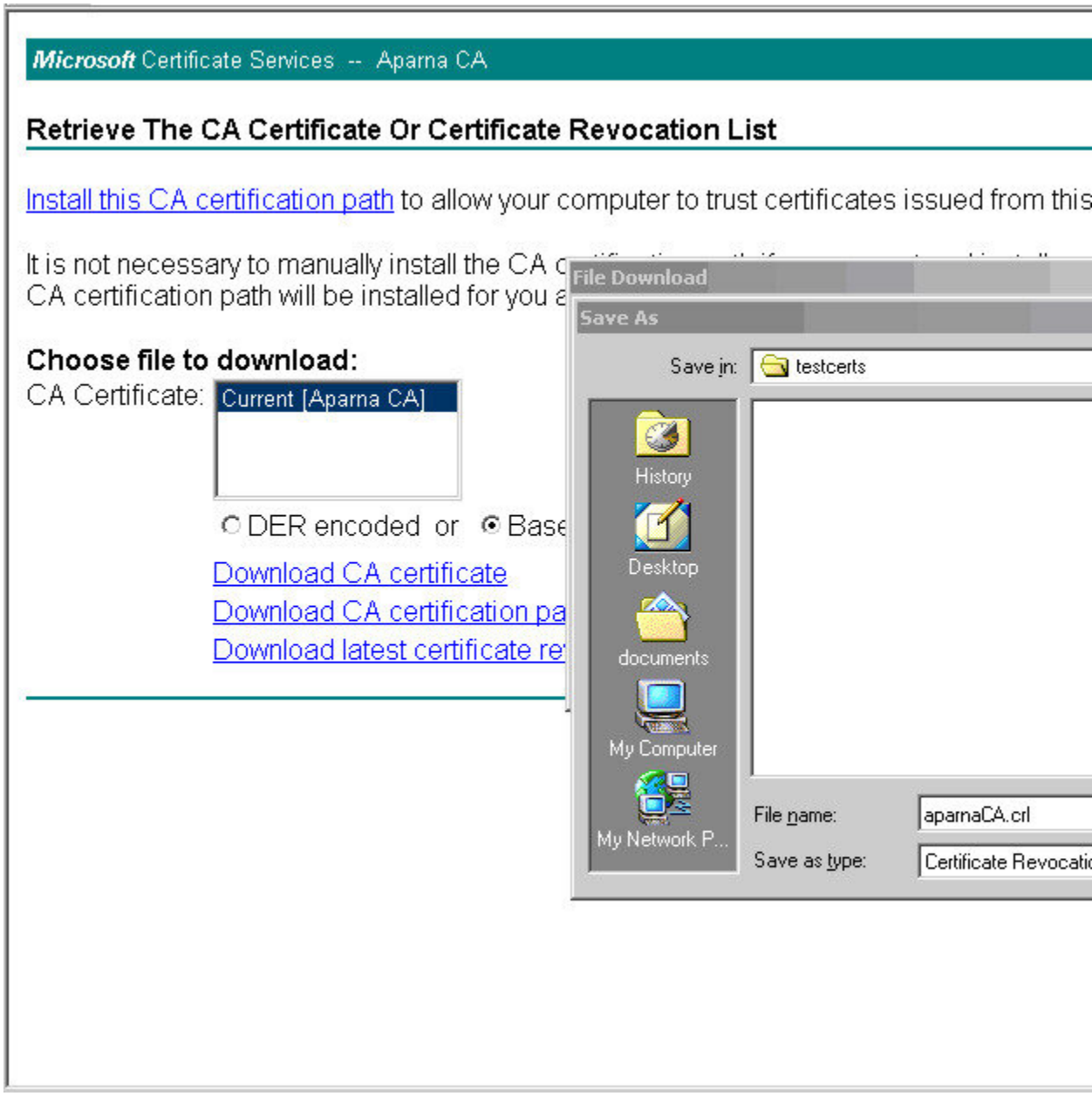
ステップ 2 [Download latest certificate revocation list] をクリックします。



