Archives of
Transport System
Telematics

Volume 12

Issue 2

May 2019

The Importance of the Cryptographic Key Management System for the Cybersecurity of the ERTMS System

A. KOCHAN, Ł. GRUBA, E. KOPER
WARSAW UNIVERSITY OF TECHNOLOGY, Koszykowa 75, 00-662 Warsaw, Poland
EMAIL: ako@wt.pw.edu.pl

ABSTRACT
The ERTMS system is intended to provide an interoperable approach to train control and signalling in the European Union. The basis for effective train control at ETCS Level 2 is wireless data transmission via GSM-R. This transmission must be protected by cryptographic techniques to ensure its safety. The authors in their article present technical solutions and their applications related to cryptographic keys. They present the requirements that have been formulated for the cryptographic key management system. They discuss its architecture, functions and possibilities of increasing the security of management processes with the use of solutions applied in other branches of the economy. In the last point of the article attention is drawn to the threats posted by the complex process of managing a set of cryptographic keys, the number of which can be measured by tens of thousands.

KEYWORDS: cybersecurity, cryptographic keys, ERTMS/ETCS

1. Introduction

The ERTMS is a system which main purpose is to ensure the interoperability between the rail systems of the EU Member States. It consists of two components:

- ERTMS/ETCS - European Train Control System ensuring the unified Control-Command and Signalling functions, interfaces and performances,
- ERTMS/GSM-R - digital wireless communication system used for the transmission of speech and ERTMS/ETCS data.

In terms of technical solutions, the ERTMS is based on computer technology and digital telecommunication. The telecommunications solutions used in ERTMS largely use widely known standards, which apart from unquestionable advantages brings with them a number of known cybersecurity problems. These problems are multidimensional. They concern transmitted data, control of access rights, hardware configuration and working conditions.

ERTMS/ETCS on-board equipment (ETCS on-board entities) and track-side equipment (ETCS track-side entities) exchange information using the EURORADIO protocol [9]. ETCS on-board entities shall be able to authenticate the ETCS track-side entities in order to exchange data with them - confirm that they are who they claim to be. Track-side ETCS entities also must be able to authenticate on-board ETCS entities (authentication is mutual). Moreover, the authenticity and integrity of any data exchanged between ETCS on-board entities and ETCS track-side entities are verified [6, 7].

The EURORADIO protocol provides:

- identification and authentication of ETCS entities during the establishment of the secure communication session,
- authenticate the source and ensure the integrity of each transmitted message.

The cryptographic methods that assume the use of cryptographic keys are used to perform the above mentioned functions. Cryptographic keys are a binary sequence, which is

used for processing (securing) the transmitted data. Ensuring the confidentiality of keys is necessary to ensure the security of connections carried out with the use of EURORADIO protocol.

Due to the need to use large number of keys as well as their cybersecurity, it is necessary to have a systematic approach to managing their collection and equipping them with an appropriate system to perform this task.

2. Cryptographic keys

2.1 Keys

A cryptographic key is an information that allows the execution of a certain cryptographic operation. A cryptographic key may take a binary or text form. Among the cryptographic operations it can be distinguished:

- encryption - the process of protecting information against unauthorized interpretation, converts plain text into ciphertext,
- decryption - the process opposite to encryption, based on the ciphertext, plain text, that can be interpreted, is obtained,
- digital signature - process of transforming information which aims to ensure its authenticity,
- digital signature verification - verification of the authenticity of information signed with a digital signature.

2.2 Cryptographic algorithms

2.2.1 Symmetric algorithms

Cryptographic symmetric algorithms are those in which the same key is used to encrypt and decrypt messages.

Due to the fact that the same key is used for both operations, it is necessary to provide additional technical and organisational means ensuring that the key will only be in the possession of the participants of the information exchange.

