EEIG ERTMS Users Group – KMC Expert Group

KMS Guideline

23E064
1A
24.05.2023

Modification history

Version	Date	Modification / Description	Editor
0A	26.04.2023	Initial Draft by EUG KMC Expert Group	Metz, Roger Poschinger, Richard
0B	24.05.2023	Updates after EUG KMC Expert Group Review	Metz, Roger Poschinger, Richard
1A	24.05.2023	Final version agreed by the EUG KMC Expert Group	Metz, Roger Poschinger, Richard

Table of Contents

Table of Figures

1 Introduction

1.1 Scope

1.1.1.1 The purpose of this document is to fill the solution gap between the interface descriptions of ETCS Key Management, needed KMC setups and needed inter-KMC arrangements. It aims to provide recommended solutions for KMC setups and inter-KMC arrangements. It presents results of the 2022 and 2023 workshops of the EUG KMS expert group and consolidates the results with the measure documents of the ERTMS Security Core Group (ESCG). The document expands the definitions of the 2015 EUG KMS documents and focuses on presenting new results.

1.2 References

1.2.1.1 Subsets and EUG publication are referenced directly with their corresponding ID.

1.2.1.2 Other referenced documents:

[1] *RFC 2119,* 1997.

1.3 Abbreviations

AES ..... *Advanced Encryption Standard*
CRL ..... *Certificate Revocation List*
ESCG ..... *ERTMS Security Core Group*
EUG ..... *ERTMS Users Group*
IM ..... *Infrastructure Manager*
LZMA ..... *Lempel–Ziv–Markov chain algorithm*
OCSP ..... *Online Certificate Status Protocol*

ERTMS Abbreviations are listed in SUBSET-023

1.4 Authors

1.4.1.1 The following members of the EUG KMC Expert Group were involved in creating this document:

- ERTMS User Group (EUG)
  - Richard Poschinger
  - Roger Metz

1.5 Applicability and Document Status

1.5.1.1 In order to ensure the usability for tender documents, this document is using classifications and requirement key words. This classification does not result in any binding requirements for members of the EUG or other involved parties. The documents will be updated in the future to be adapted to a changed threat landscape, updated standards, and newly developed security solutions.

1.6 Definition of Requirement Types

1.6.1.1 This document uses key words indicating requirement levels according to RFC 2119 [1]. Each clause in this document is classified as follows:

M	Mandatory	function must be implemented as specified
O	Optional	not mandatory, must be as specified if implemented
I	Informative	included for clarification purposes only
R	Recommendation	included as recommendation

Texts without a tag do not constitute a requirement.

2 Guideline

2.1 Application of 2015 ORS and FRS Document

2.1.1.1 The 2015 Organizational Requirements Specification (ORS) [EUG 14E040] and Functional Requirements Specification (FRS) [EUG 14E039] were used as the EUG input to On-Line Key Management which resulted in Subset 137. These documents are available to members of the EUG. **(I)**

2.1.1.2 These original inputs contain some differences to the interface definition in Subset 137. **(I)**

2.1.1.3 The ORS and FRS documents contain a broader scope than the interface definition. **(I)**

2.1.1.4 The following chapters of the 2015 FRS document are recommended for the implementation of an On-line KMS: **(I)**

- Chapter 3.5 Functional requirements related to performance and availability of on-line KMS
- Chapter 4 Key Management Functions

2.1.1.5 The following chapters of the 2015 ORS document are recommended for the implementation of an On-line KMS: **(I)**

- Chapter 3.3 KMAC related scenarios
- Chapter 3.7 Degraded modes

2.2 ESCG Measures Implementation

2.2.1.1 The ERTMS Security Core Group has created security measures which can be used as an input to tenders for ERTMS components. **(I)**

2.2.1.2 The following measure documents have been published and are a recommended input regarding KMS security: **(I)**

- Recommended Security Measures SoS3 [EUG 23E058]
- Recommended Security Measures Future TSI [EUG 23E057]

