A magyarországi kulcsmenedzsment központ megvalósítása és a kulcsmenedzsment szervezési kérdései

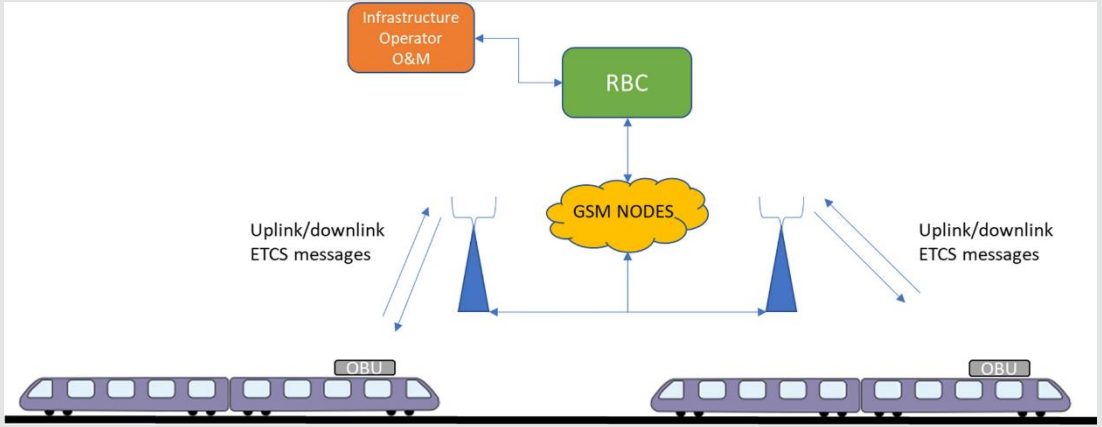
Dr. Szabó Géza

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.

Kép forrása: Radio communication-based method for analysis of train driving in an ERTMS signaling environment; Tomas Rosberg & Birgitta Thorslund; European Transport Research Review volume 14, Article number: 18 (2022)

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.

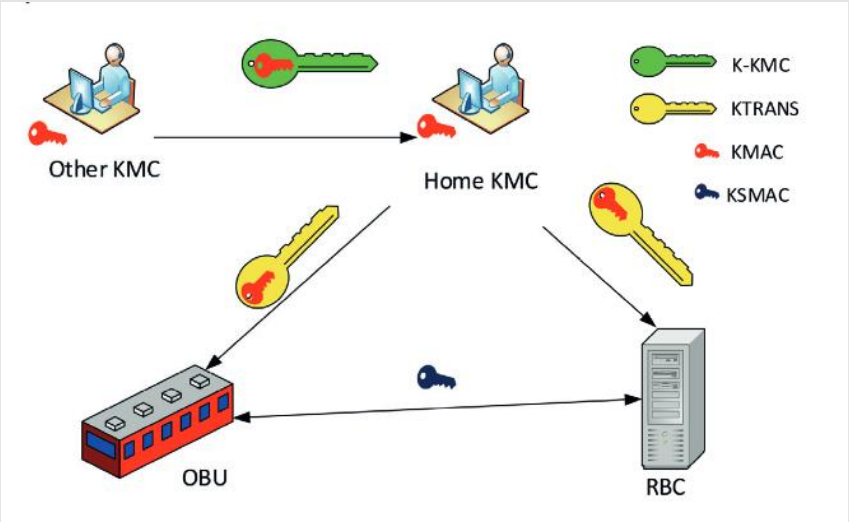
Category	Cat. 1.	Cat. 2.	Cat. 3.
Repetition	+	++	++
Deletion	+	++	++
Insertion	+	++	++
Re-sequence	+	+	++
Corruption	++	++	++
Delay	+	++	++
Masquerade	-	-	++

1. A kulcsmenedzsment bevezetése - kulcsok

- KMAC és KsMAC

ANSI X3.92 (1981)
ANSI X9.52 (1998)
Triple key, 3x64bit DES

- KTRANS
- K-KMAC



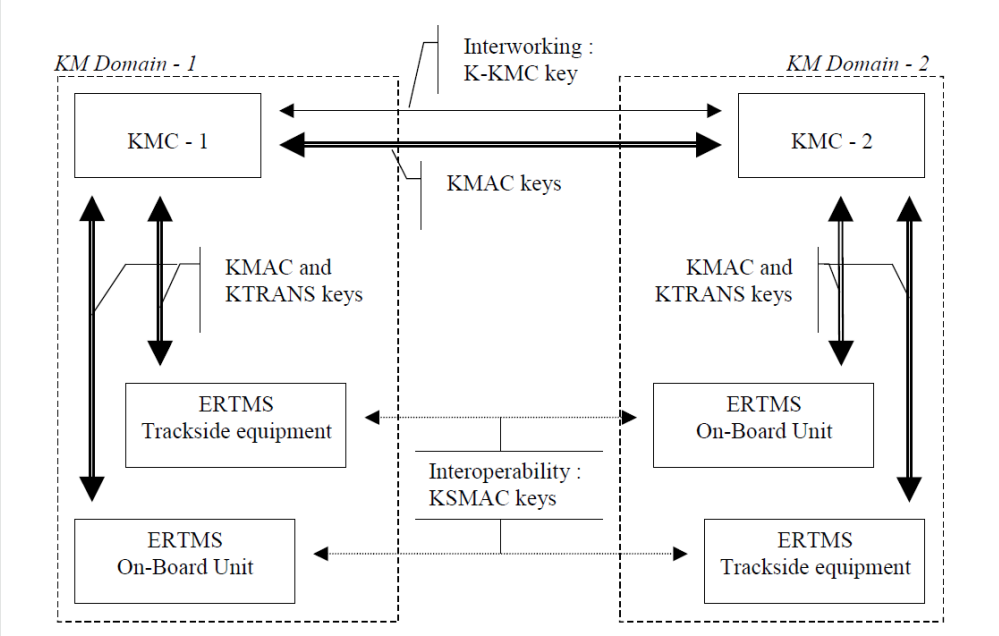
Kép forrása: The Importance of the Cryptographic Key Management System for the Cybersecurity of the ERTMS System; A. KOCHAN, Ł. GRUBA, E. KOPER; Archives of Transport System Telematics, Volume 12, Issue 2, May 2019

1. A kulcsmenedzsment bevezetése - kulcsok

- KMAC és KsMAC

ANSI X3.92 (1981)
ANSI X9.52 (1998)
Triple key, 3x64bit DES

- KTRANS
- K-KMAC



Kép forrása: SUBSET-038

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.

