

NAME

gnutls_pbkdf2 - API function

SYNOPSIS

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

```
int gnutls_pbkdf2(gnutls_mac_algorithm_t mac, const gnutls_datum_t * key, const gnutls_datum_t * salt, unsigned iter_count, void * output, size_t length);
```

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 salt

unsigned iter_count

the iteration count

void * output the output value

size_t length the desired length of the output key

DESCRIPTION

This function will derive a variable length keying material from a password according to PKCS 5 PBKDF2.

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

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/>