Git-Anon: Anonymous Git with Signatures

MASTER PROJECT BY ERIK ESCHER (33443)

Goals

- Anonymize Authorship towards the public
- Ability to share select information in a closed group
- Cryptographically verifiable assertions about the signatory
- Unlinkability
- Decentralized / Offline support
- Compatibility with existing tooling

Motivation

- Development history contains sensitive/embarrassing information
  - Work times, durations and absences
  - Individual abilities, habits, …
  - Mistakes and responsibilities
- GDPR, „Right to be Forgotten“, …
- Controversial projects, International Law, …
- Valuable for other team members

Primer on Git

- Distributed
- Complete history
- Often public
- “Rewriting History” causes problems

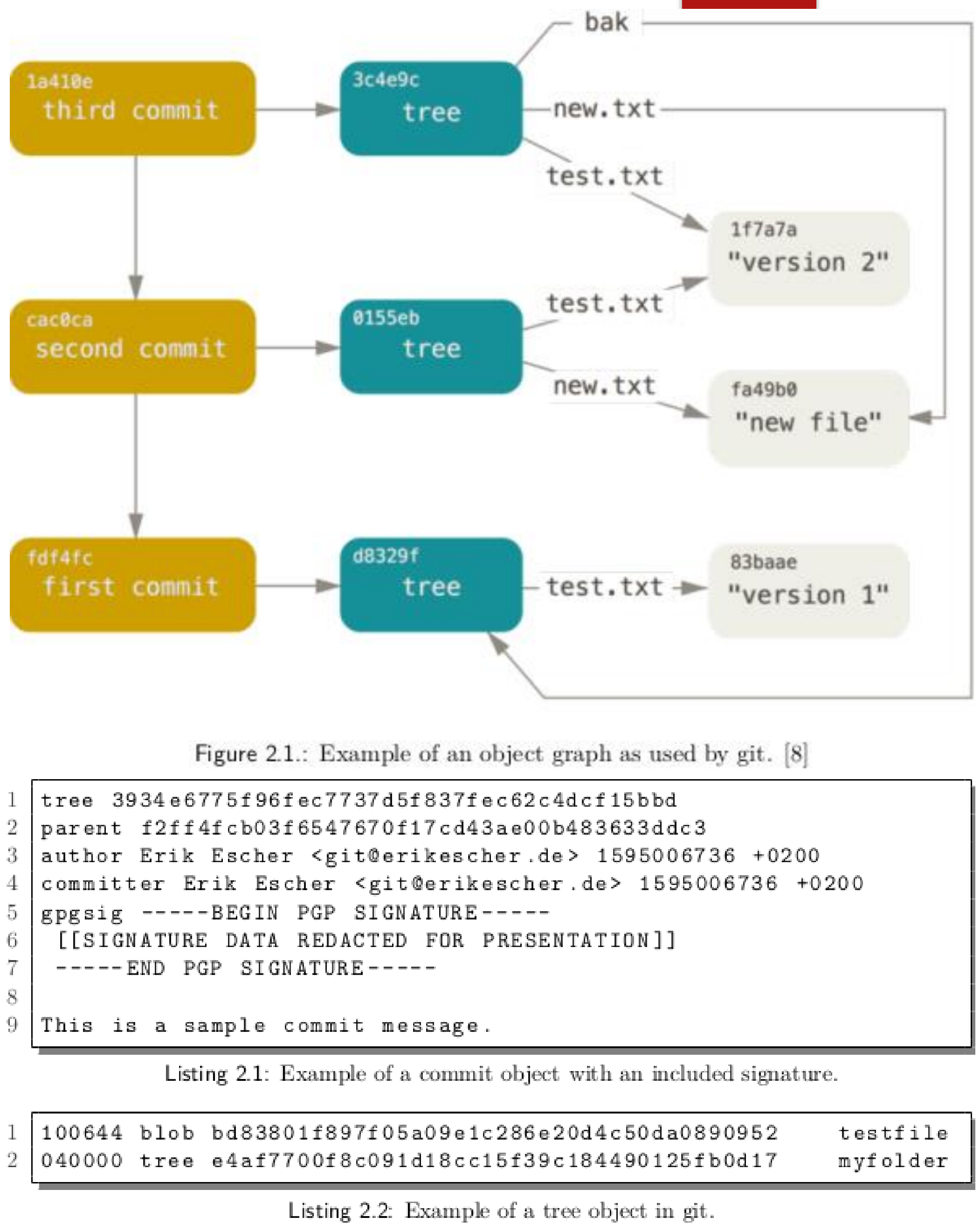

bak
1a410e
third commit
3c4e9c
tree
new.txt
test.txt
1f7a7a
"version 2"
cac0ca
second commit
0155eb
tree
test.txt
new.txt
fa49b0
"new file"
fdf4fc
first commit
d8329f
tree
test.txt
83baae
"version 1"

Figure 2.1.: Example of an object graph as used by git. [8]

```
tree 3934e6775f96fec7737d5f837fec62c4dcf15bbd
parent f2ff4fcb03f6547670f17cd43ae00b483633ddc3
author Erik Escher <git@erikescher.de> 1595006736 +0200
committer Erik Escher <git@erikescher.de> 1595006736 +0200
gpgsig -----BEGIN PGP SIGNATURE-----
 [[SIGNATURE DATA REDACTED FOR PRESENTATION]]
 -----END PGP SIGNATURE-----

This is a sample commit message.
```

Listing 2.1: Example of a commit object with an included signature.

```
100644 blob bd83801f897f05a09e1c286e20d4c50da0890952    testfile
040000 tree e4af7700f8c091d18cc15f39c184490125fb0d17    myfolder
```

Listing 2.2: Example of a tree object in git.

Primer on OpenPGP

- Composed of packets
- Asymmetric key pairs
  - “Erik Escher <erik@erikescher.de>“
    - Attested via Certifications
  - “Erik Escher (Student) <erik.escher@hs-weingarten.de>”
    - Attested via Certifications
  - “John Doe”
- Can be split up and recombined

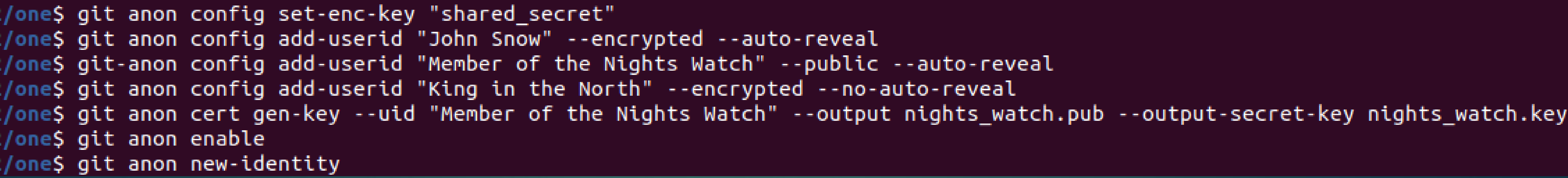
Solution/Implementation

- Ephemeral signature keys per commit
  - Key information stored in content addressed storage
  - UserIDs contain claims about the user's attributes/names
  - CAs optionally certify UserIDs to confirm the attributes
- References to keys where names are needed
- → Cryptographically verifiable assertions about the keyholder

