On the Problems of Centralized Security Management

Petr Ogrocki
petr.ogrocki@vabo.cz

Department of communication systems management
Military Academy
Brno, Czech Republic

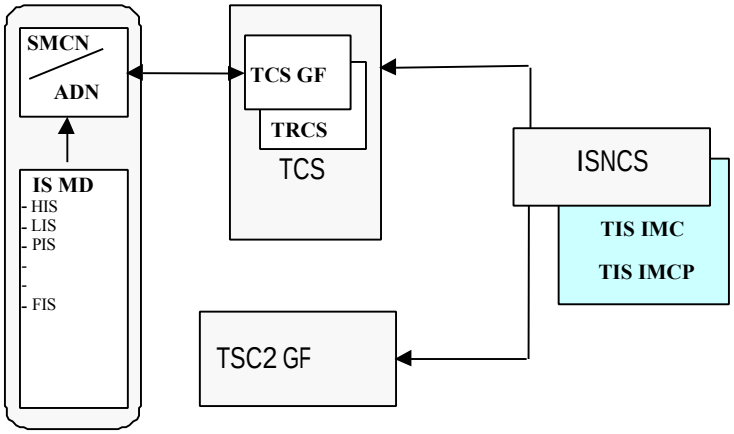
Abstract

This paper is dealing with problems of centralized security management. The first part is dedicated to two development phases, which cohere with implementation of cryptography security mechanisms into tactical information systems. The first stage represents activities connected with planning of communication and information security, especially activities, which are based on planning and applying of cryptography subsystems. The second stage describes problems of separate cryptography system, which have their own key management, planning and supervision. This section deals with location of Tactical Security Control Point, its tasks, equipment and it recommends suitable measures for building Tactical Security Control Point. The second part of the article explains activities connected with the program of the integrated control of cryptography protections for tactical command level. The system of integrated control, which is described in this part, simplifies planning activities. It provides very effective planning and management of cryptography protection on the tactical command level by preserving essential mobility. At the end, there are useful recommendations for the Czech Army tactical systems concerning automation of security control.

Keywords: security management, cryptography system, Tactical Security Control Point.

1. Introduction

Considering problems of security management for automated control of tactical communication within the Integrated System of Administration and Control of Tactical Information System the article is searching for a new method. This method could be used for planning, management, and audit of tactical information security system without further remarkable requirements for technique and personnel. The aim is as follows: to support both mobility and operability of security subsystems, which can only be achieved via consistent automation of routine activities. Cryptography is the main tool for information protection within TIS. It is important for entire communication and information infrastructure. There is one fact which we should take into consideration: tactical information systems, unlike the Stationary Military Communications Network / Army Data Network as well as information systems working in that environment, have to provide a reliable operation under dynamic conditions which have been continuously changed day by day. TIS must stay in operation even in situations where considerable disintegration of particular large units and formations is anticipated being a part of isolated implementation. There are similar requirements for security technologies implementation within TIS, where cryptography plays the most critical role. TIS Cryptography, unlike stationary Communication and Information Systems, must be much closer interconnected with communication and information systems implementation, and must be able to follow the changes in the course of tactical operations. It is required to be operable in case the TIS is separated into single fragments. Therefore it becomes necessary to include such issues as: activities associated with planned implementation of security technologies, its management and function check-ups which should not complicate the process of current changes within TIS, and, at the same time, the intended security functions could be kept.



Legend:

SMCN/ADN	Stationary Military Communications Network / Army Data Network
IS MD	Information Systems of Ministry of Defence
HIS	Headquarters Information System
LIS	Logistics Information System
PIS	Personnel Information System
FIS	Finance Information System
TCS	Tactical Communications System
TCS GF	Tactical Communications System for Ground Forces
TRCS	Tactical Radio Communications System
TS C2 GF	Tactical System of Command and Control for Ground Forces
ISNCS	Integrated System and Network Control System
TIS IMCP	TIS Integrated Management of Cryptography Protection

Figure 1. Position of TIS Integrated Management of Cryptography Protection in Integrated System and Network Control System.