ステップ 3 [File Download] ダイアログボックスで、[Save] をクリックします。



ステップ 4 [Save As] ダイアログボックスで、保存するファイル名を入力して、[Save] をクリックします。



ステップ 5 Microsoft Windows の type コマンドを入力して、CRL を表示します。

Related Topics

証明書取消確認方法の設定 （19 ページ）

CRL のインポート

CRL を CA に対応するトラストポイントにインポートする手順は、次のとおりです。

Procedure

ステップ 1 CRL ファイルを Cisco NX-OS デバイスのブートフラッシュにコピーします。

```
Device-1# copy tftp:apranaCA.crl bootflash:aparnaCA.crl
```

ステップ 2 CRL を設定します。

```
Device-1# configure terminal
Device-1(config)# crypto ca crl request myCA bootflash:aparnaCA.crl
Device-1(config)#
```

ステップ 3 CRL の内容を表示します。

```
Device-1(config)# show crypto ca crl myCA
Trustpoint: myCA
CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
Yourcompany/OU=netstorage/CN=Aparna CA
        Last Update: Nov 12 04:36:04 2005 GMT
        Next Update: Nov 19 16:56:04 2005 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1
            1.3.6.1.4.1.311.21.1:
                ...
Revoked Certificates:
    Serial Number: 611B09A1000000000002
        Revocation Date: Aug 16 21:52:19 2005 GMT
Serial Number: 4CDE464E000000000003
        Revocation Date: Aug 16 21:52:29 2005 GMT
    Serial Number: 4CFC2B42000000000004
        Revocation Date: Aug 16 21:52:41 2005 GMT
    Serial Number: 6C699EC2000000000005
        Revocation Date: Aug 16 21:52:52 2005 GMT
    Serial Number: 6CCF7DDC000000000006
        Revocation Date: Jun  8 00:12:04 2005 GMT
    Serial Number: 70CC4FFF000000000007
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 4D9B1116000000000008
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 52A80230000000000009
        Revocation Date: Jun 27 23:47:06 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            CA Compromise
Serial Number: 5349AD4600000000000A
        Revocation Date: Jun 27 23:47:22 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            CA Compromise
Serial Number: 53BD173C00000000000B
        Revocation Date: Jul  4 18:04:01 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Certificate Hold
Serial Number: 591E7ACE00000000000C
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E00000000000D
        Revocation Date: Jun 29 22:07:25 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Key Compromise
Serial Number: 5DAB771300000000000E
```

```
        Revocation Date: Jul 14 00:33:56 2005 GMT
    Serial Number: 5DAE53CD000000000000F
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5DB140D3000000000010
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5E2D7C1B000000000011
        Revocation Date: Jul  6 21:12:10 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Cessation Of Operation
Serial Number: 16DB4F8F000000000012
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 261C3924000000000013
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 262B5202000000000014
        Revocation Date: Jul 14 00:33:10 2005 GMT
    Serial Number: 2634C7F2000000000015
        Revocation Date: Jul 14 00:32:45 2005 GMT
    Serial Number: 2635B000000000000016
        Revocation Date: Jul 14 00:31:51 2005 GMT
    Serial Number: 26485040000000000017
        Revocation Date: Jul 14 00:32:25 2005 GMT
    Serial Number: 2A276357000000000018
Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 3F88CBF7000000000019
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 6E4B5F5F00000000001A
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 725B89D800000000001B
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 735A887800000000001C
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 148511C700000000001D
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 14A7170100000000001E
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 14FC45B500000000001F
        Revocation Date: Aug 17 18:30:42 2005 GMT
    Serial Number: 486CE80B000000000020
        Revocation Date: Aug 17 18:30:43 2005 GMT
    Serial Number: 4CA4A3AA000000000021
        Revocation Date: Aug 17 18:30:43 2005 GMT
    Serial Number: 1AA55C8E00000000002F
        Revocation Date: Sep  5 17:07:06 2005 GMT
    Serial Number: 3F0845DD00000000003F
        Revocation Date: Sep  8 20:24:32 2005 GMT
    Serial Number: 3F619B7E000000000042
        Revocation Date: Sep  8 21:40:48 2005 GMT
    Serial Number: 6313C463000000000052
        Revocation Date: Sep 19 17:37:18 2005 GMT
    Serial Number: 7C3861E3000000000060
        Revocation Date: Sep 20 17:52:56 2005 GMT
    Serial Number: 7C6EE351000000000061
        Revocation Date: Sep 20 18:52:30 2005 GMT
    Serial Number: 0A338EA1000000000074   <-- Revoked identity certificate
        Revocation Date: Nov 12 04:34:42 2005 GMT
    Signature Algorithm: sha1WithRSAEncryption
        0b:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32:
        44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96:
        29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1:
        1a:9f:1a:49:b7:9c:58:24:d7:72
```

