Subject: Core/SSL: AES-256-GCM encryption and decryption support
Posted by Oblivion on Mon, 05 May 2025 13:01:53 GMT
View Forum Message <> Reply to Message

Hi,

U++ nightly builds have gained AES-256-GCM encryption and decryption support, meaning you can have a high quality blob encrpytion/decryption using a password/passphrase.

Public API:

```
class Aes256Gcm : NoCopy {
public:
    Aes256Gcm();
    ~Aes256Gcm();

    Aes256Gcm& Iteration(int n);
    Aes256Gcm& Chunksize(int sz);

    bool Encrypt(Stream& in, const String& password, Stream& out);
    bool Decrypt(Stream& in, const String& password, Stream& out);
    bool Encrypt(const String& in, const String& password, String& out);
    bool Decrypt(const String& in, const String& password, String& out);

    Gate<int64, int64> WhenProgress;
    String GetErrorDesc() const;
};

String AES256Encrypt(const String& in, const String& password, Gate<int64, int64>
WhenProgress = Null);
String AES256Decrypt(const String& in, const String& password, Gate<int64, int64>
WhenProgress = Null);
bool AES256Encrypt(Stream& in, const String& password, Stream& out, Gate<int64, int64>
WhenProgress = Null);
bool AES256Decrypt(Stream& in, const String& password, Stream& out, Gate<int64, int64>
WhenProgress = Null);
```

Detailed info can be found here

Best regards,
Oblivion