NAME

gnutls_decode_ber_digest_info - API function

SYNOPSIS

#include <gnutls/crypto.h>

int gnutls_decode_ber_digest_info(const gnutls_datum_t * *info***, gnutls_digest_algorithm_t *** *hash***, unsigned char *** *digest***, unsigned int *** *digest_size***);**

ARGUMENTS

const gnutls_datum_t * info

an RSA BER encoded DigestInfo structure

gnutls_digest_algorithm_t * hash

will contain the hash algorithm of the structure

unsigned char * digest

will contain the hash output of the structure

unsigned int * digest_size

will contain the hash size of the structure; initially must hold the maximum size of *digest*

DESCRIPTION

This function will parse an RSA PKCS**1** 1.5 DigestInfo structure and report the hash algorithm used as well as the digest data.

RETURNS

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

SINCE

3.5.0

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/