

A magyarországi kulcsmenedzsment központ megvalósítása és a kulcsmenedzsment szervezési kérdései

Dr. Szabó Géza

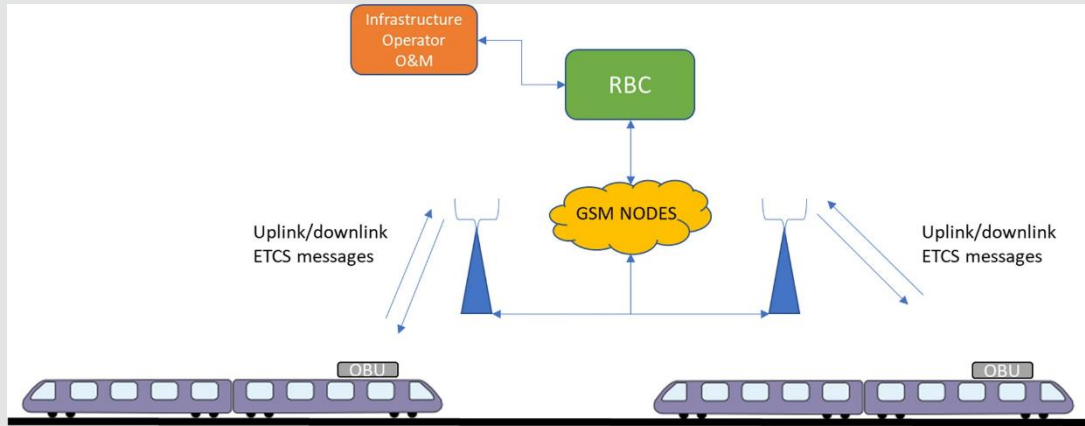


Tartalom

1. A kulcsmenedzsment áttekintése
2. A magyarországi KMC megvalósítás
3. A magyarországi KMC tanúsítása
4. A KMC használata, kulcsmenedzsment nemzeti szinten

1. A kulcsmenedzsment bevezetése

- ETCS L2 és L3: kommunikáció a pályaoldal (RBC) és a jármű (OBU) között GSM-R hálózaton keresztül,
- A GSM-R nyilvános hozzáférésű hálózat.



- MSZ-EN 50159 kommunikáció biztonsága, három kategória; fenyegetések és szükséges védelmek az egyes kategóriákban.

1. A kulcsmenedzsment bevezetése – EN50159

2011. január

MAGYAR SZABVÁNY

MSZ EN 50159

Vasúti alkalmazások. Távközlő-, jelző- és adatfeldolgozó rendszerek. Biztonsági távközlés átviteli rendszerekben

Table 1 – Threats/Defences matrix

Threats	Defences							
	Sequence number	Time stamp	Time-out	Source and destination identifiers	Feed-back message	Identification procedure	Safety code	Cryptographic techniques
Repetition	X	X						
Deletion	X							
Insertion	X			X ^a	X ^b	X ^b		
Re-sequence	X	X						
Corruption							X ^c	X
Delay		X	X					
Masquerade					X ^b	X ^b		X ^c

^a Only applicable for source identifier.
Will only detect insertion from invalid source.
If unique identifiers cannot be determined because of unknown users, a cryptographic technique shall be used, see 7.3.8.

^b Application dependent.

^c See 7.4.3 and Clause C.2.

Category	Cat. 1.	Cat. 2.	Cat. 3.
Repetition	+	++	++
Deletion	+	++	++
Insertion	+	++	++
Re-sequence	+	+	++
Corruption	++	++	++
Delay	+	++	++
Masquerade	-	-	++

