GitHub's SSH key fingerprints

Public key fingerprints can be used to validate a connection to a remote server.

These are GitHub's public key fingerprints:

- `SHA256:uNiVztksCsDhcc0u9e8BujQXVUpKZIDTMczCvj3tD2s` (RSA)
- `SHA256:br9IjFspm1vxR3iA35FWE+4VTyz1hYVLIE2t1/CeyWQ` (DSA - deprecated)
- `SHA256:p2QAMXNIC1TJYWeIOttrVc98/R1BUFWu3/LiyKgUfQM` (ECDSA)
- `SHA256:+DiY3wvvV6TuJJhbpZisF/zLDA0zPMSvHdkr4UvCOqU` (Ed25519)

You can add the following ssh key entries to your `~/.ssh/known_hosts` file to avoid manually verifying GitHub hosts:

```
github.com ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIOMqqnkVzrm0SdG6UOoqKLsabgH5C9okWi0dh2l9GKJl
github.com ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEmKSENjQEezOmxkZMy7opKgwFB9nkt5

github.com ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCj7ndNxQowgcQnjshcLrqPEiiphnt+VTTvDP6mHBL9j1aNUkY4Ue1g
```

For more information, see "[Meta](#).."

Legal

© 2023 GitHub, Inc.   [Terms](#)   [Privacy](#)   [Status](#)   [Pricing](#)   [Expert services](#)   [Blog](#)