NAME

gnutls_tpm_privkey_generate - API function

SYNOPSIS

#include <gnutls/tpm.h>

int gnutls_tpm_privkey_generate(gnutls_pk_algorithm_t *pk***, unsigned int** *bits***, const char *** *srk_password***, const char *** *key_password***, gnutls_tpmkey_fmt_t** *format***, gnutls_x509_crt_fmt_t** *pub_format***, gnutls_datum_t *** *privkey***, gnutls_datum_t *** *pubkey***, unsigned int** *flags***);**

ARGUMENTS

gnutls_pk_algorithm_t pk
: the public key algorithm

unsigned int bits
: the security bits

const char * srk_password
: a password to protect the exported key (optional)

const char * key_password
: the password for the TPM (optional)

gnutls_tpmkey_fmt_t format
: the format of the private key

gnutls_x509_crt_fmt_t pub_format
: the format of the public key

gnutls_datum_t * privkey
: the generated key

gnutls_datum_t * pubkey
: the corresponding public key (may be null)

unsigned int flags
: should be a list of GNUTLS_TPM_* flags

DESCRIPTION

This function will generate a private key in the TPM chip. The private key will be generated within the

chip and will be exported in a wrapped with TPM's master key form. Furthermore the wrapped key can be protected with the provided *password* .

Note that bits in TPM is quantized value. If the input value is not one of the allowed values, then it will be quantized to one of 512, 1024, 2048, 4096, 8192 and 16384.

Allowed flags are:

RETURNS

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

SINCE

3.1.0

REPORTING BUGS

Report bugs to <bugs@gnutls.org>.
Home page: https://www.gnutls.org

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/