M6 Admin

Teknisk översikt

Om M6 Admin | Systemarkitektur | Säkerhet | Teknisk fakta

Om M6 Admin

M6 Admin är RCOs nya webbaserade administrationsgränssnitt och det första steget mot en ny administrationsplattform. Lösningen installeras centralt och nås via en webbläsare, vilket innebär att ingen separat M6-klient behöver installeras på användarens arbetsdator. M6 Admin använder samma SQL-databas och befintliga behörighetsstruktur som R-CARD M5. Det innebär att M6 Admin kan införas i den befintliga systemmiljön samtidigt som administrationen successivt flyttas över till det webbaserade gränssnittet.

En stegvis övergång

Den första versionen av M6 Admin kompletterar R-CARD M5 klienten. M6 Admin används för de funktioner som finns tillgängliga i det nya gränssnittet, medan M5 klienten fortsatt kan användas för övriga funktioner. På sikt kommer M6 Admin att ersätta R-CARD M5 klienten.

Webbaserad administration

M6 Admin installeras centralt och användaren ansluter via webbläsaren.

Gemensam systemdata

M6 Admin och R-CARD M5 använder samma SQL-databas.

Befintlig behörighetsstruktur

Operatörer och säkerhetsgrupper från R-CARD M5 återanvänds.

Central uppdatering

Uppdateringar sker centralt på servern och kräver ingen lokal uppdatering på användarnas arbetsdatorer.

M6 Admin i befintlig systemmiljö

M6 Admin bygger vidare på den befintliga R-CARD M5-miljön. Det webbaserade gränssnittet och M5 klienten använder samma SQL-databas och kan användas parallellt under övergången till M6 Admin. M6 Admin använder också samma operatörer och säkerhetsgrupper som R-CARD M5. Den befintliga behörighetsstrukturen styr därmed vilka delar av M6 Admin en operatör får se och använda. Vissa grundinställningar görs fortfarande i R-CARD M5 klienten medan den löpande administrationen successivt flyttas över till M6 Admin.

Systemarkitektur

R-CARD M5 bygger på en gemensam SQL-databas. M5 klienten och M6 Admin är två olika administrationsvägar mot samma system och kan användas parallellt.

RA Server

RA Server hanterar M5 klientens kommunikation med passersystemet och SQL-databasen.