2.3 Contact Details

2.3.1.1 During the processes of the described scenarios personal communication between the key managers of both KMCs might be required. To limit the risk of identity theft in this communication the EUG provides a platform for securely exchanging contact information. The contact information of the key managers is provided signed by the KMS representative of the corresponding organization and only shared internally via a platform which requires authentication. **(I)**

2.4 Key Validity

2.4.1.1 The impact of compromised KMACs can be reduced by changing the key regularly. A key validity period of less than two years is recommended. This might not be applicable for Off-Line KM for operational reasons. **(I)**

2.5 Security Agreements

2.5.1.1 To prevent compromission of keys, the secure handling of keys across all involved organization needs to be ensured. Through binding agreements, these requirements can be defined and enforced between the KMS owners. **(I)**

2.5.2 Between IM and Home KMC Owner of the Vehicle

2.5.2.1 The following proposals can be used by the Infrastructure Manger (IM) to ensure mutual trust and the security of key handling of home KMC owner of the vehicle using or connecting to the IM's key domain. **(I)**

2.5.2.2 The IM may require the home KMC owner of the vehicle to establish an ISMS which includes the KMS scope. **(R)**

2.5.2.3 The IM may require the home KMC owner of the vehicle to proof the implementation of an ISMS which includes the KMS scope using certificates. **(R)**

2.5.2.4 The IM may require the home KMC owner of the vehicle to implement security requirements issued by the EUG. **(R)**

Note: The requirements applicable for the vehicle owner are a subset of the requirements proposed in the EUG KMS Guideline and ESCG documents.

2.5.2.5 The IM may require the home KMC owner of the vehicle to ensure audits of KMS specific requirements conducted by **(R)**

- a qualified independent auditor
- or a regulatory body
- or auditors provided by the IM.

2.5.2.6 The IM may define procedures and rules for handling infringements of this agreement. **(R)**

2.5.2.7 If the KMC is operated as a service these requirements may be implemented to the service provider. **(R)**

2.5.2.8 The IM shall ensure that the security agreement is compliant to European (inter alia non-discriminatory and transparent conditions for access to railway infrastructure) and country-specific law. **(M)**

2.5.3 Between IM and foreign IM

2.5.3.1 To ensure mutual trust and the security of key handling, the IMs may establish bilateral agreements regarding security integrating the security requirements issued by the EUG. **(I)**

2.6 Secure Transfer in Off-Line KMS using Encrypted Archives

2.6.1.1 ESCG requires the encryption of transferred secret keys using AES 256 according to M_001 of the ESCG Security Measures SoS 3 [EUG 23E058]. **(I)**

2.6.1.2 The key manager may encrypt secret keys using encrypted archives. **(R)**

2.6.1.3 The following options are available: **(I)**

- 7z format with AES 256 including file name encryption and LZMA compression. (recommended)
- Zed Encrypt
- Gpg4win

2.6.1.4 The password used to encrypt the archive shall contain at least 12 characters, 4 different types of characters and shall be randomly created. **(M)**

2.6.1.5 Further requirements on protection of secret keys are available in ESCG Security Measures SoS 3 [EUG 23E058]. **(I)**

2.6.1.6 If the encrypted archives are sent via e-mail, receiver or sender side filters might block the transfer of these attachments. Whitelisting of these file extensions and types might be required for email accounts used for key management based on encrypted archives. **(I)**

2.6.1.7 To ensure secure long-term development of Off-Line KMS the 3DES encryption of transferred KMACs in Subset 038 and Subset 114 needs to be replaced by a state of the art and cryptographically secure encryption algorithm. This change would affect interoperability and requires changes in an upcoming TSI. The EUG KMS group will evaluate if a change request regarding the usage of a secure encryption algorithm can be raised. **(I)**

2.7 Packet Inspection for KMS Connections

2.7.1.1 The protection of network perimeters requires detailed monitoring of the network. This means that the inspection of packets might be required at the organizations or zone boundaries. If packet inspection is applied for online key management connections traversing these boundaries, the content of the TLS connection might be decrypted before it reaches the endpoint of the KMC. Hence the content of the KM connection can be analysed. **(I)**

2.7.1.2 The following implications on security are expected: **(I)**

- Breaking the paradigm of end-to-end protection might result in a loss of integrity and confidentiality as no uninterrupted cryptographic protection is ensured between both endpoints.
- As KMACs are included in the inspection process, the KMACs are processed outside of the KMS environment.
- Vulnerabilities of packet inspection systems impact the security of the KMS.

