

Rammeavtalen Bilag 9

Kundens tekniske plattform

Pust- og bevegelsessensor (PBS)

Arkivreferanse anskaffelse: SAK 25/317160

Arkivreferanse kontrakt: SAK xx/xxxxx

Leverandør: [navn leverandør]

Innholdsfortegnelse

1.	Innledning.....	3
2.	Generell beskrivelse av Politiets IT-infrastruktur	3
2.1.	Plattform og datasentre.....	3
2.2.	Tilgangsstyring	3
2.3.	Arbeidsflater og enheter	3
2.4.	Servere	4
2.5.	Lagring	4
2.6.	E-post	4
2.7.	Utskrift	4
2.8.	Integrasjoner.....	4
2.9.	Databaseplattform.....	5
2.10.	Applikasjonsplattformen	5
2.11.	Metrikker	5
2.12.	Applikasjonslogg	5
2.13.	Kryptering av kommunikasjon.....	5
2.14.	Sentral sporingsløsning	5
2.15.	Infrastruktur	5

1. Innledning

Bilag 9 inneholder en beskrivelse av kundens nåværende infrastruktur, plattform, programvare og de systemer Leverandørens leveranse skal samvirke med og eventuelt integreres mot.

2. Generell beskrivelse av Politiets IT-infrastruktur

Bilaget beskriver Politiets infrastruktur og klientplattform pr i dag som løsningen skal samspille med.

2.1. Plattform og datasentre

Kundens IT-infrastruktur er basert på en sentralisert modell hvor datakraften håndteres av flere gjensidig redundante datasentre som driftes av Politiets IKT-tjenester.

Kundens tjenestesteder er tilknyttet datasentrene via et lukket og kryptert fjernnettverk (WAN). I WAN'et er båndbredden til de enkelte tjenestestedene fastsatt av oppgavetyper og antall medarbeidere. Den enkelte løsning kan ikke forvente at hele kapasiteten er tilgjengelig til sitt formål.

For å sikre kommunikasjon mellom systemer benyttes allment anerkjente krypteringsmekanismer. På forespørsel kan aksepterte cipher suites oppgis fra politiet.

Det er etablert en sentral overvåkningsløsning basert på DX UIM, som benyttes til å monitorere helsetilstanden til de ulike løsningene til Kunden. Løsningen er basert på bruk av agenter som installeres sammen med de ulike løsningene, og monitorerer aktuelle prosesser. Løsningen forutsetter at systemet er installert i PIT sin infrastruktur.

Politiet benytter seg i tillegg av flere mindre støttesystemer for overvåking og monitorering som er open source og interoperabelt med det meste av moderne teknologi.

Det gis ikke permanent eller selvstendig fjerntilgang til politiets nettverk uten ytterligere avtale. Slik tilgang kan ikke forutsettes innvilget.

2.2. Tilgangsstyring

Kunden benytter Active Directory for å håndtere tilgangskontroll til IT-infrastrukturen og fagapplikasjoner.

Kunden benytter i tillegg Microsoft multifaktor for pålogging.

Kunden benytter Identity Manager fra One Identity for å håndtere tildeling av tilganger til IT-infrastrukturen og fagapplikasjoner via grupper i Active Directory on-premise og Entra ID i sky. Gruppene tildelt brukere kan presenteres via token fra Open ID Connect.

For brukere som må provisjoneres inn i løsningen (utover AD og Entra ID) bør dette skje automatisk basert på OIDC påloggingen. Alternativt kan det skje via et SCIM API som Identity Manager kaller.

Kunden benytter i tillegg Microsoft multifaktor for pålogging.

2.3. Arbeidsflater og enheter

Politiets sentrale arbeidsflate leveres via en on-prem terminalserverløsning basert på Citrix Virtual Apps and desktops. Denne leverer en skrivebordsflate til brukere basert på Microsoft Windows operativsystem. Profiler og brukerinnstillinger administreres med Citrix Workspace Environment Manager. Applikasjonsvirtualisering foretrekkes på applikasjoner som må installeres direkte i terminalserverimaget. Det er ingen åpen

tilgang til internett fra den sentrale arbeidsflaten. Tilgang til internett går via en separat Citrix publisert applikasjon.

Nettleser som benyttes i terminalserverløsningen er Microsoft Edge og Google Chrome (norskspråklig versjon for begge). Microsoft Office benyttes som kontorstøtteløsning.

