

Kundens tekniske plattform

Juni 2018



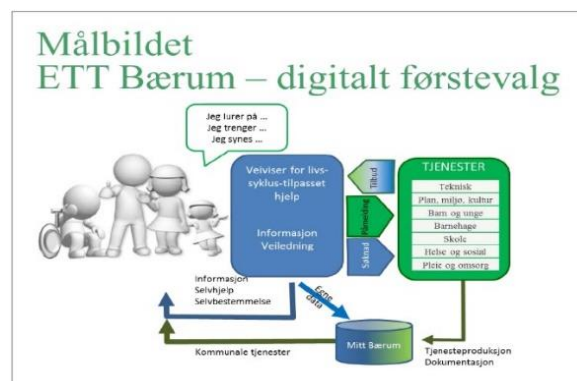
BÆRUM KOMMUNE

Bærum kommune har fire fokusområder innen teknologiarkitektur; informasjonssikkerhet, dokumentasjonsforvaltning, identitetsstyring og integrasjon. Formålet med dette dokumentet er at leverandører og andre interessenter skal se hvor Bærum kommune har sitt fokus og bedre forstå krav knyttet til arkitektur og teknologi som settes i anskaffelsesprosjektene.

Arkitektur – behov og føringer

Bærum kommune har behov for en arkitektur som understøtter Difis arkitekturprinsipper¹, med spesiell vekt på tjenesteorientering, der komponenter tilbyr og konsumerer informasjon via standardiserte grensesnitt. Krav til arkitektur og teknologi har til hensikt å sørge for at ny løsning er i tråd med arkitekturprinsippene og legge til rette for effektiv integrasjon og gjenbruk av data. Data som forvaltes skal gjøres så åpne som mulig for innsyn for innbygger/næringsliv, samt for integrasjon i andre system for effektiv gjenbruk i andre delprosesser.

Figuren til høyre viser hovedmålbildet som Bærum har lagt til grunn for kommunens arkitektur. Tanken er at innbyggere og næringsliv får nødvendig innsyn i egne data, og at kommunen kan tilby tjenester på bakgrunn av tilgjengelig informasjon. Bærebjelken i målbildet er at kommunen har en enhetlig strategi for kommunikasjon med innbyggerne. Det kan bety at Leverandør skal ha løsninger som er mulige å bygge inn i Bærums nåværende og fremtidige kommunikasjonskanal med innbyggeren.



Bærum kommune vektlegger nasjonale føringer i sine løsninger og prosjekter. Av disse vektlegges særskilt prinsippet om tjenesteorientering for å sikre en fremtidsrettet og fleksibel arkitektur, samt sikkerhet for å sikre bl.a. trygghet for ivaretagelse av personvern som spesielt sentralt.

I tillegg har Bærum kommune følgende prinsipper/føringer som skal legges til grunn ved valg av nye løsninger:

- **Brukeren i sentrum** - «All virksomhetsendring fokuserer på enkelhet for brukerne med størst mulig grad av automatisering, oppgaveforenkling og intuitive grensesnitt»
- **Informasjon som sentral ressurs** - «Informasjon er en ressurs som skal forvaltes og i størst mulig grad gjøres tilgjengelig for effektiv bruk på tvers av prosesser og tjenesteområder»
- **Størst mulig verdi for virksomheten som helhet**- «Valg og prioriteringer må baseres på hvilke alternativ som gir størst verdi for virksomheten som helhet».
- **Helhetlig livssyklus** – «Valg av teknologi og løsninger må ta utgangspunkt i totaleffektivitet og totalkostnad gjennom hele livssyklusen til teknologien og løsningen».
- **Følger standarder** – «Tjenester som realiseres skal følge relevante standarder, retningslinjer; både internasjonale, nasjonale, sektorspesifikke og lokale»
- **Benytter anerkjent og velprøvd teknologi** – «Virksomhetskritiske tjenester og sentral infrastruktur er basert på anerkjent og velprøvd teknologi med god tilgang på kompetanse og support»

¹ <https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/nasjonal-arkitektur>

Fire fokusområder

Bærum kommune ønsker å sette fokus på de områdene vi mener det behøves ekstra oppmerksomhet på, både fra eget hold og fra eksterne virksomheter. Vi ser bl.a. at identitetsstyring og tilgangsadministrasjon er et område som mange leverandører av programvare har utfordringer med. Ved å beskrive med enkle ord behovene vi som kommune har er målet at kravene som er satt i en anskaffelse blir tydeligere.

