



# Simplify signing Git commits and tags with SSH keys

2022 Git Merge Workshop



**Andy Feller** 🐱 (meow)

GitHub Expert Services

@andyfeller



# Outcomes



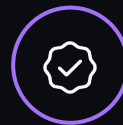
## Understand motivation

Nature of the problem, importance



## Gain firsthand experience

Setup, signing, verifying



## Have adoption plan

From one person to repository-wide



# Which would you accept?

The image displays two side-by-side GitHub commit comparison views. The left view shows a commit by 'andyfeller' with the message 'Adding fizz buzz'. The commit is signed, and the status is 'Verified'. A green circle highlights the 'Verified' status and the SSH key fingerprint. The right view shows a commit by 'ashtom' with the message 'I am Tom and I totally wrote this ... not'. The commit is not signed, and the status is 'Unverified'. A blue circle highlights the 'Unverified' status and the SSH key fingerprint.

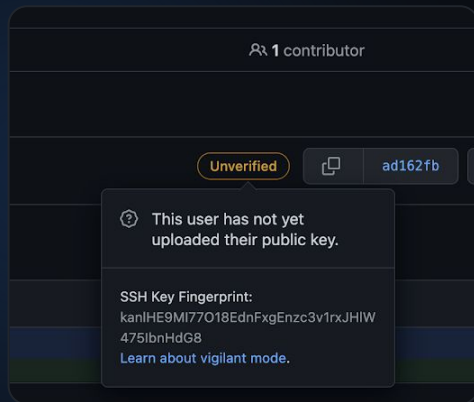
**Left Screenshot (Verified):**

- base: main ← compare: is-andyfeller ✓ Able to merge. These branches can be automatically merged.
- 1 commit 1 file changed 1 contributor
- Commits on Aug 27, 2022
- Adding fizz buzz
- andyfeller committed 13 days ago
- Showing 1 changed file with 1 addition and 0 deletions.
- 1 fizz
- Verified 549857d
- This commit was signed with the committer's verified signature.
- andyfeller Andy Feller
- SSH Key Fingerprint: kanlHE9MI77O18EdnFxEznc3v1rxJHIW 475lbnHdG8
- Learn about vigilant mode.

**Right Screenshot (Unverified):**

- base: main ← compare: not-ashtom ✓ Able to merge. These branches can be automatically merged.
- 1 commit 1 file changed 1 contributor
- Commits on Aug 26, 2022
- I am Tom and I totally wrote this ... not
- ashtom committed 13 days ago
- Showing 1 changed file with 1 addition and 0 deletions.
- 1 foo
- Unverified ad162fb
- This user has not yet uploaded their public key.
- SSH Key Fingerprint: kanlHE9MI77O18EdnFxEznc3v1rxJHIW 475lbnHdG8
- Learn about vigilant mode.

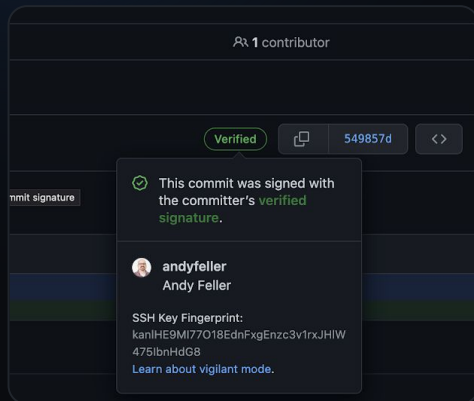




## Unverified



Signed content that cannot be verified against authors and committers.



## Verified



Signed content that has been verified to keys on file for authors and committers.