Kép forrása: The Importance of the Cryptographic Key Management System for the Cybersecurity of the ERTMS System; A. KOCHAN, Ł. GRUBA, E. KOPER; Archives of Transport System Telematics, Volume 12, Issue 2, May 2019

2. A magyarországi KMC megvalósítás

Előzmények: ideiglenes kulcskezelés

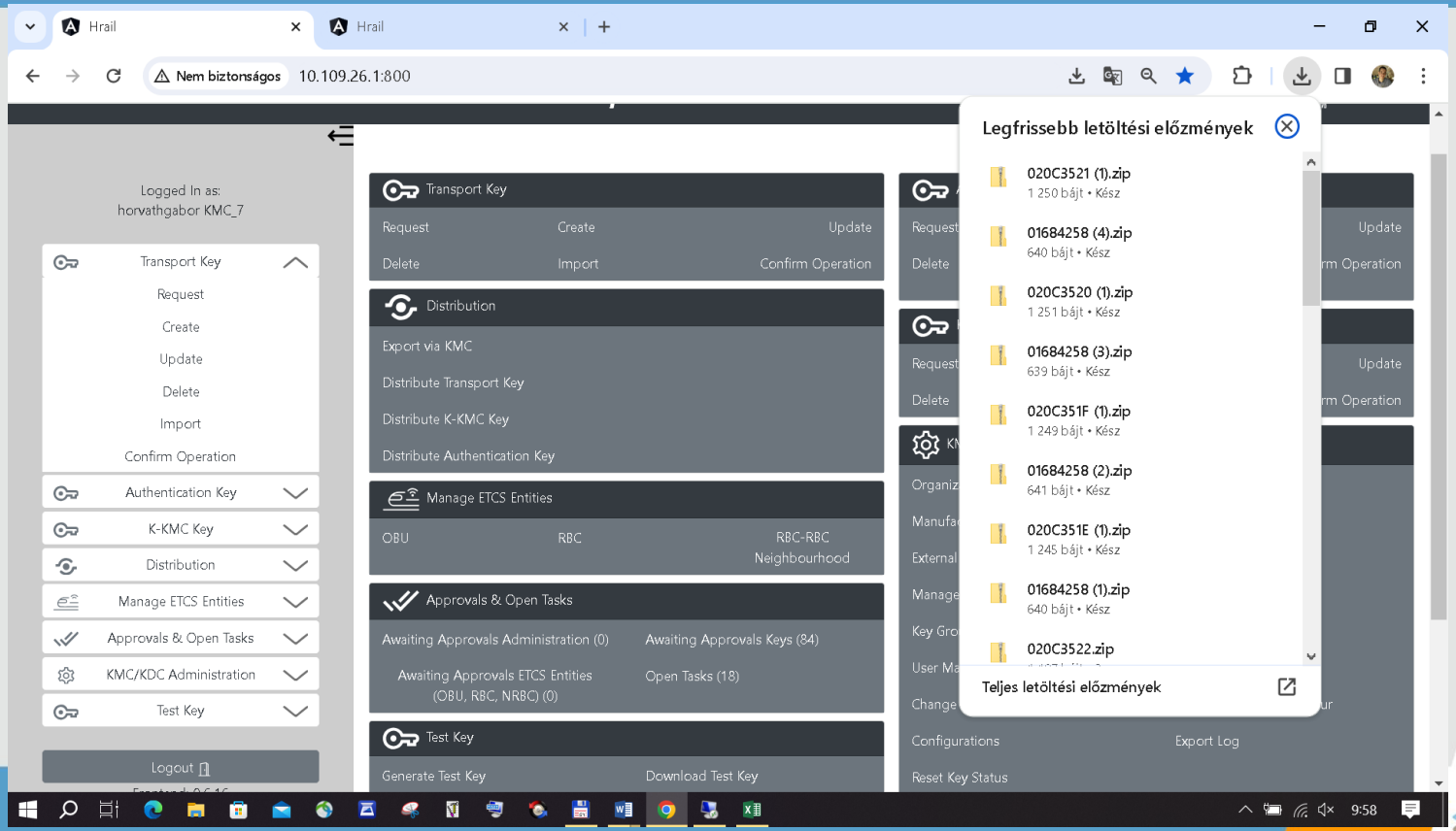
AppEVO Zrt. – BME ITS Nzrt. – Rail Expert Consult (REC)
MÁV Zrt. szakmai együttműködés