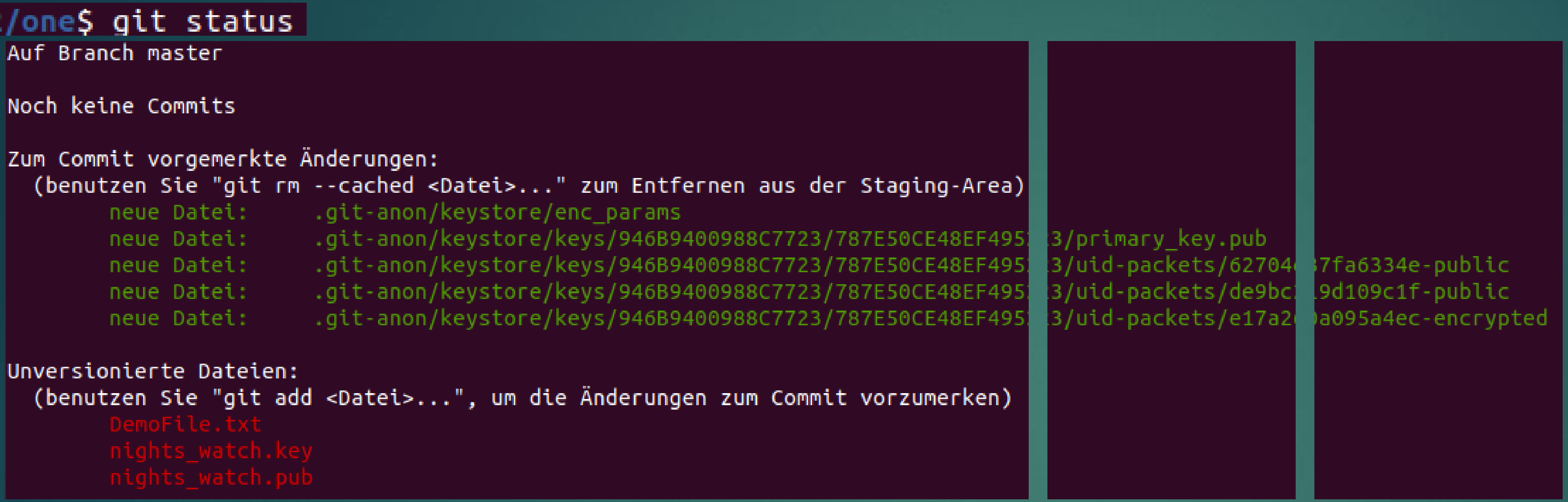
Solution/Implementation

- UserIDs are distributed selectively
  - Databases, mail, different repository, file shares, …
  - Encrypted Publishing
    - Subfolder or Branch in the repository
    - Blockchain
  - → Currently: symmetrically encrypted in a subfolder
  - → External storage would allow deletion

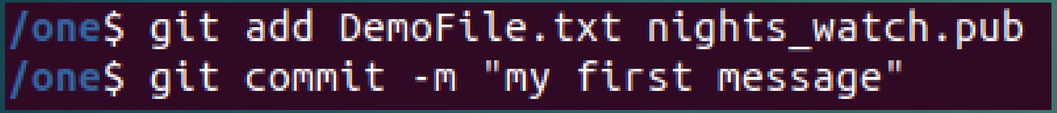
DEMO



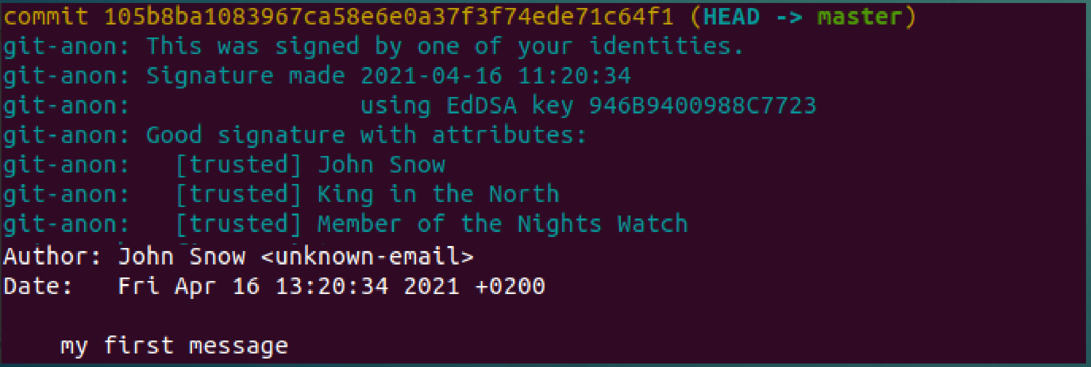
```
/one$ git anon config set-enc-key "shared_secret"
/one$ git anon config add-userid "John Snow" --encrypted --auto-reveal
/one$ git-anon config add-userid "Member of the Nights Watch" --public --auto-reveal
/one$ git anon config add-userid "King in the North" --encrypted --no-auto-reveal
/one$ git anon cert gen-key --uid "Member of the Nights Watch" --output nights_watch.pub --output-secret-key nights_watch.key
/one$ git anon enable
/one$ git anon new-identity
```