In compliance with Fig. 1 it is possible to find out the solution of the Integrated Management of Cryptography Protection within TIS as a managing element operating in parallel to the Integrated System and Network Control. This separated parallel affiliation is necessary considering the information security rules. The entire integration of both service and security functions results in security degradation, and contradicts the law. Both control systems must be in close interaction and co-operate, however, not substitute one for another. The paper does not deal with further aspects of TIS information security. These problems have been solved as an integral part of individual TIS information systems, and possible solutions are included in a security project.

2. Implementation of cryptography protection into tactical information system

This chapter presents a flow chart, which characterises function and activities related to implementation of cryptography security aspects into tactical information system. The flow chart in Fig. 2 demonstrates that presented activities are divided into two steps. This arrangement results from technical properties of individual cryptography subsystems, which considerably restrict the chance of both unified management and key management.

Step **I**, characterised by activities related to planning, can be shared by every system. Step **II** will be divided according to encryption subsystems used. There will always have to be considered a specialised human factor on the step **I** and **II** interface.

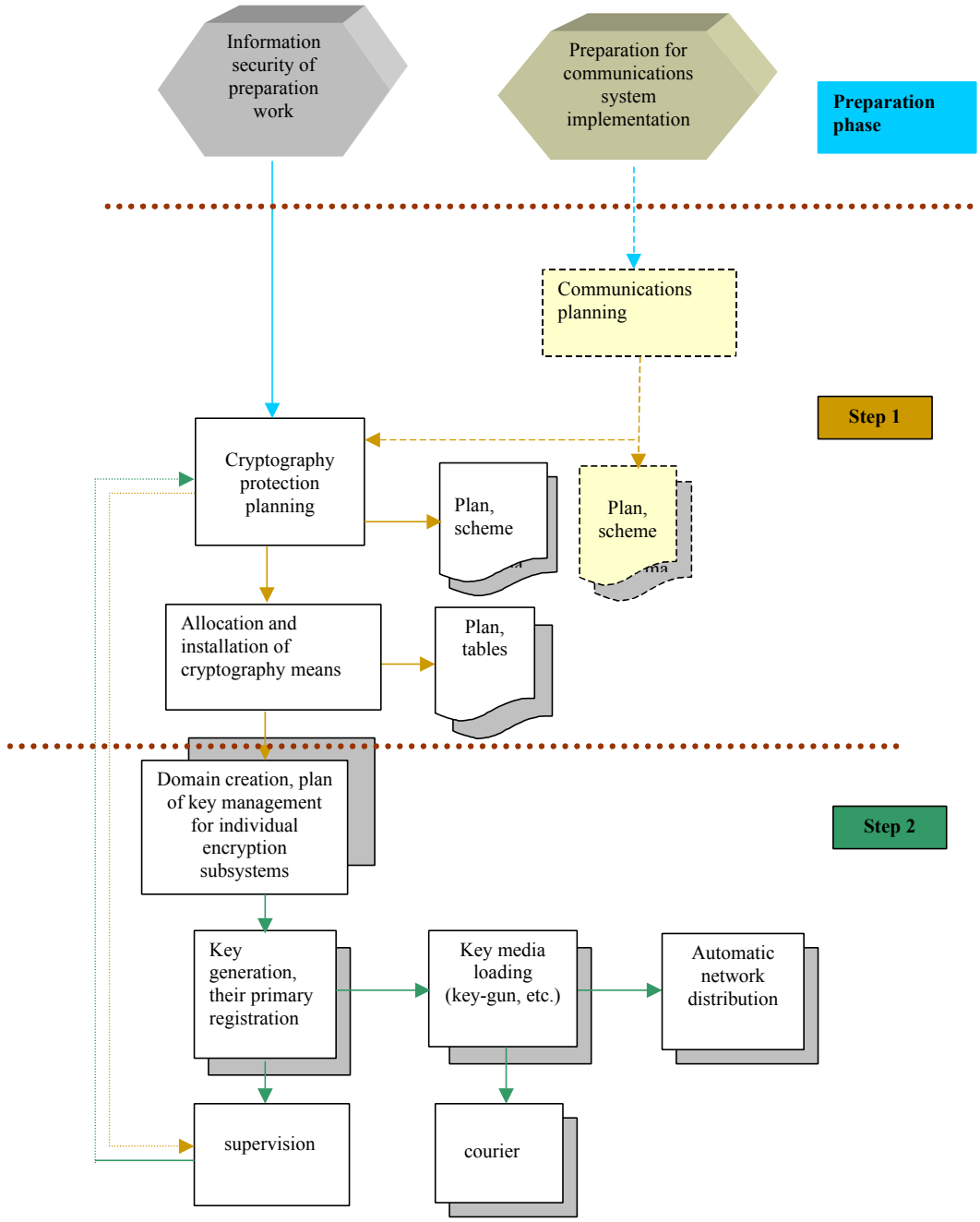


Figure 2. Flow chart of functions related to cryptography protection application within TIS information system.

Step I:

This step can be characterised as the step aimed at planning when the security body - planner - considers communications environment planning documents, and having resulted from them he himself creates a plan with implemented cryptography subsystems. Regarding the SW tools availability, this activity can comparatively easy be automated, i.e. it is possible to create network graphic documents, charts, domains, etc. via a machine script. Having passed a certain modification there can also be used program tools ”COMNET”, ”net VIZ”, etc. In case it is simultaneously used for projects both in communications and security sections of this step, its application is efficient. You will also succeed if there is close (personal) co-operation between Communications and Information Systems planners and security subsystems planners.

The decision concerning the fact whether the shared planning program is to be applied or developed should be made within the approval procedure of TIS development results or before the work on security project starts.

Step II:

This step has always consider the fact that the entire cryptography subsystems were, are and will be purchased or developed as independent systems with their key management and their planning and supervision programs. Unfortunately, there can hardly be found shared points which could enable a uniform computer administration of a key management and supervision; it proved necessary to consider that fact.

Therefore this step will have to consider the fact that every encryption subsystem will have a separated key management and its own way how to distribute and implement keys and get audit reports.