2.2.2 Asymmetric algorithms

Asymmetric algorithms are those in which one can distinguish:

- public key – publicly known,
- private key - by definition it is known only to the owner.
-

Asymmetric algorithms use complex mathematical operations in their operations, therefore encryption and decryption of information takes much longer than in symmetric algorithms.

Use of keys in asymmetric algorithms:

- encryption - decryption: a public key is used for encryption and a private key for decryption,
- digital signature - digital signature verification: a private key is used to generate digital signatures, a public key to verify them.

3 Keys in ERTMS/ETCS system

3.1 Types of keys

Three levels of cryptographic keys can be distinguished in ERTMS/ETCS [9]. The use of keys is shown on a Fig.1.

Cryptographic keys in the ERTMS/ETCS system, depending on their level, have different functions, however, the primary purpose of their use is to ensure the safety of data transmission, carried out in the track-train relationship using the wireless communication system.

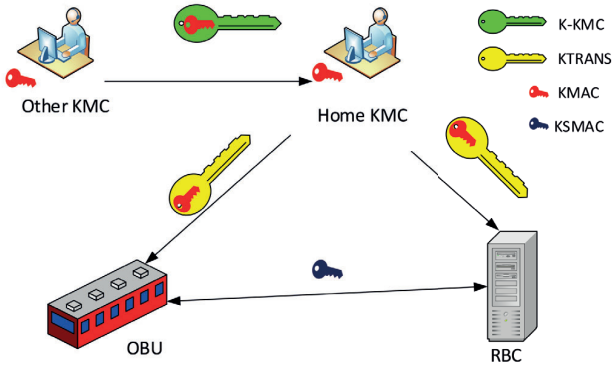

Fig. 1. Use of cryptographic keys in the ERTMS/ETCS system [own study]

3.2 Level 3 keys

The level 3 keys are transport keys, used to secure the transfer of the KMAC. The use of level 3 keys is necessary in offline type of level 2 keys distribution.

KTRANS – keys used for securely transferring level 2 keys from KMC to ETCS entities. The transfer of the KMAC key is only possible if both entities involved in the exchange are equipped with the same KTRANS key. KTRANS consists of a pair of keys:

- KTRANS 1 - key used to verify the authenticity and integrity of messages transmitted between the KMC and the ETCS entity,
- KTRANS2 – key used to encrypt KMAC keys transferred between KMC and KMAC entities,

K-KMC - transport key used to protect communication between KMCs. Transfer of the KMAC key is possible only if both parties involved in the exchange have the same K-KMC key. The K-KMC key consists of:

- K-KMC1 - key used for verification of the authenticity and integrity of messages transmitted between KMCs,
- K-KMC2 - used to encrypt KMAC keys transferred between KMCs.

KTRANS and K-KMC have the same task - to secure the transfer of the KMAC key. The factor that differentiates them is the entities between which the KMAC key exchange takes place.

Before passing the KMAC key in the KMC message, it is encrypted with a 3DES algorithm using the KTRANS2/K-KMC2 key. The encrypted KMAC key is placed in the K-STRUCT structure and then this structure is part of the KMC message, which header contains the ETCS identifiers of the sender and the recipient. On the basis of such a complete message (excluding the CBC-MAC field) and using the KTRANS1/K-KMC1 key, the CBC-MAC value is calculated, which is then attached to the message. The message structure constructed in this way is transmitted to the ETCS entity or KMC. After receiving the message, the CBC-MAC value is calculated (based on the message content and KTRANS2/K-KMC2). CBC-MAC is a technique for constructing a message authentication code from a block cipher. CBC-MAC field (precisely - its value) is used to verify authenticity and integrity of received message. The message can be considered authenticated and with integrity not compromised if the calculated CBC-MAC value is consistent with that contained in the message.

3.3 Level 2 key

Authentication keys (KMAC, Kab) - are used when establishing a secure connection of the EURORADIO protocol, where it is used for mutual identification and authentication of RBC (Radio block Centre) and OBU (On-board unit) and for determination of the session key. In structure of every ETCS entities these keys are assigned to specific entities. Two entities sharing a common level 2 key can establish a secure communication session with EURORADIO protocol.