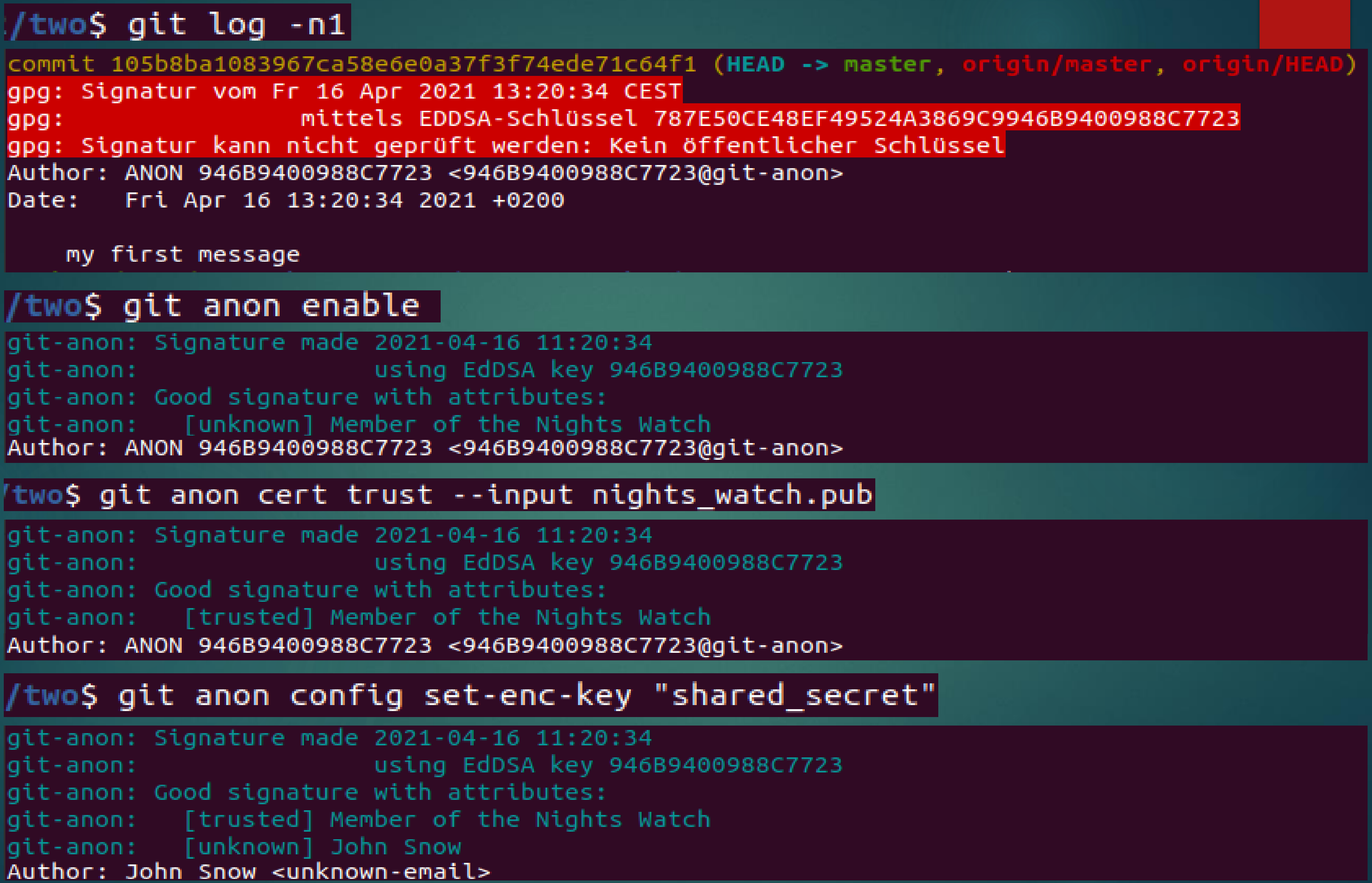
```
/one$ git status
Auf Branch master

Noch keine Commits

Zum Commit vorgemerkte Änderungen:
  (benutzen Sie "git rm --cached <Datei>..." zum Entfernen aus der Staging-Area)
        neue Datei:     .git-anon/keystore/enc_params
        neue Datei:     .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF495 3/primary_key.pub
        neue Datei:     .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF495 3/uid-packets/62704 7fa6334e-public
        neue Datei:     .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF495 3/uid-packets/de9bc 9d109c1f-public
        neue Datei:     .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF495 3/uid-packets/e17a2 a095a4ec-encrypted

Unversionierte Dateien:
  (benutzen Sie "git add <Datei>...", um die Änderungen zum Commit vorzumerken)
        DemoFile.txt
        nights_watch.key
        nights_watch.pub
```



```
/one$ git add DemoFile.txt nights_watch.pub
/one$ git commit -m "my first message"
```



```
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master)
git-anon: This was signed by one of your identities.
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                 using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [trusted] John Snow
git-anon:   [trusted] King in the North
git-anon:   [trusted] Member of the Nights Watch
Author: John Snow <unknown-email>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
```



```
:/two$ git log -n1
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master, origin/master, origin/HEAD)
gpg: Signatur vom Fr 16 Apr 2021 13:20:34 CEST
gpg:                mittels EDDSA-Schlüssel 787E50CE48EF49524A3869C9946B9400988C7723
gpg: Signatur kann nicht geprüft werden: Kein öffentlicher Schlüssel
Author: ANON 946B9400988C7723 <946B9400988C7723@git-anon>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
```

```
/two$ git anon enable
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [unknown] Member of the Nights Watch
Author: ANON 946B9400988C7723 <946B9400988C7723@git-anon>
```

```
/two$ git anon cert trust --input nights_watch.pub
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [trusted] Member of the Nights Watch
Author: ANON 946B9400988C7723 <946B9400988C7723@git-anon>
```

```
/two$ git anon config set-enc-key "shared_secret"
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [trusted] Member of the Nights Watch
git-anon:   [unknown] John Snow
Author: John Snow <unknown-email>
```

Conclusion

Outlook

Open Source Release

- https://github.com/erikescher/git-anon
- https://pypi.org/package/git-anon

Thanks for your attention!

Questions?

[32]

- https://github.com/erikescher/git-anon
- https://pypi.org/package/git-anon

Sources

[1] Andrew Ayer. git-crypt - transparent file encryption in git. 2020. url: https://www.agwa.name/projects/git-crypt/ (visited on 2020-07-24).

[2] Andrew Ayer. Ubuntu Manpage: git-crypt - transparent file encryption in Git. Ed. by Canonical Ltd. 2020. url: https://manpages.ubuntu.com/manpages/focal/man1/git-crypt.1.html (visited on 2020-07-24).

[3] Andrew Ayer and other Contributors. GitHub: git-crypt - transparent file encryption in git. Version 7c129cdd3830a55a8611eecf82af08cd3301f7f2. 2020-04-28. url: https://github.com/AGWA/git-crypt (visited on 2020-07-24).

[4] Bundesamt für Sicherheit in der Informationstechnik. BSI - Bundesamt für Sicherheit in der Informationstechnik. 2020. url: https://www.bsi.bund.de/ (visited on 2020-07-31).

[5] Cambridge University Press. Anonymity - Cambridge English Dictionary. url: https://dictionary.cambridge.org/de/worterbuch/englisch/anonymity (visited on 2020-08-04).

[6] Scott Chacon, Jason Long, and Other Contributors. Git. Version 7714726. 2021-03-03. url: https://git-scm.com (visited on 2021-03-13).

[7] Scott Chacon, Jason Long, and Other Contributors. Git - Reference. Version 7714726. 2021-03-03. url: https://git-scm.com/docs (visited on 2021-03-13).

