**KMS WG**

# IT Security Threat identification, Risk Analysis and Recommendations

PUBLIC VERSION

KPMG IT Advisory
Amstelveen, April 2013
This report contains 46 pages

A1200002009.KE5.RA

# Colofon

Peter Kornelisse, director (Kornelisse.Peter@kpmg.nl)

Ronald Heil, senior manager (Heil.Ronald@kpmg.nl)

KPMG IT Advisory
Laan van Langerhuize 1
1186 DS Amstelveen
The Netherlands

*Note that this public document is limited on request by and in agreement with the KMS WG, as the content in the full but restricted report provides confidential details on the threats and risks of the underlying systems.*

# Contents

# 1 Introduction

## 1.1 Background

The European Rail Traffic Management System (ERTMS) employs open standards and commoditised global technologies (such as GSM and GPRS) for signalling and train control. The question arises on how the new generation of trains can be protected, what are the new threat scenarios, and whether the 'train control systems of the future' are vulnerable.

Safety engineers usually tend to regard security as 'nice to have' within their daily operations. Still, it should be noted that security breaches can have serious safety consequences. There are numbers of scenarios, such as transmitting falsified radio messages indicating a too high speed limit to the train driver, or by compromising the on board unit (OBU) within a train that controls the speed and braking capability of the train. Software maintenance or upgrades can also lead to incidents (security breaches) as for example outsiders gain access to internal information such as the used communication protocols, control commands, encryption methods and authorisation procedures.

The security of the Euroradio protocol used to safely transmit movement authorities is currently largely dependent on the security of the key management and the key distribution process[1]. ERTMS Application Level 2 and Application Level 3 rely on the use of secret symmetrical cryptographic keys for Triple DES/CBC-MAC authentication and protection of the integrity of the data exchanged between the OBU and trackside equipment, transmitted via the GSM network for railways (GSM-R). The keys are generated and maintained in the Key Management System (KMS).

The KMS WG has the challenge of identifying and analysing threats applying to the ERTMS environment, and determining the weaknesses related to these threats, resulting in an adequate overview of current risks.

## 1.2 Objective

The objective of the report is to present a structured threat model and risk analysis:

- Identification of threats after reviewing the relevant documentation, inspecting physical components, and interviewing key stakeholders.
- Creation of a structured threat model that provides an overview of security threats.
- Analysis of the risks associated with the threats and a categorisation in 'Tolerable', 'Undesirable' and 'Intolerable' threats based upon the likelihood and impact.
- Providing recommendations for the 'Intolerable' and 'Undesirable' threats.

[1] UNISIG SUBSET-038

### 1.2.1 Limitations

KPMG delivers a report of findings, no overall conclusion with regard to security and/or completeness of threats, risk analysis and recommendations is provided. Please note that certain identified threats, risks and/or recommendations might be evaluated by the KMS WG as not feasible or not relevant due to particular features (or limitations) of the ERTMS system, which KPMG is not (made) aware of or are outside the scope of this engagement.

Due to nature of this engagement, KPMG and any company owned by, or affiliated with KPMG and their respective principals, employees and affiliates, are not responsible for any damage, demands, liabilities and claims for personal injuries and/or property damage that may be caused by or ensue from this report.

## 1.3 Scope definition

### 1.3.1 ERTMS Application Level in scope

In agreement with the KMS WG, the scope focuses on:

- ERTMS Application Level 2
  - In ERTMS Application Level 2, the train detection is performed by track based hardware, and
- ERTMS Application Level 3
  - In ERTMS Application Level 3, there is an onboard train integrity system, the train position detection is performed with information coming from the train. The train communicates its location to the RBC that will use this information to define movement authorities.

Note that ERTMS Application Level 1 is agreed to be excluded for this analysis as there is basically no communication with the train other than via the induction transmission blocks in the rails (known as balises), no data communication via radio is involved.

### 1.3.2 Background on the Reference Case and Variations

***The Reference Case***

The threat and risk analysis is based upon ERTMS Application Level 2 using the GSM-R transmission system including Euroradio and offline key management, this will be indicated to as the Reference Case.

The KMS WG has provided additional information for the Reference Case by:

- Taking the design document from one of the KMS WG members and select the relevant descriptions.
- Providing a short additional description on the intended reference case.

KPMG processed the above-mentioned documents and created a clear reference case document, which is included in Appendix B.

***The Variations***

Since the implementation of ERTMS can vary slightly per country, e.g. one unique key for each train versus one key for all trains, or for example the choice of using ERTMS Application Level 3, there are variations to the reference case that are also considered in the threat and risk analysis but kept separate for clarity.

### 1.3.3 Object in scope

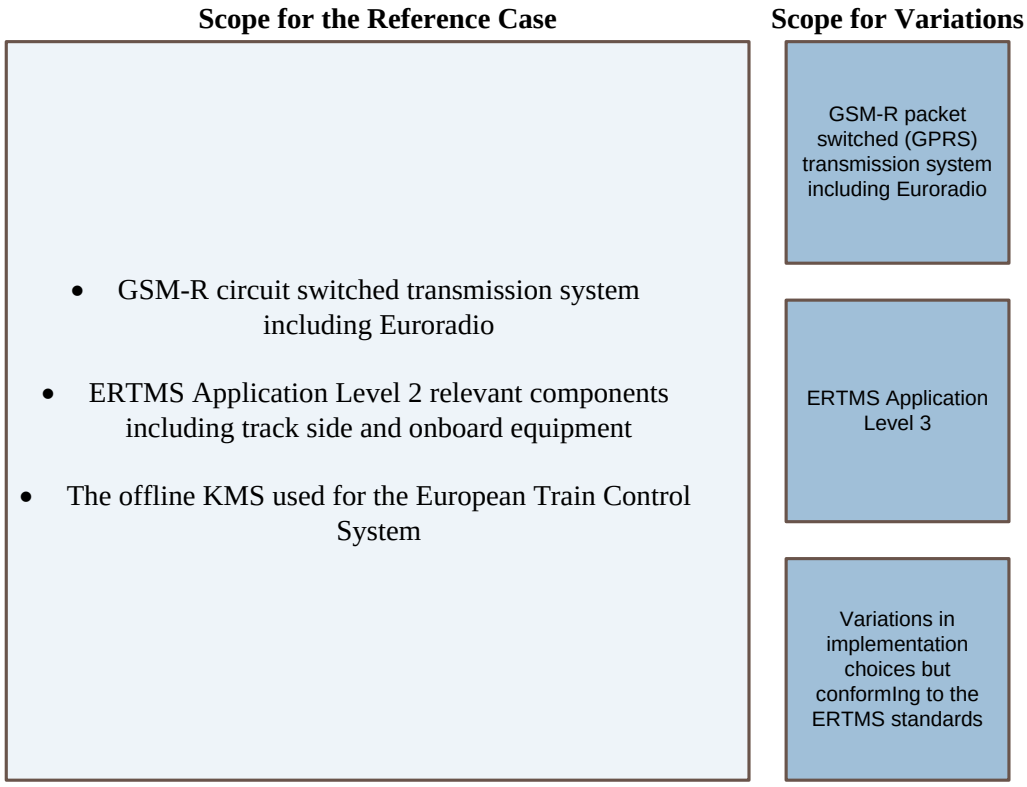


*Figure 1 - Overview of the objects in scope: Reference Case and Variations*

#### *1.3.3.1 Scope for the Reference Case*

In agreement with the KMS WG the following is the scope for the Reference Case:

- GSM-R circuit switched transmission system including Euroradio.
- ERTMS relevant components including track side and onboard equipment.
- The offline key management system used for the European Train Control System (ETCS).

#### *1.3.3.2 Scope for the Variations to the Reference Case*

As some countries make different choices and/or apply variations, the KMS WG selected the following as in scope for the Variations to the Reference Case:

- GSM-R packet switched (GPRS) transmission system including Euroradio.
- ERTMS Application Level 3.
- Variations in implementation choices but conform to the ERTMS standards.

#### *1.3.3.3 Out of scope*

- Online Key Management Systems as the specifications are not formally completed yet.
- Components that are not part of the ERTMS specifications, such as interlocking.

### 1.3.4 EUG documents in scope

For this report, various documents produced by the KMS WG are in scope. These documents are restricted and are not publicly accessible.

The overall threats identification and risk analysis is performed for the conditions specified in the Reference Case (see Appendix B), which were assembled by KPMG based on confidential documents provided by the KMS WG and discussions during the workgroup meetings. The key management procedures and access and authorisation controls on the GSM-R network rely on national or local implementations and as such are not covered by the ERTMS specifications. The purpose of the Reference Case is to outline what is included in the scope of this report.

In addition, note that other KMS WG documents and information sources have been reviewed. Please refer to paragraph 1.5.4 for an overview.

## 1.4 Approach

Step 1 – Scope identification

In the initial meeting between the KMS WG and KPMG, the scope for the threat and risk and mitigation analysis was decided upon.

Step 2 – Threat identification

As a base of our analysis, main threats were identified and discussed with the KMS WG. These main threats were further analysed to identify the underlying causes, threat objects and threat events.

Step 3 – Risk analysis

The threats resulting from the threat analysis were assessed based upon impact and likelihood and are classified as 'Tolerable', 'Undesirable' and 'Intolerable'.

Step 4 – Recommendations

Recommendations were provided on European and national level which can be implemented to reduce the likelihood or impact of the 'Undesirable' and 'Intolerable' risks.

Step 5 – Documentation of results

KPMG provided several intermediate deliverables to the KMS WG to keep track of the progress and to receive intermediate feedback. The report is the final deliverable resulting from the threat identification and risk assessment.

