TRONDHEIM
KOMMUNE

Organisering og teknisk plattform

1 Innledning

1.1 Formål og overordnet beskrivelse

Dokumentet beskriver organisering, IT-prosesser, driftsmodell og realisert arkitektur av IKT tjenester i Trondheim kommune, med fokus på nåsituasjon.

Målgruppen for dokumentet er leverandører som skal levere IKT- utstyr og løsninger beskrevet i kravspesifikasjon.
Intern målgruppe er personer som jobber med anskaffelser av IT-løsninger i Trondheim kommune.

Ved spørsmål ta kontakt med: it-tjenesten.postmottak@trondheim.kommune.no

2 IT i Trondheim kommune

2.1 Omfang

For å understøtte tjenesteproduksjonen til innbyggere benyttes det et stort antall fagsystemer[1] og en rekke andre applikasjoner. Trondheim kommune har et hybrid IKT-landskap og i porteføljen er det både skyløsninger, hyllevare, legacy-systemer[2] og systemer bygd for og av Trondheim kommune.

IKT i kommunen består av et stort antall brukere og omfatter alt fra helse, undervisning, administrasjon, kartdata, byggeteknisk overvåkning, kultur og næring til publikumstjenester og deltakelse på sosiale media.

Brukergruppene er sammensatt og mangfoldig. Det er svært varierende behov, avhengig av organisasjonstilhørighet og rolle. Noen ansatte har faste kontorplasser, mens andre har høy mobilitet. Enkelte må være tilgjengelig hele tiden, mens andre kan styre tiden sin mer selv. Mange ansatte er avhengig av IKT for å få gjort jobben sin, mens andre igjen kan utføre jobben sin uten tilgang til egen PC. Noen arbeider både innendørs og utendørs.

Trondheim kommune har som mål at innbyggere og næringsliv i størst mulig grad skal ta i bruk kommunens tjenester gjennom et digitalt grensesnitt, og derfor satser mer på skytjenester iom. skytjenester har mange fleksibiliteter med tanke på nå dem. Trondheim kommunes IKT-løsninger skal understøtte tjenesteproduksjonen og tjenestens digitale dialog med innbygger og næringsliv. Målet er å minimalisere omfang av tjenester som krever lokalt installert programvare på klienter.

[1] Med fagsystem forstås IT-systemer med integrert arbeidsflyt brukt til å understøtte spesifikke arbeidsprosesser innen et fagområde typisk saksbehandlingssystem.[2] 'Legacy'-applikasjoner kan være både kjøpt og bygd men kjennetegnes av at det er applikasjoner basert på gammel/foreldet teknologi men som man fortsatt velger å bruke fordi det gir virksomheten den funksjonaliteten/prosess-støtten som det er behov for.

2.2 Ansvar og organisering

Fagområdet IKT er organisert under Kommunaldirektør for organisasjon. Kommunedirektørens fagstab har ressurser innenfor informasjonssikkerhet, IKT-strategi, Virksomhetsarkitekt og porteføljeforvaltning. IT-tjenesten har ansvar for felles IKT-tjenester.

Ansvaret for fellessystemer som sak og arkiv, er lagt til fagenheter inn under Kommunaldirektør for organisasjon.

Ansvar for fagapplikasjoner ligger til det enkelte virksomhetsområdet.

2.2.1 IT- tjenesten

IT- tjenesten har ansvaret for leveranser av IKT-tjenester blant annet infrastruktur, arbeidsstasjon, publiseringsløsning, ERP - systemer, utskrift, telefoni, pasientvarsling, stamnett (både kablet- og trådløst nett), lagring som omfatter både privat skylagring og offentlig skylagring, kontorstøtteverktøy som e-post, tekstbehandler regneark og andre basisprogram som Adobe, nettlesere osv., applikasjons- og databasedrift, serverdrift, drift og utvikling av tjenesteinovasjonsplattformen (TIP) , utvikling av webapplikasjoner, brukeradministrasjon og IT-brukerhjelp til virksomheten.

IT- tjenesten bistår også enheter og organisasjonen i forbindelse med IKT-anskaffelser og større nasjonale og regionale og ikke minst kommunes interne IT - prosjekter.

2.2.2 Tjenesteansvar

Trondheim kommune har definert to sentrale begreper: **tjenesteeier** og **tjenesteforvalter**.
Tjenesteeier har det overordnet ansvaret for tjenesten mens tjenesteforvalter har det daglige ansvaret for tjenesten.
Tjenesteforvaltere har det daglige ansvaret for fagapplikasjoner når det gjelder tilganger, feilmelding, endringer knyttet til applikasjonen, men alle henvender seg til IT-Brukerhjelp og så videresendes det til driftsleverandør hvor tjenesteforvaltere også blir involvert i spesielle tilfeller.

2.3 Driftsmodell

Trondheim kommune har siden 1992 satt ut driften av alle data- og telefonisystemer, herunder nettverk, perifert datautstyr, applikasjon, telefoni og pasientvarsling. Siden 2011 har Trondheim kommune valgt multi vendors driftsmodell hvor de fleste av IKT-tjenestedrift er outsourcet til flere leverandører.

- Kommunikasjonstjenester (intern infrastruktur) leveres av TietoEvry AS.
- Applikasjonsdrifttjenester og pasient varslingsløsninger leveres av Sopra Steria AS.
- Drift av telefoniløsningen leveres av Atea AS.
- Trafikk, abonnement og tjenester på fasttelefoni og mobiltelefoni leveres av TietoEvry AS med Telenor som underleverandør.
- Multifunksjonsmaskiner og tjenester leveres av Dustin Norway AS.
- SMART-utskriftsløsning (follow me print) driftes av Sopra Steria som en del av Utskriftstjenesten

For fagapplikasjonene er det inngått egne support- og vedlikeholdsavtaler med de ulike applikasjonsleverandørene.

