Mechanics Transport Communications ISSN 1312-3823
Academic journal issue 2, 2010
article № 0471
http://www.mtc-aj.com

PROPOSAL OF KEY MANAGEMENT SYSTEM FOR ETCS LEVEL 2

Mária Franeková, Miroslav Voštenák
maria.franekova@fel.uniza.sk

University of Žilina, Faculty of Electrical Engineering, Univerzitná 1, 010 26 Žilina SLOVAK REPUBLIC

Key words: *European Train Control System, Euroradio protocol, cryptography techniques, Key Management System, symmetric cryptography, Advanced Encryption Standard, key generation, key distribution*

Abstract: *The paper deals with problems of developing Key Management System (KMS) for European Train Control System in application level 2. The solution of KMS is necessary for all cryptography procedures which are used within communications between entities of stationary and mobile parts of European Train Control System (ETCS) across Global System of Mobile for Railway (GSM –R) . Authors the proposal of KMS on the base on symmetric cryptography techniques are mentioned. In detail the possibilities of generation and distribution of keys in one domain and between ETCS domains is solved.*

1. Introduction

Incompatibility between interlocking systems in railway transport in Europe can be changed with using ETCS (*European Train Control System*), which is partook of international project ERTMS (*European Rail Traffic Management System*) [1], which is developed from 1992 in Europe. The aim of ERTMS is to create standardised European system in railway, common for all countries of EU (*European Union*), which allows transport of trains with ETCS equipment in all European railway lines. According to equipment of track side of ERTMS/ETCS we can differ the three basic application levels L1, L2 a L3 [2]. For ETCS L2 and L3 the necessary part of solution is system GSM-R (*Global System for Mobile Communications – Railway)*, which realises the radio transmission between stationary and mobile parts of ETCS system via safety cryptography protocol.

In ERTMS/ETCS L2 (see Figure 1) the train (on board unit) and RBC (*Radio Block Centrals*) exchange the information via Euroradio protocol across open untrusted transmission system. If train wants to communicate with RBC must verify if communication with this RBC is valid and oppositely. This procedure is based on concrete cryptography techniques which used secret keys [3]. Nowadays KMS for support cryptography algorithms tools for generation, distribution, actualisation of keys is not exist. There are many project under construction which developing KMS on the base of off-line and on-line base [4], [5]. It is well known that the safety of cryptography mechanisms is based on confidentiality of keys mainly. For keeping the interoperability the uniform KMS for all European railway networks is necessary to develop however it is not possible nowadays for the reason of using many different types of interlocking systems in European countries [6].

The solution of KMS in the paper is based on the assumption that the uniform ETCS system L2 is valid in all countries of Europe.

The meanings of symbol used in Figure 1 are the following:

- FFFIS *Form Fit Functional Interface Specification*
- FIS *Functional Interface Specification*
- TIU *Train Interface Unit*
- MMI *Man Machine Interface*
- JRU Juridical Recording Unit
- BTM *Balize Transmission Unit*
- LTM *Loop Transmission Module*

