

NAME

gnutls_prf_early - API function

SYNOPSIS

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

```
int gnutls_prf_early(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

This function is similar to **gnutls_prf_rfc5705()**, but only works in TLS 1.3 or later to export early keying material.

Note that the keying material is only available after the ClientHello message is processed and before the application traffic keys are established. Therefore this function shall be called in a handshake hook function for **GNUTLS_HANDSHAKE_CLIENT_HELLO**.

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

3.6.8

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/>