Subject: Re: Using openssl functions on U++
Posted by Zardos on Thu, 13 Dec 2007 08:32:54 GMT
View Forum Message <> Reply to Message

ealabarce wrote on Thu, 13 December 2007 06:30Thanks Ralf, i have a cuestion, the two projects are the class, or I only need the CryptOpenSsl.zip one, or the UnitTest.zip is part of the class, now, to use the class i need only a declaration like "Rsa Firma;", like other classes and then access to the methods. because im doing this:

You can leave out the UnitTest package. I just attached it to make the CryptOpenSsl compile.

If you remove the UnitTest remove

```
#ifdef _DEBUG
TEST(Rsa) {
 Rsa rsa;
 rsa.GenerateKeyPair(512);

 String pri = rsa.PrivateKeyToPem();
 String pub = rsa.PublicKeyToPem();

 Rsa rsa2;
 rsa2.PrivateKeyFromPem(pri);

 String pri2 = rsa2.PrivateKeyToPem();
 String pub2 = rsa.PublicKeyToPem();

 CHECK(pri == pri2);
 CHECK(pub == pub2);
 CHECK(rsa.VerifySHA("Kleiner Test", rsa2.SignSHA("Kleiner Test")));
 CHECK(rsa.Decrypt(rsa2.Encrypt("Kleiner Test")) == "Kleiner Test");
 CHECK(!rsa.VerifySHA("Kleiner Test", rsa2.SignSHA("@Kleiner Test")));
}
#endif
```

...from CryptOpenSsl.cpp

and
#include <UnitTest/UnitTest.h> from CryptOpenSsl.h

Quote:But when I compile the project, the compiler show me this error:

```
C:\ElectroFactUPP\firmafactSAT_GUI\main.cpp: In member function `void
firmafactSAT_GUI::CargarSe
 llo()':
C:\ElectroFactUPP\firmafactSAT_GUI\main.cpp:53: error: `rsa' undeclared (first use this function
 )
```

I need to put a include to a some file?

Thanks for the help...

add: #include <openssl/md5.h> to CryptOpenSsl.h

The .h file now looks like this (UnitTest.h is still included - remove it if you want. See note above):

```
#ifndef _CryptOpenSsl_CryptOpenSsl_h_
#define _CryptOpenSsl_CryptOpenSsl_h_

// ----------------------------------------------------------------------------------------

#include <Core/Core.h>
#include <UnitTest/UnitTest.h>

 #define OPENSSL_THREAD_DEFINES
 #include <openssl/opensslconf.h>
 #if !defined(OPENSSL_THREADS)
 @@@
 #endif

#include <openssl/rsa.h>
#include <openssl/md5.h>
#include <openssl/engine.h>
#include <openssl/pem.h>

using namespace Upp;

// ----------------------------------------------------------------------------------------

String ToString(BIGNUM *b);
BIGNUM * ToBigNum(String& str);
String ToString(BIO *bp);
BIO * ToBIO(String &str);

// ----------------------------------------------------------------------------------------

struct Rsa : public Moveable<Rsa> {
 Rsa() { rsa = NULL; }
 ~Rsa() { if(rsa) RSA_free(rsa); }

 void GenerateKeyPair(int bits = 1024, int exponent = 17);

 String PrivateKeyToPem();
 String PublicKeyToPem();
 void PrivateKeyFromPem(const String &pem);
 void PrivateKeyFromPem(uint8 *d, int l);
```

```
 void PublicKeyFromPem(const String &pem);
 void PublicKeyFromPem(uint8 *d, int l);

 String SignSHA(const String &msg);
 String SignMD5(const String &msg);  // Added by me
 String Decrypt(const String &msg, int padding = RSA_PKCS1_OAEP_PADDING);

 bool VerifySHA(const String &msg, const String &sig);
 bool VerifyMD5(const String &msg, const String &sig); // Added by me
 String Encrypt(const String &msg, int padding = RSA_PKCS1_OAEP_PADDING);

 int MaxMsgCount(int padding = RSA_PKCS1_OAEP_PADDING);

 void Serialize(Stream &s);

protected:
 RSA *rsa;
};

// ----------------------------------------------------------------------------------------

#endif
```

- Ralf