2.7.1.3 These aspects can result in **(I)**

- the compromise of transferred KMACs which leads to a loss of security of Euroradio connections and a possible impact on the systems safety.
- the compromise of transferred KMACs which leads to a revocation of KMACs and a potential operational unavailability of the system.
- the compromise of transferred KMACS which can be used to setup a faked KMAC entity and a possible impact on the safety of the system connected to this entity.
- the manipulation of transferred KMACs which can result in the operational unavailability of the system.

2.7.1.4 Figure 1 illustrates the use of packet inspection tools in key management connections. In this case the green operator inspects packets transferred between its own KMC and the KMC of the blue organization. **(I)**

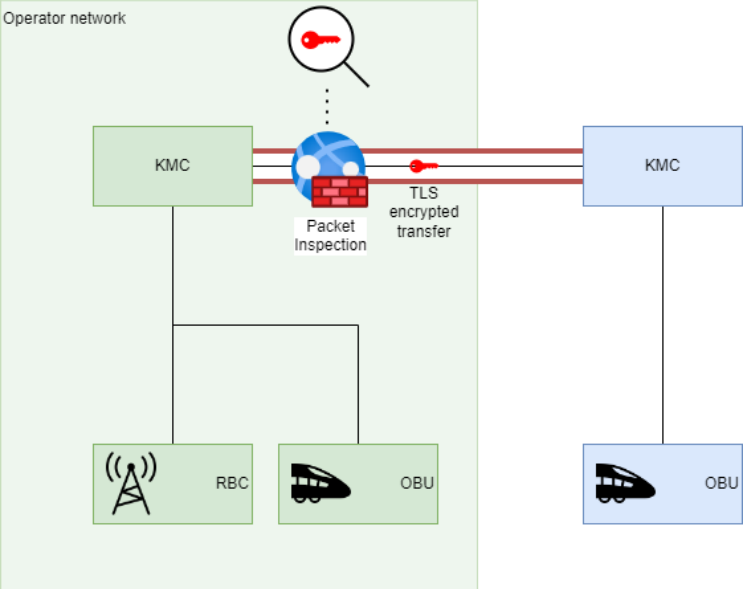

Figure 1: Packet Inspection

2.8 PKI

2.8.1.1 The following chapters provide fundamental information and requirements for an online KMC PKI. The aspects of availability, structure, and migration from an initial national solution to an international solution are covered. **(I)**

2.8.2 PKI related Unavailability

2.8.2.1 According to the results of the ERTMS User Group KMC workshops the following was defined: **(I)**

- The recommended maximal downtime of the PKI services is 72 hours.
- Improvement of resilience can be achieved through second or third PKI (Internet PKI).
- Improvement of resilience and independency when applying own roots in addition to an Internet PKI.

2.8.3 Registration Authority

2.8.3.1 The framework needed for standardisation of an interoperable enrolment procedure should allow for a certain freedom of choice in the actual implementation. It is imperative that a good and flexible enrolment process is developed considering standardised implementation best practices. **(I)**

2.8.3.2 Enrolment procedures are described in 2015 ORS [EUG 14E040]. These procedures are partly based on outdated assumptions and not compliant to Subset 137. **(I)**

2.8.4 Certification Authority

2.8.4.1 The Certification Authority (CA) shall be the trusted party responsible for validating the identity of the KMS entities. **(M)**

2.8.5 Certificate Revocation

2.8.5.1 Two certificate revocation technologies exist: **(I)**

- Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate and is required according to Subset 137.
- Certificate Revocation List (CRL) is a list of digital certificates that have been revoked by the issuing certificate authority.

