

Arkitekturbeskrivelse

Dette dokumentet detaljerer arkitekturen for adgangskontroll.

Version : v0.90

Dato : 10. september 2018



Versjonshistorikk

Dato endret	Versjonsnr.	Forfatter	Godkjent av:	Kommentarer
20.05.2018	0.50	Tristan Rolstad		Opprettet dokumentet
6.09.2018	0.60	Henrik Christiansen		Tilpasset språk
10.09.2018	0.90	Tristan Rolstad	Tristan Rolstad	Oppdatert dokument

Innhold

Versjonshistorikk.....	1
Innhold	2
Formål med dokumentet.....	3
Innledning og bakgrunn	3
Problembeskrivelse	3
Føringer	3
Fremtidige behov.....	4
Begrepsforklaring.....	4
Avgrensninger.....	4
Funksjonsbeskrivelser	5
Adgangssystem.....	5
Kortlesere og adgangskort	5
Arkitektur	6
Skybaserte løsninger.....	6

Formål med dokumentet

Dette dokumentet er ment for å beskrive Bærum kommunes krav til løsning for adgangskontroll, for å sikre at kommunen velger løsninger og leverandører som passer i det overordnede bildet nå og i fremover.

Dokumentet er en del av kommunens arkitekturbibliotek, og er ett underdokument til referansearkitekturen for tingenes internett (IoT). Dokumentet er skrevet detaljert nok til at det kan leses frittstående, og føringene her er de gjeldende for adgangskontroll.

Innledning og bakgrunn

Problembeskrivelse

Adgangskontroll i Bærum kommune består i dag av en rekke ulike systemer og tekniske løsninger, fra flere leverandører og med ulike versjoner av systemene fra hver leverandør.

Bærum kommune vedlikeholder og administrerer i dag adganger i mange systemer, og situasjon er at nøkkelkort i de aller fleste tilfeller ikke kan gjenbrukes på tvers av lokasjoner. Det er heller ingen sentral styring og tilsyn av adgangssystemene, og flere av løsningene er uforholdsmessig dyre i drift grunnet teknisk tilstand. Gjennom ett sentralt system for administrasjon, med tilgang til å styre hvert enkelt adgangskontrollsystem, ønsker kommunen å effektivisere, forenkle, forbedre og sikre at gjeldende lover og regler overholdes.

Føringer

Som en følge av Digitaliseringsstrategien og innføringen av ny personvernforordning, er det behov for å samkjøre adgangssystem og legge til rette for å etablere et toppsystem. Med denne tilnærmingen og den fremtidige løsningen for toppsystem vil Bærum kommune kunne velge fritt blant leverandører av adgangssystemer, og tilpasse adgangssystemet til de ulike lokasjonenes sikkerhetsnivå. Den helhetlige tankegangen innebærer at alle adgangssystem kan kommunisere med hverandre gjennom et toppsystem.

En dør inn er et politisk besluttet prosjekt som skal lette tilgangen for publikum inn i Bærum kommunes lokaler.

Det er i utgangspunktet ikke ønskelig med forskjellige adgangssystem. Grunnen til at det bør åpnes opp for det er at det vil være svært kostnadskrevende å standardisere på et system all den tid vi har såpass mange eksisterende anlegg hvor kortleseren er avhengig av et gitt adgangssystem. Videre er utviklingen på området såpass høy at det vil være ressurskrevende å stadig oppdatere kommunens bygg-håndbøker og kravspesifikasjonene. Derfor er det vurdert som bedre å innføre et toppsystem som kan styre alle adgangssystemene.

Fremtidige behov

Det jobbes for en felles løsning for ID-kort, slik at alle kommunens ansatte kan gå med et gyldig ID-kort synlig når de er på jobb. ID-kortets utforming vil variere noe ift. type stilling, men felles for alle er at hver enkelt medarbeider har et kort som også kan benyttes til adgangskontroll, både med kortleser av gammel type, berøringsfrie og med chip for autentisering inn i sikrede systemer. For at ansatte skal slippe å gå med brikker og kort for hver lokasjon de skal ha tilgang til, og hvert enkelt bruksområde, vil et sentralt administrert kort kunne gi riktig tilgang til riktig tid.

Det vil være behov for å få tilgang ved hjelp av mobiltelefon for å støtte midlertidige tilganger. Dette kan være tilganger for publikum, eller for håndverkere som skal utføre arbeid i Bærum kommunes lokaler over en kort periode. Her er det ingen endelig standard grunnet markedets modenhet, men felles er at det skal være lav terskel for å ta det i bruk (dvs. ikke registrering hos 3. part, osv.)

Begrepsforklaring

Uttrykk	Beskrivelse
Adgangssystem	Styringssystemet for adgangskontroll
Adgangskort	Fysisk kort eller brikke, som leses av en kortleser.
IoT-knutepunkt	Et samlande knutepunkt i referansearkitekturen, som kobler sammen adgangssystemene og tilrettelegger for bruk av et toppsystem
Toppsystem	Et overordnet system for administrasjon av adgangssystem

Avgrensninger

Adgangskontroll som beskrevet her, er ikke en del av eLås i Pleie og omsorg.

Funksjonsbeskrivelser

Funksjonsbeskrivelsen deles opp i adgangssystem og kortlesere og adgangskort/adgangsbrikke. Med adgangssystem menes styringssystemet, mens det fysiske laget med adgangskort og kortlesere er beskrevet separat.

Adgangssystem

Adgangssystemet må levere et API som kan integreres mot IoT-knutepunktet og via dette et toppsystem i referansearkitekturen.

Informasjon og instruksjoner må kunne sendes og mottas av adgangssystemet gjennom API-et.