2. A magyarországi KMC megvalósítás

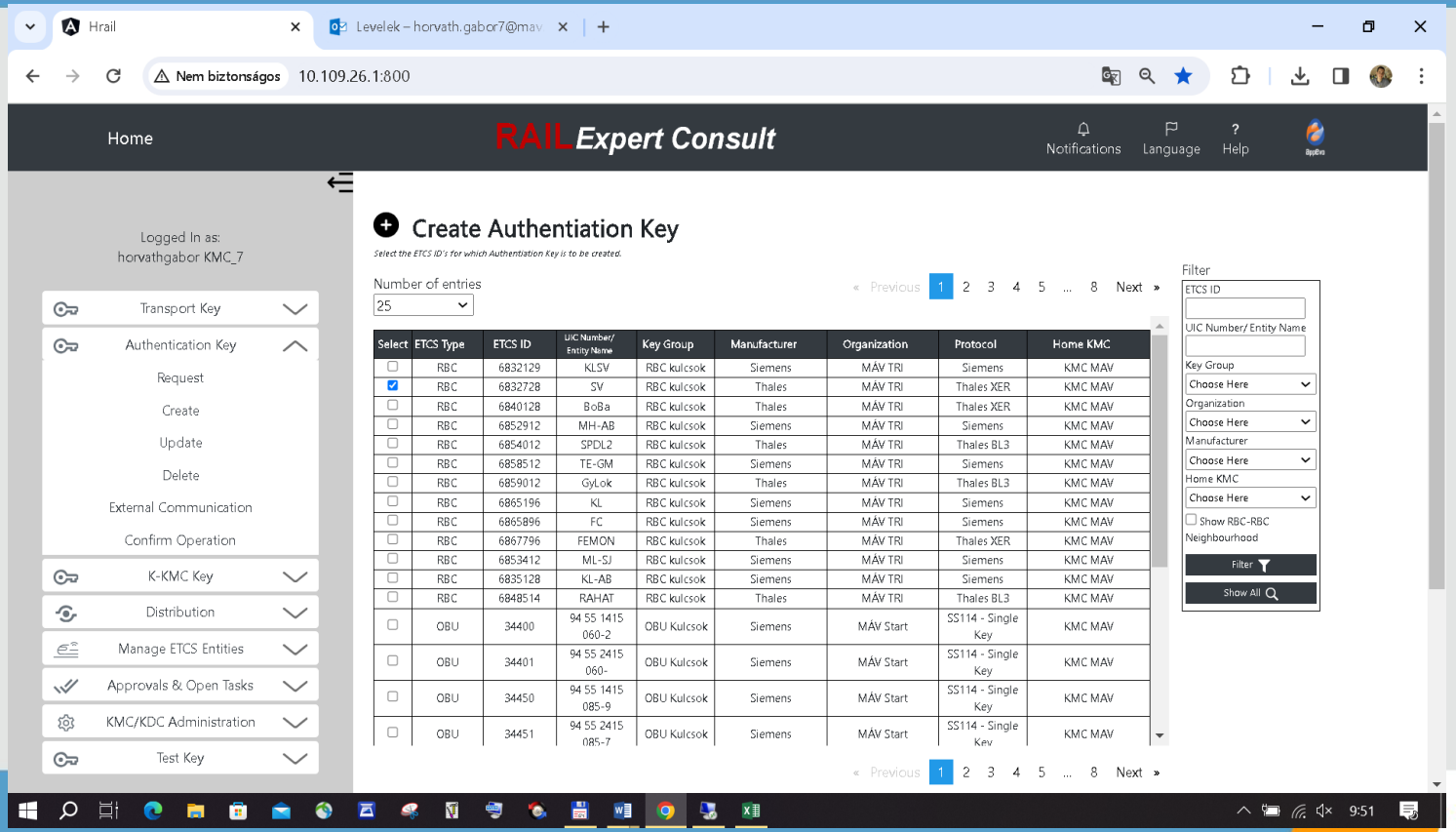
Redundáns, hidegtartalékolt hardver a MÁV Zrt. informatikai hálózatba integrálva,

KMC és KDC
Web-es elérési felület
Jogosultsági szintek
Adatbáziskezelés, archívumok
Saját és idegen szervezet kezelése

