NAME

gnutls_dh_params_generate2 - API function

SYNOPSIS

#include <gnutls/gnutls.h>

int gnutls_dh_params_generate2(gnutls_dh_params_t *dparams***, unsigned int** *bits***);**

ARGUMENTS

gnutls_dh_params_t dparams
The parameters

unsigned int bits
is the prime's number of bits

DESCRIPTION

This function will generate a new pair of prime and generator for use in the Diffie-Hellman key exchange. This may take long time.

It is recommended not to set the number of bits directly, but use **gnutls_sec_param_to_pk_bits()** instead. Also note that the DH parameters are only useful to servers. Since clients use the parameters sent by the server, it's of no use to call this in client side.

The parameters generated are of the DSA form. It also is possible to generate provable parameters (following the Shawe-Taylor algorithm), using **gnutls_x509_privkey_generate2()** with DSA option and the **GNUTLS_PRIVKEY_FLAG_PROVABLE** flag set. These can the be imported with **gnutls_dh_params_import_dsa()**.

It is no longer recommended for applications to generate parameters. See the "Parameter generation" section in the manual.

RETURNS

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

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/