NAME

gitformat-signature - Git cryptographic signature formats

SYNOPSIS

<[tag|commit] object header(s)>
<over-the-wire protocol>

DESCRIPTION

Git uses cryptographic signatures in various places, currently objects (tags, commits, mergetags) and transactions (pushes). In every case, the command which is about to create an object or transaction determines a payload from that, calls an external program to obtain a detached signature for the payload (**gpg -bsa** in the case of PGP signatures), and embeds the signature into the object or transaction.

Signatures begin with an "ASCII Armor" header line and end with a tail line, which differ depending on signature type (as selected by **gpg.format**, see **git-config**(1)). These are, for **gpg.format** values:

gpg (PGP)
: **-----BEGIN PGP SIGNATURE-----** and **-----END PGP SIGNATURE-----**. Or, if gpg is told to produce RFC1991 signatures, **-----BEGIN PGP MESSAGE-----** and **-----END PGP MESSAGE-----**

ssh (SSH)
: **-----BEGIN SSH SIGNATURE-----** and **-----END SSH SIGNATURE-----**

x509 (X.509)
: **-----BEGIN SIGNED MESSAGE-----** and **-----END SIGNED MESSAGE-----**

Signatures sometimes appear as a part of the normal payload (e.g. a signed tag has the signature block appended after the payload that the signature applies to), and sometimes appear in the value of an object header (e.g. a merge commit that merged a signed tag would have the entire tag contents on its "mergetag" header). In the case of the latter, the usual multi-line formatting rule for object headers applies. I.e. the second and subsequent lines are prefixed with a SP to signal that the line is continued from the previous line.

This is even true for an originally empty line. In the following examples, the end of line that ends with a whitespace letter is highlighted with a **$** sign; if you are trying to recreate these example by hand, do not cut and paste them--they are there primarily to highlight extra whitespace at the end of some lines.

The signed payload and the way the signature is embedded depends on the type of the object resp. transaction.

TAG SIGNATURES

- by: **git tag -s**

- annotated tag object

- append the signature to the unsigned tag object

- tag **signedtag** with subject **signed tag**

```
object 04b871796dc0420f8e7561a895b52484b701d51a
type commit
tag signedtag
tagger C O Mitter <committer@example.com> 1465981006 +0000

signed tag

signed tag message body
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQEcBAABAgAGBQJXYRhOAAoJEGEJLoW3InGJklkIAIcnhL7RwEb/+QeX9enkXhxn
rxfdqrvWd1K80sl2TOt8Bg/NYwrUBw/RWJ+sg/hhHp4WtvE1HDGHlkEz3y11Lkuh
8tSxS3qKTxXUGozyPGuE90sJfExhZlW4knIQ1wt/yWqM+33E9pN4hzPqLwyrdods
q8FWEqPPUbSJXoMbRPw04S5jrLtZSsUWbRYjmJCHzlhSfFWW4eFd37uquIaLUBS0
rkC3Jrx7420jkIpgFcTI2s60uhSQLzgcCwdA2ukSYIRnjg/zDkj8+3h/GaROJ72x
lZyI6HWixKJkWw8lE9aAOD9TmTW9sFJwcVAzmAuFX2kUreDUKMZduGcoRYGpD7E=
=jpXa
-----END PGP SIGNATURE-----
```

- with: **git verify-tag [-v]** or **git tag -v**

```
gpg: Signature made Wed Jun 15 10:56:46 2016 CEST using RSA key ID B7227189
gpg: Good signature from "Eris Discordia <discord@example.net>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: D4BE 2231 1AD3 131E 5EDA  29A4 6109 2E85 B722 7189
object 04b871796dc0420f8e7561a895b52484b701d51a
type commit
tag signedtag
tagger C O Mitter <committer@example.com> 1465981006 +0000

signed tag

signed tag message body
```

COMMIT SIGNATURES

- by: **git commit -S**

- commit object

- header entry **gpgsig** (content is preceded by a space)

- commit with subject **signed commit**

```
tree eebfed94e75e7760540d1485c740902590a00332
parent 04b871796dc0420f8e7561a895b52484b701d51a
author A U Thor <author@example.com> 1465981137 +0000
committer C O Mitter <committer@example.com> 1465981137 +0000
gpgsig -----BEGIN PGP SIGNATURE-----
 Version: GnuPG v1
 $
 iQEcBAABAgAGBQJXYRjRAAoJEGEJLoW3InGJ3IwIAIY4SA6GxY3BjL60YyvsJPh/
 HRCJwH+w7wt3Yc/9/bW2F+gF72kdHOOs2jfv+OZhq0q4OAN6fvVSczISY/82LpS7
 DVdMQj2/YcHDT4xrDNBnXnviDO9G7am/9OE77kEbXrp7QPxvhjkicHNwy2rEflAA
 zn075rtEERDHr8nRYiDh8eVrefSO7D+bdQ7gv+7GsYMsd2auJWi1dHOSfTr9HIF4
 HJhWXT9d2f8W+diRYXGh4X0wYiGg6na/soXc+vdtDYBzIxanRqjg8jCAeo1eOTk1
```