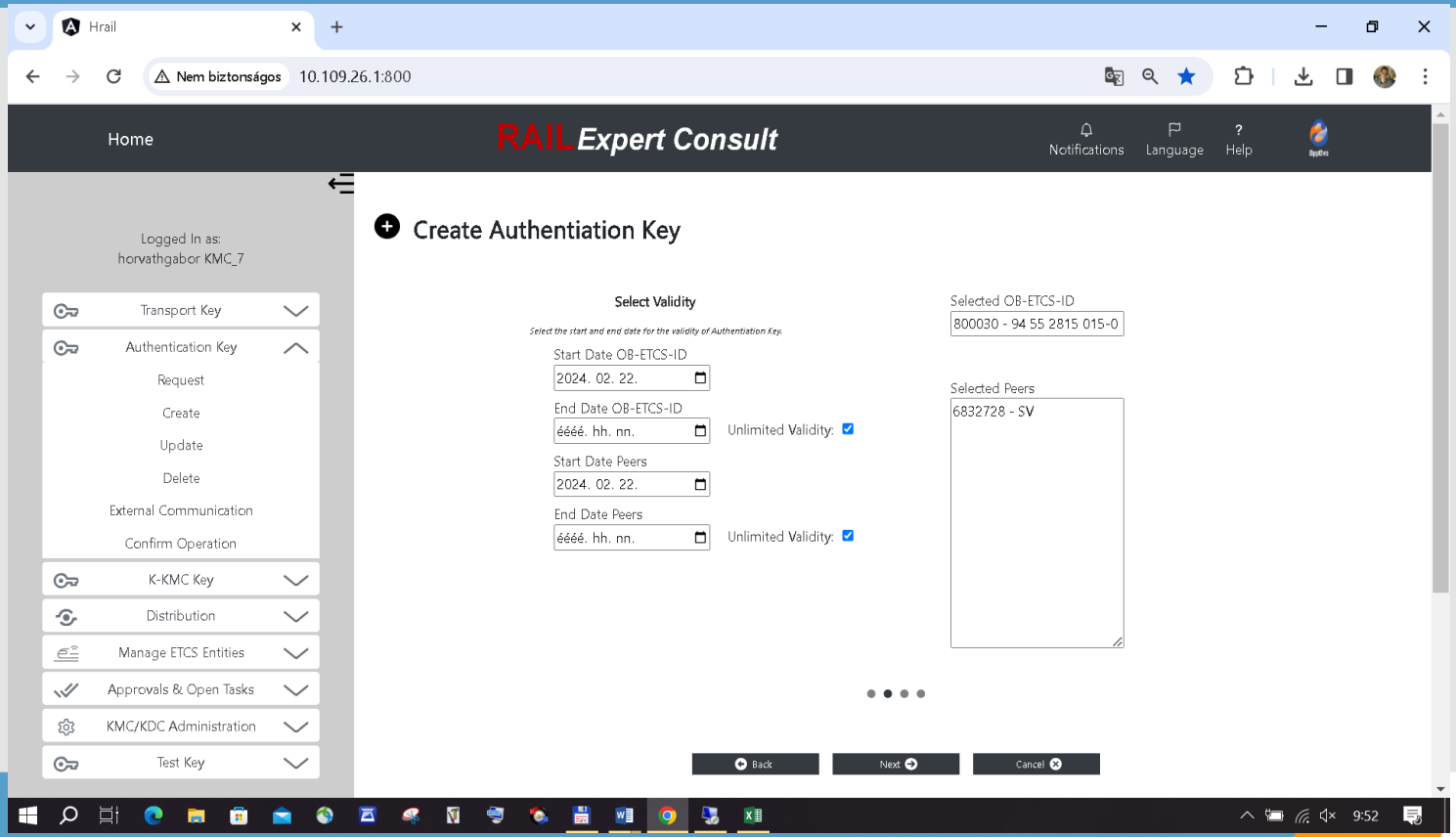
2. A magyarországi KMC megvalósítás



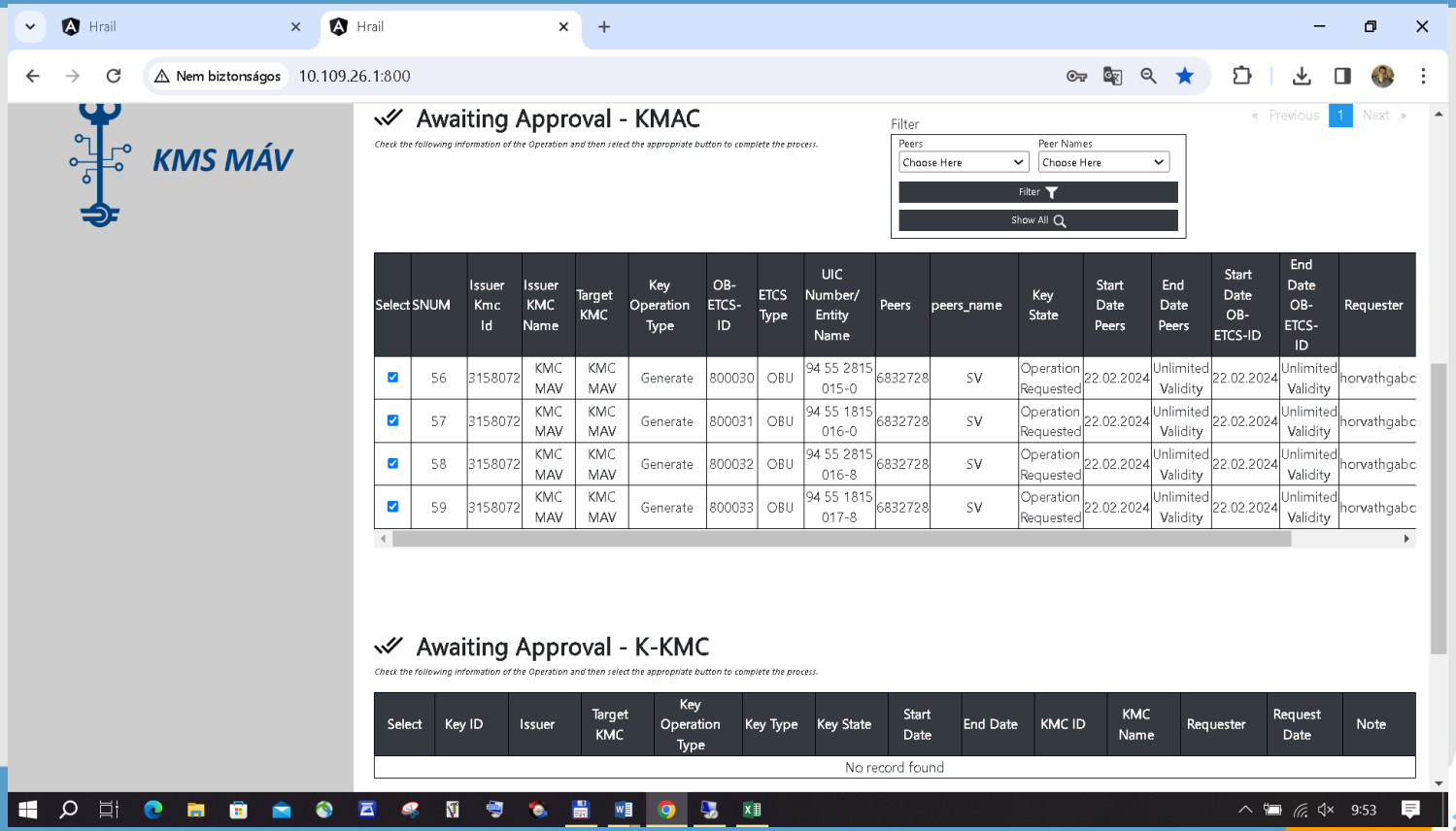
2. A magyarországi KMC megvalósítás



2. A magyarországi KMC megvalósítás



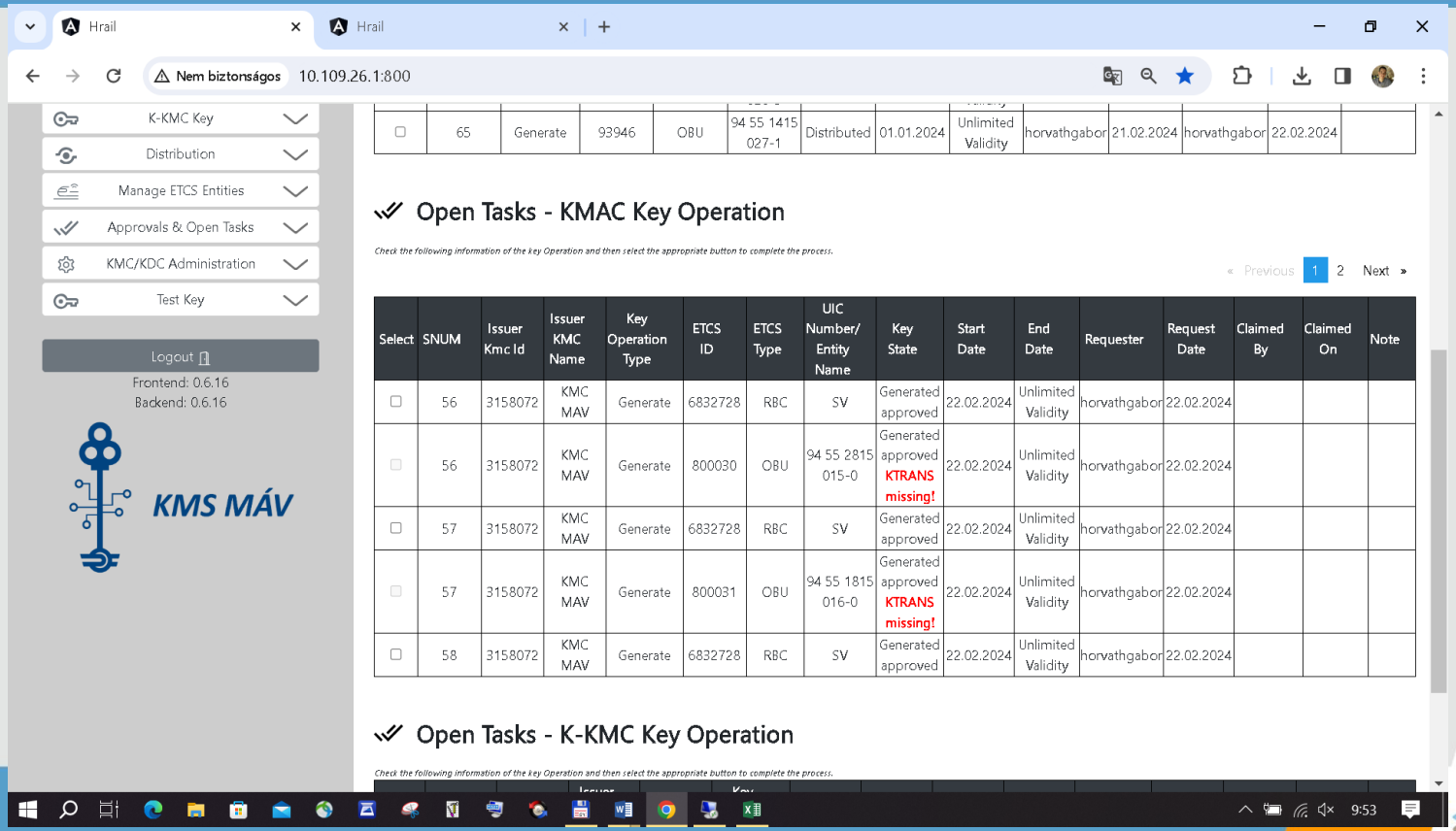
2. A magyarországi KMC megvalósítás



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
☑	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
☑	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
☑	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
☑	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

