Using TLS on svasey.org

To encrypt your communication with this site, and more importantly make sure you are talking to the right server[1], you can use Transport Layer Security.

To do so, simply change the `http` in the URL to `https`. If you use Firefox, you can use addons such as Redirector[2] to avoid doing this manually.

1 Downloading my certificate

Because I haven't paid large corporations to sign my certificate, most browsers will issue a warning when visiting this site with HTTPS.

This is why you should download my certificate, explicitely verify its PGP signature, and tell your browser to trust it. More explicitely, on a UNIX-like system you can run the following commands:

```
$ wget http://certs.svasey.org/svasey_org.cer http://certs.svasey.org/svasey_org.cer.s
$ gpg --verify svasey_org.cer.sig
```

For the last command to work, you will need to fetch my PGP key[3]. You can then tell your browser to trust `svasey_org.cer`. The way to do this is browser-dependent.

You can also replace `svasey_org` by `svasey_root` in the above instructions, in order to download my self-signed root certificate.

2 Fingerprints

2.1 Root certificate

The fingerprints of the svasey root certificate (svasey_root.cer[4]) are:

```
SHA1: D2:E0:1C:64:AF:02:EF:12:CB:8D:4E:6A:65:C2:D1:2F:57:53:02:4C
MD5 : 4C:F4:49:FE:2B:AE:03:EE:B0:86:43:D5:8A:09:DF:BB
```

2.2 svasey.org certificate

The fingerprints of the `svasey.org` certificate (svasey_org.cer[5]) are:

```
SHA1: CC:2F:2D:8A:59:88:66:87:35:31:1C:BB:D1:35:B0:B5:4B:5E:E7:5D
MD5 : 57:21:E4:21:FB:85:5D:A0:B4:21:0C:93:CF:95:13:D7
```

[1] https://secure.wikimedia.org/wikipedia/en/wiki/Man_in_the_middle_attack

[2] https://addons.mozilla.org/en-US/firefox/addon/redirector/

[3] http://about_en.html#privacy-now

[4] http://certs.svasey.org/svasey_root.cer

[5] http://certs.svasey.org/svasey_org.cer