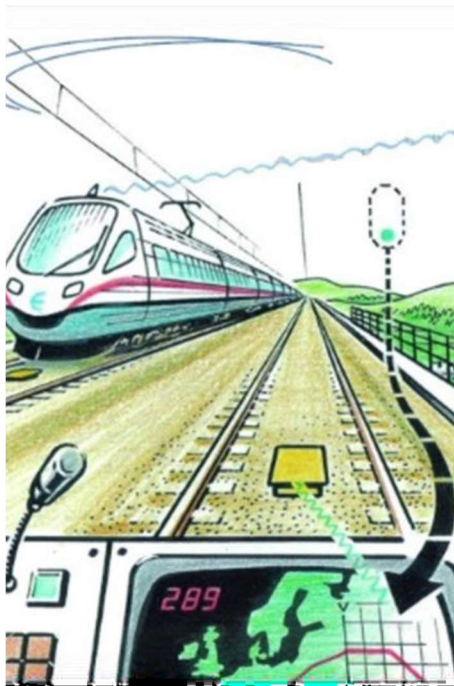


Market consultation

ERTMS – Towards a future-proof Key Management System (KMS)



Version	1.0
Date	22-4-2020
Status	Final
TN ref	TN 263123

Table of contents

List of Abbreviations	3
1 Future-proof Key Management System (KMS).....	4
1.1 Introduction.....	4
1.2 Objective	4
1.3 Scope	4
1.4 Structure.....	4
2 Key Management System (KMS).....	5
2.1 Introduction.....	5
2.1.1 Key Management System (KMS).....	5
2.1.2 Functional system decomposition.....	5
2.1.3 Intended architecture	7
2.1.4 Applicable technical references	8
2.2 Questions	8
2.2.1 Questionnaire KMC Solution.....	8
3 Procedure of the market consultation.....	11
3.1 Approach to the market players	11
3.2 Process	11
3.3 Planning	11
3.4 Rules of the market consultation.....	12

List of Abbreviations

API		Application Program Interface
ERTMS		European Rail Traffic Management System
ETCS		European Train Control System
GSM-R		Global System for Mobile Communications - Railways
KMC		Key Management Center: Central element in the KMS where an organisation can manage its keys under its responsibility
KMC Solution		Solution for a KMC which can consists of (1, or 1+2, or 1+2+3): 1. Application; 2. Platform (Hardware, Operating System - OS); 3. Services (Hosting, IT Management)
KMS		Key Management System; The (composition of) system(s) for performing key management
NS		Nederlandse Spoorwegen (Dutch Railways)
OBU		On Board Unit (Equipment): The equipment carried on the train with the aim of supervising vehicle operation
RBC		Radio Block Center
RU		Railway Undertaking

1 Future-proof Key Management System (KMS)

1.1 Introduction

The market consultation ERTMS KMS is a collaboration between, ProRail, NS and other railway operators. ProRail is the operator of the railway infrastructure in the Netherlands. NS is the principal passenger railway operator in the Netherlands and provides rail services on the Dutch main rail network.

The European Rail Traffic Management System (ERTMS) is the European standard for train protection. Systems based on this standard will serve as a replacement for the current ATB (Automatic Train Protection) system. The advantages of ERTMS lie in the areas of safety and interoperability, as well as in capacity, speed and reliability.

This market consultation for ProRail, NS and other railway operators (hereafter: initiators) will be directed by ProRail. The market consultation has as primary goal to gain insight into all possibilities for acquisition of a Key Management Center Solution (KMC Solution) resulting in a future-proof Key Management System. Initiators asks market players to provide answers on defined questions relating to the subject KMC Solution for a future-proof KMS for ERTMS. This particularly concerns aspects relating to the understandability and feasibility of the requested solution. Ideas for improvement are also requested from market players. This will allow initiators to reach a common understanding of the possibilities within the market, set high standards on quality and allowing the lead time for the possible tenders to be reduced. Initiators believe that it is important to obtain concrete information from those market players who are capable or have experience in delivery or development of a KMC Solution.

1.2 Objective

This document contains all relevant information for the ERTMS KMS market consultation: the process of the consultation, its conditions and more detailed information about the topic.

Initiators would like to clearly state that in this phase no parties will be selected. No rights may be derived from this document and/or participation in this market consultation within the framework of the possible future tender. Completion of the questionnaire is mandatory but if not, will not result in admission or exclusion in any possible future tendering procedure.

Initiators request market players only to respond to this market consultation when they are capable or have experience in delivery of a KMC Solution, as further detailed in chapter 2 of this document.

