Verifying signatures

When downloading a release of Haketilo or Hydrilla, you might want to make sure the files are authentic and have not been tampered with. You can do this using the cryptographic signatures we provide.

New releases are signed using both GNU Privacy Guard (GPG) and Signify tool from the OpenBSD operating system (which can also be used on other systems, including FSF-approved ones like Trisquel). Your best bet is performing the verification using **both**, although in general Signify is considered more secure.

For the purpose of instructions below, let's make the following assumptions:

- We're verifying the integrity of Haketilo 1.0-beta1 source tarball (the procedure would be analogous when verifying other files).
- We're using a POSIX-compliant shell.
- We have access to wget command for downloading files.
- The following files have been downloaded into current directory (links here are the same as those present on Haketilo's old releases page):
  - haketilo-1.0b1.tar.gz
  - haketilo-1.0b1.tar.gz.sig
  - haketilo-1.0b1.tar.gz.asc

Verifying using Signify

First, you need to have the Signify tool installed. For Trisquel and other GNU/Linux distributions in Debian family, you can use a command like sudo apt install signify-openbsd. For Parabola and other Arch derivatives, you install with sudo pacman -Syu signify. On Guix it is guix install signify. On Fedora and other GNU/Linux distributions using RPM package manager you'd run sudo dnf install signify. An alternative command to achieve the same under RPM-powered distributions is sudo yum install signify.

Before you verify the signature, you need the public Signify key of Haketilo's maintainer, Wojtek Kosior. You can download it with this command:

```
wget https://koszko.org/key.pub
```

Now, ensure the downloaded key.pub file contains, besides the untrusted comment, only the **RWQSf2wUdpjAtrmt7D3t9iHrHFL/GpqXOF+NxECx8ck7swrx6tNzDkM9** string. If the string is different, it means someone's doing something nasty and you should not proceed.

You can now perform the verification with this command:

```
signify-openbsd -V -p key.pub -x haketilo-1.0b1.tar.gz.sig -m haketilo-1.0b1.tar.gz
```

Of course, you'll need to swap signify-openbsd for just signify on systems where the tool is named this way. Regardless, the output should be:

```
Signature Verified
```

If it is something else, it means verification failed and you should not trust the file you downloaded. For more information about using Signify see its manual page.

Verifying using GPG

The PGP signatures we're providing can be verified using any tool that conforms to the OpenPGP standard. Nevertheless, the instructions we give here concern using the most popular GPG tool for the task. It is most likely already installed on the GNU/Linux distribution you're using. Let's assume it is available under the gpg command.

You need the public key of Haketilo's maintainer, Wojtek Kosior. The command below will check if gpg's database already contains that key and will download and import it if not.

```
gpg --list-key koszko@koszko.org > /dev/null 2>&1 || (wget https://koszko.org/key.gpg 2>/dev/null && gpg --import key.gpg)
```

You can now perform the verification with this command:

```
gpg --verify haketilo-1.0b1.tar.gz.asc
```

It should output something like:

```
gpg: assuming signed data in 'haketilo-1.0b1.tar.gz'
gpg: Signature made Fri 25 Feb 2022 05:17:50 PM CET
gpg:                using EDDSA key E9727060E3C5637C8A4F4B424BC5221C5A79FD1A
gpg: Good signature from "W. Kosior <koszko@koszko.org>" [unknown]
gpg:                 aka "Wojciech Kosior <wk@koszkonutek-tmp.pl.eu.org>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: E972 7060 E3C5 637C 8A4F  4B42 4BC5 221C 5A79 FD1A
```

The most important thing is that the **E972 7060 E3C5 637C 8A4F 4B42 4BC5 221C 5A79 FD1A** string is present and matches. If not, it means someone's doing something nasty and you should not trust the file you downloaded.

Final considerations

The trust you can put in cryptographic signatures is at best as strong as your confidence that the public key you use for verification does indeed belong to the developer. Someone who tricks you into using a different key (for example by breaking into our server and swapping key files) can make a modified release file look like the legitimate one. For this reason it is a good idea to have public keys (fingerprints) posted in various places. The user should then make sure the key is the same as advertised in at least some of those places. Wojtek's public keys can be found in the following locations:

- the gitlab.trisquel.info account
- signed Haketilo/Hydrilla release tags (only PGP signatures and need to be extracted from the PGP data block)
- our LibrePlanet 2022 presentation

Additionally, Wojtek's GPG and Signify keys are cross-signed with each other[1].

---

1. https://koszko.org/en/koszko.html#pubkeys ↩