

---

Subject: Using openssl functions on U++  
Posted by [ealabarce](#) on Sun, 09 Dec 2007 21:13:32 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

How to implement openssl on U++ (no sockets) functions like dgst, md5, working with certificates.

For example:  
I need to make in code this commands:

```
openssl.exe dgst -md5 -sign firma.pem  
openssl.exe enc -base64 -A
```

but U++ don't include openssl, im working with ultimate++ ver. 2007.1 with mingw on windows.

Thanks

---

---

Subject: Re: Using openssl functions on U++  
Posted by [rylek](#) on Sun, 09 Dec 2007 23:14:16 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Hello!

U++ contains a very thin wrapper over openssl in the Web/SSL package. This basically implements SSL-based streaming sockets only, all additional work like certificate management has to be done directly via calls to the openssl library. For certain special functions there are tools in the U++ itself, namely the MD5 digest or the BASE64 encoding (see Web/util.h, Base64Encode / Decode & MD5Digest). Some time ago I posted somewhere here a snippet of code demonstrating the usage (mainly the initialization phase) of the SSL-based sockets, if you don't find it, I can re-post it here.

Regards

Tomas Rylek

---

---

Subject: Re: Using openssl functions on U++  
Posted by [ealabarce](#) on Mon, 10 Dec 2007 00:25:42 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Hi rylek, and thanks for the fast answer, well im try to find the form to get this, but I'm new on c++ and its hard to me, im try this code, on new empty project an add a webssl package to the project this is may code (maybe all is wrong )

```
#include <iostream>
```

```
#include <Web/Web.h>
using namespace std;

int main()
{
    char *text;
    char *salida;
    text = "Hola a todos";
    salida=Base64Encode(MD5Digest(*text));
    cout << "Salida en base64 para la digestion de " << text << " = " << salida;
    return 1;
}
```

And when i compile, return this errors:

```
C:\ElectroFactUPP\testssl\main.cpp: In function `int main()':
C:\ElectroFactUPP\testssl\main.cpp:10: error: `MD5Digest' undeclared (first use this func
tion)
C:\ElectroFactUPP\testssl\main.cpp:10: error: (Each undeclared identifier is reported onl
y once for each function it appears in.)
C:\ElectroFactUPP\testssl\main.cpp:10: error: `Base64Encode' undeclared (first use this f
unction)
C:\ElectroFactUPP\testssl\main.cpp:13:2: warning: no newline at end of file
testssl: 1 file(s) built in (0:03.25), 3250 msec / file, duration = 3250 msec
```

There were errors. (0:03.28)

-----

Excuse my poor experience on c++ but i want to take the next step and pass all my applications on realbasic to c++ using ultimate++.

Thanks a lot for your assistance....

Best Regards.

Note: Excuse my poor english too

---

Subject: Re: Using openssl functions on U++  
Posted by [waxblood](#) on Mon, 10 Dec 2007 04:35:34 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

U++ is written in standard C++, but it doesn't use c++ standard template library (stl) for efficiency reasons, so you should avoid using anything which is included in std namespace - you could start by not writing using namespace std at all for example

This is the corrected version of your program:

```
// not needed std stuff
//#include <iostream>

#include <Web/Web.h>

//not needed, too
//using namespace std;

using namespace UPP; //write this, otherwise upp functions won't get recognised

int main()
{
char *text = "Hola a todos";

String salida; //in this case seems better to use String - NOTE: this is Ultimate++ String, not
std::string

//text = "Hola a todos"; // you can write a thing like this only at initialization time

salida = Base64Encode(MD5Digest(text)); // if you write *text you pass MD5Digest a _single_
char, not a vector of chars

//Upp way to std::cout is writing Cout()
Cout() << "Salida en base64 para la digestion de " << text << " = " << salida;

return 0; //Why return 1? If we got so far return 0 (no error) seems better
}
```

I suggest you to read :

String tutorial

<http://www.ultimatepp.org/srcdoc/Core/CoreTutorial/en-us.htm> |

As for String/char\* conversions,

[http://www.ultimatepp.org/forum/index.php?t=msg&goto=125111&#msg\\_12511](http://www.ultimatepp.org/forum/index.php?t=msg&goto=125111&#msg_12511)

David

---

---

Subject: Re: Using openssl functions on U++  
Posted by [ealabarce](#) on Mon, 10 Dec 2007 20:34:06 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Thanks so much, David, I need read an make all tutorials, im working on that, thanks for the help.