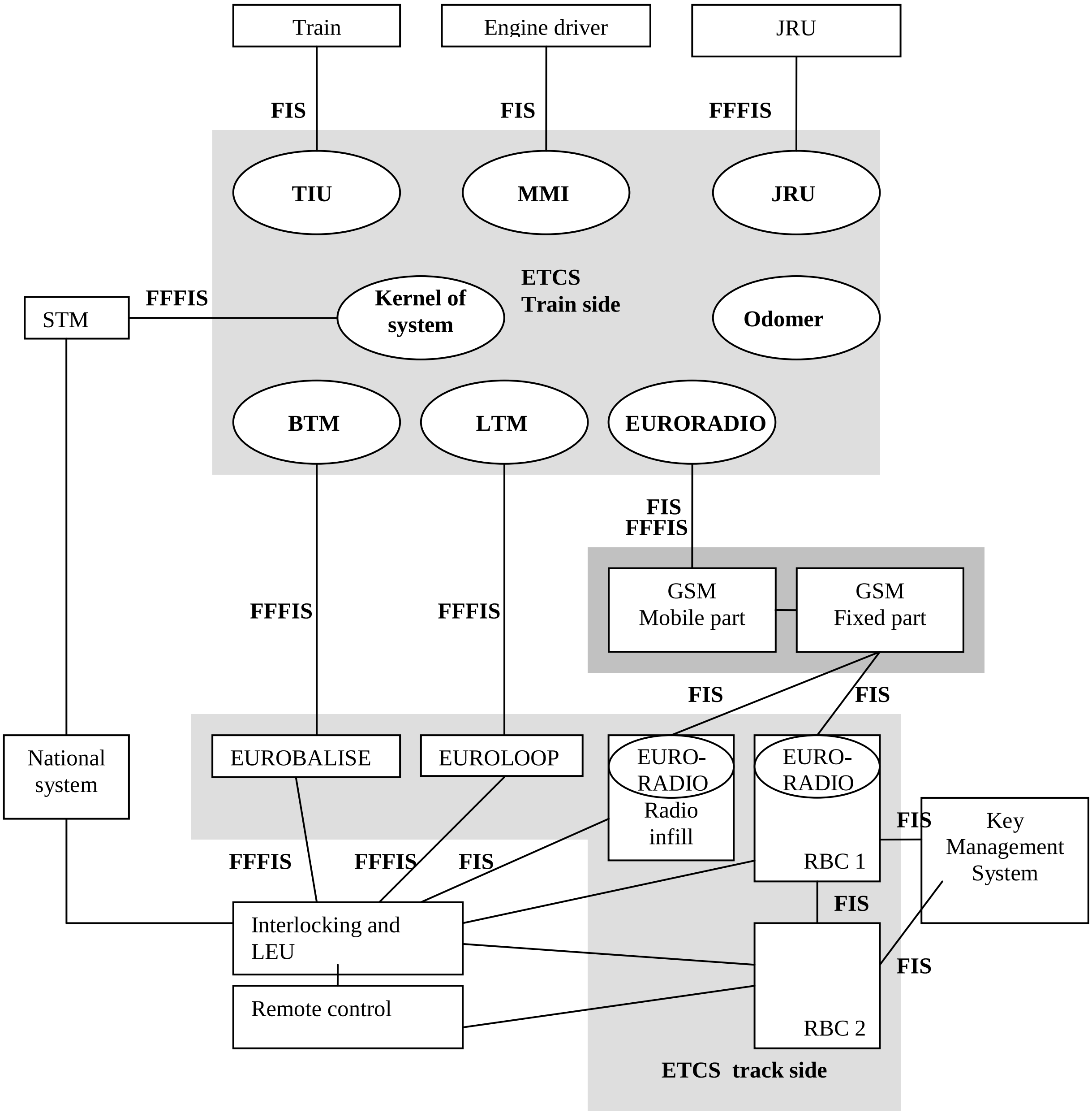

Fig. 1 Architecture of ETCS L2

2. Possibilities of KMS realisations

KMS is possible to realise via cryptography techniques on the base of symmetric key or on the base of asymmetric keys. Mostly advantages of both cryptography solutions are applied today in COTS (*Commercial of Transmission System*).

Solution on the base of symmetric cryptography assumes the existence of certification authority CA in communication network which trust all communication entities. Every entities A_i share with CA own symmetric key k_i. Assume that the keys were distributed across safety channel. If two entities wanted to communicate together than CA generates the relation key *k*, which sends in secret form to communicated entities (see Figure 2).

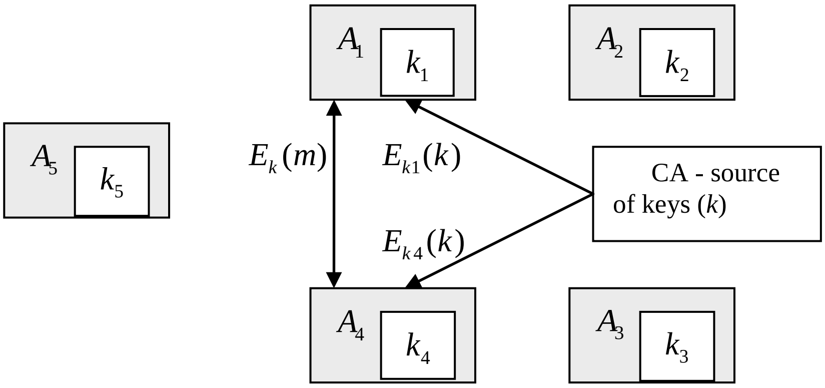

Fig. 2 KMS used certification authority

The advantages of this solution are the following:

- Connection and disconnection of subjects into network is easy.
- Every subject remembers only one secret key.