Siden 2016 har Trondheim kommune valgt å insource flere IKT-tjenester for å ivareta kompetanse internt i kommunen. Dette omfatter blant annet Service Desk, TjenesteIntegrasjon Plattformen (TIP) og Brukeradministrasjon og digital arbeidsflate hvor det benyttes Microsofts modern Endpoint Management System (Intune) samt Azure Active Directory for identitetshåndtering .

Trondheim kommunen satser mer på skyløsninger og har anskaffet flere SaaS løsninger blant annet for G-Suite tjenester (Google gruppevare - og kontorstøtte), HR-Portal (Lønn/HR), Webinnsyn, saksbehandlingssystemet ServiceNow, eByggesak, Oppvekst Administrativ system (OAS), Digital Meldebok, Økonomisystem (LIFT), TQM osv. I tillegg har Trondheim kommune begynt å bruke IaaS tjenester fra Google GCP (Google Cloud PLatform) og noe fra Azure for test, POC og pilotering av tjenester.

2.4 Service desk

Trondheim kommune har siden oktober 2016 selv overtatt driften av Service Desk. Tjenesten benevnes som IT-brukerhjelp.

IT-brukerhjelp håndterer flere typer henvendelser som feilmeldinger, spørsmål, behov for veiledning, og enkelte bestillinger. IT-brukerhjelp har ansvar for videreformidling og oppfølging av feilsituasjoner mot kommunens andre tjeneste- og driftsleverandører. Alle Kundens ansatte kan kontakte IT-brukerhjelp.
Tjenesten omfatter blant annet følgende:

- Mottak, registrering, kategorisering og oppfølging av henvendelser
- Løsning av enkle feil direkte. For andre feilsituasjoner skal saken tildeles ansvarlig tjenesteleverandør
- Henvisning av feil knyttet til fagapplikasjoner til Kundens tjenesteforvaltere
- Resetting av passord
- Veiledning i bruk av endeutstyr, kontorstøtteapplikasjoner og enkelte fellesapplikasjoner
- Informasjon om IKT-tjenester samt endringer og driftsavvik knyttet til disse tjenestene
- Videreformidling av bestillinger og informasjon om bestillingsrutiner
- Configuration Management System (CMS)
- Dashboard; sammenstilling og presentasjon av data fra Kundens tjenesteleverandører og Kundens egen organisasjon ved hjelp av moderne Business Intelligence-løsninger.

I snitt er det ca. 5000 henvendelser til IT-brukerhjelp pr. måned. Henvendelsene er knyttet til IKT-tjenester i både det administrative nettet, Elevnett og ASP-tjenester. For elevene er det skolens IKT-personell som kontakter IT-brukerhjelp dersom IKT-veiledere ikke klarer å hjelpe eleven.

Brukerne som henvender seg til Service Desk har svært varierende IKT-kompetanse. Brukerne har også svært ulik grad av tilgang til og benyttelse av IKT-tjenestene.

2.5 Brukeradministrasjonstjenesten

Trondheim kommune har insourcet brukeradministrasjonstjenesten fra 1. juni 2017. Mesteparten av denne tjenesten sine oppgaver er nå automatisert, blant annet opprettelse av brukerkonto for ansatte i TKE og TKA domene, samt autoritativ kilde for innhenting av brukerdata fra Trondheim kommune sitt HR- system. Tjenesten omfatter blant annet følgende:

- Klargjøring og tildeling av tilgang til ulike interne- og skytjenester
- Manuel opprettelse av brukerkonto for en gruppe brukere som leverer tjenester til Trondheim kommune blant annet innleide konsulenter, studenter osv.
- Sletting av brukerkonto i både domene og G-Suite etter at ansettelsesforholdet er opphørt

Noen nøkkeltall

TK-nett benyttes av administrativ sektor

- 23453 aktive brukerobjekter hvorav 20675 er aktive ansattbrukere (tall pr. 11.05.22)
- 2891 stasjonære pc'er og 9610 bærbare pc'er (tall pr. 11.05.22)
- 744 nettskrivere/multifunksjonsmaskiner og 200 lokale skrivere (tall pr. 15.12.20)

Elevnett benyttes av elever i grunnskolen

- 27621 brukere (tall pr. 11.05.22)
- 17680 chromebook (tall pr. 11.05.2022)
- 123 multifunksjonsmaskiner (tall pr. 15.12.2020)
- 114 lokaler skrivere som ikke er en del av felles utskriftstjenesten.

Den sentrale delen av nettet består av fiber. Mindre enheter uten fibertilknytning, er koblet opp via ADSL/SHDSL. Få av slike samband står igjen og vil erstattes av fibersamband i løpet av 2021. Skolene er i all hovedsak tilknyttet nettet via fiber.

Kommunens telefoniløsning omfatter både (tall pr. 12.05.2022):

Navnet	Antall Helse	Antall Admin	Antall DTA	Totalt	Kommentar
Digitale terminaler	79	43		122	
Analoge terminaler	594	120		714	
Dect (Legacy)	166	563		729	Tradisjonell dect
Ip Terminaler	1873	2097	39	4009	Sip, sip dect, Ip terminaler, Romenheter sykehjem
Virtuellenummer	242	744	56	1042	Nummer som ikke har terminaler tilknyttet

Kommunen har valgt å benytte et begrenset utvalg modeller av både telefoner, PC-er og skrivere. Dette er gjort med tanke på vedlikehold og kompatibilitet.

2.6 IT Service Management

Oppfølging av IKT-drift og forvaltning hos Trondheim kommune er organisert delvis etter ITIL v.3 (IT Infrastructure Library), et internasjonalt rammeverk for IT-virksomheter. Samhandlingen mellom Trondheim kommune og kommunens tjenesteleverandører er delvis basert på denne standarden.

Fagapplikasjonsleverandører bistår sammen med tjenesteleverandørene (drift) ved feilsøking, kapasitetsvurderinger, risikovurderinger, kontinuitetsplanlegging m.m.

