NAME

gnutls_hkdf_expand - API function

SYNOPSIS

#include <gnutls/crypto.h>

int gnutls_hkdf_expand(gnutls_mac_algorithm_t *mac***, const gnutls_datum_t *** *key***, const gnutls_datum_t *** *info***, void *** *output***, size_t** *length***);**

ARGUMENTS

gnutls_mac_algorithm_t mac
: the mac algorithm used internally

const gnutls_datum_t * key
: the pseudorandom key created with HKDF-Extract

const gnutls_datum_t * info
: the optional informational data

void * output
: the output value of the expand operation

size_t length
: the desired length of the output key

DESCRIPTION

This function will derive a variable length keying material from the pseudorandom key using the HKDF-Expand function as defined in RFC 5869.

RETURNS

Zero or a negative error code on error.

SINCE

3.6.13

REPORTING BUGS

Report bugs to <bugs@gnutls.org>.
Home page: https://www.gnutls.org

COPYRIGHT

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/