ProRail

Welkom

ERTMS Key management

Inrichting en uitdagingen

Jaco Schoonen

3 oktober 2012

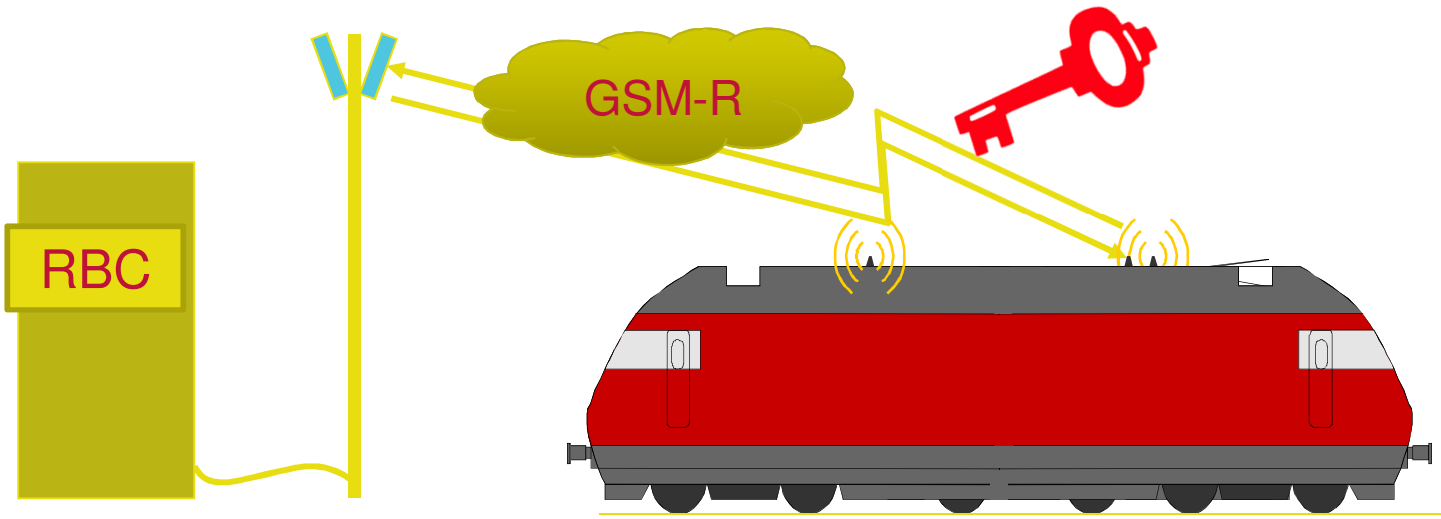
ProRail

Agenda

- Wat is ERTMS Key Management ?
- Inrichting van Key Management in Nederland
- Uitdagingen
- Verbeteringen
- Waarom is Key Management nodig?
- Conclusie

Wat is ERTMS Key Management?

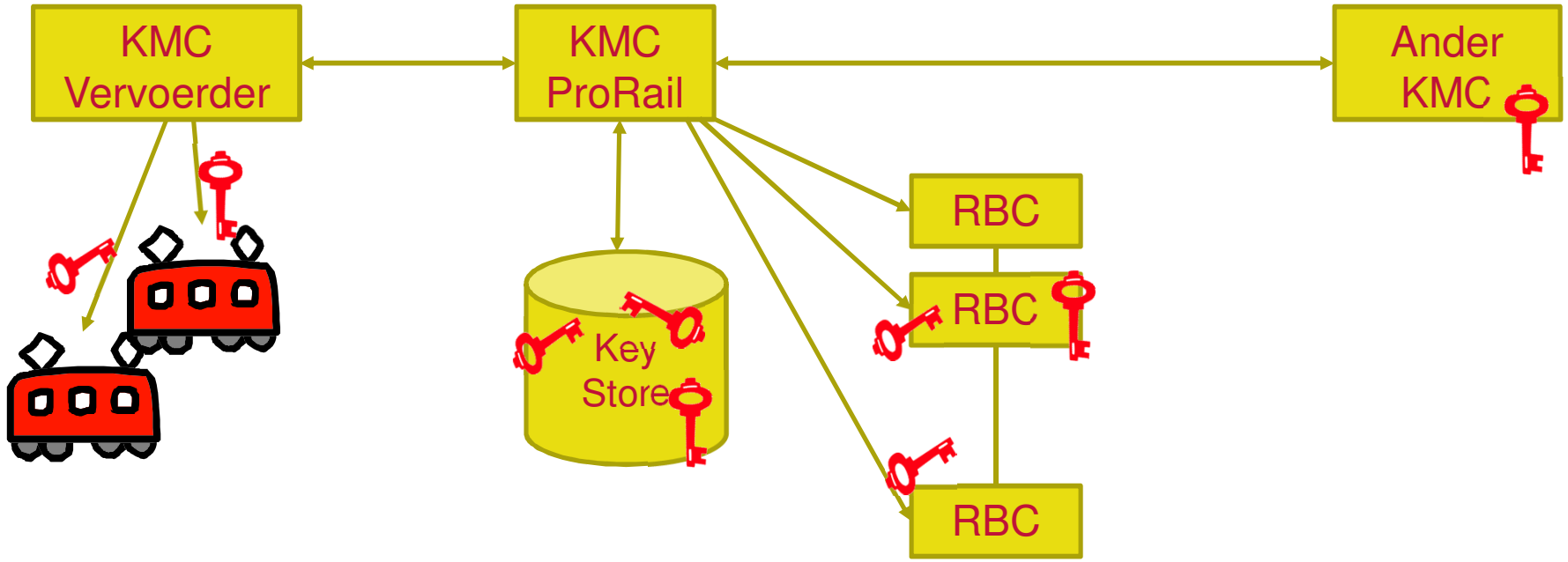
- Bij ERTMS Levels 2 en 3 vind communicatie tussen trein en baan plaats via een GSM-R verbinding. De integriteit en authenticiteit van deze communicatie zijn belangrijk voor het veilig functioneren van ERTMS
- Bij de opbouw en gebruik van de veilige verbinding worden cryptografische sleutels gebruikt