1. A kulcsmenedzsment bevezetése - kulcsok

- KMAC és KsMAC

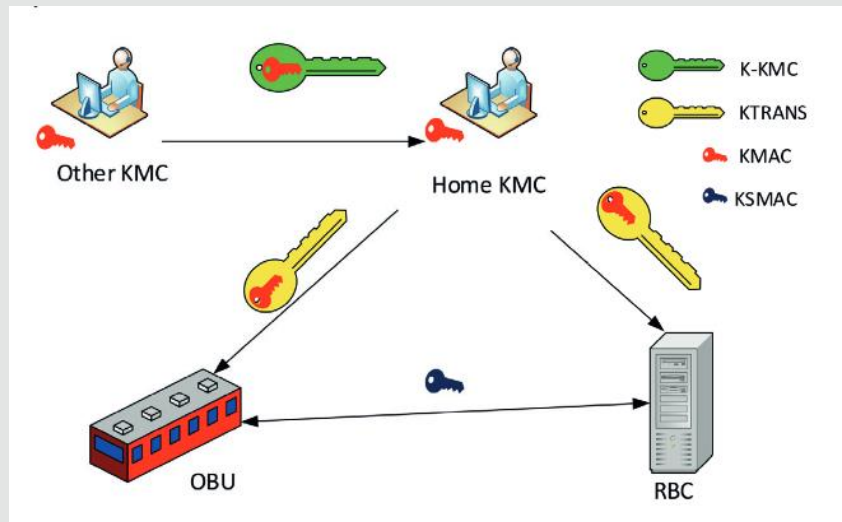
ANSI X3.92 (1981)

ANSI X9.52 (1998)

Triple key, 3x64bit DES

- KTRANS

- K-KMAC



1. A kulcsmenedzsment bevezetése - kulcsok

- KMAC és KsMAC

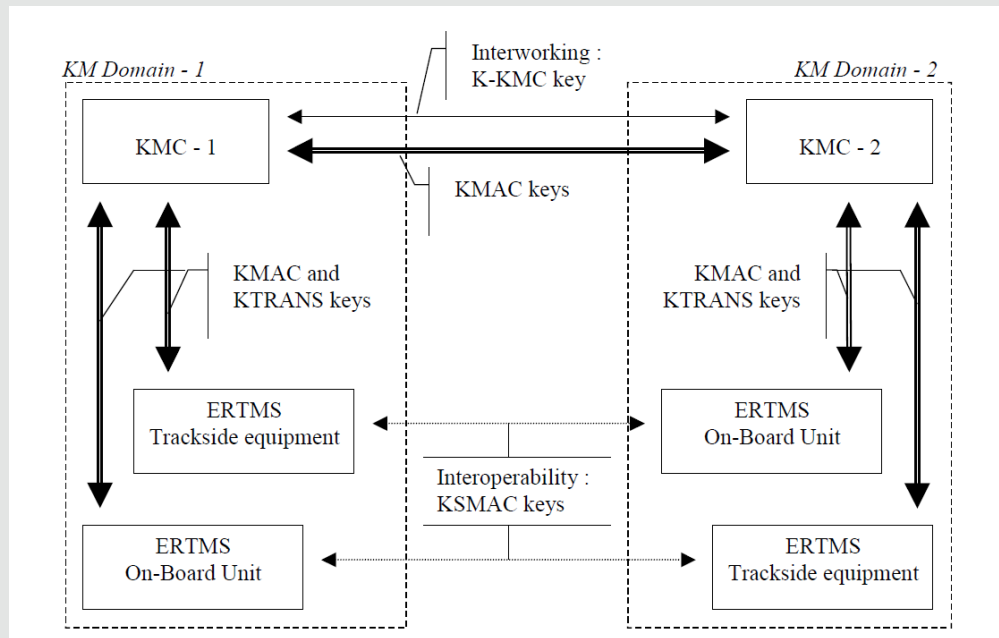
ANSI X3.92 (1981)

ANSI X9.52 (1998)

Triple key, 3x64bit DES

- KTRANS

- K-KMAC



1. A kulcsmenedzsment bevezetése - kulcsbetöltés

- Off-line (SUBSET-038 és SUBSET 114)
- On-line (SUBSET 137)
- Kvázi on-line (magic box)

SUBSET-038 Offline key management FIS
SUBSET-114 KMC-ETCS Entity Off-line KM FIS
SUBSET-137 On-line Key Management FFFIS

1. A kulcsmenedzsment bevezetése – KMC és KMS

- KMC: kulcsok generálása, módosítása, visszavonása, menedzselése, letöltése stb.
- KMS: KMC + kulcsmenedzsment folyamatok szabályozása, folyamatdokumentálás stb.