2.7 Administrasjon av lisenser og lisensregnskap

Trondheim kommune håndterer selv SAM (Software Asset Management) funksjonen, som innbefatter oversikt over lisenser og bruken av disse. Kunden benytter Xensam som verktøy for å detektere programvareinstallasjoner og holde oversikt over alle lisensavtaler og lisenser. Det vil være et krav om installasjon av xsearchklient på alle servere og PC-er som benyttes i produksjonen mot Kunde. Det kan gjøres unntak fra dette kravet der leverandøren har det totale ansvaret for lisensiering av maskinvare.

3 Realisert infrastruktur

3.1 IT arkitektur

Trondheim kommune har i sin IT strategi definert sentrale virksomhetsmål og IT suksessfaktorer. I forbindelse med spesifikasjon av utstyrs- og systemanskaffelser, samt inngåelse av nye IKT drift- og utviklingsavtaler er det definert et behov for å utvikle en hoved arkitektur dekkende alle IT forvaltning.

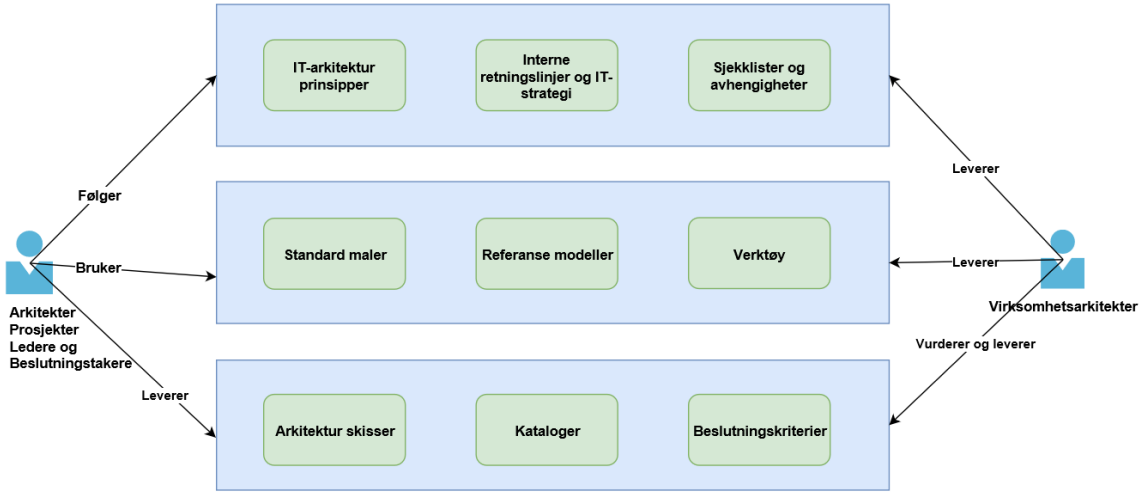
En fornuftig arkitektur er en forutsetning for en vellykket implementering av en helhetlig IT strategi. Mange private og offentlige virksomheter etablerer arkitektur på virksomhetsnivå, det vil si at arkitektur etableres mer helhetlig i virksomheten og ikke innenfor de enkelte applikasjonene som tidligere (monolittisk arkitektur). De viktigste fordelene med dette er flere synergier mellom de ulike applikasjonene, og mindre avhengigheter mellom kunde og leverandør og mer kostnadseffektiv og håndterbar integrasjon mellom applikasjoner og tjenester.

IT arkitekturen inneholder retningslinjer for hvordan nye systemer skal etableres, hvordan de skal benytte standard fellestjenester, hvordan systemer, tjenester og arbeidsprosesser skal dokumenteres og hvordan en felles driftsarkitektur skal se ut.

Trondheim kommune har en IT arkitektur som dekker følgende områder:

- Virksomhedsarkitektur som definerer forretningsprocesser.
- Teknologiarkitektur som definerer maskinvare og programvare som bygger opp under TK sin forretnings – og applikasjonsarkitektur.
- Applikasjonsarkitektur som representerer en logisk modell av systemer / tjenester som støtter opp under forretningsarkitekturen blant annet automatiserte tjenester, avhengigheter mellom ulike applikasjoner og tjenester osv..
- Informasjonsarkitektur som representerer modeller som viser hva virksomheten trenger å vite for å kunne gjennomføre prosessene og aktivitetene.
- Sikkerhetsarkitektur som setter taktiske og tekniske føringer og tiltak for realisering av gjeldende retningslinjer for informasjonssikkerhet definert i Trondheim kommune sin informasjonssikkerhetsstrategi

Skissen under viser hvordan overordnet IT arkitekturen forvaltes i Trondheim kommune.



3.2 Virtualisering

Virtualisering er preferert i realisering av servere. Det benyttes VMWare vSphere 7.
Det benyttes SAN fra HPE 3PAR Hewlett Packard Enterprise (HPE).

3.3 Server og databaser

Trondheim kommune bruker MS Server 2012 og oppover, alt nytt realiseres på MS Server 2019, Linux Red Hat, Rocky og Ubuntu samt MS SQL og Oracle databaser.

3.3.1 Applikasjonsservere

Det benyttes p.t. primært følgende applikasjonsservere:

- Intern sone: MS Windows Server 2012 R2 / 2016 R2/ 2019
- Sikret sone: MS Windows Server 2012 R2 / 2016 R2/ 2019

Terminalserver intern og sikker sone:

- Terminalserver: Citrix XenApp 7.9
- Aksesseres vha. ICA-klient /Citrix Workspace 20.10.0.20
- Trondheim kommune har innført TSPluse for å nå filtjenester via chromebook via Terminal server

3.3.2 CAG (Citrix Access Gateway) og Lastbalansering

Trondheim kommune bruker Netscaler for CAG (Citrix Access Gateway) funksjon, publisering og lastbalansering av tjenester. Det benyttes to stykker av Citrix NetScaler Mbps Enterprise Edition versjon 11.1.56.19 nc for ovennevnte formål.