[8] Scott Chacon and Ben Straub. Pro git: Everything you need to know about Git. English. Second. Apress, url: https://git-scm.com/book/en/v2.

[9] Debian Project. Popularity Contest Statistics – Debian Quality Assurance - qa.debian.org/. 2020-10-09. url: https://qa.debian.org/popcon-graph.php?packages=git+mercurial+subversion+bazaar+cvs&show_installed=on&show_vote=on&want_legend=on&want_ticks=on&from_date=&to_date=&hlght_date=&date_fmt=%25Y-%25m&beenhere=1 (visited on 2020-10-09).

[10] Gitlab Developers. Repository mirroring - Gitlab. Version ae7269d1eac6d4ab2970a740797cebbe9328ffd1. 2020-07-03. url: https://docs.gitlab.com/ee/user/project/repository/repository_mirroring.html (visited on 2020-07-24).

[11] Thomas Durieux et al. Anonymous Github. 2020-06-10. url: https://anonymous.4open.science/ (visited on 2020-08-06).

[12] Thomas Durieux et al. Anonymous Github. Version add12b45ecaf3bfa41e44cd283b1705ccdd3acee. 2020-06-10. url: https://github.com/tdurieux/anonymous_github/ (visited on 2020-08-06).

Sources

[13] Hal Finney et al. OpenPGP Message Format. RFC 4880. 2007-11. doi: 10.17487/RFC4880. url: https://rfc-editor.org/rfc/rfc4880.txt (visited on 2020-07-30).

[14] Python Software Foundation. PyPI - The Python Package Index. 2020. url: https://pypi.org (visited on 2021-03-11).

[15] g10 Code GmbH. The GNU Privacy Guard. 2020-07-09. url: https://gnupg.org (visited on 2020-07-30).

[16] Governikus GmbH & Co. KG. Beglaubigung OpenPGP-Schlüssel. 2020. url: https://pgp.governikus.de/pgp/ (visited on 2020-07-31).

[17] Governikus GmbH & Co. KG. Governikus KG. 2020. url: https://www.governikus.de/ (visited on 2020-07-31).

[18] Owen Jacobson. Notes Towards Detached Signatures in Git. Initial publishing date likely earlier but unknown. See also : https://github.com/grimoire-ca/bliki/commit/ee3370cfa5cb17261f722c501c94edf0a431f91d. 2020-01-30. url: https://grimoire.ca/git/detached-sigs/ (visited on 2020-07-28).

[19] Jason Kulatunga. gitMask - Develop Anonymously. 2020. url: https://www.gitmask.com/ (visited on 2020-07-24).

[20] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf. v0.34. 2010-08. url: http://dud.inf.tu-dresden.de/literatur/Anon%5C_Terminology%5C_v0.34.pdf (visited on 2020-08-05).

[21] Proton Technologies AG. Everything you need to know about the "Right to be forgotten". GDPR.eu. Section: GDPR Overview. 2018-11-05. url: https://gdpr.eu/right-to-be-forgotten/ (visited on 2020-10-09).

[22] Pete Resnick. Internet Message Format. RFC 2822. 2001-04. doi: 10.17487/RFC2822. url: https://rfc-editor.org/rfc/rfc2822.txt (visited on 2020-10-09).

[23] Synopsis, Inc. Compare Repositories - Open Hub - www.openhub.net/. Compare Repositories. url: https://www.openhub.net/repositories/compare (visited on 2020-10-09).

[24] Peter Todd. Solving the PGP Revocation Problem with OpenTimestamps for Git Commits. 2016-09-26. url: https://petertodd.org/2016/opentimestamps-git-integration (visited on 2021-03-13).

Sources

[25] Sebastien Varrette. Using Git-crypt to Protect Sensitive Data. 2018-12-07. url: https://varrette.gforge.uni.lu/blog/2018/12/07/using-git-crypt-to-protect-sensitive-data/#removing-a-collaborator-from- the- vault (visited on 2020-07-24).

[26] Lance R. Vick et al. Github: Git Signatures. Version 979f207a1c1342b9342aa58be914fc51a0c62f87. 2018-10-03. url: https://github.com/hashbang/git-signatures (visited on 2020-07-28).

[27] Wikipedia contributors. Anonymity — Wikipedia, The Free Encyclopedia. 2020. url: https://en.wikipedia.org/w/index.php?title=Anonymity&oldid=969056091 (visited on 2020-08-04).

[28] Wikipedia contributors. Pseudonymity — Wikipedia, The Free Encyclopedia. 2020. url: https://en.wikipedia.org/w/index.php?title=Pseudonymity&oldid=967108928 (visited on 2020-08-04).

[29] Wikipedia contributors. Right to be forgotten. In: en.wikipedia.org/. Page Version ID: 979590717. 2020-09-21. url: https://en.wikipedia.org/w/index.php?title=Right_to_be_forgotten&oldid=979590717 (visited on 2020-10-09).

[30] Wiktionary. anonymous — Wiktionary, The Free Dictionary. 2020. url: https://en.wiktionary.org/w/index.php?title=anonymous&oldid=59666697 (visited on 2020-08-04).

[31] Wiktionary. pseudonymous — Wiktionary, The Free Dictionary. 2020. url: https://en.wiktionary.org/w/index.php?title=pseudonymous&oldid=59415419 (visited on 2020-08-04).

[32] https://office.microsoft.com/de-de/images/results.aspx?qu=00423171.wmf&ex=2#ai:MC900423171 (visited on 2013-07-01).