# Understand motivation

```
$ git cat-file -p d7a327072ed28cb660924d903ae7c3c22f6c13d1
```

```
tree 1a0ea28e98cc913b83a26347cab3e0df98a36ece
parent 25c3e34e22861e7bef8d5f177ea8809d8f547068
parent a5124518546d6680626d806c36085099333fac4c
author Andy Feller <andyfeller@github.com> 1661707548 -0400
committer Andy Feller <andyfeller@github.com> 1661707548 -0400
gpgsig -----BEGIN SSH SIGNATURE-----
U1NIU0lHAAAAAQAAADMAAAALc3NoLWVkJU1MTkAAAAgAuowLNeV7cU7+ho4jLGSa61imG
JnxMf652Yfgxz9rVUAAAADZ2l0AAAAAAMAAZzaGE1MTIAAABTAAAC3NzaC1lZDI1NTE5
AAAAQDHypmlmi0bdrpWD6T5kl1YQwSTKcfcQuFog7SuinZ3/tMAAt1zDXba1Ua0KvIigAQ
nHX5FueI8ze7p0wPKN0gY=
-----END SSH SIGNATURE-----
```

```
Merge branch 'main' of github.com:git-merge-workshops/simplify-signing-with-ssh
```



# Code signing capabilities

1

GPG

Introduced in 2012 with Git 1.7.9

2

X509 or S/MIME

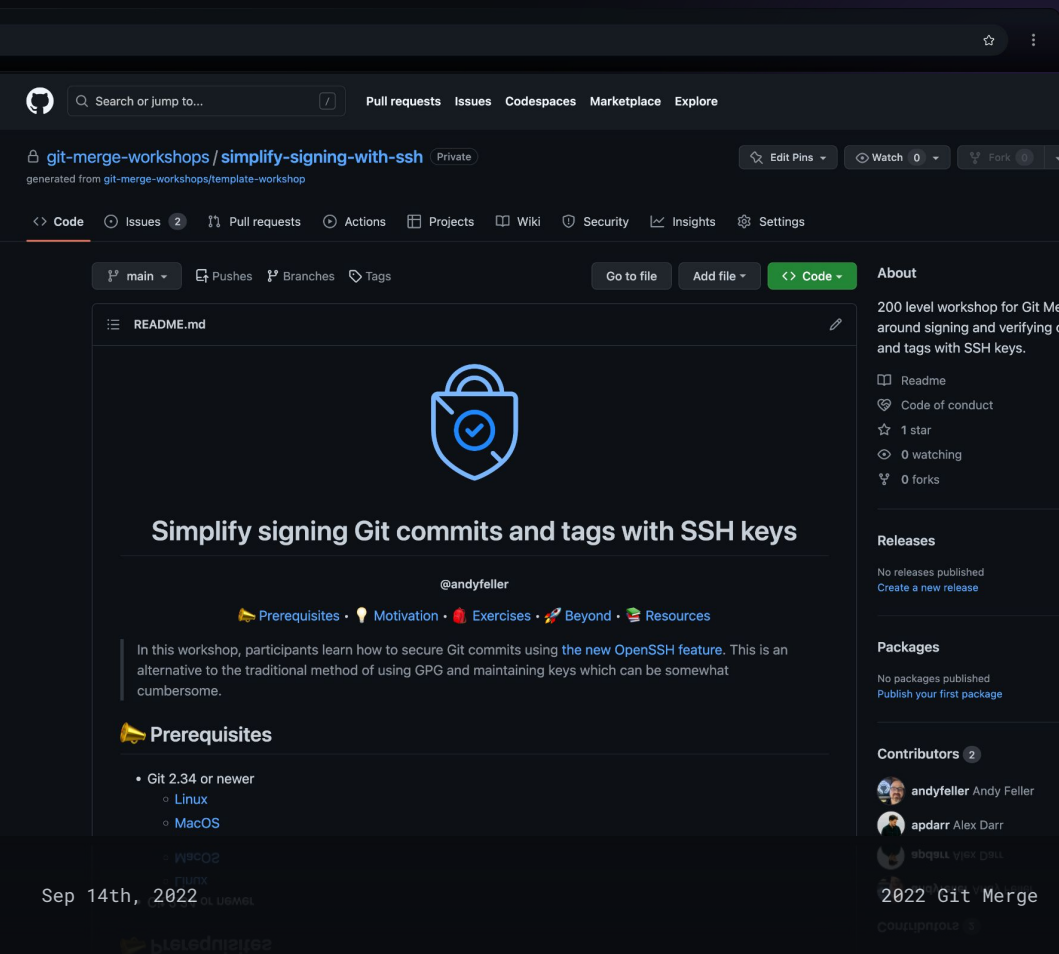
Introduced in 2019 with Git 2.19.0

3

SSH

Introduced in 2021 with Git 2.34.0





The screenshot shows the GitHub interface for the repository `git-merge-workshops/simplify-signing-with-ssh`. The repository is private and was generated from a template. The main content area displays the `README.md` file, which features a blue padlock icon with a checkmark. The title of the workshop is "Simplify signing Git commits and tags with SSH keys" by `@andyfeller`. The README includes navigation links for Prerequisites, Motivation, Exercises, Beyond, and Resources. It describes the workshop's goal: to teach participants how to secure Git commits using the new OpenSSH feature, as an alternative to the