認証局相互運用性の実装

認証局（CA）相互運用性は、IP Security（IPSec）、Secure Socket Layer（SSL）および Secure Shell（SSH）プロトコルのサポートとして提供されます。 このモジュールでは、CA 相互運用性を実装する方法について説明します。

CA 相互運用性は、デバイスが CA からデジタル証明書を取得および使用できるように、Cisco ASR 9000 Series Router デバイスと CA の通信を許可します。 IPSec は CA を使用せずにネットワークで実装できますが、CA を使用すると、IPSec の管理性と拡張性が提供されます。

（注） このモジュールで使用される公開キーインフラストラクチャ（PKI）コマンドの詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*』の「*Public Key Infrastructure Commands on* Cisco ASR 9000 シリーズ ルータ」モジュールを参照してください。 このモジュールで言及する他のコマンドについては、コマンド リファレンス マスター インデックス（オンライン検索）を使用して、該当するマニュアルを参照してください。

認証局相互運用性の実装に関する機能履歴

リリース	変更点
リリース 3.7.2	この機能を追加しました。

• 参考資料，17 ページ

認証局の実装に関する前提条件

CA 相互運用性を実装するには、次の前提条件を満たす必要があります。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- セキュリティ ソフトウェアのパッケージインストレーション エンベロープ（PIE）をインストールしてアクティブにする必要があります。

  オプションの PIE インストールの詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*』を参照してください。
- この相互運用性機能を設定する前に、ネットワークでCA を使用可能にする必要があります。CA は、Cisco Systems PKI プロトコル、Simple Certificate Enrollment Protocol（SCEP）（以前の Certificate Enrollment Protocol（CEP））をサポートする必要があります。

認証局の実装に関する制約事項

Cisco IOS XR ソフトウェアは、2048 ビットを超える CA サーバ公開キーをサポートしません。

認証局の実装について

CA を実装するには、次の概念を理解する必要があります。

認証局相互運用性のサポートされている標準

シスコでは次の標準をサポートしています。

- IPsec：IP Security Protocol（IP セキュリティ プロトコル）。 IPSec は、データ保護、参加しているピア間のデータ整合性およびデータ認証を提供するオープン スタンダードです。 IPSec は、IP レイヤでこれらのセキュリティ サービスを提供し、インターネット キー交換（IKE）を使用して、ローカル ポリシーに基づいてプロトコルとアルゴリズムのネゴシエーションを処理し、IPSec で使用する暗号化および認証キーを生成します。 IPSec を使用することにより、ホスト ペア間、セキュリティ ゲートウェイ ペア間、またはセキュリティ ゲートウェイとホスト間の 1 つ以上のデータ フローを保護できます。
- IKE：Oakley キー交換や Skeme キー交換をインターネット セキュリティ アソシエーションおよびキー管理プロトコル（ISAKMP）フレームワーク内部に実装したハイブリッド プロトコルです。 IKE は他のプロトコルで使用できますが、その初期実装時は IPSec プロトコルで

使用します。 IKE は、IPSec ピアの認証を提供し、IPSec キーを交渉し、IPSec セキュリティ アソシエーション（SA）を交渉します。

- Public-Key Cryptography Standard #7（PKCS #7）：証明書登録メッセージの暗号化および署名に使用される RSA Data Security Inc. の標準。
- Public-Key Cryptography Standard #10（PKCS #10）：証明書要求のための RSA Data Security Inc. の標準構文。
- RSA キー：RSA は公開キー暗号化システムで、Ron Rivest、Adi Shamir、Leonard Adelman の 3 名によって開発されました。 RSA キーは、1 つの公開キーと 1 つの秘密キーのペアになっています。
- SSL：Secure Socket Layer プロトコル。
- X.509v3 証明書：同等のデジタル ID カードを各デバイスに提供することで、IPSec で保護されたネットワークの拡張を可能にする証明書サポート。 2 台の装置が通信する際、デジタル証明書を交換することで ID を証明します（これにより、各ピアで公開キーを手動で交換したり、各ピアで共有キーを手動で指定したりする必要がなくなります）。 これらの証明書は CA から取得されます。 X.509 は、ITU の X.500 標準の一部です。

認証局

次の項では、CA の背景情報を説明します。

CA の目的

CA は、証明書要求を管理し、参加する IPSec ネットワーク デバイスへの証明書の発行します。これらのサービスは、参加デバイスのキー管理を一元化して行います。