2. A magyarországi KMC megvalósítás

Előzmények: ideiglenes kulcskezelés

AppEVO Zrt. – BME ITS Nzrt. – Rail Expert Consult (REC)
MÁV Zrt. szakmai együttműködés

2. A magyarországi KMC megvalósítás

Redundáns, hidegtartalékolt hardver a MÁV Zrt. informatikai hálózatba integrálva,

KMC és KDC

Web-es elérési felület

Jogosultsági szintek

Adatbáziskezelés, archívumok

Saját és idegen szervezet kezelése

2. A magyarországi KMC megvalósítás

The screenshot shows the Hrail web application interface. The browser address bar indicates the URL is 10.109.26.1:800. The user is logged in as horvathgabor KMC_7. The sidebar menu includes sections for Transport Key, Authentication Key, K-KMC Key, Distribution, Manage ETCS Entities, Approvals & Open Tasks, KMC/KDC Administration, and Test Key. The main dashboard displays sections for Transport Key, Distribution, Manage ETCS Entities, Approvals & Open Tasks, and Test Key. A modal window titled "Legfrissebb letöltési előzmények" (Latest download logs) is open, showing a list of download records with details such as file name, size, and status.

File Name	Size	Status
020C3521 (1).zip	1 250 bájt	Kész
01684258 (4).zip	640 bájt	Kész
020C3520 (1).zip	1 251 bájt	Kész
01684258 (3).zip	639 bájt	Kész
020C351F (1).zip	1 249 bájt	Kész
01684258 (2).zip	641 bájt	Kész
020C351E (1).zip	1 245 bájt	Kész
01684258 (1).zip	640 bájt	Kész
020C3522.zip		



2. A magyarországi KMC megvalósítás

Home **RAILExpert Consult** Notifications Language Help

Logged In as: horvathgabor KMC_7

Transport Key Authentication Key Request Create Update Delete External Communication Confirm Operation K-KMC Key Distribution Manage ETCS Entities Approvals & Open Tasks KMC/KDC Administration Test Key

Create Authentication Key

Select the ETCS ID's for which Authentication Key is to be created.

Number of entries: 25

Select	ETCS Type	ETCS ID	UIC Number/Entry Name	Key Group	Manufacturer	Organization	Protocol	Home KMC
<input type="checkbox"/>	RBC	6832129	KLSV	RBC kulcsok	Siemens	MÁV TRI	Siemens	KMC MAV
<input checked="" type="checkbox"/>	RBC	6832728	SV	RBC kulcsok	Thales	MÁV TRI	Thales XER	KMC MAV
<input type="checkbox"/>	RBC	6840128	BoBa	RBC kulcsok	Thales	MÁV TRI	Thales XER	KMC MAV
<input type="checkbox"/>	RBC	6852912	MH-AB	RBC kulcsok	Siemens	MÁV TRI	Siemens	KMC MAV
<input type="checkbox"/>	RBC	6854012	SPDL2	RBC kulcsok	Thales	MÁV TRI	Thales BL3	KMC MAV
<input type="checkbox"/>	RBC	6858512	TE-GM	RBC kulcsok	Siemens	MÁV TRI	Siemens	KMC MAV
<input type="checkbox"/>	RBC	6859012	GyLok	RBC kulcsok	Thales	MÁV TRI	Thales BL3	KMC MAV
<input type="checkbox"/>	RBC	6865196	KL	RBC kulcsok	Siemens	MÁV TRI	Siemens	KMC MAV
<input type="checkbox"/>	RBC	6865896	FC	RBC kulcsok	Siemens	MÁV TRI	Siemens	KMC MAV
<input type="checkbox"/>	RBC	6867796	FEMON	RBC kulcsok	Thales	MÁV TRI	Thales XER	KMC MAV
<input type="checkbox"/>	RBC	6853412	ML-SJ	RBC kulcsok	Siemens	MÁV TRI	Siemens	KMC MAV
<input type="checkbox"/>	RBC	6835128	KL-AB	RBC kulcsok	Siemens	MÁV TRI	Siemens	KMC MAV
<input type="checkbox"/>	RBC	6848514	RAHAT	RBC kulcsok	Thales	MÁV TRI	Thales BL3	KMC MAV
<input type="checkbox"/>	OBU	34400	94 55 1415 060-2	OBU Kulcsok	Siemens	MÁV Start	SS114 - Single Key	KMC MAV
<input type="checkbox"/>	OBU	34401	94 55 2415 060-	OBU Kulcsok	Siemens	MÁV Start	SS114 - Single Key	KMC MAV
<input type="checkbox"/>	OBU	34450	94 55 1415 085-9	OBU Kulcsok	Siemens	MÁV Start	SS114 - Single Key	KMC MAV
<input type="checkbox"/>	OBU	34451	94 55 2415 085-7	OBU Kulcsok	Siemens	MÁV Start	SS114 - Single Key	KMC MAV

