Lånekassen

Bilag 1 - Kravspesifikasjon

for anskaffelse av

Aksesspunkt for bankfiler

Saksnummer 2023/231

Innhold

1 Forklaring til kravspesifikasjonen 3
1.1 Leverandørens besvarelse 3
2 Generelle krav til tjenesten 3
2.1 Bakgrunn 3
2.2 Utbetaling 3
2.3 Innbetaling 5
3 Generelle krav til aksesspunkt for bankfiler (Peppol) 7
4 Overordnede krav til etableringsfasen 9
5 Krav til Informasjonssikkerhet og personvern 11
6 Tjenestenivå (SLA), standardiserte kompensasjoner m.v. 17

1 Forklaring til kravspesifikasjonen

Kravene i tabellene under er gitt prioritet som følger:

Kode	Betydning
A	Absolutte krav som er obligatoriske krav, og manglende oppfyllelse vil føre til avvisning.
B	Bør-krav. Leverandøren kan velge om han ønsker å tilby tjenesten og i hvilken grad kravet oppfylles. Graden av oppfyllelse vurderes under tildelingskriteriet Kvalitet etter innbyrdes vekting som nevnt over.

For besvarelse av kravspesifikasjonen, se Bilag 2.

I tabellene fremgår det en beskrivelse av hvilke krav Lånekassen har, om det er et A eller B krav, samt hvordan leverandørene skal dokumentere oppfyllelse av kravet.

1.1 Leverandørens besvarelse

Besvarelsen skal gis som beskrevet under hvert krav i denne kravspesifikasjonen i konkurransegrunnlagets Bilag 2 og Bilag 2 Vedlegg 2.2.

For alle A-krav skal oppfyllelsen av kravet bekreftes oppfylt i egenerklæringsskjema, Bilag 2, Vedlegg 2.2.

For A-krav merket med A* skal det i tillegg til egenerklæring gis en skriftlig besvarelse i konkurransegrunnlagets Bilag 2, se kapitlene under.

Besvarelse/utfylling av Databehandleravtale gjøres i Databehandleravtale, Bilag – Vedlegg 2.1

Pristilbud skal gis i SSA-L Bilag 6.

