FORSVARSBYGG

Vedlegg 7

Faglig oppdragsbeskrivelse

1 OM LEVERANSENE

1.1 Generelt om leveransen

Forsvarsbygg overtok forvaltningen av boliger og kvarter (hybler) til Forsvarets ansatte i 2015. Totalt forvalter Forsvarsbygg ca. 1800 boliger og 6000 kvarter (spredt på om lag 300 bygg) på ulike lokasjoner i Norge. Disse leies i hovedsak ut til Forsvarets ansatte for kortere eller lengre perioder.

I forbindelse med forvaltningsoverføringen overtok Forsvarsbygg IKT-infrastrukturen fra Forsvaret. Siden 2015 har Forsvarsbygg byttet ut rekke støttesystemer hvor en rekke manuelle arbeidsprosesser er erstattet med automatiserte løsninger. I tillegg har endringene bidratt til bedre brukeropplevelser og tilgjengelighet 24/7 for Forsvarets ansatte. Nedenfor beskrives de ulike delprosjektene:

Basen: Forsvarsbygg har utviklet en internettbasert selvbetjeningsportal «Basen» (www.forsvarsbygg.no/basen). Basen er bygd opp i moduler og hver modul tar for seg en type funksjonalitet/tjenester. Dette er front end mot brukere i Forsvaret. Basen er under stadig utvikling med tanke på å levere ulike tjenester mot brukerne og er integrert mot flere av FBs støttesystemer mht. korttids og langtidsleie.

Bookingsystem for korttidsleie: Det er anskaffet et komplett booking- og administreringssystem for hoteller (VisBook) med integrasjon mot Basen, Invite og Xpand. Det vil si at VisBook administrerer informasjon om ledige rom, priser, belegg, sengeplasser og status. Gjesten bestiller og betaler for overnattingen på Basen og ordren kommer automatisk inn i VisBook for videre behandling av bolig- og kvarter forvalter i Forsvarsbygg (BOK-forvalter).

Xpand: Per i dag benyttes Xpand som system mht. kontrakts forvaltning, befaringer etc. Xpand er integrert mot Basen, VisBook og via Biztalk til Invite (e-lås flåtestyring). Xpand skal på sikt byttes ut (trolig innen 2025) og Forsvarsbygg er i prosess mht. å anskaffe et nytt system for langtidsleie. Et nytt system, skal på samme måte som Xpand, integreres mot Basen, slik at kontrakts informasjon om leietaker blant annet kan leses rett inn i Xpand og legge til rette for digital signatur, digital nøkkelhåndtering etc.

Digital nøkkelhåndtering (e-Lås): Nøkkeladministrasjon er en aktivitet som må foretas hver gang en overnattingsgjest ankommer eller forlater et forlegningsbygg eller hvor et blir inngått en leiekontrakt med en beboer som skal bo i en bolig eller kvarter. Nøkkeladministrasjon opptar mye av bolig- og kvarterforvalterens tidsbruk.

Forsvarsbygg har derfor erstattet dagens helmanuelle nøkkeladministrasjon ved utleie av kvarter ved å automatisere aktivitetene tilknyttet nøkkelhåndtering ved å anskaffe et låssystem/flåtestyringsverktøy (Invite) inkludert låser og tilleggsutstyr som er integrert med Basen, VisBook og Xpand gjennom Biztalk.

På korttidsovernatting fungerer løsningen slik at gjesten bestiller overnatting i Basen og får tildelt rom. I forkant av ankomst til lokasjonen får gjesten beskjed om at rommet er klart og at de kan låse opp døren med app eller pinkode. På avreisedato sjekker gjesten selv ut og belastes for overnatting på sitt kort. Den digitale nøkkelen eller pinkoden fungerer kun i tidsrommet for selve bestillingen.

På langtidsleie fungerer løsningen slik at beboer søker og får tildelt en bolig eller kvarter i Basen. Leietaker skriver under på sin leiekontrakt digitalt. Ved innflytting får beboer en sms med pin kode til døren eller at de kan låse seg inn via app. Den digitale nøkkelen er kun gyldig i leieperioden.

Invite er Forsvarsbyggs flåtestyringsverktøy mht. nøkkeladministrasjon. Systemet er levert av selskapet Intin og har spesialisert seg på å levere smarthusteknologi. Forsvarsbygg benytter seg av Invite til å automatisere utlevering av nøkler samt flåtestyring (oversiktsbilde over låsene) inkludert fjernstyring og «helsesjekk» på låsene. Systemet benyttes av bolig- og kvarterforvaltere i Forsvarsbygg og Servicesenteret.

1.2 Formål med anskaffelsen

Formålet med anskaffelsen er å dekke Forsvarsbyggs behov for kjøp og support, service og vedlikehold av elektroniske/digitale låser inkludert evt tilleggsutstyr som må til for å dekke kravspesifikasjon.

Alt utstyr skal kunne integreres med Basen og Invite som flåtestyringsverktøy knyttet til e-lås.

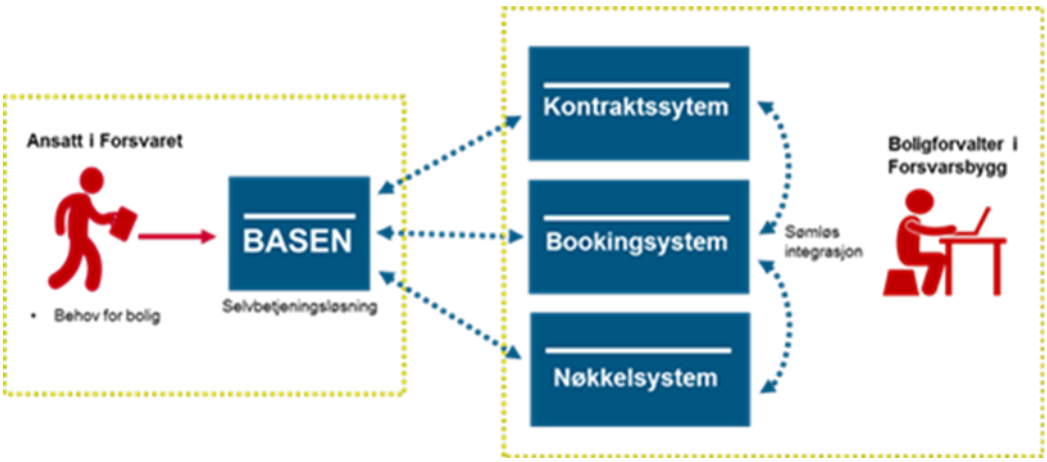
I tillegg må en fremtidig leverandør ivareta behovet Forsvarsbygg har for support, service og vedlikehold av eksisterende låspark (Danalock). Se prisskjema for informasjon om hvilke lokasjoner det er etablert e-lås.

Det er ikke aktuelt å gå tilbake til produksjon av nøkkelkort eller nøkkelbrikker. Løsningen er og skal være heldigital.

Det er viktig for Forsvarsbygg at leverandør har utstyr og personell som kan benyttes innenfor og utenfor leir.

Leverandøren skal levere både installasjon, drift, support, vedlikehold, feilretting og bytte av låser i hele levetiden til låsen med mulighet for integrasjon med Forsvarsbyggs systemer.

Rammeavtalen skal dekke behov mht etablering av e-lås på lokasjoner hvor dette ikke er i dag. Per i dag gjelder dette følgende lokasjoner; Rena, Setermoen, Kuhaugen, Wallemsviken, Ørland, Linderud, Værnes og Kirkenes. Totalt er det snakk om ca 3500 låser inkludert tilleggsutstyr og smarthuber. Leverandøren vil også måtte levere ekstra låser til bygg på lokasjoner hvor vi har e-lås i dag (nybygg e.l.). I tillegg er det aktuelt å etablere e-lås på ca 1800 boliger, samt nye bygg som kommer inn i porteføljen ila avtaleperioden.



Krav til lås:

Må kunne støtte en eller flere av følgende former for å åpne og låse en lås:

- mobiltelefon og bluetooth-låser med BLE-teknologi
- mobiltelefon og NFC-teknologi
- kode/kodepanel (Låsen skal kunne motta kode gjennom vårt helintegrerte flåtestyringssystem som bruker smarthuber.)
- Fysisk nøkkel

Primærløsning vil være online låser som støtter radiokommunikasjon (BLE-teknologi/NFC-teknologi),pin kode og app. Det skal være mulig å benytte fysisk nøkkel til å åpne døren.

Låser:

Leverandøren skal tilby låser som kan integreres med flåtestyringssystem (Invite) som Forsvarsbygg har i dag.

På de lokasjoner hvor det allerede er installert Danalock forventes det at leverandør tilbyr smarthuber eller annen teknologi som kan integreres mot eksisterende installerte base av låser, kodepanel og Invite flåtestyringssystem.

I takt med den teknologiske utviklingen i markedet er det en fordel om låser/tilleggsutstyr kan integreres mot Forsvarsbygg sine SD-anlegg i tillegg til at de tilbys som en del av smart hus løsninger og andre styringssystemer for port åpnere, lys og strøm som er utviklet for boliger og andre bygg.

