

---

Subject: SSLSocket VerifyPeer -> how to set trusted CAs?

Posted by [fallingdutch](#) on Tue, 19 Dec 2006 11:08:32 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hi

at the moment i am looking around for a way to set my own CA to be trusted.

The openssl function is:

```
int SSL_CTX_load_verify_locations(SSL_CTX *ctx, const char *CAfile, const char *CApath);
```

And now i am wondering wether there is another way or it is not yet implemented?

Bas

---

---

Subject: Re: SSLSocket VerifyPeer -> how to set trusted CAs?

Posted by [rylek](#) on Tue, 19 Dec 2006 21:17:54 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hello!

You're right, there is currently no wrapper for the function you mentioned. To be honest, when implementing the SSL wrapper I felt rather overwhelmed with the broad range of various structures and functions the SSL library offers. As I had no clear idea which ones were really important, I chose a minimalistic approach, wrapping only as much as I felt absolutely necessary to make the SSL socket up and running. I think some time ago I posted somewhere here a code snippet demonstrating SSL initialization within one of my commercial applications, which showed this very clearly.

Regards

Tomas

---

---

Subject: Re: SSLSocket VerifyPeer -> how to set trusted CAs?

Posted by [fallingdutch](#) on Tue, 19 Dec 2006 21:30:27 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Yes, Thomas, you did paste such a code, i remembered it, too and it was the same i am using for XmlRpc, so i was pretty glad that i understood your SSL implementation.

Will you extend the SSL Socket implementation or do you want to keep it the way it is?

I thought of another function, too `SSL_CTX_use_certificate_file` and `SSL_CTX_use_PrivateKey_file` eg by `UseCertificateFile()`

If you want i can send Mirek a patch to patch the SSL implementation.

Bas

---