

NAME

gnutls_pkcs8_info - API function

SYNOPSIS

```
#include <gnutls/x509.h>
```

```
int gnutls_pkcs8_info(const gnutls_datum_t * data, gnutls_x509_cert_fmt_t format, unsigned int *
schema, unsigned int * cipher, void * salt, unsigned int * salt_size, unsigned int * iter_count, char **
oid);
```

ARGUMENTS

const gnutls_datum_t * data

Holds the PKCS 8 data

gnutls_x509_cert_fmt_t format

the format of the PKCS 8 data

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 algorithms used in a particular PKCS 8 structure. 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 PKCS 8 structures 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 isn't an encrypted key,
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.

SINCE

3.4.0

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/>