The disadvantages of this solution are the following:

- CA must remember *n* secret keys for long time.
- Every communication needs the first realise the communication with CA.
- CA is able to read all messages (risk of safety).

With the use the solution on the base of asymmetric cryptography every subjects in network owns the pairs of keys (public and secret). Public together with identity of subject are store in public list. If subject A_1 wants to send enciphering message e. g. to subject A_6 obtains from public list public key e_6 of subject A_6, then the message with using this key is enciphering and is sending to subject A_6 [7]. Key management System on the base of asymmetric cryptography is illustrated in the Figure 3.

Note: For distribution of public key there is not require secure channel

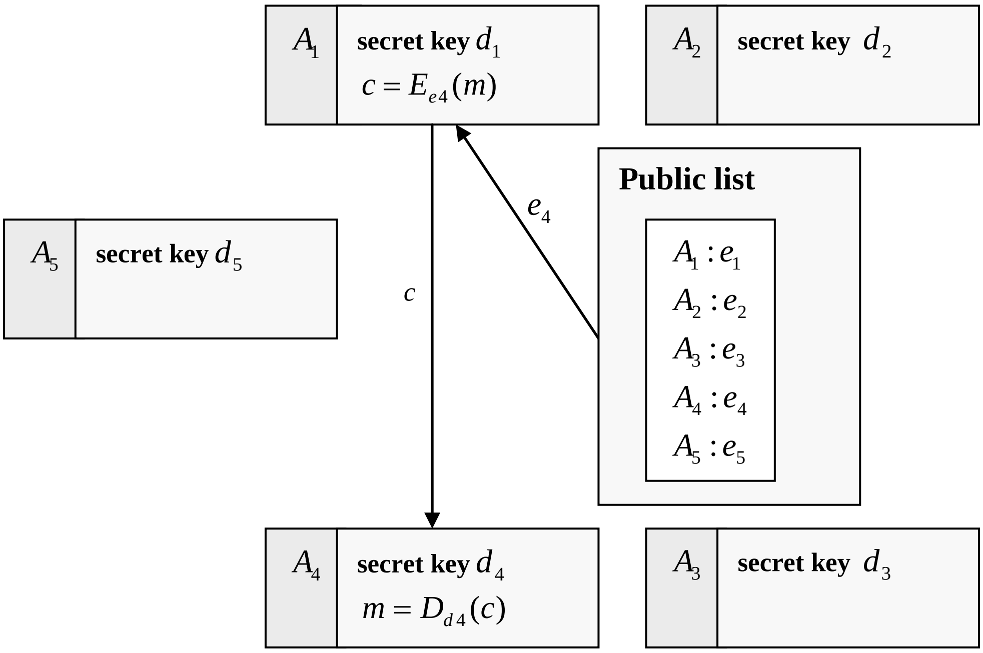

Fig. 3 KMS used techniques of public keys

The advantages of this solution are the following:

- The solution does not need CA.
- Public list can be located in every subject.
- Communication is secure (when we assume passive attack only).

The disadvantages of this solution are the following:

- The possibility to change the public list (when we assume active attack).

Note: As prevention against the active attacks we can use CA for certification of public keys of all subjects.

3. Proposal of KMS on the base of symmetric cryptography

Solution of KMS on the base of symmetric cryptography assumes the use ETCS system in level 2. Next we predicted that every communication domains have one KMS only which has the own hierarchy of keys.

Note: As communication domain the authors mean the zone of railway networks for one state.

Nowadays for data assurance is recommended to use symmetric block algorithm AES (*Advanced Encryption Standard*), which is considered as computationally safety algorithm. Algorithm has optional length of keys 128, 192, 256 bits. In solution we select the length of key 192 bits. Detail about AES algorithm we can find e. g. in [8]. The meaning of using keys within our solution of KMS is defined in Table 1.

Tab. 1 Hierarchy of keys of KMS and their applying

Key (length of key)	**Applying**
K-AKT (192 bits)	Symmetric key uses for exchange of information between two KMS domains.
K-TRANS (192 bits)	Symmetric key defines for exchange of keys *K-MAC* between home and neighbouring domain.
K-MAC (192 bits)	Symmetric key uses for enciphering / deciphering of messages between the train and RBC.