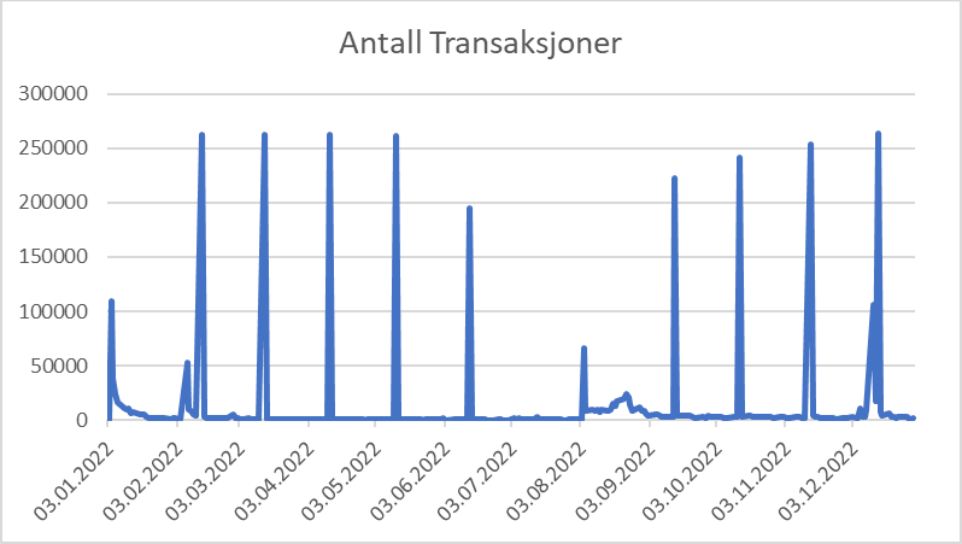
2 Generelle krav til tjenesten

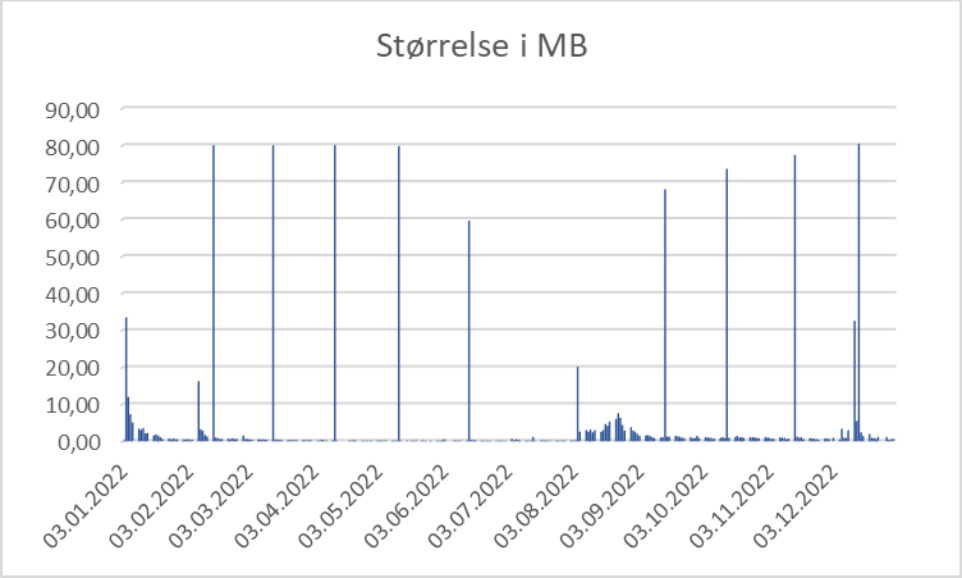
2.1 Bakgrunn

Hensikten med anskaffelsen er å understøtte Lånekassens hovedformål som er utbetaling av utdanningsstøtte til elever og studenter, samt motta tilbakebetaling av studielån. I 2022 gjennomførte Lånekassen 3,3 millioner utbetalinger og mottok 7 millioner innbetalinger.

2.2 Utbetaling

Lånekassen gjennomfører som hovedregel månedlig utbetaling av studiestøtten slik at pengene skal være tilgjengelig på kundens konto en virkedag før den 15. i måneden. Som figuren under viser, har derfor Lånekassen noen overføringer gjennom året med spesielt høyt transaksjonsvolum.





I begynnelsen av høst- og vår semestrene er utbetalingene fordelt noe mer utover hele måneden. Derfor ser vi lavere topper i disse to månedene.

I juli er det generelt få kunder som får utbetaling, derfor lavt volum i denne perioden.

I juni er det færre kunder som har rett på støtte, men også i juni er det er høyt volum.

Utbetalingene fra Lånekassen er for kundene som regel deres livsgrunnlag. Utbetalingene er planlagt og kundene har ofte lav buffer fra før på konto. En forsinkelse i overføringene vil derfor av mange kunder oppleves som kritisk.

Lånekassen har utbetalinger hver dag. En liten andel av utbetalingene gjelder refusjoner til kunder som har betalt inn for mye på studielånet.

Lånekassen har i årene 2017-2021 opplevd en vekst i antall kunder som får støtte på ca. 5 %. Lånekassen legger til grunn at denne utviklingen vil fortsatt. Introduksjon av ny ordning for utdanningsstøtte vil kunne øke dagens volum.

Overordnet statistikk for 2022:

Antall transaksjoner totalt	3 325 609
Antall MB totalt (Telepay)	1 015
Maks antall transaksjoner per dag	263 210

Lånekassen gjennomførte i 2022 utbetalinger på 252 virkedager.

