M6 Admin

Teknisk oversikt

Om M6 Admin | Systemarkitektur | Sikkerhet | Tekniske fakta

Om M6 Admin

M6 Admin er RCOs nye nettleserbaserte administrasjonsgrensesnitt og det første trinnet mot en ny administrasjonsplattform. Løsningen installeres sentralt og nås via en nettleser, noe som betyr at det ikke er behov for å installere en egen M6-klient på arbeidsstasjoner. M6 Admin benytter den samme SQL-databasen og eksisterende tilgangsstrukturen som R-CARD M5. Dette gjør det mulig å ta i bruk M6 Admin i eksisterende systemmiljøer, samtidig som administrasjonen gradvis kan flyttes over til det nye grensesnittet.

En trinnvis overgang

Den første versjonen av M6 Admin kompletterer R-CARD M5-klienten. M6 Admin brukes til funksjonene som er tilgjengelige i det nye grensesnittet, mens M5-klienten fortsatt kan benyttes for øvrige funksjoner. På sikt vil M6 Admin erstatte R-CARD M5-klienten.

Nettleserbasert administrasjon

M6 Admin installeres sentralt, og brukeren kobler seg til via nettleseren.

Felles systemdata

M6 Admin og R-CARD M5 benytter den samme SQL-databasen.

Eksisterende tilgangsstruktur

Operatører og sikkerhetsgrupper fra R-CARD M5 gjenbrukes.

Sentral oppdatering

Oppdateringer utføres sentralt på serveren og krever ingen lokal oppdatering på operatørenes arbeidsstasjoner.

M6 Admin i eksisterende systemmiljø

M6 Admin bygger videre på det eksisterende R-CARD M5-miljøet. M6 Admin og M5-klienten benytter den samme SQL-databasen, slik at begge kan brukes parallelt i overgangsperioden. M6 Admin benytter også de samme operatørene og operatørgruppene som R-CARD M5. Den eksisterende tilgangsstrukturen styrer dermed hvilke deler av M6 Admin en operatør kan se og bruke. Enkelte grunninnstillinger administreres fortsatt i R-CARD M5-klienten, mens den daglige administrasjonen gradvis flyttes over til M6 Admin.

Systemarkitektur

R-CARD M5 bygger på en felles SQL-database. M5-klienten og M6 Admin er to ulike administrasjonsgrensesnitt mot det samme systemet og kan brukes parallelt.

RaServer

RaServer håndterer kommunikasjonen mellom M5-klienten, adgangskontrollsystemet og SQL-databasen.

