IJIRR

International Journal of Information Research and Review
Vol. 03, Issue, 11, pp. 3217-3220, November, 2016

Research Article

WORKING WITH THE KEY INFORMATION

[1]Aloev Rakhmatillo Djuraevich, [2,*]Nurullaev Mirkhon Mukhammadovich and [3]Alaev Ruhillo Habibovich

[1]Professor, Department ofMathematical Modeling & Cryptanalysis, National University of Uzbekistan named M. Ulugbek, Tashkent, Uzbekistan
[2]Research Scholar, Department of Information Technology, Bukhara Engineering Technological Institute, Bukhara, Uzbekistan
[3]ResearchScholar, Department of Mathematical Modeling & Cryptanalysis, National University of Uzbekistan Named M. Ulugbek, Tashkent, Uzbekistan

ARTICLE INFO

Article History:

Received 18th August, 2016
Received in revised form
22nd September, 2016
Accepted 14th October, 2016
Published online November, 30th 2016

Keywords:

Kidney Cancer,
Human Development Index,
Asia.

ABSTRACT

Previous works of authors addresses the specific issues of ensuring informationsecurity in information systems by using its own means of cryptographic protectionof information. The present paper describes the main characteristics and capabilitiesof the CSP in “Working with key information”.

INTRODUCTION

Cryptographic protection of information (CPI) is an effective way and a key component of the entire spectrum of issues of information security in information systems (IS) and Information Protection transmitted through communication channels. In (Aloev et al., 2013) are given the functionality of the CSP developed by the authors of this article. Cryptographic Service Provider (CSP) is intended to create encryption keys, private and public keys of electronic digital signature (EDS), and the creation of electronic signature authentication, hashing, encryption, and data simulation protection using algorithms described in (GOST19.201-78, 1981; O'zDSt 1092, 2009; O'zDSt 1106, 2009;O'zDSt 1105, 2009;GOST R 28147-89, 1989; GOSTR 34.11-94, 1994;GOSTR 34.10-2001,2001).In (Aloev, 2014) described the overall structure of the software CSP proposed by the authors of this article. It is implemented as nine dynamic libraries and four interface programs.

Corresponding author: NurullaevMirkhonMukhammadovich,
Research Scholar, Department of Information Technology, Bukhara Engineering Technological Institute, Bukhara, Uzbekistan.

The present paper describes the main characteristics and capabilities of the CSP in "Working with key information". The development is based on standards (RFC4357, 2001; PKCS# 5 v2.0, 1999).CSP "Working with key information" is designed to create encryption keys, private and public keys of EDS.CSP "Working with key information" can be used in telecommunication networks, public information systems, enterprise information systems through integration into application software provides storage, processing and transmission of information and the exchange of information and ensuring the legal value of electronic documents.CSP "Working with key information" performs the following functions:

- formation of keys
- work with key information stored on external media.

Functions with key information

CSP "Working with key information" is working with key information in the key container storage (Key Container).

Since the cryptographic protection of information is built in accordance with the technology Microsoft, then the container contains the following keys:

- **AT_KEYEXCHANGE**– key used to encrypt and exchange session keys;
- **AT_SIGNATURE**– keys used to create and verify digital signatures.

Note. Private Keys (encryption keys and secret keys signatures) contained in the container are protected with a security key, which is derived from the value of the value of the user's PIN tokens.Call cryptographic procedures CSP "Working with key information" by using PKCS # 11 interface. Fundamental concepts of PKCS #11 interface are slot and token. The token is a repository of some personal information (various keys, certificates, private data, etc.), and the slot acts as a bridge between a computer and a token that can be connected various tokens at different times.

For *AT_KEYEXCHANGE* and *AT_SIGNATURE* can be used as the same, and the various slots of the PKCS #11.A means of cryptographic protection of information supports working with the containers located on the computer hard drive and removable media such as Flash Memory and Smart Card.Each container has a unique name consisting of a prefix, or multiple prefixes and name. The prefixes in the name of the container are separated by the symbol "\". The name of the container may be from zero to three prefixes:

Container Name = [pref1\][pref2\][pref3\]Name

To locate the carrier is carried out for the first prefix in the name of the container, depending on the presence of the flag in the function *CPAcquireContext CRYPT_MACHINE_KEYSET.* The name of the second container is a reference to the prefix slot *AT_KEYEXCHANGE*, and the third - for *AT_SIGNATURE*. If the third prefix is absent, the *AT_KEYEXCHANGE* and *AT_SIGNATURE* stored on the same slot.Protection of private-token objects made using cryptographic interface *PKCS#5*. This algorithm solves two problems at once: private-data encoding and protection against accidental or deliberate distortions.

The software random number generator

The random number generator for generating random numbers used for cryptographic key generation.

Initialization states

To initialize the sensor, we use a source of external entropy - mechanism "Electronic Roulette" (biological random number). For the implementation of the "electronic roulette" is used software module GUI.DLL. The first call software random number generator with the "electronic roulette" removed 32 bytes - software initialization vector of random numbers. In making random checks the quality through statistical criteria.

