

**NAME**

gnutls\_prf\_rfc5705 - API function

**SYNOPSIS**

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

```
int gnutls_prf_rfc5705(gnutls_session_t session, size_t label_size, const char * label, size_t context_size, const char * context, 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 context\_size

length of the *extra* variable.

const char \* context

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**

Exports keying material from TLS/DTLS session to an application, as specified in RFC5705.

In the TLS versions prior to 1.3, it applies the TLS Pseudo-Random-Function (PRF) on the master secret and the provided data, seeded with the client and server random fields.

In TLS 1.3, it applies HKDF on the exporter master secret derived from the master secret.

The *label* variable usually contains a string denoting the purpose for the generated data.

The *context* 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 that, to provide the RFC5705 context, the *context* variable must be non-null.

## RETURNS

**GNUTLS\_E\_SUCCESS** on success, or an error code.

## SINCE

3.4.4

## 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/>