Lead Standards Committee:	Control Command and Signalling	**Date:**	
Supporting Standards Committee:	Traffic Operation and Management	**Date:**	
Subject:	60-month review of RIS-0743-CCS issue 1, *ERTMS Key Management.*		
Sponsor:	Ged Neacy		
Author:	Alex Savopoulos		

1. Purpose of the paper

1.1 This paper sets out the outcome of the 60-month review of RIS-0743-CCS issue 1, ERTMS Key Management. Standards Committee(s) approval and support is sought for the recommendations and way forward.

2. Background

2.1 The European Rail Traffic Management System (ERTMS) involves the exchange of information between trackside equipment and trains and vice versa in the form of data messages. When radio is used for these data messages a secure connection is required, and corresponding keys must be available on either side of the connection.

2.2 As set out in RIS-0743-CCS, for the GB mainline there is one National ERTMS Key Management Centre that covers online and offline key management which is administered by Network Rail This was considered the simplest, most efficient solution because it has the minimum number of interfaces and has low risk associated with possible ERTMS security features, and provides one point of contact for all stakeholders regarding ERTMS key management.

2.3 RIS-0743-CCS is used by Railway Undertakers (RUs) and Infrastructure Managers (IMs) and covers requirements, guidance and rationale on:

a) Requesting an ERTMS Key including the details the applicant provides

b) Conditions that need to be achieved for the GB KMC to issue an ERTMS key

c) Deletion of an ERTMS key

d) De-registration of an ERTMS key

2.4 The NR Online Key Management System programme started around 2018/2019. Although the initial concept was to align all components of the key management process to the one national OKMS as envisaged by the RIS, it was determined that it was not economically feasible to migrate to a single KMCs at the same time. The applied solution is to retain the legacy systems offline until when it is operationally and financially feasible to migrate them into the national GB OKMS in future.

2.5 The current GB ERTMS deployments rely on offline key management where cryptographic keys enable ERTMS train-to-trackside communications. To work, they are manually installed on RBCs (Radio Block Centres) and OBUs (Onboard Units) via the Key Management Centres.

2.6 The legacy KMCs will remain in place until such point that the entities are upgraded to Baseline 3 Release 2 (v3.6.0) and therefore capable of online distribution. It is anticipated that this upgrade will be later for the legacy RBCs than the OBUs and therefore the RBC would need to remain under the legacy KMC for some time. This introduces a KMC-to-KMC interface, as the OBU would now be operating under the OKMS key management domain, whilst the RBC remains under the legacy KMC key management domain. This interface will be via the offline KMC-KMC messages defined in Subset-038.

2.7 As at the time of this 60-month review there is no known available evidence that the RIS has been used, and the intended one GB KMC as envisaged by the RIS is yet to happen. Instead, there are presently five (5) independent KMCs that are for Cambrian, Thameslink, GWML 0-12, RIDC Melton Mowbray and Northern City Line respectively.

3. Impacts on the standard(s) following publication/entering into force

3.1 Consideration has been given to the following during the assessment:

a) Business case for change – RIS-0743-CCS issue one was published before RSSB introduced the business case for change process.

b) Deviations – RIS-0743-CCS is a RIS, therefore there is no obligation to seek approval from an RSSB standards committee to deviate from a requirement.

c) Current projects or proposals being processed:

3.2 There is an ongoing related Network Rail programme, the Online Key Management System (OKMS) and its output has an impact on this RIS (discussed below).

3.3 Relevant notes and specific changes required - In discussion with the OKMS programme the following items are suggested updates to the RIS:

(i) That the RIS be reviewed and amended to recognise and include the existence of multiple legacy Key Management Centres (KMCs) as they are presently in operation though not mentioned in RIS-0743-CCS issue one.

(ii) The requirements, guidance and rationale to be updated to accommodate the change from ‘GB KMC’ to ‘GB Key administrator’ and guidance to explain interaction between new online KMC with the legacy KMCs. Network Rail, National Records Group (NRG) is the ‘GB Key administrator’.

(iii) That the RIS be amended to highlight that the legacy KMCs would remain functional until further notice.

(iv) That the RIS be amended to recognise and structure the envisaged ongoing legacy KMCs interaction with the national GB KMC.

(v) That the RIS explains that full Integration of all the KMCs into the single OKMS will be achieved in the future after Baseline 3 Release 2 or a later baseline is implemented on all RBCs and OBUs.