Antall transaksjoner	Antall ganger
0 – 4 999	204
5 000 – 9 999	18
10 000 – 19 999	13
20 000 – 99 999	6
100 000 – 260 000	6
260 000 – 263 210	5

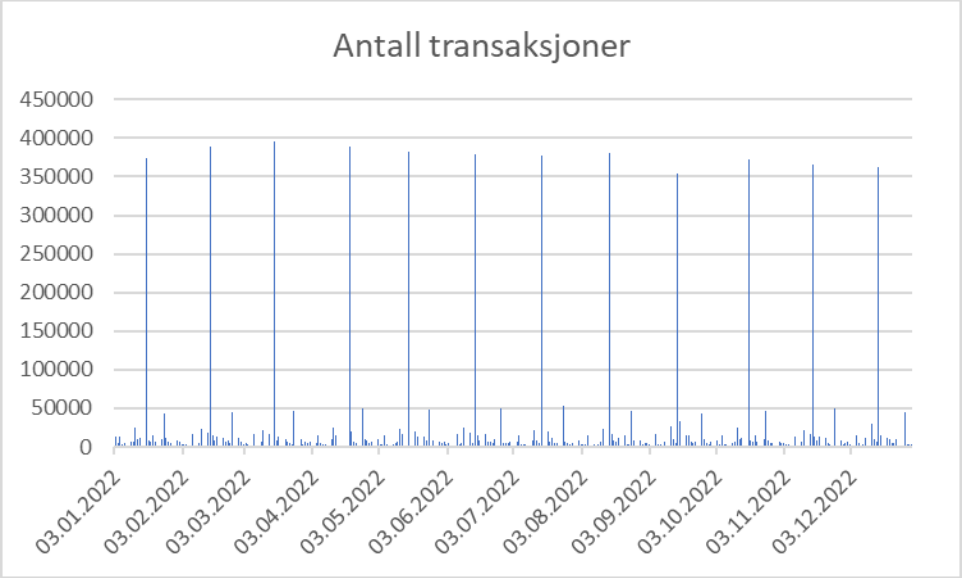
De største filene var i gjennomsnitt på 80 MB. De minste filene i gjennomsnitt på 0,5 MB.

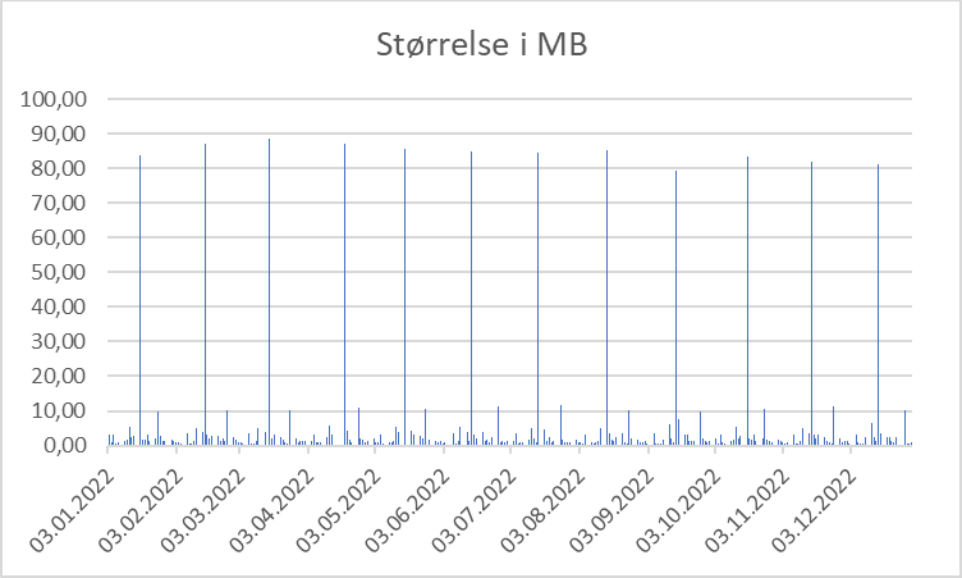
2.3 Innbetaling

Ved utgangen 2022 hadde Lånekassen 772 000 kunder som tilbakebetalte studielånet. Disse kundene har månedlig forfall. Antall innbetalinger per måned ligger på cirka 600.000.

Kundens forfall er fordelt på tre hoveddatoer; 5., 15. og 25. Dersom kunden ikke har gjort et valg, er standard forfallsdato den 15. i måneden.

Utenom disse datoene kommer det inn innbetalinger i mindre volum hver dag. Disse innbetalingene er for sene betalinger eller ekstra ordinære innbetalinger.





Overordnet statistikk for 2022:

Antall transaksjoner totalt	7 057 127
Antall MB totalt (Cremul)	1 580
Maks antall transaksjoner per dag	395 715

Lånekassen gjennomførte i 2022 innlesing av innbetalinger (cremul) på 252 virkedager.