The key hierarchy of symmetric keys between two domains A and B is illustrated in the Figure 4.

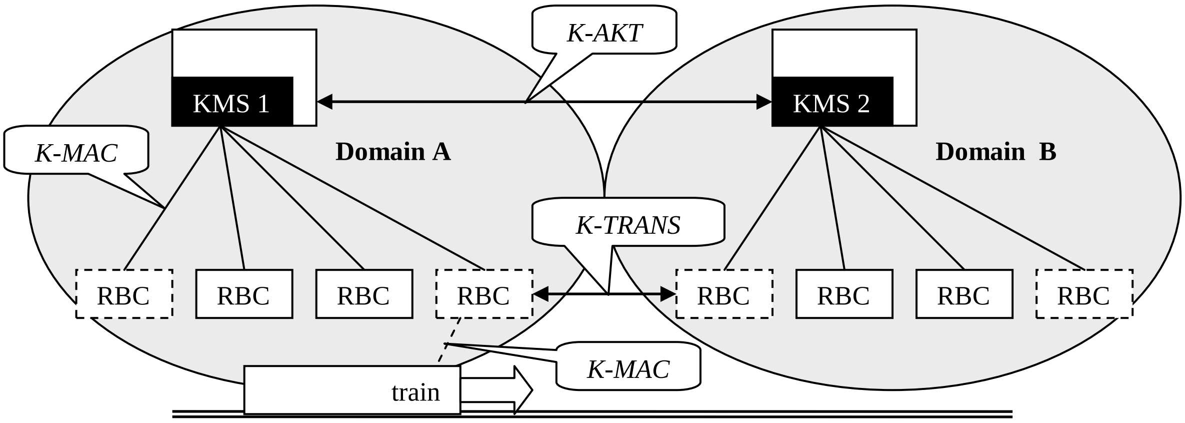

Fig. 4 Hierarchy of keys between two domains of ETCS

3.1 Solution of keys generation

Function of keys generation must be realised by justified person and by safety manner. Every generated key must be validated (finding the weakness keys or the existed keys). For this reason the function of validation of keys is located into generator of key. Designing internal structure of generating of symmetric keys is illustrated in the Figure 5.

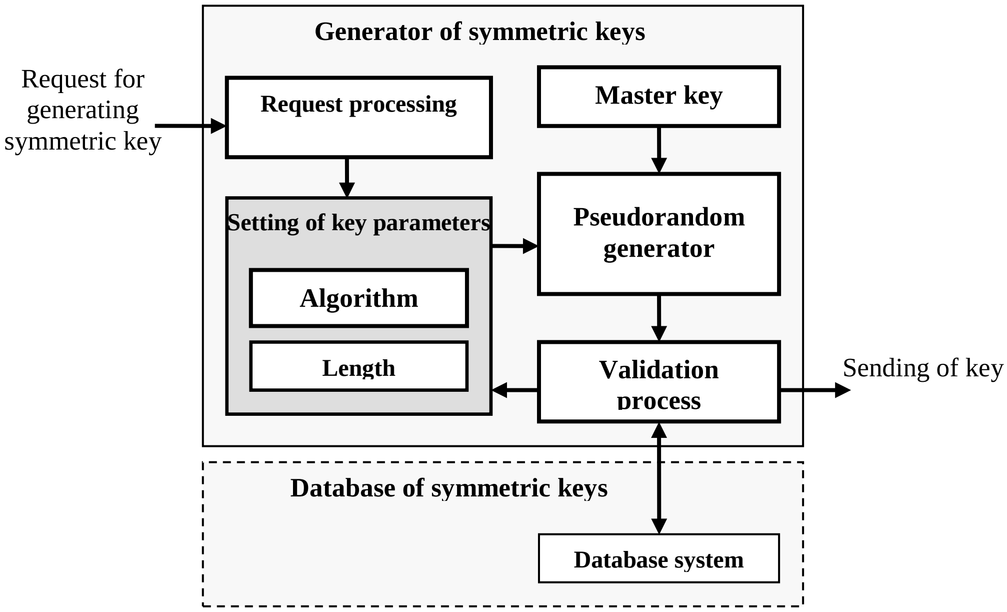
Generator of symmetric keys
Request for generating symmetric key
Request processing
Master key
Setting of key parameters
Pseudorandom generator
Algorithm
Length
Validation process
Sending of key
Database of symmetric keys
Database system