1.3 Målgrupper og brukerroller av låser i låssystemet

Målgruppevalget for låssystemet er gitt av dagens utgangspunkt i brukerbehov, kjente utfordringer i målgruppene og et ønske om størst mulig effekt av digitale låser.

Hovedmålgruppene for låsene og låssystemet er leietakere, overnattingsgjester, bolig- og kvarterforvalter, driftspersonell, renhold, superbrukere og administratorer.

Gruppene er:

Overnattingsgjester og leietakere

Overnattingsgjester er forsvarsansatte og andre kunder som er gitt muligheten for å kunne bruke Forsvarsbyggs tilbud om overnatting ved egne fasiliteter ved landets forskjellige militærleirer (arenaer).

Leietakere er ansatte (inkludert deres familier) i Forsvaret som tildeles bolig eller kvarter (hybel) etter en søknadsprosess hvor tildelingen besluttes av Forsvaret. Leieperioden varierer, men strekker seg stort sett fra ett til tre år.

Bolig- og kvarterforvalter (Overnattingsstedet)

Bolig- og kvarterforvaltere er forvaltere av både overnattingsrom ved eksempelvis en militærleir, men også av enkeltstående boliger og hybler (kvarter) som tildeles forsvarsansatte for en lengre periode. Overnattingsrom kan benyttes både av korttids- og langtidsgjester.

Superbrukere (Servicesenter)

Superbrukere er ansatte ved Forsvarsbyggs Servicesenter og enkelte Bolig- og kvarterforvaltere i regionene som ved behov skal kunne tre inn og støtte det enkelte overnattingssted. Superbrukere skal derfor ha rettigheter til å utføre alle oppgaver den enkelte Bolig- og kvarterforvalter har tilgang til i alle regioner/lokasjoner.

Driftspersonell og renhold (Forsvarsbygg og eksterne)

Driftspersonell er ansatte ved Forsvarsbyggs driftsavdelinger og renhold er ansatte hos renholdsleverandør med avtale. Renhold vil på sikt overføres tilbake til Forsvarsbygg og utføres av egne ansatte. Driftspersonell og renhold skal ha tilganger til en eller flere leire og flere bygg.

Admin brukere

Admin brukere er ansatte i Forsvarsbygg som skal ha tilganger til å opprette brukere, tilgangsstyring og administrere systemet. De skal også ved behov skal kunne tre inn og støtte det enkelte overnattingssted. Admin brukere skal derfor ha rettigheter til å utføre alle oppgaver den enkelte Bolig- og kvarterforvalter har tilgang til.

2 Krav til leveransen

Ved utfylling av kravtabellene vil de enkelte kravene være merket med kravkategori. Kravkategorier og prioritet gir Forsvarsbygg viktig informasjon, slik at de kan prioritere de ulike kravene og at de vil bli brukt i forbindelse med vurdering og vekting av tilbudene.

Kolonnen «Nr.»: Angir rekkefølgen på de ulike kravene

Kolonnen «Kategori»: Kravene vektes etter hvor viktig de er for at løsningen skal fungere

Kravkategori	Betydning av kravkode
A	Absolutt krav. Dersom kravet ikke oppfylles, vil hele tilbudet bli avvist
B	Kravet er avgjørende og svaret vil gi en score og være en del av vektingen. Denne type krav vil kreve en beskrivelse fra tilbyder. Dersom flere B krav er utilfredsstillende besvart, kan tilbudet bli vurdert å ikke oppfylle forespørselens intensjoner. Dette kan da medføre at tilbudet avvises. Score fra 0 til 10
C	Kravet er ikke avgjørende for at vi skal få realisert løsningen, men gir løsningen en økt nytteverdi. Score fra 0 til 7

Kolonnen «Beskrivelse»: Angir beskrivelsen av kravet Forsvarsbygg stiller til leverandør

Kolonnen «Svar»: Her skal leverandør svare i henhold til oppsettet nedenfor

Svarkode	Betydning av kode
J	JA, kravet vil tilfredsstilles
N	NEI, kravet vil ikke tilfredsstilles
F	FORBEHOLD, her skal det beskrives hva forbeholdet består av og hvilke konsekvenser dette har i kolonnen «Besvarelse / Ref.».

Hvis leverandør angir «F» på noen av kravene er det viktig at løsningen beskrives på en slik måte at Forsvarsbygg kan identifisere og vurdere konsekvensene på en god måte.

Hvis leverandør ikke oppfyller et B krav med dagens løsning kan han tilby å utvikle funksjonaliteten for å dekke kravet. Det må i så fall spesifiseres når funksjonaliteten er klar for Forsvarsbygg å ta i bruk og om det krever tilpasninger når utviklet løsning er ferdig.

Der besvarelse ikke kan begrenses til en celle i tabellen, kan info legges til som vedlegg med henvisning til aktuelt kravnummer.

Kolonnen «instruks og krav til besvarelse»: Her skal det besvares på hvordan tilbudt løsning dekker krav der svarkolonne er bekreftet med «J»/«F», eller refereres til dokumentasjon/løsningsbeskrivelse hvor svaret utdypes ytterligere. Hvis leverandør ønsker å benytte vedlegg som annen dokumentasjon for besvarelse er det særdeles viktig at det henvises til korrekt referanse i forespørsel.

Til en del av tabellene er det også tatt inn en formålsbeskrivelse. Disse gir viktige føringer for løsning på/håndtering av tilhørende krav.

Leverandøren skal til hver av tabellene også vurdere om det kan tilbys annen form for løsning som støtter opp under formålet, men som ikke eksplisitt er stilt opp som et krav. Dette kommenteres særskilt.

Ved besvarelse er det viktig at det påpekes om funksjonalitet dekkes av 3. parts løsning, og at dette tas med som en del av kostnadsbilde i forbindelse med innkjøp, implementering og drift.

2.1 Generelle krav

Nr.	Kategori	Beskrivelse
1	A	**Kvalitetskrav** Låser i skallsikringen som f. eks ytterdører skal være FG-godkjent klasse 3.
2	A	**Kvalitetskrav** Tilbyder skal ikke operere med bindingstid på tilbudte produkter/løsninger som løper ut over rammeavtalens varighet.
3	B	**Kvalitetskrav** Det er en fordel om eksisterende låskasser og sylindere i størst mulig grad kan gjenbrukes sammen med ny digital lås. Leverandør må beskrive alternativ(e) løsning(er) og beskrive hva disse er og hvordan de vil fungere.
4	B	**Kvalitetskrav** Leverandøren må kunne tilby online funksjonalitet som en del av denne avtale. Ved hub/gateway basert løsning er det en fordel om hub kan strømforsynes via nettverkskabel (PoE)
5	B	**Bruker tilgang** De forskjellige brukerne i FB må kunne ha tilgang til lås systemet for å lage f. eks midlertidige tilganger til rom ved bruk av PIN koder eller digitale nøkler ol. Beskriv hvordan brukerne har tilgang til låssystemet og hvilke primære funksjoner som støttes. Gi informasjon om det er behov for å installere klient-programvare på PC-er lokalt på overnattingssted eller om det tilbys web basert brukergrensesnitt.

6	A	**Teknisk løsning** - **back up løsning** Det skal være mulig for BOK forvalter og servicesenter å gi tilgang til rom ifm. avvikshåndtering. Beskrive de vanligste feilsituasjoner som kan oppstå enten på system eller lås inkludert back up løsning til leverandøren og hvordan avvik kan håndteres. Eks: bruker kommer ikke inn på rommet med mobiltelefonen eller nøkkel. Beskriv hvordan tilgang til lås der batteri er defekt vil løses.
7	A	**Skalerbarheta** Låsene inkludert tilleggsutstyr, huber og integrasjonen som tilbys må kunne skaleres til ett stort antall lokasjoner og dører. Totalt sett har Forsvarsbygg om lag 6000 kvarter, 256 kasernerom (flersengsrom) og 1800 boliger som tilbys leietakere og overnattingsgjester.
8	B	**Skalerbarhet** Hva gjelder drifts- og renholdspersonell så skal de gjerne ha tilgang til en rekke bygg og dører. Løsningen som tilbys må være brukervennlig slik at man lett får korrekt type tilgang/digital nøkkel Leverandøren bes beskrive sin løsning mht enkel tildeling og bruk av digitalnøkler for denne type brukergrupper.
9	B	**Robusthet** Totalt sett har Forsvarsbygg om lag 6000 kvarter, 256 kasernerom (flersengsrom) og 1800 boliger som tilbys leietakere og overnattingsgjester. Det er ikke alle steder Forsvarsbygg har bemanning. Lokasjonen fjernstyres derfor fra andre lokasjoner. I tillegg ankommer det personell i Forsvaret til alle døgnets tider. Det er derfor et stort behov for en robust løsning. Leverandøren bes beskrive hvordan robusthet er ivaretatt og om noen hensyn må tas.
10	B	**Robusthet** Løsningen som tilbys må være robust mht høysesong (perioden juni til august for eks). I perioder er det mye personell som flytter inn og ut av hybler, boliger m.m. Løsningen (låser med tilleggsutstyr og huber) må kunne håndtere samtidighet mht utsendelse av pinkoder, digitale nøkler samtidig som forrige nøkkel skal deaktiveres på korrekt tidspunkt. Leverandøren bes beskrive hvordan robusthet er ivaretatt og om noen hensyn må tas.
11	B	**Geografisk tilgjengelighet** Eksisterende låspark og tilbudte låser, tilleggsutstyr og smarthuber skal kunne installeres, vedlikeholdes og supporteres på Forsvarets lokasjoner over hele landet. Beskriv eventuelle begrensninger på leveransemuligheter i Norge.