Note

取り消されたデバイスのアイデンティティ証明書（シリアル番号は 0A338EA1000000000074）が最後に表示されています。

PKI に関する追加情報

ここでは、PKI の実装に関する追加情報について説明します。

PKI の関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	*Cisco NX-OS* ライセンス ガイド
VRF コンフィギュレーション	『*Cisco Nexus 9000* シリーズ *NX-OS* ユニキャスト ルーティング設定ガイド』

PKI の標準規格

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

Cisco SUDI 証明書チェーンを使用したデバイス構成証明

Cisco NX-OSリリース 10.6(2) 以降、 Cisco Nexus 9000 スイッチは、 Cisco Secure Unique Device Identifier（SUDI）証明書チェーンの構成証明と署名をサポートします。この機能により、スイッチは SUDI 証明書チェーンを表示し、ユーザーが提供するナンスに基づいて署名を生成でき、デバイス本人確認と外部システムとの統合をサポートします。

SUDI 証明書チェーン証明書の利点

この機能は、複数の利点を提供します：

- デバイス本人確認（Device identity verification）：管理者および自動システムは、SUDI 証明書チェーンと署名を取得してスイッチのアイデンティティを検証できます。
- バックエンドシステムとの統合：スイッチは、CLI コマンドを使用して SUDI 証明書チェーンと署名を表示できます。出力は自動化してバックエンドサーバーが使用するために JSON 形式で利用できます。

- 自動化および規則遵守ワークフローのサポート：JSON でのCLI出力により、証明書チェーンと署名の取得と処理の自動化が可能になり、既存の顧客システムとの統合が促進されます。
- セキュアなオンボーディングとゼロ トラスト ワークフローのサポート：重要なインフラインフラストラクチャへのアクセスを許可する前に、デバイスの信頼性が必要な環境でデバイス アイデンティティの証明を有効にします。

SUDI 証明書チェーン構成証明および署名の仕組み

Cisco NX-OSリリース 10.6（2）により、 Cisco Nexus 9000 スイッチはセキュアな固有デバイス識別子（SUDI）証明書チェーンを表示し、デバイス構成構成証明の署名を生成できます。このプロセスにより、ユーザーは標準規格のCLI コマンドを介して証明書チェーンと署名を確認することで、スイッチを認証ます。

process_summary

このプロセスにより、ユーザーはSUDI 証明書チェーンを取得し、スイッチ CLI を使用してデバイス構成証明の署名を生成できます。

process_workflow

SUDI 証明書の構成証明と署名のプロセスには、次の手順が含まれます：

1. ユーザーは CLI を介してスイッチにアクセスし、SUDI 証明書チェーンを取得するか、または指定された値（nonce）を使用して署名付き応答を生成する要求を開始します。
2. スイッチは、セキュア ストレージから SUDI 証明書チェーンを取得します。
3. ナンスが指定されている場合、スイッチは証明書チェーンとナンスを使用して署名を生成します。
4. スイッチは、証明書チェーンと、該当する場合は、選択した出力形式で署名を表示します。
5. ユーザーは、表示された情報をデバイスの検証や外部システムとの統合に使用できます。