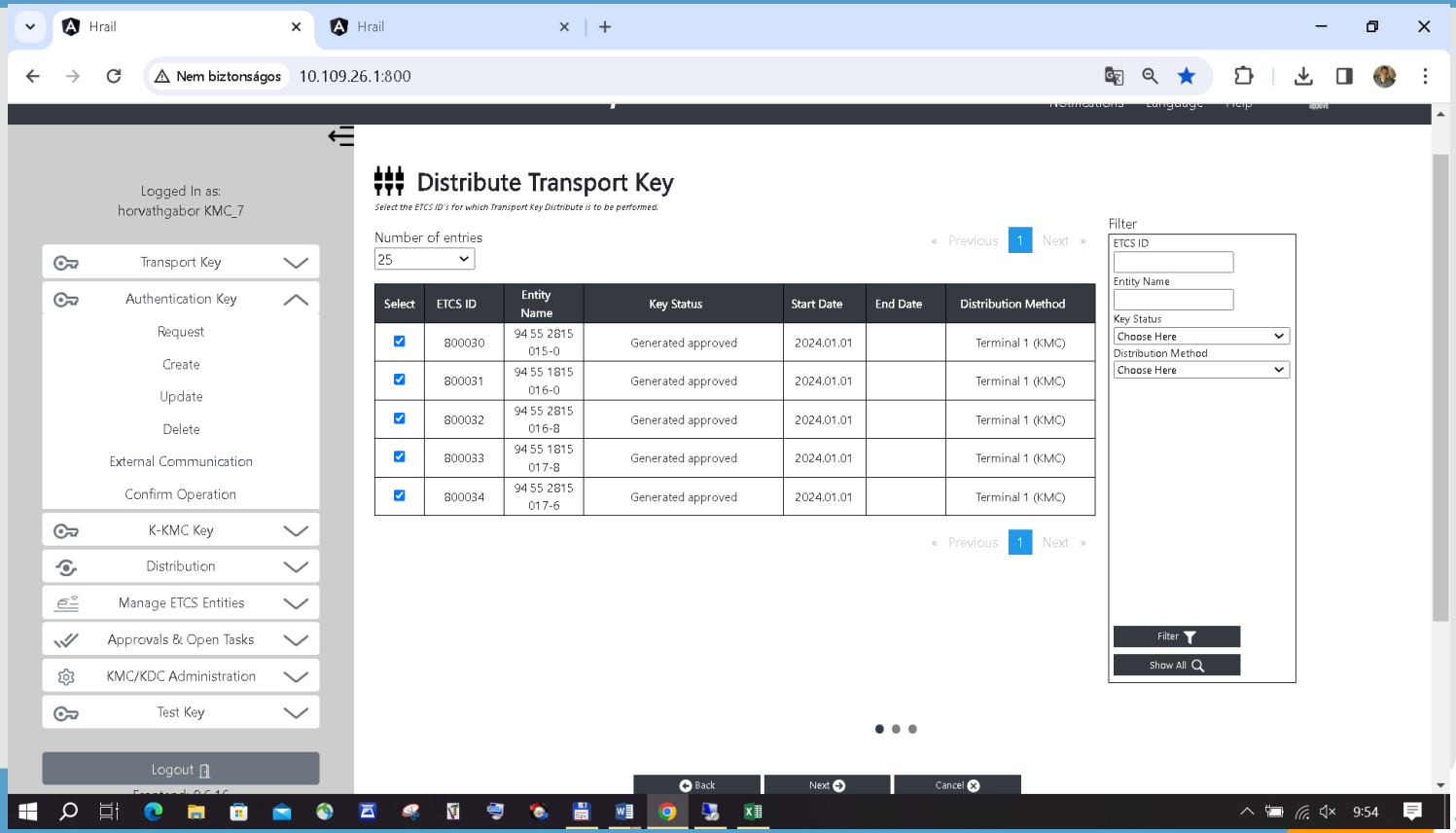
Select	Key ID	Issuer	Target KMC	Key Operation Type	Key Type	Key State	Start Date	End Date	KMC ID	KMC Name	Requester	Request Date	Note
No record found													

