

NAME

gnutls_pubkey_import_gost_raw - API function

SYNOPSIS

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

```
int gnutls_pubkey_import_gost_raw(gnutls_pubkey_t key, gnutls_ecc_curve_t curve,  
gnutls_digest_algorithm_t digest, gnutls_gost_paramset_t paramset, const gnutls_datum_t * x, const  
gnutls_datum_t * y);
```

ARGUMENTS

gnutls_pubkey_t key

The structure to store the parsed key

gnutls_ecc_curve_t curve

holds the curve

gnutls_digest_algorithm_t digest

holds the digest

gnutls_gost_paramset_t paramset

holds the parameters id

const gnutls_datum_t * x

holds the x-coordinate

const gnutls_datum_t * y

holds the y-coordinate

DESCRIPTION

This function will convert the given GOST public key's parameters to a **gnutls_pubkey_t**. The output will be stored in *key*. *digest* should be one of GNUTLS_DIG_GOSR_94, GNUTLS_DIG_STREEBOG_256 or GNUTLS_DIG_STREEBOG_512. If *paramset* is set to GNUTLS_GOST_PARAMSET_UNKNOWN default one will be selected depending on *digest*.

NOTE

parameters should be stored with least significant byte first. On version 3.6.3 big-endian format was used incorrectly.

RETURNS

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

SINCE

3.6.3

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/>