NAME

gnutls_certificate_set_retrieve_function3 - API function

SYNOPSIS

#include <gnutls/abstract.h>

void gnutls_certificate_set_retrieve_function3(gnutls_certificate_credentials_t *cred***,**
gnutls_certificate_retrieve_function3 * *func***);**

ARGUMENTS

gnutls_certificate_credentials_t cred
is a **gnutls_certificate_credentials_t** type.

gnutls_certificate_retrieve_function3 * func
is the callback function

DESCRIPTION

This function sets a callback to be called in order to retrieve the certificate and OCSP responses to be used in the handshake. *func* will be called only if the peer requests a certificate either during handshake or during post-handshake authentication.

The callback's function prototype is defined in 'abstract.h':

int gnutls_certificate_retrieve_function3(gnutls_session_t, const struct gnutls_cert_retr_st *info, gnutls_pcert_st **certs, unsigned int *certs_length, gnutls_ocsp_data_st **ocsp, unsigned int *ocsp_length, gnutls_privkey_t *privkey, unsigned int *flags);

The info field of the callback contains:
req_ca_dn which is a list with the CA names that the server considers trusted. This is a hint and typically the client should send a certificate that is signed by one of these CAs. These names, when available, are DER encoded. To get a more meaningful value use the function **gnutls_x509_rdn_get()**.
pk_algos contains a list with server's acceptable public key algorithms. The certificate returned should support the server's given algorithms.

The callback should fill-in the following values:

certs should contain an allocated list of certificates and public keys.
certs_length is the size of the previous list.
ocsp should contain an allocated list of OCSP responses.
ocsp_length is the size of the previous list.

privkey is the private key.

If flags in the callback are set to **GNUTLS_CERT_RETR_DEINIT_ALL** then all provided values must be allocated using **gnutls_malloc()**, and will be released by gnutls; otherwise they will not be touched by gnutls.

The callback function should set the certificate and OCSP response list to be sent, and return 0 on success. If no certificates are available, the *certs_length* and *ocsp_length* should be set to zero. The return value (-1) indicates error and the handshake will be terminated. If both certificates are set in the credentials and a callback is available, the callback takes predence.

Raw public-keys: In case raw public-keys are negotiated as certificate type, certificates that would normally hold the public-key material are not available. In that case,
certs contains an allocated list with only the public key. Since there is no certificate, there is also no certificate status. Therefore, OCSP information should not be set.

SINCE

3.6.3

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/