Husbanken

Kundens kravspesifikasjon

Andre krav

Bilag 1B til tilpasningsavtalen for lånesystem

INNHOLD

1. BRUKEROPPLEVELSE OG BRUKSKVALITET

Brukeren i sentrum

Husbanken skal sette brukeren i sentrum. Brukeren kan være innbyggere, egne ansatte, andre offentlige og private virksomheter, etc. Vi skal sikre at tjenesten oppfyller deres behov.[1]

Dette betyr at brukerne må kunne bruke løsningen, det vil si at:

- Løsningen er universelt utformet og tilpasset.
- Løsningen er kompatibel med brukernes utstyr.

Det betyr også at løsningen skal være utformet slik at den er enkel å sette seg inn i og bruke.

- Løsningen er brukervennlig.
- Løsningen er tilgjengelig på norsk og har et klart og brukertilpasset språk.
- Løsningen inneholder hjelp og veiledning til å bruke den.

Til slutt betyr det også at løsningen skal være utformet slik at det gir en positiv bruksopplevelse. Det betyr blant annet at løsningen er rask og ikke «henger».

1.1. Universell utforming og brukertilpasning

Eventuelle selvbetjeningsløsninger skal være universelt utformet slik at flest mulig skal kunne benytte seg av tjenestene til Husbanken[2]. Funksjonalitet rettet mot Husbankens egne ansatte bør også være universelt utformet og tilrettelagt slik at også personer med funksjonsnedsettelse har mulighet til å få eller beholde arbeid.[3]

Nr.	Krav
1.1	Systemet i sin helhet skal være universelt utformet. Tjenesten skal utformes i samsvar med Web Content Accessibility Guidelines 2.0 (WCAG 2.0)/NS/ISO/IEC 40500:2012 på nivå A, AA og AAA.[4] Leverandøren skal i Bilag 2B beskrive i hvilken grad og hvordan de sikrer universell utforming og brukertilpasning. Hvis deler av løsningen ikke tilfredsstiller noen av kravene, skal leverandøren angi hvilke det er snakk om og hva avvikene består i.
1.1.1	Systemet skal utforme ferdigstilte tekstdokumenter i henhold til PDF/UA (ISO 14289).
1.1.2	Eventuelle selvbetjeningsløsninger skal være universelt utformet. Tjenesten skal som minimum utformes i samsvar med Web Content Accessibility Guidelines 2.0 (WCAG 2.0)/NS/ISO/IEC 40500:2012 på nivå A og AA med unntak for suksesskriteriene 1.2.3, 1.2.4 og 1.2.5.18.[5]
1.1.3	Systemet og brukerrettet skriftlig materiell skal være på norsk.
1.1.4	Systemet og skriftlig materiell skal være på klart språk.[6] [7]

[1]
[2] Likestillings- og diskrimineringsloven §§ 17 og 18.
[3] Likestillings- og diskrimineringsloven §§ 22 og 26.
[4] Referansekatalogen
[5] Forskrift om universell utforming av IKT-løsninger § 4 1. ledd.
[6] Avsnitt 1.1 i H-7/17 Digitaliseringsrundskrivet avsnitt, Kommunal- og moderniseringsdepartementet 8.9.2017
[7] Avsnitt 4.4.5 i Virksomhets- og økonomiinstruks for Husbanken, Kommunal- og moderniseringsdepartementet 26.5.2014

Nr.	Krav
1.1.5	Systemet skal utforme selvbetjeningsløsninger og korrespondanse i brukerens foretrukne målform (bokmål eller nynorsk).[8]
1.1.6	Systemet skal definere hvilket språk nettsider er skrevet i ved hjelp av ISO 639 slik at siden kan leses opp og oversettes. For språk med språkkoder i ISO 638-1 (to bokstavers kode), skal denne brukes. Entydige koder skal brukes fremfor språkgruppekoder. Det betyr at det må skilles mellom ulike samiske språk og mellom bokmål og nynorsk.[9]

1.2. Brukervennlighet

Brukervennlighet sikrer at brukerne får gjort det de skal raskt og effektivt på en måte som oppleves positivt. Det betyr at systemet skal være:

1. Lett å lære seg
2. Effektivt i bruk
3. Lett å huske hvordan man bruker
4. Sikrer at man ikke gjør unødvendige feil og at det er lett å rette feil man har gjort
5. Behagelig i bruk

I selvbetjeningsløsninger er det at løsningen er lett å lære seg viktigere enn at det er effektivt i bruk, mens det for interne brukere som skal bruke systemet mye er det omvendt.