SQL-databasen

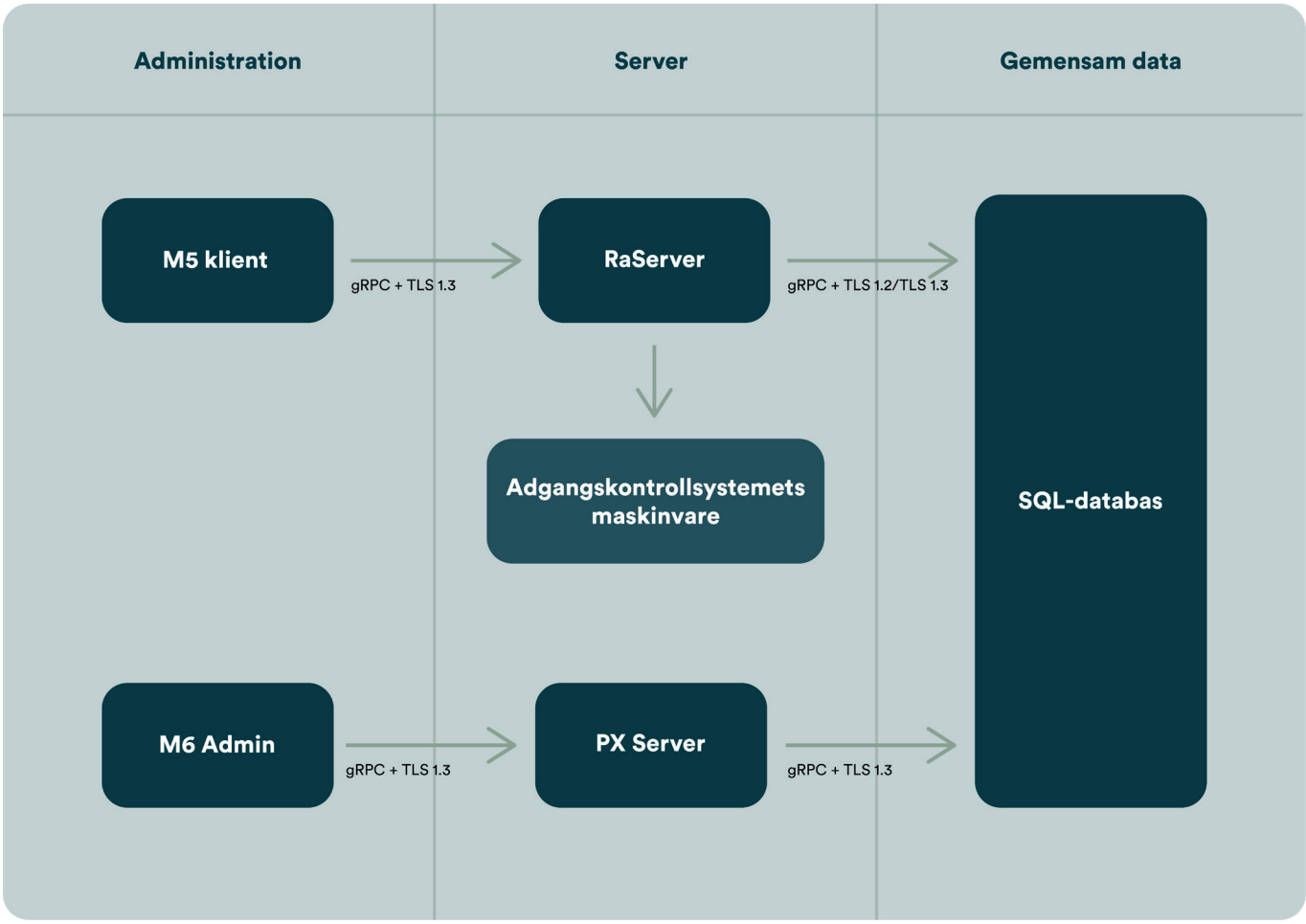
SQL-databasen lagrer systemdata og er den felles databasen for R-CARD M5.

R-CARD M5 klient

M5-klienten er det tradisjonelle administrasjonsprogrammet som kommuniserer med RaServer.

PX Server

PX Server er servertjenesten som benyttes av M6 Admin. Kommunikasjonen via PX Server skjer med gRPC, og M6 Admin benytter TLS 1.3.



Kommunikasjon og sikkerhet

M5 klienten → RaServer

Kommunikasjonen skjer via gRPC og er beskyttet med TLS 1.3. M5-klienten benytter et automatisk generert, selvsignert sertifikat for tilkoblingen.

RaServer → SQL-databas

Kommunikasjonen skjer via gRPC. TLS 1.2 er standard, mens TLS 1.3 støtter egne eller CA-utstedte sertifikater.

M6 Admin → PX Server

Kommunikasjonen skjer via gRPC, og M6 Admin benytter TLS 1.3. Standardporten er TCP 443. Dersom TCP 443 er opptatt, kan en annen port konfigureres.

PX Server → SQL-databas

Kommunikasjonen skjer via gRPC og TLS 1.3.

Sertifikater

M6 Admin benyttes TLS 1.3. Et selvsignert sertifikat følger med M6 Admin-installasjonen og kan velges under installasjonen. Bruken av dette sertifikatet er valgfritt. PX Server kan også benytte virksomhetens eget sertifikat, for eksempel et CA-utstedt serversertifikat.

Systemkrav og installasjon

For å kunne bruke M6 Admin kreves et eksisterende R-CARD M5-miljø.

Systemkrav

R-CARD M5: Versjon 5.52 eller nyere må være installert på serveren hvor M6 Admin skal installeres.

Servermiljø: Windows 11, Windows Server 2022 eller nyere.

.NET Framework: Versjon 4.8.1 eller nyere.

SQL Server: 2016 eller nyere.

Installasjon: M6 Admin installeres sentralt på serveren der R-CARD M5 er installert.

Sertifikat ved installasjon

Under installasjonen tilbys bruk av et medfølgende selvsignert sertifikat. Bruk av dette sertifikatet er valgfri, og PX Server kan i stedet konfigureres med virksomhetens eget sertifikat.