3.3.3 Databaser

- Databasehotell (intern sone)
    - MSSQL
        - DB: MS SQL Server 2014 R2
        - DB: MS-SQL 2008R2
        - OS: MS Windows Server 2012 R2
    - Oracle
        - DB: Oracle PP Enterprise Edition 110g, 11c og 12c

        - OS: Red hut Enterprise Server 5.7

- Databasehotell (sikker sone)
    - MSSQL
        - DB: MS SQL Enterprise Edition Server 2014
        - OS: MS Windows Server 2012 R2
    - Oracle
        - DB: Oracle PP Enterprise Edition 110g, 11c og 12c
        - OS: Red hat Enterprise Linux Server 5.7

3.3.4 Lagringsløsninger og Backup og gjenoppretting

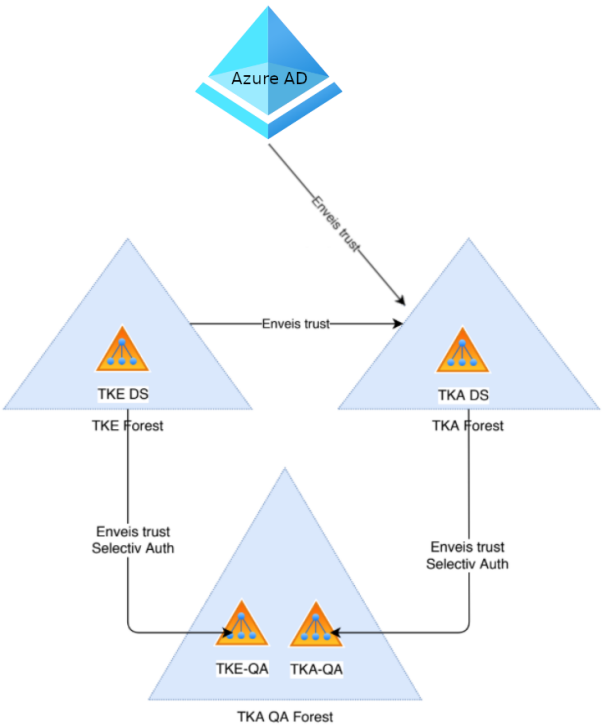
- Det benyttes SAN fra HPE 3PAR OS 3.3.1 MU1 Hewlett Packard Enterprise (HPE).
- For backup benyttes IBM sin Tivoli Storage Management system.

3.4 Katalogtjenester

For autentisering av interne brukere, og ressurser benyttes MS AD (Microsoft Active Directory) og MS AAD som kataloger. Autoritativ kilde for ansattinformasjon er Trondheim kommune sitt HR-system. Tjenester som trenger kerberosautentisering og som ligger i våre nett benytter AD, eksterne tjenester benytter i stor grad Azure AD OIDC eller SAML.

Trondheim kommune sitt nett er delt i to domener kalt TKA (Trondheim kommune Adminnett) og TKE (Trondheim kommune Elevnett) med egne forest (skog) og en trust i mellom. Det eksisterer QA for både TKA AD og TKE AD i egen forest med enveis trust fra produksjon til QA. Formålet med AD er autentisering, autorisering og brukerkatalog.

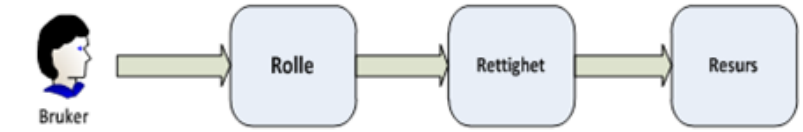
Trondheim kommune har etablert Azure AD der alle brukerobjekter synkroniseres fra on-premise AD. Skissen under viser det totale arkitekturen til on-prem AD og AAD.

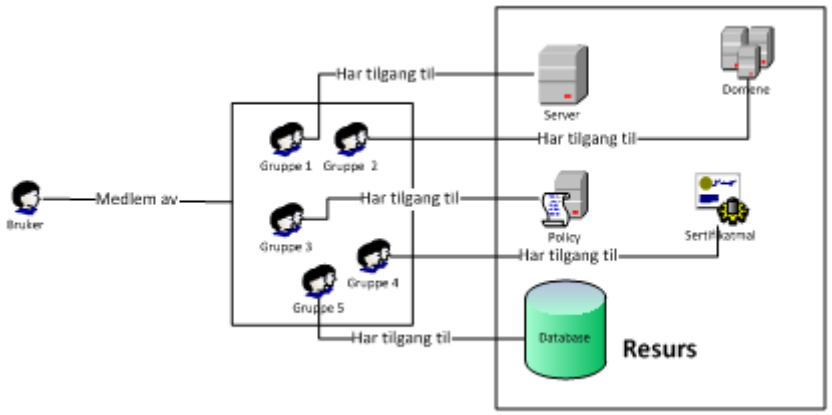


(Figur over: Kundens Microsoft Active Directory)

3.4.1 Brukerkatalog og ansattautentisering

Trondheim kommune bruker en hybrid modell av tilgangsstyring av rollebasert og medlemskap i en sikkerhetsgruppe som gir tilgang til ressurser i nettet. Dessuten benyttes det Google IdP og Azure AD,, for autentisering av brukere mot skyløsninger. Autentisering til nettet og de fleste tjenester skjer via AD ved hjelp enten LDAP eller Kerberos protokollene. Trondheim kommune har lagt til rette for at pålogging med OpenID eller SAML. Figurene under viser de to modellene Trondheim kommune benyttes.





3.4.2 SSO (Single Sign On)

Trondheim kommune bruker MS Azure Federation Services og Google IdP med både SAML eller OpenIDConnect som protokoll for autentisering for å oppnå Single Sign On (SSO).
ADFS er nylig faset ut og alle tjenester og applikasjoner som hadde vært føderert med den er migrert over til Azure AD. Sistnevnte benyttes som en standard pålogging og SSO mekanisme i Trondheim kommune.

