

**NAME**

gnutls\_privkey\_sign\_data - API function

**SYNOPSIS**

```
#include <gnutls/abstract.h>
```

```
int gnutls_privkey_sign_data(gnutls_privkey_t signer, gnutls_digest_algorithm_t hash, unsigned int flags, const gnutls_datum_t * data, gnutls_datum_t * signature);
```

**ARGUMENTS**

gnutls\_privkey\_t *signer*

Holds the key

gnutls\_digest\_algorithm\_t *hash*

should be a digest algorithm

unsigned int *flags*

Zero or one of **gnutls\_privkey\_flags\_t**

const gnutls\_datum\_t \* *data*

holds the data to be signed

gnutls\_datum\_t \* *signature*

will contain the signature allocated with **gnutls\_malloc()**

**DESCRIPTION**

This function will sign the given data using a signature algorithm supported by the private key. Signature algorithms are always used together with a hash functions. Different hash functions may be used for the RSA algorithm, but only the SHA family for the DSA keys.

You may use **gnutls\_pubkey\_get\_preferred\_hash\_algorithm()** to determine the hash algorithm.

**RETURNS**

On success, **GNUTLS\_E\_SUCCESS** (0) is returned, otherwise a negative error value.

**SINCE**

2.12.0

**REPORTING BUGS**

Report bugs to <bugs@gnutls.org>.

Home page: <https://www.gnutls.org>

## **COPYRIGHT**

Copyright (C) 2001- Free Software Foundation, Inc., and others.

Copying and distribution of this file, with or without modification, are permitted in any medium without royalty provided the copyright notice and this notice are preserved.

## **SEE ALSO**

The full documentation for **gnutls** is maintained as a Texinfo manual. If the `/usr/local/share/doc/gnutls/` directory does not contain the HTML form visit

<https://www.gnutls.org/manual/>