12	A	**Sikkerhet nøkkeltildeling** Overføring av data mellom systemer skal være kryptert. Beskriv hvordan sikkerhetsløsning for overføring/tildeling av digital nøkkel og kode til mobiltelefon håndteres. Hvilken grad og type av kryptering benyttes for kommunikasjon. Beskriv krav til internettkommunikasjon for nøkkel-database og integrasjonsløsning. Beskriv også hvor evt servere tilknyttet låssystem eller tilleggsutstyr for lås kjøres geografisk.
13	A	**Master-Key** Løsning må ha mulighet til å utstede Master-Key der man kan skreddersy hvilken tilgang en slik Master-key skal kunne ha, i tillegg til fysisk systemnøkkel.
14	B	**Låsforvaltning** Leverandøren må kostnadsfritt tilby informasjon som for eksempel serienummer eller annen ID knyttet til låsen, tilleggsutstyr og huber som er nødvendig mht Invite flåtestyring. Hvis låsene kommer med sitt eget system, så må leverandøren beskrive hvordan systemet fungerer og spesielt integrasjonen med Invite, slik at Forsvarsbygg kan holde kontroll på hvilke låser som står på hvilke dører med tanke på å gi riktig tilgang til riktige punkter. Navn på lås og talltastatur må kunne endres ihht Forsvarsbygg sin standard.
15	B	**Mobile brukerløsninger** Det forutsettes at låssystemet også kan fullverdig betjenes på mobile flater som nettbrett og mobil. Leverandøren bes beskrive hvordan dette utføres.
16	B	**Tilgangsstyring/rettighetsstyring servicepersonell** Låsene og tilhørende system skal støtte ulike brukertyper som Forsvarsbygg har definert og ha funksjon for tilgangsstyring av nøkler integrert via Invite, samt med mulighet til å gi servicepersonell rettigheter etter behov. Administratorer, superbrukere, BOK-forvaltere, renholds- og driftspersonell må kunne gis tilgang til et sett definerte låser. Dette må kunne administreres enten ved å gi disse tilganger til grupper i områder eller til enkelt låser innen områder. Beskriv hvilke inndelingsmåter eller strukturer systemet støtter. Disse tilgangene, enten gjennom mobiltelefon eller alternativ løsning, må kunne styres sentralt, fra region og fra lokasjon i forhold til tilgangspunkter, varighet, tidsrom i døgnet, dager i uken.
17	B	**Tilgangsmatriser** Låsene skal bidra til å sikre at en gjest har tilgang til flere rom med en digitalnøkkel og/eller PIN kode gjennom integrasjon med Invite. F.eks. Hoveddør i forlegning, overnattingsrom, messe og øvrige fellesrom. Leverandøren må beskrive hvilke muligheter som finnes.

18	A	**Tidsstyring** Låsene som tilbys må støtte tidsstyringen via Invite for brukere når disse skal ha tilgang til å aksessere låser enten i områder med flere lokasjoner eller enkelt låser. For eks: Fra dato XX kl 14:00 – dato YY kl. 09:00
19	A	**Funksjon mobil** Løsningen skal støtte bruk av mobiltelefon. Beskriv hvordan mobil interagerer med selve låsen ved bruk av trådløs kommunikasjon for å åpne låsen? Er det krav til avstand for å åpne låsen? Vil lås fungere kun ved berøring ved åpning med mobiltelefon? Er det andre måter en gjest kan motta informasjon på f. eks mobil eller e-post som gir tilgang til å åpne lås(er).
20	B	**Mobilstøtte** Tilbudt lås system med tilhørende software må kunne støtte alle typer Android og iOS telefoner. Hvis det er unntak beskriv hvilke versjoner som støttes.
21	B	**Trådløs versjon** Låssystemet skal støtte trådløs overføring av lås tilgangsinformasjon til mobiltelefon, samt opplåsing og låsing fra mobil. Beskriv hvilken trådløs teknologi og versjon som benyttes i løsning, eksempelvis BLE, NFC, Zwave e.l.
22	A	**Online styring** Det skal være mulighet å fjernstyre aktivering av låser gjennom integrasjonen med Invite. Beskriv hvilke muligheter man har for fjernstyring og aktivering av låsen gjennom Invite og medfølgende system. Beskriv hvilken mulighet man har til å styre låser i bygg fra sentralt sted, f.eks. Servicesenteret.
23	C	**Varslingsanlegg** Låssystemet må også kunne integreres må også kunne integreres mot ulike SD anlegg. Løsningen bør kunne integreres med brannvarsling slik at ved evt brann låses samtlige dører opp og blir oppe. Det bør kunne separeres på byggnivå på lokasjonen. Hvordan løses dette i tilbudt løsning.
24	B	**Rapporteringsmuligheter** Det må kunne tas ut rapporter fra låser og tilleggsutstyr: Innlogging/utlogging Opplåsing av dør/gjenlåsing av dør Feilslåtte forsøk

		Feil/brudd/nedetid Mulighet for egendefinerte rapporter Hvor lang tid logges data Hvor hyppig logges data Mulighet for eksport av loggdata, formater som støttes og lignende Beskriv hvilke rapporteringsmuligheter som finnes.

2.2 Krav til teknisk installasjon og låser inkludert tilleggsutstyr og huber

Nr.	Kategori	Beskrivelse
1	A	**Kvalitetskrav** Tilbudt løsning skal fungere med skandinavisk dørblad og låstype. Dersom det er dørblader eller låser som leverandørens produkter ikke støtter må dette beskrives.
2	B	**Kvalitetskrav** Låser må kunne installeres på alle typer dører på boliger/kvarter. Forsvarsbygg disponerer ett stort antall bygg med høy variasjon av type dører. Hvilke minstekrav stiller låssystemene til dør og dørkarm for installasjon? Beskriv hvis det er avvik/utfordringer knyttet til installasjon.
3	B	**Kvalitetskrav** Låser, tilleggsutstyr og huber fra leverandøren skal fungere både på kvarter (hybler), soldatforlegninger (flersengsrom) og enkeltstående boliger utenfor leir. Beskriv hvilke låsprodukter med tilleggsutstyr og huber som tilbys for de ulike boalternativene og bruksmåter.
4	C	**Kalibrering** Lås skal kunne kalibreres både via app og mekanisk Leverandøren bes beskrive hvordan låsen kan kalibreres via ulike metoder.
5	A	**Kvalitetskrav** Låser må kunne åpnes og låses med digital nøkkel/app via blåtann eller NFC, PIN kode, og fysisk nøkkel (systemnøkkel). Sluttbruker skal kunne se status på sin dør/lås, låse opp og låse døren via app uansett hvor man befinner seg (fjernstyring av lås). Leverandør må tilby alternativ(e) løsning(er) for tilgang. Beskriv hva disse er og hvordan de vil fungere.

		Hvilke alternative løsninger har man for låsing av dør? Smekklås, aktiv låsing med app, tastatur og systemnøkkel, etc.
6	B	**Kvalitetskrav** Leverandør skal beskrive kvaliteten på låsene inkludert tilleggsutstyr (talltastatur) og huber. Hvordan er tilbudte låssystemer (låser inkludert tilleggsutstyr) sikret mot brann, høy varme, vann, støv, slag/vibrasjon etc. Beskriv også hvordan lås og evt tilleggsutstyr kan skjermes/sikres mot hærverk.
7	B	**Kvalitetskrav** Beskriv hvordan låser og tilleggsutstyr påvirkes av kulde og frost, eksempelvis for ytterdører til boliger og inngangsdører til kvarter fra svalgang eller friskluft. Beskriv løsning for hvordan Forsvarsbygg kan benytte låssystem og eventuell alternativ lås eller tilleggsutstyr som gjør det mulig å bruke elås på lokasjoner med kuldeperioder og svalgangbygg (eksempel Skjold) hvor man i perioder kan ha kulde ned til minus 30 - 40. Har for eksempel leverandøren tilleggsutstyr som skjermer og/eller varmer opp kodepanelet i ekstreme kuldeperioder? Det er ønskelig at leverandøren kan tilby ulike låser for ytterdør mht kuldetoleranse. Leverandøren bes oppgi hvor mange kuldegrader låsen inkludert tilleggsutstyret er garantert for.
8	A	**Kvalitetskrav** Leverandør skal oppgi levetid og garanti på tilbudte låser inkludert tilleggsutstyr og huber. Beskriv estimert levetid og garanti. Hvis forskjellige komponenter har forskjellig levetid og garanti bes dette å spesifiseres for hver komponent.
9	A	**Kvalitetskrav** Enkelte fellesdører vil ha høy trafikk av beboere og egner seg derfor ikke for batteridrift. Leverandør må tilby løsning for f.eks magnetlås, UMV e.l. som kan styres på samme måte som øvrige dører. Beskriv typer som tilbys og hvilke krav som stilles for at dette skal fungere.
10	B	**Kvalitetskrav** Låsene, samt tilleggsutstyr bør være motstandsdyktig mot Electro Magnetic Pulse (EMP) Leverandøren bes beskrive i hvilken grad er tilbudte låssystemer motstandsdyktig mot Electro Magnetic Pulse (EMP).
11	A	**Kvalitetskrav** Låsen skal ha tilbakerømmingsfunksjon (brannsikkerhet). Beskriv hvordan løsningen tilrettelegger for dette. Finnes det mulighet til å forsinke automatisk låsing av dør? Kan disse varieres fra lokasjon til lokasjon og individuelt fra dør til dør?

