Subject: [SOLVED] Purpose of HttpRequest::SSLCertificate
Posted by Xemuth on Mon, 25 Mar 2019 15:55:26 GMT
View Forum Message <> Reply to Message

Hello Upp,

I'm trying to use custom certificats with HttpRequest so I did somethink like this :

requete3.SSLCertificate("TEST","TEST",false );


I was expecting to retrieve this keyWord "TEST"  into <Core/SSL> socket.cpp Start() Function by using debug mode but the fact is I never find "TEST" Keyword.
Is it a bug or I just didnt understand the use case of SSLCertificate ?

Another Question, this method is used to set the certificate used to handshake with the server ?

Can someone explain me how Core/SSL select the right certificate to handshake the server ?


PS : Theide version is 12883, Compiled 03/24/2019 01:32:00 (the latest version atm)

Thanks in advance.

Best regard

Subject: Re: Purpose of HttpRequest::SSLCertificate
Posted by mirek on Tue, 26 Mar 2019 07:29:45 GMT
View Forum Message <> Reply to Message

Check

bool SslContext::UseCertificate(String certdata, String pkeydata, bool cert_asn1)

and corresponding SSL functions - that is where those values are consumed.

Subject: Re: Purpose of HttpRequest::SSLCertificate
Posted by Xemuth on Tue, 26 Mar 2019 11:09:27 GMT
View Forum Message <> Reply to Message

Hi Mirek,

Thanks for your reply.

By looking deeply the code of CORE/SSL. In
 bool TcpSocket::SSLImp::Start()
this Happen :

if(socket.cert.GetCount())
    context.UseCertificate(socket.cert, socket.pkey, socket.asn1);

I guess, the purpose of this is to change the certificate when socket.cert.GetCount() > 0
but the probleme is, with this kind of code :

 HttpRequest requete3(requete2.GetRedirectUrl());
 requete3.GET();
 requete3.StdHeaders(true);
 requete3.SSLCertificate("TEST","TEST",false );
 Cout() <<  requete3.Execute();

this  :   if(socket.cert.GetCount())   is never equal to true.

may be that attaching the socket to the SSLImp structure does not work well, Or I'm just stupid
and didnt understood how to use it :d

What you think about it ?

Thanks in advance.

Best regard

---

## Subject: Re: Purpose of HttpRequest::SSLCertificate
Posted by Xemuth on Tue, 26 Mar 2019 11:30:27 GMT

the socket cert and pkey data is reseted when HttpRequest::Execute() is called due to :

call of void HttpRequest::StartConnect() in DNS phase

by modifing the method a bit it work. Is there any way to do Execute method specify a Phase ?
If you want I could  do a fix then post it here.

---

## Subject: Re: Purpose of HttpRequest::SSLCertificate
Posted by Xemuth on Tue, 26 Mar 2019 15:18:22 GMT

Well,
Since I'm stupid I thought SSlCertificate was made to set

the certificate to send in case of TSL SSL certificate request Authentification.
But it's just used to make the server side of Https server.

Well sorry guys...