There is the only way-out of that situation: to install the set of control programs into one efficient computation system (HW base integration only). That mentioned integration can be serviceable considering the mobility of the security management centre, and it can comparatively easy be carried out.

The supervision program development is a good chance how the audit results from single cryptography systems could be integrated, and the security officer in the centre would be able to control security and monitor situation in encryption subsystems. The security subsystems supervision efficiency requires close (personal) co-operation with relevant supervision body for Communication and Information control Systems.

It is necessary to find a solution for the step II and at the same time make a decision where the security management centre for tactical level is to be located. For the time being the optimal solution results in centre set-up on the brigade level as this position provides enough means and manoeuvrability for possible changes within security structures which may call for inevitable changes regarding subordinate units during combat activities. We can take it for granted that on that level there will also be possible to monitor those changes via a cryptography technique and key management without considerable problems.

Efficient supervision of cryptography subsystems is in charge of security management centres which are being created. Information concerning cryptography subsystems operation and function varies for individual subsystems and this fact cannot be efficiently modified. The best possibility for integrated supervision and management are only provided by data systems which are arranged for centralised operation. There is a completely different situation in case of tactical radio cryptography protection, since the communication environment itself and its cryptography protection eliminates conditions for central management in fact.

The supervision centre is integrated into shared HW configuration.

The established TIS security management centre will be represented with one computation centre (workstation) which, in fact, will consist of three modules:

- Program for network information security planning
- Set of programs (of companies´) for key management planning for individual cryptography subsystems (bulk encrypts, IP encrypts, text encrypts, radio security equipment, ciphonies, etc.) which are always included in supplies of single purchased cryptography systems.
- The program of security management centre supervision which integrates audit reports on individual encryption systems and gives a comprehensive survey how cryptography protections can operate. Resulting from this fact, it is necessary to design a program as follows: the program shall be a penetration of a file of audit reports and specific parts from the networks information security planning program, particularly graphic ones.

Referring to that, it becomes necessary as follows:

1. to have control over tenders for encryption subsystems for ”BULK” encrypts, ”TCP/IP encrypts,” ”ciphonies” so that there could be possible to meet one of requirements, i.e. to integrate the key management and supervision program into the expected integrated supervision program of the TIS cryptography protection,

2. to start to develop the specified software, however, the agreement with encryption subsystems suppliers has to be made in advance, so that their software products designed for Key Management could be integrated into software which is being developed.

