NAME

CURLOPT_SSL_VERIFYPEER − verify the peer's SSL certificate

SYNOPSIS

#include <curl/curl.h>

CURLcode curl_easy_setopt(CURL *handle, CURLOPT_SSL_VERIFYPEER, long verify);

DESCRIPTION

Pass a long as parameter to enable or disable.

This option determines whether curl verifies the authenticity of the peer's certificate. A value of 1 means curl verifies; 0 (zero) means it doesn't.

When negotiating a TLS or SSL connection, the server sends a certificate indicating its identity. Curl verifies whether the certificate is authentic, i.e. that you can trust that the server is who the certificate says it is. This trust is based on a chain of digital signatures, rooted in certification authority (CA) certificates you supply. curl uses a default bundle of CA certificates (the path for that is determined at build time) and you can specify alternate certificates with the *CURLOPT_CAINFO(3)* option or the *CURLOPT_CAPATH(3)* option.

When *CURLOPT_SSL_VERIFYPEER(3)* is enabled, and the verification fails to prove that the certificate is authentic, the connection fails. When the option is zero, the peer certificate verification succeeds regardless.

Authenticating the certificate is not enough to be sure about the server. You typically also want to ensure that the server is the server you mean to be talking to. Use *CURLOPT_SSL_VERIFYHOST(3)* for that. The check that the host name in the certificate is valid for the host name you're connecting to is done independently of the *CURLOPT_SSL_VERIFYPEER(3)* option.

WARNING: disabling verification of the certificate allows bad guys to man-in-the-middle the communication without you knowing it. Disabling verification makes the communication insecure. Just having encryption on a transfer is not enough as you cannot be sure that you are communicating with the correct endpoint.

DEFAULT

By default, curl assumes a value of 1.

PROTOCOLS

All TLS based protocols: HTTPS, FTPS, IMAPS, POP3, SMTPS etc.

EXAMPLE

TODO

AVAILABILITY

If built TLS enabled.

RETURN VALUE

Returns CURLE_OK if the option is supported, and CURLE_UNKNOWN_OPTION if not.

SEE ALSO

CURLOPT_SSL_VERIFYHOST(3),