SQL-databasen

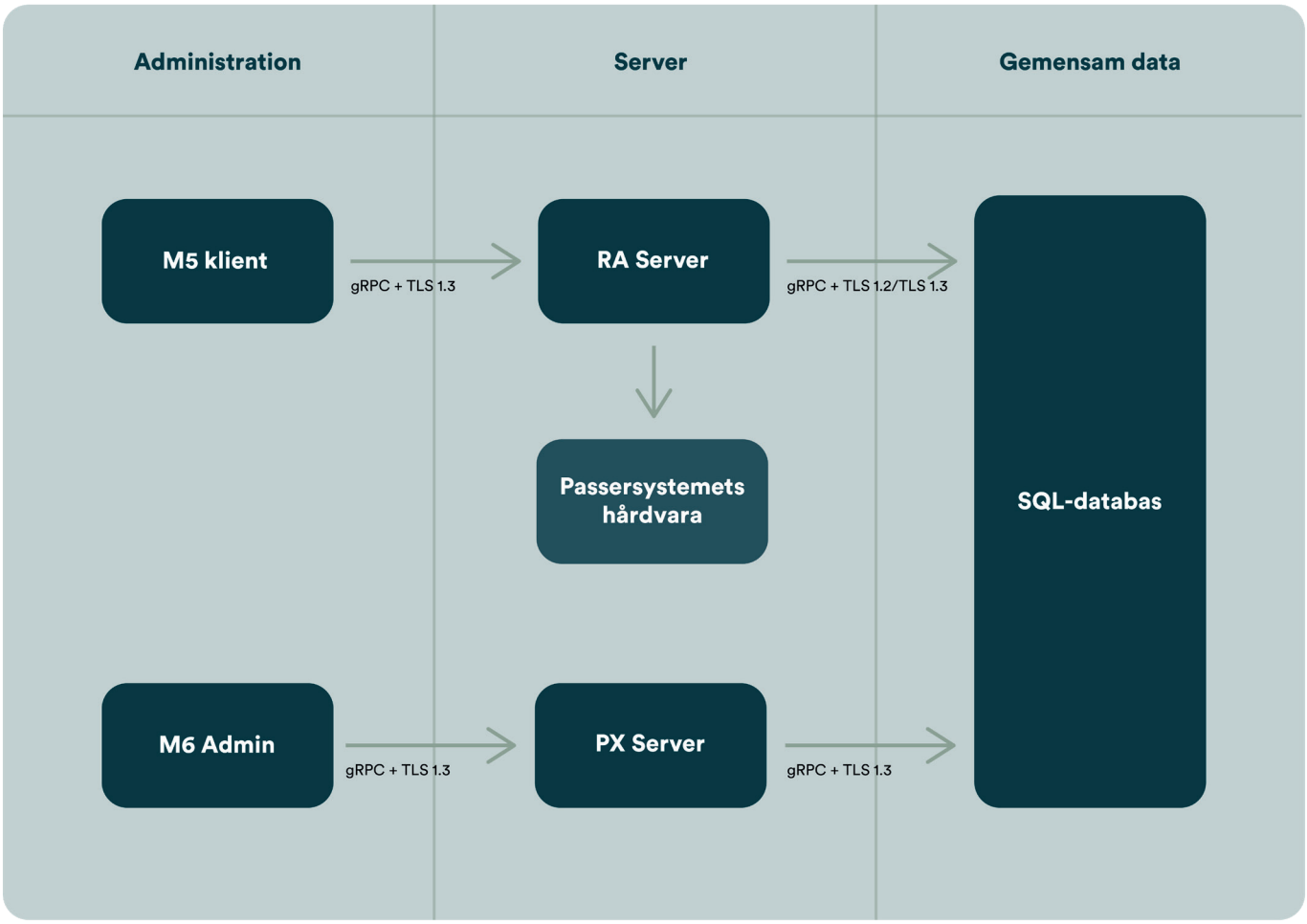
SQL-databasen lagrar systemdata och är den gemensamma databasen för R-CARD M5.

R-CARD M5 klient

M5 klienten är det traditionella administrationsprogrammet som kommunicerar med RA Server.

PX Server

PX Server är servertjänsten som används av M6 Admin. Kommunikation via PX Server sker med gRPC och M6 Admin använder alltid TLS 1.3.



Kommunikation och säkerhet

M5 klienten → RA Server

Kommunikationen sker med gRPC och skyddas med TLS 1.3. M5 klienten använder ett automatiskt genererat självsignerat certifikat för anslutningen.

RA Server → SQL-databas

Kommunikationen sker med gRPC. TLS 1.2 är standard och TLS 1.3 stöder eget eller CA-utfärdat certifikat.

M6 Admin → PX Server

Kommunikationen sker med gRPC och M6 Admin använder alltid TLS 1.3. Standardporten är TCP 443. Om TCP 443 är upptagen kan en annan port konfigureras.

PX Server → SQL-databas

Kommunikationen sker med gRPC och TLS 1.3. För M6 Admin används alltid TLS 1.3.

Certifikat

Ett självsignerat certifikat följer med M6 Admin-installationen och kan väljas vid installationen. Det är valfritt att använda. PX Server kan även använda organisationens eget certifikat, exempelvis ett CA-utfärdat servercertifikat.

Systemkrav och installation

För att kunna använda M6 Admin krävs en befintlig R-CARD M5-miljö.

Systemkrav

R-CARD M5: version 5.52 eller senare ska vara installerad på servern där M6 Admin installeras.

Servermiljö: Windows 11 eller Windows Server 2022 eller senare.

.NET Framework: version 4.8.1 eller senare.

SQL Server: 2016 eller senare.

Installation: M6 Admin installeras centralt på servern där R-CARD M5 är installerat.

