

NAME

gnutls_privkey_import_ext - API function

SYNOPSIS

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

```
int gnutls_privkey_import_ext(gnutls_privkey_t pkey, gnutls_pk_algorithm_t pk, void * userdata,  
gnutls_privkey_sign_func sign_func, gnutls_privkey_decrypt_func decrypt_func, unsigned int flags);
```

ARGUMENTS

gnutls_privkey_t pkey

The private key

gnutls_pk_algorithm_t pk

The public key algorithm

void * userdata

private data to be provided to the callbacks

gnutls_privkey_sign_func sign_func

callback for signature operations

gnutls_privkey_decrypt_func decrypt_func

callback for decryption operations

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 two callbacks must be non-null.

Note that the signing function is supposed to "raw" sign data, i.e., without any hashing or preprocessing. In case of RSA the DigestInfo will be provided, and the signing function is expected to do the PKCS 1 1.5 padding and the exponentiation.

See also **gnutls_privkey_import_ext3()**.

RETURNS

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

SINCE

3.0

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/>