3. Characteristics of program of integrated management of cryptography protection for tactical information system

The principle of integrated management of cryptography protection results from closed co-operation between the planners for Communications and Information Systems and security (Fig. 3). It is necessary to keep in mind the fact that both planners have the same software available, which is on-purpose aimed so in information and communication planning systems, and their final product consists of a communication plan (scheme) which is based on digital geographical map and further necessary charts. The communication plan, or its result is integrated into the security computation system of a planner and he keeps working. In the interactive mode he manually integrates single icons of encrypts and arranges interconnection including further relevant data, he specifies participants of individual domains. Resulting from data specified like that, the system generates tables with specific types of cryptography protection. The cryptography communication map is generated at the same time.

Tables with specific types of cryptography protection are simultaneously transferred via a program boundary **I** on inputs of individual key management program (1,2,…..,n) relevant to specific types of cryptography technique used. These modules are run by an operator (new key generation, system function monitoring, etc.), modules for some types of cryptography systems are run at intervals so that partial audit reports could be obtained. These audit data are summarised in the audit integration program segment, which is, in addition, supported by manual operator input, and the audit is supplemented with further relevant information from the systems whose automatic audit is hardly possible. The transfer between single audit outputs and program audit integration segment is carried out via a program boundary **II.** This segment output is further processed in a module of output audit periodic recovery which controls the interval of individual cryptography subsystem check-up; the summarised results of audit reports are presented on the display, printed and the database of it is made on HDD.

The integrated management of cryptography protection is characterised only in general plan considering the complicated implementation itself. While looking for the solution, there is highly desirable good co-operation with suppliers of individual types of security technologies which had been selected for TIS creation (as a matter of fact it is a ”joint-venture”). Special attention has to be drawn to the expert responsible for the software as he shall have professional skills concerning use of particular security technologies and key management as well. This fact, however, calls for higher demands in personnel security field.

The system of integrated management of cryptography protection, based on characteristics above, is up to certain extent able to simplify and improve operations related to cryptography subsystem management. As a mater of fact, a skilfully designed system based on the presented philosophy makes one professional expert possible as follows: efficient semi-automated management and planning of a set of several different cartography systems at real time as one unit. The advantage can be seen in comparatively low requirements regarding further hardware, space, service and staff. The characterised system is able to meet requirements for mobility and operability within tactical information system environment.

