



GN

Published by:

**RSSB
Block 2
Angel Square
1 Torrens Street
London
EC1V 1NY**

**© Copyright 2011
Rail Safety and Standards Board Limited**

GE/GN8603

Guidance on ERTMS Key Management

Issue 1 December 2011

Rail Industry Guidance Note for GE/RT8403



Documents
Document Sharing Hub

Guidance on ERTMS Key Management

Issue record

Issue	Date	Comments
One	December 2011	Supports national deployment of the European Rail Traffic Management System (ERTMS).

Superseded documents

This Rail Industry Guidance Note does not supersede any other Railway Group documents.

Supply

The authoritative version of this document is available at www.rgsonline.co.uk. Uncontrolled copies of this document can be obtained from Communications, RSSB, Block 2, Angel Square, 1 Torrens Street, London EC1V 1NY, telephone 020 3142 5400 or e-mail enquirydesk@rssb.co.uk. Other Standards and associated documents can also be viewed at www.rgsonline.co.uk.

Guidance on ERTMS Key Management

Contents

Section	Description	Page
Part 1	Introduction	4
1.1	Purpose of this document	4
1.2	Introduction	4
1.3	Copyright	5
1.4	Approval and authorisation of this document	5
Part 2	Guidance on Requirements for ERTMS Key Management	6
2.1	ERTMS Key Management Domain	6
2.2	Management of the ERTMS keys	6
Part 3	Application of this document	10
3.1	Application - infrastructure managers	10
3.2	Application - railway undertakings	10
3.3	Health and safety responsibilities	11
Appendices		
Appendix A	Overview of the GB ERTMS Key Management System	12
Appendix B	Functional Principles of the GB ERTMS KMS	14
Definitions		16
References		18

Guidance on ERTMS Key Management

Part 1 Introduction

1.1 Purpose of this document

- 1.1.1 This document gives guidance on interpreting the requirements of Railway Group Standard GE/RT8403 ERTMS Key Management, issue one. It does not constitute a recommended method of meeting any set of mandatory requirements.
- 1.1.2 All requirements in GE/RT8403 are reproduced in the sections that follow. Guidance is provided as a series of sequentially numbered clauses prefixed 'GN' immediately below the boxed text to which it relates. Where there is no guidance given, this is stated.
- 1.1.3 Specific responsibilities and compliance requirements are laid down in the Railway Group Standard itself.

1.2 Introduction

1.2.1 Background

- 1.2.1.1 ERTMS exchanges information between trackside equipment and trains and vice versa in the form of data messages; these data messages include movement authorities and other information which is fundamental to operation in ERTMS.
- 1.2.1.2 Data messages can be sent by radio. Particularly when using radio, it is important that the right data messages go to the correct train and to the correct trackside equipment.
- 1.2.1.3 When a radio link is being set up between the trackside equipment and a train, a process is used to determine that the trackside equipment and the train are genuinely what they claim to be so that the data messages can be routed correctly.
- 1.2.1.4 The process uses a complex mathematical algorithm to establish the communication link which requires the trackside equipment and the train to exchange secret numbers. Only when the secret numbers match the expectations of both the trackside equipment and the train can a communication link be created between the trackside equipment and a train so that information, such as movement authorities, can be sent.
- 1.2.1.5 These secret numbers are known as cryptographic keys and are essentially long numbers.
- 1.2.1.6 So that ERTMS can work, arrangements are required to provide that the cryptographic keys are installed in the correct trackside equipment and trains, and that they remain secret. To achieve this, when the cryptographic keys are created or deleted, they are protected themselves by other cryptographic keys.

1.2.2 Scope

- 1.2.2.1 This document is only applicable when ERTMS-fitted trains are operating on ERTMS-fitted infrastructure and when data radio communication is used.
- 1.2.2.2 GE/RT8403 ERTMS Key Management sets out national arrangements for the generation, distribution, request and deletion of cryptographic keys for the mainline railway so that the requirements in the HS CCS TSI and CR CCS TSI can be implemented. GE/RT8403 therefore complements (and does not duplicate or supersede) the requirements in the HS CCS TSI and CR CCS TSI.
- 1.2.2.3 The national arrangements in GE/RT8403 also include:
 - a) Establishment of a single key management area (ERTMS Key Management Domain) for the mainline railway.

