****

HP Access Control - HP AC ReadMeFirst

****

August 2018

The HP AC releases consists of the following:

- ReadMeFirst (this document)
- Solution package (zip file)
- Signature file (asc file)
- Release Notes (pdf file)

Beginning with the HP AC v15.0.0 release, the HP AC package has been code signed by HP. The contents of this readme will help you verify through GPG that the solution package you received has been signed with digital private keys only held by HP. This ensures that the package has not been manipulated by a third party.

Complete the following steps to verify that the solution package has been signed and has not been manipulated:

Step 1 - Download the Key:

Download and Save (e.g. Save As "087C31C4.asc") the public key to your local directory using the following link:

ftp://ftp.hp.com/pub/keys/2015-03/087C31C4.pub

[NOTE: If your target machine remains the same, this only needs to be done one time.]

Step 2 - Setup a GPG tool:

Download and Install the gpg tool using the following link:

https://www.gnupg.org/download/index.html

e.g. "Gpg4win" is one of the gpg tools that can be downloaded and installed for this verification process. Steps 3 and 4 (below) were verified using the "Gpg4win" GPG tool.

Step 3 - Verify the Key:

Because you have downloaded the key from a public FTP site hosted by HP (from Step 1 above), you can ultimately trust that this public key is indeed from HP. Therefore, edit the key to set the trust level of the key for proper verification.

[NOTE: The verification example is with a command prompt (Windows Key + R, and type “cmd”).]

a) Import the certificate:

C:\Program Files (x86)\GNU\GnuPG>gpg –-import /path_to_the_key/file_name_of_the_key

b) Find the "key_name" of the key (e.g. "087C31C4.asc"), type the following command and select the key that you need to trust. E.g.,

C:\Program Files (x86)\GNU\GnuPG>gpg --list-keys

Example of a "key_name" "Hewlett-Packard Company RSA (HP Codesigning Service) - 1"

c) Edit the key:

E.g.,
C:\Program Files (x86)\GNU\GnuPG>gpg --edit-key <key_name>

d) Trust the key: Type the command "trust", and select "5" for trusting the key ultimately. Confirm (type 'y') and type "quit" to exit.

Step 4 - Verify the digital signature of the signed file:

Option 1 -- Command prompt:

Use the GPG tool to validate and verify the digital signature of the signed file via the commmand prompt. The output from the command indicates the validity of the signature. Specify the .asc (detached signature) file and the corresponding input file in the command:

C:\Program Files (x86)\GNU\GnuPG>gpg --verify <filename.zip.asc> <filename.zip>

If the level of trust on the key has not been set, you will see a trust level warning similar to this:

gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.

When trusted identity has been verified, the verification output would be similar to this:

gpg: Signature made Thu 03 Jan 2013 04:48:47 PM UTC using RSA key ID 5CE2D476
gpg: Good signature from "Hewlett-Packard Company RSA (HP Codesigning Service)"

Option 2 -- GUI:

This option assumes you have "Gpg4win" GPG setup.

a) Open the GPG GUI tool (e.g., gpg4win's Kleopatra)

b) Select "Import certificates" to import the key (e.g. "087C31C4.asc") that you have already downloaded and saved from Step 1.

b) Select "File" --> "Decrypt/Verify Files..."
    1) select the <filename.zip.asc> file
    2) select the <filename.zip> file from the "Signed data:" area
    3) select "Decrypt/Verify"

d) Verify that the results are successful (i.e., signed by HP).