Algorithm operation

Scheme of software random number is as follows:

- set the elliptic curve E of the order Q over large prime field by equation $y^2=x^3+ax+b \bmod P$, where a simple module P and the coefficients a and b are structural parameters of software random number generator;
- define two points A = (XA, YA) and B = (XB, YB), belonging to a curve are also structural parameters of software random number generator. The internal state of software random number generator is the point of an elliptic curve S;
- it is initialized the initial value S_0 of the internal state S by external source of entropy;
- it is initialized the value $S_0$by the following rule: S_0 = X*A, where X is the external entropy source, presented in the form of an integer on modulo P, and the operation "*" is the multiplication of an integer on the point of the curve.

Each time a software random number generator for the next output value of the internal state is changed according to the rule:

$S_i= (S_{i-1})_x * A$, i = 1,2… .

Where *i* - number indicating the number of treatment after initialization;$(S)_x$–*x*-coordinate of the point of elliptic curve.
The output at the*i*-th address to the random number is *x*-coordinate of the point *T* of the elliptic curve *E*, calculated from the following formula:

$T_i = (S_i)_x * B$, i = 1,2… .

Block diagram of software random number generator is shown in Figure 1.

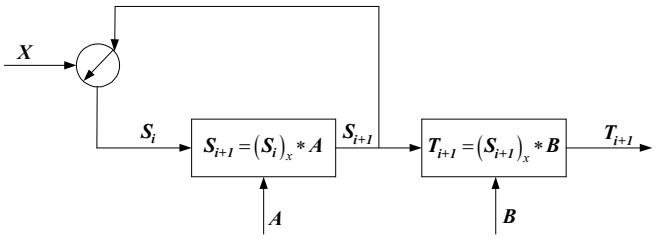

Fig. 1. Block diagram of software random number generator

Sensor session keys

Sensor session key is built based on the cryptographic algorithm GOST 28147-89, a mode-XOR feedback. The sensor is used as the key initializes the sequence length of 32 bytes.

The sensor parcels synchronous

To develop the sensor parcels synchronous used linear shift register *R*, contains 47 byte cells *R[0],…,R[46]*.

The initialization procedure is as follows:

- recorded a special clock vector, generated with the help of software random number, in the register cell *R[0],…,R[31]*;
- written random bytes, emanating from the internal random number generator of the current time, in a cell registers *R[32],…,R[39]*;
- write zeros into the cells of register *R[40],…,R[46]*.
- Register scrolling 47 beats during idling, i.e., output has not activated for any purpose.

Movement *R* register in the *j*-th beat of work occurs according to the following rules:

Values are calculated

T = R[0] << 1, if MSB of *R[0]* is 0,
T = R[0] << 1 ^ 0xE7, if the MSB of *R[0]* is 1,
T = T ^ R[40];

It is shifted register cell R:

R[i] = R[i+1], i = 0,…,45;
R[46] = T;

3) produced the register value *G(G[0],…,G[7])*, with eight bytes long, starting with 48-th beat of work of the register R;
4) it is computed the values of output bytes *G[0],…,G[7]* by adding the values for the last eight bytes of cells *R[39],…,R[46]* of the R register with the help of eight byte mask *M* as follows: *G[I] = R[39 + i] ^ M[i], i = 0,…,7*.

The mask *M* is represented by an array of the following eight bytes:
const BYTE FixedMask [8] = {

0x19, 0x3B, 0x0E, 0xDC, 0xCF, 0x51, 0x6A, 0x33
}
Output byte *G[0],…,G[7]* are used as the next portion of the random number generation at the sensor parcels synchronous.

The overall structure

CSP "Working with key information" is implemented in the following dynamic library:

- **CSP.DLL**– loading interface CSP using Crypto API;
- **CSPFUNC.DLL**– loading CSP interface directly;
- **PKCS11.DLL**–loading interface PKCS # 11 (PKCS # 11 interface for CSP "Working with key information" PKCS # 11);
- **SCTOKEN.DLL**–functions work with a smart card through the interface PKCS # 11;
- **VTOKEN.DLL**–work with virtual slots and tokens through PKCS # 11 interface;

The above are placed in the library folder WINDOWS \ SYSTEM32. Also, in CSP "Working with key information" includes the following modules:

- ***GUI.DLL***–interface to enter the password to the key, random number generation by using the mechanism of "electronic roulette";
- ***PKCS11INI.EXE***–initialization of virtual slots and tokens for the interface PKCS # 11;
- ***CSPCON.DLL*** – dynamic library to support the operations of export and import the private keys in a format PFX.

Note. KEYMANAGER.EXE program and its two supporting dynamic libraries are intended to test the operation with the CSP certificates and private keys.

Interface CSP "Working with key information" PKCS # 11 is implemented in the form of three dynamic link libraries PKCS11.DLL, SCTOKEN.DLL and VTOKEN.DLL, which are placed in the system directory WINDOWS \ SYSTEM32. In addition, executable PKCS11INI.EXE, designed to create a virtual slots and tokens for the interface CSP "Working with key information" PKCS # 11, GUI.DLL - interface to enter the password to the key and random number generation by using "electronic roulette."

