NAME

gnutls_privkey_sign_hash2 - API function

SYNOPSIS

#include <gnutls/abstract.h>

int gnutls_privkey_sign_hash2(gnutls_privkey_t *signer***, gnutls_sign_algorithm_t** *algo***, unsigned int** *flags***, const gnutls_datum_t *** *hash_data***, gnutls_datum_t *** *signature***);**

ARGUMENTS

gnutls_privkey_t signer
: Holds the signer’s key

gnutls_sign_algorithm_t algo
: The signature algorithm used

unsigned int flags
: Zero or one of **gnutls_privkey_flags_t**

const gnutls_datum_t * hash_data
: holds the data to be signed

gnutls_datum_t * signature
: will contain newly allocated signature

DESCRIPTION

This function will sign the given hashed data using the specified signature algorithm. This function is an enhancement of **gnutls_privkey_sign_hash()**, as it allows utilizing a alternative signature algorithm where possible (e.g, use an RSA key with RSA-PSS).

The flags may be **GNUTLS_PRIVKEY_SIGN_FLAG_TLS1_RSA**. In that case this function will ignore *hash_algo* and perform a raw PKCS1 signature. Note that this flag is supported since 3.6.9.

Note also that, not all algorithm support signing already hashed data. When signing with Ed25519, **gnutls_privkey_sign_data2()** should be used instead.

RETURNS

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

SINCE

3.6.0

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/