Sluttbrukerne når politiets arbeidsflater gjennom politieide enheter. For stasjonære og bærbare pc'er (Windows, macOS) er disse administrert via Microsoft Intune. Det er ingen direkte tilgang fra operativsystemet lokalt på disse enhetene inn til den sentrale arbeidsflaten, og politiets sentrale nettverk.

Arbeidsflatene i Politiet er i endring. Det jobbes med å gjøre flere applikasjoner tilgjengelig direkte på enhetene ved hjelp av moderne tilgangsløsninger. Virtuelle arbeidsflater i sky er også teknologi som vurderes tas i bruk.

Mobile enheter, som mobiltelefon og nettbrett (Android/iOS), er pr i dag administrert via politiets mobile plattform (EMM) Citrix XenMobile, på sikt vil disse enhetene også legges over i Microsoft Intune.

Applikasjoner for mobile enheter, kan både være egenutviklet av politiet, og levert av 3. parts leverandører. Applikasjoner for mobile enheter (Android/iOS) installeres, administreres og styres via politiets mobile plattform, og integreres med mobilplattformens SDK.

Leverandører må forholde seg til politiets til enhver tid prefererte mobilplattform dersom tjenesten skal leveres på politiets mobile enheter.

2.4. Servere

Øvrige servere for fagsystem og tjenester er i dag installert på virtuelle servere, med operativsystemene Windows Server, Redhat eller Ubuntu Linux. Vi benytter kun utgaver av operativsystem som er innenfor ordinær support fra leverandør.

Alle servere er tilknyttet et høykapasitets lagringsnettverk eller objektlagring.

2.5. Lagring

All fillagring, felles filområder og lignende leveres av en dedikert nettverkstilknyttet filserverløsning (NAS) fra NetApp.

2.6. E-post

Politiet benytter i dag Microsoft Exchange Server som eposttjener.

2.7. Utskrift

Politiet benytter seg av multifunksjonsmaskiner levert av Canon. Alle multifunksjonsskrivere er satt opp med embedded sikker utskrift og skanning. Sikker utskrift består av ca.1700 maskiner. Primært står maskinene On-Prem i politinettet, men det er en del maskiner som står tilkoblet sikker utskrift i en hybrid løsning der multifunksjonsmaskiner og/eller klienter er tilkoblet utenfor politinettet opp mot sky-løsning. Politiet har i tillegg et større antall (ca.500stk) skrivere satt opp i kjøbasert direkte print-løsning i politinettet On-Prem.

2.8. Integrasjoner

For integrasjon mot eksterne løsninger utenfor politinettet, kan både synkron og asynkron meldingsutveksling benyttes. For asynkron så er dette kun når det initieres innenfra. For innkommende skal det være en synkron front.

Den foretrukne integrasjonsmetoden er løse koblinger mot Apache Kafka eller RESTful API med OIDC/OAUTH2 autentisering.

For integrasjon mot interne løsninger (innenfor politinettet), kan både synkron og asynkron meldingsutveksling benyttes. Integrasjonene er basert på bruk av Webservices med REST. Der det utveksles større mengder data benyttes asynkron, for oppslag er det typisk REST.

Vi benytter Apache Kafka som distribuert strømme- og meldingsutvekslingsplattform i dag.

2.9. Databaseplattform

Microsoft SQL Server Enterprise Edition er databaseplattformen som benyttes. Alle installasjoner settes opp med AlwaysOn.

Andre databaseplattformer kan vurderes, etter kundens godkjenning.

Installasjoner med stand-alone aksepteres ikke.

2.10. Applikasjonsplattformen

Orkestreringsløsningen som benyttes til applikasjonsplattformen er Kubernetes, og applikasjoner skal leveres som OCI-container(e). Container(e) må kunne kjøres frakoblet internett. Det støttes kun baseimages på Linux. Baseimages må passere intern sårbarhetsskanning. Forutsetter at systemet er installert i PIT sin infrastruktur.

2.11. Metrikker

Kunden bruker Prometheus for innsamling av metrikker og Grafana for visualisering av metrikker.

2.12. Applikasjonslogg

Kunden bruker ELK stack for innsamling og visualisering av logger.