Best Regards

---

Subject: Re: Using openssl functions on U++  
Posted by [ealabarce](#) on Wed, 12 Dec 2007 20:11:45 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Hello again, well im reading the documentation, and now i can get the md5 and the base64 convection, but now I need to sign the md5 with a rsa .key private file, I trying to understand who to do this, viewing on the openssl.org API documentation, but I some confuse, let me explain:

First I initalize a RSA struture like this:  
RSA \*FirmaDigital;

Then i use the FileIn Stream:  
FileIn StreamArchivoFirma;

Get a new Struct of RSA  
FirmaDigital=RSA\_new();

My cuestion is, who to put the file stream on the memory structure of RSA.

Thanks in advance.

---

Subject: Re: Using openssl functions on U++  
Posted by [Zardos](#) on Wed, 12 Dec 2007 21:00:58 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

ealabarce wrote on Wed, 12 December 2007 21:11Hello again, well im reading the documentation, and now i can get the md5 and the base64 convection, but now I need to sign the md5 with a rsa .key private file, I trying to understand who to do this, viewing on the openssl.org API documentation, but I some confuse, let me explain:

First I initalize a RSA struture like this:  
RSA \*FirmaDigital;

---

Then i use the FileIn Stream:  
FileIn StreamArchivoFirma;

Get a new Struct of RSA  
FirmaDigital=RSA\_new();

My cuestion is, who to put the file stream on the memory structure of RSA.

Thanks in advance.

I have attached a Upp package "CryptOpenSsl.zip".

There is a class with the following intefarce:

```
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 Decrypt(const String &msg, int padding = RSA_PKCS1_OAEP_PADDING);
```

```
bool VerifySHA(const String &msg, const String &sig);  
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;  
};
```

```
a example:  
#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 = rsa2.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

```

Use "SignSHA" and "VerifySHA" for signing and verification.  
"Encrypt" and "Decrypt" for crypting.

The functions "PrivateKeyToPem" "PublicKeyToPem" "PrivateKeyFromPem"  
"PublicKeyFromPem" are useful, too. Use them to store or load a public / private key.

Just look in the cpp file how it is done and copy what you need or tweak the class for your requirements.

- Ralf

## File Attachments

- 1) [CryptOpenSsl.zip](#), downloaded 454 times
- 2) [UnitTest.zip](#), downloaded 416 times

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 question, 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 archivo 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 archivo 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...

---

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 06:30 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:

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 = rsa2.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 OPENSSSL_THREAD_DEFINES  
#include <openssl/opensslconf.h>  
#if !defined(OPENSSSL_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

---

Subject: Re: Using openssl functions on U++  
 Posted by [Zardos](#) on Thu, 13 Dec 2007 08:42:30 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Just another remark:

Make sure you call `GenerateKeyPair(...)` or `PrivateKeyFromPem(...)` before signing a message!

`GenerateKeyPair`: creates a new (random) public/private key pair. The private key is used for signing and decryption. The public key is used to verify a signed messages and to encrypt a message

`PrivateKeyFromPem`: reads a private key from a string -> `PrivateKeyToPem` save a private key to a string. The string is in PEM format, probably what you need

To verify a message you need a public key. Use `PublicKeyFromPem(...)` for this.

- Ralf

---

---

Subject: Re: Using openssl functions on U++  
Posted by [nixnixnix](#) on Tue, 14 Jul 2009 00:51:27 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

when I add the code

```
#include <openssl/ssl.h>
```

in my program I get an error so I assume I need to download the openssl source from the web (which I have done). Now where do I put it please and why are there lines in `Web/ssl` which reference this when it isn't there?

Cheers,

Nick

---

---

Subject: Re: Using openssl functions on U++  
Posted by [nixnixnix](#) on Fri, 24 Jul 2009 19:14:33 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Ok, got it to compile in win32 and win64 but not for a DEBUG build. Any ideas on how to debug with openssl compiled in please?

Nick

---

---

Subject: Re: Using openssl functions on U++  
Posted by [nixnixnix](#) on Mon, 10 Aug 2009 18:48:00 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Ok I had problems linking for several reasons which I will list here for anyone else who comes across this thread with similar issues:

- 1) didn't specify the libraries in the package organizer (Project->Package Organizer)
- 2) tried to use the same libraries for both 32 and 64 bit builds - no no no! Need to download both builds from <http://www.slproweb.com/products/Win32OpenSSL.html>
- 3) need to specify libraries that match your build. I was using MSC9 and linking statically so I need to use the libraries in `..\OpenSSL\lib\VC\static\`

Hope this helps,

Nick

---