The KMAC key has a defined validity period defined by the start and end of validity dates. It is also possible to give an unlimited validity of the key.

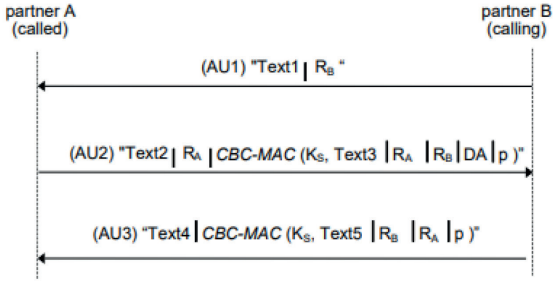

Fig. 2 Information sequence for establishing a secure EURORADIO protocol connection [9]

During the connection establishment two random numbers are transmitted. Random numbers $R_X(X \in \{A,B\})$ are subdivided into left $(R_X L R_X L)$ and right $(R_X R R_X R)$ 32-bit blocs:

$$R_A = R_{A^L} \mid R_{A^R}$$
$$R_B = R_{B^L} \mid R_{B^R}$$

Three 64-bit keys DES K_{S_1}, K_{S_2} and K_{S_3} are calculated according to the following formulas:

$$K_{s_1} = MAC\left(R_{A^L} \mid R_{B^L}, K_{AB}\right) = DES(K_3, DES^{-1}\left(K_2, DES\left(K_1, R_{A^L} \mid R_{B^L}\right)\right))$$
$$K_{s_2} = MAC\left(R_{A^R} \mid R_{B^R}, K_{AB}\right) = DES(K_3, DES^{-1}\left(K_2, DES\left(K_1, R_{A^R} \mid R_{B^R}\right)\right))$$
$$K_{s_3} = MAC\left(R_{A^L} \mid R_{B^L}, K'_{AB}\right) = DES(K_1, DES^{-1}\left(K_2, DES\left(K_3, R_{A^L} \mid R_{B^L}\right)\right))$$

Where | is a concatenation operator, DES is the encryption function of the DES algorithm, and DES^{-1} is the inverse DES encryption, or decryption.

The KSMAC session key is a concatenation K_{S_1}, K_{S_2} and K_{S_3} :

$$KSMAC = K_{s_1} \mid K_{s_2} \mid K_{s_3}$$

3.4 K-STRUCT structure

All operations performed on the keys are performed by executing in the ETCS entity commands contained in messages from the KMC. The structures of these messages depend on the way they are distributed (offline or online). If it is necessary to include the KMAC key in a specific message, it is transmitted using the KSTRUCT structure, which is a organised set of information that is transmitted together with the KMAC key.

Table 1. K-STRUCT structure [own study based on 6]

Field (at SUBSET-114 [6])	Field (at SUBSET-137 [7])	Description
K-LENGTH	K-LENGTH	Key length in octets (24 for KMAC)
KM-ETCS-ID-EXP	K-IDENTIFER	Unique KMC identifier that generated the authentication key
SNUM	ETCS-ID-EXP	Unique key serial number (with KM-ETCS-ID-EXP uniquely identifies a triple key)
ENC (KMAC)	KMAC	Authentication key encrypted with KTRANS2
PEER-SUM	PEER-NUM	Number of ETCS entities (on-board or track-side) in the structure. This number shall be equal to or greater than 1.
PEER-ETCS-ID-EXPi	ETCS-ID-EXP [PEER-NUM]	ETCS identifier extended by the number of the unit stored in the structure (from 1 to the number resulting from PEER-SUM)
VALID-PERIOD	VALID-PERIOD	Period of validity of the key

3.5 Level 1 keys

Session keys (KSMAC, Ks) - are used to directly protect the transmitted data. The session key ensures the integrity and authenticity of the transmitted data, i.e. it is used to protect the message against modification and to ensure that no unauthorized person can pretend to be the initiator of the message (masquerade). Session keys shall be designated during the authentication of the ETCS entities using level 2 keys. Session keys are unique for each communication session and may only be used by entities sharing the same authentication key (KMAC). KSMAC keys are symmetric keys used in both directions of communication.