Fig. 5 Internal structure of symmetric keys generator

As it is illustrated in the Figure 5 generator of symmetric keys consist for the following parts:

- **Request processing** – this block from the message request recognizes the type of request, from which knows which types of symmetric keys have to generate (*K-MAC*, *K-TRANS* or *K-AKT*). In received message the identification numbers of subjects for which will be generating the key are located.
- **Setting of keys parameters** – this block sets the parameters for chosen algorithm AES and its required length 192 bits. (This is 48 mark chains. The valid marks are the following: 0123456789ABCDEF). Setting parameters are sent to block of pseudorandom generator.
- **Master key** – this is the central symmetric key, which justified person located into system. With the help of master key and pseudorandom generator the sub-keys will be generated as section keys (it is valid for one communication connection only).
- **Pseudorandom generator** – this generator generates pseudorandom 48 mark chains, which depends from setting of key parameters and from master key. Every key after generating is validated.
- **Validation process –** this process is realised before distribution of key to requester. During this process the key is verified (if is not weak or does not exist). In this process it is necessary to have connection with database of keys. Negative answer from database means that generated key is not valid. Positive answer means the key is valid, is stored into database of key during relation and then it is sent to user.

3.2 Solution of the keys distribution

Process of keys distribution is realised after validation for all generated keys. During realisation of KMS it is necessary to distribute the first generated keys for particular subjects. The first distribution would be realised by justified person or justified team. Installation of key facilities for particular subjects is illustrated in the Table 2.

Table 2 Keys facilities for particular subject of ETCS

	Keys		
Subjects	*K-MAC*	*K-TRANS*	*K-AKT*
station RBC	X		
end station of RBC	X	X	
train (on board unit)	X		
KMS	X	X	X

Note: KMS can contain several *K-TRANS* and *K-AKT*. The number of keys depends on number of neighbour domains.

After the first distribution of keys next keys distribution will be realised in safety manner (e. g. by key *K-MAC*) for particular RBC stations and trains. Internal structure of symmetric keys distribution is illustrated in the Figure 6.

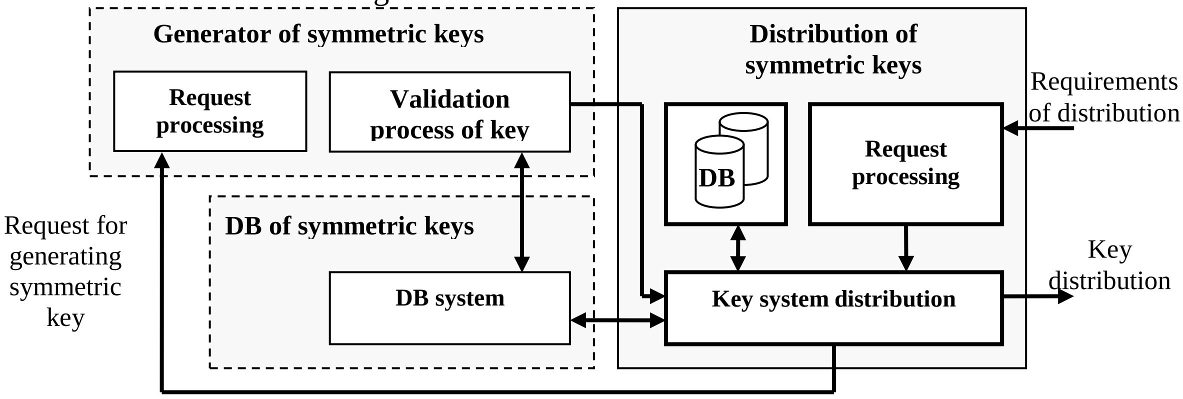
Generator of symmetric keys
Request processing
Validation process of key
Distribution of symmetric keys
Requirements of distribution
DB
Request processing
Request for generating symmetric key
DB of symmetric keys
DB system
Key system distribution
Key distribution

Fig. 6 Internal structure of symmetric keys distribution

Symmetric keys distribution consists from the following parts:

- **DB** – database in which will be stored all realised distribution for particular subjects of ETCS. Data will be used within process of actualisation or liquidation of keys.
- **Request processing** – it is the input block for receiving the requirement of key distribution. The block recognises the type of requirement of distribution (distribution of *K-MAC*, *K-TRANS* or *K-AKT*).
- **Key system distribution** – realises the following distribution operations:
  - – Distribution for particular subjects.
  - – Storage to database all realised distribution operations.
  - – To create the request for key generation.
  - – Receiving new generated keys from key generator.
  - – Receiving the key which provides to DB of keys.
  - – Receiving new key which is generated in other domain and provides it to DB of keys.