3.5 Smartutskrifttjeneste

SMART-utskrift er utskriftsløsning TK benytter hvor man tar i bruk funksjonalitet for å få adgangskontroll på MFP-ene og også ha mulighet for å hente utskriftene på hvilken som helst skriver, (follow-me-print/pull-print). TK bruker PaperCut løsning til dette formålet. Formålet med denne tjenesten er å sikre at utskrift ikke komme uvedkommende i hende samt å imøtekomme lovpålagte krav fra datatilsynet. Det er også krav om 2-faktor autentisering for utskrifter. Dette er realisert med krav om PIN i tillegg til RFID-kort for de brukerne som har tilgang til sikre applikasjoner.

3.6 Tjeneste Innovasjonsplattform (TIP)

Tjeneste InnovasjonsPlattformen (TIP) er en tjeneste og integrasjonsplattform laget av og for Trondheim kommune med smidig metodikk og moderne teknologi. Plattformen er primært basert på åpen kildekode med Golang som rammeverk. Tjenesten kan også levere tilpassede APIer etter behovet. Det kan også lages en integrasjon hvor data mappes mellom de forskjellige systemene før

det sendes videre. Tjenesten kan ta imot og sende data på alle mulige formater, men det foretrekkes at det så ofte som mulig blir brukt JSON format.

Alle APIer som eksponeres på TIP er beskyttet. Hvilken autentisering som brukes varierer, men det stilles strenge krav til sikkerhet.

Denne tjenesten er i stadig videreutvikling av utviklingsavdelingen. Utviklingsavdelingen har kjørt et lengre prosjekt sammen med arkitekturavdelingen for å se på moderniseringsalternativ for plattformen. I prosjektet ble det benyttet industristandard åpen kildekode-tjenester som blant annet Kubernetes. Dette prosjektet ga gode resultater, og IT-Tjenesten er i prosess med å realisere moderniseringen av plattformen. Dette innebærer å bygge plattformen på ny – på Kubernetes – i en offentlig skyplattform, for så å flytte applikasjonene én og én til ny plattform.

Tjenesten har innebygd overvåkning, sikkerhet, logging tjenester, og overvåkes 24/7 av utviklingsavdelingen.

3.7 Endeutstyr

3.7.1 Arbeidsflate

Arbeidsflate innbefatter tradisjonelle PC-produkter som Windows maskiner, Chromebooks, nettbrett, smart-devices og mobiltelefoner. Som en del av modernisering av tjenester og plattformen har Trondheim kommune innført Chromebook som er et arbeidsverktøy og nå betraktes den som et fullverdig arbeidsverktøy hvor ansatte kan utføre sine digitale arbeidsoppgaver ved de fleste virksomhetsområdene. Målet er å minimalisere omfang av tjenester som krever lokalt installert programvare på klienter, dvs at som hovedregel så skal web grensesnitt benyttes gjennom nettleser. Målsetningen er at for fremtiden skal fagprogramvare i størst utstrekning være platformuavhengige.

Windows maskiner:

- 12580 MS Windows 10 Professional

Smart-devices:

- 8851

Chrome enheter

- Chrome enheter for møterom 116
- Chromebook i admin nett 281
- I skolesektor er det innført chromebook (17680).

Nettbrett

- Apple iOS

Mobiltelefoner

- Android
- Apple iOS

3.8 Basisprogram og ASP-løsninger

3.8.1 Gruppevare

- Google Workspace (e-post, chat, Meet, kalender, Current , kontorstøtteverktøy og m.m.)

3.8.2 Kontorstøtte

- Google Workspace er innført i Trondheim kommune og brukes primært som kontorstøtteverktøy som Team-disk, Google Drive og dens tilhørende tjenester.
- Lokalt installert Word og Excel 2016 kun for enkelte ansatte med dokumentert tjenestelig behov. Siste kartlegging tilsa 550 ansatte med et slikt dokumentert behov. Behovet ansees å minske etter hvert som flere fagsystemer blir skybaserte og fagsystemer tar over som verktøy for relevant tekstproduksjon.

3.8.3 Nettleser

- Google Chrome med standardoppsettet og SSO basert på SAML og OIDC fra MS Azure AD og Google IdP for enkelte tjenester
- Edge også er tilgjengelig og kan benyttes av brukere.
- Andre nettlesere installeres av den enkelte bruker fra programvaresenter som gir tilgang til godkjente programmer

3.8.4 ASP (Application Service Provider) løsninger

Trondheim kommune satser mer på skyløsninger i det siste grunnet mer modenhet i nevnte løsninger. ASP-løsninger er skyløsninger Trondheim kommune har satset på å bruke siden 2014 blant annet HR-systemet Bluegarden, E-byggesak, TK-Arkiv, ServiceNow, LIFT, TQM, CIM, Helseplattformen, Modulus Barn og diverse kartløsninger osv.

3.8.4.1 Lønn og HR-system Bluegarden

Trondheim kommune har innført lønn og HR-system fra Visma med innebygd webcruiter som driftes av vår applikasjonsleverandør Visma. Systemet har mange moduler med ulike funksjonaliteter blant annet timeføring med innebygd arbeidsmiljøloven. Systemet har all ansatt informasjon, enhetsinformasjon som brukes av andre konsuments systemer eksempelvis Trondheim kommunes Active Directory for automatisk opprettelse av brukerkontoer i domenet og intranett og kommuneweb for publisering og dermed regnes som en master kilde.

3.9 Kommunikasjon

3.9.1 Stamnett

Telenor er leverandør av to 10 Gbps internettlinjer med basis innholdsfiltrering og DDoS beskyttelse i Trondheim. Internettlinjene leveres på to steder inn til kommunens kjernenett for å ivareta geografisk redundans.

