NAME

gnutls_pkcs12_bag_enc_info - API function

SYNOPSIS

#include <gnutls/pkcs12.h>

int gnutls_pkcs12_bag_enc_info(gnutls_pkcs12_bag_t *bag*, **unsigned int *** *schema*, **unsigned int *** *cipher*, **void *** *salt*, **unsigned int *** *salt_size*, **unsigned int *** *iter_count*, **char **** *oid*);

ARGUMENTS

gnutls_pkcs12_bag_t bag

> The bag

unsigned int * schema

> indicate the schema as one of **gnutls_pkcs_encrypt_flags_t**

unsigned int * cipher

> the cipher used as **gnutls_cipher_algorithm_t**

void * salt   PBKDF2 salt (if non-NULL then *salt_size* initially holds its size)

unsigned int * salt_size

> PBKDF2 salt size

unsigned int * iter_count

> PBKDF2 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 encryption algorithms used in an encrypted bag. If the structure algorithms are unknown the code **GNUTLS_E_UNKNOWN_CIPHER_TYPE** will be returned, and only *oid* , will be set. That is, *oid* will be set on encrypted bags 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 bag isn't encrypted, **GNUTLS_E_UNKNOWN_CIPHER_TYPE** if the structure's encryption 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

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/