NAME

gnutls_pubkey_get_preferred_hash_algorithm - API function

SYNOPSIS

#include <gnutls/abstract.h>

int gnutls_pubkey_get_preferred_hash_algorithm(gnutls_pubkey_t *key***, gnutls_digest_algorithm_t *** *hash***, unsigned int *** *mand***);**

ARGUMENTS

gnutls_pubkey_t key
: Holds the certificate

gnutls_digest_algorithm_t * hash
: The result of the call with the hash algorithm used for signature

unsigned int * mand
: If non zero it means that the algorithm MUST use this hash. May be NULL.

DESCRIPTION

This function will read the certificate and return the appropriate digest algorithm to use for signing with this certificate. Some certificates (i.e. DSA might not be able to sign without the preferred algorithm).

To get the signature algorithm instead of just the hash use **gnutls_pk_to_sign()** with the algorithm of the certificate/key and the provided *hash* .

RETURNS

the 0 if the hash algorithm is found. A negative error code is returned on error.

SINCE

2.12.0

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/