Informasjonssikkerhet

Informasjonssikkerhet er svært viktig for Bærum kommune. Kommunen benytter et rammeverk basert på ISO 2700x, og må i tillegg overholde kravene i Norm for informasjonssikkerhet² der det behandles personsensitive data. Informasjonssikkerhet betyr i korthet at vi må ha systemer og rutiner som ivaretar tre viktige hensyn: konfidensialitet, integritet og tilgjengelighet.

- **Konfidensialitet** betyr at informasjonen vi lagrer kun skal kunne leses av de som er autoriserte og har behov for informasjonen i sitt arbeid.
- **Integritet** betyr at informasjonen vi lagrer alltid skal være korrekt og fullstendig. Det er svært viktig at ingen andre enn de som er autorisert har mulighet til å endre eller slette data.
- **Tilgjengelighet** betyr at informasjonen alltid må være tilgjengelig for autoriserte brukere når de har behov for dataene.

Det er svært viktig at tilbudt løsning opprettholder kommunens håndtering av personopplysninger, ikke minst med tanke på ny personvernforordning som kommer mai 2018.

Dokumentasjonsforvaltning

Bærum kommune stiller krav til at fagsystemene som anskaffes understøtter en helhetlig dokumentasjonsforvaltning. Tidligere ble begrepet arkiv, og arkivering benyttet, men for å ivareta hele fokusområdet benyttes nå begrepet dokumentasjonsforvaltning.

Kommunen har flere lovkrav som skal dekkes, deriblant arkivloven, offentleglova, forvaltningslova og flere særlover og forskrifter. Målet med disse kravene er at Bærum kommune som virksomhet skal ivareta behovene for dokumentasjon for å kunne utøve en forsvarlig tjeneste i nåtid og fremtid

God informasjons- og dokumentasjonsforvaltning handler om å kunne legge frem bevis på saksbehandling i form av gjennomførte transaksjoner, aktiviteter og prosesser. Det handler om rask og enkel tilgang til informasjonen virksomhetens ansatte trenger for å kunne utføre sine arbeidsoppgaver på en effektiv måte. Dokumentasjon skal **forvaltes og bevares på en måte som sikrer dens autenticitet, pålitelighet, integritet og brukervennlighet**.

Kommunen jobber aktivt med digitalisering på flere nivåer, og en god forvaltning av dokumentasjon er nødvendig for å understøtte digitaliseringstiltakene som pågår. Et eksempel er MinSide hvor innbyggerne får et kontaktpunkt inn mot kommunen for både innsyn, saksbehandling, samhandling med kommunen, mm.

² <https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet>

Identitetsstyring og tilgangsadministrasjon

Bærum kommune utvikler en ny løsning for å styre og administrere tilganger og identiteter som skal være ferdige innen ny personvernforordning trer i kraft³. Løsningen vil bestå av en selvbetjeningsplattform hvor brukerne selv kan nullstille sitt eget passord, få oversikt over tilgangene de har og be om nye tilganger. Tilgangsstyringen er basert på rollebasert tilgang. Dette forenkler prosessen med å oppdatere tilganger, slik at en leder ikke trenger å være usikker på hva hver ansatt kommer til å trenge, og slipper å bruke tid på å avklare de grunnleggende behovene for tilganger.

- Når en **nyansatt** kommer første dag på jobb vil alle basistilganger for rollen være klare. Det eneste den nyansatte trenger å gjøre er å sette passordet sitt for så å logge inn og begynne å jobbe.
- Når en ansatt **byter tjenesteområde** vil løsningen automatisk gi den ansatte nye tilganger og fjerne de gamle iht. de rollene vedkommende har fått.
- Når en **ansatt slutter** skal alle tilgangene i kommunens systemer automatisk fjernes og oversikten arkiveres. Målsettingen er at identitets- og tilgangsadministrasjon skal skje sentralt i den nye løsningen og ikke i de enkelte fagsystemene.