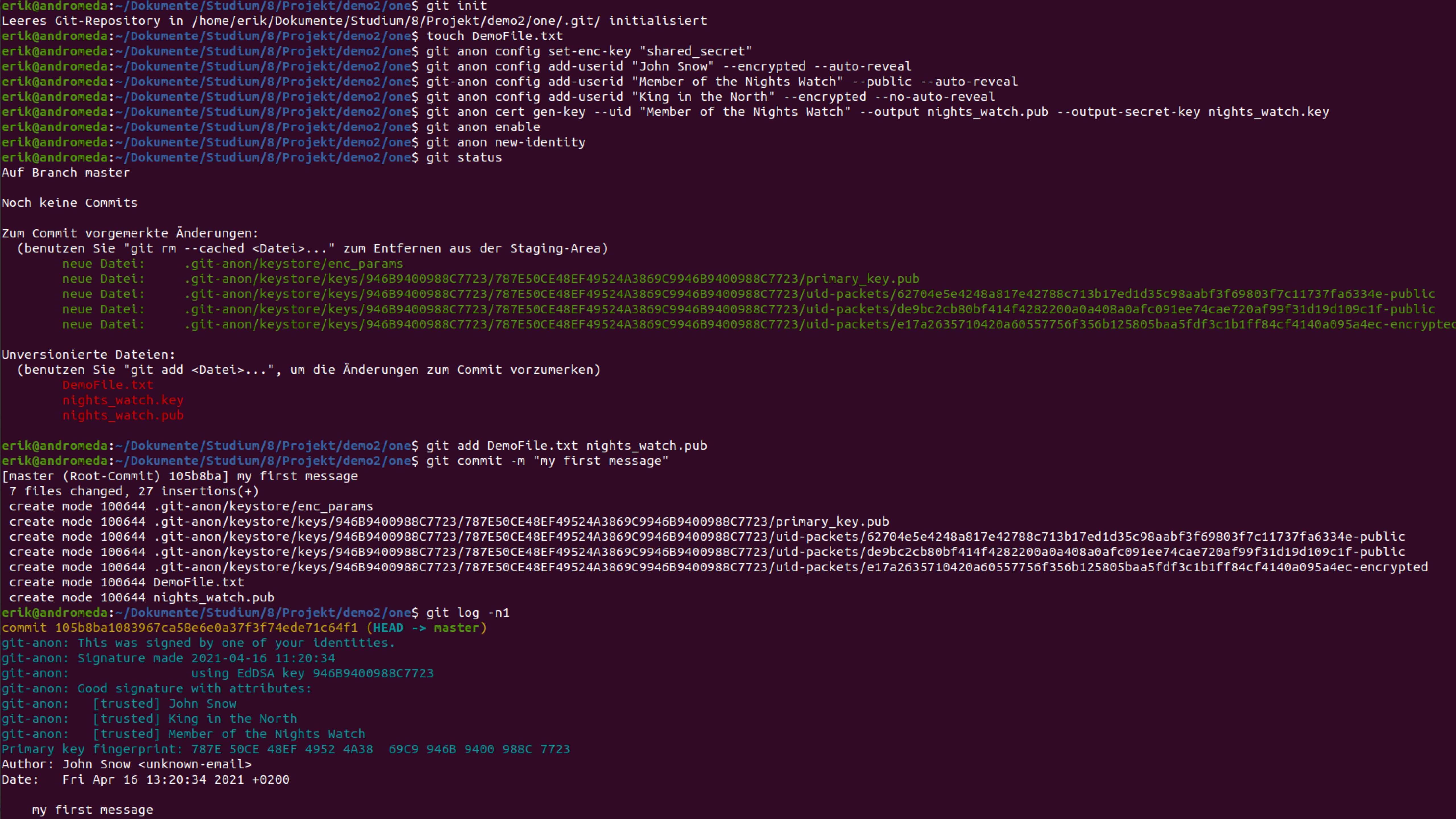
Backup-Slides

Why OpenPGP and not <insert simple signature system>

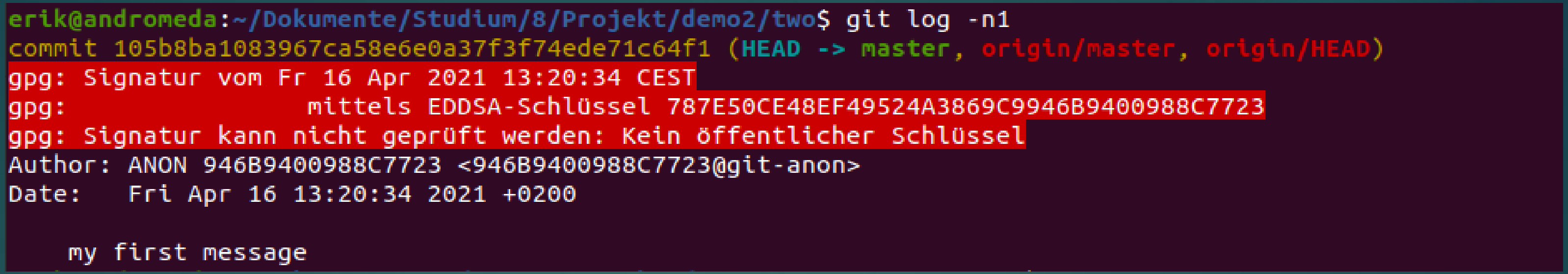
- Alternatives:
  - Signify
  - Plain Signatures
- Git specifies OpenPGP signatures(though it does not check and should work with others)
- GPG provides useful features
  - deals with partial certificate information
  - Simplifies Certifications from existing GPG Keys
  - Certification model is suitable
  - Security guarantees for certification and recombining keys
- GPG binaries are available on (almost) all Linux systems simplifying verification without special software (this could be made easier)
- Future versions might switch to such a system

Existing Solutions

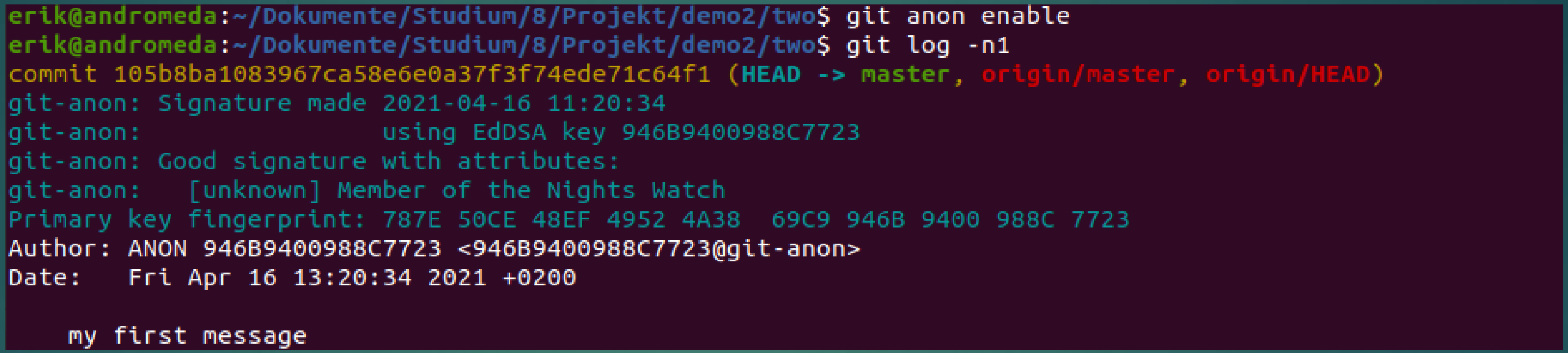
- Long-Term Pseudonyms
  - Easy to compromise accidentally
- External Anonymization Systems
  - Requires trust in the operator
  - Identitiy often cannot be revealed easily later
  - Often relies on nobody attempting to bypass it
  - Signatures typically impossible/useless