2.8.5.2 The CRL is easier to maintain and use than the OCSP approach and therefore the preferred solution from the EUG KMC Expert Group if there is centralized management. The implementation of CRLs may only be considered inside a KMS domain to avoid conflicts in interfaces relevant for interoperability. The usage of CRLs in future TSI depends on changes introduced by Subset 146. **(I)**

2.8.5.3 A OCSP responder (a server typically run and maintained by the certificate issuer) shall be available, if OCSP is used. **(M)**

2.8.5.4 The accessibility to the CRL or to the OCSP responder including the mobile networks (GSM-R/FRMCS and roaming) shall be ensured. **(M)**

2.8.6 Network Separation across PKIs

2.8.6.1 As the KMS entity (e.g. a train) needs to connect to its own home KMC it requires a connection to its PKI. The PKI of the home KMC might be part of another network e.g., if the train is driving in a foreign infrastructure. Hence the entity needs access to amongst others its corresponding OCSP responder. **(I)**

2.8.6.2 Figure 2 shows a possible solution, with an additional interface to an external CRL/OCSP. **(I)**

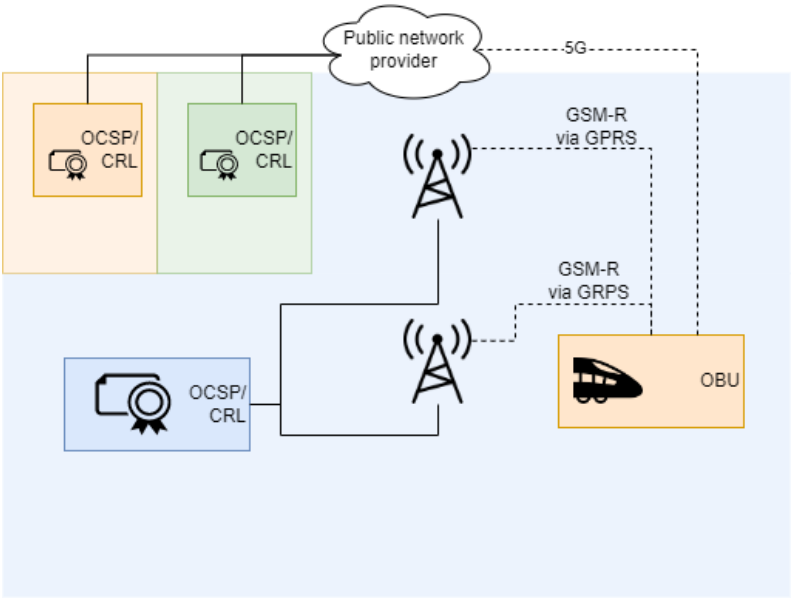

Figure 2: Connection to CRL/OCSP

2.8.6.3 Network separation and connectivity to CRL or OCSP (e.g.: category 2 networks for ETCS and interlocking) shall be considered. **(M)**

2.8.6.4 Security analyses for this potential external interface shall be performed. **(M)**

2.8.6.5 Security requirements for this potential external interface shall be specified. **(M)**

2.8.7 Trust between two KMCs (not belonging to the same CA)

2.8.7.1 Using Online KM both KMCs establish a trust relation, as explained in the following chapters. **(I)**

2.8.7.2 The EUG KMC work group plans to work on a centralized joint approach which is the preferred solution. **(I)**

2.8.7.3 Migration from one PKI model to another PKI model and the support of different PKI models simultaneously shall be possible. **(M)**

