

Author: JAS, ØBL	Date: 21.12.2022	Revision: H	Document no: RMD-010
Systemarkitektur, RoomMate			

1 INNLEDNING

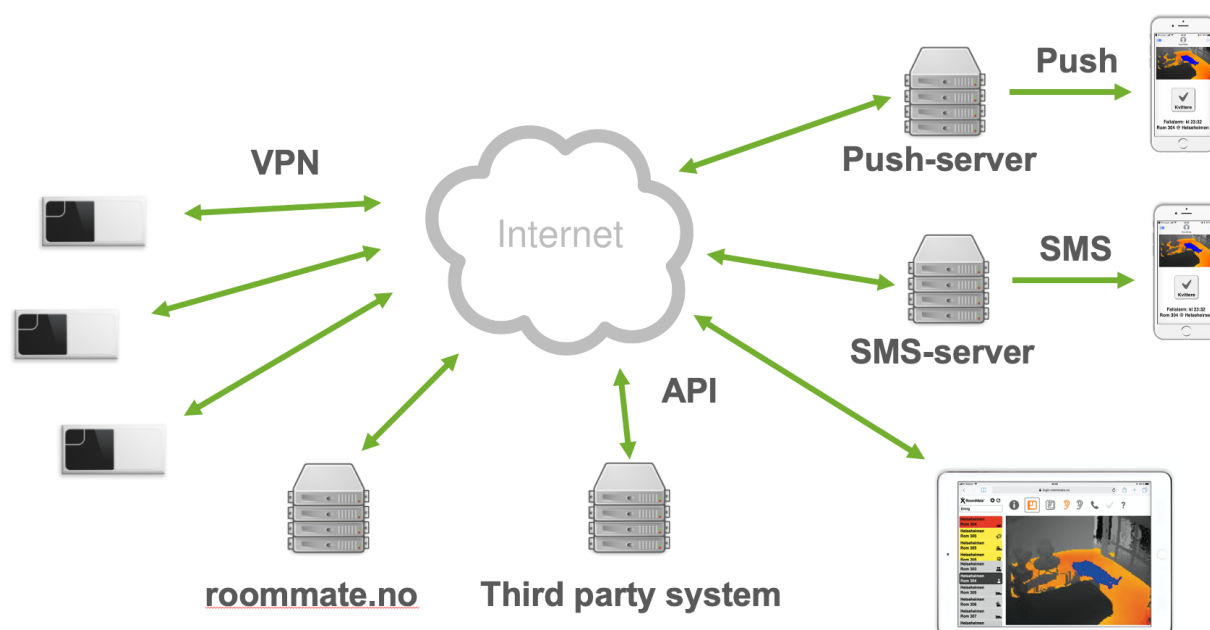
Dette dokumentet gir en kortfattet oversikt over systemarkitektur og dataflyt i RoomMate-systemet.

I tillegg til dette dokumentet så henvises det til øvrig dokumentasjon for RoomMate-systemet. Spesielt kan følgende dokumenter være av interesse:

- RMD-001, «*Installasjonsveiledning, RoomMate*»
- RMD-009, «*RoomMate API*»

2 SYSTEMARKITEKTUR

Overordnet systemarkitektur er vist i figuren nedenfor



Til venstre ses RoomMate-sensorene som er utplassert hos brukerne. RoomMate-sensorene kommuniserer via en kryptert VPN-kanal med en sentral RoomMate-server («*roommate.no*»). Denne server er en fysisk server eid av RoomMate AS og plassert i et sikkert profesjonelt datasenter i Oslo. RoomMate-sensorene har en egen innbygd datamaskin og det er her det gjøres databehandling for å detektere kritiske situasjoner. Det sendes derfor kun informasjon til roommate.no-serveren når det gjennomføres tilsyn eller når en alarm eller varsel skal sendes.

RoomMate har flere produksjonsservere som benytter forskjellige IP-adresser og brukerne av RoomMate systemet må åpne for en IP-range som gjør at RoomMate kan balansere og fordele last mellom disse. Dette gjelder både for sensorer og webklienter og app'er.

Alarmer og varsler kan for eksempel være at en person faller. Disse alarmer sendes til brukeren som push-melding til egen RoomMate-app eller som SMS (illustrert øverst til høyre). Brukeren kan da også velge å logge inn på roommate.no-serveren for å gjennomføre et tilsyn som vist på iPad'en nederst til

Author: JAS, ØBL	Date: 21.12.2022	Revision: H	Document no: RMD-010
Systemarkitektur, RoomMate			

høyre. Innlogging gjøres med brukernavn, passord og en egen kode (to-faktor-autentisering) samt mulighet for IP-filtrering. Kode for to-faktor-autentisering sendes vis SMS eller push-melding til app.

Hvis RoomMate-serveren på grunn av en feil ikke er tilgjengelig så kan RoomMate-sensorene selv sende alarmer og varsler på SMS via SMS-serveren. Det er ikke mulig å gjennomføre tilsyn hvis RoomMate-serveren ikke er tilgjengelig.

I tillegg til bruk av RoomMate som et stand-alone system som beskrevet ovenfor er det også mulig å integrere RoomMate-systemet inn i et eksternt system for alarmhåndtering. Dette er vist som et «Third party system» i figuren ovenfor. Et eget API for dette er implementert på RoomMate-serveren og all kommunikasjon mellom tredjepartssystemet og RoomMate-systemet går via RoomMate-serveren.

