NAME

gnutls_dh_set_prime_bits - API function

SYNOPSIS

#include <gnutls/gnutls.h>

void gnutls_dh_set_prime_bits(gnutls_session_t *session***, unsigned int** *bits***);**

ARGUMENTS

gnutls_session_t session

is a **gnutls_session_t** type.

unsigned int bits

is the number of bits

DESCRIPTION

This function sets the number of bits, for use in a Diffie-Hellman key exchange. This is used both in DH ephemeral and DH anonymous cipher suites. This will set the minimum size of the prime that will be used for the handshake.

In the client side it sets the minimum accepted number of bits. If a server sends a prime with less bits than that **GNUTLS_E_DH_PRIME_UNACCEPTABLE** will be returned by the handshake.

Note that this function will warn via the audit log for value that are believed to be weak.

The function has no effect in server side.

Note that since 3.1.7 this function is deprecated. The minimum number of bits is set by the priority string level. Also this function must be called after **gnutls_priority_set_direct()** or the set value may be overridden by the selected priority options.

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/