

## NAME

gnutls\_verify\_stored\_pubkey - API function

## SYNOPSIS

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

```
int gnutls_verify_stored_pubkey(const char * db_name, gnutls_tdb_t tdb, const char * host, const char  
* service, gnutls_certificate_type_t cert_type, const gnutls_datum_t * cert, unsigned int flags);
```

## ARGUMENTS

const char \* db\_name

A file specifying the stored keys (use NULL for the default)

gnutls\_tdb\_t tdb

A storage structure or NULL to use the default

const char \* host

The peer's name

const char \* service

non-NULL if this key is specific to a service (e.g. http)

gnutls\_certificate\_type\_t cert\_type

The type of the certificate

const gnutls\_datum\_t \* cert

The raw (der) data of the certificate

unsigned int flags

should be 0.

## DESCRIPTION

This function will try to verify a raw public-key or a public-key provided via a raw (DER-encoded) certificate using a list of stored public keys. The *service* field if non-NULL should be a port number.

The *db\_name* variable if non-null specifies a custom backend for the retrieval of entries. If it is NULL then the default file backend will be used. In POSIX-like systems the file backend uses the \$HOME/.gnutls/known\_hosts file.

Note that if the custom storage backend is provided the retrieval function should return

**GNUTLS\_E\_CERTIFICATE\_KEY\_MISMATCH** if the host/service pair is found but key doesn't match, **GNUTLS\_E\_NO\_CERTIFICATE\_FOUND** if no such host/service with the given key is found, and 0 if it was found. The storage function should return 0 on success.

As of GnuTLS 3.6.6 this function also verifies raw public keys.

## RETURNS

If no associated public key is found then **GNUTLS\_E\_NO\_CERTIFICATE\_FOUND** will be returned. If a key is found but does not match **GNUTLS\_E\_CERTIFICATE\_KEY\_MISMATCH** is returned. On success, **GNUTLS\_E\_SUCCESS** (0) is returned, or a negative error value on other errors.

## SINCE

3.0.13

## 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/>