NAME

gnutls_prf - API function

SYNOPSIS

#include <gnutls/gnutls.h>

int gnutls_prf(gnutls_session_t *session***, size_t** *label_size***, const char *** *label***, int** *server_random_first***, size_t** *extra_size***, const char *** *extra***, size_t** *outsize***, char *** *out***);**

ARGUMENTS

gnutls_session_t session
: is a **gnutls_session_t** type.

size_t label_size
: length of the *label* variable.

const char * label
: label used in PRF computation, typically a short string.

int server_random_first
: non-zero if server random field should be first in seed

size_t extra_size
: length of the *extra* variable.

const char * extra
: optional extra data to seed the PRF with.

size_t outsize
: size of pre-allocated output buffer to hold the output.

char * out
: pre-allocated buffer to hold the generated data.

DESCRIPTION

Applies the TLS Pseudo-Random-Function (PRF) on the master secret and the provided data, seeded with the client and server random fields. For the key expansion specified in RFC5705 see **gnutls_prf_rfc5705()**.

The *label* variable usually contains a string denoting the purpose for the generated data. The *server_random_first* indicates whether the client random field or the server random field should be first in the seed. Non-zero indicates that the server random field is first, 0 that the client random field is

first.

The *extra* variable can be used to add more data to the seed, after the random variables. It can be used to make sure the generated output is strongly connected to some additional data (e.g., a string used in user authentication).

The output is placed in *out* , which must be pre-allocated.

NOTE

This function produces identical output with **gnutls_prf_rfc5705()** when *server_random_first* is set to 0 and *extra* is **NULL**. Under TLS1.3 this function will only operate when these conditions are true, or otherwise return **GNUTLS_E_INVALID_REQUEST**.

RETURNS

GNUTLS_E_SUCCESS on success, or an error code.

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/