Inrichting - Organisatie

- ProRail heeft één Key Management Center voor alle ERTMS-baanvakken
- ProRail beheert alleen de sleutels in de RBC's, niet in de treinen.
- Sleutelbeheer in de treinen is in Nederland een taak en verantwoordelijkheid van de vervoerder.
  Optioneel door leasemaatschappij ipv vervoerder.
- Infrabeheerder genereert doorgaans de sleutels.
- Sleutels worden gebruikt als technisch hulpmiddel, niet om toegang tot baanvakken te beperken.

Uitwisseling tussen onderdelen



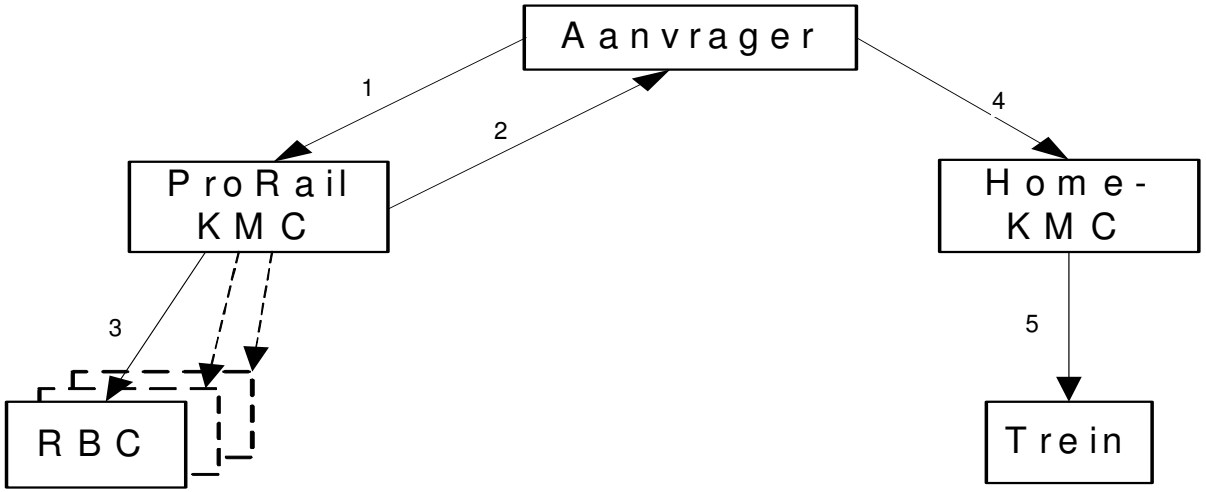
KMC Key store

- KMC beheert een matrix met de relaties tussen trein, baan en sleutels:

Trein	RBC 1	RBC 2	RBC 3
1	Sleutel 1	Sleutel 2	
2	Sleutel 3		
3			Sleutel 4
4	Sleutel 100	Sleutel 100	Sleutel 100

- RBC heeft een tabel met Treinnummers en sleutels
- Trein heeft een tabel met RBC-nummers en sleutels
- Sleutels zijn symmetrisch, d.w.z. dezelfde sleutel in RBC en trein

