Subject: OpenSSL encryption and hashing functions in U++
Posted by koldo on Fri, 07 May 2010 20:01:33 GMT
View Forum Message <> Reply to Message

Mindtraveller and me wanted to propose you to include OpenSSL encryption and hashing functions in U++.

Perhaps the adequate place would be package Web/SSL.

Functions to include there are now in AESStream bazaar package. They support for now:

- AES: AES-128/192/256 stream encryption
- SHA-2: SHA-224/256/384/512 string hashing

What do you think?

Subject: Re: OpenSSL encryption and hashing functions in U++
Posted by koldo on Tue, 11 May 2010 07:10:29 GMT
View Forum Message <> Reply to Message

Here I explain you some advantages of functions proposed:

- AESStream: It is an easy way to do strong encryption of Strings or files.

- SHA-2: Actually U++ includes SHA-1 support. However, from Wikipedia:
SHA-1 is being retired for most government uses; the U.S. National Institute of Standards and Technology says,
"Federal agencies should stop using SHA-1 for...applications that require collision resistance as soon as practical,
and must use the SHA-2 family of hash functions for these applications after 2010"
Thanks to OpenSSL the SHA-2 implementation is very thin and simple.

Subject: Re: OpenSSL encryption and hashing functions in U++
Posted by Mindtraveller on Tue, 11 May 2010 16:28:41 GMT
View Forum Message <> Reply to Message

koldo, AFAIR you suggested to switch to some other library with less restrictive license.
I'd like to ask Mirek what he thinks about adding new classes to Web/SSL and receiving our efforts on switching from OpenSSL.

Subject: Re: OpenSSL encryption and hashing functions in U++
Posted by koldo on Wed, 12 May 2010 05:48:51 GMT
View Forum Message <> Reply to Message

Mindtraveller wrote on Tue, 11 May 2010 18:28koldo, AFAIR you suggested to switch to some other library with less restrictive license.
I'd like to ask Mirek what he thinks about adding new classes to Web/SSL and receiving our efforts on switching from OpenSSL.
Hello Mindtraveller

he has to decide .

About using other library instead of OpenSSL, well, that is a second and secondary question.
Why?: It exists a library called OpenTLS that wants to cover all OpenSSL features with a less restrictive license. However:

- OpenTLS seems to be in a preliminary state and it should have to be studied if it covers all options required by Web/SSL
- OpenSSL license is not bad as it permits commercial and non-commercial use. However it is not completely compatible with GPL (http://en.wikipedia.org/wiki/OpenSSL)

Subject: Re: OpenSSL encryption and hashing functions in U++
Posted by Mindtraveller on Wed, 12 May 2010 05:53:36 GMT
View Forum Message <> Reply to Message

If OpenSSL permits commercial use, I see no real need to change it with other library.