OpenSSL を使用した PKCS12 ファイルの生成

始める前に

- OpenSSL は、HDS セットアップ ツールでの読み込みに適した形式で PKCS12 ファイルを作成するために使用できるツールの 1 つです。他にも使用できる手段はありますが、いずれかの手段をサポートまたは優先することはありません。
- OpenSSL を使用する場合は、「X.509 証明書の要件」で説明している x.509 証明書の要件を満たすファイルを作成できるよう、ガイドラインとして以下の手順に従ってください。ファイルを作成する前に、適用される要件を理解する必要があります。
- サポートされている環境に OpenSSL をインストールします。ソフトウェアおよびドキュメントについては、https://www.openssl.orgを参照してください。
- 秘密キーを作成します。
- 認証局（CA）からサーバ証明書を受け取った後、以下の手順に従います。

手順

ステップ 1 CA からサーバ証明書を受け取ったら、`hdsnode. pem` として保存します。

ステップ 2 証明書をテキストとして表示し、詳細を確認します。

```
openssl x509 -text -noout -in hdsnode.pem
```

ステップ 3 テキスト エディタを使用して、`hdsnode-bundle.pem` という名前の証明書バンドル ファイルを作成します。バンドルファイルには、サーバ証明書、中間 CA 証明書、およびルート CA 証明書が次の形式で含まれている必要があります。

```
-----BEGIN CERTIFICATE-----
### Server certificate. ###
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
###  Intermediate CA certificate. ###
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

OpenSSL を使用した PKCS12 ファイルの生成

```
###  Root CA certificate. ###
-----END CERTIFICATE-----
```

ステップ 4 フレンドリ名 `kms-private-key` を使用して .p12 ファイルを作成します。

```
openssl pkcs12 -export -inkey hdsnode.key -in hdsnode-bundle.pem -name kms-private-key
-caname kms-private-key -out hdsnode.p12
```

ステップ 5 サーバ証明書の詳細を確認します。

a) `openssl pkcs12 -in hdsnode.p12`

b) プロンプトが表示されたらパスワードを入力して秘密キーを暗号化し、暗号化された状態で出力されるようにします。次に、秘密キーと最初の証明書に **`friendlyName: kms-private-key`** という行が含まれていることを確認します。

例：

```
bash$ openssl pkcs12 -in hdsnode.p12
Enter Import Password:
MAC verified OK
Bag Attributes
    friendlyName: kms-private-key
    localKeyID: 54 69 6D 65 20 31 34 39 30 37 33 32 35 30 39 33 31 34
Key Attributes: <No Attributes>
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
<redacted>
-----END ENCRYPTED PRIVATE KEY-----
Bag Attributes
    friendlyName: kms-private-key
    localKeyID: 54 69 6D 65 20 31 34 39 30 37 33 32 35 30 39 33 31 34
subject=/CN=hds1.org6.portun.us
issuer=/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
-----BEGIN CERTIFICATE-----
<redacted>
-----END CERTIFICATE-----
Bag Attributes
    friendlyName: CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US
subject=/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
issuer=/O=Digital Signature Trust Co./CN=DST Root CA X3
-----BEGIN CERTIFICATE-----
<redacted>
-----END CERTIFICATE-----
```

次のタスク

「Hybrid Data Security の前提条件への対応」に戻ります。「HDS ホストの構成 ISO の作成」では、この `hdsnode.p12` ファイルと、このファイルに設定したパスワードを使用します。