

A MODEL OF SOFTWARE CRYPTOGRAPHY SYSTEM FOR DATA PROTECTION IN DISTRIBUTION INFORMATION SYSTEMS

Dr. Veselin Tselkov
State Commission on Information Security

And Dr. Nikolai Stoianov
Defence Advanced Research Institute

Abstract: This paper presents a model of software cryptography system for data protection in Distribution Information Systems. The architecture, functional features and components of the system are explained. The solutions for files, e-mail and web protection are presented. The solutions comprise the authors' experience in development and implementation of systems for information security in the Automated Information Systems of Bulgarian Armed Forces.

Keywords: computer security, information security, cryptography, cryptographic software, data protection, file security, e-mail security, web security.

1. INTRODUCTION

The development of Internet as the biggest world network puts it in the basis of the Information Society. The number of corporate systems based on the Internet technologies is gradually increasing. This leads to a rise in the threats and attacks to the corporate Intranets. That's why the problems of security become more serious and more actual.

The architecture of a corporate Intranet consists of nodes (local networks from workstations, servers, and communication devices) and internetworking communications [3].

We can point out development of defensive technologies such as:

- firewalls;
- virtual private networks (VPNs);
- traffic management;
- network management and audit;
- applications management and audit;
- intrusion detection systems;
- identification and authentication;
- encryption.

Cryptographic algorithms and mechanisms (symmetrical and asymmetrical) are the basis of almost all defensive technologies. In a significant part of commercially distributed products and technologies there are either government restrictions on the use of cryptographic mechanisms (for example, there are restrictions to the length of the keys in the United States) or necessity of receiving special licenses allowing their purchase [5, 6].

The requirements for using their own cryptographic systems are needed for corporations with top secret data.

CSSW is a solution for cryptographic software to protect the information in a corporate Intranet.

2. THE BASIC CSSW SERVICES

CSSW [8] is a Windows based model of software system for cryptographic protection of data in distribution information systems. CSSW uses symmetrical and asymmetrical algorithms and provides the following services [1, 2, 7]:

- identification and authentication of users;
- identification and authentication of applications;
- cryptographic protection on file and block data levels;
- digital signature;
- access control to cryptographic functions;
- logs;
- cryptographic application program interface (CAPI).

3. ARCHITECTURE OF CSSW

CSSW consists of the following modules (fig. 1):

- Crypto Machine (CM);
- Crypto Application Program Interface (CAPI);
- Local Crypto Server (LCS);
- Global Crypto Server (GCS);
- Security Administration and Control Center (SACC);
- Crypto Keys Distribution and Management Center (CKDMC);
- Security Applications.

Descriptions

Crypto Machine

The Crypto Machine is a system process, working on all workstations and servers. It is an OLE Automation Server providing access control and CAPI.

Crypto Application Program Interface

Crypto Application Program Interface is included in Crypto Machine. It provides a set of cryptographic functions to user applications, which must be developed as an OLE Automation Client.

Local Crypto Server

There is a Local Crypto Server in every node. LCS consists of:

- Crypto Container (CC). CC is a storage for cryptographic keys, system tables and logs of all users in its node;
- Crypto Requests and Keys Exchange (CRKE). CRKE realizes interactions in processes of key requests and exchange.

