

NAME

gnutls_dh_get_group - API function

SYNOPSIS

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

```
int gnutls_dh_get_group(gnutls_session_t session, gnutls_datum_t * raw_gen, gnutls_datum_t * raw_prime);
```

ARGUMENTS

gnutls_session_t session
is a gnutls session

gnutls_datum_t * raw_gen
will hold the generator.

gnutls_datum_t * raw_prime
will hold the prime.

DESCRIPTION

This function will return the group parameters used in the last Diffie-Hellman key exchange with the peer. These are the prime and the generator used. This function should be used for both anonymous and ephemeral Diffie-Hellman. The output parameters must be freed with **gnutls_free()**.

Note, that the prime and generator are exported as non-negative integers and may include a leading zero byte.

RETURNS

On success, **GNUTLS_E_SUCCESS** (0) is returned, otherwise an 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/>