Antall transaksjoner	Antall ganger
0 – 4 999	73
5 000 – 9 999	86
10 000 – 19 999	55
20 000 – 99 999	26
100 000 – 260 000	0
260 000 – 395 715	12

3 Generelle krav til aksesspunkt for bankfiler (Peppol)

Lånekassen har behov for å inngå rammeavtale om aksesspunkt for bankfiler for å imøtekomme krav til ny meldingsstandard ISO20022 for betalingsmeldinger mellom virksomheten og bank. I tillegg til ny standard PEPPOL Payment for sikring og transport av meldinger mellom banken og virksomheten. Aksesspunktet skal levere tjenester og følge definerte standarder og krav for PEPPOL Payment for betalingsmeldinger.

Krav nr	Generelle krav til aksesspunkt for bankfiler	Prioritet (A, B)	Dokumentasjon
3.1	**Overordnet** Tjenesten må være godkjent Aksesspunkt for betalingsfiler fra regional PEPPOL myndighet i Norge. Tjenesten må ha sertifisering/godkjenning fra nasjonal PEPPOL myndighet i Norge som aksesspunkt for betalingsfiler i hele kontraktsperioden.	A*	Sertifisering/dokumentasjon vedlegges tilbudet.
3.2	**Språk** Kommunikasjonsspråk herunder dokumentasjon, mellom partene skal være norsk.	A	Egenerklæring
3.3	**Lokasjon** Aksesspunktet skal driftes i leverandørens infrastruktur.	A	Egenerklæring
3.4	**Registrering i SMP/ELMA** Leverandør av aksesspunktet skal håndtere registreringen av Lånekassens enheter i SMP/ELMA.	A	Egenerklæring
3.5	**Kapasitet** Tjenestens funksjonalitet skal kunne betjene det minimumsvolum som er beskrevet med hensyn til topper. Tjenesten skal kunne skalere kapasitet opp i hele kontraktsperioden.	A	Egenerklæring

Krav nr	Generelle krav til aksesspunkt for bankfiler	Prioritet (A, B)	Dokumentasjon
3.6	**Testmiljø** Leverandøren skal tilby test-aksesspunkt og konsulenter for å støtte Lånekassen og partnere for testing av ISO 20022 filer over PEPPOL Payment infrastruktur. Test-aksesspunktet skal være tilgjengelig under hele kontraktsperioden. Testmiljøet skal gå fra Lånekassen til/fra bank.	A*	Leverandøren skal beskrive hvordan test av infrastruktur og overføring av filer kan gjennomføres.
3.7	**Integrasjon** Tilgjengelige grensesnitt for utveksling av betalingsfiler skal være veldokumenterte og eksempelkode for grensesnitt(ene), med kontrakt, tilgjengeliggjøres Kunden uten ugrunnet opphold.	A*	Leverandøren skal dokumentere tilgjengelige grensesnitt inklusive tilhørende sikkerhetsmekanismer.
3.8	**Kvitteringer** Mottakskvittering (RC4), avviksmeldinger (RC4b) skal returneres til Kunden. Andre feil som medfører at aksesspunktet ikke kan videreformidle meldingen skal returneres til Kunden. Det skal være mulig å utvide med andre kvitteringer/ meldinger. Kvitteringer/tekniske meldinger skal også tilgjengeliggjøres Kunden på en oversiktlig måte.	A	Egenerklæring

4 Overordnede krav til etableringsfasen

Inn- og utbetalinger er kritisk for Lånekassens kjernevirksomhet. Aksesspunkt for bankfiler vil være ett av flere ledd i denne prosessen og god dokumentasjon av tjenesten er derfor helt avgjørende.

Lånekassen skal ta i bruk ny meldingsstandard ISO20022 for betalingsmeldinger mellom virksomheten og bank innen 31/12-2023. I tillegg skal det innføres ny standard PEPPOL Payment for sikring og transport av meldinger mellom banken og virksomheten. Utbetaling til studenter er Lånekassens viktigste verdi og det er derfor kritisk at alle planer sikrer overgang til nytt filformat (ISO20022) innen fristen. Belastningen på Lånekassen sin organisasjon i forbindelse med overgang til nytt år (des/jan) tilsier at etablering av aksesspunkt for bankfiler må ferdigstilles i god tid før dette.