Integrasjoner

I Bærum kommune regnes all informasjon om innbyggere, saksbehandling og tjenesteproduksjon som sentrale ressurser. Det er derfor viktig for kommunen å ha kontroll over og tilgang til all slik informasjon.

For å kunne støtte målbildet «ETT Bærum – digitalt førstevalg», beskrevet ovenfor, skal alle løsninger tilby grensesnitt (API) som gir tilgang til all informasjon som er lagret i løsningen. Grensesnittet skal være basert på åpne standarder og skal ha støtte for sikkerhet som er tilstrekkelig for den informasjonen som er lagret i løsningen. Hvis det finnes nasjonale standarder, og/eller føringer, skal disse benyttes.

API skal både gi mulighet for søk og oppslag av informasjon som for eksempel er egnet for bruk i en MinSide-løsning for kommunens innbyggere, og for å kunne hente ut komplette datasett for eksempel for å kunne konvertere data over til annen løsning.

Bærum kommune har implementert en Enterprise service bus (ESB) basert på Mule ESB (<http://www.mulesoft.com>), BK-ESB. Nye integrasjoner mellom systemer i Bærum kommune skal implementeres som tjenester i BK-ESB hvis det ikke finnes tungtveiende grunner for å løse integrasjonen på en annen måte.

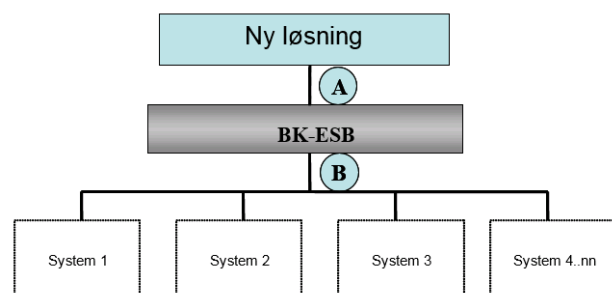
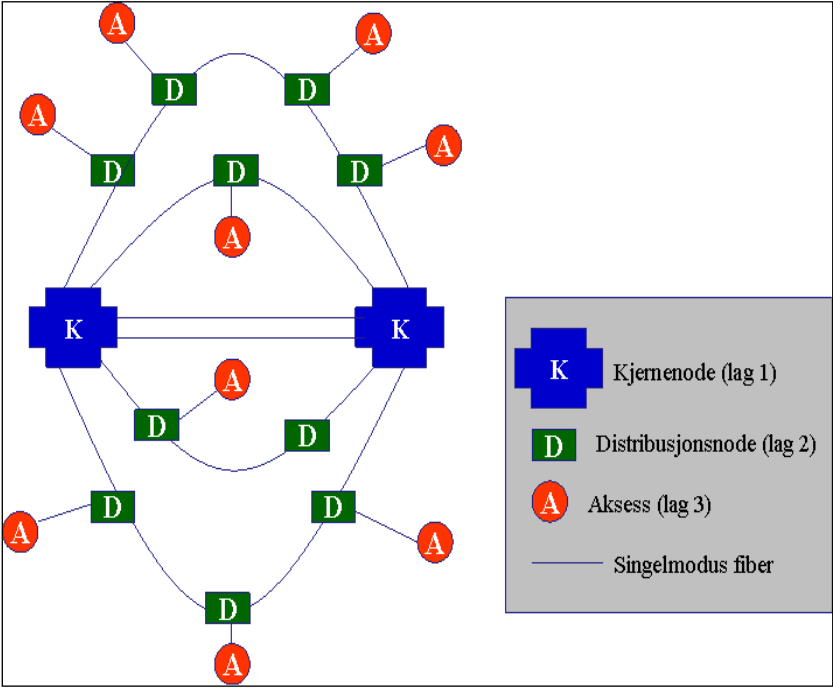