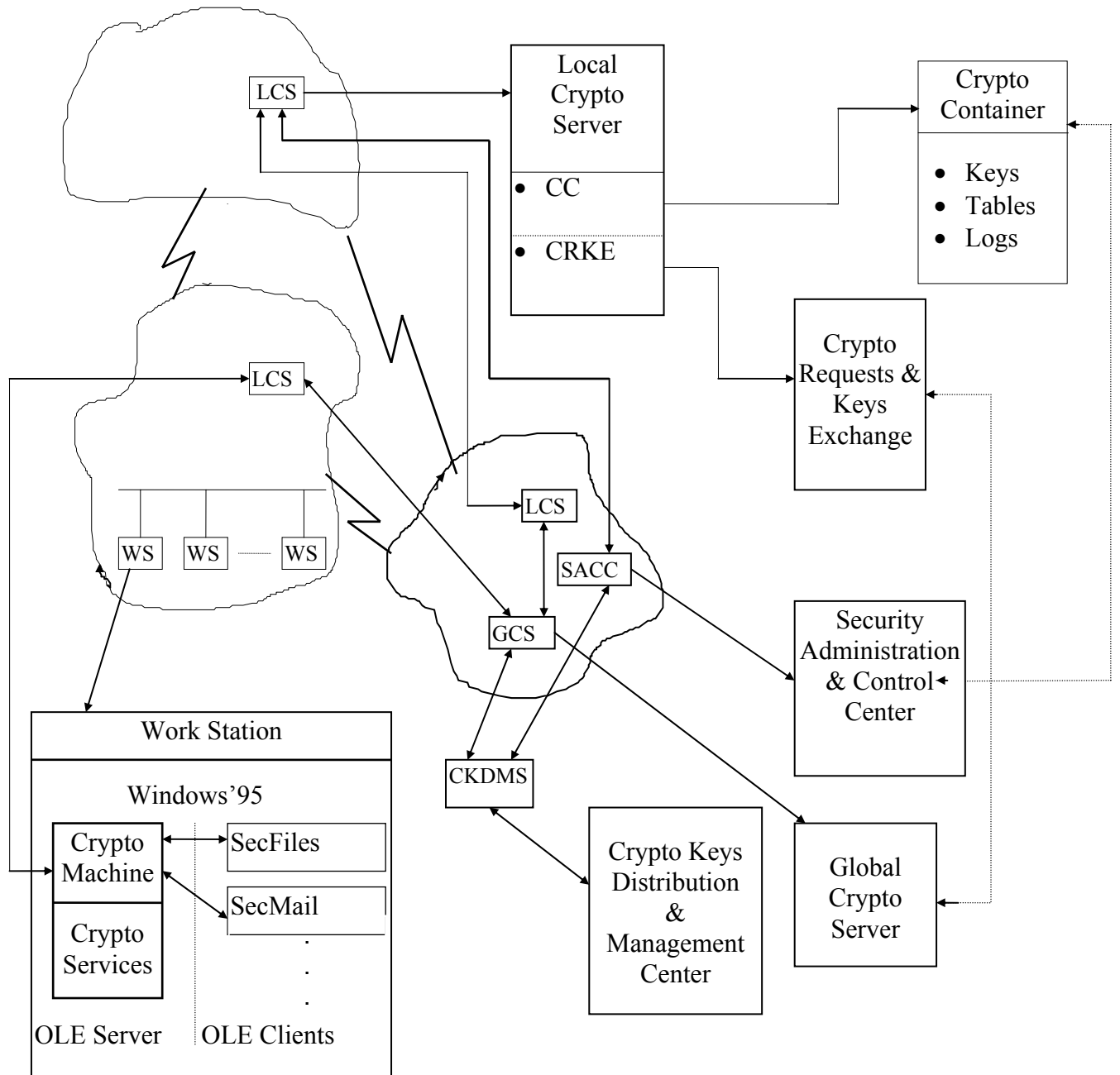


Fig. 1. Architecture of CSSW

Global Crypto Server

The module Global Crypto Server executes requests for cryptographic keys and manages their distribution. It is only one for the whole corporate Intranet and controls all Local Crypto Servers.

Security Administration and Control Center

The module Security Administration and Control Center administers and controls the executed tasks with the system CSSW. Connected with all LCS, SACC summarizes and analyzes the information of all logs.

Crypto Keys Distribution and Management Center

Crypto Keys Distribution and Management Center generates, distributes and manages keys and passwords. It is connected with GCS.

Security Applications

CSSW is an open system for designing and developing information security applications. Some of its typical applications are disk, directory, file, e-mail, clipboard, or data base protection. Based on Microsoft standards, all of CSSW's applications can be integrated with Microsoft products (MS Office, for example).

4. ORGANIZATIONAL STRUCTURES

CSSW works due to the following structures:

- Administration and Control Center (ACC);
- Key Distribution and Management Center (KDMC);
- Security administrators (SA).

Administration and Control Center

SACC works in the ACC. SACC executes:

- definition of users, resources, and access rights;
- definition of schemes for information interactions;
- correspondence with KDMC;
- control of the state of CSSW;
- detection and reaction to destructive events;
- control of logs and audit.

Key Distribution and Management Center

KDMC generates keys and passwords according to the definitions by SACC.

Security Administrators

SA supports LCS (GCS) in the node by:

- defining users, resources, and access rights in the node;
- defining schemes for information interactions;
- configuring LCS;
- supporting cryptographic tools;
- installing and administrating both user's and LCS's software;
- corresponding with ACC;
- detecting and reacting to destructive events;
- controlling logs and auditing.