## 1.5 Report

### 1.5.1 Distribution

This deliverable is the public version of the final restricted report for the KMS WG and as such can be distributed in the public domain.

### 1.5.2 Structure

The report structure is as follows: A management summary of the performed approach and the results are included in Chapter 2.

For further reference, the Reference Case is attached in Appendix B. Background information on hacker terminology and cybercrime is provided in Appendix C and an analysis of the used cryptographic algorithms within the Euroradio protocol is provided in Appendix D.

The other chapters with detailed threats, risks and recommendations for the Reference Case and variations have been left out on purpose in this public version.

### 1.5.3 Acronyms and abbreviations

For clarity the following acronyms and abbreviations have been used:

| Acronym or abbreviation | Explanation |
|---|---|
| ERTMS | European Rail Traffic Management System |
| ETCS | European Train Control System |
| EUG | ERTMS Users Group (including KMS WG) |
| Euroradio | Protocol to transmit messages using a shared key to establish a secure communications channel. Provides authenticity and integrity of messages. |
| GPRS | General Packet Radio Service |
| GSM-R | GSM mobile communications standard for railway operations |
| Infrastructure manager | Any public body or undertaking responsible in particular for establishing and maintaining railway infrastructure, as well as for operating the control and safety systems |
| KDC | Key Distribution Centre |
| KMC | Key Management Centre |
| KMS | Key Management System |
| KMS WG | Key Management System Working Group (part of ERTMS Users Group) |
| OBU | On-Board Unit |
| Railway industry | Railway undertakings, railway infrastructure managers, suppliers and other related stakeholders and third parties |
| Railway undertaking | Any private or public undertaking whose main business is to provide rail transport services for goods and/or passengers with a requirement that the undertaking should ensure traction |
| RBC | Radio Block Centre |
| Third parties | Third parties are, for example, vendors, maintenance personnel, contractors and temporary staff |

*Table 1 - Acronym or Abbreviation explanation*

### 1.5.4 Information sources used

KPMG used the following documents on ERTMS and KMS components, KMS and GSM-R threats identification, and IT security risk assessment as input for the threat identification and risk and mitigation analysis.

#### *1.5.4.1 UNISIG subsets*

The public UNISIG subsets are the standards used as a basis for our threat and risk analysis.

1. UNISIG SUBSET-026, System Requirement Specification, Version 3.3.0

2. UNISIG SUBSET-037, Euroradio FIS, Version 3.0.0
3. UNISIG SUBSET-038, Off-line Key Management FIS, Version 3.0.0
4. UNISIG SUBSET 088, ETCS Application Levels 1 & 2 - Safety Analysis, Version 2.3.0
5. UNISIG SUBSET-114, KMC-ETCS Entity Off-line KM FIS, Version 1.0.0

#### *1.5.4.2 Confidential information sources provided by the KMS WG:*

6. Overview of threats to the KMS and the GSMR-GPRS transmission system including Euroradio as identified by KMS WG.
7. Description of the Reference Case
8. KMS Diversity description including implementation specific aspects
9. Operational design document from one of the KMS WG members including relevant descriptions for the Reference Case
10. Boundaries between ETCS and GSM-R
11. ETCS-GPRS principles

# 2 Management Summary

## 2.1 Introduction

The Key Management System Working Group (hereafter referred to as KMS WG) requested KPMG to identify potential additional threats and/or improvements, perform a risk analysis and provide recommendations, based on reviewing and analysing the initial threat analysis work done by the KMS WG, complemented with reviewing relevant UNISIG documentation, and discussions and interviews with key stakeholders.

This analysis was agreed in the engagement letter of 26 October 2012, with reference A1200002009, titled “Engagement letter for Security analysis ERTMS key management”. The fieldwork was completed between November 2012 and March 2013.

KPMG delivers a report of findings, no overall conclusion with regard to security and/or completeness of threats, risk analysis and recommendations is provided. Please note that certain identified threats, risks and/or recommendations might be evaluated by the KMS WG as not feasible or not relevant due to particular features (or limitations) of the ERTMS system, which KPMG is not (made) aware of or are outside the scope of this engagement.

Due to nature of this engagement, KPMG and any company owned by, or affiliated with KPMG and their respective principals, employees and affiliates, are not responsible for any damage, demands, liabilities and claims for personal injuries and/or property damage that may be caused by or ensue from this report.

## 2.2 Results

***Threat identification***

The introduced threat model, as documented in this deliverable, allows for a clear structuring and facilitates the discussion of the identified risks and threats. Based on that threat model, the threat identification resulted in a total of 7 main threats, 11 causes, 25 threat objects and 53 threat events which have been discussed and agreed upon during the KMS WG meetings.

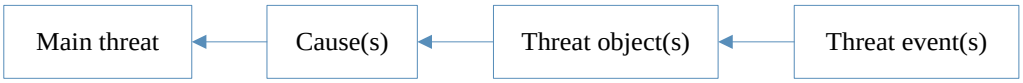


*Figure 2 - the threat model*

***Risk analysis***

The risk analysis was performed on the level of threat objects as it enabled us to evaluate the overall likelihood based on the underlying threat events, and determine the overall impact by evaluating the causes and main threats the specific threat objects could result in.

Of the identified threat objects, within the scope of the Reference Case, 18 are considered to be ‘Intolerable’, 4 are considered to be ‘Undesirable’, and only 3 are considered to be ‘Tolerable’.

The analysis of the impact and likelihood is performed based upon the overall judgement of KPMG and the KMS WG based on the Reference Case and the feedback by KMS WG on the 'generic' implementation (thoughts) at the time of the analysis. It should be noted that the railway infrastructure managers or other related entities may have a lower or higher judgement depending on measures implemented (or known to them) which are not considered in our analysis.

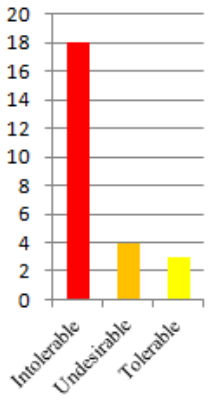


*Figure 3 - Overview of Intolerable, Undesirable and Tolerable threat objects*

***Recommendations***

For the 18 threat objects with a risk level of 'Intolerable' and for the 4 threat objects with a risk level of 'Undesirable', a total of 41 recommendations were made covering the most detailed level of the model, namely the threat events, in order to provide mitigation options to reduce the likelihood and/or impact of the identified risks corresponding with the threat objects.

The recommendations should be at least evaluated and adequately addressed on National/Regional/Local level, whilst for several recommendations there is an increased gain in effectiveness and consistency possible if the recommendations are addressed on European level. The recommendations are described in detail in paragraph 2.3.5.

The management of the EUG and other ERTMS related entities should realise that the usage of strong cryptographic keys is essential to the security of ERTMS and without the implementation of additional measures and/or major improvements, the risk is high that the identified safety and non safety related main threats will materialise with a high impact.

## 2.3 Overview: Threat identification, Risk Analysis and Recommendations

### 2.3.1 Structured approach

Five meetings were held between November 2012 and March 2013 with the KMS WG and KPMG to obtain background information on the specifications and the system itself, to discuss and to agree upon identified threats, assessed risk levels and recommendations.

The following table shows the approach taken and the output resulting from each step. These steps are described further below.

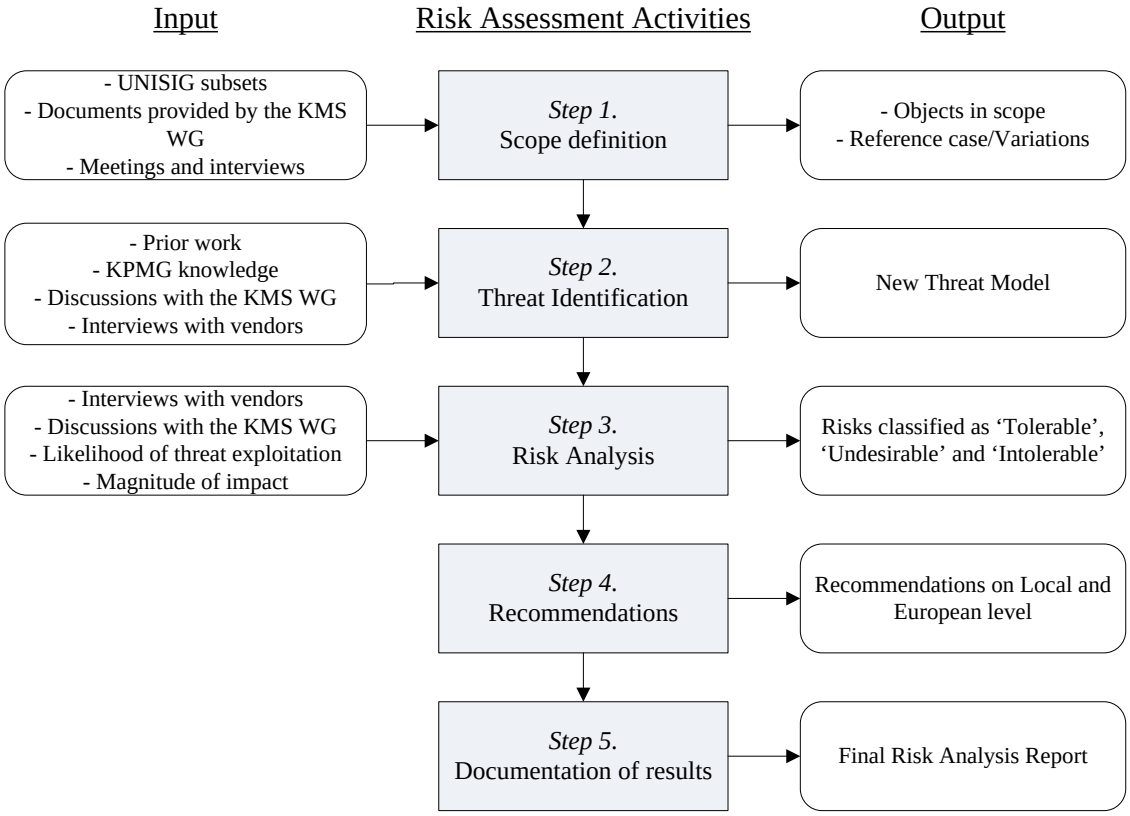


*Figure 4 Approach followed*

### 2.3.2 Step 1: Scope definition

As first step, the scope for the risk analysis was decided upon and was determined to be ERTMS Application Level 2 using the GSM-R circuit switched transmission system including Euroradio and offline key management. This scope is referred to as the Reference Case, for which KPMG was provided with documents describing the reference implementation to be used as primary input for the risk analysis, refer to paragraph 1.5.4.