Guidance on ERTMS Key Management

- b) Establishment of a single administrator for the ERTMS Key Management Domain.

- 1.2.2.4 Appendix A gives an overview of, and Appendix B sets out the functional principles for, the GB ERTMS Key Management System.

1.3 Copyright

- 1.3.1 Copyright in the Railway Group documents is owned by Rail Safety and Standards Board Limited. All rights are hereby reserved. No Railway Group document (in whole or in part) may be reproduced, stored in a retrieval system, or transmitted, in any form or means, without the prior written permission of Rail Safety and Standards Board Limited, or as expressly permitted by law.
- 1.3.2 RSSB members are granted copyright licence in accordance with the Constitution Agreement relating to Rail Safety and Standards Board Limited.
- 1.3.3 In circumstances where Rail Safety and Standards Board Limited has granted a particular person or organisation permission to copy extracts from Railway Group documents, Rail Safety and Standards Board Limited accepts no responsibility for, nor any liability in connection with, the use of such extracts, or any claims arising therefrom. This disclaimer applies to all forms of media in which extracts from Railway Group Standards may be reproduced.

1.4 Approval and authorisation of this document

- 1.4.1 The content of this document was approved by Control, Command and Signalling Standards Committee on 25 August 2011.
- 1.4.2 This document was authorised by RSSB on 19 October 2011.

Guidance on ERTMS Key Management

Part 2 Guidance on Requirements for ERTMS Key Management

2.1 ERTMS Key Management Domain

2.1.1 Architecture

- 2.1.1.1 There shall be a single ERTMS Key Management Centre (KMC) for the GB mainline railway. The architecture is set out in Appendix A.
- 2.1.1.2 Network Rail shall be the administrator of the GB ERTMS KMC.
- 2.1.1.3 An ERTMS entity shall not have the GB ERTMS Key Management (KM) Domain as its home domain if it is a member of any other KM Domain.

- GN1 Of all the possible architectures, this is the simplest, most efficient and hence the most cost effective solution. It has:
 - a) The minimum number of interfaces.
 - b) The minimum risk associated with possible ERTMS security issues.
 - c) One contact point for all stakeholders regarding ERTMS key management.
- GN2 The ERTMS Key Management System (KMS) is not a safety related part of ETCS. This is indicated in ERTMS/ETCS Subset-091.
- GN3 The roles of respective organisations involved in key management are defined in ERTMS/ETCS Subset-038.
- GN4 Membership of a single domain and the concepts of home domain / home KMC are stated in ERTMS/ETCS Subset-038.
- GN5 There is the potential for incompatibility issues for an ERTMS entity if it is a member of more than one domain, because there is nothing to determine whether unintended effects could arise within a Foreign KM Domain that may affect the GB ERTMS KM Domain. Therefore this standard is based on membership of a single domain, either the GB ERTMS KM Domain or a Foreign KM Domain.

2.2 Management of the ERTMS keys

2.2.1 Generation of keys

- 2.2.1.1 The ERTMS KMC shall generate the ERTMS keys and the associated messages for key operation to be used by the relevant Key Distribution Centre (KDC).
- 2.2.1.2 Each ERTMS key shall be assigned a unique identifier.
- 2.2.1.3 The unique identifier shall not relate to the content of the ERTMS key in any way.
- 2.2.1.4 For each Radio Block Centre (RBC) and Radio Infill Unit (RIU) the maximum validity period for an ERTMS key shall be chosen.
- 2.2.1.5 The maximum validity period for a RBC or a RIU ERTMS key shall be notified to the GB ERTMS KMC administrator.
- 2.2.1.6 The validity period of an ERTMS key shall be no longer than the shortest validity period specified for any RBC or RIU on which it is to be stored.