2. A magyarországi KMC megvalósítás

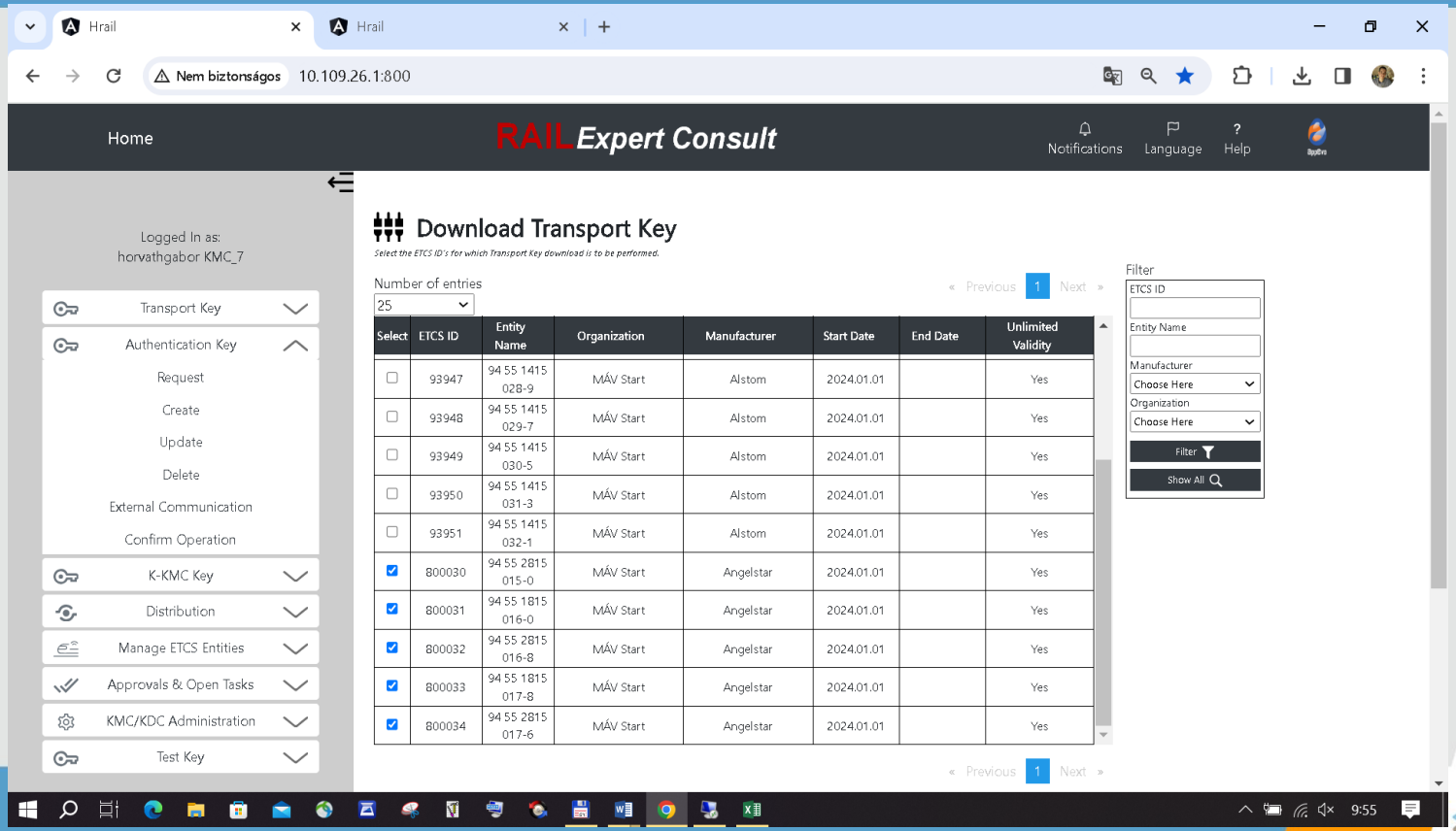


Select	SNUM	Issuer Kmc Id	Issuer KMC Name	Key Operation Type	ETCS ID	ETCS Type	UIC Number/ Entity Name	Key State	Start Date	End Date	Requester	Request Date	Claimed By	Claimed On	Note
☐	65	Generate	93946	OBU	94 55 1415 027-1	Distributed	01.01.2024	Unlimited Validity	horvathgabor	21.02.2024	horvathgabor	22.02.2024			
☐	56	3158072	KMC MAV	Generate	6832728	RBC	SV	Generated approved	22.02.2024	Unlimited Validity	horvathgabor	22.02.2024			
	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			
☐	57	3158072	KMC MAV	Generate	6832728	RBC	SV	Generated approved	22.02.2024	Unlimited Validity	horvathgabor	22.02.2024			
	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			
☐	58	3158072	KMC MAV	Generate	6832728	RBC	SV	Generated approved	22.02.2024	Unlimited Validity	horvathgabor	22.02.2024			