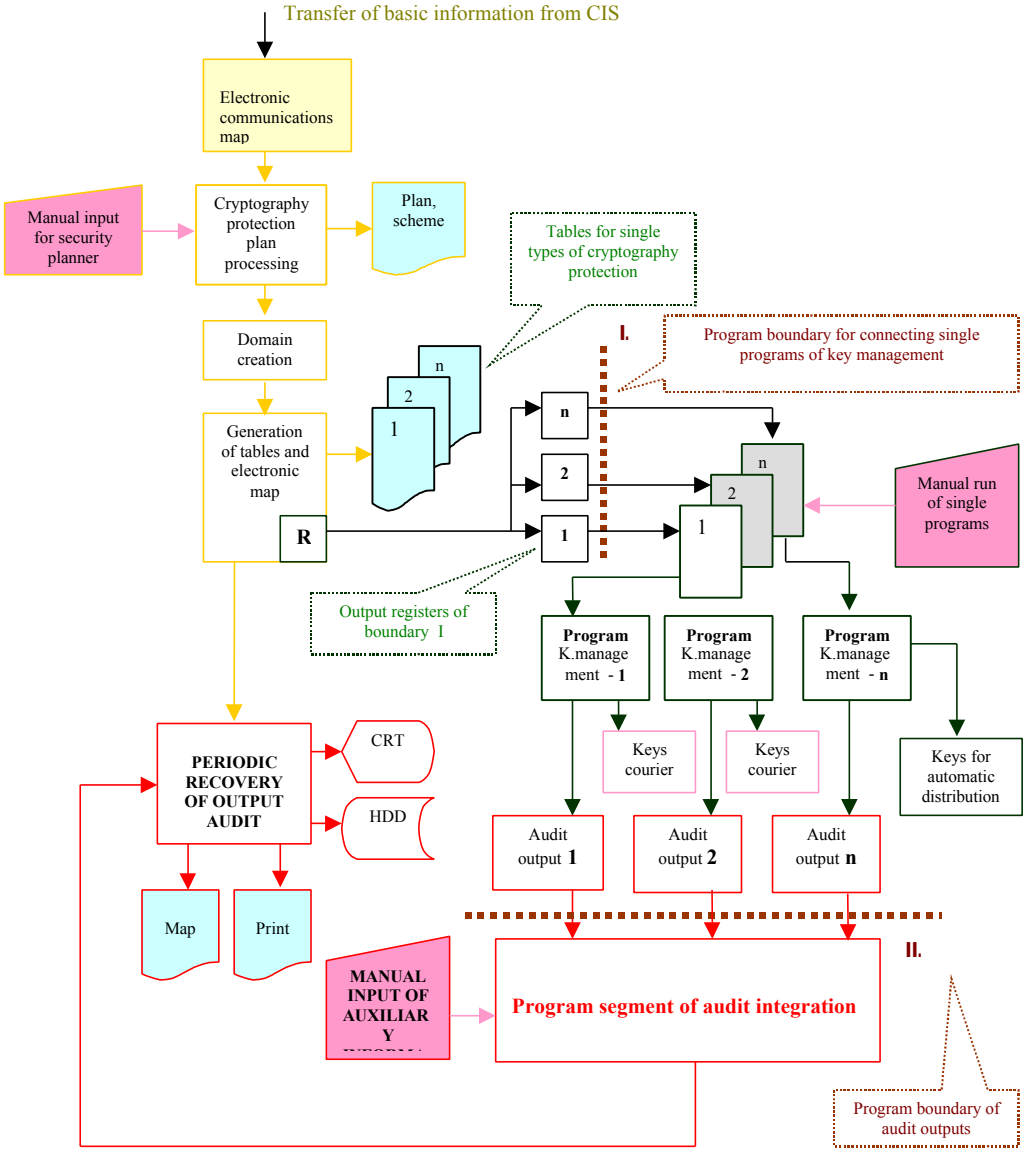


Figure 3. Flow chart of integrated management of TIS cryptography protection.

The main problem of presented integration is in variability and remarkable software advance differences of single encryption subsystems, and problems connected with co-operation with suppliers themselves.

4. Conclusions

The paper results from current situation in implementation of cryptography protection into communication and information systems within the Ministry of Defence of the Czech Republic. The author tried to search for maximum balance between costs and energy spent on the latest encryption technique and required automation efficiency. The presented solution can be characterised as the most economical since further expenditure on research and development are concentrated just on the problem how to create a new software, write the application software interface in order to interconnect current software with purchased cryptography systems and a new product. The development itself will consist of integration of manager programs of individual cryptography subsystems without ill-effects on function and cryptography principles. Fig. 3 presents acceptable way how a new program can be structured in algorithms.

In conclusion it could be said that there are other way-outs for management of systems of cryptography protection as well. They are, for example, as follows: the designed cryptography systems can be kept as autonomous, i.e. a supervision point will consist of several computation systems. The disadvantage of that solution consists in requirement for space, low mobility, more service staff. The advantage consists in low integration costs and high autonomy of individual systems. There is also another way: to integrate individual cryptography subsystems (its management segments) loaded in single devices, and the manual input of individual audit report into the cryptography protection planning program can be substituted for the application program interface. By and large, the presented solution is acceptable, however, it lacks required automation elements. Its advantage consists in higher mobility and operability of the management system.

5. References

[1] Kolektiv autoru: Spojovací systémy, Západoceská universita, Plzen, 1997.

[2] Pužman, J.: Datové služby a síte, CVUT, Praha, 1994.

[3] Kolektiv autoru: OTS VR PozS ACR, úvodní studie OTS VR PozS, kniha c.1, VTÚE, Praha, 1998.

[4] Kolektiv autoru: TAKOM PozS a VzS ACR, úvodní studie, kniha c.2, VTÚE, Praha, 1998.