Nr.	Krav
1.2	Systemet skal være brukervennlig. Leverandøren skal i Bilag 2B beskrive sine prinsipper og fremgangsmåter for brukerinteraksjonsdesign og brukervennlighet.
1.2.1	I eventuelle selvbetjeningsløsninger skal minst 90 prosent av brukerne med grunnleggende digitale ferdigheter kunne ferdigstille samtlige funksjoner på under 5 minutter uten å ha benyttet løsningen fra før, fått opplæring eller veiledning.
1.2.2	Systemet skal være effektivt å bruke uten pekeenhet slik at musearm unngås og man kan arbeide raskt i systemet. De 80 prosent mest benyttede funksjonene skal være tilgjengelig med hurtigtaster.
1.2.3	Systemet skal sikre at den den enkelte bruker har sine mest brukte funksjoner lett tilgjengelig.
1.2.4	Eventuelle selvbetjeningsløsninger skal ha brukergrensesnitt som er i henhold til Husbankens designprofil slik at Husbankens selvbetjeningsløsninger gir en enhetlig og helhetlig brukeropplevelse.
1.2.5	Eventuell korrespondanse skal følge Husbankens grafiske profil som beskrevet i den vedlagte profilhåndboken slik at Husbanken fremstår samordnet og enhetlig.

[8] Mållova § 6.
[9] Referansekatalogen

1.3. Kompatibilitet

Nr.	Krav
1.3.1	Eventuelle selvbetjeningsløsninger skal være tilpasset bruk på smarttelefoner, nettbrett og personlige datamaskiner, helst gjennom adaptiv design. Leverandøren skal i Bilag 2B beskrive hvordan løsningen er tilpasset ulike typer enheter.
1.3.2	Selvbetjeningsløsningen skal være tilgjengelig på alle plattformer (operativsystem og eventuelle nettlesere) som står for mer enn to prosent av bruken i Norge. Leverandøren skal i Bilag 2B: • beskrive hvordan kompatibilitet av selvbetjeningsløsningen med de mest utbredte plattformene er sikret. • beskrive hvilke plattformer (operativsystem, nettleser) selvbetjeningsløsningen vil være tilgjengelig på.
1.3.3	Systemet skal utforme nettsider i HTML 5.0 formatert ved hjelp av CSS 3. [10] De skal være implementert slik at den kan vises i lesbar og funksjonell form i en nettleser med bare støtte for HTML 4.01 (W3C 1999) og/eller CSS2.[11]
1.3.4	Systemet skal bruke UTF-8 (ISO/IEC 10646) som tegnsett[12].
1.3.5	Systemet skal bruke JPEG (ISE/IEC 10918-1:1994) eller PNG (ISO/IEC 15948:2003) for alle bilder på eventuelle selvbetjeningsløsninger.[13]
1.3.6	Systemet skal utforme ferdigstilte tekstdokumenter i PDF 1-4 1-6. PDF 1.7 (ISO 32000-1:2008) eller PDF/A (ISO 19500-1:2005).[14]
1.3.7	Systemet skal utforme ferdigstilte, ikke-signerte, arkivverdige tekstdokumenter i PDF A-1a eller b (ISO 19005-1) eller PDF A-2a, b eller u (ISO 19005-2) slik at de er i format som egner seg for arkivering.[15]
1.3.8	Systemet skal utforme ferdigstilte, signerte, arkivverdige tekstdokumenter i PDF A-2a, b eller u (ISO 19005-2) og PAdES (ETSI TS 102 778) slik at de er i format som egner seg for arkivering og er like bindende som dokumenter med håndskrevne signaturer. [16]

1.4. Ytelse

Nr.	Krav
1.4	Systemet skal fremstå som raskt og responsivt. Leverandøren skal i Bilag 2B beskrive hvordan ytelse ivaretas i systemet og hvordan det kan overvåkes i ordinær drift.
1.4.1	Systemet skal gjøre det mulig å foreta endringer og navigere fra side til side på under 0,5 sekund med en forbindelse med båndbredde på 2 Mbit/s og latenstid på 100 ms.
1.4.2	Systemet skal ikke bruke mer enn 1 sekund på å lagre.