The KSMAC session key fixed when the connection is established shall be used during the procedure of calculating the CBC-MAC field value or each message being transmitted. This field allows to authenticate the message source and verify its integrity.

When preparing a message to be sent on the basis of a previously prepared message and KSMAC key, the value of the CBC-MAC field is calculated and added to the message. The prepared message is sent to the destination, where on its basis (excluding the CBC-MAC field) and using the KSMAC key established for a given communication session the CBC-MAC value is calculated. If the calculated value of the CBC-MAC field is equal to that attached to the received message, the message source is considered authenticated and the message itself has confirmed integrity.

4. Cryptographic key management system requirements

4.1 Cryptographic key management system

From the point of view of cybersecurity, the Key Management System (KMS) plays an important role. Its correct operation, both technical and organisational, is a necessary condition for maintaining the confidentiality of all types of cryptographic keys and, as a result, for ensuring the security of data transmission between the ETCS on-board subsystem of trains and the ETCS track-side subsystem. Key management is one of the basic parameters formulated in TSI [11]. This basic parameter specifies the requirements for the management of cryptographic keys for the protection of radio transmission data.

In 2018 Transport Certification Center at Warsaw University of Technology carried out for PKP Polskie Linie Kolejowe S.A. a work entitled "Concept of cryptographic key management system for ETCS in accordance with requirements specified in baseline 3". As part of the work, the requirements for the cryptographic key management system formulated in the Technical Specifications for Interoperability of the ERTMS/ETCS system and the requirements for similar systems used in other companies and organizations were analyzed. On the basis of the analysis, the concept of a cryptographic key management system for the railway lines managed by PKP Polskie Linie Kolejowe S.A. (KMS PLK) was developed.

The following entities are involved in the cryptographic key management process:

- operators of KMS in the head office of the infrastructure manager (CZK),
- users of the keys, i.e:
  - railway undertakings,
  - the local branch offices of the infrastructure manager,
- operators of KMS of other infrastructure managers.

The primary task of the cryptographic key management system is to provide the technical and organizational means to allow:

- generation,
- distribution,
- replacement (uploading new keys),
- update,
- storage,
- use,
- removal,
- exchange of keys with other KMSs,

in a manner convenient for the user and ensuring secure and effective use of the system which is utilizing cryptographic keys. Due to the complexity of the structure of ETCS entities, the distribution of keys from CZK to ETCS entities is an important activity, which can take place fully automatically (online) or in specific cases with human intervention (offline).

In terms of organisation, the KMS consists of:

- cryptographic key management centre - CZK,
- field key distribution centres - KDC,
- ETCS entities.

Most of the above mentioned functionalities of the KMS are implemented by the CZK, which uses an IT system consisting of the following components:

- KMC - a secure module implementing elementary functionalities of the KMS,
- PKI - public key infrastructure,
- a management module of the KMS - coordinating the cooperation of the other components,
- KMS database,
- keys database,
- user interface (CZK operator, KDC coordinator) - in the form of a web application of the public access channel.

The system is centralized. These components are elements of the key management centre.

4.2 KMC

The KMC is the executive unit of the key management system (KMS). The functions performed by the KMC should be included:

- performing key operations:
  - generation of keys,
  - storage of keys,
  - archiving the keys,
- preparing KMC messages on:
  - installation of the KTRANS transport key,
  - replacement of KMAC authentication keys,
  - remove the keys,
  - to add an authentication key,
  - change the ETCS entities associated with the key,
  - update of the key validity period,
- KMC message distribution - online distribution,
- interpretation of notification from ETCS entities,

It should be noted that the KMC is handling a specific set of ETCS entities (this set is called the KM domain). A single ETCS entity can only be registered in one KM domain. Consequently, a single ETCS entity can only receive keys from a single KMC called the Home KMC, even if these keys relate to ETCS entities outside the given KM domain. In this case, an interface between different KMS is used.

