NAME

gnutls_x509_privkey_import_pkcs8 - API function

SYNOPSIS

#include <gnutls/x509.h>

int gnutls_x509_privkey_import_pkcs8(gnutls_x509_privkey_t *key***, const gnutls_datum_t *** *data***, gnutls_x509_crt_fmt_t** *format***, const char *** *password***, unsigned int** *flags***);**

ARGUMENTS

gnutls_x509_privkey_t key
: The data to store the parsed key

const gnutls_datum_t * data
: The DER or PEM encoded key.

gnutls_x509_crt_fmt_t format
: One of DER or PEM

const char * password
: the password to decrypt the key (if it is encrypted).

unsigned int flags
: 0 if encrypted or GNUTLS_PKCS_PLAIN if not encrypted.

DESCRIPTION

This function will convert the given DER or PEM encoded PKCS8 2.0 encrypted key to the native gnutls_x509_privkey_t format. The output will be stored in *key* . Both RSA and DSA keys can be imported, and flags can only be used to indicate an unencrypted key.

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

If the Certificate is PEM encoded it should have a header of "ENCRYPTED PRIVATE KEY", or "PRIVATE KEY". You only need to specify the flags if the key is DER encoded, since in that case the encryption status cannot be auto-detected.

If the **GNUTLS_PKCS_PLAIN** flag is specified and the supplied data are encrypted then **GNUTLS_E_DECRYPTION_FAILED** is returned.

RETURNS

On success, **GNUTLS_E_SUCCESS** (0) is returned, otherwise a negative error value.

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/