12	B	**Kvalitetskrav** Låsen og låssytemet skal gi mulighet for å sikre at rommet ikke forlates ulåst. Leverandøren bes beskrive hvordan lås eller systemet håndterer dette? Vil f. eks bruker varsles? Kan sluttbruker sjekke status i app?
13	B	**Kvalitetskrav** Låsene skal kunne varsle om lavt batteri, samt logge dette inn til Invite med varsling om at batteri må byttes.
14	B	**Kvalitetskrav** Leverandør skal oppgi levetid for batteriet i låsene. Beskriv estimert hyppighet for behov av utskifting av batteri på låser, samt eventuell endring av dette ved kaldere klima. Gjerne basert på antatt antall låseoperasjoner i døgnet eller i batteriets levetid.
15	B	**Kvalitetskrav** Det må være enkelt å bytte batterier. Beskriv hvordan utskifting av batteri i låser utføres, og hvorvidt dette kan utføres av driftspersonell og Bolig- og kvarterforvalter i Forsvarsbygg, eller krever autorisert servicepersonell fra leverandør.
16	A	**Kvalitetskrav** I dagens løsning benyttes det smarthub for styring av lås og kommunikasjon mellom lås og Invite. Leverandøren må kunne tilby smarthub som en del av denne avtale. Leverandøren må også beskrive hvordan disse installeres og integreres mot Invite og mot lås.
17	B	**Kvalitetskrav** På en del av Forsvarets lokasjoner er det ikke velfungerende internettlinjer. På en del av Forsvarets lokasjoner er det ikke velfungerende internettlinjer. Leverandøren må derfor kunne løse online funksjonalitet via en 4G/5G løsning. Leverandøren må også beskrive hvordan disse installeres
18	A	**Kvalitetskrav** Det må påregnes noe utskiftning av låskasser, sylindere, beslag etc for å få god nok kvalitet på total installasjonen. Leverandøren må kunne tilby dette som en del av leveransen etter behov.

19	B	**Vedlikehold og service** Leverandør skal oppgi vedlikeholds- og serviceoppgaver for låsene. Enkelte lokasjoner er langt unna, noe som medfører reisetid for en evt reparatør. Det er derfor ønskelig at Forsvarsbygg skal ha mulighet til å kunne foreta «nødhjelp» selv. Beskriv hvilke vedlikeholds- og serviceoppgaver som kan utføres av Bolig- og kvarterforvalter og Forsvarsbygg driftspersonell, samt hvilke oppgaver som krever bistand fra autorisert leverandør. F.eks. bytte batteri, kalibrering av lås, synkronisering lås, uthenting av loggdata, utskifting av defekt lås, aktivering av ny lås.
20	B	**Dokumentasjon** Leverandøren skal levere FDV dokumentasjon for Låser inkludert kodepanel samt tilleggsutstyr og kabling. Dokumentasjonen skal inkludere beskrivelse av låser inkludert tilleggsutstyr, kabling, hvilke låser som er tilknyttet hvilken Smarthub etc. Leverandøren skal gi eksempler på dokumentasjon Forsvarsbygg vil motta på installasjoner låser, låssystemer, oppsett, service og vedlikehold, samt opplæringsmateriell. Beskriv opplæringen av Forsvarsbygg sitt personell og eventuelt underleverandør på fagsystemer til Forsvarsbygg ved installasjon av lås system og integrasjon. Beskriv prosedyre for integrasjon mellom tilbudte låser og Invite.

2.3 Krav til SLA, tilgjengelighet og beredskap

Tilbyder skal tilby SLA. Leverandør må redegjøre for sin løsning for brukerstøtte (telefonsupport m.m., åpningstider, generell beskrivelse av løsningen). Hvis leverandøren garanterer svar innenfor gitte frister, skal dette fremgå.

Leverandørs tilbudte SLA skal vedlegges tilbudet.

Kunden skal melde feil uten ugrunnet opphold. Leverandøren skal bistå med feilsøking og med å rette feilen innenfor de rammer som er definert i dette avsnitt. Dersom avtalte frister ikke overholdes, kan Forsvarsbygg kreve standardisert kompensasjon.

Hvis ikke annet er angitt skal hendelser relatert til tjenester og produkter som omfattes av denne avtale, og som er rapportert til leverandørens Servicedesk, håndteres i henhold til tabeller under:

Reaksjonstidene vil bli drøftet i forhandlingene og tabellene nedenfor blir revidert for endelig tilbud. Leverandøren bes komme med forslag på kompensasjonsordning ved avvik.

Gjentatte avvik fra dette anses som vesentlig mislighold.

2.3.1 SLA krav

2.3.1.1 Tabell 1 krav til servicenivå programvare

Kategori	Reaksjonstider Basis periode 1 (0700 – 1700)	Reaksjonstider Basis periode 2 (1700 – 0700)	Definisjon og eksempler	Leverandørens feilrettingsarbeid
Kritisk	Så snart som mulig og innen 30 minutter.	Så snart som mulig og senest innen 30 minutter til vakttelefon.	Hele eller vesentlige deler tjenesten er utilgjengelig. Feil som medfører at tjenesten stopper, at data går tapt, eller at andre funksjoner som etter en objektiv vurdering er kritiske for Kunden, ikke virker som avtalt.	Løpende inntil feilen er utbedret evt. inntil en tilfredsstillende midlertidig løsning er etablert.
A (Høy)	Så snart som mulig og senest innen 2 timer.	Senest innen 4 timer.	Enkelte kritiske funksjoner kan ikke utføres.	Inntil feilen er utbedret.
B (Middels)	Innen 8 timer	n/a	Enkelte funksjoner kan ikke utføres eller gir feil resultat.	Inntil feilen er utbedret.
C (Lav)	Neste virkedag	n/a	Feil med lite omfang eller konsekvens for kundens daglige bruk av tjenestene/produktene.	Etter nærmere avtale med kunden

2.3.1.2 Tabell 2 SLA krav brukerstøtte og support

Kategori	Reaksjonstider Basis periode 1 (0700 – 1700)	Mål om løsningstid	Leverandørens feilrettingsarbeid
Support- saker på telefon eller chat	Brukerstøtte skal starte snarest mulig og innen 4 timer.	Etter nærmere avtale med kunden	Dersom det viser seg å være en feil, skal Kunden melde det inn i feilrapporteringssystemet
Support- saker på web eller e-post	Brukerstøtte skal starte snarest mulig og innen 8 timer.	Etter nærmere avtale med kunden	Dersom det viser seg å være en feil, skal Kunden melde det inn i feilrapporteringssystemet

2.3.1.3 Tabell 3 låser, tilleggsutstyr og lokal infrastruktur, dokumentasjon

Ref tabellens punkt 1A og 1B forbeholder Forsvarsbygg seg retten til å velge mellom de to ulike variantene per lokasjon.

Nr.	Beskrivelse	Tilbyder svarer Ja, Nei eller beskriver
1A	**Vedlikehold og service** Tilbyder skal gjennomføre årlig korrektivt vedlikehold. Dette inkluderer generelt vedlikehold av låskasse, sylinder, elektronisk lås, tilleggsutstyr, batteriskift, utsendelse av reserve låser, tilleggsutstyr, samt bytte av defekte låser, tilleggsutstyr og huber. Alle lokasjoner skal ha reserve låser inkludert tilleggsutstyr, og det skal automatisk ettersendes nye når reserveutstyr er benyttet etc. Utrykning utover årlig korrektivt vedlikehold i situasjoner som krever dette (inkludert evt nødvendig utskiftning av utstyr). All inclusive modell. Leverandør skal beskrive metodikk og rutine for kvalitetssikring av at årlig vedlikehold/service er gjennomført (f.eks. ved at QR kode scannes på den enkelte dør). Leverandør skal spesifisere hva som er inkludert i årlig korrektivt service/vedlikehold og om dette gir utvidede garantier for eksempel livstidsgaranti på låsen inkludert utstyr.	
1B	**Vedlikehold og service** Løpende utsendelse av ekstralåser og tilleggsutstyr for de lokasjoner som velger å bytte lås og ekstrautstyr selv (utover de årlige vedlikeholdsrundene). Leverandøren må tilby nødvendig support for kalibrering av og innlegging av lås i smart hub, samt evt nødvending registrering av kode. Leverandør skal spesifisere hva som er inkludert, samt beskrive en rutine for dette.	
2	**Vedlikehold og service** Leverandør skal oppgi vedlikeholds- og serviceoppgaver for låsene. Enkelte lokasjoner er langt unna, noe som medfører reisetid for en evt reparatør. Det er derfor ønskelig at Forsvarsbygg skal ha mulighet til å kunne foreta «nødhjelp» selv. Beskriv hvilke vedlikeholds- og serviceoppgaver som kan utføres av Bolig- og kvarterforvalter og Forsvarsbygg driftspersonell, samt hvilke oppgaver som krever bistand fra autorisert leverandør. F.eks. bytte batteri, kalibrering av lås, synkronisering lås, uthenting av loggdata, utskifting av defekt lås, aktivering av ny lås.	
3	**Vedlikehold og service** Tilbyder skal kunne tilby bytteservice innen 12 timer (utover de årlige vedlikeholdsrundene).	
4	**Utrykning**	

