## 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

## 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/