Creating a Code Signing Key

To assist our users in verifying the authenticity of our software releases, we digitally sign them.

Requirements

We have borrowed heavily from the release signing policy used by the ASF.

When generating your code signing key:

1. Use a 4096 bit RSA key with SHA512 hash
2. Use your real name, preferred email address, and "CODE SIGNING KEY" as the comment.
3. Use a strong password to protect your key

Once generated, you should:

- Keep your private key file on a safe, secure computer, and make sure you have a secure backup.
- Never use this key for purposes other than code signing or signing other keys.

1. Generate Your Key

Carefully follow the instructions here to generate your key and check that SHA1 is avoided.

Tip: Popular binaries for GnuPG 2.x can be found here:

- Linux
- Mac OS X (or "brew install gpg2")
- Windows

Note: After initially generating your key with GnuPG 2.x (gpg2), you can work with it using the more commonly-available 1.4.9 release (gpg).

2. Publish Your Public Key

To enable people and Sonatype to find your public key, you must publish it to a well-known keyserver. Due to the deprecation of the majority of SKS keyservers in 2019 we now have the options of:

- keys.openpgp.org (Hagrid)
- keyserver.ubuntu.com (hockeypuck)
- pgp.mit.edu (SKS)

In the efforts to reduce the publication of private information the Hagrid server will not reveal or allow searching with the email address a key is tied to without explicit approval. Because keyservers no longer store and distribute third-party signatures (those adding via signing someone's key) the "Web of trust" is harder to track. Therefore it is not necessary to reveal your email address when publishing your key unless you really want to.
For the below commands, *yourKeyID* is the last 8 digits of your public key fingerprint. Fingerprints may be used instead of key IDs. To find your fingerprint use the command

```
gpg -K
```

keys.openpgp.org (Hagrid)

Not revealing your email address

```
gpg --keyserver keys.openpgp.org --send-key [yourKeyID | Fingerprint]
```

Publishing your email address with your key

```
gpg --export your_address@example.net | curl -T - https://keys.openpgp.org
```

keyserver.ubuntu.com (HockeyPuck)

```
gpg --keyserver keyserver.ubuntu.com --send-key [yourKeyID | Fingerprint]
```

pgp.mit.edu (SKS)

```
gpg --keyserver pgp.mit.edu --send-key [yourKeyID | Fingerprint]
```

This will upload your public key to a well-known keyserver, which will then trigger other connected keyservers to get a copy.

3. Publish Your Key Fingerprint

Add your fingerprint to the Fedora Committers page.