

## NAME

dane\_verify\_cert - API function

## SYNOPSIS

```
#include <gnutls/dane.h>
```

```
int dane_verify_cert(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 constraints 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

Copyright (C) 2001-2023 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/>