NAME

gnutls_pkcs11_privkey_generate2 - API function

SYNOPSIS

#include <gnutls/pkcs11.h>

int gnutls_pkcs11_privkey_generate2(const char * *url***, gnutls_pk_algorithm_t** *pk***, unsigned int** *bits***, const char *** *label***, gnutls_x509_crt_fmt_t** *fmt***, gnutls_datum_t *** *pubkey***, unsigned int** *flags***);**

ARGUMENTS

const char * url
: a token URL

gnutls_pk_algorithm_t pk
: the public key algorithm

unsigned int bits
: the security bits

const char * label
: a label

gnutls_x509_crt_fmt_t fmt
: the format of output params. PEM or DER

gnutls_datum_t * pubkey
: will hold the public key (may be **NULL**)

unsigned int flags
: zero or an OR'ed sequence of **GNUTLS_PKCS11_OBJ_FLAGs**

DESCRIPTION

This function will generate a private key in the specified by the *url* token. The private key will be generate within the token and will not be exportable. This function will store the DER-encoded public key in the SubjectPublicKeyInfo format in *pubkey* . The *pubkey* should be deinitialized using **gnutls_free()**.

Note that when generating an elliptic curve key, the curve can be substituted in the place of the bits parameter using the **GNUTLS_CURVE_TO_BITS()** macro.

RETURNS

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

SINCE

3.1.5

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/