traditional GPG method. A "Prerequisites" section lists "Git 2.34 or newer" with sub-points for "Linux" and "MacOS". The right sidebar shows repository statistics: 1 star, 0 watching, and 0 forks. It also lists sections for Releases, Packages, and Contributors, with two contributors shown: `andyfeller` (Andy Feller) and `apdarr` (Alex Darr).



# Gain firsthand experience

Navigate to workshop repository

[github.com/git-merge-workshops/simplify-signing-with-ssh](https://github.com/git-merge-workshops/simplify-signing-with-ssh)

@andyfeller





# Exercises

30 minutes

Will introduce each before following along in repository.

Raise 🙋 if you need help!

- 1 Setup workstation
- 2 Signing and verifying commits
- 3 Signing and verifying merges
- 4 Signing and verifying tags
- 5 Signing past commits and tags



```
git config gpg.format ssh  
git config user.signingkey ...  
git config gpg.ssh.allowedSignersFile ...
```

```
andyfeller@github.com ssh-ed25519  
AAAAC3NzaC1lZDI1NTE5AAAAILGK6uBGvfjK+DGqiDguxD  
FUoScNC/hwKQ02clco0nz8
```

```
andrew.feller@gmail.com ssh-ed25519  
AAAAC3NzaC1lZDI1NTE5AAAAIALqMCzXle3F0/oa0Iyxkm  
utYphiZ8TH+udmH4Mc/a1V
```

# Setup workstation

## Local repository creation & setup

SSH signing is built upon several OpenSSH features:

- public and private keys
- allowed signers
- ssh-agent

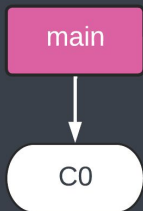


# Signing and verifying commits

Verifying setup with basic commit

```
git commit -S  
git verify-commit  
git log --show-signature
```

```
git config commit.gpgsign true  
git config log.showSignature true
```