	Tilbyder bør tilbyd utrykning på lås (inkludert evt nødvendig utskiftning av utstyr)	
5	**Opplæring** Tilbyder skal kunne tilby fysisk grunnopplæring på brukerstedet ved levering av låser og tilleggsutstyr.	
6	**Dokumentasjon** Leverandøren skal levere FDV dokumentasjon for Låser inkludert kodepanel samt tilleggsutstyr og kabling. Dokumentasjonen skal inkludere beskrivelse av låser inkludert tilleggsutstyr, kabling, hvilke låser som er tilknyttet hvilken Smarthub etc. Leverandøren skal gi eksempler på dokumentasjon Forsvarsbygg vil motta på installasjoner låser, låssystemer, oppsett, service og vedlikehold, samt opplæringsmateriell. Beskriv opplæringen av Forsvarsbygg sitt personell og eventuelt underleverandør på fagsystemer til Forsvarsbygg ved installasjon av lås system og integrasjon. Beskriv prosedyre for integrasjon mellom tilbudte låser og Invite.	

2.3.2 Øvrige krav til SLA, tilgjengelighet og beredskap

Nr.	Kategori	Beskrivelse
1	B	**Krav til tilgjengelighet, beredskap og SLA** Forsvarsbygg ønsker innspill fra leverandør hvis nivå eller bruk av tjenester anbefales endret for å få bedret ytelse og kost/nytte.
2	C	**Krav til tilgjengelighet, beredskap og SLA** Leverandøren skal gi tilbud på oppetid gitt SLA på 99,5 og 99,7.
3	A	**Krav til tilgjengelighet, beredskap og SLA** Leverandør skal ha supportsystem og rutine for feilretting og håndtering av nedetid. Beskriv hvordan løsning håndterer nedetid pga. strømbrudd, nettverksbrudd på sentral infrastruktur hvis systemet går ned eller lignende. Vil Forsvarsbygg ha bruker tilgang til support verktøyet?
4	A	**Krav til tilgjengelighet, beredskap og SLA** Det forventes at eventuelt låssystem tilhørende låsene kan startes opp automatisk etter eventuelt driftsbrudd slik at slik at løsningen igjen fungerer med utsendelse av koder/elektroniske nøkler.
5	B	**Krav til tilgjengelighet, beredskap og SLA** Dersom avtalte frister ikke overholdes, kan Forsvarsbygg kreve standardisert kompensasjon. Leverandøren bes komme med forslag på kompensasjonsordning ved ikke opprettholdt oppetid og avvik ihht SLA.

6	B	**SLA krav - Tilgjengelighet på låssystemet/tjenesten, håndtering av feil og leverandørens reaksjonstid** Leverandøren plikter å informere Forsvarsbygg om evt.driftsstans i bakenforliggende systemer tilknyttet låsene. Slik varsling skal gis så raskt som mulig når hendelsen inntreffer. Leverandøren plikter å utarbeide rutiner for dette.
7	C	**Krav til tilgjengelighet, beredskap og SLA** Planlagt applikasjonsdriftsstans skal som hovedregel gjennomføres etter kl. 17.00 på virkedager og/eller til helg/helligdager.
8	C	**Krav til tilgjengelighet, beredskap og SLA** Leverandøren plikter å informere Forsvarsbygg om evt. planlagt driftsstans for bakenforliggende låssystemer. Slik varsling skal gis så raskt som mulig, senest 48 timer før driftsstansen inntreffer.
9	B	**Krav til tilgjengelighet, beredskap og SLA** Leverandøren plikter å informere Forsvarsbygg om kritiske eller alvorlige feil. Slik varsling skal gis så raskt som mulig når hendelsen inntreffer. Leverandøren plikter å utarbeide rutiner for dette.
10	B	**Krav til tilgjengelighet, beredskap og SLA** Leverandøren plikter å rapportere avvik fra avtalt tjenestenivå til Forsvarsbygg etter endt måleperiode. Alvorlige avvik skal varsles omgående. Leverandøren plikter å utarbeide rutiner for dette.
11	B	**Krav til tilgjengelighet, beredskap og SLA** Leverandøren plikter å levere loggedata etter angitt format fra kunde inn til felles loggeverktøy for Forsvarsbygg.
12	C	**Krav til tilgjengelighet, beredskap og SLA** Hvis ikke annet er angitt skal hendelser relatert til tjenester og produkter som omfattes av denne avtale, håndteres i henhold til tabell 1 ref avsnitt 2.3.1.1. Tilbyder skal i tilbudet redegjøre for sitt servicenivå herunder bistand til feilsøking og retting av feil m.m. Dersom leverandør ikke kan levere på krav gjengitt i tabell 1, skal tilbyder i tilbudet redegjøre for sin løsning for mht feilretting og SLA krav. Leverandør bes komme med forslag til SLA krav og frister ref tabell 1.
13	B	**Krav til tilgjengelighet, beredskap og SLA** Leverandøren bes beskrive rutiner for driftsstans og varsling av avvik.
14	B	**Innmelding av feil, support og brukerstøtte** Forsvarsbygg vil ha mulighet til å kunne kontakte leverandøren ved eventuelle feil som ikke oppdages automatisk av leverandør. Forsvarsbygg forventer effektiv håndtering, mulighet for å kunne følge status på innmeldt sak og at saken løses raskt.

		Alle henvendelser til leverandøren skal registreres og følges opp i et servicedeskverktøy. Navngitte personer hos kunden skal ha tilgang til servicedeskverktøyet. Leverandøren bes beskrive sin løsning og komme med forslag til rutine.
15	C	**Support og brukerstøtte** Hvis ikke annet er angitt skal åpningstider, hendelser relatert til tjenester og produkter som omfattes av denne avtale, håndteres i henhold til tabell 2 ref avsnitt 2.3.1.2. Dersom leverandør ikke kan levere på krav gjengitt i tabell 2, skal tilbyder i tilbudet redegjøre for sin løsning for brukerstøtte (telefonsupport m.m., åpningstider, generell beskrivelse av løsningen) og SLA krav. Leverandør bes komme med forslag til SLA krav og frister ref tabell 2.
16	B	**Servicedesk verktøy - Support og brukerstøtte** Når en sak registreres, skal servicedeskverktøyet automatisk sende ut en e-post og/eller SMS til innmelder med referansenummer til henvendelsen. I forbindelse med innmelding skal innmelder kunne velge om man vil holdes oppdatert med status endringer og/eller kommentarer i forbindelse med saksbehandlingen. Når saken avsluttes, skal leverandøren sette saken til «løst» og innmelder skal automatisk bli varslet på e-post og/eller SMS før sak lukkes. Dersom innmelder ikke er fornøyd med løsningen skal innmelder kunne klage/svare på e-posten innen 3 dager. Servicedesk skal da gjenoppta saken. Når saken er endelig løst, skal den settes i status «Lukket». Hvis det senere kommer en sak på samme hendelse, skal det opprettes ny sak. Det er vesentlig at eventuelle underleverandører har tilgang og oppdaterer sakene i systemet slik at innmelder holdes løpende oppdatert.
17	B	**Servicedesk verktøy - Support og brukerstøtte** Nøkkelfunksjonalitet ved kundens tilgang til servicedeskverktøy skal være: - Registrere feil, supportsaker eller bestillinger direkte på egne eller andres vegne. - Få enkel oversikt og status på alle saker registrert på kunden. - Kunden skal kunne selektere på periode dato, uke, måned og år. - Ta ut forhåndsdefinerte rapporter over antall innmeldte saker og status disse. Tilbyder bes legge ved eksempler eller en beskrivelse av funksjonalitet.
18	B	**Servicedesk verktøy - Support og brukerstøtte** Tilbyder skal kunne tilby opplæring på servicedeskvertøyet.
19	C	**Behov for ekstra beredskap** Forsvarsbygg skal ha en opsjon der en kan bestille økt beredskap ved behov. Dette kan tenkes brukt ved større oppgraderinger, endringer eller lignende som kan påvirke produksjonsplattform.

20	B	**Oppgraderingssyklus** Leverandør skal ha en rutine for oppgradering av programvare på låser, tilleggsutstyr og huber. Beskriv modell for vedlikehold oppgradering av firmware/programvare som følger med foreslåtte løsning. Hvordan tilgjengeliggjøres nye versjoner av programvare til Forsvarsbygg? Beskrive evt kostnader som tilkommer ved oppdateringer?
21	B	**Installering av programrettelser, firmware mv.** Dersom det er avtalt at Leverandøren kan rette feil ved å sende eller gjøre tilgjengelig for Kunden en programrettelse, skal dette, samt rutiner for slik tilgjengeliggjøring, fremkomme her både for lås, tilleggsutstyr og huber. Eventuelle frister for hvor raskt Kunden skal teste og ta i bruk programrettelser fra Leverandøren skal fremkomme her.
22	B	**Nye versjoner** Hvis det skal gjelde spesifikke tidsfrister for oppgradering til nye versjoner av alminnelig brukt programvare som inngår i Kundens tekniske plattform, skal disse spesifiseres her. Eventuell programvare som er unntatt fra bestemmelsen om tidsfrister, skal spesifiseres her.

