EEIG ERTMS Users Group
123-133 Rue Froissart, 1040 Brussels, Belgium
Tel: +32 (0)2 673.99.33 - TVA BE0455.935.830
Website: www.ertms.be E-mail: info@ertms.be

ERTMS USERS GROUP – ENGINEERING GUIDELINE

81. Extension Key Request Function

Reference: 20E234
Version: 2-
Date: 2024-06-28

Modification history

Version	Date	Modification / Description	Editor
0.1	02/12/2019	First draft	J.Schoonen
0.2	02/03/2020	Comments after ESG80 and ESG81	JG
1	31/03/2020	Finalised	ATJ, GR
1a	2023-04-19	Reference number 20E068 replaced by 20E234 due to duplication	A. Bäärnhielm
1b	2024-04-08	Corrections to document style and layout, and editorial corrections.	A. Bäärnhielm
2-	2024-06-28	Official version	EUG

Table of Contents

1. Introduction

1.1 Foreword

1.1.1.1 Starting with Baseline 3 Release 2, the TSI CCS [2] contains On-line Key management for the safety layer. This function is described in SUBSET-137 [1].

1.1.1.2 In SUBSET-137 [1] section 5.2.9, a “Request Key Operation” is described. This function is intended to allow an on-board KMC to request for keys at a trackside KMC. The message-format, as described in section 5.3.9 of SUBSET137 [1] (see also Appendix A of this document), is too limited to support a fully automated KMC in certain operational scenarios.

1.1.1.3 This guideline describes a solution to provide the extra information for a key operation request while remaining fully compatible with SUBSET-137 [1]. This solution will allow automated processing of requests.

1.1.1.4 To allow automated processing both relevant KMC’s need to implement the same solution.

1.1.1.5 This guideline is part of a bundle of guidelines with the Overall ETCS guideline [3] being the main guideline which will redirect the reader to the relevant guidelines. Be aware that the Overall ETCS guideline may also include recommendations which are related to the topics addressed in this guideline.

1.2 Scope and Field of Application

1.2.1.1 This guideline is applicable for Key Management Centres (KMC’s) that support on-line key management as defined by SUBSET-137 [1], which was introduced in ERTMS/ETCS Baseline 3 Release 2.

1.2.1.2 This guideline provides the recommended solution to implement in on-line KMC’s to optimize key requests and enable full automation of the key management process. The decision to use an automatic process depends on the project.

1.2.1.3 This guideline is only applicable to the interface between KMC’s. On this interface the ETCS System Version is not relevant and therefore the guideline is applicable for all System Versions.

1.3 Document structure

1.3.1.1 Chapter 1 introduces the document and defines the scope.

1.3.1.2 Chapter 2 provides definitions, abbreviations and references used in this document.

1.3.1.3 Chapter 3 provides the extension of the key request operation.

1.3.1.4 In the Appendix A, a copy of the message structure as defined in SUBSET-137 [1] is provided.

2. References and Abbreviations

2.1 Abbreviations

2.1.1.1 The following table includes acronyms and abbreviations which are used in the current document:

Abbreviation	Description
KMC	Key Management Centre

2.2 References

2.2.1.1 The following documents and versions apply:

Ref. N°	Document Reference	Title	Version
[1]	SUBSET-137	On-line Key Management FFFIS	V1.0.0 2015-12-17
[2]	TSI CCS 2016/919	Regulation (EU) 2016/919	2016-05-27
[3]	22E087	Overall ETCS	1-

3. Extension Key Request Operation

3.1 Principles

3.1.1.1 With Online Key management the possibility is introduced to highly automate the key management process. However, with the messages as described in SUBSET-137 [1] it is not possible to fully automate the key request operation as essential information may be missing.

3.1.1.2 Most notably: it is not possible to request keys for a specific trackside (RBC). This can be the case if for example keys are required for the main line, but not for a freight or high-speed line. Another example is if for a certain line the train is not compatible with the infrastructure, keys would not be requested for this line (e.g. electric train would not request keys for a track without catenary).

3.1.1.3 Keys are typically generated by the infrastructure manager, however the KMC of the infrastructure manager does not have detailed knowledge about the trains for which keys are requested. Therefore, the KMC requesting keys should supply this information.

