NAME

gnutls_pubkey_verify_hash2 - API function

SYNOPSIS

#include <gnutls/abstract.h>

int gnutls_pubkey_verify_hash2(gnutls_pubkey_t *key***, gnutls_sign_algorithm_t** *algo***, unsigned int** *flags***, const gnutls_datum_t *** *hash***, const gnutls_datum_t *** *signature***);**

ARGUMENTS

gnutls_pubkey_t key

Holds the public key

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 * hash

holds the hash digest to be verified

const gnutls_datum_t * signature

contains the signature

DESCRIPTION

This function will verify the given signed digest, using the parameters from the public key. Note that unlike **gnutls_privkey_sign_hash()**, this function accepts a signature algorithm instead of a digest algorithm. You can use **gnutls_pk_to_sign()** to get the appropriate value.

RETURNS

In case of a verification failure **GNUTLS_E_PK_SIG_VERIFY_FAILED** is returned, and zero or positive code on success. For known to be insecure signatures this function will return **GNUTLS_E_INSUFFICIENT_SECURITY** unless the flag **GNUTLS_VERIFY_ALLOW_BROKEN** is specified.

SINCE

3.0

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/