2.4 Krav til integrasjoner til låser fra back end forvaltning og sentralstyring gjennom **API og mellomvare (Biztalk)**

Basen inneholder informasjon om brukeren og bookingen og er Frontend systemet til Forsvarsbygg. Basen kommuniserer til Invite Flåtestyring for Elås gjennom applikasjonene VisBook og en Biztalk integrasjon. Invite skal kommuniserer videre med installerte låser, låseapper og eventuell låsprogramvare.

Flåtestyringsverktøyet Invite benytter et REST API og kaller på låsesystemet for å gi tilganger. Integrasjon mot Invite® er derfor et krav.

Nr.	Kategori	Beskrivelse
1	A	Låsens nøkkel skal endres ved bestilling og endring av booking som følge av integrasjon. Forklaring: Det skal være mulig å fra Basen bookingsystemet å sende ny booking eller endring av booking, samt sletting av booking gjennom API til låssystem for tilgang til lås i definert periode. Dette skal kunne gi tilgang f. eks gjennom mobiltelefon ved BLE, kode, eller lignende.
2	A	Låsens nøkkel skal endres når tilgang deaktiveres gjennom systemene. Forklaring: I tilfeller der sluttbruker sjekker ut før definert oppholdstid skal det være mulig å deaktivere tilgang til rom gjennom mobiltelefon og BLE eller alternativ løsning som eks PIN kode. Dette pga sikkerhet samt for å kunne tilgjengeliggjøre rom for andre.

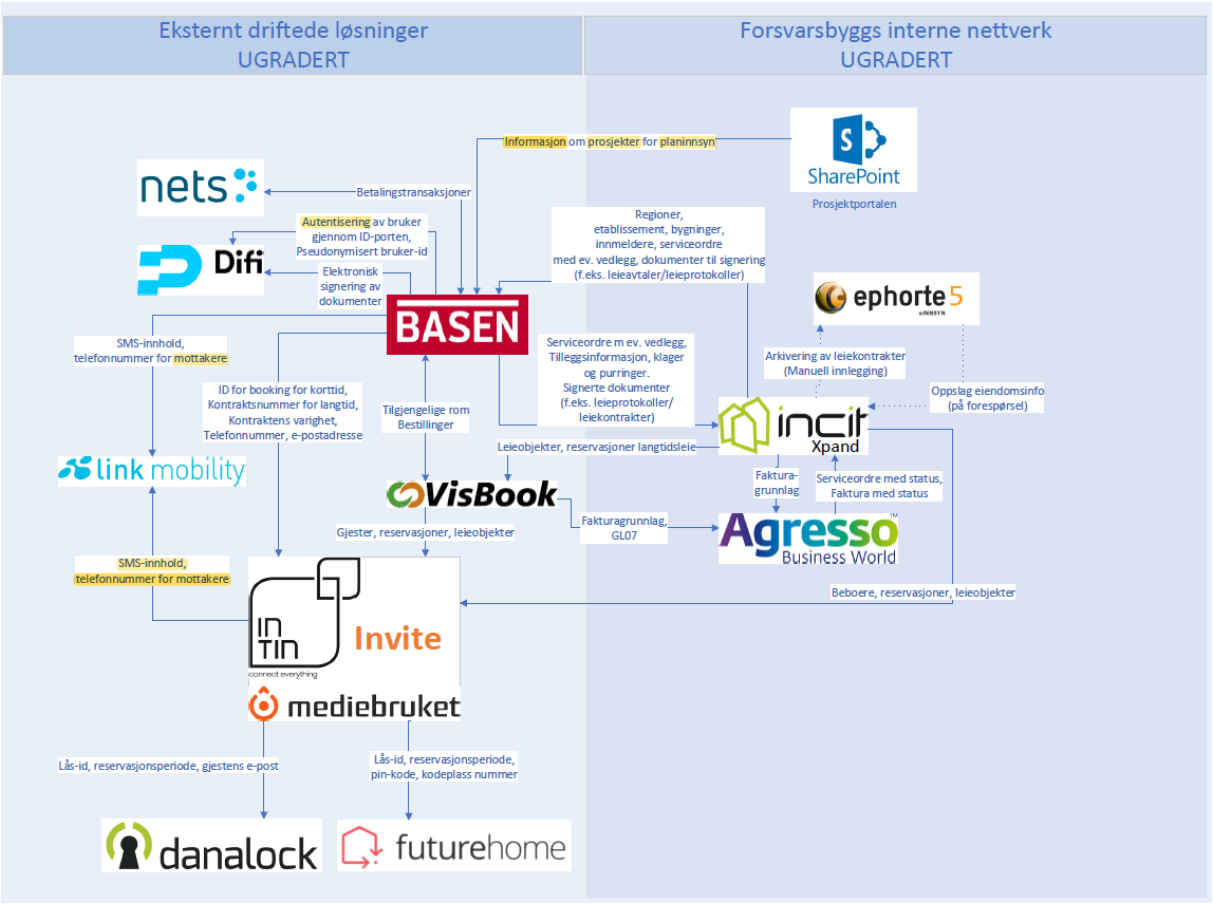
3	A	Låsens nøkkel skal endres ved fristilling av rom Forklaring: Tilsvarende i tilfeller der sluttbruker ikke sjekker inn eller lar være å benytte rom innen definert tidsramme så skal Forsvarsbygg kunne frigi rom i bookingsystemet og tilgang fjernes for sluttbruker gjennom mobiltelefon via eksempelvis BLE eller alternativ løsning.
4	A	Låsens nøkkel skal endres ved endring av romtildeling I tilfeller der sluttbruker er blitt tildelt rom, men tildelt rom endres av Bolig- og kvarterforvalter eller Servicesenteret må dette kunne håndteres av løsning slik at tildelt elektronisk nøkkel eller kode deaktiveres, og ny nøkkel eller kode til nytt rom tilgjengeliggjøres.
5	B	Låsens nøkkel skal endres ved å gi korttidstilgang til rom Låsen skal støtte korttids tilgang til rom for bruker når dette styres gjennom Invite flåtestyring (og bakenforliggende integrasjoner). Dette kan være behov for teknikere, eller i tilfeller der bruker ikke lenger har tilgang til rom, men har behov for kort tilgang til rom for uthenting av gjenglemte artikler. Beskriv eventuelt også alternative måter hvis det finnes, samt en anbefalt metode.
6	A	**Låssystem skal støtte integrasjon til Invite flåtestyring** Låssystemet må ha et standard grensesnitt for integrasjon med flåtestyringssystemet Invite for Forsvarsbygg.
7	A	**Grensesnitt Invite (flåtestyringssystem)** Låssystemet må kunne integreres mot API for Forsvarsbygg sitt Elås Flåtestyringssytem Invite som igjen er integrert moe Basen Frontend, Visbook og Xpand. Se beskrivelse for API https://api.visitinvite.com/api-docs/ For nærmere info om systemer, tjenester og krav til funksjonalitet se kapittel 1.1 ink systemskisse. Tilbyder bes beskrive hvordan generell integrasjon ivaretas.
8	B	**Utveksling av informasjon til Invite** Låser og tilleggsutstyr må støtte toveis dialog med Invite mht låsestatus, lagring av digitale nøkler, batteristatus etc. Leverandøren må beskrive hvilke muligheter som finnes.
9	B	**Hyppighet og form på kommunikasjon til lås** Leverandør må beskrive hyppigheten av kommunikasjon mellom lås, tilleggsutstyr og flåtestyringssystem Invite
10	B	**Krav fra låssystemet til kundens miljø** Leverandør må oppgi eventuelle krav som låssystemet stiller til Forsvarsbygg Beskriv eventuelle krav som stilles til flåtestyringssystem, dører, kvarterbygg eller annet

11	B	**Krav til integrasjon med Invite** Sette tidsavgrenset PIN kode på lås. Tidssperiode lengde må støtte alt fra 15 minutter til flere år. Tidsperiode må kunne settes fra nåtidspunkt, men også for en tidsperiode med oppstart frem i tid.
12	B	**Krav til integrasjon med Invite** Sette tidsavgrenset digital nøkkel på lås(app). Tidsperiode lengde må støtte alt fra 15 minutter til flere år. Tidsperiode må kunne settes fra nåtidspunkt, men også for en tidsperiode med oppstart frem i tid.
13	B	**Krav til integrasjon med Invite** Låse opp og igjen
14	B	**Krav til integrasjon med Invite** Sende låsstatus og batteristatus
15	B	**Krav til integrasjon med Invite** Låssystemet må kunne sende en app invitasjon som inneholder en eller flere digitale nøkler
16	B	**Krav til integrasjon med Invite** Invite må få informasjon fra Låssystemet om gjest har app bruker allerede basert på mobilnummer. Invite vil da informere gjest om at nøkkel er lagt til på eksisterende bruker istedenfor å sende ny app invitasjon
17	B	**Krav til integrasjon med Invite** Det må kunne opprettes PIN og digital nøkkel uten krav om e-post eller navn på gjest
18	B	**Krav til integrasjon med Invite** Nøkkelsystemet må ha sporingsløsning på tildelt Pin eller digital nøkkel slik at sletting, endring, bytte av rom kan utføres
19	B	**Krav til integrasjon med Invite** Det må kunne gis tilgang til minimum 10 personer i samme tidsperiode fra Invite både digitalt og med PIN. Dette siden det oftest er flere som trenger tilgang til et rom i samme periode som for eksempel driftspersonell, gjester, renhold.
20	B	**Krav til integrasjon med Invite** Leverandøren må beskrive hvordan systemet løser samtidig tilgang til fellesdører og romdører for en gjest. Både PIN og digital nøkkel
21	B	**Krav til integrasjon med Invite** Leverandøren må beskrive hvordan systemet håndterer en samtidig booking av 20 rom til ulike gjester med ulik tidsrestriksjon i samme korridor. Ta med forventet tidsbruk.