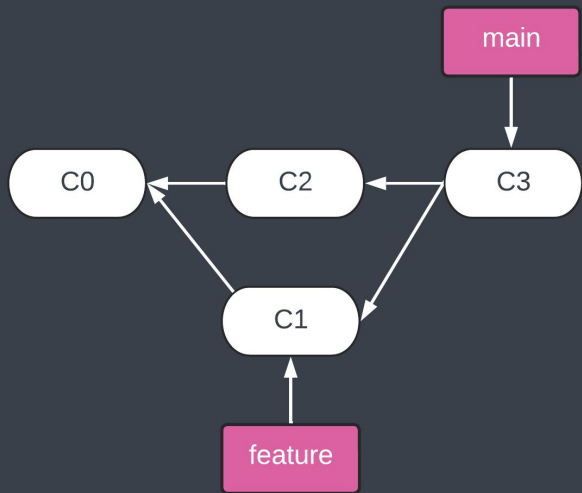


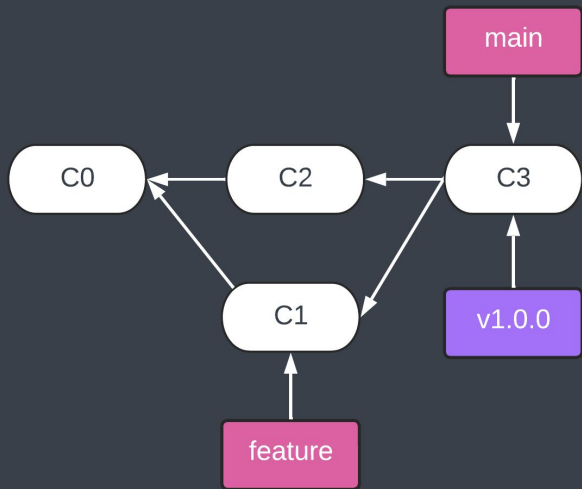
# Signing and verifying merges

Merge verification intricacies

```
git merge --verify-signatures
```

```
git config merge.verifySignatures  
true
```





# Signing and verifying tags

Using annotated tags

```
git tag -s  
git verify-tag
```

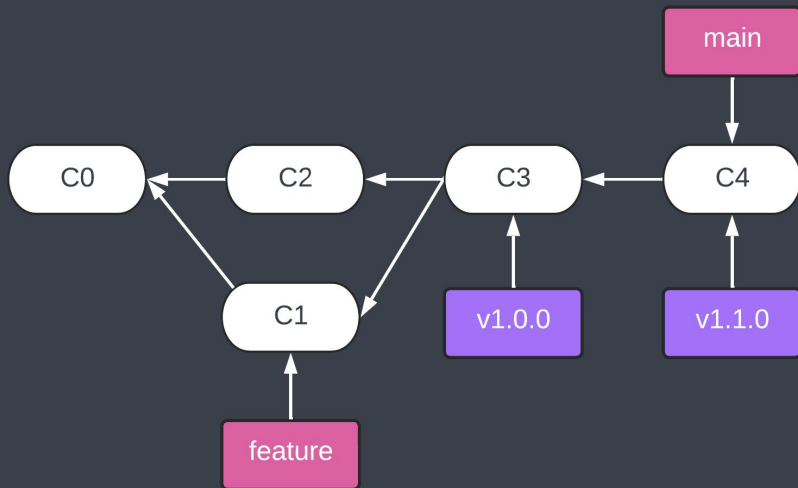
```
git config tag.gpgsign true
```



# Signing past commits and tags

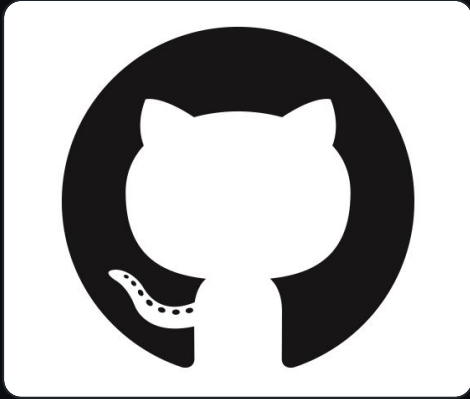
Fixing unsigned oversights

```
git commit -amend  
git tag -s -f
```





# Have adoption plan



GA

[Aug 23rd 2022](#)



In progress

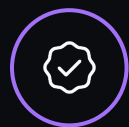
[#343879](#)



In progress

[BCLOUD-3166](#)





# Have adoption plan

## Scale challenges

SSH signing keys will have similar needs to GPG signing:

- Distributed
- Discoverable
- Revocation strategy

## Varies by vendor

Emerging vendor support can make adoption easier:

- Signing key APIs
- Vigilant mode
- Enforce signing

## Trusted allowed signers file

Commit allowed signers file to repository as a short term workaround while vendor support emerges.





# Thank you





# Q&A 🤔