5. CSSW DESCRIPTION

CSSW description includes description of nodes, workstations (users), applications, and groups of keys for each application. For each workstation the applications, which will use the cryptographic functions of the Crypto Machine module and the accessible (to this application) groups of keys are described.

Each workstation needs:

- a list of security applications working on this workstation;
- a list of available groups of keys for each security application.

CSSW tools

Depending on its use CSSW tools are separated as follows:

- software tools for a workstation;
- software tools for a SA;
- software tools for the KDMC;
- software tools for the ACC.

Software tools for a workstation

The software tools for a workstation include:

- Crypto Machine;
- Security Applications.

Data exchange between Crypto Machine and security application is based on the standard Windows interface - Object Linked and Embedded (OLE). The Crypto Machine is an OLE Automation Server and security applications are OLE Automation Clients.

Each application, which uses the Crypto Machine is identified and authenticated. If this is done successfully, the application receives a list of available groups of keys and continues to work normally.

Every Crypto Machine writes the executed tasks in a log file. The log files can be accessed from the ACC or SA

6. SECURITY APPLICATIONS

The Security Applications of CSSW presented in this paper are as follows:

- File protection [1];
- E-mail protection;
- Web protection;

"File protection"***Functional abilities***

The application "File protection" provides abilities for:

- File encryption;
- File decryption;
- File precryption;
- View;
- File state;
- Log files;

Preparation for work

Beforehand preparation of "File protection" includes:

- defining users;
- defining group cryptographic keys;
- Generation, distribution and installation of system and key materials.

"E-mail protection"

The application "E-mail protection" provides abilities for:

- Messages encryption;
- Messages authentication;
- Sender identification;
- Non repudiation.

Functional abilities

The application "E-mail protection" provides abilities for:

- E-mail protection;
- Common address book;
- Audit and control.

Level of protection

Protection of e-mail covers all elements of the e-mail:

- Subject;
- Text (basic message);
- Attachment files (documents, tables, images, etc.).

Architecture of "E-mail protection"

Architecture of "E-mail protection" consists of the following modules (fig. 2):

- End user module, including Plug-in for MS Outlook and application Security Mail;
- E-mail support module;
- Audit and control module;
- Crypto keys distribution and management module.

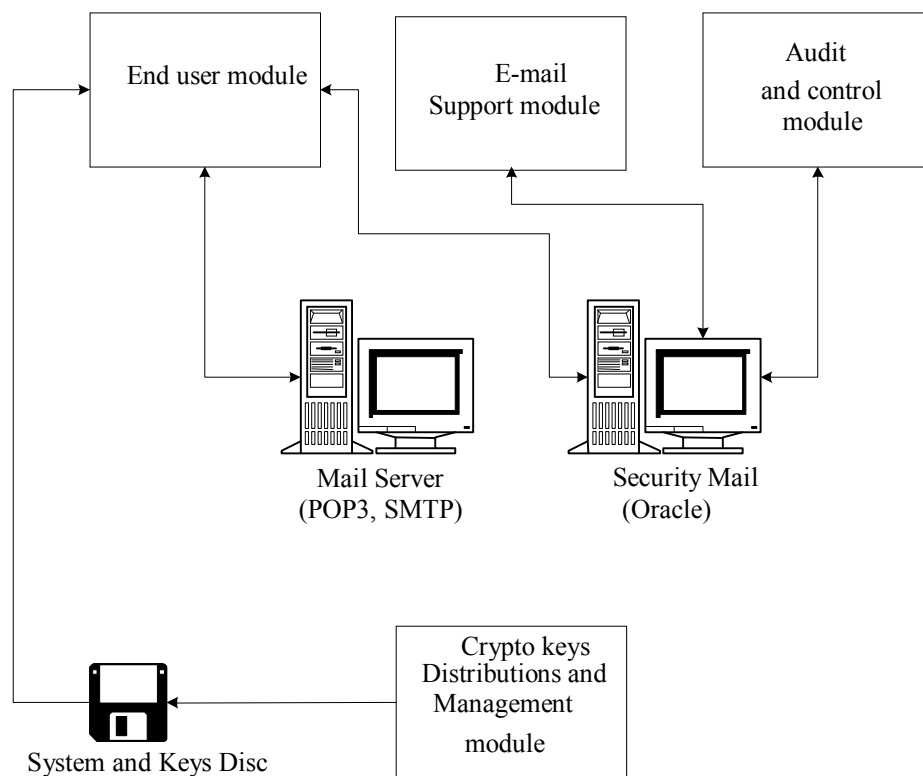


Fig. 2 Architecture of application "E-mail protection"