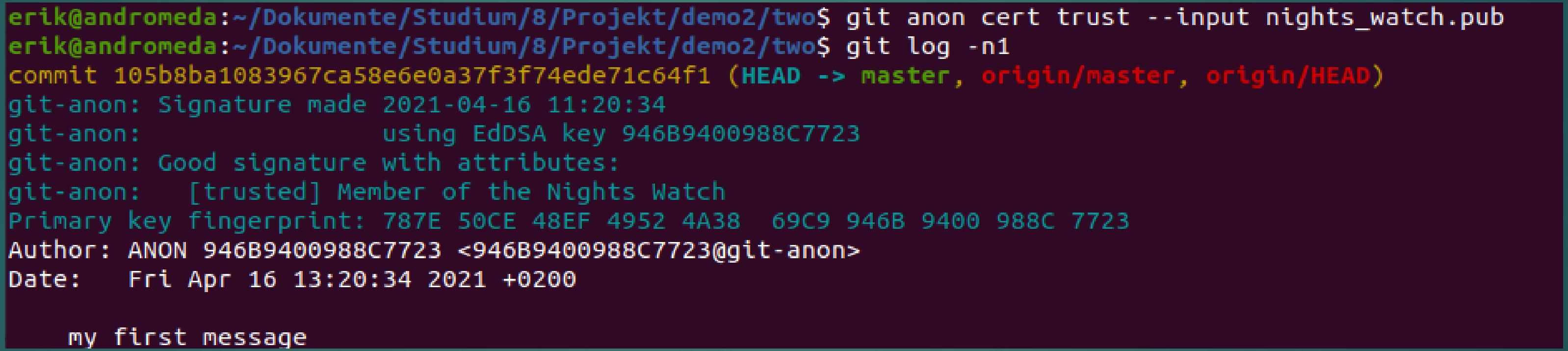
```
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git init
Leeres Git-Repository in /home/erik/Dokumente/Studium/8/Projekt/demo2/one/.git/ initialisiert
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ touch DemoFile.txt
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git anon config set-enc-key "shared_secret"
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git anon config add-userid "John Snow" --encrypted --auto-reveal
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git-anon config add-userid "Member of the Nights Watch" --public --auto-reveal
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git anon config add-userid "King in the North" --encrypted --no-auto-reveal
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git anon cert gen-key --uid "Member of the Nights Watch" --output nights_watch.pub --output-secret-key nights_watch.key
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git anon enable
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git anon new-identity
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git status
Auf Branch master

Noch keine Commits

Zum Commit vorgemerkte Änderungen:
  (benutzen Sie "git rm --cached <Datei>..." zum Entfernen aus der Staging-Area)
        neue Datei:     .git-anon/keystore/enc_params
        neue Datei:     .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF49524A3869C9946B9400988C7723/primary_key.pub
        neue Datei:     .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF49524A3869C9946B9400988C7723/uid-packets/62704e5e4248a817e42788c713b17ed1d35c98aabf3f69803f7c11737fa6334e-public
        neue Datei:     .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF49524A3869C9946B9400988C7723/uid-packets/de9bc2cb80bf414f4282200a0a408a0afc091ee74cae720af99f31d19d109c1f-public
        neue Datei:     .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF49524A3869C9946B9400988C7723/uid-packets/e17a2635710420a60557756f356b125805baa5fdf3c1b1ff84cf4140a095a4ec-encrypted

Unversionierte Dateien:
  (benutzen Sie "git add <Datei>...", um die Änderungen zum Commit vorzumerken)
        DemoFile.txt
        nights_watch.key
        nights_watch.pub

erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git add DemoFile.txt nights_watch.pub
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git commit -m "my first message"
[master (Root-Commit) 105b8ba] my first message
 7 files changed, 27 insertions(+)
 create mode 100644 .git-anon/keystore/enc_params
 create mode 100644 .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF49524A3869C9946B9400988C7723/primary_key.pub
 create mode 100644 .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF49524A3869C9946B9400988C7723/uid-packets/62704e5e4248a817e42788c713b17ed1d35c98aabf3f69803f7c11737fa6334e-public
 create mode 100644 .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF49524A3869C9946B9400988C7723/uid-packets/de9bc2cb80bf414f4282200a0a408a0afc091ee74cae720af99f31d19d109c1f-public
 create mode 100644 .git-anon/keystore/keys/946B9400988C7723/787E50CE48EF49524A3869C9946B9400988C7723/uid-packets/e17a2635710420a60557756f356b125805baa5fdf3c1b1ff84cf4140a095a4ec-encrypted
 create mode 100644 DemoFile.txt
 create mode 100644 nights_watch.pub
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/one$ git log -n1
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master)
git-anon: This was signed by one of your identities.
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [trusted] John Snow
git-anon:   [trusted] King in the North
git-anon:   [trusted] Member of the Nights Watch
Primary key fingerprint: 787E 50CE 48EF 4952 4A38  69C9 946B 9400 988C 7723
Author: John Snow <unknown-email>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
```



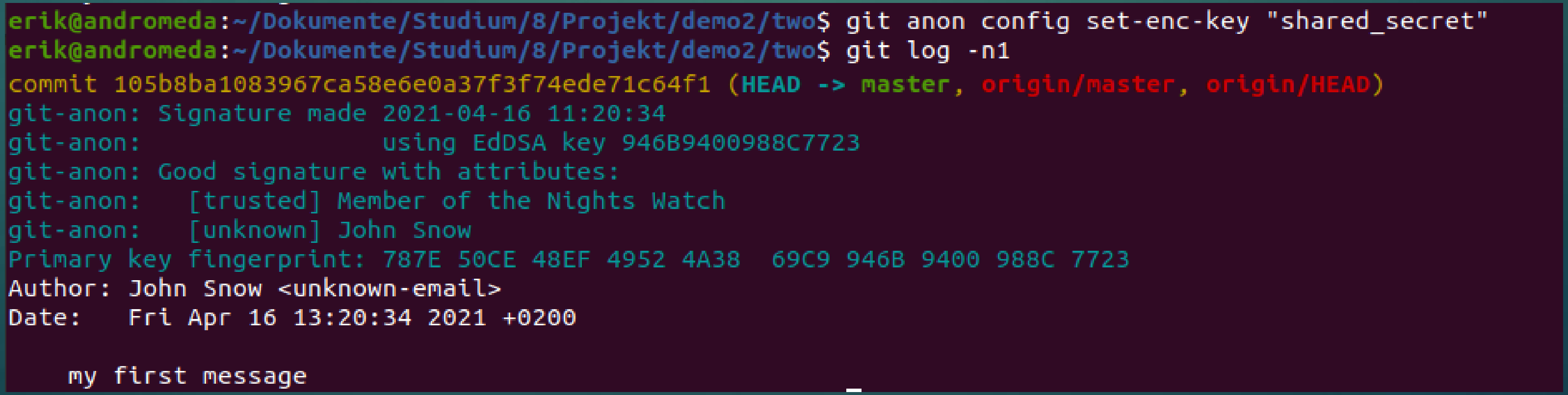
```
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/two$ git log -n1
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master, origin/master, origin/HEAD)
gpg: Signatur vom Fr 16 Apr 2021 13:20:34 CEST
gpg:                mittels EDDSA-Schlüssel 787E50CE48EF49524A3869C9946B9400988C7723
gpg: Signatur kann nicht geprüft werden: Kein öffentlicher Schlüssel
Author: ANON 946B9400988C7723 <946B9400988C7723@git-anon>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
```