CA は、IPSec ネットワーク デバイスの管理を簡素化します。 CA は、ルータなど、複数の IPSec 対応デバイスを含むネットワークで使用できます。

Public Key Cryptography によりイネーブルにされたデジタル署名は、デバイスおよび個人ユーザをデジタル認証します。 RSA 暗号化システムなどの Public Key Cryptography では、各ユーザは、公開キーと秘密キーの両方を含むキーペアを使用します。 これらのキーは、補足として機能し、一方で暗号化されたものは、もう一方で復号化できます。 つまり、シグニチャは、データがユーザの秘密キーで暗号化されるときに形成されます。 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。 メッセージは、送信側の公開キーを使用して復号化できるため、秘密キーの所有者、つまり送信者がメッセージを作成することになります。 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。

デジタル証明書はリンクを提供します。 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。 証明書自体は、受信者が身元を証明し、デジタル証明書を作成するうえで確実に信頼できるサード パーティである、CA により署名されます。

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。 通常、このプロセスは、アウトオブバンドで、またはインストールで行われる操作により処理されます。 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。 IKE は、IPSec の必須要素で、デジタル証明書を使用して、SA を設定する前にピア デバイスの拡張性を認証します。

デジタル シグニチャがない場合、ユーザは、IPSec を使用するデバイスの各ペア間で公開キーまたはシークレットを手動で交換して、通信を保護する必要があります。 証明書がない場合、ネットワークに新しいデバイスが追加されるたびに、安全に通信を行う他のすべてのデバイスで設定を変更する必要があります。 デジタル証明書がある場合、各デバイスは、CA に登録されます。 2 台のデバイスが通信する場合、証明書を交換し、データをデジタル署名して、お互いを認証します。 新しいデバイスがネットワークに追加されると、ユーザは、そのデバイスを CA に登録します。他のデバイスでは変更の必要はありません。 新しいデバイスが IPSec 接続を試行すると、証明書が自動的に交換され、デバイスを認証できます。

CA がない IPSec

CA を使用せずに、2 つの Cisco ルータ間で IPSec サービス（暗号化など）をイネーブルにする場合、最初に、各ルータにもう一方のルータのキー（RSA 公開キーや共有キー）が存在するか確認する必要があります。 つまり、次のいずれかの操作を手動で実行する必要があります。

- 各ルータで、もう一方のルータの RSA 公開キーを入力します。
- 各ルータで、両方のルータで使用される共有キーを指定します。

複数の Cisco ルータをメッシュ トポロジで配置し、すべてのルータ間で IPSec トラフィックを交換させる場合には、最初に、すべてのルータ間に共有キーまたは RSA 公開キーを設定する必要があります。

IPSec ネットワークに新しいルータを追加するごとに、新しいルータと既存の各ルータ間にキーを設定する必要があります

したがって、IPSec サービスを必要とするデバイスが増えるほど、キー管理は複雑になります。 このアプローチでは、より大型で複雑な暗号化ネットワークには拡張できません。

CA がある IPSec

CA を使用する場合、すべての暗号化ルータ間でキーを設定する必要はありません。 代わりに、加入させる各ルータを CA に個別に登録し、各ルータの証明書を要求します。 この登録が完了していれば、各加入ルータは、他のすべての加入ルータをダイナミックに認証できます。

ネットワークに新しい IPSec ルータを追加する場合、新しいルータが CA に証明書を要求するように設定するだけでよく、既存の他のすべての IPSec ルータとの間に複数のキー設定を行う必要はありません。

複数のトラストポイント CA がある IPSec

複数のトラストポイント CA がある場合、証明書をピアに発行した CA にルータを登録する必要はありません。 その代わり、信頼できる複数の CA にルータを設定します。 そのため、ルータは、設定された CA（信頼できるルート）を使用して、ルータ ID で定義されている同じ CA により発行されていない証明を、ピアが提供したかどうかを検証できます。

複数の CA を設定することにより、IKE を使用して IPSec トンネルを確立する場合に、異なるドメイン（異なる CA）に登録した 2 台以上のルータ間で相互の ID を確認できます。

SCEP では、各ルータは、CA（登録 CA）で設定されます。 CA は、CA の秘密キーで署名されるルータに証明書を発行します。同じドメインのピアの証明書を確認するため、ルータは、登録CA のルート証明書でも設定されます。