[10] Referansekatalogen
[11] Forskrift om IT-standarder i offentlig forvaltning § 4
[12] Forskrift om IT-standarder i offentlig forvaltning § 8 og 9
[13] Forskrift om IT-standarder i offentlig forvaltning § 6.
[14] Forskrift om IT-standarder i offentlig forvaltning § 5
[15] Riksarkivarens forskrift §§ 5-17 og 5-18.
[16] Riksarkivarens forskrift §§ 5-17 og 5-18.

Nr.	Krav
1.4.3	Systemet skal ikke bruke mer enn 2 sekunder på å ta ut en rapport.

2. INFORMASJONSSIKKERHET OG PERSONVERN

Virksomhetskritisk beskyttelsesbehov

Systemet som helhet har et virksomhetskritisk beskyttelsesbehov, og klassifiseres dermed med sikkerhetsnivå høy. Systemet inneholder særlige kategorier av personopplysninger som det er strenge krav til beskyttelse av for å ivareta personvernet. Systemet er også et økonomisystem som må beskyttes for å hindre økonomisk kriminalitet som svindel, tyveri og underslag.

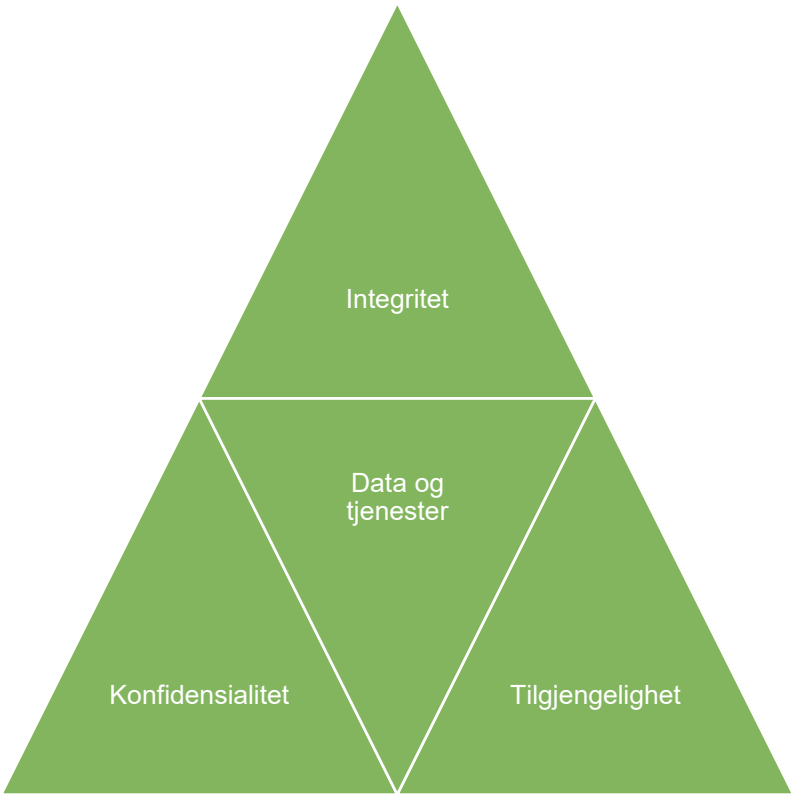
Informasjonssikkerhet

Integrasjonssikkerhet består i å sikre konfidensialitet, integritet og tilgjengelighet på systemet og dataene i systemet både mot ulykker og mot ondsinnede handlinger.

Konfidensialitet betyr at informasjon som skal behandles fortrolig eller skal holdes hemmelig ikke kommer på avveie. I dette systemet gjelder dette blant annet personopplysninger og mulige forretningshemmeligheter hos lånesøkere. Konfidensialitet betyr også at ingen får anledning til å gjøre noe de ikke har myndighet til, for eksempel å utbetale penger til seg selv.