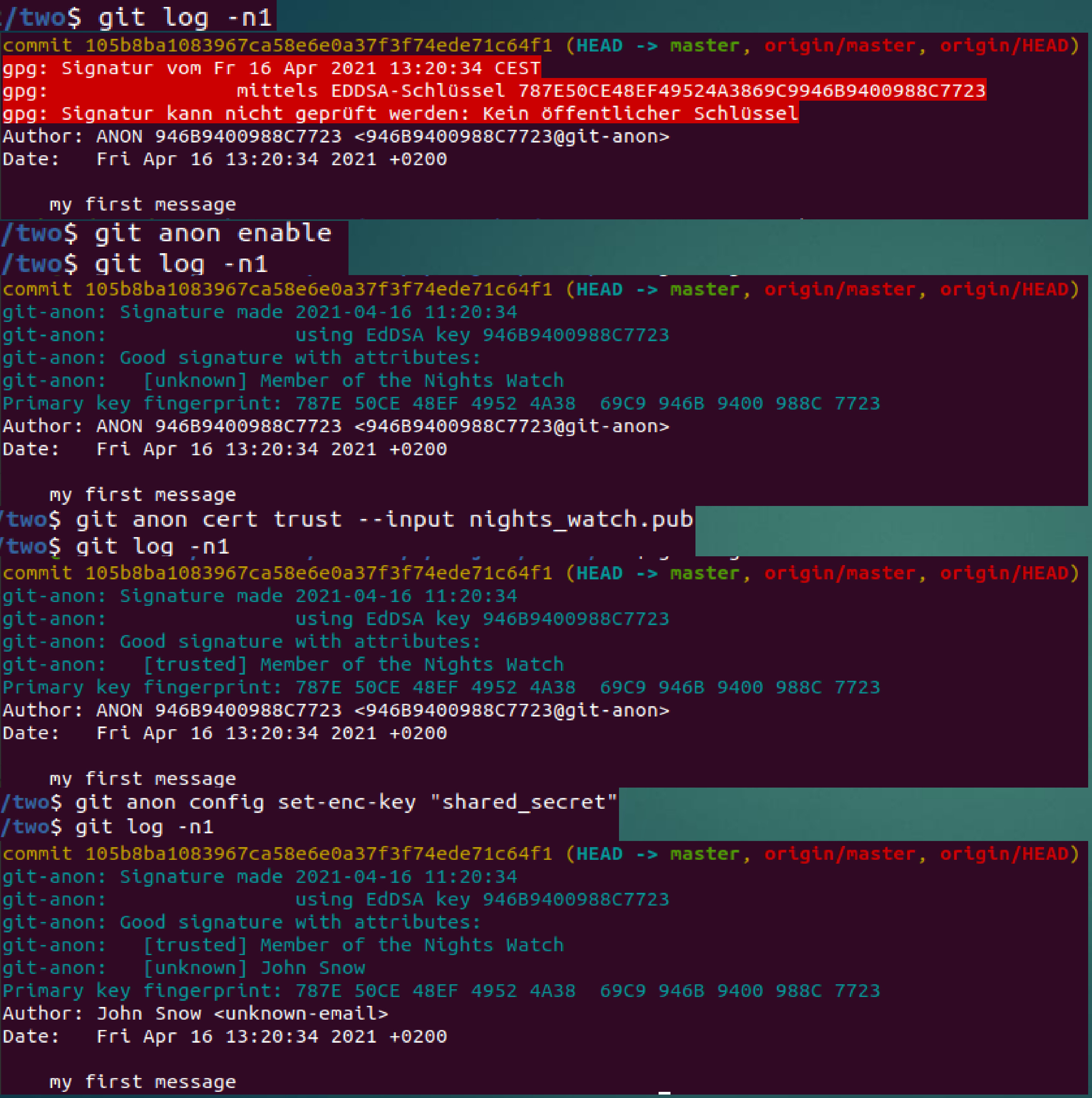
```
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/two$ git anon enable
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/two$ git log -n1
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master, origin/master, origin/HEAD)
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [unknown] Member of the Nights Watch
Primary key fingerprint: 787E 50CE 48EF 4952 4A38  69C9 946B 9400 988C 7723
Author: ANON 946B9400988C7723 <946B9400988C7723@git-anon>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
```



```
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/two$ git anon cert trust --input nights_watch.pub
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/two$ git log -n1
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master, origin/master, origin/HEAD)
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [trusted] Member of the Nights Watch
Primary key fingerprint: 787E 50CE 48EF 4952 4A38  69C9 946B 9400 988C 7723
Author: ANON 946B9400988C7723 <946B9400988C7723@git-anon>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
```



