

NAME

gnutls_certificate_set_retrieve_function2 - API function

SYNOPSIS

```
#include <gnutls/abstract.h>
```

```
void gnutls_certificate_set_retrieve_function2(gnutls_certificate_credentials_t cred,
gnutls_certificate_retrieve_function2 * func);
```

ARGUMENTS

gnutls_certificate_credentials_t cred
is a **gnutls_certificate_credentials_t** type.

gnutls_certificate_retrieve_function2 * func
is the callback function

DESCRIPTION

This function sets a callback to be called in order to retrieve the certificate to be used in the handshake. The callback will take control only if a certificate is requested by the peer.

The callback's function prototype is: int (*callback)(gnutls_session_t, const gnutls_datum_t* req_ca_dn, int nreqs, const gnutls_pk_algorithm_t* pk_algos, int pk_algos_length, gnutls_pcert_st** pcert, unsigned int *pcert_length, gnutls_privkey_t * pkey);

req_ca_dn is only used in X.509 certificates. Contains 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.

pcert should contain a single certificate and public key or a list of them.

pcert_length is the size of the previous list.

pkey is the private key.

If the callback function is provided then gnutls will call it, in the handshake, after the certificate request message has been received. All the provided by the callback values will not be released or modified by

gnutls.

In server side `pk_algos` and `req_ca_dn` are NULL.

The callback function should set the certificate list to be sent, and return 0 on success. If no certificate was selected then the number of certificates should be set to zero. The 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 precedence.

SINCE

3.0

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/>