1.3 Scope

The scope of the intended assignment primarily consists of either delivery and implementation or development, delivery and implementation of a KMC Solution with possible supported services.

1.4 Structure

Chapter 2 contains more detailed content relating to the topic off the market consultation plus a questionnaire and in chapter 3 we provide an explanation of the market consultation procedure and rules of engagement.

2 Key Management System (KMS)

2.1 Introduction

2.1.1 Key Management System (KMS)

The KMS manages (data-)keys as used on the Dutch ERTMS-network. The ERTMS train protection system uses wireless communications over GSM-R. This communication is secured by these keys. This security setup requires that identical and valid keys are needed at both end points of a communication link. Without a valid key no 'train-track' communication is possible, and the ERTMS-train cannot run.

Secure communication, safe train operation

In order to maintain a secure communication these keys need to be secret and managed confidentially. Keys are generated from one source only and need to be transported and deployed to those locations / ERTMS entities which need secure communication.

Trackside entities are the Radio Block Centers, under the responsibility of ProRail. Train bound entities are the ETCS Onboard Units (OBU), with a responsibility by those as agreed when put into service. In general, these are train owners, keepers, operators or lease companies. Hereafter, referred to as Railway Undertaking (RU).

With a valid key onboard an ERTMS-train can run on a designated part of the Dutch ERTMS-network.

2.1.2 Functional system decomposition

The KMS is a composition of several systems. In Figure 1 a schematic overview is presented. The most common system in there is the KMC; Key Management Center.

KMC

With a KMC, an organization can manage its keys under its responsibility. Keys have a life cycle: key request, generation, distribution, loading, updating, consistency check, revocation and deletion.

Infra manager KMC

For the Dutch railway infrastructure only ProRail will generate keys and load relevant keys into the RBC's. In addition, keys will be securely transported to the Operator KMC. These tasks are performed by the ProRail KMC.

Operator KMC

The Operator KMC's request and receive keys from infra managers KMC, store these keys and then transfer these keys to the relevant on-board unit (train) at a suitable moment. These KMC's will monitor key validity and will request new keys before they expire.

The interfaces between subsystems are standardized by ERA and are a mandatory part of the TSI's¹. In the Figure below these are indicated with straight and dashed lines; this is not an indication of the amount of interfaces.

Offline interface

Dashed lines indicate "offline" interfaces, meaning no direct digital connection between the different entities. This can be a physical medium (USB, memory-card, CD or laptop) or included in an email to transport the messages to another location where the messages are imported in the KMC, RBC or OBU.

To secure the messages during transport a transport key is used.

This is the typical way of working in current ERTMS systems.

Online interface

Straight lines indicate 'online' interfaces where keys are securely transported over an electronic connection (either fixed network or GSM-R) directly between KMC's and RBC's or OBU's.

This is the future way to transport keys, with offline as fallback

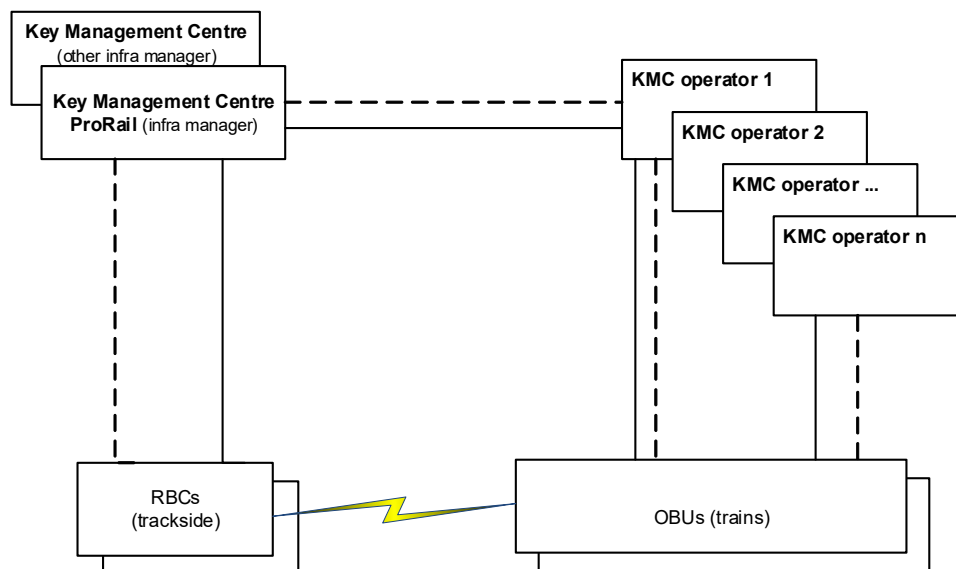


Figure 1: Key Management System is a composition of several subsystems

The operator KMC's have no inter-connections, just like the KMC's of infra managers have no inter-connections. An operator that operates on international ERTMS lines will have to contact the infra manager in each country to request and receive appropriate keys. In the figure this is indicated as "other infra manager"-KMC. The operator KMC will only connect to its own trains.