Certifikat vid installation

Vid installationen erbjuds ett medföljande självsignerat certifikat. Användningen är valfri och PX Server kan istället konfigureras med organisationens eget certifikat.

Tekniska rekommendationer och konfiguration

1. Övergång från DCOM till gRPC.
   RCO rekommenderar att kunder går över till gRPC från DCOM. Vid nyinstallation ska gRPC vara förstahandsvalet. Vid uppgradering av befintliga installationer som använder DCOM rekommenderas byte till gRPC. Stödet för DCOM kommer tas bort i en framtida version av M6 Admin.
2. Nätverksport
   Standardport för M6 Admin via HTTPS är TCP 443. Om porten används kan en annan port konfigureras.
3. Databasplacering
   För högsta driftsäkerhet rekommenderas att SQL Server och R-CARD M5 ligger i samma nätverkssegment.
4. PX Server
   Tjänsten behöver vara startad för att M6 Admin ska vara tillgängligt. Kommunikation via PX Server sker med gRPC och M6 Admin använder alltid TLS 1.3.
5. Certifikat
   PX Server kan använda organisationens egna servercertifikat från certifikatlager eller importerade PFX-, P12- och PEM-certifikat. Det medföljande självsignerade certifikatet är valfritt.
6. Klientlicenser
   M6 Admin använder samma klientlicenser som R-CARD M5 klienten. M5 klienten och M6 Admin delar på de samtidiga klientlicenserna.
7. Uppdatering och versionsberoenden
   M6 Admin är utvecklat för att i stor utsträckning kunna uppdateras separat från R-CARD M5. Tekniska versionsberoenden kan dock förekomma. Uppdateringen sker centralt på servern och kräver därför ingen lokal uppdatering på användarnas arbetsdatorer.

Vad är TLS och gRPC?

TLS skyddar kommunikationen

TLS (Transport Layer Security) är säkerhetsprotokollet som skyddar data när den skickas mellan två komponenter.

TLS krypterar trafiken, skyddar den mot manipulation och använder certifikat för att verifiera identiteten på den server som klienten ansluter till.

TLS 1.2 och TLS 1.3

TLS 1.2 är en etablerad och säker standard när den är korrekt konfigurerad. TLS 1.3 är den nyare versionen och förenklar protokollet genom att ta bort äldre kryptografiska alternativ, använda säkrare standardval och korta ned anslutningsförloppet. Resultatet är en modernare säkerhetsnivå med mindre utrymme för osäkra äldre inställningar.

I den nya kommunikationsarkitekturen används gRPC mellan M5 Klient och RA Server samt mellan RA Server och SQL-databasen. M5 Klient till RA Server skyddas med TLS 1.3. Mellan RA Server och SQL-databasen är TLS 1.2 standard, med stöd för TLS 1.3 när SQL-miljön och certifikathanteringen uppfyller kraven. M6 Admin använder alltid TLS 1.3 för kommunikationen via PX Server.

Certifikatet och TLS-versionen är två olika saker

Ett självsignerat certifikat och ett CA-utfärdat certifikat kan båda användas för krypterad TLS-kommunikation.

Skillnaden ligger främst i hur certifikatet blir betrott. Ett självsignerat certifikat måste uttryckligen göras betrott i den aktuella miljön, medan ett CA-utfärdat certifikat kan passa in i organisationens befintliga PKI och certifikathantering.

gRPC beskriver hur systemen pratar med varandra

gRPC är ett modernt ramverk för kommunikation mellan program och tjänster. Det bygger normalt på HTTP/2 och är utformat för snabba, strukturerade anrop mellan systemkomponenter. gRPC kan använda kompakta binära meddelanden och stödjer både vanliga anrop och strömmande kommunikation.

I M6 Admin sker all kommunikation via PX Server med gRPC och M6 Admin använder alltid TLS 1.3. gRPC beskriver hur information och anrop utbyts, medan TLS 1.3 skyddar själva kommunikationskanalen. De två teknikerna kompletterar alltså varandra.

Vi reserverar oss för eventuella tryckfel. Funktioner, specifikationer och systemegenskaper kan komma att ändras efter tryckdatum.




RCO