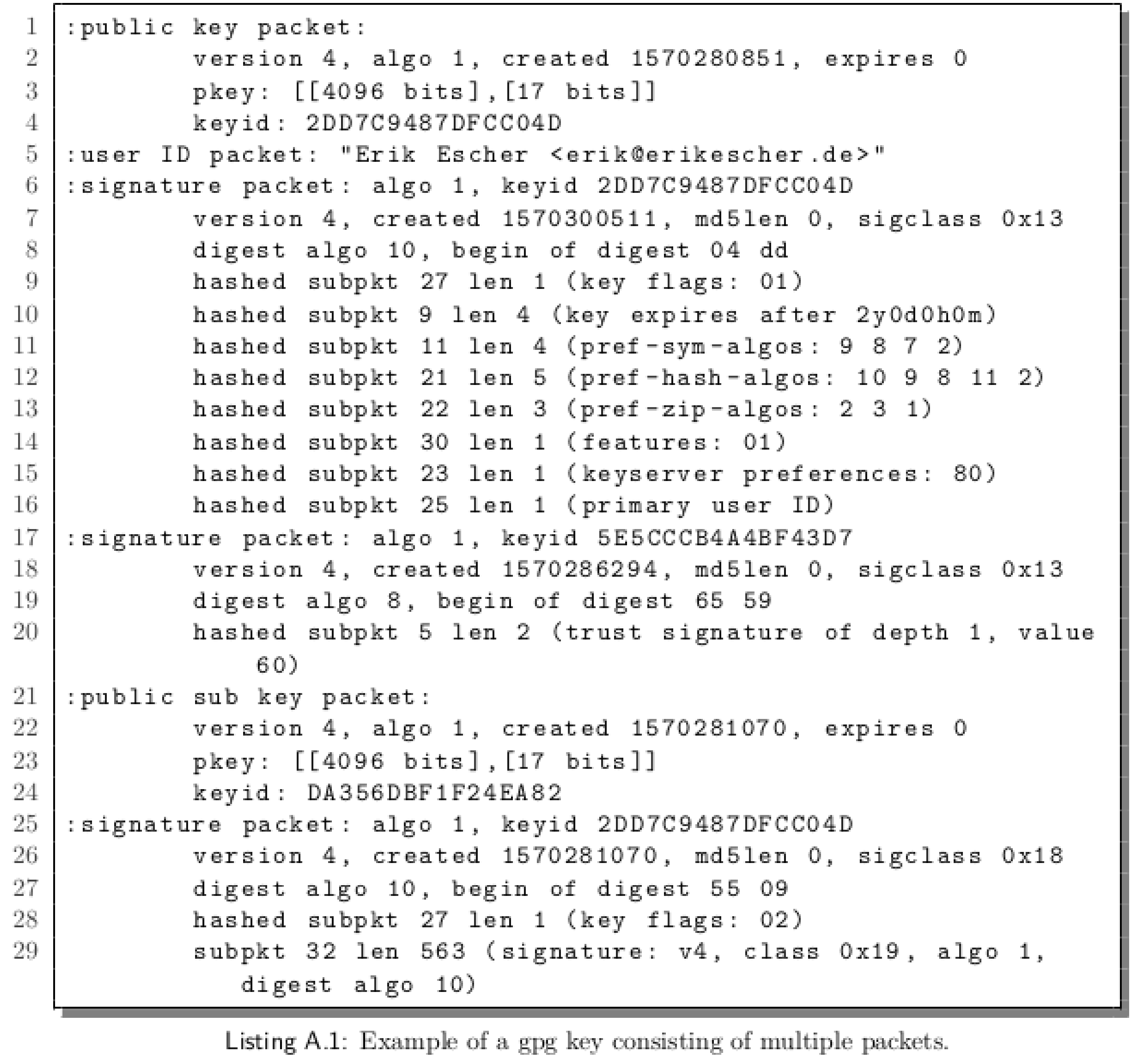
```
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/two$ git anon config set-enc-key "shared_secret"
erik@andromeda:~/Dokumente/Studium/8/Projekt/demo2/two$ git log -n1
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master, origin/master, origin/HEAD)
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [trusted] Member of the Nights Watch
git-anon:   [unknown] John Snow
Primary key fingerprint: 787E 50CE 48EF 4952 4A38  69C9 946B 9400 988C 7723
Author: John Snow <unknown-email>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
```



```
/two$ git log -n1
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master, origin/master, origin/HEAD)
gpg: Signatur vom Fr 16 Apr 2021 13:20:34 CEST
gpg:                mittels EDDSA-Schlüssel 787E50CE48EF49524A3869C9946B9400988C7723
gpg: Signatur kann nicht geprüft werden: Kein öffentlicher Schlüssel
Author: ANON 946B9400988C7723 <946B9400988C7723@git-anon>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
/two$ git anon enable
/two$ git log -n1
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master, origin/master, origin/HEAD)
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [unknown] Member of the Nights Watch
Primary key fingerprint: 787E 50CE 48EF 4952 4A38  69C9 946B 9400 988C 7723
Author: ANON 946B9400988C7723 <946B9400988C7723@git-anon>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
/two$ git anon cert trust --input nights_watch.pub
/two$ git log -n1
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master, origin/master, origin/HEAD)
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [trusted] Member of the Nights Watch
Primary key fingerprint: 787E 50CE 48EF 4952 4A38  69C9 946B 9400 988C 7723
Author: ANON 946B9400988C7723 <946B9400988C7723@git-anon>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
/two$ git anon config set-enc-key "shared_secret"
/two$ git log -n1
commit 105b8ba1083967ca58e6e0a37f3f74ede71c64f1 (HEAD -> master, origin/master, origin/HEAD)
git-anon: Signature made 2021-04-16 11:20:34
git-anon:                using EdDSA key 946B9400988C7723
git-anon: Good signature with attributes:
git-anon:   [trusted] Member of the Nights Watch
git-anon:   [unknown] John Snow
Primary key fingerprint: 787E 50CE 48EF 4952 4A38  69C9 946B 9400 988C 7723
Author: John Snow <unknown-email>
Date:   Fri Apr 16 13:20:34 2021 +0200

    my first message
```

Potential Extensions

- Replacing/Augmenting Connection Based Authentication with Content Based Authentication



```
:public key packet:
        version 4, algo 1, created 1570280851, expires 0
        pkey: [[4096 bits],[17 bits]]
        keyid: 2DD7C9487DFCC04D
:user ID packet: "Erik Escher <erik@erikescher.de>"
:signature packet: algo 1, keyid 2DD7C9487DFCC04D
        version 4, created 1570300511, md5len 0, sigclass 0x13
        digest algo 10, begin of digest 04 dd
        hashed subpkt 27 len 1 (key flags: 01)
        hashed subpkt 9 len 4 (key expires after 2y0d0h0m)
        hashed subpkt 11 len 4 (pref-sym-algos: 9 8 7 2)
        hashed subpkt 21 len 5 (pref-hash-algos: 10 9 8 11 2)
        hashed subpkt 22 len 3 (pref-zip-algos: 2 3 1)
        hashed subpkt 30 len 1 (features: 01)
        hashed subpkt 23 len 1 (keyserver preferences: 80)
        hashed subpkt 25 len 1 (primary user ID)
:signature packet: algo 1, keyid 5E5CCCB4A4BF43D7
        version 4, created 1570286294, md5len 0, sigclass 0x13
        digest algo 8, begin of digest 65 59
        hashed subpkt 5 len 2 (trust signature of depth 1, value 60)
:public sub key packet:
        version 4, algo 1, created 1570281070, expires 0
        pkey: [[4096 bits],[17 bits]]
        keyid: DA356DBF1F24EA82
:signature packet: algo 1, keyid 2DD7C9487DFCC04D
        version 4, created 1570281070, md5len 0, sigclass 0x18
        digest algo 10, begin of digest 55 09
        hashed subpkt 27 len 1 (key flags: 02)
        subpkt 32 len 563 (signature: v4, class 0x19, algo 1, digest algo 10)
```

Listing A.1: Example of a gpg key consisting of multiple packets.