End user module

End user module consists of the followings:

- MS Outlook;
- Plug-in module and SecMail

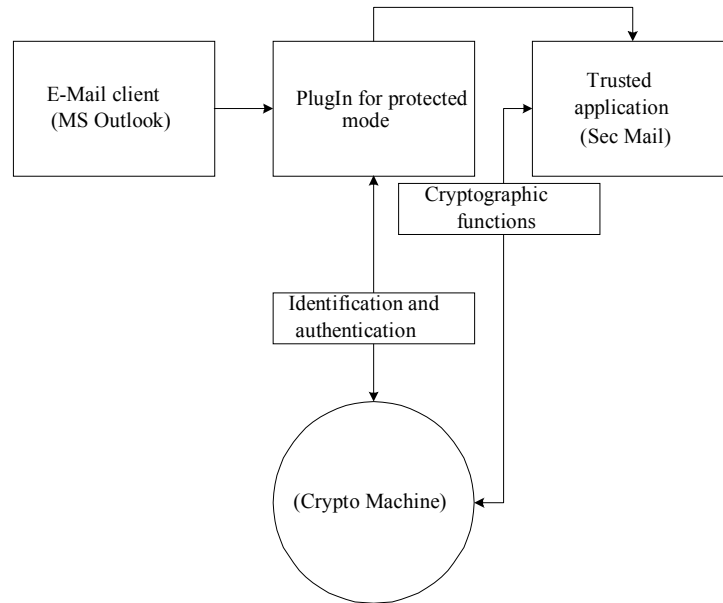


Fig. 3 Architecture of "end user module"

Technology of application "E-mail protection" work is shown on Fig.4

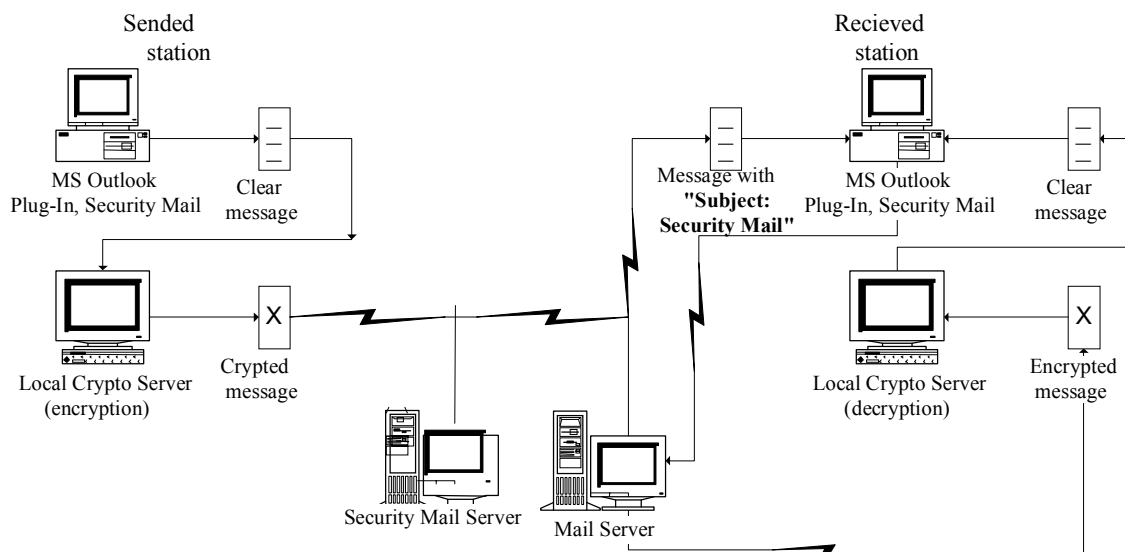


Fig. 4. Scheme of technology of application "E-mail protection"

Web protection

Functional abilities

Functional abilities of the application "Web protection" are:

- Development and publication of protected web pages;
- Identification and authentication of protected web server;
- Identification and authentication of users in protected web server;
- Authorizing user's access to protected web pages;
- Trusted communication between user and server;

- Audit and control of user's access.

Level of protection

Protection of web covers all elements of the e-mail:

- Contents;
- Parameters;
- Linked files (documents, tables, images, etc.).

