

Removing your site from the Wayback Machine (GPG)

A quick-ish and easy-ish guide

Amolith

2019-06-04T21:57:00-04:00

Contents

| | |
|--|---|
| Preface | 1 |
| Getting set up | 1 |
| Installation & Generating Keys | 1 |
| Email | 2 |
| Verifying Identities | 2 |
| Sending the email | 3 |

Preface

If you simply want to remove your website and nothing else, read through the setup and verifying identities sections then continue from the **For domains you own** section of the previous post. If you're wanting to address accounts/profiles on websites you don't own, read on.

In addition to dealing with the Wayback Machine, this article is also supposed to help you get started using GPG in every-day life for general security and privacy.

Getting set up

Installation & Generating Keys

First of all, you'll want to install GPG. The package on most distributions should be just be `gnupg`. - Debian: `sudo apt install gnupg` - Arch: `sudo pacman -S gnupg` - Fedora: `sudo dnf install gnupg`

The next step is generating your key. While it will take a bit longer to generate, a stronger key will be more secure. Also make sure you read this excerpt from the `man` page as it contains a useful warning.

WARNINGS

Use a *good* password for your user account and a *good* passphrase to protect your secret key. This passphrase is the weakest part of the whole system. Programs to do dictionary attacks on your secret keyring are very easy to write and so you should protect your `~/.gnupg/` directory very well.

With that said, use `gpg --full-gen-key` to get started. Keep in mind that you don't actually have to use your real name or personal email address. If you *want* a personal key, go ahead and create one but you can also use a pseudonym and fake address if you'd like.

1. I would use the default (1) of "RSA and RSA".
2. Again, you can use default but I would recommend 4096 bits because it's much more secure. This does mean, however, that it will take longer to generate the key.
3. An expiry date is recommended but you don't necessarily have to set one.
4. You *don't* have to use your real name. You can use a pseudonym if you wish.
5. You *don't* have to use your personal email. You can use a pseudonymous one if you wish.
6. You don't need a comment
7. Confirm
8. Come up with a *secure* password or, even better, a *passphrase*.
9. Move your mouse around a bit, type, something like that while it's generating the key.

Email

I use [Thunderbird](#) for email and there is a great add-on for it called [Enigmail](#). It's quite easy to set up and use but there is a really annoying bug that you'll experience when replying in threaded mode. If you want to encrypt a reply, simply open the editor in a new window.

Verifying Identities

In general, all you'll have to do is type something along the lines of:

```
I am <your-name-here> and I own the following accounts: - Account
1 - <link> - Account 2 - <link> - Etc.
```

You'll save that in a text file, run `gpg --clearsign file.txt`, copy the output, then paste it wherever it needs to go, whether that's a blog, a GitHub gist, etc. With Twitter/Mastodon and their character limit, this won't quite work. The best solution there is probably to post a link to a gpg-signed message on your website that links back to the post.

Really, all you have to do is tie all of your accounts together in as close-knit a web as you can and sign with your GPG key wherever possible. Linking everything to everything else would definitely work but it should also be enough to link everything to a single document on your website (or a gist in GitHub etc.) that links back to all of those.

I'm probably not explaining very well so here's a diagram showing it.

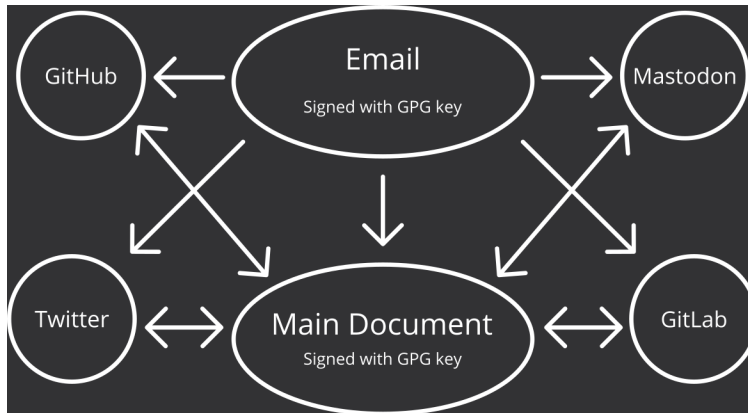


Figure 1: a diagram illustrating the text below

Note that the email links to everything else but nothing links back to the email. It's the main document that's at the centre of it all. Make sure both it and the email are signed. If you toot, link to the toot in the main document. If you make a gist, link to the gist in the main document.

Sending the email

Once you have all the groundwork laid out, you'll be ready to send the email; the address is info@archive.org. Explain what you would like done and link to the document requesting your domain exclusion first as that's the easiest to verify. In the next paragraph, I would explain a little bit about what you've set up with signing messages and creating the "Web of Verification" (lol). Under that, I would link to the posts asking for the accounts to be removed. Make sure those posts also link back to the main document. Be polite, say thank you, then send the email!