Additionally, variations to the Reference Case were considered. These included GSM-R with GPRS (packet switched), ERTMS Application Level 3 and other variations in implementation choices which conform to the ERTMS standards as these may be implemented in practice.

The full scope is described in paragraph 1.3.

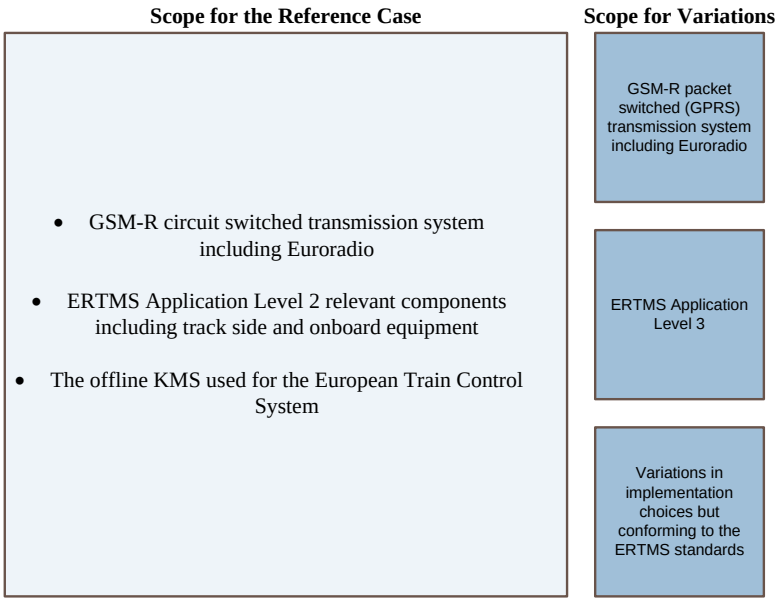


*Figure 5 Overview of scope for the Reference Case and Variations*

### 2.3.3 Step 2: Threat identification

Although the initial work done by the KMS WG, as documented in KMS WG confidential document 12E039 'Threats to KMS and the GSM-R transmission system including Euroradio', provides insight in possible threats and related causes to both GSM-R including Euroradio and offline KMS, KPMG noted that the initial work could be improved by applying a more firm structure of threats, specifically enabling the structured identification of potential threats not identified by the KMS WG.

This restructuring by KPMG, resulted in a new threat model with grouped threats with the purpose to better support the identification and categorisation of threats, enabling a structured iterative threat analysis and sound follow-up discussion during the KMS WG meetings in Brussels. The grouping also helped the participants to handle the large number of threats related to the various components in the ERTMS environment.

The new threat model was designed based upon main threats (both safety and non-safety related) to the ERTMS system. The main threats can be the result of various causes which result from threat events that are grouped in threat objects, as figured below.

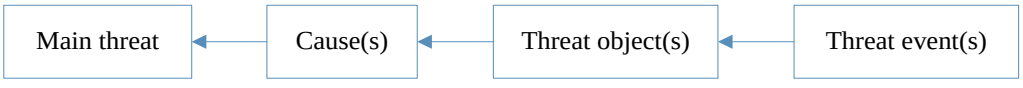


*Figure 6 Threats Categorisation Approach*

In addition to the analysis of the Reference Case, KPMG analysed the variations to the Reference Case to identify additional applicable causes, threat objects and threat events.

The next paragraphs cover the main threats, causes, threat objects and threat events. Note that this public document is limited on request by and in agreement with KMS WG, as the content provides confidential details on the threats and risks of the underlying system. In order to keep the structure of the report, the restricted details were masked with a black overlay. The chapters with the detailed breakdown of threats and risks for the Reference Case and the Variations were removed on purpose.

#### *2.3.3.1 Main threats*

KPMG identified four main threats corresponding to the main functions of ERTMS, the ability to drive safely for a specific distance and do so with a safe speed. In addition, three threats that are not directly safety related were identified by KPMG:

***Drive safely for a specific distance***

- Train collision.
- Train stop.
- Train 'disappears'.

***Drive with a safe speed***

- Train derailment.

***Other sorts of threats – non safety related***

- Public unrest/unsafe situations.
- Railway industry unrest.
- Cyber attack enabled by hacking ERTMS components.

#### *2.3.3.2 Causes*

In order to identify the causes leading to the main threat, KPMG analysed the relevant UNISIG subsets as described in paragraph 1.5.4.1 and held limited discussions with vendors[2]. Additionally, the causes were discussed and agreed upon during the KMS WG meetings in Brussels.

As a result, a table was created containing the main threats (in the left column) and the causes (in the right column) which can result in the respective main threat.

[2] Please note that KPMG also performed a limited visit to a training lab in The Netherlands.

| # | Main threats | Cause |
|---|---|---|
| 1 | Train collision | [redacted] |
| 2 | Train stop | |

*Table 2Main threats and causes*

***Example***

[redacted]

For each of the causes, example scenarios were defined to visualise how the cause can lead to the main threat. However, due to confidentiality these examples are not included in this report (the public version).

### *2.3.3.3 Threat objects*

The causes are further divided into specific threat objects that can lead to the particular cause. This is registered in a table, such as displayed below. The left column shows the causes, the right column shows the threat objects which can lead to the particular cause.

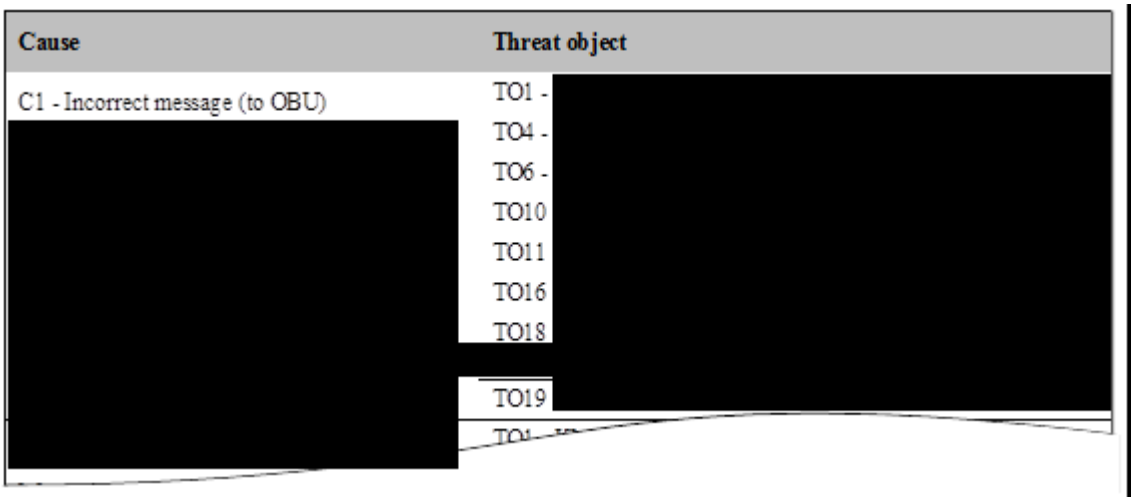


*Table 3 Causes and Threat objects*

***Example***

*Inactivity of the communication channel (threat object TO11) can lead to a delayed message (part of incorrect message) being sent to the OBU (referenced as cause C1).*

### *2.3.3.4 Threat events*

A threat object consists of a further subdivision in threat events and/or additional threat objects.

The following table shows an example of a subdivision of a threat object into several threat events and other threat objects.

| Threat objects | Threat events/threat objects |
|---|---|
| TO1 - KMAC exposed [redacted] | TE1 - [redacted]<br>TE2 -<br>TE3 -<br>TE4 -<br>TE5 -<br>TO3 -<br>TO9 -<br>TO12<br>TO13<br>TO14 |

*Table 4 Threat objects and Threat events*

***Example***

[redacted]

In the case of recurring threat events, additional threat objects were defined.

***Example***

[redacted]

### 2.3.4 Step 3: Risk analysis

KPMG performed a risk analysis on the identified threat objects to categorise the threat objects in ‘tolerable’, ‘undesirable’ and ‘intolerable’. The categorisation is performed based upon an analysis of impact and likelihood.

The likelihood of a threat object materialising is based upon the threat events associated with the threat group. The impact is based upon the causes and main threats the threat object can lead to. For the risk analysis, the whole chain from threat event to main threat is considered.

The following table contains an example report for threat object TO1 – KMAC exposed.