Architecture of "Web protection"

Architecture of "Web protection" consists of the following modules (fig. 5):

- End user module, including Plug-in for MS Internet Explorer and application Security Web;
- Module for development and publication of protected web pages;
- Module for user's identification and authentication in protected web server;
- Audit and control module;
- Crypto keys distribution and management module.

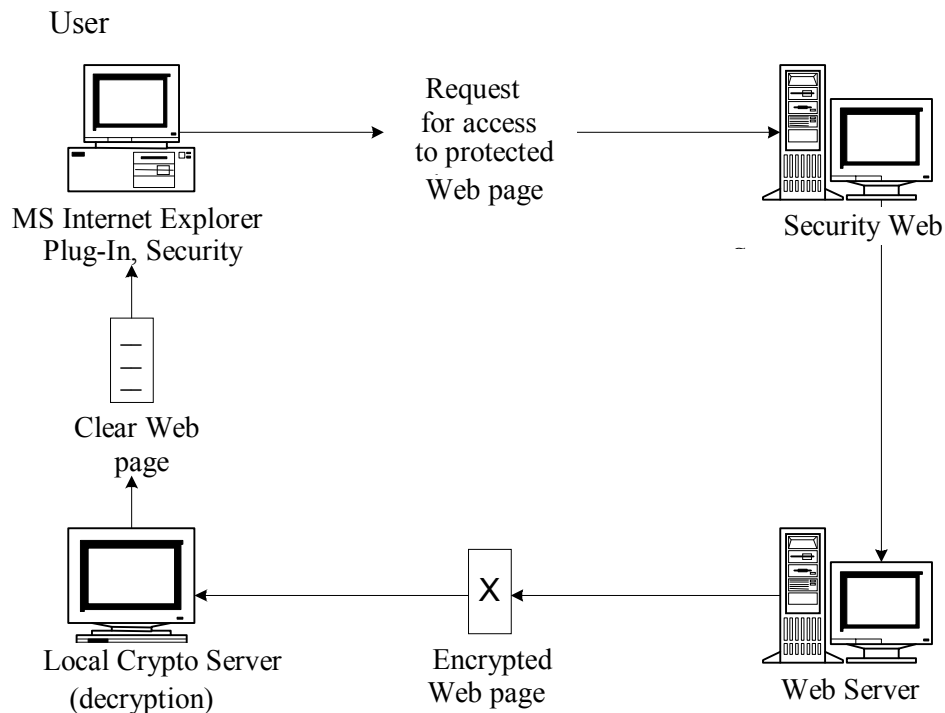


Fig. 5 Architecture of "Web protection"

Technology of "Web protection" work

Technology of "Web protection" work is as following:

- System initializing;
- Development of non-protected web pages;
- Defining access levels of each page;
- Protection (encryption) of each page with according cryptographic key;
- Publication of protected pages;
- Development of access control lists;
- Access to protected pages;

- Logs of actions on protected pages;
- Logs of actions of users;
- Audit, control and analysis of system's actions.

CONCLUSION

CSSW was designed on DELPHI and based on DBMS ORACLE. It was applied in projects of the Defence Advanced Research Institute of the Military Academy "G.S. Rakovski".

REFERENCES:

1. V. Tselkov, etc., A software security tools for information protection in PCs – “CS_SECURE_TOOLS”, The First National Conferences “JNFORMATIC’94”, Sofia, CAI, 1994, pp. 235-240.
2. D. Pargov, V. Tselkov, etc., Security in the Computer Systems, Information Aspects of Security and Development of Modern Societies, AFSEA Sofia, 11 - 13 September 1996, pp. 93-98.
3. V. Tselkov, etc., Security of Information System on Internet, AFCEA, Sofia, 4-5 December, 1997, pp. 40-48.
4. M. Cantu, Mastering Delphi 5. , Sofia, Softpress, 2000.
5. Br. Schneir, Applied Cryptology, John Wiley & Son, Inc., 1996.
6. RSA, <http://rsa.com>.
7. Deborah Russell and G. Ganemi, Computer Security Basics, O’Reily & Associates, Inc., 1991.
8. V. Tselkov, Cryptographic Solution for Information Protection in a Corporate Intranet, Information & Security, vol. 4, 2000, ProCon Ltd., Sofia, pp. 97 - 104.

Dr. Veselin Tselkov
Associate Professor
State Commission on Information Security