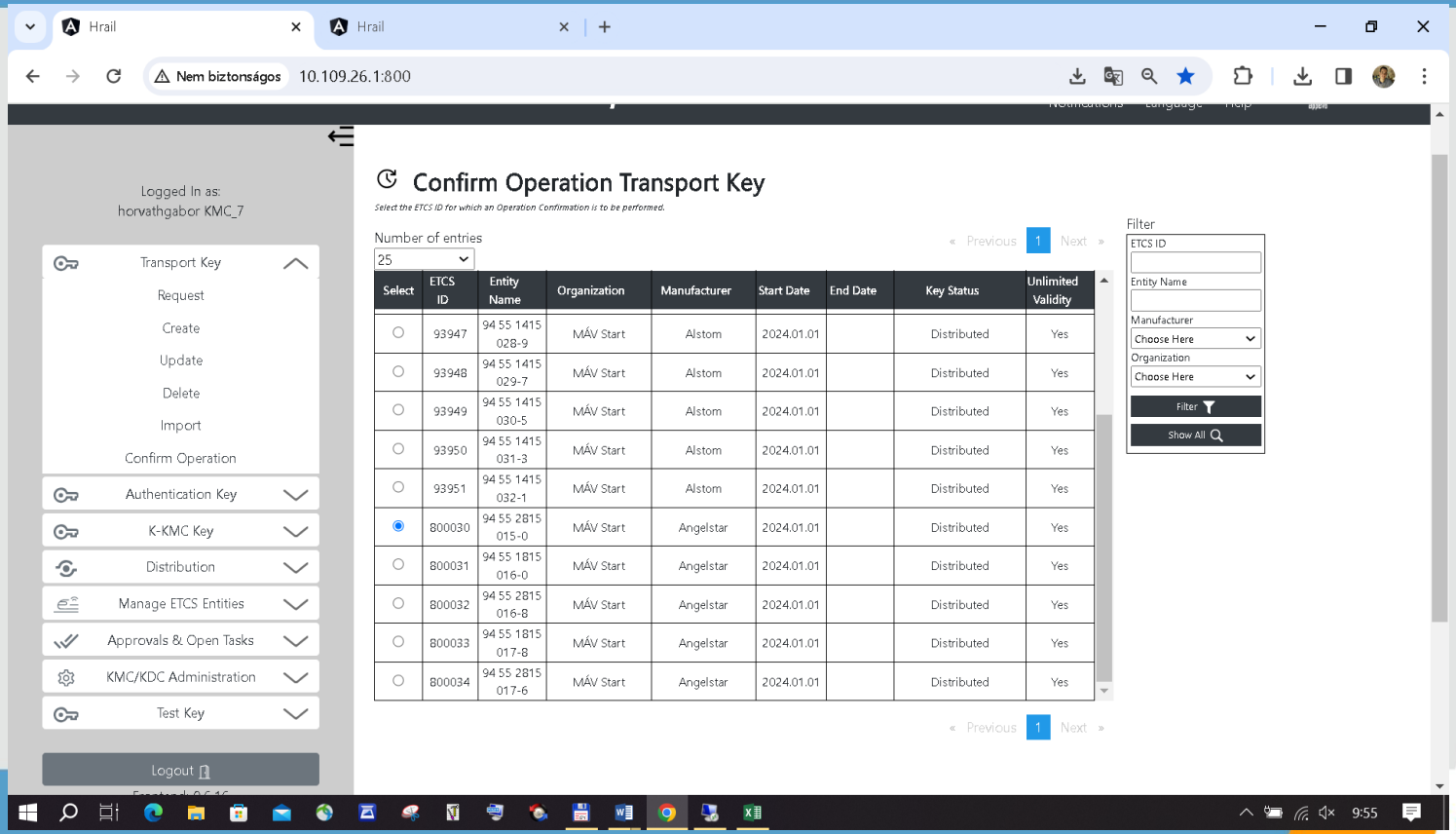
2. A magyarországi KMC megvalósítás



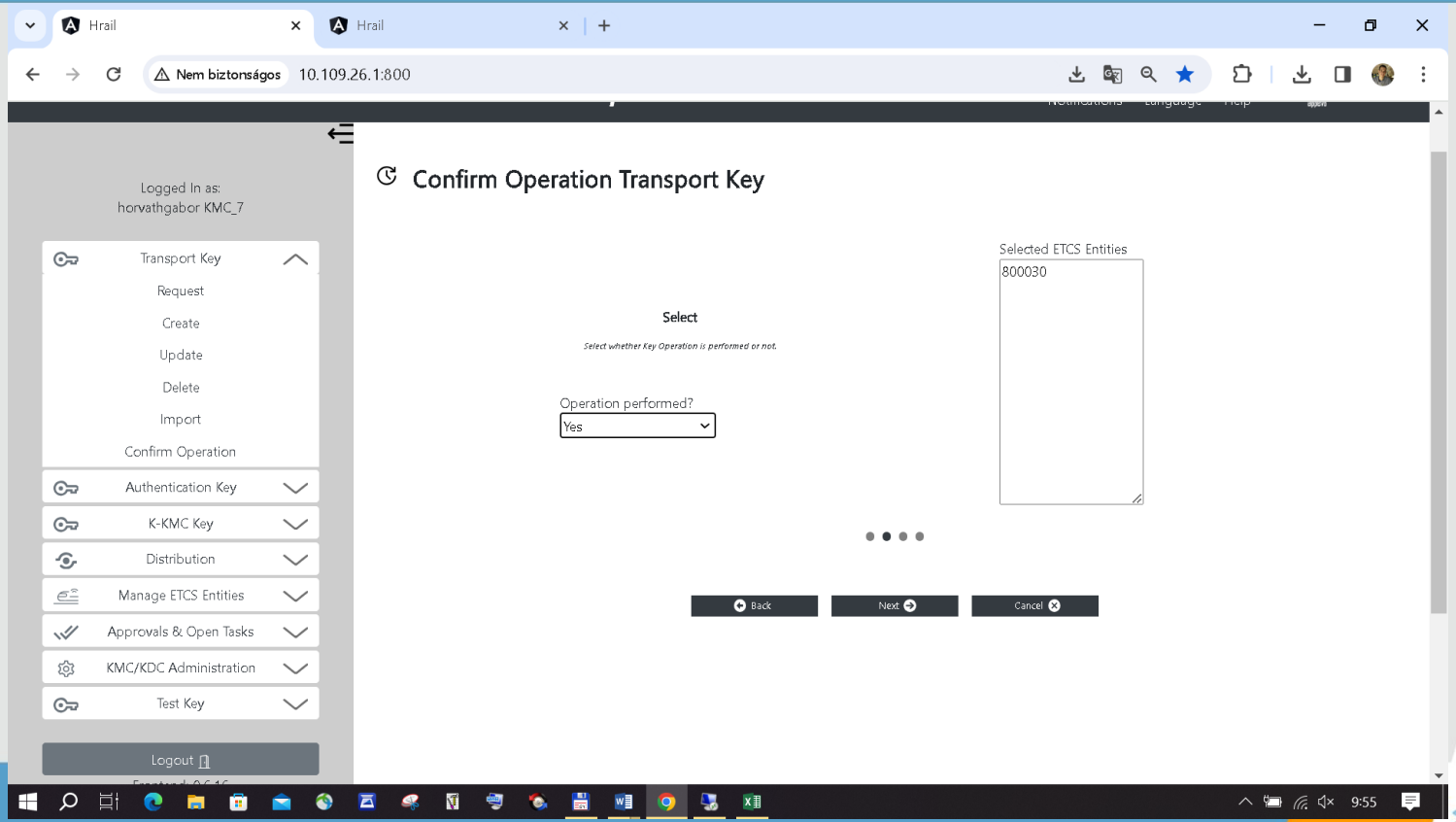
2. A magyarországi KMC megvalósítás



2. A magyarországi KMC megvalósítás



2. A magyarországi KMC megvalósítás



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

Rail Industry Standard
RIS-0743-CCS
Issue: One
Date: March 2017

ERTMS Key Management

Synopsis

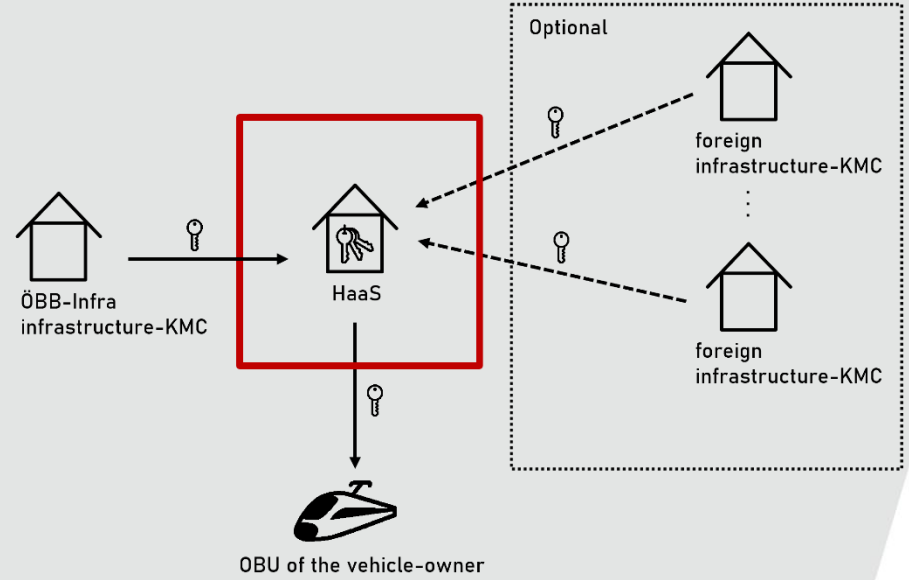
This document contains requirements for the management of cryptographic keys on the mainline railway to facilitate secure European Rail Traffic Management System (ERTMS) data radio communication. ERTMS exchanges information between trackside equipment and trains and vice versa in the form of data messages. 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



Kép forrása:https://infrastruktur.oebb.at/en/partners/rail-network/documents-and-data/etcs-train-control/etcs-key-management/haas

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.

A magyarországi kulcsmenedzsment központ megvalósítása és a kulcsmenedzsment szervezési kérdései

Dr. Szabó Géza
E-mail: szabo.geza@bmeits.hu