檔案簽章驗證
Cloud Volumes ONTAP

NetApp
June 11, 2024

目錄

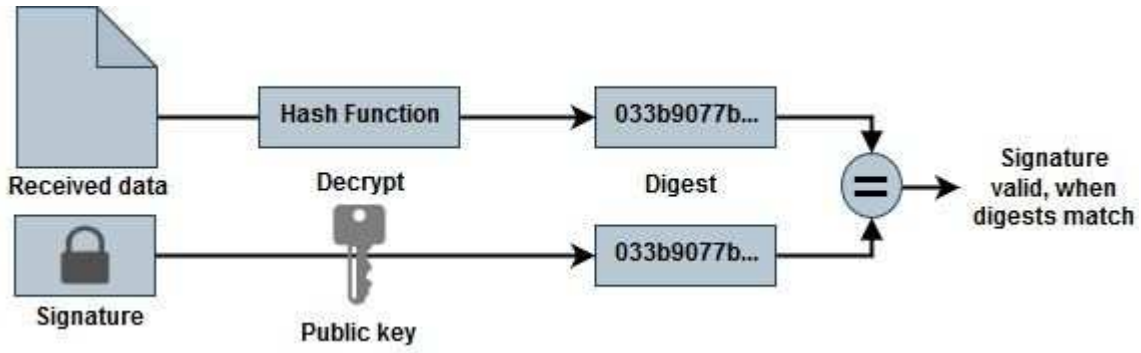
檔案簽章驗證

檔案簽章驗證

Azure 影像驗證程序將使用雜湊功能、從 VHD 檔案產生內含前導式 1MB 等量區塊的摘要、並結束 512B 等量區塊區塊區塊。為了符合簽署程序、使用 SHA256 進行雜湊。您需要從 VHD 檔案移除前導式 1MB 和最終版 512B 、然後驗證 VHD 檔案的其餘部分。

檔案簽章驗證工作流程摘要

以下是檔案簽章驗證工作流程程序的概觀。



- 從下載 Azure Image Digest 檔案 "NetApp 支援網站" 然後擷取摘要檔案（ .SIG ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

  請參閱 "下載 Azure Image Digest File" 以取得更多資訊。

- 驗證信任鏈結。
- 從公開金鑰憑證（ .pem ）擷取公開金鑰（ .pub ）。
- 解壓縮的公開金鑰用於解密摘要檔案。然後將結果與從映像檔案建立的新未加密暫存檔案摘要進行比較、並移除前導式 1MB 與結尾 512 位元組的檔案。

  此步驟可透過下列 openssl 命令來達成。

  - 一般 CLI 聲明如下所示：

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

  - 如果檔案相符、則 Openssl CLI 工具會顯示「驗證成功」訊息、如果檔案不符、則會顯示「驗證失敗」訊息。

Linux 上的檔案簽章驗證

您可以依照下列步驟驗證匯出的 VHD 檔案簽章適用於 Linux 。

步驟

1. 從下載 Azure Image Digest 檔案 "NetApp 支援網站" 然後擷取摘要檔案（ .SIG ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

   請參閱 "下載 Azure Image Digest File" 以取得更多資訊。

2. 驗證信任鏈結。

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

3. 移除前導的 1MB （ 1048576 位元組）、並結束 512 位元組的 VHD 檔案。

   如果使用「 tail 」、選項「 -c +K 」會以指定檔案的 KTH 位元組開始輸出位元組。因此、 1048577 會傳送至 'tail -c 。

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

4. 使用 openssl 從憑證擷取公開金鑰、並使用簽章檔案和公開金鑰驗證等量分佈的檔案（ sign.tmp ）。

   如果輸入檔通過驗證、則會顯示命令
   " 驗證正常 " 。否則將顯示「驗證失敗」。

```
% 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. 清理工作區。

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

Mac OS 上的檔案簽章驗證

您可以依照下列步驟、驗證 Mac OS 匯出的 VHD 檔案簽章。

步驟

1. 從下載 Azure Image Digest 檔案 "NetApp 支援網站" 然後擷取摘要檔案（ .SIG ）、公開金鑰憑證檔案（ .pem ）和鏈結憑證檔案（ .pem ）。

   請參閱 "下載 Azure Image Digest File" 以取得更多資訊。

2. 驗證信任鏈結。

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

3. 移除前導的 1MB （ 1048576 位元組）、並結束 512 位元組的 VHD 檔案。

   如果使用「 tail 」、選項「 -c +K 」會以 KTH 位元組開始輸出位元組
   指定檔案的。因此、 1048577 會傳送至 'tail -c 。大約需要 13 分鐘
   以在 Mac OS 上完成 tail 命令。

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

4. 使用 openssl 從憑證擷取公開金鑰、並驗證等量分割
   檔案（ sign.tmp ）、含簽章檔案和公開金鑰。

   如果輸入檔案通過驗證、命令會顯示「驗證正常」。
   否則將顯示「驗證失敗」。

```
% 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. 清理工作區。

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