異なるドメインからピアの証明書を確認するには、そのピアのドメインの登録 CA のルート証明書をルータで安全に設定する必要があります。

IKE フェーズ I の署名の検証中、発信側は CA 証明書のリストを応答側に送信します。応答側は、リストのいずれかの CA により発行される証明書を送信する必要があります。 証明書が検証されたら、証明書に含まれる公開キーを公開キー リングに保存します。

複数のルート CA がある場合、バーチャル プライベート ネットワーク（VPN）ユーザは、一方のドメインで信頼を確立して、もう一方のドメインで簡単かつ安全に配布できます。 そのため、異なるドメインで認証されるエンティティ間の必要なプライベート通信チャネルが発生します。

IPSec デバイスにより CA 証明書の使用方法

2 台の IPSec ルータが IPSec で保護されたトラフィックを交換するには、最初に相互に認証しあう必要があります。認証されていない場合、IPSec 保護が適用されません。 この認証を行うには、IKE を使用します。

CA を使用しない場合、ルータは、RSA 暗号化ナンスまたは事前共有キーを使用してリモート ルータに自身を認証します。 いずれの方式でも、2 つのルータ間でキーを事前に設定しておく必要があります。

CA を使用する場合、ルータはリモート ルータに証明書を送信し、何らかの公開キー暗号法を実行することによって、ルータ スイッチに対して自身を認証します。 各ルータは、CA により発行されて検証された、ルータ固有の証明書を送信する必要があります。 このプロセスが有効なのは、各ルータの証明書にルータの公開キーがカプセル化され、各証明書が CA によって認証されることにより、すべての加入ルータが CA を認証局として認識するからです。 この機構は、RSA シグニチャを使用する IKE と呼ばれます。

ルータは、証明書が期限切れになるまで、複数の IPSec ピアに対して、複数の IPSec セッション用に自身の証明書を継続的に送信できます。 証明書が期限満了になったときは、ルータの管理者は新しい証明書を CA から入手する必要があります。

ルータが別のドメイン（異なる CA）のピアから証明書を受信した場合、ルータの CA からダウンロードした証明書失効リスト（CRL）には、そのピアの証明書情報は含まれません。 そのため、Lightweight Directory Access Protocol（LDAP）URL で設定したトラストポイントで発行された CRL をチェックして、ピアの証明書が失効しているかどうかを確認します。

LDAP URL で設定されているトラストポイントにより発行された CRL を照会するには、トラストポイント コンフィギュレーション モードで **query url** コマンドを使用します。

CA 登録局

CA によっては、実装の一部として登録局（RA）を使用します。 RA は CA のプロキシの役割を果たすサーバであるため、CA が使用できないときも CA 機能は継続しています。

CA 相互運用性の実装方法

この項では、次の手順について説明します。

ルータのホスト名および IP ドメイン名の設定

この作業では、ルータのホスト名および IP ドメイン名を設定します。

ルータのホスト名および IP ドメイン名が未設定の場合には、これらを設定する必要があります。ホスト名および IP ドメイン名が必要なのは、ルータが完全修飾ドメイン名（FQDN）を IPSec により使用されるキーおよび証明書に割り当て、ルータに割り当てられたホスト名および IP ドメイン名に FQDN が基づいているためです。 たとえば、router20.example.com という名前の証明書は、router20 というルータのホスト名と example.com というルータの IP ドメイン名に基づいています。

手順の概要

1. **configure**
2. **hostname** *name*
3. **domain name domain-name**
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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。

	コマンドまたはアクション	目的
ステップ 2	**hostname** *name* 例： `RP/0/RSP0/CPU0:router(config)# hostname myhost`	ルータのホスト名を設定します。
ステップ 3	**domain name domain-name** 例： `RP/0/RSP0/CPU0:router(config)# domain name mydomain.com`	ルータの IP ドメイン名を設定します。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータがEXECモードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーションファイルに設定変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

RSA キー ペアの生成

RSA キー ペアを生成します。

RSA キー ペアはIKE キー交換管理メッセージの署名および暗号化に使用されます。また、ルータの証明書を取得する際に必要です。

手順の概要

1. **crypto key generate rsa** [**usage keys** | **general-keys**] [**keypair-label**]
2. **crypto key zeroize rsa** [**keypair-label**]
3. show crypto key mypubkey rsa

