CHAPTER 9

RSA キー マネージャと SME

この章では、SME と連携するように RSA キー マネージャ（RKM）をセットアップする際に従うべき手順について説明します。

この章では、次の事項について説明します。

- RKM の前提条件（9-1 ページ）
- RKM の設定（9-1 ページ）
- RKM の機能の履歴（9-6 ページ）

（注） RSA キー マネージャは SME ディスクではサポートされません。これは SME テープにのみ適用されます。

RKM の前提条件

Cisco KMC と RKM との間で完全に機能するセキュリティ ソリューションを実装するには、RKM アプリケーションをインストールしてセットアップする必要があります。

次のアプリケーションが必要です。

- Windows WK2、XP、または W2K3 ホスト
- DCNM-SAN サーバ リリース 3.2(3)
- OpenSSL
- JAVA JDK または JRE

RKM の設定

SME と連携するように RKM をセットアップするプロセスには、次の作業が含まれます。

- RKM アプリケーションのインストール（9-2 ページ）
- CA 証明書の生成（9-2 ページ）
- Java Keytool を使用した JKS ファイルの作成（9-4 ページ）
- RKM での証明書の配置（9-5 ページ）
- Cisco KMC から RKM への移行（9-5 ページ）

これらの作業が完了すると、SME のキー マネージャとして RSA を選択して、クラスタを作成できます。

RKM アプリケーションのインストール

RKM アプリケーションをインストールするには、『*RSA Install Guide*』に記載されている説明に従ってください。

CA 証明書の生成

このプロセスで作成したファイルは、OpenSSL プログラムの /bin ディレクトリに保存されます。

前提条件

- CA 証明書を生成するには、OpenSSL システムへのアクセスが必要です。Windows バージョンは、http://gnuwin32.sourceforge.net/packages/openssl.htm で取得できます。

手順の詳細

CA 証明書を生成するには、次の手順を実行します。

ステップ 1　ディレクトリ内の openssl.exe をダブルクリックします。

ステップ 2　OpenSSL アプリケーションを使用してキーを作成します。次のコマンドを入力します。

```
OpenSSL> genrsa -out rt.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.++++++
.......++++++
e is 65537 (0x10001)
```

ステップ 3　証明書が有効である期間を設定します。この日付を追跡します。

(注)　クライアント証明書とサーバ証明書に異なる共通名を使用します。

```
OpenSSL> req -new -key rt.key -x509 -days 365 -out rt.cert
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:home
Email Address []:
```

ステップ 4　適切な pkcs12 証明書を作成します。エクスポート パスワードは、RSA SME のインストールに必要なパスワードです。

```
OpenSSL> pkcs12 -export -in rt.cert -inkey rt.key -out rt.p12
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
```

ステップ 5　クライアント用の新しいキーを生成します。

```
OpenSSL> genrsa -out client.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
..................++++++
....++++++
e is 65537 (0x10001)
```

ステップ 6　client.csr ファイルを作成します。これは所有者です。共通名は、発行元のホームとは異なっていなければなりません。

```
OpenSSL> req -new -key client.key -out client.csr
You are about to be asked to enter information that will be incorporated into your
certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:cae
Common Name (eg, YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

ステップ 7　証明書が有効である期間を設定します。この日付を追跡します。

```
OpenSSL> x509 -req -days 365 -in client.csr -CA rt.cert -CAkey rt.key -CAcreateserial -out
client.cert
Loading 'screen' into random state - done
Signature ok
subject=/C=AU/ST=wi/L=hudson/O=cisco/OU=cae/CN=mikef/emailAddress=mikef@cisco.com
Getting CA Private Key
```

ステップ 8　pkcs12 証明書を作成します。

```
OpenSSL> pkcs12 -export -in client.cert -inkey client.key -out client.p12
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL> genrsa -out server.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
..++++++
..................++++++
e is 65537 (0x10001)
```

ステップ 9　新しいサーバ キーを作成します。これは所有者です。共通名は、発行元のホームとは異なっていなければなりません。