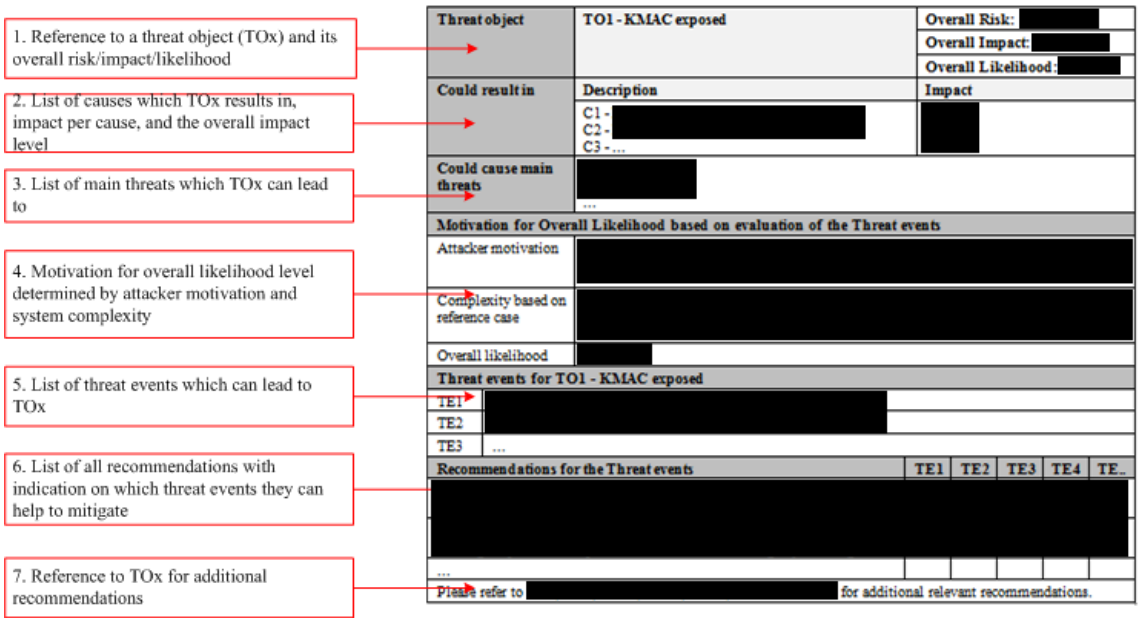


*Figure 7 Example risk analysis table of a Threat object*

The example risk analysis table contains seven reference numbers which are explained in more detail below.

The main header of the table contains the overall risk level, the overall impact and the overall likelihood [1]. The impact is derived from the causes the threat object can result in [2]. The likelihood is described in the motivation and is based on attacker motivation and complexity of the attack [4]. Additionally, the list of main threats which the threat object can lead to is described [3].

The threat events associated with to this object are added to be able to obtain a concise overview of the threats [5]. Finally the recommendations are described including a reference to the threat events which are covered by the recommendation [6]. As other threat objects can also have relevant recommendations, since they can lead to the current threat object, a reference is made [7].

### 2.3.5 Step 4: Recommendations

KPMG provided recommendations to reduce the likelihood or impact of those threat objects and threat events that were categorised as ‘intolerable’ or ‘undesirable’. In total 41 unique recommendations were made, that should be evaluated and adequately addressed on National/Regional/Local level, whilst for several recommendations there is an increased gain in effectiveness and consistency possible if the recommendations are addressed on European level. Something to be further decided and followed upon by the EUG and related ERTMS entities.

The recommendations[3] can be summarised as follows, grouped by Governance, People, Process and Technology:

**Governance**

- Draft and implement policies, procedures and guidelines on the secure configuration, commissioning, operation, maintenance and decommissioning of all ERTMS related equipment.
- Clearly establish roles and responsibilities with regard to the secure handling of keys and the security of the ERTMS related equipment.
- Establish an eco system between third parties (e.g. vendors, maintenance, etc.) and the ERTMS users in which 'trust' is good, but being in control is better.
- Establish an environment that minimises the number of people that handle keys and guaranteeing that keys are not processed unencrypted (plain text) during any phase of the key life cycle. The ERTMS environment should be transparent but secure.
- Apply the transition from Safety thoughts to Safety and Security.

**People**

- Periodically perform and evaluate security awareness and technical training for personnel responsible for ERTMS including key handling.

**Process**

- Draft and implement cyber threat incident response procedures, that cover both technical response and (media) communication, legal and managerial level, to adequately handle situations such as the (perceived) exposure of keys, imminent or confronted threats and for example situations such as unavailability or denial of service attacks.
- Draft and implement procedures and guidelines for the generation (including periodic renewal) of secure keys used in the ERTMS environment such as KMAC, KTRANS, K-KMC and session keys.
- Draft and implement logical and physical access control measures to prevent unauthorised access to ERTMS related equipment (including all interfaces) during any phase of its respective life cycle (e.g. from initial deployment, operation, maintenance, to decommissioning), this is including strict guidelines on secure and limited remote access (by anyone).
- Draft and implement (continues) security monitoring and periodical security verification of ERTMS related equipment (also cover non regular IT components) and track side, this is

[3] Please note that some of the recommendations provided are also applicable for ERTMS Application Level 1 and ERTMS Application Level 3.

including for example the verification of GSM-R, RBC and OBU log messages for irregularities.

- Draft and implement Software Life Cycle and Patch Management procedures for ERTMS related equipment (also cover non regular IT components).
- Establish contracts with third parties to formalise agreements with regard to secure handling of keys and secure management of IT and ERTMS components according to specifications.
- Draft and implement Business Continuity and Disaster Recovery procedures. In addition, these must be tested frequently via periodic walk through and real life tests.
- Draft and implement guidelines to perform security verification and system audits on each ERTMS implementation (and major changes) to verify that the implementation is performed according to the specification and to identify security weaknesses in the implementation. It is recommended to perform these verifications periodically.

**Technology**

- Investigate how the security of (end-to-end) communication can be improved.
- Investigate how the security of the communication from balises can be improved.
- Investigate whether improvements can be made on the deniability / traceability of keys, including the possibility to verify if a key is authentic.
- Investigate and provide guidelines to the EUG on the secure usage of components that are connected to ERTMS components but are not part of the ERTMS specifications.
- Investigate and provide guidelines regarding the hardening of the ERTMS components and applications, they should only provide the functionality that is strictly required by removing unnecessary functionality and applying the most strict security configuration, this is also applicable to the (embedded) Operating Systems, databases and other file systems the devices operate on.
- Investigate the option to use GSM-R caller/SIM card white listing to prevent unknown devices from calling and communicating with specific ERTMS components. Similar principle can be applied to the communication between any of the ERTMS components, as they must only accept data from known trusted sources.

For all unique recommendations, KPMG provided references to the threat objects which risk can be (partly) mitigated by implementing the related recommendations. In addition, the total number of relevant threat events is stated, in order to give a better overview of the recommendation value. These details are not included in the public version of the report.

### 2.3.6 Step 5: Documentation of results

KPMG provided several intermediate deliverables to the KMS WG to keep track of the progress and to receive intermediate feedback during the project. These deliverables resulted in a full report restricted to the KMS WG participants and a public version of the full final report (this report).

# 3 Threat identification Reference Case and Variations

Due to confidentiality this chapter is not included in this public version of the report.

# 4 Risk analysis and Recommendations – Reference Case and Variations

Due to confidentiality this chapter is not included in this public version of the report.

# A Index Appendices

# B Reference Case

## B.1 Introduction

The Reference Case is based upon ERTMS Application Level 2 using the GSM-R transmission system including Euroradio and offline key management. The KMS WG has provided additional information for the Reference Case by:

- Taking the design document from one of the KMS WG members and select the relevant descriptions and providing a short additional description on the intended reference case.

KPMG processed these documents and created a clear reference case document, which is this chapter. It should be noted that the content is based on the sentences and drawings as provided by the KMS WG.