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto key generate rsa** [**usage keys** | **general-keys**] [**keypair-label**] 例： `RP/0/RSP0/CPU0:router# crypto key generate rsa general-keys`	RSA キー ペアを生成します。 • **usage keys** キーワードを使用して、特殊用途キーを指定します。**general-keys** キーワードを使用して、汎用 RSA キーを指定します。 • *keypair-label* 引数は、RSA キー ペアを指定する RSA キー ペア ラベルです。
ステップ 2	**crypto key zeroize rsa** [**keypair-label**] 例： `RP/0/RSP0/CPU0:router# crypto key zeroize rsa key1`	（任意）ルータからすべての RSA を削除します。 • 場合によっては、すべての RSA キーをルータから削除します。 たとえば、何らかの原因で RSA キーペアの信用性が失われ、使用しなくなった場合、そのキーペアを削除します。 • 特定の RSA キー ペアを削除するには、*keypair-label* 引数を使用します。
ステップ 3	show crypto key mypubkey rsa 例： `RP/0/RSP0/CPU0:router# show crypto key mypubkey rsa`	（任意）ルータの RSA 公開キーを表示します。

公開キーのルータへのインポート

公開キーをルータにインポートします。

公開キーがルータにインポートされ、ユーザが認証されます。

手順の概要

1. **crypto key import authentication rsa** [**usage keys** | **general-keys**] [**keypair-label**]
2. show crypto key mypubkey rsa

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto key import authentication rsa** [**usage keys** | **general-keys**] [**keypair-label**] 例： `RP/0/RSP0/CPU0:router# crypto key import authentication rsa general-keys`	RSA キー ペアを生成します。 • **usage keys** キーワードを使用して、特殊用途キーを指定します。**general-keys** キーワードを使用して、汎用 RSA キーを指定します。 • *keypair-label* 引数は、RSA キー ペアを指定する RSA キー ペア ラベルです。
ステップ 2	show crypto key mypubkey rsa 例： `RP/0/RSP0/CPU0:router# show crypto key mypubkey rsa`	（任意）ルータの RSA 公開キーを表示します。

認証局の宣言および信頼できるポイントの設定

CA を宣言し、信頼できるポイントを設定します。

手順の概要

1. **configure**
2. **crypto ca trustpoint ca-name**
3. **enrollment url CA-URL**
4. **query url LDAP-URL**
5. **enrollment retry period minutes**
6. **enrollment retry count number**
7. **rsakeypair keypair-label**
8. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 trustpoint ca-name** 例： `RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca`	CA を宣言します。 • ルータがピアに対して発行された証明書を確認できるように、選択した名前で信頼できるポイントを設定します。 • 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	**enrollment url CA-URL** 例： `RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://ca.domain.com/certsrv/mscep/mscep.dll`	CA の URL を指定します。 • URL には、非標準 cgi-bin スクリプトの場所が含まれている必要があります。
ステップ 4	**query url LDAP-URL** 例： `RP/0/RSP0/CPU0:router(config-trustp)# query url ldap://my-ldap.domain.com`	（任意）CA システムにより LDAP プロトコルがサポートされている場合、LDAP サーバの位置を指定します。
ステップ 5	**enrollment retry period minutes** 例： `RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 2`	（任意）再試行期間を指定します。 • 証明書の要求後、ルータは CA からの証明書の受け取りを待機します。ルータが期間（再試行期間）内に証明書を受け取らない場合、ルータは、別の証明書要求を送信します。 • 範囲は 1 ～ 60 分です。 デフォルトは 1 分です。
ステップ 6	**enrollment retry count number** 例： `RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry count 10`	（任意）失敗した証明書要求送信を続行する回数を指定します。 • 範囲は 1 ～ 100 です。

	コマンドまたはアクション	目的
ステップ 7	**rsakeypair keypair-label** 例： `RP/0/RSP0/CPU0:router(config-trustp)# rsakeypair mykey`	（任意）このトラストポイントに **crypto key generate rsa** コマンドを使用して生成した指定 RSA キー ペアを指定します。 • このキーペアを設定しない場合、トラストポイントは現在の設定のデフォルトの RSA キーを使用します。

ステップ 8	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーションファイルに設定変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

CA の認証

CA をルータに対して認証します。

ルータは、CA の公開キーを含む CA の自己署名証明書を取得して CA を認証する必要があります。 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。

