

NAME

gnutls_x509_privkey_generate2 - API function

SYNOPSIS

```
#include <gnutls/x509.h>
```

```
int gnutls_x509_privkey_generate2(gnutls_x509_privkey_t key, gnutls_pk_algorithm_t algo, unsigned
int bits, unsigned int flags, const gnutls_keygen_data_st * data, unsigned data_size);
```

ARGUMENTS

gnutls_x509_privkey_t key
a key

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

unsigned int bits
the size of the modulus

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

const gnutls_keygen_data_st * data
Allow specifying **gnutls_keygen_data_st** types such as the seed to be used.

unsigned data_size
The number of *data* available.

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. On DSA keys the PQG parameters are generated using the seed, while on RSA the two primes. To specify an explicit seed (by default a random seed is used), use the *data* with a **GNUTLS_KEYGEN_SEED** type.

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.

To export the generated keys in memory or in files it is recommended to use the PKCS8 form as it can handle all key types, and can store additional parameters such as the seed, in case of provable RSA or DSA keys. Generated keys can be exported in memory using **gnutls_privkey_export_x509()**, and then with **gnutls_x509_privkey_export2_pkcs8()**.

If key generation is part of your application, avoid setting the number of bits directly, and instead use **gnutls_sec_param_to_pk_bits()**. That way the generated keys will adapt to the security levels of the underlying GnuTLS library.

See also **gnutls_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

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/>