EdTwhcTZlI0x5pvJ3H0+4hA2jtldVtmPM4OTB0cTrEWBad7XV6YgiyuII73Ve3
=jKHM
-----END PGP SIGNATURE-----

signed commit

signed commit message body

- with: **git verify-commit [-v]** (or **git show --show-signature**)

gpg: Signature made Wed Jun 15 10:58:57 2016 CEST using RSA key ID B7227189
gpg: Good signature from "Eris Discordia <discord@example.net>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: D4BE 2231 1AD3 131E 5EDA 29A4 6109 2E85 B722 7189
tree eebfed94e75e7760540d1485c740902590a00332
parent 04b871796dc0420f8e7561a895b52484b701d51a
author A U Thor <author@example.com> 1465981137 +0000
committer C O Mitter <committer@example.com> 1465981137 +0000

signed commit

signed commit message body

MERGETAG SIGNATURES

- by: **git merge** on signed tag

- the whole signed tag object is embedded into the (merge) commit object as header entry **mergetag**

- merge of the signed tag **signedtag** as above

tree c7b1cff039a93f3600a1d18b82d26688668c7dea
parent c33429be94b5f2d3ee9b0adad223f877f174b05d

```
parent 04b871796dc0420f8e7561a895b52484b701d51a
author A U Thor <author@example.com> 1465982009 +0000
committer C O Mitter <committer@example.com> 1465982009 +0000
mergetag object 04b871796dc0420f8e7561a895b52484b701d51a
 type commit
 tag signedtag
 tagger C O Mitter <committer@example.com> 1465981006 +0000
 $
 signed tag
 $
 signed tag message body
 -----BEGIN PGP SIGNATURE-----
 Version: GnuPG v1
 $
 iQEcBAABAgAGBQJXYRhOAAoJEGEJLoW3InGJklkIAIcnhL7RwEb/+QeX9e
 rxfdqrvWd1K80sl2TOt8Bg/NYwrUBw/RWJ+sg/hhHp4WtvE1HDGHlkEz3y11L
 8tSxS3qKTxXUGozyPGuE90sJfExhZlW4knIQ1wt/yWqM+33E9pN4hzPqLwyrd
 q8FWEqPPUbSJXoMbRPw04S5jrLtZSsUWbRYjmJCHzlhSfFWW4eFd37uquIaI
 rkC3Jrx7420jkIpgFcTI2s60uhSQLzgcCwdA2ukSYIRnjg/zDkj8+3h/GaROJ72x
 lZyI6HWixKJkWw8lE9aAOD9TmTW9sFJwcVAzmAuFX2kUreDUKMZduGcol
 =jpXa
 -----END PGP SIGNATURE-----

Merge tag 'signedtag' into downstream

signed tag

signed tag message body

# gpg: Signature made Wed Jun 15 08:56:46 2016 UTC using RSA key ID B72271
# gpg: Good signature from "Eris Discordia <discord@example.net>"
# gpg: WARNING: This key is not certified with a trusted signature!
# gpg:          There is no indication that the signature belongs to the owner.
# Primary key fingerprint: D4BE 2231 1AD3 131E 5EDA  29A4 6109 2E85 B722
```

with: verification is embedded in merge commit message by default, alternatively with **git show --show-signature**:

```
commit 9863f0c76ff78712b6800e199a46aa56afbcbd49
merged tag 'signedtag'
gpg: Signature made Wed Jun 15 10:56:46 2016 CEST using RSA key ID B7227189
gpg: Good signature from "Eris Discordia <discord@example.net>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: D4BE 2231 1AD3 131E 5EDA  29A4 6109 2E85 B722 7189
Merge: c33429b 04b8717
Author: A U Thor <author@example.com>
Date:   Wed Jun 15 09:13:29 2016 +0000

    Merge tag 'signedtag' into downstream

    signed tag

    signed tag message body

    # gpg: Signature made Wed Jun 15 08:56:46 2016 UTC using RSA key ID B7227189
    # gpg: Good signature from "Eris Discordia <discord@example.net>"
    # gpg: WARNING: This key is not certified with a trusted signature!
    # gpg:          There is no indication that the signature belongs to the owner.
    # Primary key fingerprint: D4BE 2231 1AD3 131E 5EDA  29A4 6109 2E85 B722 7189
```

GIT

Part of the **git**(1) suite