Filter: ETCS ID, UIC Number/Entry Name, Key Group, Organization, Manufacturer, Home KMC, Show RBC-RBC Neighbourhood, Filter, Show All

2. A magyarországi KMC megvalósítás

The screenshot shows a web browser window with the URL `10.109.26.1:800` and the page title `Nem biztonságos`. The application header includes the logo **RAILExpert Consult** and navigation links for Notifications, Language, Help, and a user profile icon.

The user is logged in as `horvathgabor KMC_7`. A sidebar menu on the left contains the following items:

- Transport Key
- Authentication Key (expanded)
 - Request
 - Create
 - Update
 - Delete
- External Communication
- Confirm Operation
- K-KMC Key
- Distribution
- Manage ETCS Entities
- Approvals & Open Tasks
- KMC/KDC Administration
- Test Key

The main content area displays the **Create Authentication Key** form. It includes the following fields and options:

- Select Validity** (Section Header)
- Select the start and end date for the validity of Authentication Key.*
- Start Date OB-ETCS-ID**: `2024. 02. 22.`
- End Date OB-ETCS-ID**: `éééé. hh. nn.` with **Unlimited Validity:**
- Start Date Peers**: `2024. 02. 22.`
- End Date Peers**: `éééé. hh. nn.` with **Unlimited Validity:**
- Selected OB-ETCS-ID**: `800030 - 94 55 2815 015-0`
- Selected Peers**: `6832728 - SV`

At the bottom of the form, there are three buttons: **Back**, **Next**, and **Cancel**.



2. A magyarországi KMC megvalósítás

✓ Awaiting Approval - KMAC
Check the following information of the Operation and then select the appropriate button to complete the process.

Filter

Select	SNUM	Issuer Kmc Id	Issuer KMC Name	Target KMC	Key Operation Type	OB-ETCS-ID	ETCS Type	UIC Number/Entity Name	Peers	peers_name	Key State	Start Date Peers	End Date Peers	Start Date OB-ETCS-ID	End Date OB-ETCS-ID	Requester
<input checked="" type="checkbox"/>	56	3158072	KMC MAV	KMC MAV	Generate	800030	OBU	94 55 2815 015-0	6832728	SV	Operation Requested	22.02.2024	Unlimited Validity	22.02.2024	Unlimited Validity	horvathgabc
<input checked="" type="checkbox"/>	57	3158072	KMC MAV	KMC MAV	Generate	800031	OBU	94 55 1815 016-0	6832728	SV	Operation Requested	22.02.2024	Unlimited Validity	22.02.2024	Unlimited Validity	horvathgabc
<input checked="" type="checkbox"/>	58	3158072	KMC MAV	KMC MAV	Generate	800032	OBU	94 55 2815 016-8	6832728	SV	Operation Requested	22.02.2024	Unlimited Validity	22.02.2024	Unlimited Validity	horvathgabc
<input checked="" type="checkbox"/>	59	3158072	KMC MAV	KMC MAV	Generate	800033	OBU	94 55 1815 017-8	6832728	SV	Operation Requested	22.02.2024	Unlimited Validity	22.02.2024	Unlimited Validity	horvathgabc

✓ Awaiting Approval - K-KMC
Check the following information of the Operation and then select the appropriate button to complete the process.