Lånekassen benytter ikke i dag aksesspunkt for bankfiler slik at dette blir en etablering av en helt ny tjeneste for kunden. Dette gjøres på et særdeles viktig område slik at det er viktig med gode planer og rutiner for test og produksjonssetting.

Krav nr	Overordnede krav til etableringsfasen	Prioritet (A, B)	Dokumentasjon
4.1	Leverandøren bes utarbeide forslag til testplan i forbindelse med produksjonssetting hvor det fremgår hvordan man sikrer en god prosess for samarbeid og involvering av kunden, tydelig ansvarsfordeling, håndtering og eskalering av feil m.v.	B	Leverandørens beskrivelse i bilag 3
4.2	Kunden ønsker at tjenesten er etablert i produksjon innen 1.11.2023. Leverandøren bes utforme en overordnet fremdriftsplan for etablering av tjenesten som sannsynliggjør at fristen overholdes.	B	Leverandørens beskrivelse i bilag 3

Krav nr	Overordnede krav til etableringsfasen	Prioritet (A, B)	Dokumentasjon
4.3	**Tjenestespesifikasjon** Leverandøren skal i etableringsprosjektet utarbeide en tjenestespesifikasjon. Tjenestespesifikasjon skal detaljere alle relevante forhold ved Tjenesten, inkludert funksjonelle forhold. a. lagringstid for Produksjonsdata og data om Ekstern kunde, b. tilgangskontroll, c. eventuelle spesialtilpasninger til Kunden eller funksjonelle utvidelser som er tatt i bruk Tjenestespesifikasjonen skal etableres i etableringsprosjektets tidsplan og skal oppdateres ved endringer i Tjenesten.	A	Egenerklæring

Vurdering av B-krav nummer 4.1:

Det vil vurderes hvor godt leverandørens testplaner sikrer en god prosess for samarbeid og involvering av kunden, tydelig ansvarsfordeling, håndtering og eskalering av feil m.v.

Vurdering av B-krav nummer 4.2:

Det vil vurderes hvor godt leverandørens overordnede fremdriftsplan sikrer at tjenesten blir etablert i produksjon innen ønsket frist.

5 Krav til Informasjonssikkerhet og personvern

Lånekassens evne til å utføre inn- og utbetalinger er svært viktig for vår kundemasse og en forutsetning for at Lånekassen skal klare å levere på sitt samfunnsoppdrag. Tjenester som understøtter denne kapabiliteten, må derfor ivareta informasjonssikkerhet og personvern på en betryggende og god måte gitt det komplekse og dynamiske trusselbildet.

Krav nr	Krav til Informasjonssikkerhet og personvern	Prioritet (A, B)	Dokumentasjon
5.1	**Overordnet** Leverandøren har et selvstendig ansvar for å holde sikkerhetsnivået i Tjenesten som tilbys på et tilstrekkelig og forsvarlig godt nivå, med utgangspunkt i avtalens vilkår og gjeldene krav til lov- og forskriftspliktig sikring. Leverandøren skal proaktivt bidra til å foreslå forbedringer i Tjenesten knyttet til svakheter og sårbarheter i teknologi eller organisatoriske prosesser der det vil bidra til å redusere sikkerhetsrisiko.	A	Egenerklæring
5.2	**Konfidensialitet, Integritet og Tilgjengelighet** Leverandøren skal ha god forståelse for underliggende risiko og skal dokumentere hvordan Tjenesten tar hensyn til: a. konfidensialitet, b. tilgjengelighet, c. integritet Dokumentasjonen skal kunne tilgjengeliggjøres for Kunde ved forespørsel.	A	Egenerklæring
5.3	**Digitale angrep** Leverandøren skal ha prosesser, rutiner og kontroller på plass for å kunne forhindre, begrense og oppdage digitale angrep og innbrudd.	A*	Leverandøren skal beskrive hvordan dette kravet vil ivaretas slik at oppfyllelse kan kontrolleres av kunden.

