NAME

gnutls_x509_privkey_sign_data - API function

SYNOPSIS

#include <gnutls/x509.h>

int gnutls_x509_privkey_sign_data(gnutls_x509_privkey_t *key***, gnutls_digest_algorithm_t** *digest***, unsigned int** *flags***, const gnutls_datum_t *** *data***, void *** *signature***, size_t *** *signature_size***);**

ARGUMENTS

gnutls_x509_privkey_t key
: a key

gnutls_digest_algorithm_t digest
: should be a digest algorithm

unsigned int flags
: should be 0 for now

const gnutls_datum_t * data
: holds the data to be signed

void * signature
: will contain the signature

size_t * signature_size
: holds the size of signature (and will be replaced by the new size)

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 SHA-1 for the DSA keys.

If the buffer provided is not long enough to hold the output, then * *signature_size* is updated and **GNUTLS_E_SHORT_MEMORY_BUFFER** will be returned.

Use **gnutls_x509_crt_get_preferred_hash_algorithm()** to determine the hash algorithm.

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

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/