File signature verification

Cloud Volumes ONTAP

NetApp
June 27, 2024

This PDF was generated from https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/concept-azure-file-sig-verify.html on June 27, 2024. Always check docs.netapp.com for the latest.

Table of Contents

File signature verification 1
File signature verification 1
File signature verification on Linux 1
File signature verification on Mac OS 3

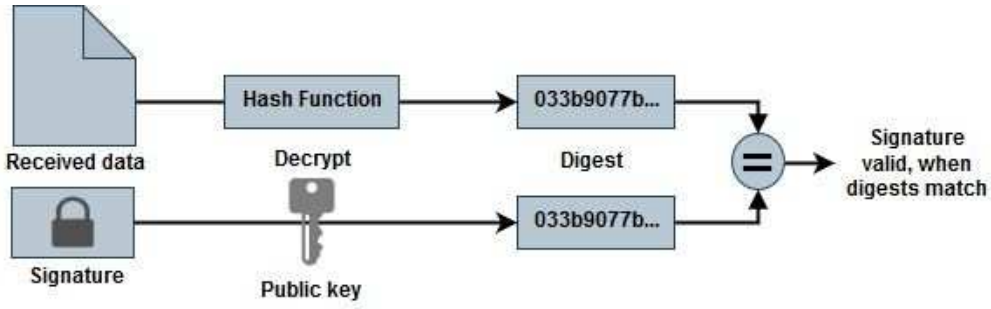
File signature verification

File signature verification

The Azure image verification process will generate a digest from the VHD file with the leading 1MB and ending 512B striped by using hash function. To match the signing procedure, SHA256 is used to hash. You need to remove the leading 1MB and final 512B from the VHD file and then verify the remaining portion of the VHD file.

File signature verification workflow summary

The following is an overview of the file signature verification workflow process.



- Download the Azure Image Digest file from the NetApp Support Site and extract the digest file(.sig), public key certificate file(.pem) and chain certificate file(.pem).

  Refer to the Download the Azure Image Digest File for more information.

- Verify the chain of trust.
- Extract the public key(.pub) from the public key certificate(.pem).
- The extracted public key is used to decrypt the digest file. The result is then compared against a new unencrypted digest of the temporary file created from the image file with leading 1MB and ending 512 bytes removed.

  This step is achieved through the following openssl command.

  - The general CLI statement appears as follows:

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

  - OpenSSL CLI tool gives a "Verified OK" message if both the files match and "Verification Failure" if they do not match.

File signature verification on Linux

You can verify an exported VHD file signature for Linux by following the steps below.

Steps

1. Download the Azure Image Digest file from the NetApp Support Site and extract the digest file(.sig), public key certificate file(.pem) and chain certificate file(.pem).

   Refer to the Download the Azure Image Digest File for more information.

2. Verify the chain of trust.

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

3. Remove the leading 1MB (1048576 Bytes) and ending 512 Bytes of VHD file.

   If 'tail' is used, the option '-c +K' outputs bytes starting with the Kth bytes of the specified file. Hence, 1048577 is passed to '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. Use openssl to extract public key from certificate and verify the striped file(sign.tmp) with the signature file and public key.

   If the input file passes the verification, the command will display
   "Verification OK". Otherwise, "Verification Failure" will display.

```
% 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. Clean up the workspace.

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

File signature verification on Mac OS

You can verify an exported VHD file signature for Mac OS by following the steps below.

Steps

1. Download the Azure Image Digest file from the NetApp Support Site and extract the digest file(.sig), public key certificate file(.pem) and chain certificate file(.pem).

   Refer to the Download the Azure Image Digest File for more information.

2. Verify the chain of trust.

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

3. Remove the leading 1MB(1048576 Bytes) and ending 512 Bytes of VHD file.

   If 'tail' is used, the option '-c +K' outputs bytes starting with the Kth bytes of the specified file. Hence, 1048577 is passed to 'tail -c'. It takes around 13m for the tail command to complete on Mac OS.

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

4. Use openssl to extract public key from certificate and verify the striped file(sign.tmp) with the signature file and public key.

   If the input file passes the verification, the command will display "Verification OK". Otherwise, "Verification Failure" will display.

```
% 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. Clean up the workspace.

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

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.