The KMS should not be identified with the KMC. KMC is only an executive unit with a defined range of functionality. In addition to the KMC, the KMS also includes other technical and organisational means allowing the cryptographic key management process to be carried out.

A number of interfaces have been specified for KMC. They are shown in Fig. 3

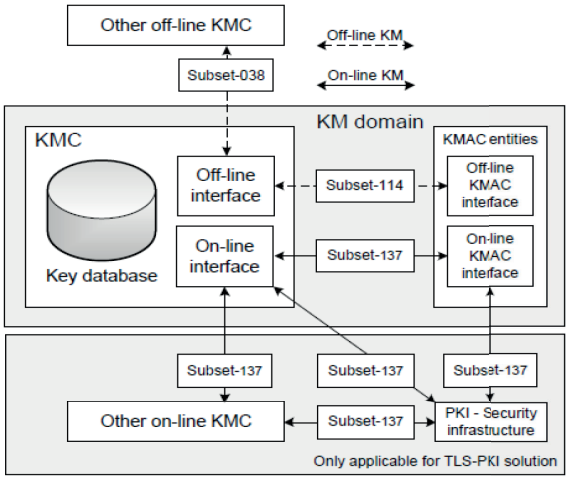

Fig. 3. General architecture of kms [7]

The KMC can be implemented as a safety hardware module (HMS).

4.3 Cybersecurity of technical infrastructure

The implementation of CZK's technical infrastructure requires the selection of appropriate elements and their combination with the observance of good computer network security practices. The proposed structure within the mentioned concept is shown in Fig. 4. The elements that make up the protection against cyber threats are:

- redundancy of the technical infrastructure of CZK, also in the geographical sense,
- secure switch for basic and redundant CZK technical infrastructure,
- the use of virtual networks to separate network traffic with different vulnerabilities,
- use of firewalls for separate subnetworks.

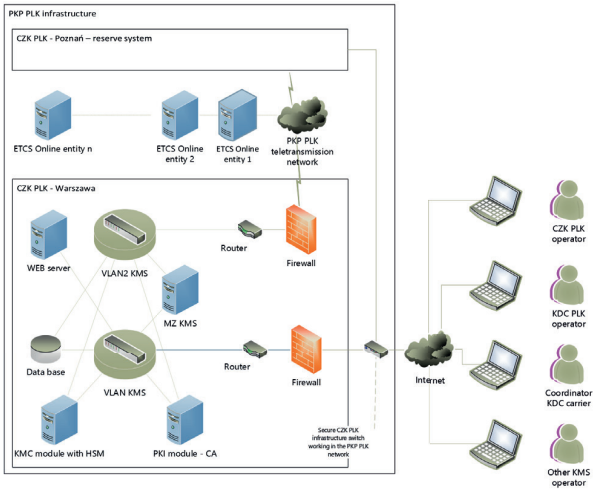

Fig. 4. Proposed configuration of KMS implementation in terms of hardware [own study]

Room in which the technical infrastructure will be installed should also be adequately protected by meeting the following conditions:

- appropriate environmental conditions,
- access control,
- appropriate power supply conditions,
- fire-fighting system,
- lack of water, sewage and gas installations (not applicable to fire-fighting system).

5. Key Distribution

5.1 Cyber-security of distribution

Key distribution activities often use data transmission over subnetworks with varying degrees of confidentiality. Therefore, they are used to protect them:

- public key infrastructure,
- TLS protocol,
- TLS certificates.

The following subsections indicate the different needs for protection against cyber threats in online and offline distribution.