The lightning-symbol indicates the primary ERTMS communication between trackside and on-board unit that is secured with the exchanged keys.

¹Specifically, the TSI/CCS 2016/919, as modified according to EU Regulation 2019/776, in which Appendix A specifies the Set of Specifications #3 including the subsets Subset-038 (offline key management), Subset-114 (off-line interface), Subset-137 (online key management)

2.1.3 Intended architecture

In **Figure 2** below the intended architecture of the future-proof KMS is shown. The red circle indicates the scope of this market consultation (KMC and KMC-related components).

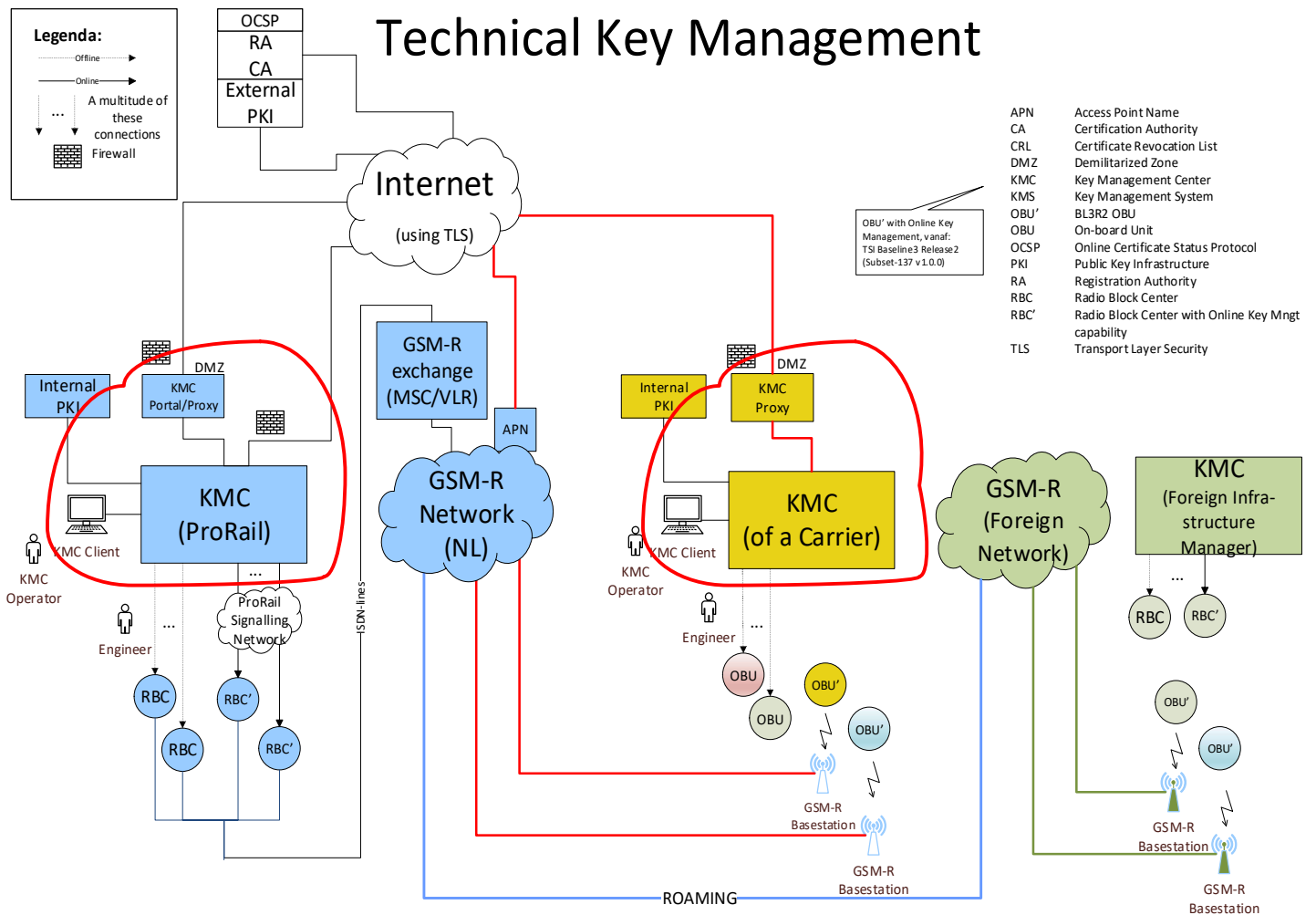


Figure 2: Intended architecture with indication of scope of this market consultation