```
OpenSSL> req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
--
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

ステップ 10　証明書が有効である期間を設定します。この日付を追跡します。

```
OpenSSL> x509 -req -days 365 -in server.csr -CA rt.cert -CAkey rt.key -CAcreateserial -out
server.cert
Loading 'screen' into random state - done
Signature ok
subject=/C=AU/ST=wi/L=town/O=cisco/OU=tac/CN=bill/emailAddress=bill@cisco.com
Getting CA Private Key
```

ステップ 11　serverpub の pkcs12 証明書を作成します。

```
OpenSSL> pkcs12 -export -in server.cert -inkey server.key -nokeys -out serverpub.p12
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
```

ステップ 12　サーバ用の pkcs12 証明書を再作成します。

```
OpenSSL> pkcs12 -export -in server.cert -inkey server.key -out server.p12
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>
```

Java Keytool を使用した JKS ファイルの作成

手順の詳細

JAVA Keytool を使用して DCNM-SAN に必要な JKS ファイルを作成するには、次の手順を実行します。

ステップ 1　OpenSSL /bin ディレクトリにある client.p12 および serverpub.p12 を、DCNM-SAN Java ツールのディレクトリ C:\Program Files\Java\jre1.5.0_11\bin にコピーします。

ステップ 2　Java /bin ディレクトリの DOS ウィンドウから、SME KMC により必要とされる JKS ファイルを作成します。

```
Import client PKCS12 keystore to JKS
keytool -importkeystore -srckeystore client.p12 -srcstoretype PKCS12 -destkeystore
sme_rkm_client.jks -deststoretype JKS
```

```
Import server PKCS12 keystore to JKS
keytool -importkeystore -srckeystore serverpub.p12 -srcstoretype PKCS12 -destkeystore
sme_rkm_trust.jks -deststoretype JKS
```

これらのキーストア ファイルを mds9000/conf/cert ディレクトリ内に配置して、DCNM-SAN を再起動します。

RKM での証明書の配置

手順の詳細

RKM で証明書を配置するには、次の手順を実行します。

ステップ 1　すべての証明書を生成したら、rt.p12 ファイルを C:\rkm-2.1.2-trial\certs\rt ディレクトリにコピーします。

ステップ 2　server.p12 ファイルを C:\rkm-2.1.2-trial\certs\server ディレクトリにコピーします。

ステップ 3　RKM を再起動します。

Cisco KMC から RKM への移行

RKM は SME のインストール時に使用できます。または SME を統合 Cisco KMC とともに後で展開することもできます。Cisco KMC を単独で使用した後に RKM を展開する場合は、RKM を SME とともに使用する前に、明示的なキー移行手順を実行する必要があります。

この項では、暗号キー、ラップ キー、および暗号ポリシー情報を、Cisco KMC から RKM に移行する手順を説明します。

（注）　移行手順は、Cisco KMC が PostgresSQL データベースまたは Oracle Express データベースをキー カタログ用に使用している場合は異なるものとなります。その相違点については、該当する箇所で説明されます。

（注）　Cisco MDS 9000 NX-OS Software Release 4.1(1c) 以降では、キーは移行前と同じ状態（アクティブまたは非アクティブ）に復元されます。

RKM の機能の履歴

表 9-1 に、この機能のリリース履歴を示します。

表 9-1　RKM の機能の履歴

機能名	リリース	機能情報
ソフトウェアの変更	5.2(1)	Release 5.2(1) では、Fabric Manager は DCNM for SAN（DCNM-SAN）という名前に変更されました。
	4.1(1c)	Release 4.1(1b) 以降、MDS SAN-OS ソフトウェアは MDS NX-OS ソフトウェアに名前が変更されました。旧リリース名は変更されておらず、参照はすべて維持されています。
RKM の移行手順	4.1(1c)	Cisco KMC から RKM への以降の手順は説明済みです。