Integritet betyr at dataene er korrekte, gyldige og fullstendige og at systemet fungerer som det skal. Det skal for eksempel ikke være mulig å endre data uten at man har myndighet til å gjøre dette.

Tilgjengelighet betyr at dataene og funksjonene er der når man har behov for dem.



Personvern

Personvern er ivaretagelse av personlig integritet og enkeltindividers mulighet for privatliv, å bestemme over seg selv og utfolde seg som de måtte ønske. Man har rett på en privat sfære som man selv kontrollerer. Dette betyr at du har behov for vern av dine **personopplysninger**, opplysninger der du er identifisert eller kan identifiseres. Man må kunne vite og bestemme når, hvordan og hvor mye informasjon om deg som blir spredd. Dette gjelder spesielt **særlige kategorier** av personopplysninger som[17]

- rasemessig eller etnisk opprinnelse
- politisk oppfatning
- religion eller filosofisk overbevisning
- fagforeningsmedlemskap
- genetikk eller med formål om å entydig identifisere en fysisk person

[17] Personvernforordningen artikkel 9

- helse
- seksuelle forhold eller seksuelle orientering

Sikkerhetsnivå

Systemet som helhet har et virksomhetskritisk beskyttelsbehov. Det har sikkerhetsnivå høy. Høy er det høyeste av Husbankens sikkerhetsnivåer:

- **Høy** – virksomhetskritisk beskyttelsesbehov
- **Middels** – beskyttelsesbehov
- **Lavt** – lite eller ingen beskyttelsesbehov

Grunnen til sikkerhetsnivået er Høy, er at systemet inneholder særlige kategorier av personopplysninger og er et økonomisystem der store beløp forvaltes. Noen av Husbankens ordninger er slik at Husbanken må behandle opplysninger om helse. I tillegg vil de med lån til ektepar og partnere være mulig å si noe om seksuell orientering.

Hvis løsningen leveres som et sett av klart adskilte komponenter, kan graden av beskyttelsesbehov variere fra komponent til komponent. Av de logiske komponentene identifisert i denne kravspesifikasjonene, bedømmer vi følgende til å kreve sikkerhetsnivå høy på grunn av at komponentene kan inneholde særlige kategorier av personopplysninger:

- låneavtale
- lånereskontro
- mislighold
- part
- dokument
- signatur
- saksbehandling

I tillegg må også kundereskontro kreve sikkerhetsnivå høy på grunn av fare for økonomisk tap. Dette gjelder også flere av komponentene nevnt over.

Øvrige komponenter anses å ha sikkerhetsnivå Middels.

2.1. Skallsikring

Systemet skal ha en minst mulig angrepsflate slik at det blir mindre sårbar for innbrudd. Tjenere, klienter og nettverk skal være herdet mot innbrudd. Dette betyr at:

- Alt er i utgangspunktet stengt
- Ting holdes mest mulig adskilt slik at et vellykket innbrudd gir minst mulig tilgang
- Det ikke benyttes systemkontoer med flere privilegier enn nødvendig
- Usikre protokoller som telnet og http ikke skal benyttes i kommunikasjon
- Usikker programvare som Flash og Java i nettlesere ikke skal benyttes

Logiske skiller

I Kundens tekniske plattform benyttes virtualisering (VMWare) og containerteknologi (OpenShift, bare på Linux) for å legge til rette for klare skiller mellom ulike tjenester uten at det gir økte kostnader.

Nettverkssikkerhet

Kundens nettverk er inndelt i soner og det benyttes brannmurer for å gi sikre skiller med filtrering på adresser, protokoller og trafikkretning.

For ekstern kommunikasjon filtreres også ulovlige tjenester og uønsket informasjon. For delene av systemet som krever et høyt sikkerhetsnivå, skal det være doble barrierer. Dette betyr at eventuelle selvbetjeningsløsninger og eksternt rettede tjenester legges i en demilitarisert sone, DMZ. I Kundens tekniske plattform benyttes en omvendt proxy implementert ved hjelp av Apache HTTP Server og ModSecurity som den andre barrieren.

Skadevare

I Kundens tekniske plattform benyttes Windows Defender for å sørge for at klienter og tjenere er fri for skadevare. Innkommende filer eksternt fra, skannes i tillegg ved hjelp av mod_clamav for ytterligere sikkerhet.

