NAME

gnutls_x509_privkey_generate - API function

SYNOPSIS

#include <gnutls/x509.h>

int gnutls_x509_privkey_generate(gnutls_x509_privkey_t *key***, gnutls_pk_algorithm_t** *algo***, unsigned int** *bits***, unsigned int** *flags***);**

ARGUMENTS

gnutls_x509_privkey_t key
: an initialized key

gnutls_pk_algorithm_t algo
: is one of the algorithms in **gnutls_pk_algorithm_t**.

unsigned int bits
: the size of the parameters to generate

unsigned int flags
: Must be zero or flags from **gnutls_privkey_flags_t**.

DESCRIPTION

This function will generate a random private key. Note that this function must be called on an initialized private key.

The flag **GNUTLS_PRIVKEY_FLAG_PROVABLE** instructs the key generation process to use algorithms like Shawe-Taylor (from FIPS PUB186-4) which generate provable parameters out of a seed for RSA and DSA keys. See **gnutls_x509_privkey_generate2()** for more information.

Note that when generating an elliptic curve key, the curve can be substituted in the place of the bits parameter using the **GNUTLS_CURVE_TO_BITS()** macro. The input to the macro is any curve from **gnutls_ecc_curve_t**.

For DSA keys, if the subgroup size needs to be specified check the **GNUTLS_SUBGROUP_TO_BITS()** macro.

It is recommended to do not set the number of *bits* directly, use **gnutls_sec_param_to_pk_bits()** instead .

See also **gnutls_privkey_generate()**, **gnutls_x509_privkey_generate2()**.

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/