## B.2 Simplistic overview

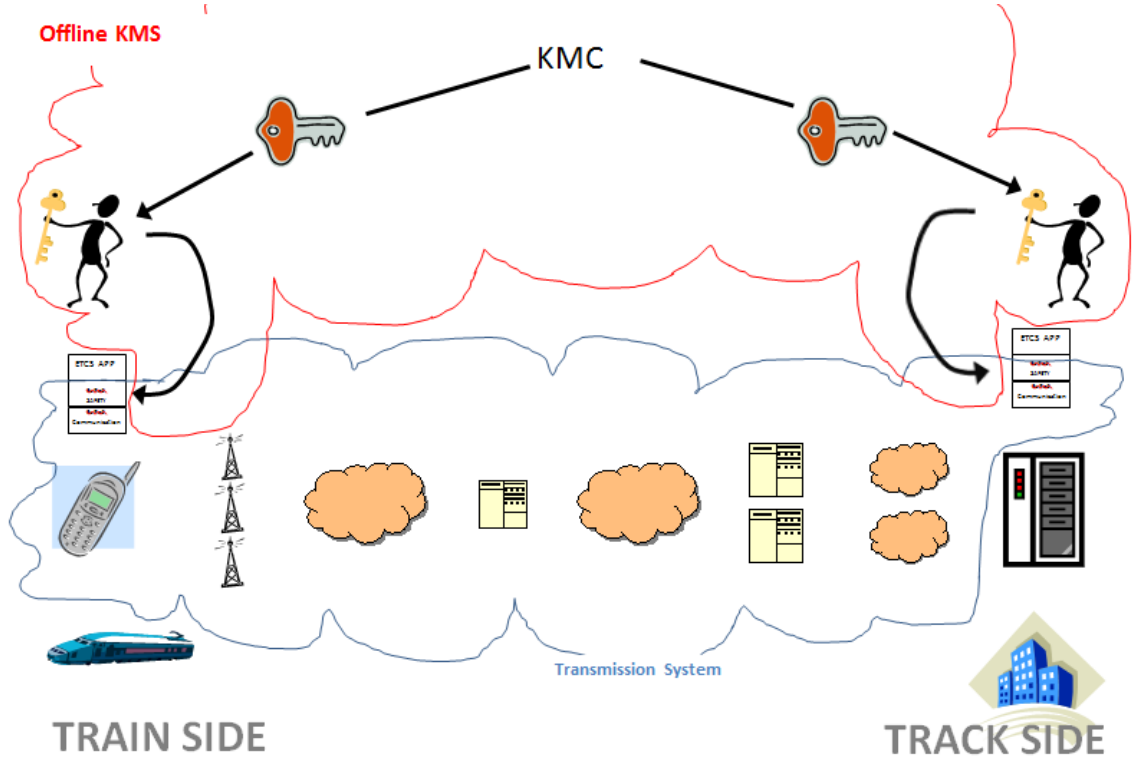


*Figure 8 - Overview of reference case*

# B.3 Offline KMS

## B.3.1 The Operational Concept KMS

An operational concept for the KMS was produced based on that being used by one of the members of the KMS WG. It was adapted and reduced by the KMS WG for the Reference Case for this analysis. The text of Chapters 1-6 from the document together with the comments inserted by the KMS WG is used to provide information for the Reference Case. Other chapters of the operational concept are more detailed process descriptions and serve as background information and are not represented in this document.

### *B.3.1.1 Introduction*

*Purpose*

Key Management (KM) comprises generation, validation, storage, distribution, updating, archiving and deleting keys. ETCS Level 2 requires keys for setting up secure connections between ETCS facilities. This operational concept is intended to enable a potential operator to plan, set up and operate a KMS.

### *B.3.1.2 Background*

*Overview*

The requirements of railway applications to secure communication in open transmission systems are specified in the CENELEC standard [EN50159-2].

For secure transmission between the ETCS entities, a security appendix (Message Authentication Code - MAC) is appended to each message you send. The aim of this MAC is to secure:

- Warranty of the message integrity.
- Warranty of the message authenticity.

Note: ETCS entities onboard are the on-board units (OBU) and trackside entities are the radio block center (RBC) or radio infill units (RIU). RIU is not discussed in this document. Logically, the statements regarding OBU - RBC relations are also applicable to OBU - RIU relations.

MAC generation and validation is based on a cryptographic method that uses symmetric keys to establish secure connections. These keys must be generated by the Key Management Center (KMC), validated, stored, distributed and installed securely in the communicating ETCS entities.

ETCS entities that are managed jointly with respect to the key management form a KM-domain - the home-KM domain. The KMC KM of this domain is also known as home-KMC. All other

domains are referred to as KM foreign domains. KM foreign domains must not necessarily be geographically adjacent to the home-KM-domain.

Subject of the key management system is the management of cryptographic keys for EURORADIO - connections. The KMS comprises i.e. the totality of all hardware and software components of the KMC and the crypto components of ETCS entities in the KM domain and the organizational arrangements for key management within and between KM domains.

See overview of the KMS architecture in Figure 16.

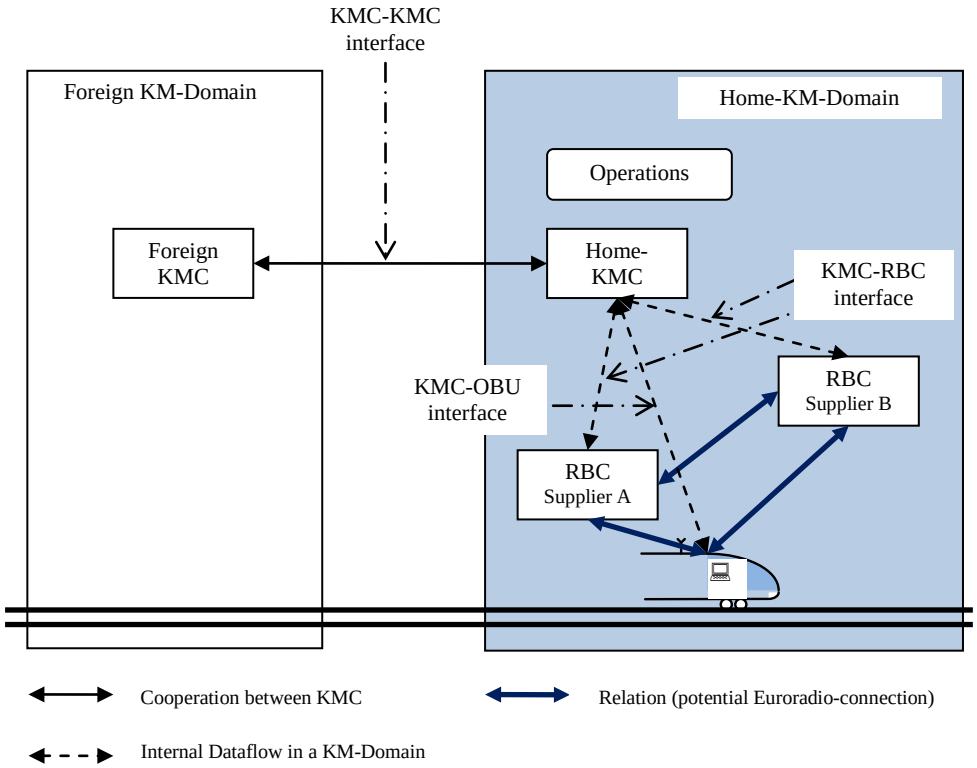


*Figure 9 - KMS Architecture*

*Key hierarchy*

For each intended euro radio connection between ETCS entities, there must be a key pre-installed in both ETCS entities. Whether this connection is established later in fact is irrelevant to the Key Management. A potential connection between Euro Radio ETCS entities will therefore be further referred to as ‘relation.’

An overview of the possible relations that are to be managed by the KMS is shown in Figure 17.

- Between home KM domain OBU and home KM domain RBC.
- Between home domain RBC‘s.
- Between foreign domain OBU home domain RBC.

- Between foreign KM domain neighboring RBC and home domain RBC.

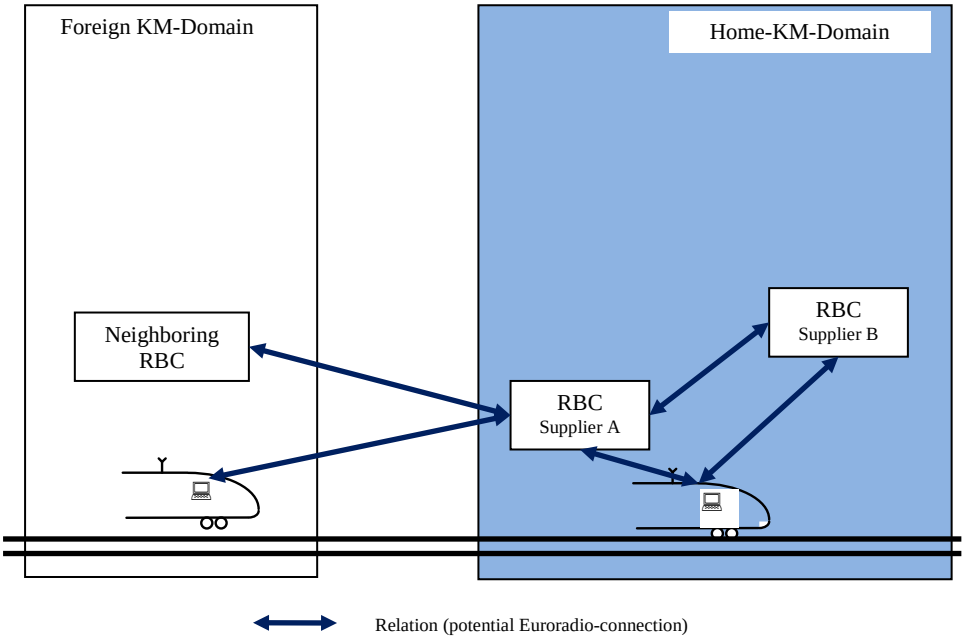


*Figure 10 - Relations*

See overview of the keys that are to be managed in the KMS in Figure 18:

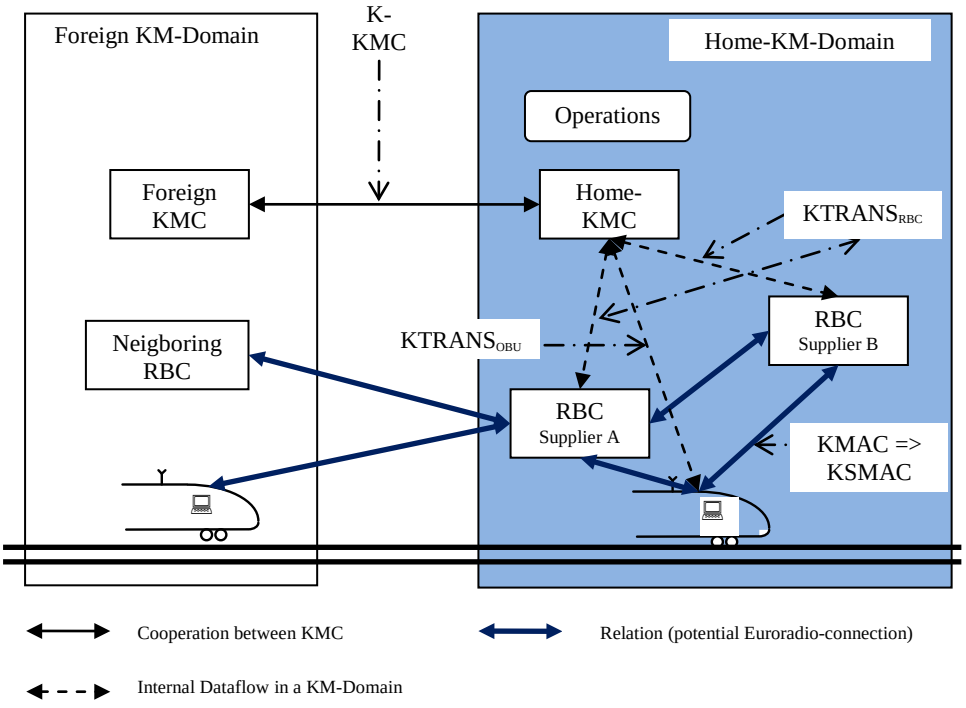


*Figure 11 - Application of keys*

Authentication KMACs are used in setting up secure vehicle-RBC connections and in crossing neigh boring domains.