Select	Key ID	Issuer	Target KMC	Key Operation Type	Key Type	Key State	Start Date	End Date	KMC ID	KMC Name	Requester	Request Date	Note
No record found													

2. A magyarországi KMC megvalósítás

Browser tabs: Hrail | Hrail

Address bar: Nem biztonságos 10.109.26.1:800


Navigation icons: Home, Back, Forward, Refresh, Search, Star, Print, Download, Share, User

Left sidebar menu:

- K-KMC Key
- Distribution
- Manage ETCS Entities
- Approvals & Open Tasks
- KMC/KDC Administration
- Test Key

Logout

Frontend: 0.6.16
Backend: 0.6.16



Select	SNUM	Issuer Kmc.Id	Issuer KMC Name	Key Operation Type	ETCS ID	ETCS Type	UIC Number/ Entity Name	Key State	Start Date	End Date	Requester	Request Date	Claimed By	Claimed On	Note
<input type="checkbox"/>	65	Generate	93946	OBU	94 55 1415 027-1	Distributed	01.01.2024	Unlimited Validity	horvathgabor	21.02.2024	horvathgabor	22.02.2024			

Open Tasks - KMAC Key Operation

Check the following information of the key Operation and then select the appropriate button to complete the process.

Navigation: Previous | 1 | 2 | Next

Select	SNUM	Issuer Kmc.Id	Issuer KMC Name	Key Operation Type	ETCS ID	ETCS Type	UIC Number/ Entity Name	Key State	Start Date	End Date	Requester	Request Date	Claimed By	Claimed On	Note
<input type="checkbox"/>	56	3158072	KMC MAV	Generate	6832728	RBC	SV	Generated approved	22.02.2024	Unlimited Validity	horvathgabor	22.02.2024			
<input type="checkbox"/>	56	3158072	KMC MAV	Generate	800030	OBU	94 55 2815 015-0	Generated approved KTRANS missing!	22.02.2024	Unlimited Validity	horvathgabor	22.02.2024			
<input type="checkbox"/>	57	3158072	KMC MAV	Generate	6832728	RBC	SV	Generated approved	22.02.2024	Unlimited Validity	horvathgabor	22.02.2024			
<input type="checkbox"/>	57	3158072	KMC MAV	Generate	800031	OBU	94 55 1815 016-0	Generated approved KTRANS missing!	22.02.2024	Unlimited Validity	horvathgabor	22.02.2024			
<input type="checkbox"/>	58	3158072	KMC MAV	Generate	6832728	RBC	SV	Generated approved	22.02.2024	Unlimited Validity	horvathgabor	22.02.2024			

Open Tasks - K-KMC Key Operation

Check the following information of the key Operation and then select the appropriate button to complete the process.

Windows taskbar: 9:53



2. A magyarországi KMC megvalósítás

Logged in as: horvathgabor KMC_7

Transport Key

- Request
- Create
- Update
- Delete
- External Communication
- Confirm Operation

K-KMC Key

Distribution

Manage ETCS Entities

Approvals & Open Tasks

KMC/KDC Administration

Test Key

Logout

Distribute Transport Key

Select the ETCS ID's for which Transport Key Distribute is to be performed.

Number of entries: 25

Select	ETCS ID	Entity Name	Key Status	Start Date	End Date	Distribution Method
<input checked="" type="checkbox"/>	800030	94 55 2815 015-0	Generated approved	2024.01.01		Terminal 1 (KMC)
<input checked="" type="checkbox"/>	800031	94 55 1815 016-0	Generated approved	2024.01.01		Terminal 1 (KMC)
<input checked="" type="checkbox"/>	800032	94 55 2815 016-8	Generated approved	2024.01.01		Terminal 1 (KMC)
<input checked="" type="checkbox"/>	800033	94 55 1815 017-8	Generated approved	2024.01.01		Terminal 1 (KMC)
<input checked="" type="checkbox"/>	800034	94 55 2815 017-6	Generated approved	2024.01.01		Terminal 1 (KMC)

Filter

ETCS ID

Entity Name

Key Status

Choose Here

Distribution Method

Choose Here

Filter

Show All

2. A magyarországi KMC megvalósítás

Home **RAILExpert Consult** Notifications Language Help RAIL

Logged In as: horvathgabor KMC_7

Download Transport Key

Select the ETCS ID's for which Transport Key download is to be performed.