(vi) That the RIS is reviewed against the OKMS high-level process and procedures document when it is formally published by the OKMS programme. Noting the review will focus on the high-level interface between users and the OKMS to make sure that terminology is consistent and whether additional guidance can be incorporated in the RIS.

d. Limited change release - no limited change release has been published.

e. Amendments and clarifications – RIS clause 2.1.2.1(a) and (b) - The OKMS programme have suggested that time is not included in the requirement since keys can only start at 0.00am.

f. Enquiries – there have been no enquiries recorded against this standard.

g. Research projects - No relevant RSSB research projects are currently ongoing which overlaps this standard’s subject matter.

h. Changes in Regulations - There are no changes in regulations that impacts on the content of this standard.

I. Changes to Technology - When existing ETCS equipment migrates to baseline 3 release 2 this is the most economic time to migrate over to the OKMS.

j. Any other observations:

The following are observations which will be considered in the development of RIS-0743-CCS Issue Two:

i.) Clause 1.3.1 of RIS-0743-CCS issue 1, ERTMS Key Management indicates that RSSB members and other stakeholders may choose to adopt this standard if they choose to. This needs clarity as all key management is to happen in accordance with the standard, so it would not be optional.

ii.) Clause G 2.2.6.5 indicates that unwanted ERTMS keys are to be deleted but does not say how that may be done to ensure complete erasure and avoid having residual data that may lead to data compromise. Further guidance will be included on this.

iii.) Appendix A indicates in A.1.3 BS EN 50159:2010 cryptography be applied but this standard has since been withdrawn and replaced with EN 50159:2010+A1:2020 so same should be reflected in the revised RIS. EN50159:2010+A1:2020 should be reviewed to determine whether any changes to the RIS are required.

iv.) The KMS Guideline 2023 issued by the ERTMS User Group (EUG) aims at proffering solutions for the existing gaps between the interface descriptions of ETCS Key Management, needed KMC setups and needed inter-KMC arrangements. This guideline needs reviewing and anything considered necessary will be captured in the revised RIS.

3.4 Review outcome

3.4.1 RIS-0743-CCS requires changing to address the observations raised in section 3 above. The main change is for the standard to reflect a change in architecture, currently the RIS only recognises a single GB ERTMS KMC whereas the new standard needs updating to reflect that there will be a National Key Management System that interacts with multiple legacy KMCs which will eventually migrate to the final solution of a National Key Management System.

4. Recommendations

4.1.1 The standard committee(s) is asked to:

a) DISCUSS the assessment of the five-year and the proposed recommendation:

Action required: Initiate a change project.

b) APPROVE/SUPPORT as appropriate:

The Lead Standards Committee to approve the recommendation and the next review date.

The Support Standards Committee(s) to support the recommendation.

c) APPROVE conclusion of the review process.

RSSB completion: [do not delete]

Standards Committee	*Meeting date*	*Decision*	*Minute numbers*		*Next review date*
			Pre-consultation review	*Post-consultation review*	
CCS		Approved			
TOM		Supported			

Appendix A Disposition table for standard(s) recommended for withdrawal

A.1 Standard number, title, issue [one table per standard]

Clause number	Clause title	Way forward	Comments

Reference:

NIST SP 800-57 Part 1 Rev. 5	Recommendation for Key Management
School of Computer Science, University of Birmingham	TRAKS: A Universal Key Management Scheme for ERTMS
17 BN04, RSSB	Briefing Note: Revised Train Voice Radio requirements
147906-TCL-REP-EMG-000014	Online Key Management System (OKMS) Processes and Procedures Issue-One. (Prepared by THALES).

Appendix B -Associated information to support the review

The information in this appendix is provided by the industry groups information manager to assist with the review. This appendix should be deleted prior to submitting the review form to the SCs.

Deviations	Nil	Nil
Request for Help	Nil	
Proposals	Nil	
RSSB Standards Programme	This document is currently not on the RSP.	
Amendments or clarifications	Nil	
Limited change releases	New document based on requirements and guidance from withdrawn GERT8403 Iss 1 and GEGN8603 Iss 1, and the latest ERTMS knowledge and requirements. 12-month review - No further action. 60-month review to be brought forward to 1/3/2021. Committee approved the proposal to revert to the 2023 five-year review date.	
Enquiries	There are currently no enquiries recorded against this document in the CRM. Please confirm with all Technical Specialists.	
Business case for change	No formal business case for change but the Network Rail project would lead to some changes.	
Information from RMDB Note: update RMDB to reflect action/decision	Nil.	
Other intelligence and relevant information	Any sources of supporting information, if anecdotal this should be clear, or referenced appropriately if not.	