

Ontwikkeling en Beheer

Key Management Center

Scope beschrijving t.b.v. selectiefase

Van	ProRail Procurement
Kenmerk	TN428394
Versie	1.0
Datum	5 december 2023
Bestand	Bijlage 9 - KMC Scope beschrijving tbv selectiefase
Onderwerp	Ontwikkeling en beheer KMC
Status	Definitief

Inhoud

1	Algemene Informatie	3
1.1	Doel van dit document	3
1.2	Algemeen	3
1.3	Doelstelling	3
1.4	Aanleiding	4
2	Scopebeschrijving	6
2.1	Uitgangspunten	6
2.2	Projectteam	6

1 Algemene Informatie

1.1 Doel van dit document

Voorliggend document is het beschrijvend document t.b.v. de aanbesteding Ontwikkeling en Beheer van een Key Management Center (KMC).

1.2 Algemeen

ProRail is verantwoordelijk voor het volledige spoorwegennet van Nederland: aanleg, onderhoud, beheer en veiligheid, en verdeelt als onafhankelijke partij de ruimte op het spoor onder de verschillende vervoerders, regelt alle treinverkeer, bouwt en beheert stations en legt nieuwe sporen aan. ProRail heeft de wettelijke verplichting om Europese interoperabiliteit te realiseren op het spoorwegennetwerk en rolt daarom het beveiligingssysteem ERTMS uit.

De ERTMS-infrastructuur wordt vrijgegeven voor het berijden door treinen, door middel van autorisatieberichten die door een daarvoor geschikte onboard unit (OBU) in het tractievoertuig ontvangen worden van een Radio Block Centre (RBC). Daar treinen draadloos communiceren met het RBC, is er binnen ERTMS voorgeschreven hoe deze communicatie beveiligd plaatsvindt. Om dit mogelijk te maken zullen sleutels (door vervoerders) aangevraagd, gemaakt, (online of offline) gedistribueerd en onderhouden moeten worden middels het Key Management Centre.

Het Key Management Centre communiceert met andere Key Management Centres om sleutels uit te wisselen (conform ERA Technical Specification for Interoperability). Het ProRail-Key Management Centre is verantwoordelijk voor het genereren van sleutels en de distributie naar de Nederlandse RBC's (zodat deze kunnen communiceren met de treinen) en naar de Key Management Centres van de vervoerders. Het Key Management Centre van de vervoerders is verantwoordelijk voor de distributie naar de treinen. Dit laatste buiten de scope van deze uitvraag.

Deze uitvraag behelst het ontwikkelen van een Key Management Centre voor ProRail die alle benodigde functies uit de doelstelling zal bevatten. Naast de ontwikkeling van de applicatie wordt ook een dienstverlening uitgevraagd voor het beheer van applicatie in samenwerking met ProRail.

1.3 Doelstelling

Met Ontwikkeling en Beheer KMC wil ProRail de volgende doelstellingen bereiken:

- Het realiseren van een applicatie binnen de ProRail omgeving voor het afhandelen van een aanvraag tot het verkrijgen, goedkeuren, genereren, opslaan, distribueren (RBCs en andere KMCs), aanstaande verloop van geldigheid signaleren, vernieuwen en na verloop verwijderen van een sleutel.
- Voldoen aan de ERTMS TSI CCS Baseline 4 (online en offline) voor de distributie van een sleutel.
- Assistentie krijgen bij de migratie van bestaande sleutels uit het huidige offline ProRail Key Management Centre dat 'end of life' is.
- Langjarig beheer en ondersteuning van de applicatie.
- Leveren van consultancy voor upgrades en wijzigingen op verzoek van ProRail.
- Implementeren van upgrades en wijzigingen op verzoek van ProRail.

1.4 Aanleiding

Het Programma ERTMS is ingericht voor de uitrol van ERTMS op basis van de ERTMS-programmabeslissing die in 2019 is genomen met de instemming van de Tweede Kamer. ERTMS wordt initieel uitgerold op een aantal baanvakken in de brede randstad en de Noordelijke lijnen. Daarnaast is het beleid van ProRail om verouderde treinbeveiligingsinstallaties landelijk te gaan vervangen door nieuwe ERTMS installaties.

Geldigheid van sleutels

Ambitie van ProRail is met sleutels te werken die een beperkte levensduur hebben: ze zullen ververst moeten worden voor hun geldigheid verloopt als de trein tenminste nog zal moeten kunnen blijven rijden in het werkgebied van de betreffende RBC's. Er kunnen ook andere redenen zijn (veiligheid) om sleutels te vervangen of juist te laten vervallen. Valide sleutels zijn randvoorwaardelijk om op een ERTMS-baanvak een rit te kunnen uitvoeren. Gezien de omvang en de toename van het aantal sleutels en sleutelverversingen van het rondrijdende materieel is online key management noodzakelijk om dat te kunnen managen.