Organisatie - Aanvraagprocedure



1) aanvraag van nieuwe sleutel
2) Aanvrager ontvangt (gecodeerde) sleutel
3) ProRail implementeert sleutel aan de baanzijde
4) Aanvrager stuurt sleutel naar Home-KMC van de trein
5) Home-KMC decodeert sleutel en implementeert deze in de trein

Inrichting - Techniek

- Offline implementatie, geen rechtstreekse koppeling tussen KMC en apparatuur.
- Export-modules voor verschillende systemen, ERTMS standaard beschrijft alleen uitwisseling tussen KMC's.
- Uitwisseling gaat versleuteld met transport-sleutels
- Functionele mailbox kmc@prorail.nl
- Eenvoudige low-tech oplossing, maar voldoet prima

Uitdagingen

Waar gaat tijd in zitten?

- Planning en dynamiek van offline systeem
- Vervoerders inlichten over het te volgen proces en de benodigde informatie
- Vaststellen van overeenkomsten met partijen omtrent geheimhouding
- Juridische kant: Hoe omgaan met verlies/openbaar worden van sleutels ?
- Europees vastgelegde specificatie beschrijft slechts interoperabiliteit en geen compleet systeem. Geen eenduidig taalgebruik/definities.
- Geen standaard-KMC-tool, veel verschillende implementaties
- Omgaan met key updates (logistiek om sleutel tegelijk in trein en RBC te plaatsen)

Uitdagingen - Vervoerders

- Voor een vervoerder is key management slechts één van de vele dingen die geregeld moeten worden voor toegang tot het spoor.
- Spoorsector is onbekend met het onderwerp digitale sleutels en security
- Vervoerders hebben vaak haast en worden soms verrast door het ontbreken van sleutels
- Onduidelijkheid over de partij die sleutels moet aanvragen (vervoerder, eigenaar, onderhoudspartij, etc)

ProRail

Verbeteringen

- Aanscherpen Europese specificaties om interpretatieverschillen te voorkomen
- Verbeteren van eisen aan systemen voor dynamische updates
- Meerdere sleutels per RBC-trein relatie om update proces te vereenvoudigen
- Koppelingen tussen apparaten en KMC middels standaard interface
- Online-updates middels nog te bepalen standaard
- Lopend onderzoek naar daadwerkelijke risico's

Waarom Key Management ?

- Huidige gebruik van sleutels ligt vast in Europese wetgeving.
- Er is geen duidelijke risico-analyse waaruit blijkt welke risico's er gemitigeerd worden en hoe groot de kans daarop is.
- Safety layer beschermt tegen spontane verstoringen (EMC, storing etc)
- In de veiligheidsonderbouwing van ERTMS zijn de gevaren van bewuste aanvallen (hackers) op het communicatiekanaal wel benoemd, maar niet gekwantificeerd. De veiligheid wordt adequaat geacht, mits de betrokken partijen kunnen aantonen dat er voldoende maatregelen zijn om de sleutels geheim te houden.
- Er is geen relatie aangebracht met andere risico's voor het spoorsysteem. Er zijn veel eenvoudigere manieren om het spoorsysteem te beïnvloeden.

Waarom Key Management ?

- Het risico dat gemitigeerd wordt is bij Level 2 dat een trein een onterechte opdracht krijgt van een andere (namaak-)RBC dan de echte.
- Bij Level 3 bestaat het risico dat er door onduidelijkheid over de exacte positie van de trein een verkeerde opdracht gestuurd wordt.
- Sleutels zijn slechts één van de vele vangnetten die er in het spoorsysteem zitten (GSM-R encryptie, call-matrix, machinist, etc.)

Veiligheid: Safety vs. security

- Safety: Alles wat nodig is voor veilig treinverkeer
- Security: IT-maatregelen om data en communicatie te beschermen
- Bij Key Management gaat het om de security-maatregelen die safety-gerelateerde data beschermen.
- Veel uiteenlopende implementaties en processen binnen Europa, daarom moeilijk te vergelijken, kwantificeren of certificeren.
- Meningen over nut & noodzaak verschillen binnen Europa (van te primitief tot zwaar overdreven).
- Onderzoek naar security-aspecten van key management loopt momenteel binnen ERTMS Users Group.

Conclusie

- Key Management is noodzakelijk en ingericht
- Nog geen uitgekristalliseerd onderdeel van ERTMS met veel verschillen en discussies binnen Europa.
- Niet alleen techniek, maar ook veel organisatie.

ProRail

Vragen