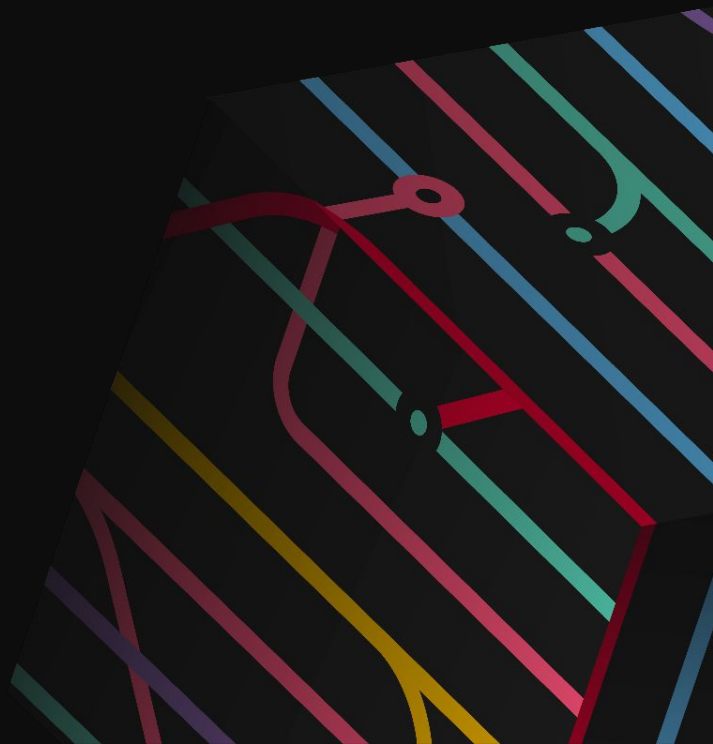


# GIT MERGE 2022

Sep 14th, 2022

2022 Git Merge



# Simplify signing Git commits and tags with SSH keys

Andy Feller

DevOps Engineer, GitHub

@andyfeller



# Outcomes



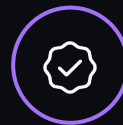
## Understand motivation

Nature of the problem, importance



## Gain firsthand experience

Setup, signing, verifying



## Have adoption plan

From one person to repository-wide





# Understand motivation

The screenshot shows a GitHub commit page for a commit on Aug 26, 2022, by user **ashtom**. The commit message is "I am Tom and I totally wrote this ... not". The commit shows 1 file changed (foo). A warning overlay is present, indicating that the user has not yet uploaded their public key. The overlay also displays the SSH Key Fingerprint: kanlHE9MI77O18EdnFxmEnzc3v1rxJHIW 475lbnHdG8 and a link to learn about vigilant mode.

1 commit      1 file changed      1 contributor

Commits on Aug 26, 2022

I am Tom and I totally wrote this ... not  
ashtom committed 18 days ago

Showing 1 changed file with 1 addition and 0 deletions.

1 foo

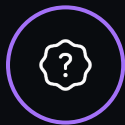
@@ -0,0 +1 @@

Unverified

This user has not yet uploaded their public key.

SSH Key Fingerprint:  
kanlHE9MI77O18EdnFxmEnzc3v1rxJHIW  
475lbnHdG8  
[Learn about vigilant mode.](#)

Sep 14th, 2022      2022 Git Merge      @andyfeller



# Understand motivation

Commits on Aug 26, 2022

**Adding fizz buzz**  
andyfeller committed 18 days ago

Showing 1 changed file with 1 addition and 0 deletions.

1 fizz

@@ -0,0 +1 @@

1

**Verified** 549857d


This commit was signed with the committer's **verified signature**.


andyfeller  
Andy Feller

SSH Key Fingerprint:  
kanlHE9MI77O18EdnFxEznc3v1rxJHIW  
475lbnHdG8  
[Learn about vigilant mode.](#)

Sep 14th, 2022 2022 Git Merge @andyfeller


Unverified

 ad


 This user has not yet uploaded their public key.


SSH Key Fingerprint:  
kanlHE9MI77O18EdnFxgEnzc3v1rxJHIW  
475lbnHdG8  
[Learn about vigilant mode.](#)

Unverified




Signed content that cannot be verified against authors and committers.

 This commit was signed with the committer's **verified signature**.