手順の概要

1. **crypto ca authenticate ca-name**
2. show crypto ca certificates

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto ca authenticate ca-name** 例： `RP/0/RSP0/CPU0:router# crypto ca authenticate myca`	CA の公開キーを含む CA 証明書を取得することで、ルータに対して CA を認証します。
ステップ 2	show crypto ca certificates 例： `RP/0/RSP0/CPU0:router# show crypto ca certificates`	（任意）CA証明書に関する情報を表示します。

独自の証明書の要求

証明書を CA から要求します。

ルータの各 RSA キー ペアに対して、署名された証明書を CA から取得する必要があります。 汎用 RSA キーを生成した場合、ルータの RSA キー ペアは 1 つだけなので、必要な証明書は 1 つだけです。 特殊用途 RSA キーを生成した場合、ルータには 2 つの RSA キー ペアがあるので、必要な証明書は 2 つです。

手順の概要

1. **crypto ca enroll ca-name**
2. show crypto ca certificates

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto ca enroll ca-name** 例： `RP/0/RSP0/CPU0:router# crypto ca enroll myca`	すべての RSA キー ペアの証明書を要求します。 • このコマンドでは、ルータは存在する RSA キー ペアと同数の証明書を要求するため、特定目的の RSA キー ペアがある場合にも、このコマンドは 1 回しか実行する必要はありません。

	コマンドまたはアクション	目的
		• このコマンドでは、設定に保存されないチャレンジパスワードを作成する必要があります。証明書を失効させる必要が生じた場合、このパスワードが要求されるので、このパスワードを覚えておく必要があります。 • 証明書はすぐに発行できます。または、登録リトライ時間に達し、タイムアウトが発生するまで、ルータが証明書要求を毎分送信します。タイムアウトが発生した場合、システム管理者に要求承認を依頼して、このコマンドを再入力します。
ステップ 2	show crypto ca certificates 例： `RP/0/RSP0/CPU0:router# show crypto ca certificates`	（任意）CA 証明書に関する情報を表示します。

カットアンドペーストによる証明書登録の設定

ルータが使用するトラストポイント認証局（CA）を宣言して、このトラストポイント CA をカットアンドペーストによる手動登録に設定します。

手順の概要

1. **configure**
2. **crypto ca trustpoint** *ca-name*
3. enrollment terminal
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
5. **crypto ca authenticate** *ca-name*
6. **crypto ca enroll** *ca-name*
7. **crypto ca import** ca- *name* **certificate**
8. show crypto ca certificates

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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 trustpoint** *ca-name*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca`
	`RP/0/RSP0/CPU0:router(config-trustp)#`
		ルータが使用するCAを宣言し、CA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。
		• *ca-name* 引数を使用して、CA の名前を指定します。

ステップ 3	enrollment terminal 例： `RP/0/RSP0/CPU0:router(config-trustp)# enrollment terminal`	カットアンドペーストによる手動での証明書登録を指定します。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 5	**crypto ca authenticate** *ca-name* 例： `RP/0/RSP0/CPU0:router# crypto ca authenticate myca`	CA の証明書を取得することにより、CA を認証します。 • *ca-name* 引数を使用して、CA の名前を指定します。ステップ 2, （14 ページ） で入力した名前と同じ名前を使用します。
ステップ 6	**crypto ca enroll** *ca-name* 例： `RP/0/RSP0/CPU0:router# crypto ca enroll myca`	CA からルータの証明書を取得します。 • *ca-name* 引数を使用して、CA の名前を指定します。ステップ 2 で入力した名前と同じ名前を使用します。
ステップ 7	**crypto ca import** ca- *name* **certificate** 例： `RP/0/RSP0/CPU0:router# crypto ca import myca certificate`	端末で証明書を手動でインポートします。 • *ca-name* 引数を使用して、CA の名前を指定します。ステップ 2 で入力した名前と同じ名前を使用します。 （注） 用途キー（シグニチャおよび暗号キー）を使用する場合は、**crypto ca import** コマンドを 2 回入力する必要があります。このコマンドを最初に入力した場合は、認証の 1 つがルータにペーストされます。2 回目に入力した場合は、他の認証がルータにペーストされます（どの認証が最初にペーストされるかは重要ではありません）。
ステップ 8	show crypto ca certificates 例： `RP/0/RSP0/CPU0:router# show crypto ca certificates`	証明書と CA 証明書に関する情報を表示します。