2.8.8 Trust between two KMCs using Trusted Peer Leaf PKI

2.8.8.1 Figure 3 shows the Trusted Peer Leaf Model. **(I)**

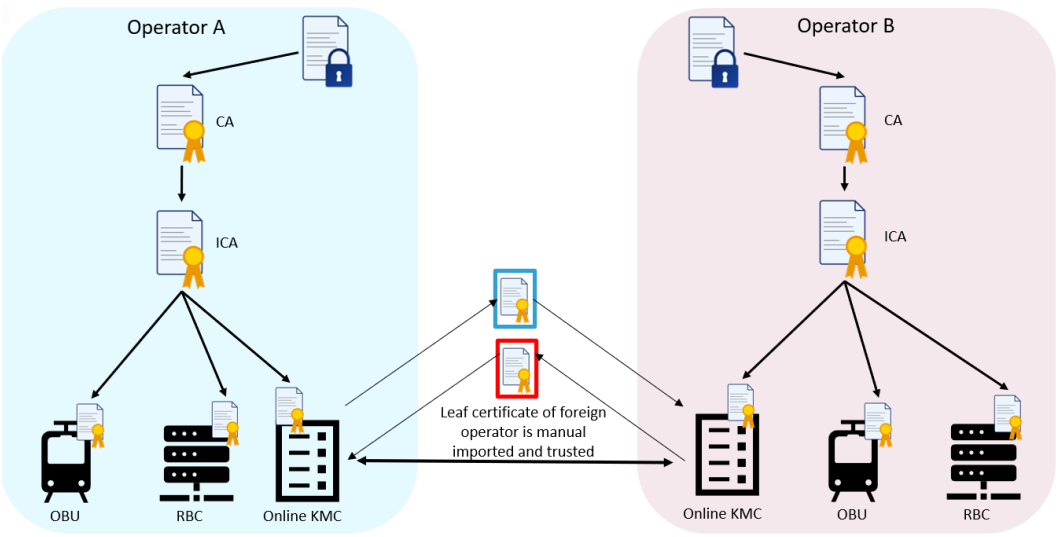

Figure 3: Trusted Peer Leaf Model

2.8.8.2 Trusted Peer Leaf PKI model enables On-line KMC connection without a third entity. **(I)**

2.8.8.3 Trust between the organizations is established by the manual exchange of certificates. **(I)**

2.8.8.4 Trusted Peer Leaf PKI model can only be used for the inter-KMC connection. **(I)**

2.8.8.5 Effort is needed to manually manage the certificates. **(I)**

2.8.9 Trust between two KMCs using Centralised Root PKI

2.8.9.1 In this scenario the Centralised Root PKI is only used for the TLS connection between the On-line KMCs. **(I)**

2.8.9.2 Figure 4 shows the integration of an Centralised Root PKI between the operators. **(I)**

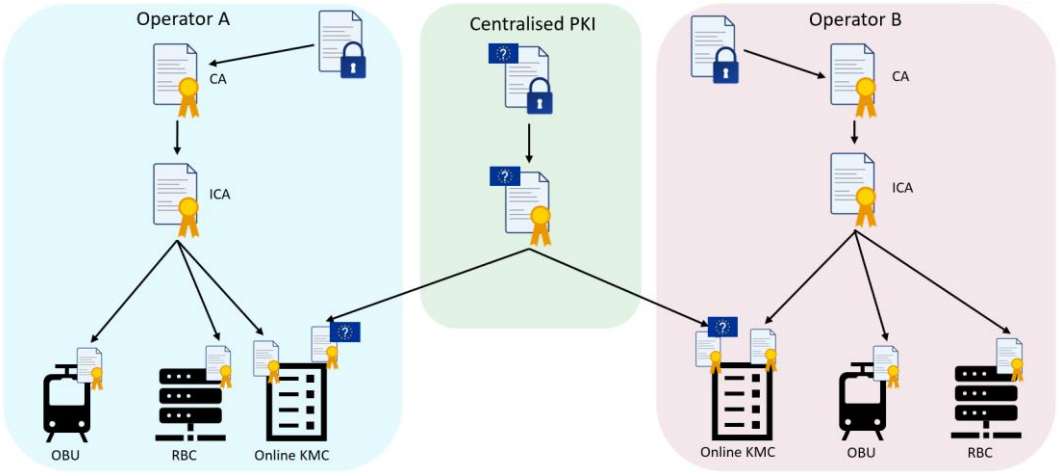

Figure 4: Centralised Root PKI Model

2.8.9.3 The trust between the organizations is established using a Centralised Root PKI. **(I)**

2.8.9.4 In this model a Centralised Root PKI is used to issue the certificates to the Online KMC. **(I)**

2.8.9.5 The certificates from the Centralised Root PKI are only used for the KMC-to-KMC communication. **(I)**

2.8.9.6 Different certificates must be supported for different connections by the Online KMC. **(I)**

2.8.9.7 Less effort, compared to the Trusted Peer Leaf Model is needed to manage the certificates. The implementation might be more complex. **(I)**

