

NAME

gnutls_x509_privkey_sign_hash - API function

SYNOPSIS

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

```
int gnutls_x509_privkey_sign_hash(gnutls_x509_privkey_t key, const gnutls_datum_t * hash,  
gnutls_datum_t * signature);
```

ARGUMENTS

gnutls_x509_privkey_t key
a key

const gnutls_datum_t * hash
holds the data to be signed

gnutls_datum_t * signature
will contain newly allocated signature

DESCRIPTION

This function will sign the given hash using the private key. Do not use this function directly unless you know what it is. Typical signing requires the data to be hashed and stored in special formats (e.g. BER Digest-Info for RSA).

This API is provided only for backwards compatibility, and thus restricted to RSA, DSA and ECDSA key types. For other key types please use **gnutls_privkey_sign_hash()** and **gnutls_privkey_sign_data()**.

RETURNS

On success, **GNUTLS_E_SUCCESS** (0) is returned, otherwise a negative error value.

Deprecated in: 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/>