Stamnett består av kjernenett og kantnett. TietoEVRY pr. i dag har driftsansvaret for Trondheim kommunes nettverksinfrastruktur og kommunikasjonstjenester slik som:

- Stamnettets infrastrukturkomponenter som brannvegger, rutere, switcher, kontrollere og gatewayer og nettets administrasjonsverktøy som HP IMC, Prime, PRTG osv.
- Stamnettets oppbygging med kjernenett, kantnett, segmenter og virtuelle nett/soner
- Sentral Internettilgang, NIX
- Sikkerhetsløsninger som IPS, IDS, Web Filtrering og videresending av logger til SOC-tjenesten
- Proaktiv overvåkning og tilrettelegging for å sikre trafikk-kvalitet med QoS (Quality of Services) etablert i kjernenettet
- Forvaltning og videreutvikling av Stamnettets fibersamband, xDSL samband og radiolink
- Administrasjon av IP-range av både private ipv4-adresser og offentlige ipv4- og ipv6 adresser

Nettverksinfrastrukturen baseres på en kjerne som rutes dynamisk på lag 3 og kant som switches på

lag 2. Nettverket er delt inn i ulike soner og presenteres på kantswitchene som VLAN. Soner i kjernenettet er etablert som egne rutede nettverk. Dette innebærer at hver lag-3 switch er konfigurert med en VRF for hver sone.

Lokasjoner hos Trondheim kommune er knyttet sammen med ulike forbindelser. Det benyttes xDSL, leide digitale linjer og leide dedikerte fiberforbindelser. Unntaksvis benyttes private fiberlinjer.

3.9.2 IP adresse plan

Trondheim kommune forvalter sine egne offentlige og private ip-adresser.

3.9.2.1 Private IP-adresse rom

For intern kommunikasjon mellom klient og server bruker Trondheim kommune private adresse rom, og for å forvalte disse adressene har TK etablert DNS tjeneste som kjører i DC. I tillegg har TK DHCP tjeneste som allokerer en dynamisk ip-adresse til en ressurs ved forespørsel fra ressursen.

3.9.2.2 Offentlige IP-adresse rom

Trondheim kommune har blitt medlem av RIPE NCC som står for Reseaux IP Europeans (RIPE) Network Coordination Center (NCC). RIPE NCC først og fremst allokerer offentlige ip-adresser av både versjon 4 (IPv4) og versjon 6 (IPv6) samt tildeler AS nummer (Autonomous system number). Med medlemskap i RIPE NCC kan en eie egne IPv4 adresser og IPv6 adresser. Trondheim kommune forvalter sine egne offentlige IP-adresser. For mer informasjon se (her).

3.10 Telefoni

3.10.1 Mobiltelefoner og nettbrett

Det er foreløpig ingen standardisering når det gjelder operativsystem for mobiltelefoner og nettbrett. Sikkerhetsutvalgets retningslinjer legger føringer på hva som kan/ikke kan benyttes.

Det stilles krav om at utstyret kan understøttes av styringssystem for mobilt utstyr (MDM) som gir mulighet for fjernstyring av devicer blant annet fjernsletting, låsing og sporing.

- Microsoft Endpoint Management benyttes pt. som styringssystem for felles mobilt utstyr.
- Google MDM brukes som styringssystem for de aller fleste personlige mobile utstyr.
- Flere miljøer benytter applikasjoner på nettbrett (med og uten SIM-kort) i sin daglige drift (Bydrift, skole, barnehager).
- Hjemmesykepleien og Trygghetspatruljen benytter mobiltelefoner (XRover) for tilgang til journal/ arbeidslister (Helseplattformen).
- Ambulerende legevakt benytter PC for mobil tilgang til Helseplattformen.
- Sikkerhetsnivåer benyttet i Trondheim kommune via mobile utstyr
    - SN02, Enkelte interne tjenester med brukernavn og passord
    - SN03, Fagapplikasjoner, e-post og kontorpakke og alle ASP-tjenester føderert med enten Azure AD eller Google IdP
    - SN04, sikkert tilgang, blant annet YubiKey med fido nøkler med eIDAS høy
    -

3.10.2 Sentral autentiserings- og autorisasjonsløsning i nettverket

Cisco ISE (Identity Services Engine) er plattformen som håndterer Trondheim kommune sin definerte sikkerhetspolicy, automatiserer aksess-kontroll og nettverkstilgang basert på roller. Cisco ISE (Identity Services Engine) er den sentrale komponenten for identitetshåndtering og tilgangskontroll. ISE håndterer en definert

sikkerhetspolicy. I dag har TK versjon 2.6 av Cisco ISE. Cisco ISE støtter seg på Microsoft AD som er kommunens sentral katalogtjeneste for både ansatte og elever i sine respektive domener (TKA og TKE)

Tilgang til kjernesvitsjer autentiseres og autoriseres gjennom ISE, og Kunden ønsker å videreføre dette regimet for kantsvitsjer.

3.10.3 Mobil Data Aksess - MDA

For å knytte trafikk fra mobile enheter i Telenors mobilnettverk inn til Trondheim Kommune/driftsleverandørens datasenter benyttes tjenesten Mobil Data Aksess (MDA). Det er satt opp to adskilte MDA for henholdsvis sikker sone og intern sone (Gemini) som kan evt. benyttes av applikasjoner i respektive soner. Det er strenge tilgang restriksjoner fra sikker sone ut mot internett.

3.10.4 Fasttelefoni

Trondheim **kommunens telefoniløsning omfatter både tradisjonell** fasttelefoni med 1768 fasttelefoner og 5513 IP-telefoner. Trondheim kommune knyttes til det offentlige telefonnettet og har en dedikert 10 000 nummerserie, 72 54 xx xx. Det benyttes fem siste siffer for å ringe internt, også fra mobiltelefon.

Trondheim kommune benytter trådbundet telefonapparat (analog-, digital- og IP-tilknytning) og DECT (digital- og IP-basert).

Trondheim kommunes løsning for fasttelefoni består av tre etablerte telefoniservere, en for helse og en for administrative enheter, samt en egen redundant løsning for Helsevakta.

Alle telefoner er enten knyttet direkte til, eller gjennom noder (LIM) til en av de to sentrale telefonserverne.

