NAME

SSL_CTX_set_psk_client_callback, SSL_set_psk_client_callback - set PSK client callback

SYNOPSIS

```
#include <openssl/ssl.h>

void SSL_CTX_set_psk_client_callback(SSL_CTX *ctx,
unsigned int (*callback)(SSL *ssl, const char *hint,
char *identity, unsigned int max_identity_len,
unsigned char *psk, unsigned int max_psk_len));
void SSL_set_psk_client_callback(SSL *ssl,
unsigned int (*callback)(SSL *ssl, const char *hint,
char *identity, unsigned int max_identity_len,
unsigned char *psk, unsigned int max_psk_len));
```

DESCRIPTION

A client application must provide a callback function which is called when the client is sending the ClientKeyExchange message to the server.

The purpose of the callback function is to select the PSK identity and the pre-shared key to use during the connection setup phase.

The callback is set using functions *SSL_CTX_set_psk_client_callback()* or *SSL_set_psk_client_callback()*. The callback function is given the connection in parameter **ssl**, a **NULL**-terminated PSK identity hint sent by the server in parameter **hint**, a buffer **identity** of length **max_identity_len** bytes where the resulting **NULL**-terminated identity is to be stored, and a buffer **psk** of length **max_psk_len** bytes where the resulting pre-shared key is to be stored.

NOTES

Note that parameter **hint** given to the callback may be **NULL**.

RETURN VALUES

Return values from the client callback are interpreted as follows:

On success (callback found a PSK identity and a pre-shared key to use) the length (> 0) of **psk** in bytes is returned.

Otherwise or on errors callback should return 0. In this case the connection setup fails.

COPYRIGHT