5.2 Offline key distribution

The distribution of cryptographic keys of the ERTMS/ETCS offline system is characterised by the fact that at least one, any stage of the cryptographic key distribution process requires human intervention. The main task of offline key distribution is the distribution of level 2 keys, for which it is necessary to transfer the level 3 key in advance.

In the offline key management system, the following entities should be distinguished:

- KMC,
- ETCS entities, of which
  - on-board entities - OBU,
  - track-side entities - RBC/RIU.

The offline distribution of cryptographic keys between KMCs is specified in SUBSET-038 [8] and the distribution between KMCs and ETCS entities in SUBSET-114 [6].

In the cryptographic key management system based on the distribution of offline cryptographic keys, operations such as:

- generation of keys,
- archiving the keys,
- creating packets (K-STRUCT) containing keys,
- creation of messages initiating the execution of specific operations on keys on ETCS entities,

are carried out by the KMC. Other functions related to the transfer of keys to their users are performed by the KMS staff (human factor), using the available data exchange channels.

KMC messages containing commands for key operation after passing the keys to the users are executed on ETCS entities. The key operation is usually performed using a USB memory stick, but

it can also be performed in another way, depending only on the user. Execution of a key operation results in a notification generated by the ETCS entity, which should be delivered to the KMC from which the message concerning the execution of a specific key operation originated.

Each key operation must be initiated by KMC.

In the case of KMS based on offline distribution, cryptographic keys can be distributed directly from the KMC to ETCS entities or with the use KDC.

It should be remembered that the KDC plays the role of an intermediary, which is manifested by the fact that::

- the KDC does not have an ETCS ID,
- the message sent by the KMC should indicate directly the ETCS entity, even if a DCM is present in the KMS structure,
- notifications from ETCS entities to the KDC should be addressed to the KMC and should contain the ETCS entity identifier. The KDC sends the notifications to the KMC, keeping the ETCS entity information in the message,
- KDC cannot modify the keys sent by KMC.

5.3 Online key distribution

The essence of this solution is to transfer KMAC keys from KMC to ETCS entities without human intervention, it means in an automatic way. This goal is achieved through the use of a teletransmission system and the use of additional mechanisms securing the exchange of keys, e.g. public key certificates generated by PKI.

In the key management system using an online interface:

- the KMC is responsible for establishing the connection to the track-side ETCS entities,
- in the case of ETCS on-board entities, they are responsible for establishing the connection to the KMC.

The ETCS on-board entities regularly contact their home KMC in order to verify that it is not necessary to carry out operations on KMAC keys. Communication between KMAC on-board equipment and KMC takes place when any of the following conditions [7] occurs:

- during activation, when the ERTMS/ETCS on-board equipment is successfully started and any tests completed successfully;
- the time elapsed since the last successful home MC session is longer than the predefined time configured in the on-board equipment. The value of this time period is defined by the home KMC and ranges from 1 hour to 1000 hours, with the default value being 10 hours;
- ETCS on-board maintenance personnel request an update of the key;
- ETCS on-board entities detect an incorrect or defective KMAC key.

If the on-board entity is unable to successfully establish a communication connection to its home KMC, it will try again every 10 minutes to reestablish it.

As mentioned earlier, online distribution uses additional mechanisms to ensure the security of the transmitted cryptographic keys. One of such mechanisms is encryption of transmission by means of TLS protocol (ETCS specifications assume the use of TLS v1.2 or later). This protocol assumes the use of digital certificates, used for authentication of devices that establish communication. These certificates must be properly distributed and maintained, which is the responsibility of PKI - Public Key Infrastructure.

The teletransmission network used to distribute cryptographic keys online may be a GSM-R system or another teletransmission network including KMCs and ETCS entities.

5.4 Distribution between KMCs

In cases where it is necessary to transfer cryptographic keys for on-board ETCS entities located in another KMC domain, the relevant keys are exchanged between the KMCs and installed in ETCS entities in accordance with the rules of the respective key management system. It is possible to exchange keys between KMCs online and offline. A cryptographic key management system that uses the exchange of KMC messages between KMCs and between KMCs and online ETCS entities is described in SUBSET-137 [7], while offline distribution is carried out in accordance with SUBSET-038 [8].