3.1.1.4 Another piece of information that is lacking, but very useful in analysis and troubleshooting between KMC and operator is the vehicle-name or number. Typically, operators are not very aware of the NID_Engine, but use names like e.g. “E186 089”, “Thalys-4306”, “BR189-360” etc.

3.2 Guideline

3.2.1.1 In SUBSET-137 [1] chapter 5.3.9, the message format for the Request Key Operation command is defined. The missing information can already be provided in the Text-field of the request-key-message. However, using natural language, does not enable automation in a reliable way.

3.2.1.2 Formatting additional information in the text-field in a well-defined format does enable automatic processing.

3.2.1.3 The solution described in this guideline is to use the optional free-format TEXT-field of the message structure defined in SUBSET-137 [1], section 5.3.9 to communicate additional information.

3.2.1.4 The following rules are used to allow automated processing of the TEXT-field:

Rule	Values	Comment
First 8 characters of the TEXT-field identify the special format to extend the key request operation as defined by this guideline	`SS137EXT`	If the first 8 characters are different or if the entire field cannot be parsed, the message will be processed according to SUBSET-137 [1] (free format TEXT).

The TEXT field is split into multiple subfields with a separation symbol	|	
Request keys for a trackside entity in Hexadecimal number	TRK-HEX:<ETCS-ID-EXP>	<ETCS-ID-EXP> as defined in SUBSET-137 [1]
Request keys for a trackside entity in decimal number	TRK-DEC:<ETCS-ID-EXP>	<ETCS-ID-EXP> as defined in SUBSET-137 [1]
Request keys for all trackside entities	TRK:ALL	
Vehicle name as known to operator	NAME:<text>	
Start date for keys	START:<VALID-PERIOD>	<VALID-PERIOD> as defined in SUBSET-137 [1]
End date for keys	END:<VALID-PERIOD>	<VALID-PERIOD> as defined in SUBSET-137 [1]
Contact information	CONTACT:<text>	
Free format text message for the operator	TXT:<text>	UTF8, excluding | symbol.
Request to resend all keys	RESEND	
Multiple subfields of the same type are allowed in any order		E.g. to request keys for multiple track-side entities
If multiple subfields provide conflicting information, only the first subfield is processed		E.g. in case multiple vehicle-names are provided
Unknown subfields are ignored		For future expansion

3.2.1.5 Example of the TEXT-field to request keys for 3 RBC's and providing a vehicle-name.

```
SS137EXT|NAME:Testtrain|TRK-DEC:23756900|TRK-
HEX:016AC00C|TRK-
HEX:016AC3F4|START:00050919|END:23311219|TXT:Thanks!
```

3.2.1.6 If one of the two communicating KMC's does not support the format described in this guideline, the information can still be read by a human operator in the TEXT-field.

3.2.1.7 Key requests that do not have information in the described format will be executed according to SUBSET-137 [1] and national rules.

3.2.1.8 The format can easily be expanded with additional information in case there is an operational need. This would lead to an update of this guideline but will not break existing implementations.

3.3 Interaction diagram

3.3.1 Key request interaction diagram

3.3.1.1 Figure 1 describes the key request interaction between on-board KMC and trackside KMC.

3.3.1.2 The request for a new key is initiated from the on-board KMC.

3.3.1.3 On reception of the request the trackside KMC checks whether the extension as described in this guideline is used. If this is the case the request can be automatically processed. If not, the KMC-operator has to add some information manually before the request can be processed and the key is delivered.

