

**NAME**

gnutls\_handshake - API function

**SYNOPSIS**

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

```
int gnutls_handshake(gnutls_session_t session);
```

**ARGUMENTS**

gnutls\_session\_t session

is a **gnutls\_session\_t** type.

**DESCRIPTION**

This function performs the handshake of the TLS/SSL protocol, and initializes the TLS session parameters.

The non-fatal errors expected by this function are: **GNUTLS\_E\_INTERRUPTED**, **GNUTLS\_E\_AGAIN**, **GNUTLS\_E\_WARNING\_ALERT\_RECEIVED**. When this function is called for re-handshake under TLS 1.2 or earlier, the non-fatal error code **GNUTLS\_E\_GOT\_APPLICATION\_DATA** may also be returned.

The former two interrupt the handshake procedure due to the transport layer being interrupted, and the latter because of a "warning" alert that was sent by the peer (it is always a good idea to check any received alerts). On these non-fatal errors call this function again, until it returns 0; cf.

**gnutls\_record\_get\_direction()** and **gnutls\_error\_is\_fatal()**. In DTLS sessions the non-fatal error **GNUTLS\_E\_LARGE\_PACKET** is also possible, and indicates that the MTU should be adjusted.

When this function is called by a server after a rehandshake request under TLS 1.2 or earlier the **GNUTLS\_E\_GOT\_APPLICATION\_DATA** error code indicates that some data were pending prior to peer initiating the handshake. Under TLS 1.3 this function when called after a successful handshake, is a no-op and always succeeds in server side; in client side this function is equivalent to **gnutls\_session\_key\_update()** with **GNUTLS\_KU\_PEER** flag.

This function handles both full and abbreviated TLS handshakes (resumption). For abbreviated handshakes, in client side, the **gnutls\_session\_set\_data()** should be called prior to this function to set parameters from a previous session. In server side, resumption is handled by either setting a DB back-end, or setting up keys for session tickets.

**RETURNS**

**GNUTLS\_E\_SUCCESS** on a successful handshake, otherwise a negative error code.

**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/>