NAME

CURLOPT_PINNEDPUBLICKEY − set pinned public key

SYNOPSIS

```
#include <curl/curl.h>

CURLcode curl_easy_setopt(CURL *handle, CURLOPT_PINNEDPUBLICKEY, char *pinnedpubkey);
```

DESCRIPTION

Pass a pointer to a zero terminated string as parameter. The string should be the file name of your pinned public key. The format expected is "PEM" or "DER".

When negotiating a TLS or SSL connection, the server sends a certificate indicating its identity. A public key is extracted from this certificate and if it does not exactly match the public key provided to this option, curl will abort the connection before sending or receiving any data.

DEFAULT

NULL

PROTOCOLS

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

EXAMPLE

```
CURL *curl = curl_easy_init();
if(curl) {
  curl_easy_setopt(curl, CURLOPT_URL, "https://example.com");
  curl_easy_setopt(curl, CURLOPT_PINNEDPUBLICKEY, "/etc/publickey.der");

  /* Perform the request */
  curl_easy_perform(curl);
}
```

PUBLIC KEY EXTRACTION

If you do not have the server’s public key file you can extract it from the server’s certificate.
openssl x509 -in www.test.com.pem -pubkey -noout > www.test.com.pubkey.pem
The public key is output in PEM format and contains a header, base64 data and a footer:
-----BEGIN PUBLIC KEY-----
[BASE 64 DATA]
-----END PUBLIC KEY-----

AVAILABILITY

Added in 7.39.0 for OpenSSL, GnuTLS and GSKit. Added in 7.43.0 for NSS and wolfSSL/CyaSSL. Other SSL backends not supported.

RETURN VALUE

Returns CURLE_OK if TLS enabled, CURLE_UNKNOWN_OPTION if not, or CURLE_OUT_OF_MEMORY if there was insufficient heap space.

SEE ALSO

CURLOPT_SSL_VERIFYPEER(3), **CURLOPT_SSL_VERIFYHOST**(3), **CURLOPT_CAINFO**(3), **CURLOPT_CAPATH**(3),