Krav nr	Krav til Informasjonssikkerhet og personvern	Prioritet (A, B)	Dokumentasjon
5.4	**Håndtering av sårbarheter** Leverandøren skal ha prosesser, rutiner og kontroller for å opprettholde en sikker konfigurasjon og for håndtering av sårbarheter og svakheter i Tjenesten som tilbys.	A*	Leverandøren skal beskrive hvilke rutiner og kontroller som finnes for sikkerhetsoppdatering og herding av løsningen. Herunder hyppighet, testing og varsling.
5.5	**Sikkerhetsbrudd** Leverandøren skal ha mekanismer på plass for å kunne monitorere og oppdage uønskede hendelser (tilsiktede og utilsiktede), og skal ha mekanismer på plass som forhindrer at Leverandøren benyttes som inngang for å infiltrere Kundens infrastruktur.	A	Egenerklæring

Krav nr	Krav til Informasjonssikkerhet og personvern	Prioritet (A, B)	Dokumentasjon
5.6	**Sikkerhetsbrudd - varsling** Dersom Leverandør oppdager sikkerhetsbrudd eller brudd på krav til personvern, skal Leverandør uten ugrunnet opphold varsle Kunden. Tiltak skal iverksettes snarest for å gjenopprette normal tilstand og hindre gjentakelse. Skriftlig rapport på hendelsen skal sendes Kunden uten ugrunnet opphold etter at sikkerhetsbruddet ble oppdaget. Dersom hendelsen ikke er løst, skal ny rapport oversendes etter at hendelsen er løst.	A	Egenerklæring
5.7	**Tilgangskontroll hos Leverandør** Leverandør skal ha implementert effektive og moderne kontroller for fysisk og logisk tilgangskontroll. Kontrollen skal omfatte all tilgang til Tjenesten. Bare godkjent personell skal ha tilgang til Tjenesten og Tjenestens Produksjonsdata. Tilgangen skal være begrenset til det som er nødvendig for å utføre pålagte oppgaver. Tilgangen må kunne kontrolleres og logges på individnivå, og sikres med sterke autentiseringsmetoder. Kunden skal på forespørsel få	A	Egenerklæring

Krav nr	Krav til Informasjonssikkerhet og personvern	Prioritet (A, B)	Dokumentasjon
	innsikt i hvem hos Leverandøren som har tilgang med begrunnelse for tjenestlig behov.		
5.8	**Sporbarhet** Det skal være tilstrekkelig sporbarhet og logging ved Tjenesten. Lese- og skrivehandlinger skal være sporbart på individnivå, herunder autorisasjoner (på og avlogginger), tilgangskontroll, transaksjoner og sporbarhet på hvem som åpner, endrer eller kopierer filer. Ved sikkerhetsbrudd skal det være mulig å spore hvilke opplysninger som har blitt eksponert. Kunden skal ha innsyn i logger ved forespørsel.	A	Egenerklæring
5.9	**Kryptering** Kommunikasjon mellom kundens Tjenester og aksesspunkt skal være sikker og kryptert og beskyttelsen skal samsvare med sikkerhetsnivå fastsatt av PEPPOL Payment-standarden.	A*	Leverandøren skal beskrive hvordan dette kravet vil ivaretas slik at oppfyllelse kan kontrolleres av kunden.
5.10	**Kontinuitet og beredskap** Leverandøren skal ha en krise- og beredskapsplan som dekker krisesituasjoner, håndtering av sikkerhetsbrudd, strømbrudd, backupløsning og reservedriftsløsninger. Planverket skal omfatte kontrolltiltak for å identifisere og redusere risikoer, begrense konsekvensene av ødeleggende hendelser og sikre rask gjenopprettelse av viktige driftsprosesser. Det forventes at Leverandørens planer er i samsvar med krav til SLA.	A*	Leverandøren skal beskrive hvordan dette kravet vil ivaretas slik at oppfyllelse kan kontrolleres av kunden.