The mechanism of "electronic roulette"

To initialize the sensor, a source of external entropy - mechanism "Electronic Roulette" (biological random number) is used. \
For the implementation of the "electronic roulette" is used software module *GUI.DLL*. The first call to a software random number generator with the "electronic roulette" removed 32 bytes - initialization vector software random number generator. In this implementation of the CSP we used BioRandom - function from the library *GUI.DLL*. The source code for the procedure call "electronic roulette" is given below.

```
typedefint ( * BioRandomFn )
(
 OUT LPBYTE lpbDest,
 IN DWORD dwNumberOfRandomBytes,
 IN HWND hParent
);

#define ROULETT_DLL_NAME "GUI.DLL"

BOOL RAND_seed(constvoid *buf, intnum)
{
BioRandomFnMyBioRandom;

 HMODULE hRoulett =
LoadLibraryEx(ROULETT_DLL_NAME,NULL,LOAD_WIT
H_ALTERED_SEARCH_PATH);
if(hRoulett == NULL)
return FALSE;
MyBioRandom =
(BioRandomFn)GetProcAddress(hRoulett,"BioRandom");
if(MyBioRandom == NULL)
return FALSE;
intretNum = MyBioRandom((LPBYTE)buf,num,NULL);
FreeLibrary(hRoulett);
return(retNum == 0);
}
```

When you create a cryptographic key, you are prompted to enter the password for the key CSP (Figure 2).

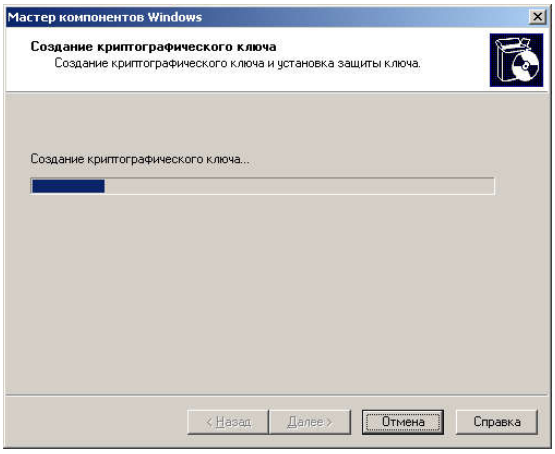

Fig. 2. Creating a cryptographic key

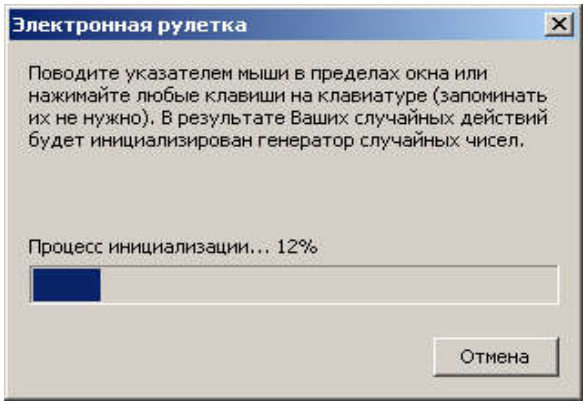

Fig. 3. Electronic roulette develop cryptographic key for the CA

Enter the password corresponding to the pin code of the token public, installed by default when you install a package CSP. You must check the box "Save password" to issuing certification authority for each new certificate did not require a password for this key.

Then, with the help of electronic roulette develop cryptographic key for the CA (Figure3).

Then follow the standard instructions that appear on the screen during installation certification authority.

REFERENCES

Aloev, R.D., Nurullaev, M.M., Alaev, R.X. 2013. Development of a cryptographic provider, based on national standards. Bulletin of the National University of Uzbekistan 2 32–35.

Aloev, R.D. Program Structure CSP. Materials Science and Engineering Conference" Applied Mathematics and Information Security". 28-30 April, Tashkent 2014. 302-306.

GOST 19.201-78: Unified software documentation. The terms of reference, the requirements for content and design.Re-release (November 1987). with Amendment number 1, approvedin September 1981.

O'zDSt 1092:2009 - Information technology. Cryptographic protection of information. The formation and verify digital signatures.

O'zDSt 1106:2009 - Information technology. Cryptographic protection of information. Hash function.

O'zDSt 1105: 2009 - Information technology. Cryptographic protection of information. The data encryption algorithm.

GOST R 28147-89 - Information Processing Systems. Cryptographic protection. Cryptographic transformation algorithm. 1989.

GOST R 34.11-94 - Information technology. Cryptographic protection of information. Hashfunction. 1994.

GOST R 34.10-2001 - Information technology. Cryptographic protection of information. The formation and verify digital signatures. 2001.

RFC 4357 - Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms.

PKCS # 5 v2.0: Password-Based Cryptography Standard. RSA Laboratories. March 25, 1999

****