Nettverket benyttes til signalisering og programvarevedlikehold, samt som bærer for intern IP-telefoni.

3.10.5 Pasientvarsling

Trondheim kommune sin drift av helsehus og helse- og velferdssentre benytter pasientvarsling til å understøtte sin drift.

Dette er etablert i alle helsehus, helse- og velferdssenter og noen bo- og aktivitetstilbud. Trondheim kommune gjennomfører en oppgradering av sine løsninger, og de fleste lokasjoner har i dag Centrak Elpas. Løsningen er distribuert med egne lokale servere per lokasjon, som sikrer fortsatt drift ved sambandsbrudd på nettverket. Løsningen er integrert med SIP-dect (telefoni) og brannvarsling. Erstatning av SIP-dect med smarttelefoner er under uttesting.

Løsningen benytter LF for dørstyring og lokalisering, IR for lokalisering, og RF for lokalisering og dekning, og kombinerer de forskjellige teknologiene for å gi funksjonalitet i løsningen.

Det er etablert et sentralisert system for logg og statistikk.

4 Sikkerhet

Kommunens datanett er under kontinuerlig utvikling for å møte virksomhetenes behov og lovpålagte

krav.

4.1 Public Key Infrastructure (PKI)

I moderne plattformer der sikkerhet er sentralt brukes sertifikattjenester i plattformene. Trondheim kommune har innført to ulike sertifikat strukturer; en offentlig struktur (Buypass), og en intern, MS Windows Server-basert struktur. Den interne delen utsteder internt SSL sertifikat for å sikre kommunikasjon internt i nettet, klientsertifikat for at klienten autentisere seg til trådløst nettet og serversertifikat for at servere autentisere seg til nettverket. Offentlig struktur delen benyttes for å utstede personsertifikat til de ansatte som har tjenstlig behov.

4.2 Kundens sikkerhetspolicy

Trondheim kommune har utarbeidet en Informasjonssikkerhetsstrategi som beskriver mål, retningslinjer og tiltak knyttet til dette arbeidet. Denne skal benyttes som styringsdokument for all behandling av informasjonssikkerhet i kommunen, og skal tas opp til revisjon årlig ved "ledelsens gjennomgang" av kommunens informasjonssikkerhet.

4.3 sikkerhetsnivå

Trondheim kommune behandler all type informasjon fra åpen til mer kritisk og personsensitive i sine systemer. Det er lagt til rette for alle fire sikkerhetsnivåer men det benytte ikke SN01.

4.4 Datahaller

Driftsleverandøren har ansvaret for datahaller (inkl. adgangskontroll og overvåkning). Hoved datahallene er i Oslo regionen, som leveres av Digiplex og Baseform , men noen servere og tjenester kjører i en tredje datahall i Trondheim, og alle disse er fysisk sikret. Adgang til datahallene gis etter behov og det er kun autorisert personell som kommer inn i en datahall.

Alle datahaller er teknisk sikret mot brann, vanninntrenging, utfall av krafttilførsel og overoppheting. Datahaller ligger lokalisert utenfor risikoområder for flom, ras og kvikkleira (naturkatastrofer) med dagens driftsleverandøren.

Datahaller har redundante løsninger for strøm, kjøling og kjerneinfrastruktur med separate føringsveier inn til datasentrene. Datahaller er sikret med løsning for nødstrøm med jevnlig test av dieselaggregatet.

Primær datasenteret har en klassifisering tilsvarende Tier III og sekundær datasenteret er bygd etter krav til Tier III.

4.5 Autorisering

Kunden har egne rutiner for brukerautorisering av brukere til nettverket, filområder på nettverksstasjoner og tilgang til fellessystemer og fagapplikasjoner.

4.6 Autentisering

For adgang til kommunens administrative nett på intern eller sikker sone skal PC eller annet mobilt IKT- utstyr være innkjøpt, forvaltet og konfigurert av IT-tjenesten eller godkjent leverandør. Program- og maskinvare - plattformer benyttet i Kundens informasjonssystem skal være standardisert. Utstyret skal være merket, og ha unik identitet som er sporbart mot hvilken bruker som har fått utstyret utlevert. Det er ikke tillatt for andre enn IT-tjenesten eller godkjent leverandør å installere annen programvare eller endre konfigurasjon.

Pålogging til kommunens utstyr og nett krever identifisering av bruker ved brukerident og passord/PIN, hvor det også benyttes Windows Hello i det utstyret som har støttet for.

Brukeren autentiseres mot Azure Active Directory (AD) ved innlogging på arbeidsstasjon. Det benyttes unikt User Principle Name (UPN) som er lik e-post adressen til vedkommende og passord .

I admin nettet har bærbare PC-er diskkryptering.

I en del av de serverbaserte fagapplikasjonene må brukere autentisere seg med unikt brukernavn og passord før de kan ta i bruk applikasjonen. Sikkerheten som benyttes i de ulike fagapplikasjoner er ulik og leverandør spesifikk.

Med eksterne brukere menes brukere som ikke er tilkoblet TKxLAN, trådbasert nettverk. Eksterne brukere med tilgang til interne ressurser som ikke er tilgjengelig fra internett benytter VPN med Azure pålogging for å koble til TK-nettet.

Trondheim kommune har etablert en lokal FEIDE autentiseringstjeneste i skolesektoren.

Trondheim kommune har etablert føderasjon mot ID-porten for pålogging og autentisering mot flere ulike fagsystemer.

4.7 Soner

Trondheim kommune følger Datatilsynets sonemodell. For å kunne begrense trafikk mellom sonene er det implementert de VRF'er på lag3 som det er behov for.