For each Euroradio connection, a temporary KSMAC session key is derived from the authentication KMAC.

Note: Session keys are not managed by the KMS and therefore not covered throughout this document.

Transport keys KTRANS serve the purpose to distribute securely the authentication KMAC from the KMC to a specific ETCS entity. KTRANS is assigned to each ETCS entity. Each Transport key KTRANS contains two parts, a KTRANS1 part for assuring the data integrity and authenticity, and a KTRANS2 part for the encryption of the authentication KMAC.

Note: The actual application of the transport key depends on the interface to the ETCS entity.

The Transport keys K-KMC serve the purpose to securely exchange authentication keys between the home KMC and specific foreign KMC's. Each Transport key K-KMC contains two parts, a K-KMC1 part for assuring the data integrity and authenticity, and a K-KMC2 part for the encryption of the authentication KMAC.

Authentication KMAC, Transport KTRANS and K-KMC are managed by the KMC.

The methods for installing authentication keys in the Crypto components are supplier specific and therefore not covered in this document.

Authentication keys for OBU-RBC relations are hereafter referred to as authentication key OBU. Authentication keys for RBC-RBC relations are hereafter referred to as authentication key RBC.

*Reference Case key assignment principle*

The Reference Case considers the following key assignment principle:

- A KMAC is assigned to an OBU and it is used only within one KM domain.

*System components of the KMC*

The KMC contains the components:

- KMC Server with database.
- KMC Clients for operating the KMC Servers.

*Functions of the KMC Servers*

The KMC server provides the following functions for authentication keys and transport keys:

- Organization of the key management.
- Generation and validation of keys.

- Secure storage of all keys used in the domain (also keys that are generated by foreign KMC's).
- Distribution of keys.
- Managing the status of keys.
- Initiating key management tasks, such as key updates prior to their expiry.
- Generating requests to ETCS entities for installing, updating or deleting keys.
- Key exchange with foreign KMC's.
- Monitoring of deadlines.
- Monitoring the confirmations that distributed keys have been installed.
- Keeping the electronic log.
- Managing the archives.

*Functions of the KMC Clients*

The KMC Client is the user interface for the KMC. With this user interface, a user can perform the necessary key management functions corresponding to the role assigned to that user:

- Requesting key management actions.
- Retrieving keys.
- Confirmation that keys have been installed.
- Read status of keys.

Note: Also for online key management (KM) are Clients required, e.g. for requesting keys for a new vehicle.

*ETCS Entities*

The KMS regulates the cooperation with the ETCS entities. However, their internal processes are not subject to the KMS. Each ETCS entity must provide the following functions for authentication keys and transport keys:

- Receive key.
- Install key in ETCS trackside/ETCS on board.
- Use key in accordance with its validity (for the reference case, an unlimited validity is considered).
- Update key when requested.
- Delete key when requested.

*Principles of Key Management*

In the Reference Case, the following principles apply to Key Management:

- Only one KMC (the home-KMC (RBC-KMC)) is responsible for the generation, validation, archiving, distributing, updating and deletion of authentication keys for OBU – RBC and RBC-RBC relations, in accordance with the operational requirements for its KM domain.
- When a vehicle intends to establish secure connections with an RBC of another KM domain, the home-KMC of the vehicle must request the KMAC from the KMC of the foreign RBC (principle 2).
- KMC's have the same rang - No hierarchy exists between KMC's.
- For the establishment of Euro Radio – connections, only knowledge of the valid authentication key of the potential OBU – RBC relations is required. All other key material data shall not be relevant.

Security in the use of cryptographic methods is limited by the protection of secret keys. Facilities and programs should be used to prevent unauthorized reading, altering or processing keys. The proper use of these means shall be regulated by instructions and processes

Technical and organizational measures must ensure that no key can leave the protected environment unprotected or ineffectively protected, and that no unauthorized people can read or change any data.

This is governed by the following principles:

- Cryptographic material and passwords must be stored so that they cannot be read or manipulated by unauthorized people.
- Keys must be accessible by authorized personnel only.
- Trusted people must be appointed and authorized for each functional role.
- Access to keys must not be tied to a specific person.
- Any measure of key management is to be recorded so with details of the persons involved and methods used.

### *B.3.1.3 Distribution of keys and cryptographic material*

*Overview*

Authentication keys and key material is to be primarily distributed electronically by the KMC to the ETCS entities. At a Key Distribution Center (KDC), the manufacturer-specific tool takes over authentication keys from the KMC and distributes it to several ETCS entities. The KDC can store keys outside of the direct control of the operator/railway and their key policy.

No online end-to-end connection is implemented between KMC and ETCS entities, the distribution of the authentication keys is supported by KMC Clients.

The KMC Client can distribute keys to several pieces of ETCS equipment. It is separated from the KMC server and the KDC. There is an offline connection between server and KDC, and between KDC and ETCS equipment.

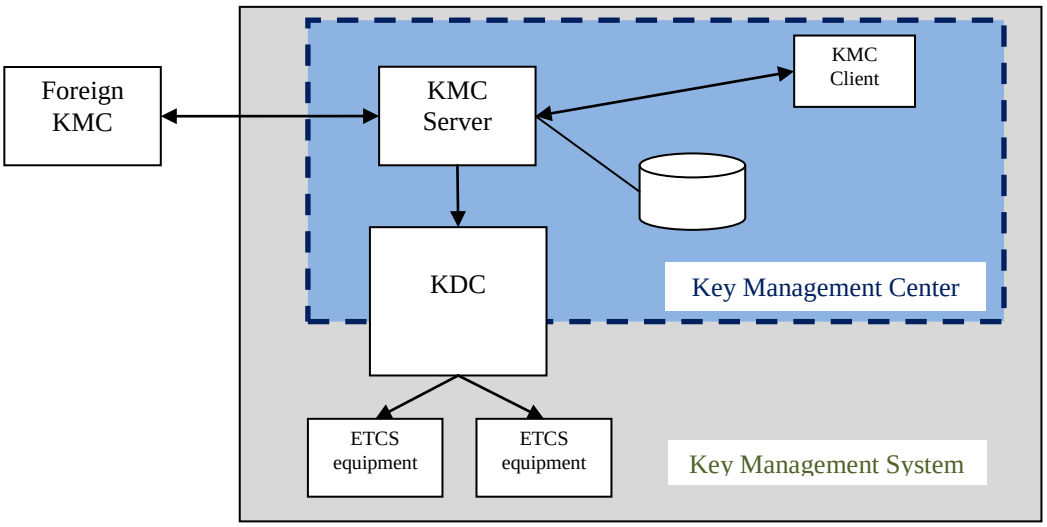


*Figure 12 - Reference Case Key distribution variant.*

*Key distribution from KMC to ETCS equipment*

The Reference Case assumes offline key distribution.

For offline Key Management, KMC Clients are used. The advantage of this approach, for instance regarding OBU Key Management, is the elimination of physical transport of a data medium with key data material between the KMC and the depot which is used for installing keys in the OBU. The KMC Client can be used as needed, and in the vicinity of the OBU.

The following steps must be taken when we speak of 'retrieving keys by means of KMC Clients':

- The authentication key is encrypted (according to the same procedure described in Subset 038 section 9.3) with the transport key KTRANS2 that is assigned to the receiving ETCS equipment or KDC.
- The integrity of key data including the encrypted authentication key is protected by a security appendix which is generated by using KTRANS1 (according to the same procedure described in [Subset-037] § 7.2.2).
- The key material and security appendix is written into a data record and provided by the KMC for the downloading by the KMC Clients.
- The Key operator(s) are informed by email that a key data record is available for download.
- One of the Key operators retrieves the data record by means of the KMC Client and creates a data file in accordance with the interface specification agreed upon for the respective ETCS equipment.

- The receiving instance (at OBU and possibly also at KDT or KDC) checks the security appendix.
- In case of a valid security appendix, the authentication key including associated key material is installed in the respective ETCS equipment during operation. For this reference case, it is assumed that authentication keys come to the ETCS equipment via a USB stick.
- The receipt, installation or deletion in ETCS equipment is confirmed to the KMC by the respective Key operator. For this reference case, this confirmation is sent via email.
- In case the check of the security appendix or the content of individual data fields resulted in errors or if the installation was not successful, a negative acknowledgment is sent to the KMC. For this reference case, this can either be done via e-mail or a phone call.

