NAME

gnutls_privkey_import_ext4 - API function

SYNOPSIS

#include <gnutls/abstract.h>

int gnutls_privkey_import_ext4(gnutls_privkey_t *pkey***, void *** *userdata***,**
gnutls_privkey_sign_data_func *sign_data_fn***, gnutls_privkey_sign_hash_func** *sign_hash_fn***,**
gnutls_privkey_decrypt_func *decrypt_fn***, gnutls_privkey_deinit_func** *deinit_fn***,**
gnutls_privkey_info_func *info_fn***, unsigned int** *flags***);**

ARGUMENTS

gnutls_privkey_t pkey
: The private key

void * userdata
: private data to be provided to the callbacks

gnutls_privkey_sign_data_func sign_data_fn
: callback for signature operations (may be **NULL**)

gnutls_privkey_sign_hash_func sign_hash_fn
: callback for signature operations (may be **NULL**)

gnutls_privkey_decrypt_func decrypt_fn
: callback for decryption operations (may be **NULL**)

gnutls_privkey_deinit_func deinit_fn
: a deinitialization function

gnutls_privkey_info_func info_fn
: returns info about the public key algorithm (should not be **NULL**)

unsigned int flags
: Flags for the import

DESCRIPTION

This function will associate the given callbacks with the **gnutls_privkey_t** type. At least one of the callbacks must be non-null. If a deinitialization function is provided then flags is assumed to contain **GNUTLS_PRIVKEY_IMPORT_AUTO_RELEASE**.

Note that in contrast with the signing function of **gnutls_privkey_import_ext3()**, the signing functions provided to this function take explicitly the signature algorithm as parameter and different functions are provided to sign the data and hashes.

The *sign_hash_fn* is to be called to sign pre-hashed data. The input to the callback is the output of the hash (such as SHA256) corresponding to the signature algorithm. For RSA PKCS**1** signatures, the signature algorithm can be set to **GNUTLS_SIGN_RSA_RAW**, and in that case the data should be handled as if they were an RSA PKCS**1** DigestInfo structure.

The *sign_data_fn* is to be called to sign data. The input data will be he data to be signed (and hashed), with the provided signature algorithm. This function is to be used for signature algorithms like Ed25519 which cannot take pre-hashed data as input.

When both *sign_data_fn* and *sign_hash_fn* functions are provided they must be able to operate on all the supported signature algorithms, unless prohibited by the type of the algorithm (e.g., as with Ed25519).

The *info_fn* must provide information on the signature algorithms supported by this private key, and should support the flags **GNUTLS_PRIVKEY_INFO_PK_ALGO**, **GNUTLS_PRIVKEY_INFO_HAVE_SIGN_ALGO** and **GNUTLS_PRIVKEY_INFO_PK_ALGO_BITS**. It must return -1 on unknown flags.

RETURNS

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

SINCE

3.6.0

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/