2.8.10 Trust between two KMCs using Bridge PKI

2.8.10.1 Figure 5 shows the integration of a Bridge between the operators. **(I)**

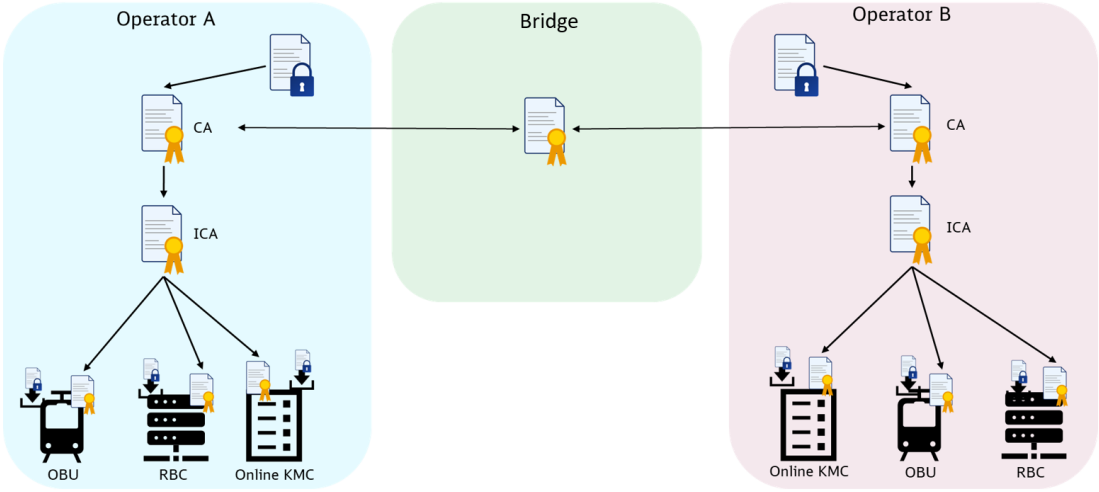

Figure 5: Bridge PKI Model

2.8.10.2 The trust between the organizations is established using a Bridge PKI. **(I)**

2.8.10.3 Certificates are cross signed with an entity, which acts as a bridge between the CAs from different KMC domains to establish trust between them. **(I)**

2.8.10.4 An entity is required to manage the bridge and to integrate new operators. **(I)**

2.8.10.5 Resilience and independence for the operators, due to the usage of own roots. **(I)**

2.8.10.6 Less effort, compared to the Trusted Peer Leaf Model is needed to manage the certificates. The implementation might be more complex. **(I)**

2.8.11 Trust between and within KM Domains using Centralised Root PKI

2.8.11.1 In this scenario the Centralised Root PKI can be used for all internal and external TLS connection for key management. **(I)**