If a data record is sent without a key (e.g. prompt to delete a key) or with a confirmation of a specific action, then the steps to encrypt and decrypt are discarded.

Transport keys for ETCS entities and KDC are distributed off-line. The encryption and decryption between KMC and ETCS equipment is discarded.

*Key exchange between 2 KMC*

If a foreign KMC only supports off-line interface to the home-KMC, keys or key material can be downloaded via KMC Clients by the home-KMC. The following steps must be taken:

- Before sending it, the authentication key is encrypted according to Subset 038 section 9.3 with the transport key K-KMC2 that is assigned to the transport between the involved KMC's.
- The integrity of key data including the encrypted authentication key is protected by a security appendix which is generated by using K-KMC1 according to [Subset-037] § 7.2.2.
- The key material and security appendix is written into a data file and provided by the KMC. For this reference case it is sent by email.
- The receiving KMC checks the security appendix.
- In case of a formal validation and a valid security appendix, the received authentication key including associated key material will be taken over by the key management of the receiving KMC.
- The receipt must be confirmed to the sending KMC.
- In case the check of the security appendix or the content of individual data fields resulted in errors or if the takeover by the key management was not successful, a negative acknowledgment is sent to the sending KMC. For this reference case it can be done by email or via a phone call.

### *B.3.1.4 Functional roles and responsibilities*

*KMS Administrator*

The KMS Administrator is responsible for all administrative duties in his/her KM domain. The KMS administrator is allowed to perform all the functions that can be performed by the remaining roles. (Except the release of requested keys) He/she may also create KM domains and manage them.

Does an error occur during the key management, then the KMS administrator is responsible for solving problems that have arisen in an appropriate manner. Is a security incident noted in connection with the key management, it is the responsibility of the KMS administrator, to inform about this issue to all organizations and individuals that are affected or potentially affected. These places/people are: KMS administrators of other KM domains, Key Manager RBC and Key Manager OBU.

The KMS administrator is responsible for the administrative arrangements for key management between KM domains. The KMS administrator evaluates the electronic logbook of the KM domain.

For this reference case, it is assumed that there is one 'main' KMS Administrator, who is responsible for all OBU and RBC tasks. When needed, there are three other people within the organization who can perform the same tasks as the KMS Administrator, when needed. These people can decrypt the KMC key database and export it to the portable storage media if they would want to do so.

*Foreign KMC*

This role provides the functions to enable communication between a foreign KMC and the home KMC. The calling of features such as key transfer, key status change can be done not only by individuals but also by other key management systems of foreign KM domains that correspond to the specification according to [Subset-038].

### *B.3.1.5 Preparation/Planning*

*Choice of key assignment principle*

In this Reference Case, the following key assignment principle is used:

- OBU-RBC Relations: Principle 2 (one KMAC each OBU for all RBC's in the home-KM-Domain).

Justification: For OBU RBC relations KMAC one KMAC each OBU for all RBC's in the home-KM-Domain is sufficient, as compromised keys only lead to the failure of one vehicle.

*Definitions required for the KM domain*

The ETCS entities of the KM domain must be determined:

- RBC, that are managed by the KMC.
- OBU in the vehicles that are managed by the KMC.
- If needed, KDC for specific OBU.

The administrative arrangements for the key management in the KM domain must be determined:

- Start date of the KMS.
- Project specific parameters:
  - Necessary time parameters like e.g. lead time for the registration of vehicles in the key management, validity period of keys.
  - Necessary release of requested keys.
  - Handling of keys (offline distribution of keys). Within this reference case, no deadline for retrieving keys exists.

*Administrative arrangements between KM domains*

In general, the infrastructure manager – not the KMC manager - (or any other authorized body) decides which vehicles are allowed to travel on the network or on certain routes. Bilateral agreements with respect to the key management are required between the respective KM domains if home domain vehicles connect with foreign KM domain RBC or if foreign vehicles connect with home-KM domain RBC – when Euro Radio connections are intended.

The administrative arrangements for key management between the KMC include:

- Cooperation rules for adopting vehicles in the key management.
- Common security concept (e.g. procedures in case of irregularities).
- ETCS ID's of the KMC.
- Start and end date of the key exchange between KMC.
- Protocols to be used between KMC.
- Inter KMC key management (responsibilities for K-KMC generation etc.).
- ETCS ID's for RBC's of each other KM domain.
- Managing of RBC-RBC relations for neighbouring transitions, when the RBC's belongs to different KM domains (Responsibility for KMAC generation etc.).
- Deadlines for KM tasks.
- Information related to the authorized KM staff.

For specific regulation in the KM domains, there is a mutual obligation to inform about e.g.:

- Authentication key validity period for OBU-RBC relations.

- Key assignment principles for OBU-RBC relations.

*KM Personal*

Personnel must be selected, trained and authorised for the functional roles to carry out anticipated KM tasks.

### B.3.2 KMS behaviour of foreign KMC

For behaviour of foreign KMC, the KMS WG suggests that Reference Case shall assume that a Railway undertaking wants to operate between Country A and Country B. In Reference case, it shall therefore be assumed that the Railway Undertaking requests the Home KMC to obtain keys from the Foreign KMC, then hand them over to the Railway Undertaking, so that its OBU gets key relations with the foreign RBC's. In this way the foreign KMC and its behaviour is studied as a foreign KMC relation of the home KMC.

### B.3.3 KMS behaviour of home OBU operators

The final installation of keys in OBU/RBC is typically done by the OBU/RBC supplier companies. Before key delivery practice can start up, the Home KMC requires the supplier to comply with a policy on how key material must be handled in a secure way. Reference case shall use the Country C policy as the main measure of security for key material that has been handed over to a supplier.

### B.3.4 KMS behaviour of foreign or third party Railway Undertakings

Reference Case shall consider that the Home KMC has no assurance of secure key handling, but must rely on the due diligence of the Railway Undertakings.

### B.3.5 Transmission system

For the system and interface definitions, Reference Case shall consider GSM-R. However, this system shall be expanded for Reference Case in such a way that also leased data networks shall be considered as a potential part of the transmission system.

### B.3.6 Reference case highlights

To summarize the major points concerning the Reference Case solutions:

- Manual implementations of KMS.
- Systems are isolated - no networks attached, exchange through CD or (verified) USB.
- Only few KMC Operators handle all the requests, one at a time.
- Several people/parties hold keys offline.
- One KMAC key is assigned per train for all lines.
- One KTRANS key is assigned for each ETCS entity.
- KMC is running 24/7 high availability requirements (potential to harm train operation if down).
- Key validity period for KMACs and KTRANS is unlimited.
- KMC controls both RBC's and OBU's.
- There are stand-alone agreements between KMCs.
- Key distribution is done via incremental updates.
- GSM-R and leased data networks are used for secure communication, no public GSM.

# C Hacker terminology/Cybercrime

This chapter provides some background information on modern cybercrime. Additionally, some insight in hacker terminology used throughout this document is given, in order to understand better the various attack scenarios.

## C.1 Modern Cybercrime

Cybercrime is any form of crime committed using computer technology. The world is changing more and more to systems being fully interconnected 24/7, largely increasing the attack surface of modern IT infrastructures. This increased exposure allows attackers with various motivations, ranging from boredom to criminal or political motives to target these systems and commit cybercrime. Cyber attacks are becoming more standardized, automated, and easier to perform, eventually becoming one of the top global risks in terms of likelihood. The question is not anymore '*whether* a cyber attack will happen' but '*when* will it happen'.

Some attackers are interested purely in stealing money, others in exposing or paralyzing business operations of corporations and government agencies. The range of cyber adversaries varies from:

- **Individual hackers -** individuals who are making unauthorized attempts to bypass the security mechanisms of informational and operational systems for their own specific purpose. They can be either insiders (disgruntled employees) or outsiders (individual phishers, malware authors).
- **Industrial spies -** individuals or groups spying to obtain secret information for commercial purposes, for example on science and technology. The goals of cyber espionage can vary from saving money on research and development to undercutting a competitor's tender.
- **Organized crime groups** - groups that use computer systems and the Internet as the main element to create fraud, such as distribution of malware, phishing, and theft of valuable information such as credit card credentials. The goal is financial gain in various forms.
- **Hacktivists -** hackers who perform attacks for a politically or socially motivated purpose. Actions of hacktivists are not aimed at individuals, but rather companies or government entities with an attempt to cause disruptions to their networks and services in order to bring public attention to some political or social cause.
- **National governments -** governments that initiate state-sponsored espionage, for example for national security purposes, or deliberately perform sabotage in other countries as part of some political operation.
- **Terrorists** - terrorist groups that moved to cyberspace with an intention to use computer, networks, and public internet to cause destruction and harm for political or ideological objectives.

In the ERTMS context, cyber attacks can be expected from any combination of the above, where the main motivation is not financial gain but an opportunity to disrupt railway industry operations and create harm for individuals. It should be also noted that intrusions to disrupt

business and operation processes are nowadays happening more often than attacks with the aim of stealing money. This is also applicable to ERTMS.

Despite an attacker's identity or motivation, a successful intrusion could cost a company a lot of trouble. For railway industry the consequences can be: loss of railway industry mission capabilities, damages to railway industry assets, harm to individuals, reputational damage and financial losses.

Systems can be vulnerable on various levels, operating system level, application level, database level and protocol level. Attacks can be performed on logical level or physical level. Additionally, social engineering methods can be employed where an attacker uses various tricks (such as calling or pretending to be someone else) to obtain additional information about or gain access to the system.

