



CryptoLib case study

Summary

CryptoLib library provides a software library for symmetric and public key cryptography.



Service

- R & D

Industry

- Telecommunications
- Applied mathematics
- Cryptography

Project Size

- Time size: 3 researchers, 2 software engineers, 1 QA engineer
- Duration: 3 months

Technology

- MS Visual C++
- Own developed library of prime and binary field arithmetics, arithmetics in elliptic curve points group over prime and binary fields, arithmetics in Jacobian of genus 2 hyperelliptic curves over prime and binary fields
- Own developed library of elliptic and hyperelliptic cryptosystems

Challenge

Final user requirements provide for user to export the following items from **CryptoLib** library:

- functions for generation/verification of a digital signature by IEEE P 1363-2000 (EC NRSA, EC DSA), ISO/IEC 15946-2 (EC KDSA, EC GDSA), GOST R34.10-2000, DSTU 4145-2002;
- functions for common secret generation by IEEE P 1363-2000 (EC KAS-DH1, EC KAS-DH2, EC KAS-MQV);
- functions for symmetric encryption/decryption by GOST 28147-89, AES;
- functions for digest generation by RIPEMD, GOST R 34.11-94.

Solution

In order to ensure the end product meeting Client's expectations NRJETIX has developed a detailed software requirements specifications (SRS).

The application architecture design and research were both developed by NRJETIX.

Demo version was provided to the Client at each milestone. Change requests delivered by Client were carefully evaluated and implemented.

Specification

CryptoLib it is a cross-platform cryptographic library to be deployed in C++ projects. From an engineering point of view it is a library that can be statically or dynamically linked with cryptographic algorithms. It consists of several main parts: a library of transformations in binary fields, a library of transformations in prime fields, a library of transformations in elliptic curve points group over prime and binary fields, a library of transformations in Jacobian of genus 2 hyperelliptic curve over prime and binary fields, a library of symmetric ciphers and a library of hash-function. In the **CryptoLib** implementation NRJETIX used latest works of the leading scientists and developers in this area as well as the research results of NRJETIX R&D lab. The developed Library is optimized for CPU with 0x86 architecture and can be run under the Microsoft Windows OS and Unix/Linux OS as well. This architecture allows using **CryptoLib** in different application.