デジタル証明書の登録

この章では、ASDM を使用してデジタル証明書を登録する方法について説明します。登録が完了すると、その証明書を使用して VPN の LAN 間トンネルおよびリモート アクセス トンネルを認証できます。認証に事前共有鍵だけを使用する場合は、この章を読む必要はありません。

この章には、次の項があります。

（注） この章の手順の実行中に、ASDM ウィンドウに表示されるアトリビュートの詳細を参照するには、**Help** をクリックしてください。

設定手順の概要

CA を登録し、トンネルを認証するための ID 証明書を取得するには、次のタスクを実行します。

（注）　この例では、自動（SCEP）登録を示します。

1. ID 証明書の鍵ペアを作成します。この鍵ペアは、RSA 鍵です。次の項の手順では、RSA 鍵ペアを生成する方法を説明します。
2. トラストポイントを作成します。この例では、トラストポイントの名前は newmsroot です。
3. 登録 URL を設定します。この例で使用している URL は、http://10.20.30.40/certsrv/mscep/mscep.dll です。
4. CA を認証します。
5. CA を登録し、ID 証明書を ASA 上に取得します。

鍵ペアについて

各ピアには、公開鍵と秘密鍵の両方を含む鍵ペアが 1 つあります。これらの鍵は補完的に動作します。一方の鍵で暗号化された通信は、もう一方の鍵で復号化されます。

鍵ペアは、RSA 鍵です。

- 鍵の最大モジュラスは 2048 で、デフォルトのサイズは 1024 ビットです。
- シグニチャ操作の場合、鍵の最大サイズは 4096 ビットです。
- 署名と暗号化の両方に使用できる汎用の RSA 鍵ペアを生成できます。*特定用途向けの* RSA 鍵ペアの場合は、それぞれの目的に応じて分かれるため、対応する ID ごとに 2 つの証明書が必要です。デフォルトの設定は、汎用です。

証明書に鍵ペアを設定するには、生成する鍵ペアを識別するラベルを指定します。次の項では、ASDM を使用して指定のラベル付きの RSA 鍵ペアを生成する方法、およびその他のパラメータのデフォルト設定を使用する方法を説明します。

RSA 鍵ペアの生成

RSA 鍵ペアを生成するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Key Pair** ウィンドウで、**Add** をクリックします。

ステップ 2　**Add Key Pair** ダイアログボックスで情報を設定します。

a. **Name :** デフォルト名を使用する場合はクリックします。または、鍵ペアの名前を入力します。この例では、デフォルトの RSA 鍵を使用しますが、代わりに key1 などの名前を入力できます。

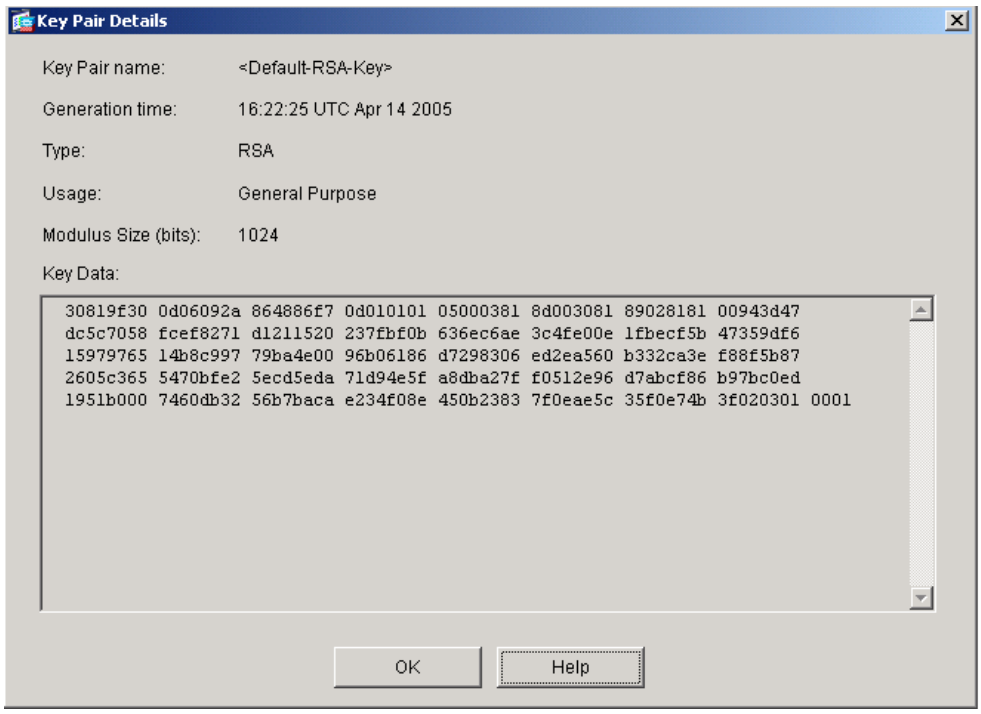
b. **Size** リスト : RSA 鍵ペアの場合、**Size** リストには、オプションとして 512、768、1024、または 2048 が表示されます。デフォルト サイズは 1024 です。この例では、デフォルト設定を受け入れます。

