NAME

gnutls_hkdf_extract - API function

SYNOPSIS

#include <gnutls/crypto.h>

int gnutls_hkdf_extract(gnutls_mac_algorithm_t *mac***, const gnutls_datum_t *** *key***, const gnutls_datum_t *** *salt***, void *** *output***);**

ARGUMENTS

gnutls_mac_algorithm_t mac
: the mac algorithm used internally

const gnutls_datum_t * key
: the initial keying material

const gnutls_datum_t * salt
: the optional salt

void * output
: the output value of the extract operation

DESCRIPTION

This function will derive a fixed-size key using the HKDF-Extract 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/