2.5 Andre krav til systemer, arkitektur, integrasjoner og dokumentasjonskrav

Nr.	Kategori	Beskrivelse
1	A	**Arkitektur og plattform for låssystem tilhørende låsene** Systemdokumentasjon skal omfatte arkitektur og plattform Beskriv arkitektur, plattform og teknologi brukt for tilbudt løsning. Det er spesielt viktig at tilbyder beskriver hvor og hvordan data lagres i løsningen samt hvordan kommunikasjon mellom lås og eventuelle øvrige lag/komponenter foregår.
2	B	**Kommunikasjon** Leverandør må dokumentere hvordan sikkerheten er ivaretatt når data transporteres mellom mobiltlf, lås, lås-systemer og flåtestyringssystem Beskriv hvordan sikkerhet i kommunikasjon håndteres i tilbudt løsning. Beskriv hvorvidt det er krav til internetttilkobling lokalt? Hva er behovet for båndbredde for overføring av nøkkel info?
3	B	**Logging** Leverandør bes beskrive hvilken logging av data som kan skrues på eller av, samt beskrive hvor data lagres og hvor lenge. Leverandør skal også støtte levering av loggedata til fellesloggeverktøy for Forsvasrbygg.
4	B	**Onboarding program** Leverandøren må dokumentere hvordan tilpasning og integrasjoner mellom Forsvarsbygg sitt flåtestyringssystem og låsleverandør sitt system samt låser håndteres. Beskriv hvordan leverandøren håndterer tilpasning og integrasjoner mellom eksisterende låsinstallasjoner, nye låser, flåtestyringssystem til Forsvarsbygg og låsleverandør/system.
5	C	**App** Leverandør må oppgi hvilken app som følger med låssystemet, eller om dette løses på annen måte via mobil. Leverandør bes oppgi om det er krav til å skru på posisjonering for å benytte app.

2.5.1 Arkitekturlandskap Basen, Elås og fagsystemer



2.6 Sikkerhetskrav

Siden løsningen skal benyttes av virksomheter i Forsvarssektoren er det generelt sterkt fokus på sikkerhet i løsningen.

Forsvarssektoren skal ha tilstrekkelig informasjonssikkerhet i cyberdomenet, og ivareta dette som en integrert del av sitt virke. Sektoren skal være forberedt på å håndtere alle former for hendelser som kan ramme egne IKT-systemer.

Selv om deler av forsvarssektorens virksomhet i cyberdomenet har likhetstrekk med tilsvarende virksomhet i det sivile samfunn, har forsvarssektoren et særskilt ansvar relatert til militære operasjoner, etterretning og håndtering av situasjoner som truer statssikkerheten. Dette stiller særlige krav til forsvarssektoren.

Forsvarssektoren forvalter en rekke IKT-systemer med ulike beskyttelsesbehov. Virksomhetene skal, basert på regelverk og risiko- og sårbarhetsanalyser, etablere oversikt over hvilke beskyttelsesbehov de ulike systemene har, og beskytte systemene i henhold til dette. Systemene skal beskyttes med tanke på sikring av informasjonens konfidensialitet, integritet, tilgjengelighet og autentisitet. Beskyttelse av egne systemer skal inngå som en integrert del av daglig systemdrift, og utføres både i normal virksomhet og i forbindelse med krise eller væpnet konflikt.

Forsvarsbygg henviser også til Digitaliseringsdirektoratet: Helhetlig styring og kontroll av informasjonssikkerhet

2.6.1 Personopplysninger

Konfidensialitet:

Konfidensialitet betyr at personopplysninger må være sikret mot at uvedkommende får kjennskap til opplysningene.

Integritet:

Med integritet menes at personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting.

Tilgjengelighet:

Tilgjengelighet betyr at personopplysninger som skal behandles, er tilgjengelig til den tid og på det sted det er behov for opplysningene.

Nr.	Kategori	Beskrivelse
1	A	**Personopplysningsloven** Systemet skal tilfredsstille krav som følger av personopplysningsloven med forskrifter og ivareta alle lovpålegg og forskrifter eksempelvis GDPR, ny lov fra 25. mai 2018. I den grad Forsvarsbygg må varsle gjeldende myndigheter om bruk av systemet, påligger det leverandøren plikt til å opplyse Forsvarsbygg om dette.
2	A	**Sikkerhetsarkitektur** Leverandøren skal beskrive løsningens sikkerhetsarkitektur, samt hvordan sikkerhet inngår som en integrert del av daglig applikasjonsdrift.
3	A	**Forhindring av inntrenging eller angrep** Løsningen skal ha sikkerhetsmekanismer for å forhindre inntrenging av uautoriserte. Løsningen skal ha sikkerhetsmekanismer for å forhindre at uautoriserte kan manipulere data, dokumenter eller rapporter.
4	C	**Forhindring av inntrenging eller angrep** Leverandøren skal beskrive sikkerhetsmekanismer som en del av løsningens arkitektur.
5	B	**Sikkerhetstesting** Løsningen og alle dens komponenter, moduler og integrasjoner skal kunne godkjennes ihht sikkerhetstesting som skal foretas av 3.part utpekt og bekostet av Forsvarsbygg. Kostnader knyttet til tetting av sikkerhetshull og retting av feil skal bekostes av leverandøren.

6	B	**Logger** Forsvarsbygg har behov for informasjon om og kontroll mht DPIA, personvernerklæring og verdivurdering av data/informasjon i løsningen/låsene m.m. som tilbys. Det må være mulig å tilpasse løsningen mht hvilken informasjon som lagres og logges. Leverandøren må beskrive hva som innhentes av informasjon, samt hva som logges og evt lagres av informasjon i systemet og på låsene inkludert tilleggsutstyr og huber.
7	B	**Nasjonal Sikkerhetsmyndighets (NSM) retningslinjer** Leverandør skal følge NSM sine råd, veiledninger og retningslinjer til krav rundt applikasjonsdriftsmiljø og sikring av dette, sikkert skymiljø og ugraderte systemer. Disse beskrives under, men er ikke begrenset til: 1. Leverandørens løsning skal ha funksjonalitet som ivaretar NSMs grunnprinsipper for IKT-sikkerhet og NSMs «Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester». 2. Ved sletting av data skal det brukes en metode som gjør at det ikke er mulig å rekonstruere og lese informasjonen i løsningen. NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer (maskinvare, programvare og tilknyttet infrastruktur), data og tjenestene de tilbyr mot uautorisert tilgang, skade eller misbruk PDF: https://nsm.no/getfile.php/133735-1592917067/Demo/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf URL: Grunnprinsipper for IKT-sikkerhet - Nasjonal sikkerhetsmyndighet (nsm.no) Merk også støtteprodukter for IKT sikkerhet inkludert eget regneark fra NSM: Støtteprodukter - Nasjonal sikkerhetsmyndighet (nsm.no) I forsvarssektoren er det en egen enhet - MilCert – som har overordnet ansvar og monitorer løsninger, og spesielt hvis de er synlige/ sårbare for sivilt personell. Loggdata skal kunne deles med dette miljøet og leverandør må samarbeide med MilCert og NSM og forholde seg til NSM sin veiledning. Hensikten med NSMs temarapport «Sikkerhetsfaglige anbefalinger ved bruk av tjenesteutsetting og skytjenester» er å bistå offentlige og private virksomheter med overordnede sikkerhetsfaglige anbefalinger ved tjenesteutsetting av IKT-tjenester herunder bruk av skytjenester. Anbefalingene er relevante for offentlige og private virksomheter som vurderer å tjenesteutsette basisdrift, applikasjonsdrift eller applikasjonsforvaltning til en ekstern tjenesteleverandør. https://nsm.no/getfile.php/133998-1593590999/Demo/Dokumenter/Rapporter/2020-07-01%20-%20Temarapport%20-%20Tjenesteutsetting.pdf • Tilbyder bes beskrive sin løsning og hvordan sikkerhet ivaretas iht Sikring av kommunikasjon/transportlag ved kommunikasjon mellom løsningen og øvrige systemer denne kommuniserer med • Tiltak for forebygging av DDoS (tjenestenektangrep) mot løsningen

