NAME

gnutls_aead_cipher_decrypt - API function

SYNOPSIS

#include <gnutls/crypto.h>

int gnutls_aead_cipher_decrypt(gnutls_aead_cipher_hd_t *handle***, const void *** *nonce***, size_t** *nonce_len***, const void *** *auth***, size_t** *auth_len***, size_t** *tag_size***, const void *** *ctext***, size_t** *ctext_len***, void *** *ptext***, size_t *** *ptext_len***);**

ARGUMENTS

gnutls_aead_cipher_hd_t handle
: is a **gnutls_aead_cipher_hd_t** type.

const void * nonce
: the nonce to set

size_t nonce_len
: The length of the nonce

const void * auth
: additional data to be authenticated

size_t auth_len
: The length of the data

size_t tag_size
: The size of the tag to use (use zero for the default)

const void * ctext
: the data to decrypt (including the authentication tag)

size_t ctext_len
: the length of data to decrypt (includes tag size)

void * ptext the decrypted data

size_t * ptext_len
: the length of decrypted data (initially must hold the maximum available size)

DESCRIPTION

This function will decrypt the given data using the algorithm specified by the context. This function must be provided the complete data to be decrypted, including the authentication tag. On several AEAD ciphers, the authentication tag is appended to the ciphertext, though this is not a general rule. This function will fail if the tag verification fails.

RETURNS

Zero or a negative error code on verification failure or other error.

SINCE

3.4.0

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/