NAME

gnutls_prf_raw - API function

SYNOPSIS

#include <gnutls/gnutls.h>

int gnutls_prf_raw(gnutls_session_t *session***, size_t** *label_size***, const char *** *label***, size_t** *seed_size***, const char *** *seed***, 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.

size_t seed_size
: length of the *seed* variable.

const char * seed
: 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

Apply the TLS Pseudo-Random-Function (PRF) on the master secret and the provided data.

The *label* variable usually contains a string denoting the purpose for the generated data. The *seed* usually contains data such as the client and server random, perhaps together with some additional data that is added to guarantee uniqueness of the output for a particular purpose.

Because the output is not guaranteed to be unique for a particular session unless *seed* includes the client random and server random fields (the PRF would output the same data on another connection resumed from the first one), it is not recommended to use this function directly. The **gnutls_prf()** function seeds the PRF with the client and server random fields directly, and is recommended if you

want to generate pseudo random data unique for each session.

NOTE

This function will only operate under TLS versions prior to 1.3. In TLS1.3 the use of PRF is replaced with HKDF and the generic exporters like **gnutls_prf_rfc5705()** should be used instead. Under TLS1.3 this function returns **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/