Dateisignatur überprüfen

Cloud Volumes ONTAP

NetApp
February 13, 2026

Inhalt

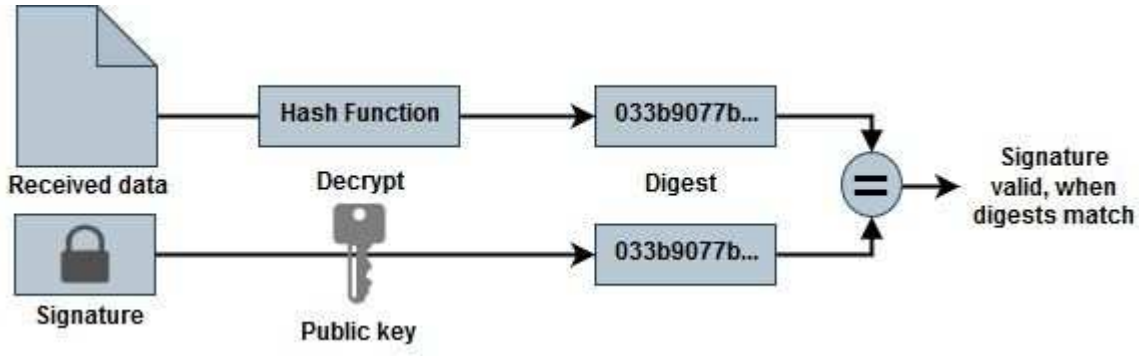
Dateisignatur überprüfen

Azure Marketplace-Imagesignaturüberprüfung für Cloud Volumes ONTAP

Der Azure-Imageüberprüfungsprozess generiert eine Digest-Datei aus der VHD-Datei, indem er am Anfang 1 MB und am Ende 512 Byte entfernt und dann eine Hash-Funktion anwendet. Um dem Signaturverfahren zu entsprechen, wird *sha256* zum Hashing verwendet.

Zusammenfassung des Workflows zur Dateisignaturüberprüfung

Nachfolgend finden Sie eine Übersicht über den Workflow-Prozess zur Dateisignaturüberprüfung.



- Herunterladen des Azure-Images von der "NetApp Support Site" und Extrahieren der Digest-Datei (.sig), der Public-Key-Zertifikatdatei (.pem) und der Kettenzertifikatdatei (.pem). Weitere Informationen finden Sie unter "Herunterladen der Azure-Image-Digest-Datei" für weitere Informationen.
- Überprüfung der Vertrauenskette.
- Extrahieren des öffentlichen Schlüssels (.pub) aus dem öffentlichen Schlüsselzertifikat (.pem).
- Entschlüsseln der Digest-Datei mithilfe des extrahierten öffentlichen Schlüssels.
- Vergleichen Sie das Ergebnis mit einem neu generierten Digest einer temporären Datei, die aus der Bilddatei erstellt wurde, nachdem 1 MB am Anfang und 512 Byte am Ende entfernt wurden. Dieser Schritt wird mithilfe des OpenSSL-Befehlszeilentools ausgeführt. Das OpenSSL-CLI-Tool zeigt eine entsprechende Meldung an, wenn die Zuordnung der Dateien erfolgreich war oder fehlgeschlagen ist.

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

Überprüfen der Azure Marketplace-Imagesignatur für Cloud Volumes ONTAP unter Linux

Die Überprüfung der Signatur einer exportierten VHD-Datei unter Linux umfasst die Validierung der Vertrauenskette, die Bearbeitung der Datei und die Überprüfung der Signatur.

Schritte

1. Laden Sie die Azure-Imagedatei von der "NetApp Support Site" und extrahieren Sie die Digest-Datei (.sig), die Public-Key-Zertifikatdatei (.pem) und die Kettenzertifikatdatei (.pem).

   Siehe "Herunterladen der Azure-Image-Digest-Datei" für weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

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

3. Entfernen Sie 1 MB (1.048.576 Bytes) am Anfang und 512 Bytes am Ende der VHD-Datei. Bei der Verwendung `tail` , Die `-c +K` Option generiert Bytes aus dem K-ten Byte der Datei. Daher geht es 1048577 an `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. Verwenden Sie OpenSSL, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die extrahierte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen.

   Die Eingabeaufforderung zeigt Meldungen an, die den Erfolg oder Misserfolg der Überprüfung basierend auf deren Erfolg anzeigen.

```
% 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. Räumen Sie den Arbeitsbereich auf.

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

Überprüfen der Azure Marketplace-Imagesignatur für Cloud Volumes ONTAP unter macOS

Die Überprüfung der Signatur einer exportierten VHD-Datei unter Linux umfasst die Validierung der Vertrauenskette, die Bearbeitung der Datei und die Überprüfung der Signatur.

Schritte

1. Laden Sie die Azure-Imagedatei von der "NetApp Support Site" und extrahieren Sie die Digest-Datei (.sig), die Public-Key-Zertifikatdatei (.pem) und die Kettenzertifikatdatei (.pem).

   Siehe "Herunterladen der Azure-Image-Digest-Datei" für weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

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

3. Entfernen Sie 1 MB (1.048.576 Bytes) am Anfang und 512 Bytes am Ende der VHD-Datei. Bei der Verwendung `tail` , Die `-c +K` Option generiert Bytes aus dem K-ten Byte der Datei. Daher geht es 1048577 an `tail -c` . Beachten Sie, dass die Ausführung des Tail-Befehls unter macOS etwa zehn Minuten dauern kann.

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

4. Verwenden Sie OpenSSL, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die extrahierte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen. Die Eingabeaufforderung zeigt Meldungen an, die den Erfolg oder Misserfolg der Überprüfung basierend auf deren Erfolg anzeigen.

```
% 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. Räumen Sie den Arbeitsbereich auf.

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