

NAME

gnutls_x509_cert_privkey_sign - API function

SYNOPSIS

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

```
int gnutls_x509_cert_privkey_sign(gnutls_x509_cert_t crt, gnutls_x509_cert_t issuer, gnutls_privkey_t issuer_key, gnutls_digest_algorithm_t dig, unsigned int flags);
```

ARGUMENTS

gnutls_x509_cert_t crt

a certificate of type **gnutls_x509_cert_t**

gnutls_x509_cert_t issuer

is the certificate of the certificate issuer

gnutls_privkey_t issuer_key

holds the issuer's private key

gnutls_digest_algorithm_t dig

The message digest to use, **GNUTLS_DIG_SHA256** is a safe choice

unsigned int flags

must be 0

DESCRIPTION

This function will sign the certificate with the issuer's private key, and will copy the issuer's information into the certificate.

This must be the last step in a certificate generation since all the previously set parameters are now signed.

A known limitation of this function is, that a newly-signed certificate will not be fully functional (e.g., for signature verification), until it is exported and re-imported.

After GnuTLS 3.6.1 the value of *dig* may be **GNUTLS_DIG_UNKNOWN**, and in that case, a suitable but reasonable for the key algorithm will be selected.

RETURNS

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

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/>