1. Make sure you have gpg4win downloaded and installed on your machine

https://www.gpg4win.org/

2. Download the three files

Download the correct release file for your machine
Download the checksum file (SHA256SUMS, a list of hashes for each release).
Download the signature file (`SHA256SUMS.asc`, the signed version of the checksums).

3. Download the Bitcoin Knots Guix signatures repository as a ZIP file from GitHub and extract it

go to

https://github.com/bitcoinknots/guix.sigs.git

click the green "code" button, download zip. Extract the zipped folder.

4. In the command prompt change into the builder keys folder

```
cd Downloads\guix.sigs-knots\guix.sigs-knots\builder-keys
```

5. import the developers signatures

```
gpg --import *.gpg
```

6. Go back into your downloads folder

```
cd C:\Users\<your-username>\Downloads
```

7. Verify the authenticity of the checksum file

```
gpg --verify SHA256SUMS.asc
```

You should see output showing developer emails and a line that says **GOOD SIGNATURE**. You'll also see the developer's public key fingerprint, which you should cross-check against trusted sources.

(Note: A warning about the key not being certified or trusted is normal unless you've set up your own web of trust. That's an advanced step for users who assign trust levels and sign keys themselves.)

8. Verify the integrity of your release

Run the following to get the checksum of the zipped release file you have downloaded (replace the filename if needed with the exact one you have downloaded):

```
certutil -hashfile bitcoin-29.1.knots20250903-win64-setup-unsigned.exe SHA256
```

You should now check this output against checksum (`SHA256SUMS`) file

```
type SHA256SUMS
```

Confirm that the two values match exactly