Verantwoordelijkheid

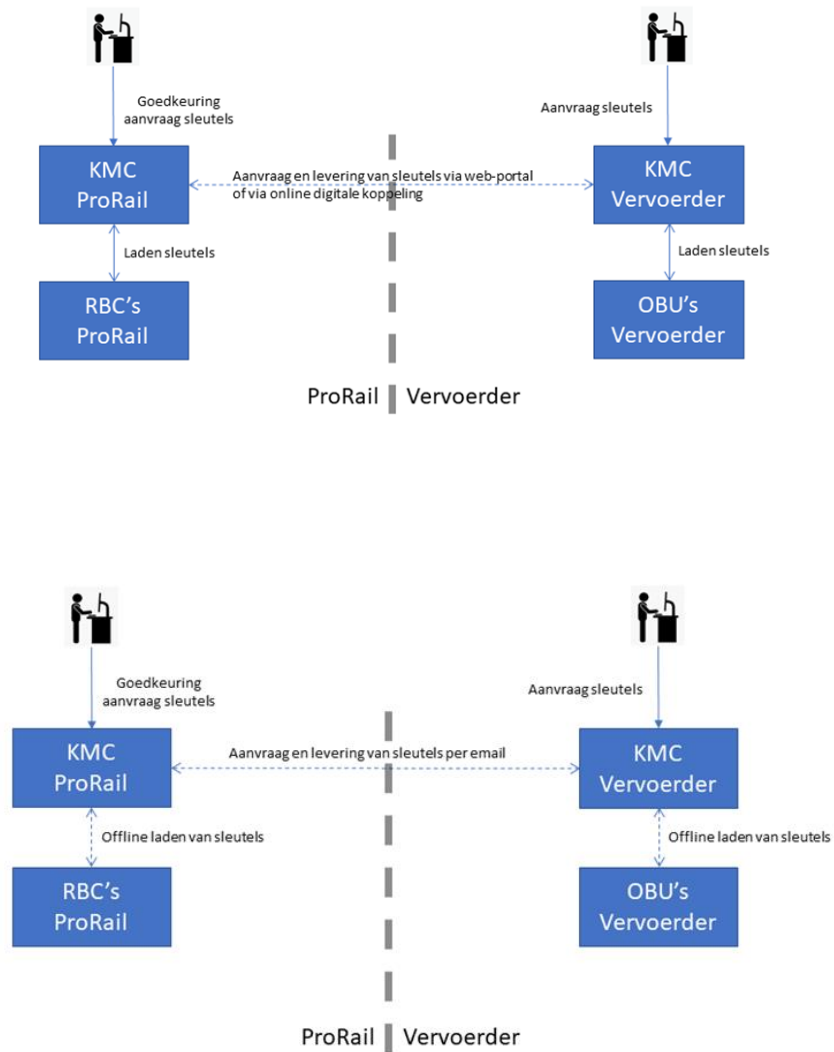
De verantwoordelijkheid voor een sleutel (o.a. generatie, geheimhouding, opslag en gebruik ervan) is vastgelegd. ProRail als infrabeheerder zorgt voor de generatie en opslag in de betreffende RBC, de vervoerder of materieleigenaar voor opslag in de OBU waarvoor de sleutel bedoeld is. Na de overdracht van de sleutel naar de vervoerder of materieleigenaar, is deze er verantwoordelijk voor zo ook voor de tijdige vervanging ervan.

Bedrijfseenheid Assetmanagement

De ETCS Key Management taak is binnen ProRail belegd bij het bedrijfsonderdeel Assetmanagement (AM). Buiten ProRail zijn medewerkers van vergelijkbare afdelingen van de vervoerders of materieleigenaar en andere infrabeheerders actief.

Huidig systeem voor ETCS Key Management

Voor de huidige ERTMS Baseline2 heeft ProRail voor de KMC-functie een offline applicatie, die de cryptografische sleutels beheert en uitgeeft. Distributie van deze cryptografische sleutels gebeurt nu nog offline via e-mail, brief of USB-stick. Het beheer- en distributieproces is nu omslachtig en levert beveiligingsrisico's op, zeker bij een landelijke uitrol van ERTMS. Enerzijds is de offline applicatie verouderd. Anderzijds biedt ERTMS Baseline 4 mogelijkheden om het proces van sleuteluitwisseling efficiënter te maken. Zo wordt het mogelijk om de doorlooptijd van het proces van het doen van een aanvraag tot het verkrijgen van een sleutel drastisch te beperken en om het proces van sleuteluitwisseling voor ERTMS-materieel verregaand te uniformeren en te automatiseren.



2 Scopebeschrijving

Binnen de scope valt:

- De ontwikkeling van de applicatie binnen de ProRail omgeving voor het afhandelen van een aanvraag tot het verkrijgen, goedkeuren, genereren, opslaan, distribueren (RBCs en andere KMCs), aanstaande verloop van geldigheid signaleren, vernieuwen en na verloop verwijderen van een sleutel.
- Integratie van de applicatie in een ProRail omgeving.
- Installeren en testen van de applicatie in een ProRail omgeving.
- Assisteren bij de migratie van bestaande sleutels uit het huidige offline ProRail Key Management Centre dat 'end of life' is.
- Beheren en ondersteunen van de applicatie op basis van een SLA.
- Leveren van consultancy voor upgrades en wijzigingen op verzoek van ProRail.
- Implementeren van upgrades en wijzigingen op verzoek van ProRail.

Buiten de scope valt:

- Online interface tussen het KMC van de vervoerder en de OBU van het materieel.

2.1 Uitgangspunten

ProRail hanteert een aantal uitgangspunten die van belang zijn voor deze aanbesteding.

- De oplossing zal binnen de ProRail Azure Cloud gerealiseerd worden. De ProRail Azure Cloud is de omgeving van waaruit ProRail publieke clouddiensten intern aanbiedt. Iedere applicatie krijgt een netwerkdeel beveiligd door firewalls.
- Communicatie van de te realiseren applicatie met de buitenwereld zal over beveiligde verbindingen plaatsvinden aan de hand van PKI en TLS certificaten die worden verzorgd door ProRail.

2.2 Projectteam

ProRail verwacht dat de opdrachtnemer de volgende specialismen zal inzetten in het projectteam:

- Projectleider/scrummaster
- Solution Architect
- Informatie analist
- UX/UI designer
- Ontwerper
- Ontwikkelaar/tester
- Testconsultant
- Specialist informatiebeveiliging