

gnutls_x509_privkey_export_rsa_raw2(3) gnutls gnutls_x509_privkey_export_rsa_raw2(3)

NAME

gnutls_x509_privkey_export_rsa_raw2 - API function

SYNOPSIS

```
#include <gnutls/x509.h>
```

```
int gnutls_x509_privkey_export_rsa_raw2(gnutls_x509_privkey_t key, gnutls_datum_t * m,  
gnutls_datum_t * e, gnutls_datum_t * d, gnutls_datum_t * p, gnutls_datum_t * q, gnutls_datum_t * u,  
gnutls_datum_t * e1, gnutls_datum_t * e2);
```

ARGUMENTS

gnutls_x509_privkey_t key
a key

gnutls_datum_t * m
will hold the modulus

gnutls_datum_t * e
will hold the public exponent

gnutls_datum_t * d
will hold the private exponent

gnutls_datum_t * p
will hold the first prime (p)

gnutls_datum_t * q
will hold the second prime (q)

gnutls_datum_t * u
will hold the coefficient

gnutls_datum_t * e1
will hold $e1 = d \bmod (p-1)$

gnutls_datum_t * e2
will hold $e2 = d \bmod (q-1)$

DESCRIPTION

This function will export the RSA private key's parameters found in the given structure. The new

parameters will be allocated using **gnutls_malloc()** and will be stored in the appropriate datum.

RETURNS

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

SINCE

2.12.0

REPORTING BUGS

Report bugs to <bugs@gnutls.org>.

Home page: <https://www.gnutls.org>

COPYRIGHT

Copyright (C) 2001-2023 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/>