Tekniske anbefalinger og konfigurasjon

1. Overgang fra DCOM til gRPC
   RCO anbefaler at kunder går over fra DCOM til gRPC. Ved nyinstallasjoner bør gRPC velges som førstevalg. Ved oppgradering av eksisterende installasjoner som benytter DCOM, anbefaler vi å migrere til gRPC. Støtten for DCOM vil bli fjernet i en fremtidig versjon av M6 Admin.
2. Nettverksport
   Standardporten for M6 Admin via HTTPS er TCP 443. Dersom porten allerede er i bruk, kan en alternativ port konfigureres.
3. Databaseplassering
   For høyest mulig driftssikkerhet anbefales det at SQL Server og R-CARD M5 befinner seg i samme nettverkssegment.
4. PX Server
   Tjenesten må være startet for at M6 Admin skal være tilgjengelig. Kommunikasjonen via PX Server skjer med gRPC, og M6 Admin benytter TLS 1.3.
5. Sertifikater
   PX Server kan benytte virksomhetens egne serversertifikater fra sertifikatlageret eller som importerte PFX-, P12- eller PEM-sertifikater. Det medfølgende selvsignerte sertifikatet er valgfritt.
6. Klientlisenser
   M6 Admin benytter de samme klientlisensene som R-CARD M5-klienten. M5-klienten og M6 Admin deler de samme klientlisensene.
7. Oppdatering og versjonsavhengigheter
   M6 Admin er utviklet for i stor grad å kunne oppdateres uavhengig av R-CARD M5, men det kan forekomme tekniske versjonsavhengigheter. Oppdateringen utføres sentralt på serveren og krever ingen lokal oppdatering på brukernes arbeidsstasjoner.

Hva er TLS og gRPC?

TLS beskytter kommunikasjonen

TLS (Transport Layer Security) er sikkerhetsprotokollen som beskytter data når de sendes mellom to komponenter.

TLS krypterer trafikken, beskytter den mot manipulering og benytter sertifikater for å verifisere identiteten til serveren som klienten kobler seg til.

TLS 1.2 og TLS 1.3

TLS 1.2 er en veletablert og sikker standard når den er riktig konfigurert. TLS 1.3 er den nyere versjonen og forenkler protokollen ved å fjerne eldre kryptografiske alternativer, benytte sikrere standardinnstillinger og redusere tiden det tar å opprette en forbindelse. Resultatet er et moderne sikkerhetsnivå med mindre risiko for usikre, eldre konfigurasjoner.

I den nye kommunikasjonsarkitekturen benyttes gRPC mellom M5-klienten og RaServer, samt mellom RaServer og SQL-databasen. Kommunikasjonen mellom M5-klienten og RaServer beskyttes med TLS 1.3. Mellom RaServer og SQL-databasen er TLS 1.2 standard, med støtte for TLS 1.3 når SQL-miljøet og sertifikathåndteringen oppfyller kravene. M6 Admin benytter TLS 1.3 for kommunikasjonen via PX Server.

Sertifikatet og TLS-versjonen er to forskjellige ting

Et selvsignert sertifikat og et CA-utstedt sertifikat kan begge brukes til kryptert TLS-kommunikasjon. Forskjellen ligger først og fremst i hvordan sertifikatets pålitelighet verifiseres. Et selvsignert sertifikat må eksplisitt gjøres pålitelig i det aktuelle miljøet, mens et CA-utstedt sertifikat kan integreres i virksomhetens eksisterende PKI- og sertifikathåndtering.

gRPC styrer hvordan systemene kommuniserer med hverandre

gRPC er et moderne rammeverk for kommunikasjon mellom programmer og tjenester. Det bygger normalt på HTTP/2 og er utviklet for raske og strukturerte kall mellom systemkomponenter. gRPC benytter kompakte binære meldinger og støtter både vanlige kall og strømmebasert kommunikasjon.

I M6 Admin skjer all kommunikasjon via PX Server over gRPC, og M6 Admin benytter alltid TLS 1.3. gRPC beskriver hvordan informasjon og kall utveksles, mens TLS 1.3 beskytter selve kommunikasjonskanalen. De to teknologiene utfyller dermed hverandre.

Vi tar forbehold om eventuelle trykkfeil. Funksjoner, spesifikasjoner og systemegenskaper kan bli endret etter trykkdatoen.




RCO