5.5 TLS Protocol

In order to ensure confidentiality, authentication of parties involved in communication and integrity of data transmission within which KMAC keys are transferred, the TLS protocol [10] was applied.

Implementation of key generation functionality and secure communication protocols requires the use of random number generators showing increased resistance to cryptanalyze attacks. Cryptographically protected random or pseudo-random number generators are used for the purpose:

- generation of a pair of public key - private key of the TLS protocol,
- pre-generation of the PSK key when the TLS-PSK solution is used,
- generation of KMAC keys,
- execution of the TLS handshake procedure.

The TLS Client is the entity establishing (initiating) a connection to the TLS server. KMC implements the TLS server and client function in online distribution for the following connections:

- KMC - KMC,
- KMC - ETCS on-board entities.

ETCS track-side entities implement a TLS server and on-board entities implement a TLS client.

Digital certificates (public key certificates) are used to authenticate entities establishing a secure connection within the TLS-PKI protocol.

5.6 Public Key Infrastructure

The implementation of the Public Key Infrastructure (PKI) in the KMS enables each ETCS entity to exchange information related to public key certificates, necessary for the transfer of cryptographic keys through an online interface.

ETCS entities communicate with PKI in the following cases:
- an application for a digital certificate or its renewal,
- check if a specific certificate is correct (the certificate can be revoked before its expiry date due to loss of confidentiality).

6. Hazards

Hazards related to cybersecurity in the environment of railway traffic control systems in general were considered in previous articles and papers of the Authors [2, 3]. Cryptographic keys and methods of their application are a tool for securing various aspects of data transmission. However, due to this role, they may also become a target of a cyber-attack. There are many hazards associated with this. Some of them are listed below in Table 2.

A factor that significantly increases the threat is the high complexity of the key management process combined with a low level of awareness of the purpose, necessity and importance of using keys. The combination of these factors leads to a preference for different types of simplifications in the configuration of the management system (e.g. by using the same keys for a very long period of time, using the same keys by different actors, etc.), which in turn leads to a significant weakening of the security features introduced. An element of the risk associated with complexity is the need to automate the distribution of keys in the face of their estimated number, which may amount to several tens of thousands. Currently, key management software providers on the Polish market promote the approach of total physical separation of workstations used to generate keys and offline distribution. This is a good solution for a number of keys not exceeding several hundred, and for larger quantities it will be difficult to implement organizationally and expensive. Automatic key distribution solutions (online type) will significantly support CZK, but they must also be properly secured, as their compromise will allow cybercriminals to influence ETCS entities practically throughout the domain.

In order to quantify these threats formulated at a very general level, specific threats should be identified by examining the structure, functionality and organisational principles of the cryptographic key management system. An example of the effect of such action are the items of Table 2, which is a part of the work on the study of threats within [1].

The presented table has a simplified form of risk management process records [5, 4] for railway systems. Apart from the obvious unambiguous identification of the threat in the form of a hazard identifier, it contains a description of the threat and the method of its mitigation. For items identified in this way, the risk level analysis is then carried out with the use of numerical indicators.

When dealing with threats, it should be remembered that this is a continuous process. Preliminary and accurate identification of threats is a good beginning of efficient threat management. This process must be continued by monitoring the identified threats and identifying new ones resulting from changes in the cryptographic key management system and its environment.

Table 2. Example of threat analysis in the process of reporting a new ETCS entity to the KMS domain Source [own study]

Hazard identifier	Description	Mitigation method
D1	Attempt to report to the domain of KMS PLK an ETCS entity which does not belong to a reporting entity	The procedure for reporting a new ETCS entity involves the demonstration of the ETCS entity's nationality.
D2	Compromising the transport key	On the CZK side, precautions are taken to ensure the confidentiality of transport keys. Including the use of multiple transport keys, each associated with a different key user. Users of keys are also obliged to keep the keys confidential, under the threat of financial penalties. If a transport key is compromised, it is necessary to replace it in all ETCS entities where it has been used.

