ファイル署名の検証

Cloud Volumes ONTAP

NetApp
June 27, 2024

目次

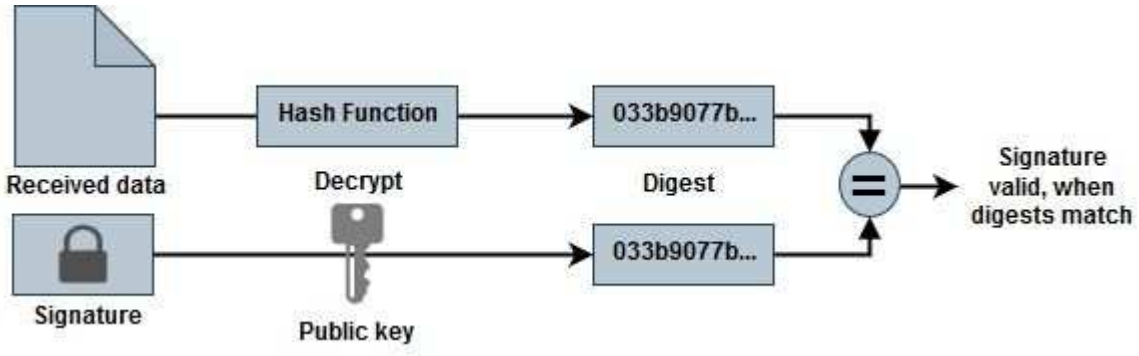
ファイル署名の検証

ファイル署名の検証

Azureイメージ検証プロセスでは、先頭に1MB、末尾に512Bのハッシュ関数を使用してストライプされたVHDファイルからダイジェストが生成されます。署名手順と照合するために、SHA256を使用してハッシュが作成されます。先頭の1MBと末尾の512BをVHDファイルから削除し、VHDファイルの残りの部分を確認する必要があります。

ファイル署名検証ワークフローの概要

次に、ファイル署名検証のワークフロープロセスの概要を示します。



- からAzure Image Digestファイルをダウンロードします。 "NetApp Support Site" そして、ダイジェストファイル（.sig）、公開鍵証明書ファイル（.pem）、チェーン証明書ファイル（.pem）を展開します。

  を参照してください "Azureイメージダイジェストファイルをダウンロード" を参照してください。

- 信頼チェーンを検証します。
- 公開鍵証明書（.pem）から公開鍵（.pub）を抽出します。
- 抽出された公開鍵は、ダイジェストファイルの復号化に使用されます。結果は、画像ファイルから作成された一時ファイルの新しい暗号化されていないダイジェストと比較され、先頭の1MBと末尾の512バイトが削除されます。

  この手順は、次のopensslコマンドを使用して実行します。

  - 一般的なCLI文は次のように表示されます。

    ```
    openssl dgst -verify <public_key> -keyform <form> <hash_function>
    -signature <digest_file> -binary <temporary_file>
    ```

  - OpenSSL CLIツールでは、両方のファイルが一致する場合は「Verified OK」メッセージが表示され、一致しない場合は「Verification Failure」というメッセージが表示されます。

Linuxでのファイル署名の検証

LinuxでエクスポートされたVHDファイルのシグネチャを確認するには、次の手順を実行します。

手順

1. からAzure Image Digestファイルをダウンロードします。 "NetApp Support Site" そして、ダイジェストファイル（.sig）、公開鍵証明書ファイル（.pem）、チェーン証明書ファイル（.pem）を展開します。

   を参照してください "Azureイメージダイジェストファイルをダウンロード" を参照してください。

2. 信頼チェーンを検証します。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 先頭の1MB（1048576バイト）と末尾の512バイトのVHDファイルを削除します。

   'taile'を使用した場合、オプション'-c + K'は指定されたファイルのKTHバイトから始まるバイトを出力します。したがって、1048577は'tail -c'に渡されます。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. opensslを使用して証明書から公開鍵を抽出し、署名ファイルと公開鍵でストライプされたファイル（sign.tmp）を確認します。

   入力ファイルが検証に合格すると、コマンドは次のように表示されます。「検証OK」。それ以外の場合は、「Verification Failure」と表示されます。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. ワークスペースをクリーンアップします。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Mac OSでのファイル署名の検証

エクスポートしたVHDファイルの署名をMac OSで確認するには、次の手順に従います。

手順

1. からAzure Image Digestファイルをダウンロードします。 "NetApp Support Site" そして、ダイジェストファイル（.sig）、公開鍵証明書ファイル（.pem）、チェーン証明書ファイル（.pem）を展開します。

   を参照してください "Azureイメージダイジェストファイルをダウンロード" を参照してください。

2. 信頼チェーンを検証します。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 先頭の1MB（1048576バイト）と末尾の512バイトのVHDファイルを削除します。

   'taile'を使用した場合、オプション'-c + K'はKTHバイトから始まるバイトを出力します。
   をクリックします。したがって、1048577は'tail -c'に渡されます。所要時間は約13mです。
   Mac OSでtailコマンドを完了します。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. opensslを使用して証明書から公開鍵を抽出し、
   署名ファイルと公開鍵を含むファイル（sign.tmp）。

   入力ファイルが検証に合格すると、コマンドは「検証OK」と表示されます。
   それ以外の場合は、「Verification Failure」と表示されます。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. ワークスペースをクリーンアップします。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

著作権に関する情報

商標に関する情報