Trondheim kommune har 3 forskjellige sonetyper:

- *Sikret sone* der det behandles personsensitive opplysninger. Hver enkelte sikrede sone er adskilt fra det interne nettverket og andre sikrede soner.
- *Intern sone* der det behandles ikke-sensitive personopplysninger. Det kan også gjelde andre virksomhetskritiske informasjon som ikke bør eksponeres utenfor virksomheten.
- *Ekstern sone* der åpen informasjon og internettbaserte tjenester skal stå, dette også kalles for DMZ (demilitarisert) sone, noe som isolere tjenester og styre trafikk mellom soner ved hjelp av teknisk utstyr. Det kan også omfatte lukket DMZ-soner der trafikk åpnes mot andre tjeneste- og applikasjonsleverandører basert på IP-adresse.

Hver sone/VRF har hver sin dedikerte OSPF-prosess. Per dags dato eksisterer det ca. 50 OSPF-prosesser i nettet. Ruting mellom sonene skjer kun via brannmur. Ruting mellom brannmurer skjer via sone/VRF TK Transport og er dynamisk ruting. PAVA- anlegg har en dedikert VRF.

I sikret sone for fagapplikasjoner og databaser står terminalservere, fagapplikasjonservere, filservere og databaseservere som behandler og lagrer informasjon som krever ekstra sikring i forbindelse med konfidensialitet, integritet og tilgjengelighet. Det er ingen arbeidsstasjoner i denne sonen. Terminalserverfarmen er delt inn i adresseområder som representerer de ulike fagapplikasjonene i sonen. Dette er grunnlaget for differensiert tilgang fra de ulike arbeidsstasjoner. Sonen er kun terminert i datarom.
I sone for sikrede arbeidsstasjoner befinner brukere som skal ha tilgang til de ulike sikrede fagapplikasjoner. Kun arbeidsstasjoner på disse sonene kan nå fagapplikasjonservere i sikret sone. Arbeidsstasjonene i disse sonene autentiserer seg mot katalogtjenesten i intern sone, og bruker ressurser i intern sone på samme måte som andre arbeidsstasjons ressurser i intern sone. Arbeidsstasjonene kan kjøre distribuerte applikasjoner fra sikret sone.

4.8 Sikkerhetsbarrierer

Alle brannmurer er som standard satt opp til å blokkere all trafikk. Den trafikk som skal tillates må defineres i brannmurregler.

All aktivitet gjennom alle brannmurer registreres i dag i logger på egen loggserver. Ordinær tilgang til Internett via http-proxy logges internt i proxy-server. Logging av andre tillatte tjenester mot eksterne nett logges i FW.

Det er etablert eksterne tilganger for ulike behov. Løsningene baseres på Cisco VPN, Citrix Access Gateway og Mobil Data Access (MDA). Autentiseringsløsninger for eksterne tilganger er basert på RADIUS, Azure basert autentisering VPN og MDA/SIM/abonnement.

Trondheim kommune har to brannmur klynger Internett-FW, og inter-server der sistnevnte håndterer trafikk mellom servere.

Trondheim kommune har innført Check Point Quantum 28000 Security Gateway som inkluderer både IPS og IDS.

Alle loggene fra brannmurtjenestene videresendes til den sentralisert SOC-tjenesten Trondheim kommune har kjøpt.

4.9 Sentral Security Operation Center (SOC-tjeneste)

SOC-tjenesten leveres gjennom applikasjonsdriftsavtalen.
Det benyttes sensorer som er plassert ut i kommunens nettverk som overvåker all trafikk mot internett passivt. Data fra sensorene analyseres hos Sopra Steria sin SOC tjenesten og gir varslinger som sendes til Sopra Sterias sikkerhetssenter (SOC). Sopra Steria sammenstiller hendelsene med egne kilder og andre loggdata levert for analyse. Varsler videresendes til avtalte mottakere i kommunen eller deres tjenesteleverandører av de tjenestene som blir berørt.

5 Sentrale systemer i Trondheim kommune

Noen sentrale system i Trondheim kommune

System	Navn	Ver.	Leverandør	Kommentar
Økonomi- og regnskapssystem	LIFT (Løsning for Innkjøp, Finans i Trondheim kommune)	m7	EVRY	ERP løsning Unit4 Business World fra EVRY er nylig innført i Trondheim kommune.
Lønnssystem	Bluegarden	2.0	Bluegarden	Lønn og HR system i produksjon fra april 2014
Rekrutteringsstøtte	Webcruiter		Webcruiter	Leveres gjennom Bluegarden fra 2014. Løsningen er autoritativ kilde for ansatt- og enhetsinformasjon i Trondheim kommune.
Tidregistrering	GAT		Gatsoft	
Sak og arkivsystem	ESA - sak og arkiv	8.0.4.1	EVRY	

Arkivløsning	TK-Arkiv	1.0	Documaster	
Publiseringsløsning (CMS) –	React	Versjon 16.6.0 - 16.8.3	React (fri kildekode)	Benyttes som rammeverk for Trondheim kommunes hjemmesider. Er fri kildekode
Publiseringsløsning (CMS)	CMS Flyt		Prokom	Fri kildekode CMS utviklet i Java. Benyttes som rammeverk for kommunens nettsider
Helsevakt	Transmed8		Locus/Cerner	Løsning for Legevakt og Trygghetspatrulje, i drift fra oktober 2015
Elektronisk pasientjournal	Helseplattformen	1.0	Helseplattformen AS	Benyttes i kommunens helse og velferdstjenester , kommunale Legevakt/Helsevakt og Skolehelsetjenester
Telefoni	Mitel MX-One	6.3	Mitel	Call Manager, IP-telefoni
TIP	Trondheim kommune Innovasjonsplattform		Utviklet av Trondheim kommune	Egenutviklet plattform basert på åpne standarder og moderne teknologier
GSE	Google Suite For Education		Google	Løsning innen skole/utdannings området
GSE for EVO	Google Suite For Education		Google	Løsning innen skole/utdannings området for Enhet for Voksenopplæring under domene trovo.no
Google Workspace	Google Workspace		Google	Gruppevare og kontorstøtte
ServiceNow	ServiceNow		Symfoni/Sopra Steria	Service desk system for flere miljø som drifter IT system i kommunen (innført våren 2016)