A KMC manages the keys for securing the normal operational track-train-communication. This operational ERTMS communication between RBC and OBU is *not* shown in **Figure 2**, only the systems and communication that are required for key management.

A KMC supports the full life cycle of an ETCS key from creation to deletion. To do this efficiently, many parts need to be partly or fully automated, for example sending/receiving new requests, a response to the request, generating and sending/receiving keys. At the trackside the KMC will load keys into the RBC.

At the on-board side the KMC will indicate loading status of all keys. It will show which keys need to be loaded manually, and in the future, it will automatically distribute keys to the on-board unit through a wireless connection.

In addition to the automated functions, it must also be possible to perform manual administrative operations. A KMC Administrator must be able to monitor and manage the system.

2.1.4 Applicable technical references

In order to comply with prevailing European standards any future-proof Dutch Key Management System shall comply with at least the following standards:

- TSI CCS 2016/919, as modified according to EU Regulation 2019/776, Annex A, Set of Specifications #3
- Guideline 81 – Extension Key request function 1.0 which can be found at:
https://ertms.be/workgroups/engineering_support

2.2 Questions

In order to come to a future-proof Key Management System, the required KMC Solution should consist of the following item(s) (or combinations 1, 1+2 or 1+2+3):

1. Application
2. Platform (Hardware & OS)
3. Services (Hosting, IT Management)

2.2.1 Questionnaire KMC Solution

2.2.1.1	Which of the following is part of your KMC Solution? - Application; - Platform (Hardware & OS); - Services (Hosting, IT Management).
2.2.1.2	Do you already have a KMC Solution which supports: 1. Offline / online key management; 2. ERTMS Subsets 38, 114 and 137 (set of specifications #3 / Baseline3 Release2); 3. Sending keys towards RBC's; 4. Retrieving keys by OBU's; 5. Do you have any references where your solution is in use?
2.2.1.3	If not, what is the expected development time for such a KMC Solution?
2.2.1.4	Can you provide the key-requests as described in [EUG Guideline 81 Key Request Extension] in addition to the messages in Subset-137?
2.2.1.5	Can you estimate the price of the KMC Solution and the expected delivery time?
2.2.1.6	To what extent can you specify the cost structure of the KMC Solution (f.e. development, maintenance and change management / updates)?

2.2.1.7	Can you provide long-term support (approx. 25 years) and how?
2.2.1.8	What possibilities do you see with regards to maintenance, quality responsibilities, third party maintenance/application-management and intellectual property of your KMC Solution?
2.2.1.9	What kind of overview or reporting functionality does your KMC Solution provide?
2.2.1.10	Can your KMC Solution be used for both KMC's that support track side infrastructure and KMC's that support trains?
2.2.1.11	What security measures does your KMC Solution have and what risks are addressed by these measures? And how and according to what (cyber) security standards will this be managed?
2.2.1.12	How does your KMC Solution fit in the intended architecture as depicted in §2.1.3, Figure 2
2.2.1.13	Does your KMC Solution provide a portal and/or API for requests, exchange and management of Keys?
2.2.1.14	What do you think about a joint incremental development of the User Interface together with end-users? Can you describe how this fits in your development process?
2.2.1.15	Does your KMC solution provide a model where different users and roles can be applied in a flexible way?
2.2.1.16	Please describe how your KMC Solution can integrate with a centralized account directory?
2.2.1.17	Existing keys need to be migrated to your KMC Solution. How can your KMC solution import the existing set of keys?
2.2.1.18	In what way does your KMC Solution prevent loss of keys, also in case of system or datacenter failure?
2.2.1.19	In what way does your KMC Solution guarantee random keys of sufficient quality?
2.2.1.20	ProRail and NS expect your KMC Solution to run on their own server platform. Will this be possible with your KMC Solution or is specific hardware required? If so, describe the system requirements.
2.2.1.21	Generated keys may under no circumstance become available to non-authorized users over the entire life cycle of the keys, What measures does your KMC Solution provide to accomplish this? What additional (management) protocols do you suggest?
2.2.1.22	Describe how your development methods implement "Security-by-Design"?
2.2.1.23	In what way does your KMC Solution ensures that only authorized TLS-connections can be made?
2.2.1.24	How will your organisation and KMC Solution support: Releases, Updates and changes to the system?
2.2.1.25	How do you ensure interoperability of your KMC solution with on board and trackside ETCS equipment from other suppliers than yourself?
2.2.1.26	How do you ensure interoperability of your KMC solution with KMC solutions from other suppliers than yourself?