認証局相互運用性の実装の設定例

この項では、次の設定例について説明します。

認証局相互運用性の設定：例

次に、CA 相互運用性を設定する例を示します。

さまざまなコマンドを説明するコメントが設定に含まれます。

```
configure
hostname myrouter
domain name mydomain.com
end
```

```
Uncommitted changes found, commit them? [yes]:yes

crypto key generate rsa mykey

The name for the keys will be:mykey
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keypair
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [1024]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]

show crypto key mypubkey rsa

Key label:mykey
Type     :RSA General purpose
Size     :1024
Created  :17:33:23 UTC Thu Sep 18 2003
Data     :
 30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CB8D86
 BF6707AA FD7E4F08 A1F70080 B9E6016B 8128004C B477817B BCF35106 BC60B06E
 07A417FD 7979D262 B35465A6 1D3B70D1 36ACAFBD 7F91D5A0 CFB0EE91 B9D52C69
 7CAF89ED F66A6A58 89EEF776 A03916CB 3663FB17 B7DBEBF8 1C54AF7F 293F3004
 C15B08A8 C6965F1E 289DD724 BD40AF59 E90E44D5 7D590000 5C4BEA9D B5020301
 0001

! The following commands declare a CA and configure a trusted point.

configure
crypto ca trustpoint myca
enrollment url http://xyz-ultra5
enrollment retry count 25
enrollment retry period 2
rsakeypair mykey
end

Uncommitted changes found, commit them? [yes]:yes

! The following command authenticates the CA to your router.

crypto ca authenticate myca

Serial Number  :01
Subject Name   :
cn=Root coax-u10 Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
Issued By      :
cn=Root coax-u10 Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
Validity Start :07:00:00 UTC Tue Aug 19 2003
Validity End   :07:00:00 UTC Wed Aug 19 2020
Fingerprint:58 71 FB 94 55 65 D4 64 38 91 2B 00 61 E9 F8 05
Do you accept this certificate?? [yes/no]:yes

! The following command requests certificates for all of your RSA key pairs.

crypto ca enroll myca

% Start certificate enrollment ...
% 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:
Re-enter Password:
    Fingerprint: 17D8B38D ED2BDF2E DF8ADBF7 A7DBE35A

! The following command displays information about your certificate and the CA certificate.

show crypto ca certificates

Trustpoint       :myca
```

```
============================================================
CA certificate
  Serial Number  :01
  Subject Name   :
        cn=Root coax-u10 Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
  Issued By      :
        cn=Root coax-u10 Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
  Validity Start :07:00:00 UTC Tue Aug 19 2003
  Validity End   :07:00:00 UTC Wed Aug 19 2020
Router certificate
  Key usage      :General Purpose
  Status         :Available
  Serial Number  :6E
  Subject Name   :
        unstructuredName=myrouter.mydomain.com,o=Cisco Systems
  Issued By      :
        cn=Root coax-u10 Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
  Validity Start :21:43:14 UTC Mon Sep 22 2003
  Validity End   :21:43:14 UTC Mon Sep 29 2003
  CRL Distribution Point
        ldap://coax-u10.cisco.com/CN=Root coax-u10 Certificate Manager,O=Cisco Systems
```

次の作業

CA 相互運用性の設定が終了したら、IKE、IPSec および SSL を設定する必要があります。 IKE 設定については、「*Implementing Internet Key Exchange Security Protocol on* Cisco ASR 9000 シリーズ ルータ」モジュール、「IPSec in the *Implementing IPSec Network Security on* Cisco ASR 9000 シリーズ ルータ」モジュールおよび「SSL in the *Implementing Secure Socket Layer on* Cisco ASR 9000 シリーズルータ」モジュールを参照してください。 これらのモジュールは、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』（この資料）にあります。

参考資料

次の項では、認証局相互運用性の実装に関連する参考資料を提供します。

関連資料

関連項目	ドキュメント名
PKI コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*』の「*Public Key Infrastructure Commands on* Cisco ASR 9000 シリーズ ルータ」モジュール

標準

標準	タイトル
この機能でサポートが追加または変更された標準はありません。また、この機能で変更された既存の標準のサポートはありません。	—

MIB

MIB	MIB リンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検出およびダウンロードするには、URL（http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）にある Cisco MIB Locator を使用して、[Cisco Access Products] メニューでプラットフォームを選択します。

RFC

RFC	タイトル
この機能でサポートが追加または変更された RFC はありません。また、この機能で変更された既存の RFC のサポートはありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html