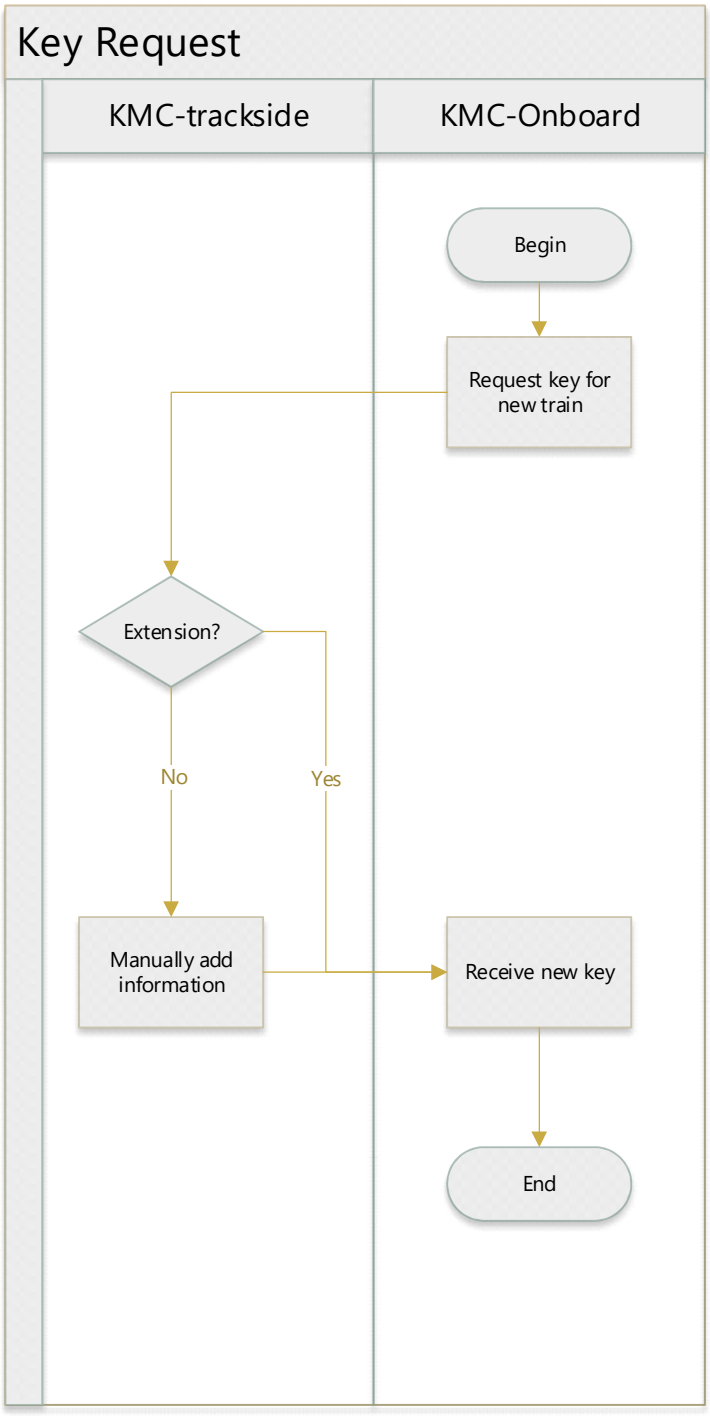

Figure 1: Key request interaction diagram

Appendix A Request Key Operation message structure

A.1.1.1 For easy reference, the entire message structure from section 5.3.9 of SUBSET-137 [1] is copied in this document (see Table 1).This guideline describes the usage of the field “TEXT” in this message.

Description	Message for requesting the issuing KMC to perform a key operation for a KMAC entity.		
Field	**Size**	**Value**	**Field description**
ETCS-ID-EXP	4		KMAC entity for which a key operation is requested.
REASON	1	0	New train operating in the issuing KM domain
		1	Modification of the area of operation in the issuing KM domain
		2	Reduction of scheduled permission in the issuing KM domain
		3	Approaching the end of validity period for some of the issued keys
		[4..200]	Reserved
		[201..255]	Undefined
VALID-PERIOD	8		Field to be included only if REASON = 2 Validity period as specified in § 4.2.3. Beginning date of validity period shall be equal to the beginning of the validity period of the key for which a request for reduction of scheduled permission is issued. End date of validity period shall be set to the date requested for reduction of scheduled permission.
PEER-NUM	2	[1..1000]	Field to be included only if REASON = 201 The number of peer entities following this field. At least one peer entity shall be specified.

ETCS-ID-EXP [PEER-NUM]	4*PEER-NUM		Field to be included only if REASON = 201 List of KMAC entities for which a key is requested Special value: 00000000 to request keys for all KMAC entities that are part of the issuing KMC.
TEXT-LENGTH	2	[0..1000]	Length of the optional text
TEXT	TEXT-LENGTH		Optional text to provide some extra information for a key operation request (if TEXT_LENGTH > 0). Text is encoded using UTF-8.

Table 1: CMD_REQUEST_KEY_OPERATION