Figure 2 - Integrasjonsgrensesnitt og informasjonsflyt

³ <https://www.datatilsynet.no/regelverk-og-skjema/nye-personvernregler/>

Teknologistandarder hos kunden

Område	Standard	Kommentar/beskrivelse
1.0 Nettverkskommunikasjon		
1.1 Hardware	Produsent: Cisco Modeller: Catalyst serie switcher (65xx, 37xx, 38xx, 29xx) og Nexus-serien	
1.2 BK-MAN	Nettverket har følgende nøkkelegenskaper: • 10 Gbit i kjerne • 1 Gbit til aksesslokasjoner. • Soneinndelt med dedikerte soner for PC-klienter, byggautomasjon, IP-telefoni m.m. • Klargjort for prioriteringsmekanismer. • Full redundans i distribusjonsnettet • Mulighet for redundant aksess (benyttes for større kontorer)	Kunden har etablert et MPLS-basert fibernett med forbindelse til de fleste lokasjoner i kommunen. Det er mer enn 250 lokasjoner tilknyttet BK-MAN. Fibernettet benytter leid mørk fiber der Kunden eier og drifter teknisk utstyr. Kapasitet og stabilitet tilstrekkelig til at Kunden kan sentralisere alle sine dataressurser (servere, lagring, Internett etc.). Løsningen er bygget opp med tre lag og vises i figuren under: 1. Lag 1, kjernenett. Bestående av to noder, en kjernenode i datarommet i Kommunegården i Sandvika og en kjernenode i et beredskapsdatarom et annet sted i Bærum kommune. 2. Lag 2, distribusjonsnett: Distribusjonsnoder bygget opp i en ringstruktur med hovedformål å etablere redundans og redusere fiberlengdene i aksessnettet. 3. Lag 3, aksessnett: Aksess fra det enkelte tjenestested til den nærmeste distribusjonsnoden.

		 Figur 5 – Skisse over nettverksstruktur
1.3 BK-LAN	BK-LAN eksisterer kun i kommunens datasentre. Det benyttes VLAN-teknologi for inndeling av nettet i soner. Termineringspunkt for de enkelte VLAN er brannmurer. Det benyttes kun statisk IP-ruting i BK-LAN. Redundans er etablert ved bruk av Rapid	BK-LAN benyttes for mange servertjenester. Noen servertjenester er også etablert i BK-MAN. Alle servertjenester tilknyttet sikker sone (der sensitive data behandles) er etablert i BK-LAN.

	Spanning Tree (IEEE 802.1W) som gir lokal redundans på lag 2. For all intern ruting benyttes det private IP-adresser basert på RFC1918.	
1.4 BK-WAN (VPN)	Løsningen har følgende nøkkelegenskaper: • VPN-forbindelse, kan benytte private IP-adresser • 1-20 Mbit kommunikasjonskapasitet for hver enkelt tilkoblet aksess. • Alle soner tilgjengelig i BK-MAN er tilgjengelig.	Tjenestesteder som ikke har fibertilknytning (MAN eller LAN), har en datatilknytning til Bærum kommune basert på DSL. Dette gjelder et fåtall av tjenestestedene i kommunen. På disse lokasjonene settes det opp en ruter som tilbyr de samme sonene som er tilgjengelige i MAN. All kommunikasjon mellom tjenestestedet og Kundens sentrale nettverk kjøres i en VPN-tunnel.
1.5 Sikkerhetsløsninger	Sonebasert segmentering av datanett med følgende overordnede sonebegreper: • Ekstern • Intern • Sikker	Kunden har flere separate sikkerhetsbarrierer som virker uavhengig av hverandre. Sikkerhetsbarrierene skiller datanettets hovedsoner og undersoner. Mot enkelte soner benyttes to separate sikkerhetsbarrierer i kombinasjon. I tillegg er det etablert filtreringstjenester basert på innhold. Sikker sone eksisterer kun i kommunens datasentere.
1.6 Eksterne leverandører		Kunden har etablert egne kommunikasjonsforbindelser med enkelte eksterne leverandører av datatjenester. Denne kommunikasjonen er regulert av forskjellige sikkerhetsbarrierer. Ved utveksling av sensitive data, passord og lignende, benyttes krypterte forbindelser. Kunden benytter også i stor grad VPN-klienter som eksterne leverandører må installere på sine PCer for å kunne jobbe på løsninger hos Kunden. VPN-autentiseringen er primært 3-faktor (SMS i tillegg til brukerID og passord).