The past few years, the industrial sector is more and more shifting from a safety to a security mindset. As an example, the energy sector can be observed. Components become more and more interconnected and common technologies are used more often. Therefore, the security of IT becomes more and more important as a security breach can have severe impact on the safety of employees within an industrial environment.

Companies start to acknowledge this. Where in the earlier days the main focus was on Health, Safety and Environment (HSE), the definition has now changed to Health, Safety, Security and Environment (HSSE) to also incorporate security. The same scenario applies to the railway environment where the components are considered to be 'safe' instead of 'secure'. The current mindset should change and should include security within the thought process and the full lifecycle of the environment.

**Cyber attack patterns for ERTMS**

Since the ERTMS specifications are public, an attacker with a motivation to identify vulnerabilities within the ERTMS infrastructure will be able to perform research fairly easy.

The systems used within the ERTMS infrastructure can be either based upon standard Operating Systems or on proprietary systems. The usage of standard software can increase the likelihood of a successful attack as known vulnerabilities may apply.

**Specific examples for ERTMS**

Due to confidentiality the examples are not included in this public version of the report.

## C.2 Hacker terminology

**Threat landscape**

The threat landscape can be considered as the total variation of threats an organisation or infrastructure faces and includes both internal and external threats ranging from malicious internal employees and contractors to professional external hackers and malware.

Over the past few years, the threat landscape shifted from unfocussed viruses created and attacks performed by bored teenagers to well funded targeted attacks aimed at specific companies and infrastructures.

**Attack surface**

The attack surface can be seen as the part of the system/infrastructure which is or can be exposed to an attacker/adversary. To be able to protect a system/infrastructure, it must be understood which part is actually exposed to the outside world, ranging from the network and application side to the physical/human side. Additionally, all interconnections between the infrastructure and other infrastructures should be known (physical and logical).

**Hardening**

Hardening is the process of securing a system by reducing the exposure and weaknesses of the system and reducing and controlling the available functionality to end users. Hardening guidelines should address at least the following subjects:

- System patching. Ensuring the system is up to date and does not contain any known vulnerabilities.
- Disabling unnecessary services. Services which are not required from a business perspective should be disabled or removed to reduce the attack surface.
- Secure configuration settings. Users should be limited in their rights to only functionality which is required for their daily operations.
- Anti-virus. Anti-virus applications should be used to reduce the chance of a virus/malware infection when removable media is used.
- Adequate password protection. Usage of trivial and non-complex passwords will make it easier for an attacker to guess or brute force the passwords.

**Specific explanations for ERTMS**

Due to confidentiality the specific explanations related to ERTMS are not included in this public version of the report.

# D Introduction to symmetric encryption technologies

## D.1 Introduction

Please note that this chapter is included to provide a basic understanding of the functioning of the encryption technologies used in ERTMS, and the underlying critical assumptions. This chapter cannot (and should not) be used to derive an evaluation of the overall security of the used encryption technologies, the security of ERTMS, and also cannot be used for deriving the parameters for the key renewal period.

## D.2 Basic overview and considerations

A block cipher is a cryptographic algorithm which takes unencrypted data, divides it into blocks of fixed size and encrypts the data block by a block with a given encryption key, examples are DES, 3DES and AES. The block cipher used in the Euroradio protocol is 3DES, which is based on the DES cipher, but it uses not one but three distinct DES keys.

Refer to paragraph D.3 for more background information on 3DES.

In the Euroradio protocol, the CBC-MAC construction is used to generate so-called message authentication codes (MACs) for messages and to derive session keys (KSMAC) from the long-term keys (KMAC).

Refer to paragraph D.4 for more background information on CBC-MAC.

### D.2.1 Considerations - it is all about the correct implementation, random values and secure keys

#### *D.2.1.1 Specific example*

Due to confidentiality the examples are not included in this public version of the report.

#### *D.2.1.2 Another industry example*

To provide some more background information, a similar situation is applicable to the older encryption technology used in wireless networks (802.11), known as WEP. WEP has to be considered insecure, but that is not mainly due to the fact that the used encryption algorithm is broken (considered to be weak for nowadays available computing power), but initially was caused due to issues with the exchanged random value known as the Initialization Vector (IV).

***Example issue 1: Weak random numbers***

For example, many hardware implementations of wireless cards provided a non random IV, which was often based on a counter that was reset every time the computer rebooted (or went to power safe mode). Quickly resulting in the same IVs being used over and over enabling an attacker to predict the correct session key and manipulate the traffic.

***Example issue 2: Induce fast generation of random numbers***

Another attack vector was related to the fact that, although on average still millions of IVs were required in order to crack the secret key, an attacker was able to speed up this process by rapidly requesting IVs at the target by specifically crafted messages at a rate of thousands per second, enabling an attacker to obtain the required number within a limited amount of time (reducing the attack from months/years to just a couple of hours or minutes).

***Example issue 3: Content prediction***

The former attack also inspired attackers to build knowledge on the IVs by predicting the content of the packages, which is in the case of TCP/IP networks doable due to the frequent transmission of for example ARP packets (resolving computer hardware addresses into IP addresses and vice versa). These packets are always the same size and the content is very much predictable, enabling an attacker to build knowledge of the session key used (as the encrypted message is available, the random value (the IV) is known and the content is partly available or guessable).

In summary the overall security is not only dependent on the security of the used algorithm but is dependent on many more factors such as:

- The correct implementation of the encryption algorithm
- Tamper resistance of the implementation to slow down crypto analysis
- The adequate functioning of the random number generators
- Generation of sufficiently random and secure keys
- The frequency of transmitted data
- Secure design and implementation of the Euroradio protocol
- The increasing computation power of attackers

## D.3 Background on DES, 3DES and AES

The Data Encryption Standard (DES) is an example of a block cipher. A block cipher is a cryptographic algorithm which takes unencrypted data, divides it into blocks of fixed size and encrypts the data block by block with a given encryption key. The Data Encryption Standard was developed in the early 1970s and uses a 64 bit key. By today's standards, the DES is considered broken because of its insufficient key length. This posed a problem, as developing a new block cipher is not a trivial task. As a stop-gap solution, the 3DES cipher was developed. 3DES with three distinct keys is the block cipher used in the Euroradio protocol.

3DES is a block cipher which is based on the DES. It uses not one, but three distinct DES keys, each 64 bits in length. It applies three rounds of DES encryption to the unencrypted data, one with each key. Even an attacker who is able to break DES would require an unfeasible amount of time to break 3DES, provided it is indeed used with three distinct keys and the assumptions mentioned in the previous and following paragraph are met.

The main disadvantage of 3DES is that it is slow: it requires three rounds of encryption for each block. A newer block cipher, the Advanced Encryption Standard, provides at least the same level of security as 3DES, but only requires one round of encryption for each block to achieve it. Its main advantage compared to 3DES is its speed; both ciphers are considered secure enough to use until at least 2030 by the U.S. National Institute for Standards and Technology (NIST)[4].

### D.3.1 Critical assumptions and difficulty

It should be noted that the time required to break 3DES is based upon the assumption that 3DES is implemented correctly and the used keys are sufficiently random and secure. The time needed to crack the encryption might be reduced considerably due to implementation errors or due to the usage of weak keys/small key spaces. Additionally, when key generation is not performed sufficiently random, the keys may be predictable.

## D.4 Background on message authentication codes (CBC-MAC with 3DES)

In the Euroradio protocol, a specific construction, CBC-MAC, is used to generate so-called message authentication codes (MACs) for messages. This construction is also used to derive session keys (KSMAC) from the long-term keys (KMAC). For several SaPDUs, a MAC is added to the message to show its authenticity and integrity (tamper-resistance). A MAC is generated by applying a key to the message in a specific way, which is commonly based on a block cipher. Any party who has the same key can verify the MAC. The CBC-MAC construction in the Euroradio protocol employs the 3DES cipher.

The CBC-MAC construction which the protocol uses is a variant of a construction specified in ISO/IEC 9797-1:2011. More specifically, it uses initial transformation 1 (encryption with the first of the three DES keys) and a variant of output transformation 3 (encryption with the second and third of the three DES-keys). This variant is probably at least as secure as the version described in the standard as it eliminates the reuse of the first DES key.

### D.4.1 CBC-MAC in the Euroradio protocol

In the Euroradio protocol, the CBC-MAC construction is used for key derivation and message authentication. The key derivation protocol may be summarised as follows (party A and B share the KMAC keys $k_1$, $k_2$ and $k_3$):

1 A and B both choose a random value ($R_A$ and $R_B$) and send these in their first messages to each other. These values are unauthenticated.

2 A and B both apply the 3DES keys they share ($k_1$, $k_2$ and $k_3$) in three different ways to the random values they provided to generate three KSMAC session keys $ks_1$, $ks_2$ and $ks_3$ with the CBC-MAC construction.

[4] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf. Please note that the 3DES cipher with three distinct keys is called 3TDEA (3-key triple data encryption algorithm) in this document.

3 The session keys are used to authenticate subsequent messages in the sequence. These subsequent message have a very structured format: other than the MAC, most messages will resemble those in other sessions.

### D.4.2 Critical assumptions and difficulty

The idea behind not authenticating the random values that both parties provide is that only someone with the KMAC keys will be able to derive the KSMAC keys. This is a valid assumption in principle, but it only holds when the random generator used to generate the random value generates enough distinct values. If one party ever reuses a random value to generate a session key, an attacker who eavesdropped on the earlier use of that particular random value will be able to replay any message passed in that session. This message will be interpreted as being authentic which may result in the ability to send specific commands, including movement authorities, possibly resulting a train stop, train derailment or train collision.