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