

NAME

gnutls_x509_privkey_export2_pkcs8 - API function

SYNOPSIS

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

```
int gnutls_x509_privkey_export2_pkcs8(gnutls_x509_privkey_t key, gnutls_x509_cert_fmt_t format,  
const char * password, unsigned int flags, gnutls_datum_t * out);
```

ARGUMENTS

gnutls_x509_privkey_t key

Holds the key

gnutls_x509_cert_fmt_t format

the format of output params. One of PEM or DER.

const char * password

the password that will be used to encrypt the key.

unsigned int flags

an ORed sequence of gnutls_pkcs_encrypt_flags_t

gnutls_datum_t * out

will contain a private key PEM or DER encoded

DESCRIPTION

This function will export the private key to a PKCS8 structure. Both RSA and DSA keys can be exported. For DSA keys we use PKCS **11** definitions. If the flags do not specify the encryption cipher, then the default 3DES (PBES2) will be used.

The *password* can be either ASCII or UTF-8 in the default PBES2 encryption schemas, or ASCII for the PKCS12 schemas.

The output buffer is allocated using **gnutls_malloc()**.

If the structure is PEM encoded, it will have a header of "BEGIN ENCRYPTED PRIVATE KEY" or "BEGIN PRIVATE KEY" if encryption is not used.

RETURNS

In case of failure a negative error code will be returned, and 0 on success.

Since 3.1.3

REPORTING BUGS

Report bugs to <bugs@gnutls.org>.

Home page: <https://www.gnutls.org>

COPYRIGHT

Copyright (C) 2001-2023 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/>