NAME

gnutls_x509_privkey_verify_seed - API function

SYNOPSIS

#include <gnutls/x509.h>

int gnutls_x509_privkey_verify_seed(gnutls_x509_privkey_t *key***, gnutls_digest_algorithm_t** *digest***, const void *** *seed***, size_t** *seed_size***);**

ARGUMENTS

gnutls_x509_privkey_t key
> should contain a **gnutls_x509_privkey_t** type

gnutls_digest_algorithm_t digest
> it contains the digest algorithm used for key generation (if applicable)

const void * seed
> the seed of the key to be checked with

size_t seed_size
> holds the size of *seed*

DESCRIPTION

This function will verify that the given private key was generated from the provided seed. If *seed* is **NULL** then the seed stored in the *key* 's structure will be used for verification.

RETURNS

In case of a verification failure **GNUTLS_E_PRIVKEY_VERIFICATION_ERROR** is returned, and zero or positive code on success.

SINCE

3.5.0

REPORTING BUGS

Report bugs to <bugs@gnutls.org>.
Home page: https://www.gnutls.org

COPYRIGHT

Copyright (C) 2001- Free Software Foundation, Inc., and others.

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/