

NAME

gnutls_pkcs11_privkey_generate3 - API function

SYNOPSIS

```
#include <gnutls/pkcs11.h>
```

```
int gnutls_pkcs11_privkey_generate3(const char * url, gnutls_pk_algorithm_t pk, unsigned int bits,
const char * label, const gnutls_datum_t * cid, gnutls_x509_cert_fmt_t fmt, gnutls_datum_t * pubkey,
unsigned int key_usage, 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

const gnutls_datum_t * cid

The CKA_ID to use for the new object

gnutls_x509_cert_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 key_usage

One of **GNUTLS_KEY_***

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.

Since 3.6.3 the objects are marked as sensitive by default unless **GNUTLS_PKCS11_OBJ_FLAG_MARK_NOT_SENSITIVE** is specified.

RETURNS

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

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/>