2.8.11.2 Figure 6 shows the integration of a Centralised Root PKI for all ETCS entities. **(I)**

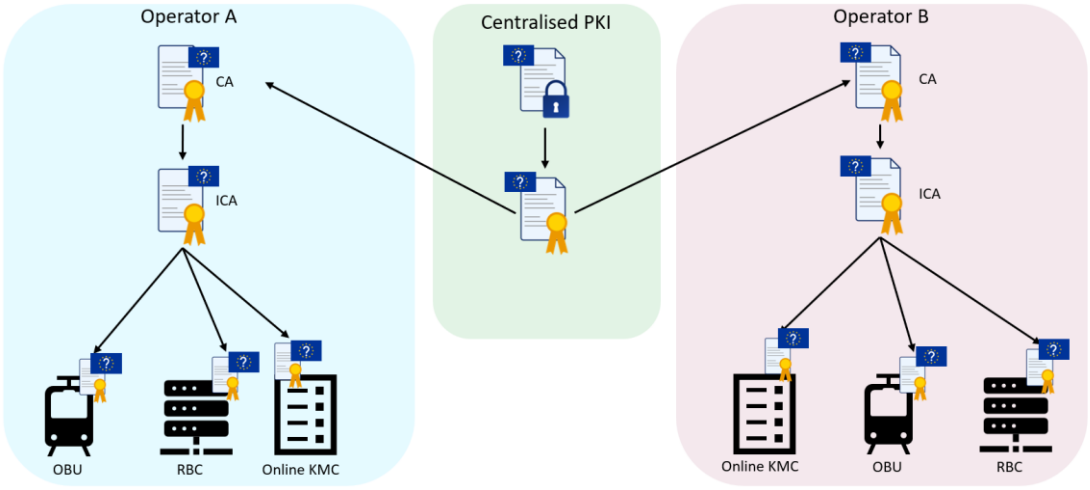

Figure 6: Centralised Root PKI Model

2.8.11.3 The trust between both organizations is established using the same root in a Centralised Root. **(I)**

2.8.11.4 All ETCS entities from both KM domains are using the same root. **(I)**

2.8.12 Migration from Trusted Peer Leaf PKI to Centralised Root PKI

2.8.12.1 The migration from the Trusted Peer Leaf structure to a Centralised Root PKI structure is possible and can be handled according to Figure 7. **(I)**

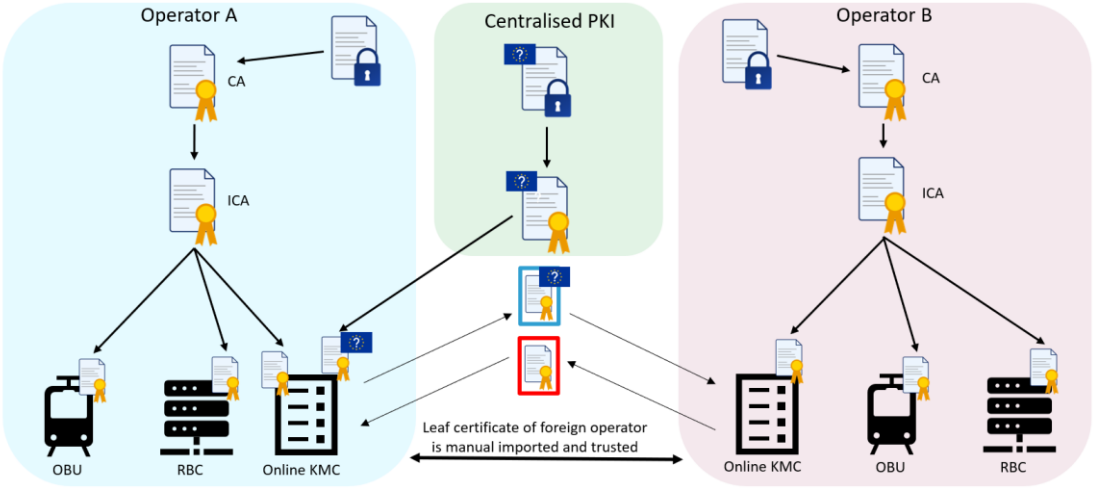

Figure 7: Migration from Trusted Peer Leaf PKI to Centralised Root PKI

2.8.12.2 The Trusted Peer Leaf certificates approach can still be used until both operators have migrated to the Centralised Root PKI, just the root changes for operator A. **(I)**

2.8.12.3 The trust from operator A to operator B is established using the Centralised Root PKI root (blue certificate) and from operator B to operator A using the trusted peer leaf from operator B (red certificate). **(I)**

2.8.13 Migration from Trusted Peer Leaf PKI to Bridge PKI

2.8.13.1 The migration from Trusted Peer Leaf to a Bridge PKI does not need issuing of new certificates and no steps in between are needed. **(I)**

2.8.13.2 The migration is completed as soon as both operators are connected via the Bridge PKI. **(I)**