NAME

gnutls_x509_crt_verify_data2 - API function

SYNOPSIS

#include <gnutls/x509.h>

int gnutls_x509_crt_verify_data2(gnutls_x509_crt_t *crt***, gnutls_sign_algorithm_t** *algo***, unsigned int** *flags***, const gnutls_datum_t *** *data***, const gnutls_datum_t *** *signature***);**

ARGUMENTS

gnutls_x509_crt_t crt

Holds the certificate to verify with

gnutls_sign_algorithm_t algo

The signature algorithm used

unsigned int flags

Zero or an OR list of **gnutls_certificate_verify_flags**

const gnutls_datum_t * data

holds the signed data

const gnutls_datum_t * signature

contains the signature

DESCRIPTION

This function will verify the given signed data, using the parameters from the certificate.

RETURNS

In case of a verification failure **GNUTLS_E_PK_SIG_VERIFY_FAILED** is returned,
GNUTLS_E_EXPIRED or **GNUTLS_E_NOT_YET_ACTIVATED** on expired or not yet activated
certificate and zero or positive code on success.

Note that since GnuTLS 3.5.6 this function introduces checks in the end certificate (*crt*), including
time checks and key usage checks.

SINCE

3.4.0

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/