NAME

gnutls_session_get_data2 - API function

SYNOPSIS

#include <gnutls/gnutls.h>

int gnutls_session_get_data2(gnutls_session_t *session***, gnutls_datum_t *** *data***);**

ARGUMENTS

gnutls_session_t session

is a **gnutls_session_t** type.

gnutls_datum_t * data

is a pointer to a datum that will hold the session.

DESCRIPTION

Returns necessary parameters to support resumption. The client should call this function and store the returned session data. A session can be resumed later by calling **gnutls_session_set_data()** with the returned data. Note that under TLS 1.3, it is recommended for clients to use session parameters only once, to prevent passive-observers from correlating the different connections.

The returned *data* are allocated and must be released using **gnutls_free**().

This function will fail if called prior to handshake completion. In case of false start TLS, the handshake completes only after data have been successfully received from the peer.

Under TLS1.3 session resumption is possible only after a session ticket is received by the client. To ensure that such a ticket has been received use **gnutls_session_get_flags()** and check for flag **GNUTLS_SFLAGS_SESSION_TICKET**; if this flag is not set, this function will wait for a new ticket within an estimated roundtrip, and if not received will return dummy data which cannot lead to resumption.

To get notified when new tickets are received by the server use **gnutls_handshake_set_hook_function()** to wait for **GNUTLS_HANDSHAKE_NEW_SESSION_TICKET** messages. Each call of **gnutls_session_get_data2()** after a ticket is received, will return session resumption data corresponding to the last received ticket.

Note that this function under TLS1.3 requires a callback to be set with **gnutls_transport_set_pull_timeout_function()** for successful operation. There was a bug before 3.6.10 which could make this function fail if that callback was not set. On later versions if not set, the function

will return a successful error code, but will return dummy data that cannot lead to a resumption.

RETURNS

On success, **GNUTLS_E_SUCCESS** (0) is returned, otherwise an error code is returned.

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/