NAME

dane_verify_crt - API function

SYNOPSIS

#include <gnutls/dane.h>

int dane_verify_crt(dane_state_t *s***, const gnutls_datum_t *** *chain***, unsigned** *chain_size***, gnutls_certificate_type_t** *chain_type***, const char *** *hostname***, const char *** *proto***, unsigned int** *port***, unsigned int** *sflags***, unsigned int** *vflags***, unsigned int *** *verify***);**

ARGUMENTS

dane_state_t s A DANE state structure (may be NULL)

const gnutls_datum_t * chain
: A certificate chain

unsigned chain_size
: The size of the chain

gnutls_certificate_type_t chain_type
: The type of the certificate chain

const char * hostname
: The hostname associated with the chain

const char * proto
: The protocol of the service connecting (e.g. tcp)

unsigned int port
: The port of the service connecting (e.g. 443)

unsigned int sflags
: Flags for the initialization of *s* (if NULL)

unsigned int vflags
: Verification flags; an OR'ed list of **dane_verify_flags_t**.

unsigned int * verify
: An OR'ed list of **dane_verify_status_t**.

DESCRIPTION

This function will verify the given certificate chain against the CA constrains and/or the certificate available via DANE. If no information via DANE can be obtained the flag **DANE_VERIFY_NO_DANE_INFO** is set. If a DNSSEC signature is not available for the DANE record then the verify flag **DANE_VERIFY_NO_DNSSEC_DATA** is set.

Due to the many possible options of DANE, there is no single threat model countered. When notifying the user about DANE verification results it may be better to mention: DANE verification did not reject the certificate, rather than mentioning a successful DANE verification.

Note that this function is designed to be run in addition to PKIX - certificate chain - verification. To be run independently the **DANE_VFLAG_ONLY_CHECK_EE_USAGE** flag should be specified; then the function will check whether the key of the peer matches the key advertised in the DANE entry.

RETURNS

a negative error code on error and **DANE_E_SUCCESS** (0) when the DANE entries were successfully parsed, irrespective of whether they were verified (see *verify* for that information). If no usable entries were encountered **DANE_E_REQUESTED_DATA_NOT_AVAILABLE** will be returned.

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/