Number of entries: 25

Select	ETCS ID	Entity Name	Organization	Manufacturer	Start Date	End Date	Unlimited Validity
<input type="checkbox"/>	93947	94 55 1415 028-9	MÁV Start	Alstom	2024.01.01		Yes
<input type="checkbox"/>	93948	94 55 1415 029-7	MÁV Start	Alstom	2024.01.01		Yes
<input type="checkbox"/>	93949	94 55 1415 030-5	MÁV Start	Alstom	2024.01.01		Yes
<input type="checkbox"/>	93950	94 55 1415 031-3	MÁV Start	Alstom	2024.01.01		Yes
<input type="checkbox"/>	93951	94 55 1415 032-1	MÁV Start	Alstom	2024.01.01		Yes
<input checked="" type="checkbox"/>	800030	94 55 2815 015-0	MÁV Start	Angelstar	2024.01.01		Yes
<input checked="" type="checkbox"/>	800031	94 55 1815 016-0	MÁV Start	Angelstar	2024.01.01		Yes
<input checked="" type="checkbox"/>	800032	94 55 2815 016-8	MÁV Start	Angelstar	2024.01.01		Yes
<input checked="" type="checkbox"/>	800033	94 55 1815 017-8	MÁV Start	Angelstar	2024.01.01		Yes
<input checked="" type="checkbox"/>	800034	94 55 2815 017-6	MÁV Start	Angelstar	2024.01.01		Yes

Filter

ETCS ID

Entity Name

Manufacturer

Organization

Show All

2. A magyarországi KMC megvalósítás

Logged In as: horvathgabor KMC_7

- Transport Key
 - Request
 - Create
 - Update
 - Delete
 - Import
 - Confirm Operation
- Authentication Key
- K-KMC Key
- Distribution
- Manage ETCS Entities
- Approvals & Open Tasks
- KMC/KDC Administration
- Test Key

Logout

Confirm Operation Transport Key

Select the ETCS ID for which an Operation Confirmation is to be performed.

Number of entries: 25

Select	ETCS ID	Entity Name	Organization	Manufacturer	Start Date	End Date	Key Status	Unlimited Validity
<input type="radio"/>	93947	94 55 1415 028-9	MÁV Start	Alstom	2024.01.01		Distributed	Yes
<input type="radio"/>	93948	94 55 1415 029-7	MÁV Start	Alstom	2024.01.01		Distributed	Yes
<input type="radio"/>	93949	94 55 1415 030-5	MÁV Start	Alstom	2024.01.01		Distributed	Yes
<input type="radio"/>	93950	94 55 1415 031-3	MÁV Start	Alstom	2024.01.01		Distributed	Yes
<input type="radio"/>	93951	94 55 1415 032-1	MÁV Start	Alstom	2024.01.01		Distributed	Yes
<input checked="" type="radio"/>	800030	94 55 2815 015-0	MÁV Start	Angelstar	2024.01.01		Distributed	Yes
<input type="radio"/>	800031	94 55 1815 016-0	MÁV Start	Angelstar	2024.01.01		Distributed	Yes
<input type="radio"/>	800032	94 55 2815 016-8	MÁV Start	Angelstar	2024.01.01		Distributed	Yes
<input type="radio"/>	800033	94 55 1815 017-8	MÁV Start	Angelstar	2024.01.01		Distributed	Yes
<input type="radio"/>	800034	94 55 2815 017-6	MÁV Start	Angelstar	2024.01.01		Distributed	Yes

Filter

- ETCS ID
- Entity Name
- Manufacturer
 - Choose Here
- Organization
 - Choose Here

Filter Show All

2. A magyarországi KMC megvalósítás

The screenshot displays the Hrail web application interface. The browser address bar shows the URL `10.109.26.1:800`. The user is logged in as `horvathgabor.KMC_7`. The sidebar menu on the left contains the following items:

- Transport Key (expanded)
 - Request
 - Create
 - Update
 - Delete
 - Import
 - Confirm Operation
- Authentication Key
- K-KMC Key
- Distribution
- Manage ETCS Entities
- Approvals & Open Tasks
- KMC/KDC Administration
- Test Key
- Logout

The main content area is titled "Confirm Operation Transport Key" and features a "Select" section with the instruction: "Select whether Key Operation is performed or not." Below this is a dropdown menu labeled "Operation performed?" with "Yes" selected. To the right, a text box titled "Selected ETCS Entities" contains the value "800030". At the bottom of the main area, there are three buttons: "Back", "Next", and "Cancel".