		Bærum kommune er tilkoblet «kommuneversjonen» av Norsk Helsenett for kommunikasjon med tjenester.
1.7 Datasenterkommunikasjon		BK-LAN oppgraderes med ny løsning, spesifikasjonene til ny kommunikasjonsløsning for datasenter er p.t. ikke klar.
1.8 Internett	Leverandør: Telenor	Kunden leier internettforbindelse med 2 x 1Gbit kapasitet terminert i to forskjellige datasentere.
1.9 Mobil datakommunikasjon	Direkte mot Internett eller via Telenor Nordic Connect	
2.0 Serverløsninger		
2.1 Hardware	Hyperconverged infrastruktur fra Dell	
2.2 Lokal lagring på server	Virtuelle diskene i VMware	Lokalt lager på servere benyttes i hovedsak for OS og Applikasjonsinstallasjon.
2.3 Backup	HP backup-robot (backup) Veritas NetBackup og Veeam (backup og recovery programvare).	Det benyttes en policybasert backupschedule som tar full backup av fildata en gang i uken. Resterende dager benyttes en kumulativ inkrementell backup. Det gjennomføres full backup av databaser hver dag.
2.4 Virtualisering	VMware vSphere	
2.5 Identitetshåndtering og katalogtjenester	NetIQ Identity Manager Microsoft AD	Det er etablert synkronisering mot Kundens HRM-løsning som benyttes via den egenutviklede
2.6 Operativsystemer	Microsoft Windows 2016 Suse Linux Enterprise Server 12	
2.7 Filtjenester	NTFS volum på Microsoft server.	
2.8 Utskriftstjenester	Follow me Print	
2.9 Databasetjenester	Microsoft SQL Server 2014 Oracle 12	Oracle og MySQL benyttes kun på spesifikke tjenester. Hvis ønsket brukt må det dokumenteres at Microsoft SQL ikke er støttet..

2.10 Applikasjons-tjenester	Microsoft Windows 2016 Microsoft IIS 10.0 Suse Linux Enterprise Server 12 Apache/Tomcat	
2.11 Antivirus	Symantec Endpoint Protection	
2.11 TerminalServer	Windows 2012 R2 og 2016 Citrix XenApp	
2.12 Aksess-løsninger	Citrix NetScaler NetIQ Access Manager	
2.13 Overvåkning	Icinga2, CiscoPrime HP SIM EZRF Mule MMC Splunk m.fl.	
3.0 Mobile enheter		
Administrasjonsverktøy	AirWatch	
Operativsystem mobiltelefon	iOS	Siste gjeldende versjon er til enhver tid standard.
Operativsystem nettbrett	iOS	Siste gjeldende versjon er til enhver tid standard.
App-distribusjon	Apple AppStore	Hvis det leveres app i tilbudt løsning skal denne være tilgjengelig gjennom Apple App store. Applikasjon skal være utviklet etter beste praksis fra AppConfig Community
Innkjøpsmetode	Volume Purchase Program	
3.1 Klientprogramvare – Windows 10		
Operativsystem arbeidsstasjon	Microsoft Windows 10 Enterprise	
Klientadministrasjon	Microsoft System Center	
Kontorstøtteprodukter	Microsoft Office 2016 Pro Plus/Standard, Microsoft Office 365 E3/E1	Avhengig av lisensavtale. Ta kontakt hvis versjon er viktig for tilbudt løsning.
E-post	Microsoft Outlook 2016	

Nettleser	Microsoft Edge	
Antivirus	Symantec Endpoint Protection	
PDF-leser	Adobe Reader	
4.0 Fagsystemer Administrasjon		
Sak- og arkivløsning	Acos WebSak Focus	NOARK 5 kjerne Tilgjengelige grensesnitt: NOARK 4 WS, Autoarkiver WS
Integrasjon	BPM Intalio BPMS ESB Mulesoft Anyplattform	
5.0 Testmiljø		
Testmiljø etableres i henhold til spesifikasjoner ved behov.		