c. **Usage** オプション : オプションは、General Purpose（署名および暗号化の両方に 1 つのペアを使用）と Special（機能ごとに 1 つのペアを使用）です。この例では、デフォルト設定（General Purpose）を受け入れます。

ステップ 3　**Generate Now** をクリックします。

ステップ 4　生成された鍵ペアを表示するには、**Show Details** をクリックします。ASDM に、鍵ペアに関する情報が表示されます。図 1-1 に出力例を示します。

図 1-1　鍵ペアの詳細表示



トラストポイントの作成

トラストポイントは CA と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および 1 つの登録済み ID 証明書とのアソシエーションを含んでいます。トラストポイントを作成するには、使用するインターフェイスの名前の項を参照してください。

トラストポイントを作成するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Trustpoint > Configuration** ウィンドウで、**Add** をクリックします。

ステップ 2　**Add Trustpoint Configuration** ダイアログボックスで、基本情報を設定します。その他のすべてのパラメータについては、デフォルト値を受け入れます。

a. **Trustpoint Name** フィールド：**Trustpoint Name** フィールドにトラストポイントの名前を入力します。この例では、名前は newmsroot です。

b. **Enrollment URL** フィールド：**Enrollment Settings** ウィンドウの **Enrollment Mode** 領域で、**Use automatic enrollment** オプションをオンにします。次に、このフィールドに登録 URL を入力します。この例では、**10.20.30.40/certsrv/mscep/mscep.dll** と入力します。

ステップ 3　Common Name（CN; 通常名）と Organizational Unit（OU; 組織ユニット）の名前を使用して、サブジェクト名を設定します。

a. **Enrollment Settings** ウィンドウの **Key Pair** リストから、このトラストポイントに対して設定した鍵ペアを選択します。この例では、鍵ペアは key1 です。

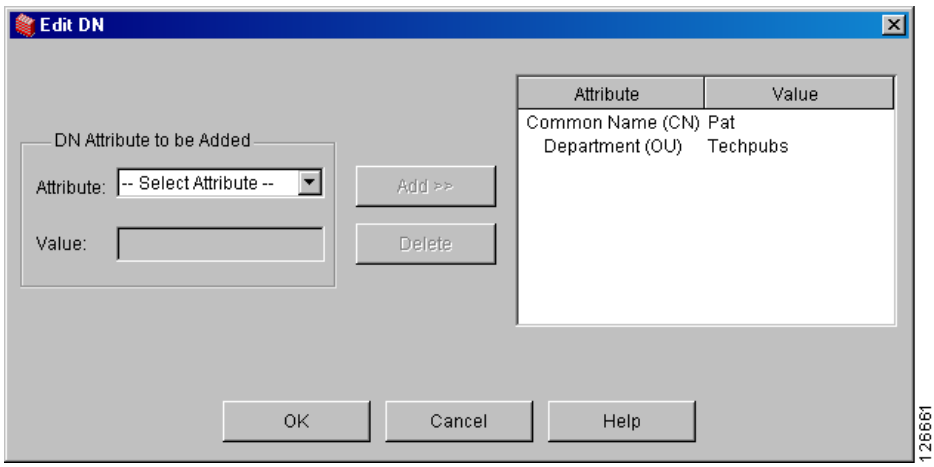
b. **Enrollment Settings** ウィンドウで、**Certificate Parameters** をクリックします。