2. A magyarországi KMC megvalósítás

Lehetséges továbblépések:

- Dokumentum-menedzsment, KMS külső folyamatok támogatása

3. A magyarországi KMC tanúsítása

KMC, mint alrendszer-rész

(Nem önállóan tanúsítható alrendszer-rész)

(Nem interoperabilitási rendszerelem, IC)

Tanúsítás eredménye: ISV (közbenső hitelesítési tanúsítvány)

Megfelelésértékelési modul: SG

(227 oldal SUBSET követelményellenőrzés és 480 oldal teszt specifikáció és eredmény)

4. A KMC használata, kulcsmenedzsment nemzeti szinten

Felhasználási lehetőségek

- Pályahálózat-működtetők és jelentősebb vállalkozó vasutak saját KMS-vel rendelkeznek
- Központosított kulcskezelés

4. A KMC használata, kulcsmenedzsment nemzeti szinten

Az angol példa:

Nemzeti szabályozás RIS-0743-CCS

Korábban:

GE/RT8403 ERTMS Key Management

GE/GN8603 Guidance on ERTMS Key Management

Uncontrolled When Printed

Document comes into force on 04/03/2017 and supersedes GERT8403 Iss 1 and GEGN8603 Iss 1 on 04/03/2017

Rail Industry Standard

RIS-0743-CCS

Issue: One

Date: March 2017

ERTMS Key Management

Synopsis

This document contains requirements for the management of cryptographic keys on the mainline railway to facilitate secure European Rail Traffic Management System (ERTMS) data radio communication. ERTMS exchanges 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.

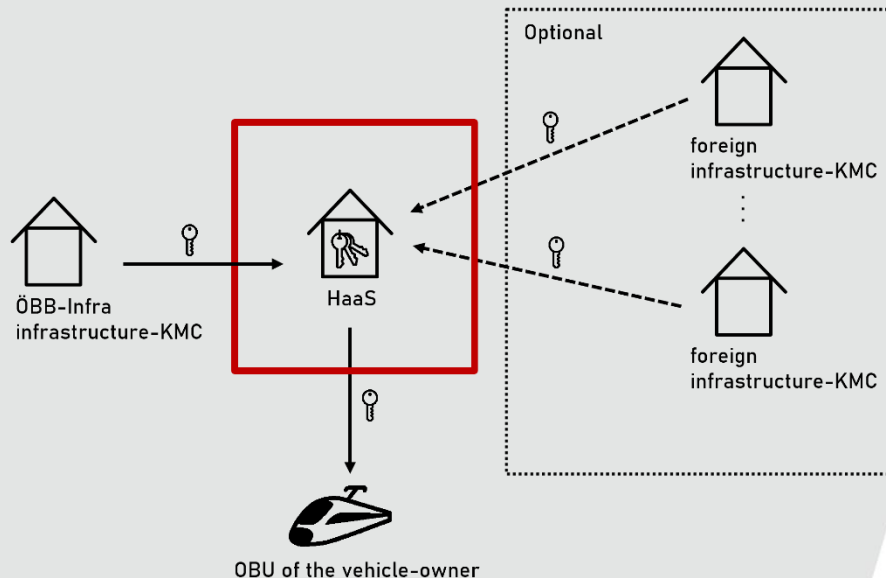


4. A KMC használata, kulcsmenedzsment nemzeti szinten

Az osztrák példa:

ÖBB HaaS szolgáltatás

Entity	NID_C (dec)	NID_KMC (dec)	KMC ETCS-ID (dec)
HaaS	384	50	6291506



Összefoglalás

Sikeres projekt, amely révén a MÁV Zrt. és Magyarország az EU élmezőnyébe sorolható interoperabilitási kulcsmenedzsmentet működtet.

A kialakuló EU gyakorlattal összhangban meg kell fontolni a KMS nemzeti szabályozás kialakítását.



KÖSZÖNJÜK A FIGYELMÜKET!

A magyarországi kulcsmenedzsment központ
megvalósítása és a kulcsmenedzsment szervezési
kérdései

Dr. Szabó Géza

E-mail: szabo.geza@bmeits.hu