

NAME

gnutls_decode_rs_value - API function

SYNOPSIS

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

```
int gnutls_decode_rs_value(const gnutls_datum_t * sig_value, gnutls_datum_t * r, gnutls_datum_t * s);
```

ARGUMENTS

const gnutls_datum_t * sig_value

holds a Dss-Sig-Value DER or BER encoded structure

gnutls_datum_t * r

will contain the r value

gnutls_datum_t * s

will contain the s value

DESCRIPTION

This function will decode the provided *sig_value* , into *r* and *s* elements. The Dss-Sig-Value is used for DSA and ECDSA signatures.

The output values may be padded with a zero byte to prevent them from being interpreted as negative values. The value should be deallocated using **gnutls_free()**.

RETURNS

On success, **GNUTLS_E_SUCCESS** (0) is returned, otherwise an error code is returned.

SINCE

3.6.0

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/>