API-et må ha støtte for administrasjon av tilganger; med dette menes det at man må kunne opprette, oppdatere/endre, og fjerne, tilganger og brukere i adgangssystemet.

API-et må gi tilgang til sikkerhetsmekanismene i adgangssystemet, for sending av informasjon om misbruk av kort, f.eks. at det har blitt forsøkt kopiert, til toppsystemet. I tilfeller hvor et adgangssystem registrerer misbruk, vil man gjennom toppsystemet kunne fjerne tilgang i alle andre adgangssystemer.

Instruksjonene som må støttes av adgangssystemets API vil også være låsing og opplåsing av dørlåser. Dette vil tillate at adgang gis eksempelvis ved hjelp av en app på en telefon, som kommuniserer med toppsystemet og sender instruksjon om opplåsing av en dør til adgangssystemet. Merk at bruk av app skal gjøres enkelt for brukeren (f.eks. må det være gode grunner for registrering av brukeren hos en ev. 3. part.)

Kortlesere og adgangskort

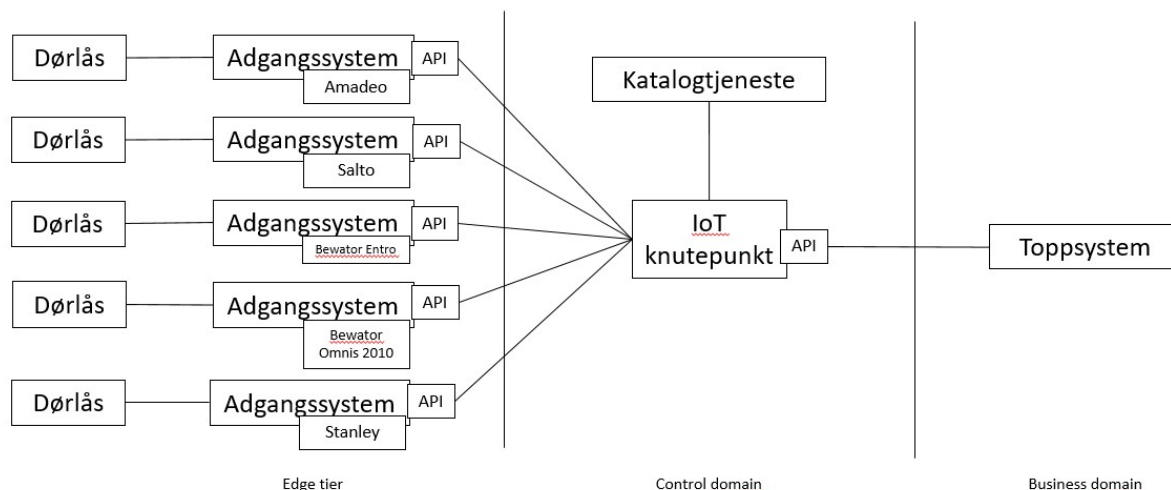
Dørlåsen, som det er referert til i den skjematiske fremstillingen, og herunder leseren og adgangskortet/adgangsbrikken, skal benytte teknologi som ikke har blitt kompromittert, eller har kjente sikkerhetshull.

Løsninger som baserer seg på kompromittert teknologi, eksempelvis Mifare Classic og Mifare DESFire (MF3ICD40), skal ikke benyttes. Lesere og adgangskort skal minimum holde et sikkerhetsnivå som Mifare DESFire EV1 teknologi, eller lignende.

Adgangskort og adgangsbrikker må bruke ikke-proprietær teknologi til adgangssystemet. F.eks. så må utveksling av data mellom berøringsfri leser og kortet foregå på bransjestandarder som støttes av flere produsenter, f.eks. RFID, NFC, eller lignende. Likeledes vil kortleseren måtte støtte den samme teknologien, og heller ikke være proprietær mot adgangssystemet. Med det menes at kortleseren må kunne lese kort fra andre produsenter i markedet via utvekslingsprotokoller som anses som bransjestandarder. Denne føringen er sentral for å kunne innføre et felles ID-kort som kan brukes på tvers av lokasjoner og adgangssystemer.

Kortlesere skal være berøringsfrie, ha tastatur for bruk av PIN-kode og lysdioder med farger for indikasjon av status. Kortlesere må kunne lese kort med flere lag for forskjellige sikkerhetsnivåer. Hvis kortleserne har batteri må livssyklus-kostnaden (LCC) være dokumentert, og batteriet må vare i minst 3 år ved normal bruk.

Arkitektur



Begrepe Edge Tier, control domain og business domain følger referansearkitektur for Industrial Internet of Things, volum G1 [IIC-PUB:G1:V1.80:20170131]

Arkitekturbildet viser hvordan adgangssystemet, her inntegnet med noen av systemene som brukes i dag, og de underliggende komponentene (dørlås, adgangskort og kortleser), henger sammen og bruker IoT-knutepunktet for å kunne etablere et toppsystem.

Skybaserte løsninger

Adgangssystemet kan i gitte leveres som en lokal installasjon eller som en skybasert løsning. I alle tilfeller må adgangssystemet behandle og lagre data i tråd med den nye personvernforordningen, og forholde seg til datatilsynets tolkning. Leverandør må kunne dokumentere hva og hvordan adgangssystemet lagrer av data knyttet til bruk, samt hvor lenge denne informasjonen lagres. I tilfellet man ønsker en skybasert løsning må databehandleravtale signeres, og denne må være godkjent av Bærum kommune før anskaffelsen gjennomføres.

En risiko- og sårbarhetsanalyse (ROS-analyse) må i alle tilfeller gjennomføres for adgangssystemet.