2.2.1.27	How do you ensure the quality of your key administration, i.e. ensure a realistic representation with respect to the keys that are actually present in the numerous on board and trackside ETCS entities?
2.2.1.28	How scalable is your KMC Solution? Can it work efficiently in a situation with 1000 trains of 10 different train types? Can your KMC Solution at least handle 50 track-side entities with each 10000 keys and what's the maximum?
2.2.1.29	How to migrate from offline key management tooling/procedures from various ETCS suppliers?
2.2.1.30	Does your KMC Solution provide interface possibilities with for example a fleet administration system?
2.2.1.31	How can your KMC Solution integrate with functional mailbox that is also used for manual key requests?
2.2.1.32	To your opinion, what is a good KMC solution for non-incumbent operators, with each a fleet of maybe 1-5 trains?
2.2.1.33	What operational services (f.e. key loading) can you offer as part of the Key management process?
2.2.1.34	What maintenance services can you offer for these cases?
2.2.1.35	To what extent does your solution use a single data model for all keys, managed by an operator or infra manager, independent of the type of key transport? (offline/online)
2.2.1.36	How modular, configurable and future proof is your solution with regards to operator/inframanager specific needs and cryptographic algorithms? (i.e. upgrade to TLS 1.3, reload root certificate)

3 Procedure of the market consultation

3.1 Approaching to the market players

This document has been published on TenderNed. Market players are requested to respond to this invitation. Insight in this market is of great value for the possible future tender procedure and much appreciated.

3.2 Process

Market players are requested to register for their participation in this market consultation in writing, before the date mentioned in section 3.3, to the following email address: rolf.jongeling@prorail.nl.

Please include your contact details (company, name, telephone, e-mail address). When doing so, please state your demonstrable experience in the subject area. The market consultation consists of two steps. At first, the participants will be asked to submit answers in writing to the questions as defined in chapter 2 of this document. Based on the replies and the final received answers several market players can and will be invited to participate in an individual, in-depth conversation. The consultation topics are of a varied nature and require expertise in various content, also detailed in chapter 2 of this document.

3.3 Planning

Below is a summary of the dates aimed for this market consultation:

Date	Activity by interested market player	Activity by Initiators
22 th of April 2020		Publication / invitation to participation market consultation by Initiators
13 th of May 2020	Deadline register participation for the market consultation	
20 th of May 2020, 12.00 hrs	Deadline for questions with regards to the provided information	
28 th of May 2020		Answers to received questions to the provided information by Initiators
10 th of June 2020, 12.00 hrs	Deadline for submitting answers to the questions as defined in Chapter 2	
June 2020	Individual in-depth conversations	
July 2020		Provide final report to all participants of the market consultation

3.4 Rules of the market consultation

Initiators have set out the following conditions pertaining to this market consultation:

- This market consultation is explicitly not part of the possible procurement procedure that may follow;
- Expressly no rights may be derived from the information that is provided for the purpose of the market consultation;
- As a result of participating in this market consultation, participants will not be given any preferential status with respect to the possible procurement procedure, nor will participation lead to exclusion from such a possible procedure;
- The market consultation is voluntary, no rights can be derived from the (insights resulting from) the market consultation and market players are understood to participate in the market consultation on a voluntary basis;
- Initiators will not provide remuneration for participation in the market consultation or for answering the questions;
- The target group for this market consultation is limited to market players who have demonstrable experience with KMC Solutions. The following parties are among those excluded from participation in this market consultation: public entities, interest groups, private individuals, the press and knowledge institutions;
- Initiators will draft an overall report of the main points of all of the individual market consultation meetings. This report will be made public (anonymous and without any commercially sensitive details);
- The primary language of the market consultation will be English;
- All communication regarding the market consultation, and submission of answers and/or reply forms, must take place via the following contact:

Rolf Jongeling, Tender manager ERTMS

Mail : Rolf.Jongeling@Prorail.nl

Tel : +31 6 14 49 08 53