Subject: Re: Using openssl functions on U++
Posted by ealabarce on Thu, 13 Dec 2007 05:30:12 GMT
View Forum Message <> Reply to Message

Thanks 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:

I add the CryptOpenSsl project to my project, and then...

On a method of my class i put this:

```
void firmafactSAT_GUI::CargarSello() //Carga archvio del sello
{
 B64.Clear(); //Clean result editfield
 Cadena=CadenaOriginal.GetData();  //Get the string to sign
 ArchivoFirma.Type("Sello Digital", "*.key"); //file type to the key file
 if (ArchivoFirma.ExecuteOpen("Seleccione el archivo de sello digital"))
 {
   RutaSello.SetText(ArchivoFirma.Get()); //Path to key file
   if (StreamArchivoFirma.Open(ArchivoFirma.Get())) //Open the file stream
    PromptOK("Archivo abierto correctamente!!!"); //only to test

   B64=Base64Encode(rsa.SignMD5(Cadena)); //sign the string and convert to base64
   //FirmaDigital=RSA_new();
   //FirmaDigital=StreamArchivoFirma.;

 }

}
```

And on the declare of my class i have the declaration of Rsa object:

```
class firmafactSAT_GUI : public WithfirmafactSAT_GUILayout<TopWindow> {
 String Cadena;      // Para guardar la cadena original del campo de edicion
 String Digestion;     // Para guardar la digestion de la cadena
 String Hexadecimal;    // Para guardar la digestion expresada en Hexadecimal
 String B64;      // Para guardar la digestion expresada en base64
 Rsa rsa; // <-- here is
 //RSA *FirmaDigital;
 FileSel ArchivoFirma;   //Selector para cargar el archivo de la firma
 FileIn  StreamArchivoFirma;  //Stream del archvio de la firma
```

..... etc.

Because I need to use MD5 I add this code to CryptOpenSsl.h

```
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;
};
```

And to CryptOpenSsl.cpp

```
String Rsa::SignMD5(const String &msg) {
 ASSERT(rsa);

 String ret(0, RSA_size(rsa));
 unsigned int len;
 uint8 h[16];

 MD5((uint8 *)~msg, msg.GetCount(), h);

 RSA_sign(NID_md5, h, 16, (uint8 *)~ret, &len, rsa);
 ret.Trim(len);
```

```
 return ret;
}

bool Rsa::VerifyMD5(const String &msg, const String &sig) {
 ASSERT(rsa);

 uint8 h[16];

 MD5((uint8 *)~msg, msg.GetCount(), h);

 return RSA_verify(NID_md5, h, 16, (uint8 *)~sig, sig.GetCount(), rsa);
}
```

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...