Every RBC station has in own DB the identification numbers of the trains only which have planed line across its sub domain and every train has in own DB identification numbers of RBC stations only, across them will travel (see the example in the Figure 7).

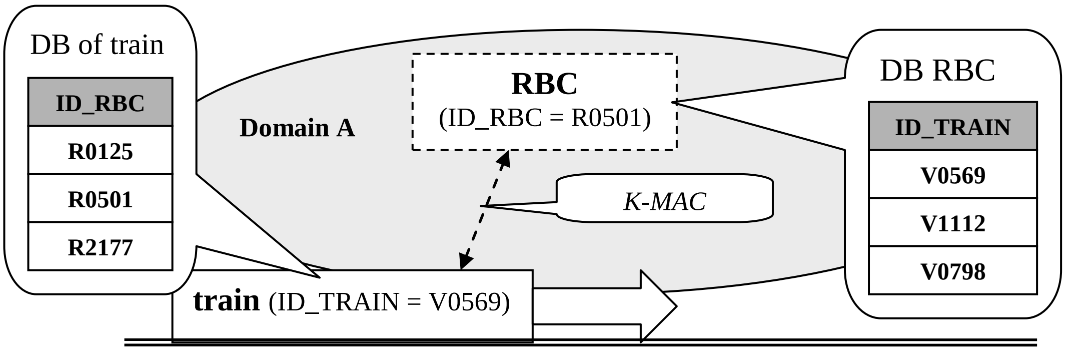

Fig. 7 Example of DB facilities of RBC station and train

4. Conclusion

For keeping of interoperability within ETCS system Level 2 or L 3 it is necessary to develop an unified Key Management System which will support all manipulation process with keys between communications entities of stationary and mobile part of ETCS (for authentication of RBC and trains during domains). KMS is very sensitive part of cryptography system especially if it is based on symmetric cryptography. According to norm valid for railway application [9] the all parts of KMS must be realised by the safety manner. In this paper the proposal of KMS system on the base of symmetric cryptography algorithms was mentioned. The authors recommend using AES standard with the length of key 192 bits. Nowadays this algorithms is resistant against all well known attracts (brute force attack and attacks to symmetric block cipher). In detail was the solution of keys generator and key distribution method described with example of process verification between RBC and train within one communication domain.

Acknowledgements

This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0023/08 "Theoretical apparatus for risk analysis and risk evaluation of transport telematic systems".

References

[1] www.ertms.com

[2] ZHRADNK J. RSTON K. : Aplikacija nad ispreplesti sistem. Textbook. više Slovak EDIS – U ilina , 2006, ISBN- 80-8070-546-1(ZÁHRADNÍK, J. - RÁSTOČNÝ, K.: *Applications of interlocking systems*. Textbook. In: Slovak. EDIS – ŽU Žilina, 2006, ISBN 80-8070-546-1)

[3] MENEZES,A. -P.van OORSCHOT, VANSTONE, S.: *Handbook of Applied Cryptography*. Textbook. CRC Press, 1996.

[4] Subset-038: *Off-line Key Management FIS*. 2005, v 2.1.9

[5] FRANEKOVÁ, M.- KÁLLAY, F.- PENIAK, P., VESTENICKÝ, P.: *Safety communication of industrial networks*. Monography. In: Slovak, EDIS - ŽU Žilina, 2007, ISBN 978-80-8070-715-6

[6] VOŠTENÁK, M.: *Key management for ETCS system*. Diploma work, University of Žilina, 2010

[7] LEVICKÝ, D.: *Cryptography in information safety*. Textbook. In: Slovak. ELFA Košice. 2005, ISBN 80-8086-022-x

[8] NIST FIPS PUB 197: *Advanced Encryption Standard* (AES). 2001

[9] EN 50159-2: *Railway applications – Communication, signalling and processing systems*. Part 2: Safety-related communication in closed transmission systems. 1998