注意事項と制約事項

- この機能は、必要なセキュアなストレージと関連サービスを提供するプラットフォームでのみサポートされます。必要なハードウェアまたはサービスがない場合、機能は利用できません。
- SUDI 証明書チェーンと署名機能には、スイッチのコマンドライン インターフェイスからのみアクセスできます。
- 署名を生成するために、ユーザーが提供するナンスが必要です。ナンスが指定されていない場合は、証明書チェーンのみが表示されます。

- 出力は標準規格または JSON 形式で表示できるため、手動での確認と自動処理の両方が可能になります。
- この機能は、デバイス認証、構成証明、または自動検証ワークフローが必要な環境を対象としています。

SUDI 証明書チェーンの構成証明と署名の確認

次のコマンドを使用して、デバイスの SUDI 証明書チェーンの構成証明および署名機能を確認します。

SUDI 証明書チェーンを表示し、ナンスを使用して署名を生成し、自動化のために JSON 形式での出力を表示できます。

このタスクでは、デバイスによって提供される構成証明および署名情報にアクセスして確認する方法を示します。

手順

ステップ 1 このコマンドを使用し、ユーザー指定のナンス値を使用して、SUDI 証明書チェーンの署名を生成します（<hex_nonce> は 16 進のナンス文字列で置き換えます）。

例：

```
sh platform security certificate sudi nonce <hex_nonce>
```

```
switch# sh platform security certificate sudi nonce abc123
------------------------------------ Node location: SUP
------------------------------------ Nonce: abc123 Certificate name: Cisco SUDI Root
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
BAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwOTkwIBcNMTYwODA5 ... -----END
CERTIFICATE----- Certificate name: Cisco SUDI CA -----BEGIN CERTIFICATE-----
MIIEZzCCA0+gAwIBAgIJCmR1UkzYYXxiMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV ... -----END
CERTIFICATE----- Certificate name: Cisco SUDI -----BEGIN CERTIFICATE-----
MIID2DCCAsCgAwIBAgIKCINIgmUgRgUJpTANBgkqhkiG9w0BAQsFADAxMR8wHQYD ... -----END
CERTIFICATE----- signature:
[redacted]
 signature_version: 2
```

SUDI 証明書チェーンおよび指定されたナンス値で生成された署名を表示します。出力には、ノードの場所、ナンス、証明書、署名、および署名バージョンが含まれます。

ノードの場所、ナンス、証明書チェーン、および署名が出力に表示されます。

ステップ 2 JSON 形式の出力を表示します。自動化やスクリプトまたは外部システムとの統合のために、「| json-pretty」オプションをコマンドに追加します。

例：

```
sh platform security certificate sudi <hex_nonce> | json-pretty
```

```
switch# sh platform security certificate sudi nonce abc123 | json-pretty
{ "system-certificates": { "TABLE_system-certificates": { "ROW_system-certificates": {
"node-location": "SUP", "nonce": "YWJjMTIz", "certificates": { "TABLE_certificate": {
```

"ROW_certificate": [{ "name": "Cisco SUDI Root",
"value":"MIIDITCCAgmgAwIBAgIJAZozWHjOFsHEMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNVBAoTBUNpc2NvMRswGQYDVQQDExJDaXNjbyBSb290...ENDCERTIFICATE-----"
 }, { "name": "Cisco SUDI CA", "value":
"MIIEZzCCA0+gAwIBAgIJCmR1UkzYYXxiMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNVBAoTBUNpc2Nv...END
CERTIFICATE-----" }, { "name": "Cisco SUDI", "value":
"MIID2DCCAsCgAwIBAgIKCINIgmUgRgUJpTANBgkqhkiG9w0BAQsFADAxMR8wHQYD...END CERTIFICATE-----"
 }] } }, "signature":
"[redacted]",
 "signature_version": "2" } } } }

自動化と統合のために、JSON 形式で SUDI 証明書チェーンと署名を提供します。出力には、ノードの場所、ナンス（Base64 エンコード）、証明書、署名、および署名バージョンが含まれます。

JSON 出力には、ノードの場所、ナンス、証明書チェーン、および署名が含まれます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。