NAME

gnutls_privkey_sign_hash - API function

SYNOPSIS

#include <gnutls/abstract.h>

int gnutls_privkey_sign_hash(gnutls_privkey_t *signer***, gnutls_digest_algorithm_t** *hash_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_digest_algorithm_t hash_algo
: The hash 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 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-XXX for the DSA keys.

You may use **gnutls_pubkey_get_preferred_hash_algorithm()** to determine the hash algorithm.

The flags may be **GNUTLS_PRIVKEY_SIGN_FLAG_TLS1_RSA** or **GNUTLS_PRIVKEY_SIGN_FLAG_RSA_PSS**. In the former case this function will ignore *hash_algo* and perform a raw PKCS1 signature, and in the latter an RSA-PSS signature will be generated.

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

RETURNS

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

SINCE

2.12.0

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/