NAME

gnutls_x509_crq_sign2 - API function

SYNOPSIS

#include <gnutls/x509.h>

int gnutls_x509_crq_sign2(gnutls_x509_crq_t *crq***, gnutls_x509_privkey_t** *key***,
gnutls_digest_algorithm_t** *dig***, unsigned int** *flags***);**

ARGUMENTS

gnutls_x509_crq_t crq
            should contain a **gnutls_x509_crq_t** type

gnutls_x509_privkey_t key
            holds a private key

gnutls_digest_algorithm_t dig
            The message digest to use, i.e., **GNUTLS_DIG_SHA256**

unsigned int flags
            must be 0

DESCRIPTION

This function will sign the certificate request with a private key. This must be the same key as the one used in **gnutls_x509_crt_set_key()** since a certificate request is self signed.

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

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

GNUTLS_E_SUCCESS on success, otherwise a negative error code.
GNUTLS_E_ASN1_VALUE_NOT_FOUND is returned if you didn't set all information in the certificate request (e.g., the version using **gnutls_x509_crq_set_version**()).

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/