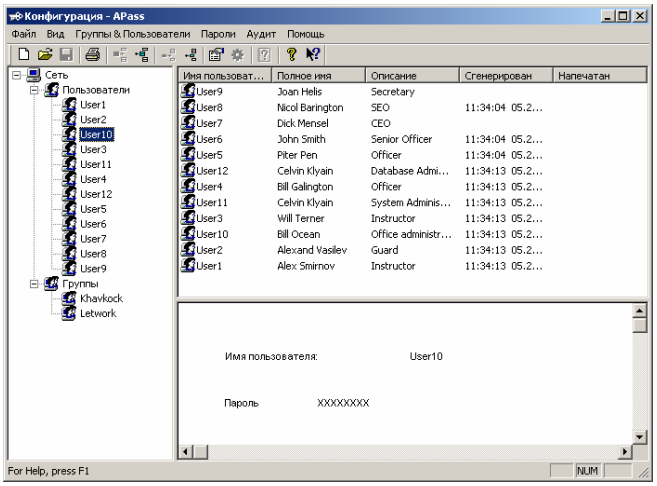
APassword case study

Summary

APassword application provides for generation, storage and distribution of passwords to client applications requiring user authentication.



Service
- R & D

Industry
- Data Security
- Cryptography
- Applied Mathematics

Project Size
- Team size: 2 software engineers, 1 QA engineers
- Calendar duration: 6 months

Technology
- MS Visual C++
- Own-developed library of cryptographic transforms

Challenge

The application end requirements were to enable security officer to :

- Manage user data
- Manage user group data
- Manage password generation process
- Manage and print out user passwords
- Manage and print out user group passwords
- Perform audit of the application administrator activities
- Keep user data encrypted in a dedicated data storage
- Provide for audit trail integrity due to digital signing.

Solution

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

The application architecture is built of three main parts: user interface, cryptographic module, encrypted users database. The architecture model was selected due to FIPS 112 standard which allowed NRJETIX save on development time, provide the required security level of user data stored in the database, and provide for easiness of further modifications if required by Client.

The application architecture design and UI design 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

APassword it is a Windows application developed using MS Visual C++. From an engineering point of view it is a standalone Windows application using strictly specialized functions of a statically linked cryptographic library. The cryptographic module was designed in accordance with FIPS 1401 and FIPS 1402 standards requirements. User data privacy is provided by means of AES symmetric block cipher as required by FIPS 197. The pseudo random number generator was developed as required by FIPS 112 based on requirements of standards: GOST 28147-89, AES, elliptic curves in standard IEEE P1363-2000. The audit log integrity is ensured by digital signing in accordance with IEEE P1363-2000 standard, and on elliptic curves. NRJETIX research lab engineers offered to implement some improvements that caused a significant increase the transforms productivity in a group of points of elliptic curve.