c. サブジェクト識別名（X.500）の値を追加するには、**Certificate Parameters** ダイアログボックスで **Edit** をクリックします。

d. **Edit DN** 領域で、**DN Attribute to be Added** の下にある **Attribute** リストからアトリビュートを選択し、**Value** フィールドに値を入力します。次に **Add** をクリックします。DN 情報を入力したら、**OK** をクリックします。

この例では、まず **Common Name (CN)** を選択し、**Value** フィールドに **Pat** と入力します。次に Add をクリックしてから、**Department (OU)** を選択して、**Value** フィールドに **Techpubs** と入力します。図 1-2 は、**Edit DN** ダイアログボックスに入力した内容を示しています。

図 1-2　サブジェクト名のアトリビュートと値



ステップ 4　ダイアログボックスを確認したら、**OK** をクリックして、残りの 2 つのダイアログボックスで **OK** をクリックします。

SCEP による証明書の取得

この項では、SCEP を使用して証明書を設定する方法を説明します。自動登録の場合は、設定するトラストポイントごとに手順を繰り返します。各トラストポイントに対する手順が完了すると、セキュリティ アプライアンスは CA 証明書をトラストポイント用に 1 つ、署名および暗号化用に 1 つまたは 2 つを受信します。これらの手順を実行しない場合、セキュリティ アプライアンスによって Base 64 形式の CA 証明書をテキストボックスに貼り付けるよう求められます。

汎用の RSA 鍵を使用する場合、受信した証明書は署名と暗号化を目的としたものです。署名と暗号化に別個の RSA 鍵を使用すると、セキュリティ アプライアンスは目的ごとに別個の証明書を受信します。

証明書を取得するには、次の手順を実行します。

ステップ 1　**Configuration > Properties > Certificate > Authentication** ウィンドウを選択します。

ステップ 2　**Trustpoint Name** リストで、トラストポイントの名前を選択します。この例では、**newmsroot** を選択します。

ステップ 3　**Authenticate** をクリックします。

ステップ 4　**Apply** をクリックします。ASDM で **Authentication Successful** ダイアログが表示されたら、**OK** をクリックします。

認証局への登録

トラストポイントを設定して認証したら、次の手順を実行して ID 証明書を登録できます。

ステップ 1　**Configuration > Properties > Certificate > Enrollment** ウィンドウで、**Trustpoint Name** リストからトラストポイントを選択します。この例では、**newmsroot** を選択します。

ステップ 2　**Enroll** をクリックします。

証明書の管理

証明書を管理するには、**Configuration > Properties > Certificate > Manage Certificates** ウィンドウを使用します。

このウィンドウを使用して、新しい証明書の追加や証明書の削除を行うことができます。

このペインには、次の情報が表示されます。

- Subject：証明書の所有者を特定します。
- Type：CA、RA 全般、RA 暗号化、RA シグニチャ、ID
- Status：Available または Pending
  - Available は、CA が登録要求を受け入れて、ID 証明書を発行したことを意味します。
  - Pending は、登録要求が処理中であるため、CA が ID 証明書をまだ発行していないことを意味します。
- Usage：証明書が使用される方法（シグニチャ、汎用、または暗号化）を特定します。

Show Details をクリックして、証明書に関する情報も表示できます。Certificate Details ダイアログには、3 つのテーブル（General、Subject、および Issuer）が表示されます。

General：タイプ、シリアル番号、ステータス、使用方法、CRL 分散ポイント、証明書の有効期間、および関連付けられたトラストポイントの値を表示します。これは、Available および Pending ステータスの両方に適用されます。

Subject：サブジェクト DN または証明書所有者の X.500 フィールドと値を表示します。これは、Available ステータスだけに適用されます。

Issuer：証明書を付与したエンティティの X.500 フィールドを表示します。これは、Available ステータスだけに適用されます。