 **andyfeller**  
Andy Feller

SSH Key Fingerprint:  
kanlHE9MI77O18EdnFxgEnzc3v1rxJHIW  
475lbnHdG8  
[Learn about vigilant mode.](#)

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-----
U1NIU0lHAAAAAQAAADMAAALc3NoLWVkJmJuMTkAAAAgAuowLNeV7cU7+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

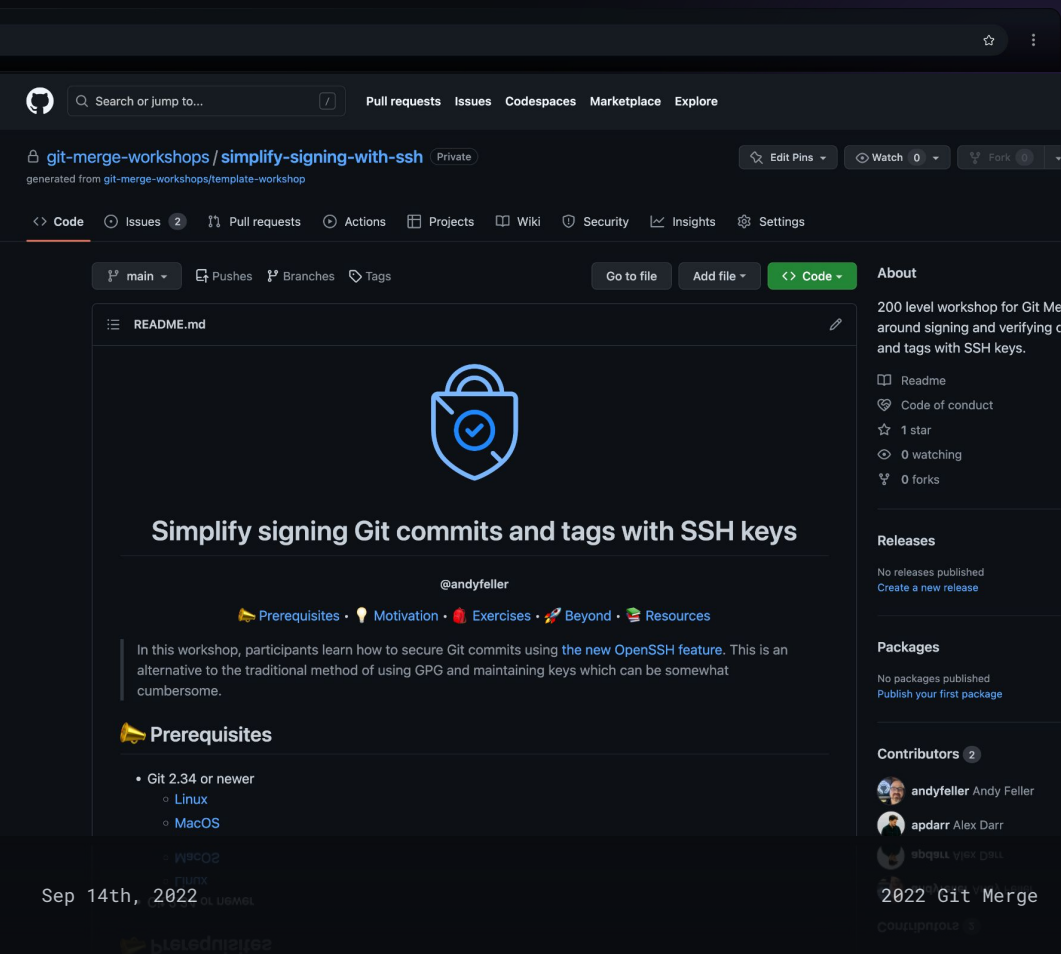
3

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 `git-merge-workshops/template-workshop`. 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 as an alternative to using GPG for signing Git commits. 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