2.1 App

RoomMate AS har utviklet en egen app for iOS og Android. Appen er tilgjengelig gratis i Apple App store og Google Play. Bruk av app fremfor SMS har en rekke fordeler:

- Meldinger kommer frem raskere
- Bedre brukergrensesnitt
- Enklere innlogging for tilsyn
- Bedre kontroll på lydvarsling med egne lyder for varsler og alarm

App'en skal brukes for alle nye installasjoner og vil på sikt overta for SMS.

Varsler, alarmer og kode for to-faktor-autentisering sendes som push-melding via en ekstern push-server (Google Firebase). Dataflyt for app-bruken er som følger:

Ta i bruk app:

1. I administrasjonssystemet til RoomMate kan man hente ut en 10-sifret kode for hver bruker av systemet.
2. Ved første oppstart av app'en så vil denne etterspørre koden.
3. App'en henter automatisk et «push-token» fra push-serveren (https).
4. App'en sender kode og push-token til RoomMate-serveren (https)
5. RoomMate-serveren genererer en unik app-id som sendes til app'en (https). App-id brukes for all videre kommunikasjon mellom app og RoomMate-server. App-id'en har en begrenset levetid før den skiftes ut.

Sende varsel eller alarm til app'en:

1. RoomMate-serveren sender en push-melding via push-serveren (https). Push-meldingen inneholder tekster som beskriver hendelsen samt informasjon om varslingslyd.
2. Når app'en åpnes så henter den informasjon om utstående varsler og alarmer fra RoomMate-serveren (https). Denne informasjon omfatter bl.a. en lenke tilsvarende den som blir formidlet via SMS.
3. Hvis RoomMate-serveren ser at levetiden til App-id'en har utløpt eller er ved å utløpe så vil den først oppdatere til ny app-id. Dette skjer som en push-melding for å være sikker på hvem som er mottaker.

App'en inneholder også en knapp for direkte innlogging i systemet. Ved bruk av denne vil to-faktor kode bli håndtert i bakgrunnen uten brukermedvirkning. Dette fordi systemet allerede vet at brukeren har den aktuelle telefon i hånden.

Author: JAS, ØBL	Date: 21.12.2022	Revision: H	Document no: RMD-010
Systemarkitektur, RoomMate			

3 KRAV TIL NETTVERK

RoomMate-systemet benytter forskjellige URL for forskjellige versjoner av systemet:

Legacy-system satt i drift i 2016. Dette systemet brukes ikke lengre for nye installasjoner.*	roommate.no
Nytt system idriftsatt 2021 i Oslo kommune	roommate2.no
Nytt system idriftsatt 2021	roommate3.no
Nytt system idriftsatt 2022	roommate4.no
Nytt system idriftsatt 2022	roommate5.no

* For legacy-systemet vil det fortsatt benyttes SMS til varsling

Kunder koblet til for eksempel roommate3.no som skal ha nye sensorer eller flere lokasjoner fortsetter på roommate3.no serveren etc.

Fra og med desember 2022 skal nye kunder eller kunder som migreres fra roommate.no kobles mot roommate4.no.

For at RoomMate system skal fungere må det gjøres en åpning i firewall for følgende IP range:

- 82.199.16.0 - 82.199.16.255

RoomMate-sensoren må være koblet til internett via Ethernet eller WiFi og som et minimum må følgende tilganger være tilgjengelig:

- VPN-tunellen settes fortrinnsvis opp på port 1194 (UDP). Hvis port 1194 ikke er åpen brukes port 443 (TCP).
- Port 123 (UDP) for NTP.
- Port 53 (TCP+UDP) for DNS.
- Hvis RoomMate-sensoren selv skal sende varsler (hvis serveren ikke er tilgjengelig) så trengs port 443 (TCP) og 587 (TCP+UDP).

For brukeren som ønsker å motta varsler og utføre tilsyn så trengs følgende tilganger:

- Port 443 (TCP)
- Port 3478 (UDP)
- Port 5349 (TCP / UDP)
- Port 50000-53999 (UDP) for audiofunksjonalitet. Dette omfatter to-veis tale og innlytt.

URL'ene som benyttes i RoomMate systemet er:

Domain	Protocol	Port
app.roommate(x).no	http / https	80 / 443
login.roommate(x).no	http / https	80 / 443
voip.roommate(x).no	wss	443
www.roommate(x).no	http / https	80 / 443
vpn.roommate(x).no	openvpn / https	1194 / 443
turn.roommate(x).no	turns	5349 / 3478

* x = ingen ting eller et helt tall

Author: JAS, ØBL	Date: 21.12.2022	Revision: H	Document no: RMD-010
Systemarkitektur, RoomMate			

For at RoomMate-app'en skal fungere er det krav til at telefonen kan motta push-meldinger. Det er derfor følgende krav til åpninger i nettverket telefonen er koblet til:

iOS

Følgende porter må være åpne: 443, 2197, 5223. Dette gjelder for adressene 17.0.0.0/8. Utfyllende informasjon om push-meldinger til iOS finnes her:
<https://support.apple.com/en-us/HT203609>

Android

Følgende porter må være åpne: 443, 5228, 5229, 5230. Enten må de være åpne for alle IP-adresser eller også må man forholde seg til en dynamisk liste over IP-adresser. Utfyllende informasjon om push-meldinger til Android finnes her:
<https://firebase.google.com/docs/cloud-messaging/concept-options#messaging-ports-and-your-firewall>