TPDECRYPT(3)

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

SYNOPSIS

#include <atmi.h>

int tpdecrypt(char *_input_, long _ilen_, char *_output_, long *_olen_, long _flags_);

For XATMI client link with _-latmiclt -latmi -lubf -lnstd -lpthread -lrt -lm_

For XATMI server link with _-latmisrv|-latmisrvnomain|-latmisrvinteg -latmi -lubf -lnstd -lpthread -lrt -lm_

Chapter 2

DESCRIPTION

Data decrypt function. Function provides access to Enduro/X built-in encryption engine. AES-128 in CBC mode algorithm is used. By default encryption key is composed from current hostname and username, but key could be retrieved from other resources by plugin interface, if configured.

input buffer contains encrypted data with corresponding data length in *ilen* (number of bytes). *output* buffer is used for clear data with corresponding data length in *olen* (number of bytes in/out).

Function may work in binary mode (the input data and output data is binary). The other mode is string mode with flag **TPEX_STRING**, where *input* is expected to be Base64 encoded data and *output* is 0x00 terminated string.

In string mode *ilen* is ignored, in binary mode *ilen* is required and must be >*0*. *olen* is used for checking output buffer sizes. In case if there is no space, the error **TPELIMIT** is returned, and *olen* variable is set to estimated space required.

In the result of function *olen* is set to number bytes written to *output* buffer.

Valid flags

TPEX_STRING In this mode expected input is EOS terminated string. On success output will contain Base64 encoded binary data.

Chapter 3

RETURN VALUE

On success, **tpencrypt()** return zero; on error, -1 is returned, with **tperrno** set to indicate the error.

Chapter 4

ERRORS

Note that **tpstrerror()** returns generic error message plus custom message with debug info from last function call.

TPEINVAL Invalid arguments to function. *input*, *ilen*, *output* or *olen* is **NULL**. For non string mode *ilen* is ⇐ **0**. Additionally in **TPEX_STRING** mode this error is if *input* data does not correspond to Base64 format or if decrypted data length does not match the string length (i.e. string is shorter - includes binary 0x00).

TPELIMIT There is not enough space in *output* buffer. Estimate is returned in *olen*.

TPEOS Operating system error occurred. E.g. cannot allocate temporary buffers.

Chapter 5

EXAMPLE

See **atmitest/test043_encrypt/atmiclt43_tp.c** for sample code.

Chapter 6

BUGS

Report bugs to support@mavimax.com

Chapter 7

SEE ALSO

tpencrypt(3) ex_env(5) exencrypt(8) exdecrypt(8) ex_devguide(guides)

Chapter 8

COPYING