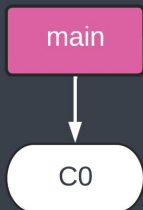


# Signing and verifying commits

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
```

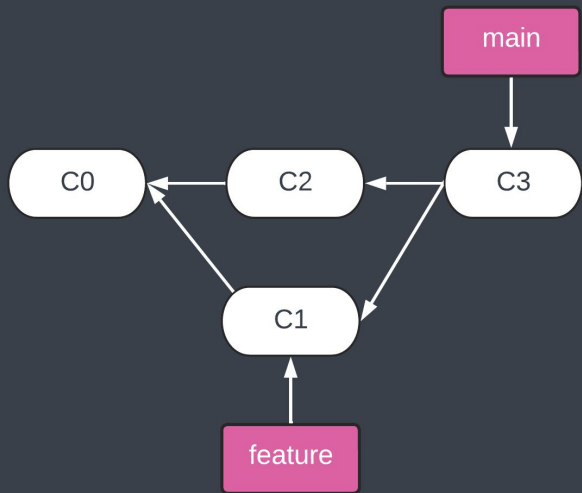


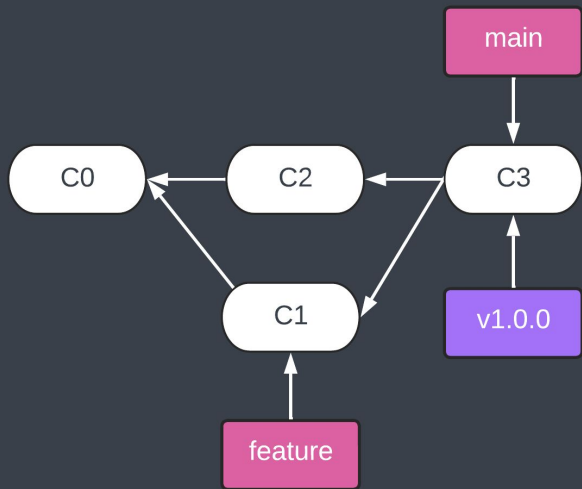
# Signing and verifying merges

Merge verification intricacies

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

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





# Signing and verifying tags

Using annotated tags, exercise end

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

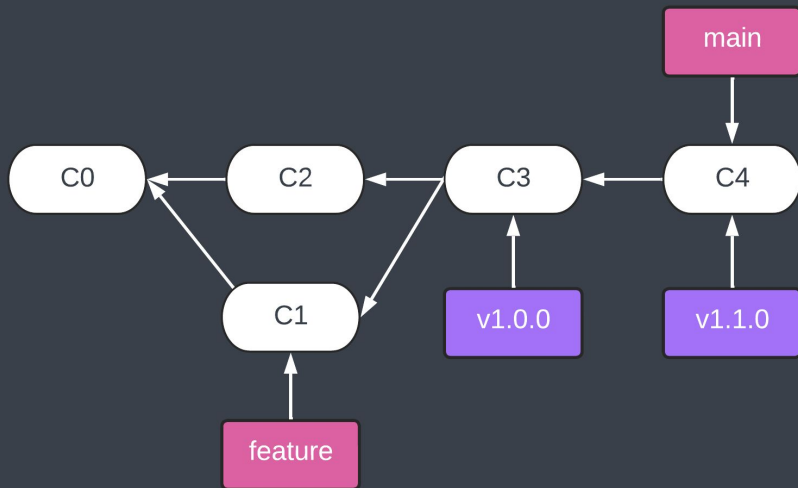
```
git config tag.gpgsign true
```



# Signing past commits and tags

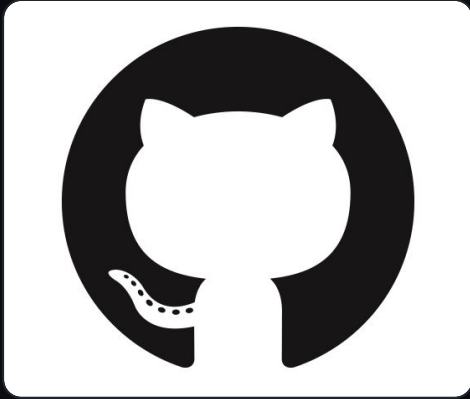
Fixing unsigned oversights

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





# Have adoption plan



GA

[Aug 23rd 2022](#)



In progress

[#343879](#)

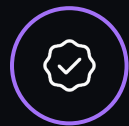


In progress

[BCLOUD-3166](#)







# Have adoption plan

## Scale challenges

SSH signing keys will have similar needs to GPG signing:

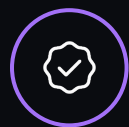
- Distributed
- Discoverable
- Revocation strategy

## Varies by vendor

Emerging vendor support can make adoption easier:

- Signing key APIs
- Vigilant mode
- Enforce signing





# Have adoption plan

## Committing allowed signers file

If necessary, commit allowed signers file to repository as a short term workaround while vendor support emerges.

## Signing involves everyone

Regardless of how you sign, it requires everyone involved to participate.

Unverified commits, merges, and tags will break workflows.





1. 🧑‍🎓 Author opinion: Enterprise challenges

2. 🌐 bitcoin/bitcoin verify-commits

Tooling for verification of PGP signed commits

This is an incomplete work in progress, but currently includes a pre-push hook script (pre-push) to ensure that their own commits are PGP signed (nearly always merge commits), and a script to verify commits against a trusted keys list.

3. 🧑‍💻 andyfeller/gh-ssh-allowed-signers

A gh extension to generate SSH allowed users file from GitHub users' signing keys.

4. 🚀 Vendor support

- GitHub: GA August 23rd 2022

- GitLab: In progress #343879

- BitBucket: In progress BCLLOUD-3166

5. 🔑 1password "Sign your Git commits with 1Password"

We're excited to announce that 1Password now allows you to set up and use SSH keys to sign your commits. With GitHub supporting SSH key signing as well, you can get that verified badge next to your user in seconds. No GPG keys required.



# Beyond

## Beyond introductory workshop

Signing is an extremely deep topic.

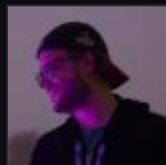
The workshop repository delves into relevant aspects for those interested beyond Git Merge.

Take with a grain of 🧂



# Thank you





# Q&A 🤔



# GIT MERGE 2022

Sep 14th, 2022

2022 Git Merge