		Som bakgrunn for å besvare dette kan leverandør se følgende vedlagte dokumenter som inneholder råd om forebyggende tiltak for systemer som ikke er underlagt kravene i sikkerhetsloven: • U-03 Sikring av Windows TLS: Inneholder NSMs anbefalinger for herding av Transport Layer Security (TLS) på ugraderte IT-systemer som anvender Windows 7 SP1, Windows Server 2008 R2 og senere versjoner. • U-04 Grunnleggende tiltak for forebygging av DDoS: Dette dokumentet beskriver noen grunnleggende tiltak for å sikre ugraderte IKT-systemer mot distribuerte tjenestenektangrep («DDoS - Distributed Denial of Service»). Tiltakene er ment å utfylle «commercial best practice». • U-12 Veiledning i DNS-filtrering: Dokumentet gir veiledning i filtrering av Domain Name System (DNS)-forespørsler ved bruk av Response Policy Zone (RPZ)-svartelister. Målgruppen er personell som drifter ugraderte, men sensitive systemer. • U-14 Sikring av kommunikasjon med TLS: Denne veiledningen er en beskrivelse av grunnleggende tiltak for sikring av kommunikasjon over usikre nett ved hjelp av TLS. • U-15 Hypertext Transport Protocol Secure: Formålet med denne veiledningen er å gi anbefalinger om hvordan man kan etablere sikker overføring av webtrafikk ved å bruke HTTPS. • U-16 Brukerautentisering mot nettsteder: Denne veiledningen beskriver hvorfor man bør benytte to-faktor autentisering, hvordan U2F fungerer og hvorfor denne protokollen bør benyttes. For ytterligere informasjon se «Veiledninger for ugraderte systemer» på NSM sine hjemmesider: Veiledere og håndbøker til sikkerhetsloven - Nasjonal sikkerhetsmyndighet (nsm.no)

2.6.2 Applikasjonsdrift, applikasjonsutvikling og lagring av data

Nr.	Kategori	Beskrivelse
1	A	Gitt kundens rolle som beredskapsorganisasjon så kreves det at: a) personellet som jobber med applikasjonen på skytjenesten skal være geografisk lokalisert i Norge og/eller b) at selskapet det inngås avtale med (Leverandøren) er etablert i land Norge har sikkerhetspolitisk samarbeid med.

2.6.3 Sikkerhetstesting, rapportering, oppfølging, evaluering og revisjon

Nr.	Kategori	Beskrivelse
1	C	Leverandøren plikter å utarbeide systemtekniske krav og jevnlig teste disse. Testdokumentasjon med testresultater skal leveres til Forsvarsbygg. Leverandøren bes i sitt tilbud beskrive metodikk, innhold for sikkerhetstesting, samt hyppighet Leverandøren bes beskrive metodikk, test sertifiseringer, type test (eks vis Penetrasjonstesting og Samsvartesting) og evt. rutiner mht. ivaretakelse av ovennevnte krav.
2	B	Leverandøren plikter å etablere rutiner for monitorering, oppfølging, evaluering og rapportering av potensielt sikkerhetstruende hendelser og sikkerhetsbrudd til Forsvarsbygg. Sikkerhetsbrudd eller mistanke om sikkerhetstruende hendelser/sikkerhetsbrudd eller forsøk på slike skal snarest rapporteres til Forsvarsbygg. Dette gjelder også virus, ondsinnet programvare samt sikkerhetsbrudd utført i vanvare. Alle tilgjengelige ressurser skal iverksettes for å forhindre, stanse og begrense et skadepotensial. Leverandøren bes beskrive sikkerhetssertifiseringer, metodikk, standard, praksis og rutiner o.l. mht. ivaretakelse av ovennevnte krav. Det er ønskelig at leverandøren fremlegger eksempler på type rapport mht rapportering av sikkerhetstruende hendelser ink virus m.m. ref krav overfor.
3	A	Utlevering av logger Leverandør skal kunne levere ut logger til Milcert eller NSM på forespørsel. Typiske eksempler kan være data på avveie, innbrudd etc.
4	B	Leverandøren plikter å gjennomføre sikkerhetsrevisjon minimum hvert 2. år for å stadfeste at virksomheten og evt. underleverandører etterlever etablerte prosedyrer og overholder kravene mht. GDPR, personopplysningsloven og NSM sine veiledninger for ugraderte nett. Revisjonen bør omfatte revisjon av hele eller deler av virksomhetens drifts- og forvaltningsprosesser for IKT, organisering av informasjonssikkerhet, roller og ansvar, samt kartlegging av sikkerhetsnivå. Leverandøren bes beskrive sertifiseringer, metodikk, standard, praksis og rutiner o.l. mht. ivaretakelse av ovennevnte krav.
5	A	Forsvarsbygg forbeholder seg retten til å teste hele eller deler av kravene selv eller gjennom tredjepart som leverandøren benytter. Kostnader til en slik test bekostes av Forsvarsbygg. Kostnader knyttet til evt. feil/avvik og tetting av eventuelle sikkerhetshull skal bekostes av leverandøren.
6	A	Leverandøren og dens konsulenter plikter å gjøre seg kjent med Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven) med aktuelle forskrifter. Samtlige konsulenter som jobber med applikasjonen Basen, dens programvare, utstyr, servere m.m. skal signere taushetserklæring og inneha nødvendige autorisasjoner ref avsnitt Sikkerhetsklarering av personell. Konsulenten og dens representanter forplikter seg til å overholde herværende avtale og til enhver tid gjeldende regelverk.

2.6.4 Tilgang på personell, sikkerhetsklarering og autorisasjon

Nr.	Kategori	Beskrivelse
1	B	**Tilgang til teknisk personell** Tilbyder skal kunne stille med et kjerneteam av teknisk personell mht utvikling og integrasjon mot Invite og annen infrastruktur.
2	C	**Tilgang til personell for montering og installasjon** Det er ønskelig med et kjerneteam av montører for installasjon/feilretting/service og vedlikehold. Leverandøren bes angi i sitt tilbud hvor disse er lokalisert mht å serve den enkelte leir, samt utrykningstid.
3	A	**Taushetserklæring** Alt personell som arbeider for Forsvarsbygg skal, før arbeidsforholdet tar til, undertegne taushetserklæring.
4	A	**Autorisasjon og klarering av installasjonspersonell/montører:** Tilbyder skal kunne stille autorisert og sikkerhetsklarert personell ved installasjon av lås eller annen lokal infrastruktur. Kravet til nivå på klarering kan variere fra lokasjon til lokasjon. Det er ikke mulig å sende ut personell som ikke innehar nødvendig klarering og autorisasjon uten særskilt avtale om følgetjenste fra Forsvarsbygg.
5	A	**Sikkerhetsklarering av teknisk personell:** Alle som jobber med Forsvarsbygg skal kunne sikkerhetsklareres til minimum nivå HEMMELIG, se vedlegg 8.
6	B	Autoriserte/sikkerhetsklarerte personer plikter å holde autorisasjons-/klareringsmyndigheten orientert om forhold som kan være av betydning for vurdering av sikkerhetsmessig skikkethet. Dette gjelder blant annet endringer i sivilstatus, strafferettslige forhold, forhold til lovlige og ulovlige rusmidler, økonomiske problemer, tilknytning til andre stater og medisinsk relaterte helseforhold. Leverandøren skal beskrive rutiner for hvordan ovenfornevnte krav overholdes.
7	B	Alt personell som gis tilgang til informasjonssystemer og/eller behandler informasjon, plikter å sette seg inn i og følge pålegg i sikkerhetsinstruks og annen relevant sikkerhetsdokumentasjon hvor dette er påkrevd. Alt personell som gis tilgang til informasjonssystemer og/eller behandler informasjon har en plikt til å beskytte og hindre at uvedkommende får innsyn eller kjennskap i informasjon inkludert skjermingsverdig og sikkerhetsgradert informasjon (Sikkerhetsloven § 12). Virksomhetens leder eller den lederen bemyndiger skal påse at bruker gis nødvendig opplæring, slik at brukeren kan operere virksomhetens informasjonssystemer på en sikkerhetsmessig forsvarlig måte. Leverandøren skal beskrive rutiner for hvordan ovenfornevnte krav overholdes.

8	B	Leverandøren plikter å rutinemessig oversende liste over personell som skal jobbe med Forsvarsbygg. Leverandøren plikter å gi Forsvarsbygg rutinemessig oversikt over alle brukere/personell (teknisk personell m.m.) som innehar administratortilgang eller kan gi seg selv administrative rettigheter, har tilgang til eller kan hente ut informasjon, driftere av evt. bakenforliggende sikkerhetsmekanismer. Dette inkluderer evt. underleverandører som står i en eller annen privilegert posisjon ovenfor informasjonssystemet. Ref konkurransegrunnlagets vedlegg J underleverandøroversikt.
9	A	Kravet om taushetserklæring og autorisering gjelder også for underleverandør og annen innleid arbeidskraft. Dersom leverandøren skal bruke personell ansatt hos underleverandører/partner/forhandler etc. skal det fremlegges en forpliktelseserklæring fra disse. Signerte forpliktelseserklæringer skal fremlegges før kontrakt signeres.