Krav nr	Krav til Informasjonssikkerhet og personvern	Prioritet (A, B)	Dokumentasjon
5.11	**Fysisk sikkerhet** Leverandøren skal sørge for at datasentre er tilstrekkelig beskyttet mot fysisk inntrengning, gjennom fysiske barrierer og adgangskontroll slik at Kundens data er sikret mot fysiske innbrudd.	B	Leverandørens skal beskrive hvordan dette kravet ivaretas og vedlegge eventuelle sertifiseringer (TIER-level, ISO27001 og lignende).
5.12	**Sikring av integrasjoner** I Digitaliseringsrundskrivet er det satt føringer for digitalisering i offentlig sektor og det fremgår at Maskinporten anbefales. Implementering av integrasjoner mellom Tjenesten og Kundens infrastruktur sikres ved hjelp av Maskinporten (API-sikring).	B	Leverandørens skal beskrive hvordan dette kravet ivaretas.
5.13	**Sporbarhet** Leverandøren skal sikre logger for å ivareta integritet, og begrense privilegerte brukeres mulighet til å endre eller slette logger.	B	Leverandørens skal beskrive hvordan dette kravet ivaretas.
5.14	**Single Sign On (SSO)** Tjenestens verktøy for å monitorere meldingsflyt skal ha støtte for "single sign-on" (SSO) som er kompatibelt med Kundens systemer, som er etablert og testet innen leveringsdag. Kunden benytter Azure AD (AAD). Leverandøren bes beskrive Tjenestenes støtte for SSO.	B	Leverandørens skal beskrive hvordan dette kravet ivaretas.

Krav nr	Krav til Informasjonssikkerhet og personvern	Prioritet (A, B)	Dokumentasjon
5.15	**Sikkerhetstest og penetrasjonstest** Leverandøren skal ha rutiner for sikkerhetstesting av tjenesten enten utført av uavhengig tredjepart eller egen testing hvor Kunde skal ha innsyn i overordnet testmetodikk. Kunden skal gjøres kjent med resultat av slik testing ved større endring av infrastruktur, og minst én gang i året. Avdekkede sikkerhetshull skal håndteres umiddelbart.	B	Leverandørens skal beskrive hvordan dette kravet ivaretas og hvilke rutiner som er etablert for for gjennomføring, håndtering og rapportering av testresultater.
5.16	**Informasjonssikkerhetsledelse** Leverandøren bør ha et dokumentert styringssystem for informasjonssikkerhet (SSIS). Dette skal danne grunnlaget for en helhetlig, planlagt, systematisk og dokumentert måte å arbeide med informasjonssikkerhet for Tjenestene Kunden kjøper. Leverandørens SSIS skal omfatte styring og kontroll over de tjenestene som tilbys Kunden. Styringssystemet bør være basert på anerkjent standard, slik som ISO 27001 eller tilsvarende.	B	Leverandøren skal beskrive hvordan dette kravet blir ivaretatt, og hvordan Leverandørens SSIS fører til godt ivaretatt sikkerhet for Kundens filer. Beskrivelsen skal spesielt legge vekt på hvordan Leverandøren arbeider for å forbedre sikkerheten i sine tjenester basert på et trusselbilde i stadig endring, og hvordan Leverandøren arbeider for å tilfredsstille Kundens sikkerhetskrav. Leverandøren skal i tillegg legge ved eventuelle sertifikater, scope-beskrivelser og anvendelses-erklæring (statement of applicability).

Vurdering av B-krav til kapittel 5:

Det vil vurderes hvor godt leverandøren møter etablert beste praksis og informasjonssikkerhets-standardarder, hvor formålet er forsvarlig og tilstrekkelig beskyttelse av Kundens informasjonsverdier.

6 Tjenestenivå (SLA), standardiserte kompensasjoner m.v.

Lånekassen vil basere seg på Leverandørens standard SLA/tjenestenivå med standardiserte kompensasjoner. Beskrivelse av tjenestenivå skal gis i avtalens Bilag 4, og må minimum inneholde følgende:

- Service Management
- Tilgjengelighet
- Responstider for tjenesten
- Metode og system for overvåkning av tjenesten med tanke på tilgjengelighet/feil og responstider/tregheter
- Reaksjonstider for henvendelser og feilsituasjoner
- Rapportering
- Endringshåndtering
- Vedlikeholdshåndtering
- Kundestøtte
- Kompensasjonsregime

Evaluering av oppfyllelse vil gjøres skjønnsmessig basert på en helhetlig vurdering av tilbudt nivå og kvalitet.