

**NAME**

gnutls\_session\_key\_update - API function

**SYNOPSIS**

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

```
int gnutls_session_key_update(gnutls_session_t session, unsigned flags);
```

**ARGUMENTS**

gnutls\_session\_t session

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

unsigned flags

zero of **GNUTLS\_KU\_PEER**

**DESCRIPTION**

This function will update/refresh the session keys when the TLS protocol is 1.3 or better. The peer is notified of the update by sending a message, so this function should be treated similarly to **gnutls\_record\_send()** --i.e., it may return **GNUTLS\_E\_AGAIN** or **GNUTLS\_E\_INTERRUPTED**.

When this flag **GNUTLS\_KU\_PEER** is specified, this function in addition to updating the local keys, will ask the peer to refresh its keys too.

If the negotiated version is not TLS 1.3 or better this function will return **GNUTLS\_E\_INVALID\_REQUEST**.

**RETURNS**

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

**SINCE**

3.6.3

**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/>