7. Conclusion

The ERTMS is intended to provide a unified, interoperable approach to train control and signalling in the European Union. The basis for effective train control at ETCS Level 2 is wireless data transmission via GSM-R. This transmission must be protected by cryptographic techniques to ensure its safety.

Due to the need to use large number of keys as well as their cybersecurity, it is necessary to have a systematic approach to managing their collection and equipping them with an appropriate system to perform this task.

From the point of view of cybersecurity, the Key Management System (KMS) plays an important role. Its proper operation is a necessary condition for the confidentiality of all types of cryptographic keys and consequently for the safety of data transmission between the on-board ETCS train subsystem and the track-side ETCS.

The article emphasises the importance of hazard identification and indicates some mitigation methods which should be conducted in accordance with [5].

The article presents technical solutions and their applications related to cryptographic keys. The requirements formulated for cryptographic key management system are presented. The architecture of the KMS, functions performed and protection against cyber threats for: data transmission between ETCS entities, distribution of keys to their users, distribution of keys between foreign KMS, technical infrastructure of CZK were discussed.

The issues presented in the article concern technical solutions, which so far have not been used in solutions designed for railway traffic control systems. It is a new area of application which requires popularization of knowledge and research on practical problems occurring in real conditions.

Bibliography

[1] KOCHAN A., et al.: Koncepcja systemu zarządzania kluczami kryptograficznymi dla systemu ETCS zgodnie z wymaganiami określonymi w Baseline 3. Zasady wymiany kluczy kryptograficznych ERTMS/ETCS z innymi zarządcami infrastruktury, RA_18331_3_3_1_SRK_BIR_PL, 1-10 s., Ośrodek Certyfikacji Transportu na Wydziale Transportu Politechniki Warszawskiej, raport naukowo-badawczy 2018

[2] KOCHAN A., KOPER E.: Cyberbezpieczeństwo systemów kierowania i sterowania ruchem kolejowym, w: TTS Technika Transportu Szynowego, nr 12, ss. 247-253, 2017

[3] KOCHAN A.: Cyberbezpieczeństwo w systemach sterowania ruchem kolejowym, 1-16 s., 2018, Ośrodek Certyfikacji Transportu na Wydziale Transportu Politechniki Warszawskiej, Konferencja Cyberbezpieczeństwo w transporcie kolejowym 2018

[4] KYCKO M., ZABŁOCKI W.: Metody oceny ryzyka w procesach inwestycyjnych obejmujących wdrożenie systemów sterowania ruchem kolejowym (SRK), w: Zeszyty Naukowe Uniwersytetu Gdańskiego. Ekonomika Transportu i Logistyka, nr 74, ss. 267-276, 2017

[5] Rozporządzenie Wykonawcze Komisji (UE) NR 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylające rozporządzenie (WE) nr 352/2009

[6] Unisig, „Subset-114 KMC-ETCS Entity Off-line KM FIS, v.1.1.0"

[7] Unisig, „Subset-137 On-line key management FFFIS v.1.0.0"

[8] Unisig "Subset -038 Off-line Key Management FIS v 3.1.0"

[9] Unisig, „Subset- 037 EuroRadio FIS, v.3.2.0"

[10] Dierks T. i Rescorla E., RFC 5246 - The transport layer security (TLS) protocol - Version 1.2., ss. 1–105, 2008

[11] Komisja Europejska, (2016/919/UE) Rozporządzenie Komisji z dnia 27 maja 2016r. w sprawie technicznej specyfikacji interoperacyjności w zakresie podsystemów «Sterowanie» systemu kolei w Unii Europejskiej (Dz. U. L 158 z dnia 15.06.2016, str. 1 i n.) 2016