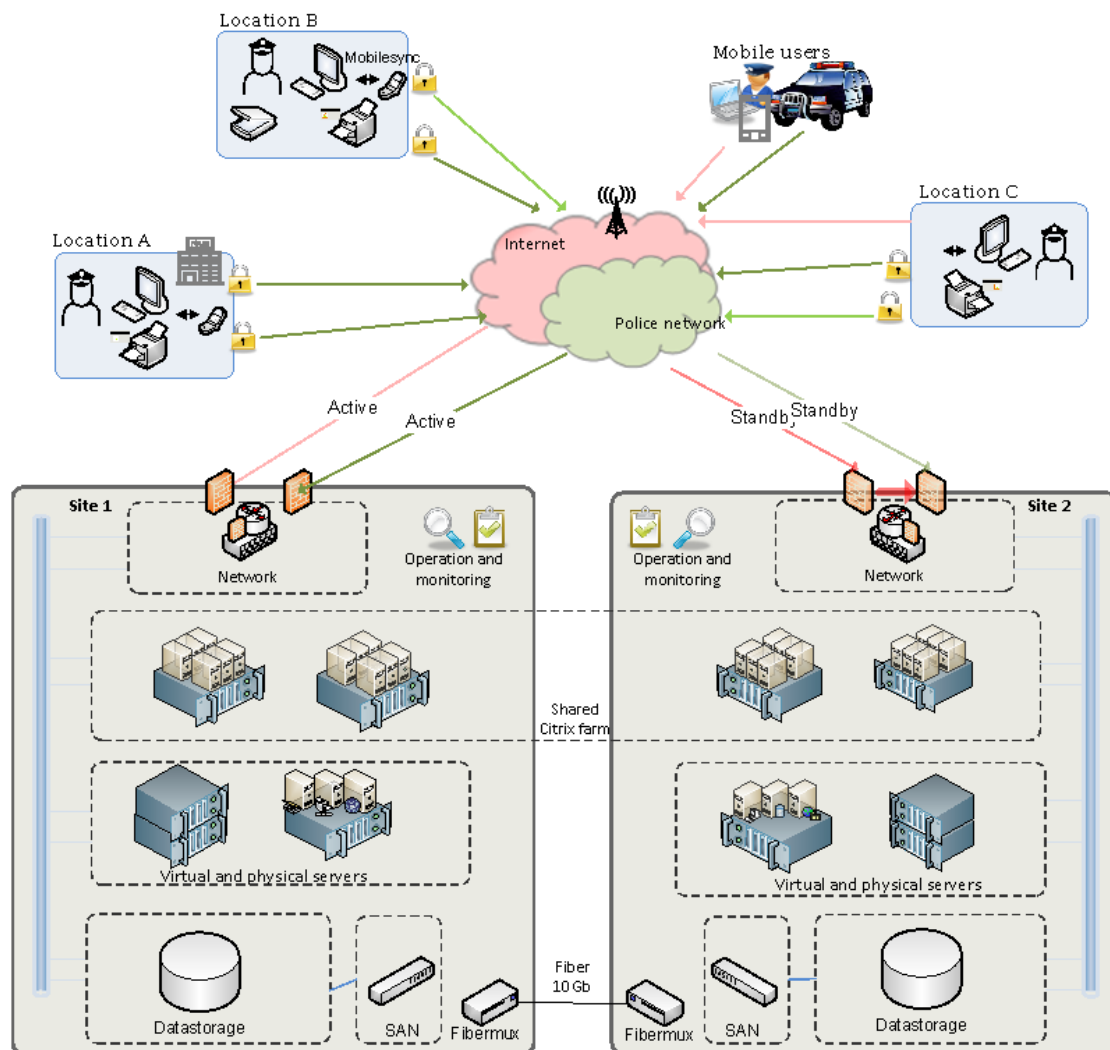
2.13. Kryptering av kommunikasjon

Kryptering er påkrevd for all utveksling av data mellom systemer. Alle applikasjoner skal støtte både å motta og sende kryptert trafikk. Versjon av protokoll og cipher suite må ses i sammenheng med informasjonen som skal beskyttes. Protokollversjoner og cipher suites som er allment anerkjent som for svake skal ikke benyttes, disse kan oppgis på forespørsel.

2.14. Sentral sporingsløsning

Kunden er gjennom Politiregisterloven (PRL) pålagt å spore hvilken bruker som utførte en gitt handling på et gitt tidspunkt knyttet til personopplysninger. Som følge av dette er det etablert en sentral sporingsløsning som overvåker bruken av de enkelte løsningene. I tillegg er det definert en sporingskontrakt som sier hva den enkelte løsning skal kunne levere til sporingsløsningen. Applikasjoner som omfattes av lovverket integreres med sentralsporingsløsning via et API og innsamling av informasjon gjøres ved bruk av agenter som overvåker trafikken inn og ut av en applikasjon. Forutsetter at systemet er installert i PIT sin infrastruktur.

2.15. Infrastruktur



Figur 1 - Figuren viser prinsipiell oppbygging av Kundens infrastruktur