NAME

gnutls_pkcs12_mac_info - API function

SYNOPSIS

#include <gnutls/pkcs12.h>

int gnutls_pkcs12_mac_info(gnutls_pkcs12_t *pkcs12***, unsigned int *** *mac***, void *** *salt***, unsigned int *** *salt_size***, unsigned int *** *iter_count***, char **** *oid***);**

ARGUMENTS

gnutls_pkcs12_t pkcs12
> A pkcs12 type

unsigned int * mac
> the MAC algorithm used as **gnutls_mac_algorithm_t**

void * salt   the salt used for string to key (if non-NULL then *salt_size* initially holds its size)

unsigned int * salt_size
> string to key salt size

unsigned int * iter_count
> string to key iteration count

char ** oid   if non-NULL it will contain an allocated null-terminated variable with the OID

DESCRIPTION

This function will provide information on the MAC algorithm used in a PKCS **12** structure. If the structure algorithms are unknown the code **GNUTLS_E_UNKNOWN_HASH_ALGORITHM** will be returned, and only *oid* , will be set. That is, *oid* will be set on structures with a MAC whether supported or not. It must be deinitialized using **gnutls_free**(). The other variables are only set on supported structures.

RETURNS

GNUTLS_E_INVALID_REQUEST if the provided structure doesn't contain a MAC, **GNUTLS_E_UNKNOWN_HASH_ALGORITHM** if the structure's MAC isn't supported, or another negative error code in case of a failure. Zero on success.

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/