Nr.	Krav
2.1.1	Systemet skal utnytte sikkerhetsmekanismene som finnes i infrastruktur og plattform. Funksjonalitet og data for ulike tjenester skal holdes adskilt og kontoer som benyttes skal kreve minst mulig av privilegier. Leverandøren skal beskrive hvordan dette gjøres i Bilag 2B.
2.1.2	Systemet skal ikke kjøres i kontoer med flere privilegier enn det som burde være nødvendig.
2.1.3	Systemet skal ikke kreve Java i nettleser på klienten.
2.1.4	Systemet skal ikke kreve Adobe Flash på klienten.
2.1.5	Systemet skal ha god nettverkssikkerhet. Leverandøren skal beskrive hvordan dette gjøres i Bilag 2B.
2.1.6	Systemet skal ikke benytte usikre protokoller til kommunikasjon.
2.1.7	Eventuell selvbetjeningsløsning skal kunne kjøre i en demilitarisert sone eller lignende, slik at det blir doble barrierer mellom systemet og eksternt nettverk.
2.1.8	Systemets eksternt rettede tjenester skal kjøre i en demilitarisert sone eller lignende, slik at det blir doble barrierer mellom systemet og eksternt nettverk.
2.1.9	Det skal være elektronisk overvåkning av ekstern nettverkstrafikk.
2.1.10	Systemet skal ha effektive hindringer mot skadevare. Leverandøren skal beskrive hvordan dette gjøres i Bilag 2B. Leverandøren skal beskrive eventuelle begrensninger som for eksempel filer som må ekskluderes fra skanning av antivirus-programvare for å sikre tilfredsstillende ytelse.

2.2. Tilgangskontroll

Systemet skal sikre at man får tilgang til data og funksjoner i systemet hvis og bare hvis man har et tjenstlig behov for det. Dette sikrer naturlig nok konfidensialitet, men det bidrar også til integritet siden det hindrer at uvedkommende i vanvare eller av ond vilje sletter eller gjør gale endringer i informasjonen.

Tilgangskontroll består av tre steg: identifikasjon, autentisering og autorisasjon.

Identitet er et sett med egenskaper knyttet til noen eller noe som navn, fødselsnummer, organisasjonsnummer, roller i en organisasjon osv.

Autentisering er å verifisere en påstått identitet. De som skal autentisere seg må inneha noe som kan bekrefte deres identitet, en **autentiseringsfaktor**. Det finnes tre forskjellige typer autentiseringsfaktorer:

- Noe personen *vet* – for eksempel et passord
- Noe personen *har* – for eksempel en passordkalkulator
- Noe personen *er* – for eksempel et fingeravtrykk

Autorisasjon er å avgjøre hva noen skal ha tilgang til å se eller å gjøre.

Kundens tekniske plattform for tilgangskontroll

Kunden har i sin tekniske plattform løsninger for identifikasjon og autentisering som bør benyttes. Kunden benytter to ulike løsninger for brukerkatalog og autentisering:

- Active Directory - Kundens egen brukerkatalog for Kundens personell og personell i kommuneforvaltningen
- ID-porten – felles innloggingsløsning til offentlige tjenester på internett utviklet og forvaltet av Direktoratet for forvaltning og IKT (Difi). Kunden, som offentlig forvaltningsorgan, bør bruke ID-porten for digitale tjenester som krever innlogging og autentisering.[18]

Kunden bruker Red Hat Single Sign-On (RH SSO) for single sign-on. Løsningen formidler identitet til applikasjonene ved hjelp av OpenID Connect. OpenID Connect er et autentiseringslag på toppen av OAuth 2.0 som gir applikasjonene informasjon om identiteten og brukerprofilen til sluttbrukerne.

Kunden bruker grupper i Active Directory for å tildele tilganger. I selvbetjeningsløsninger brukes roller i AltInn for å gi tilganger til fysiske personer på vegne av juridiske personer.

Krav til autentisering

I eventuelle selvbetjeningsløsninger skal autentisering være på sikkerhetsnivå[19] 3 eller 4. Dette betyr at det er krav om sterk autentisering og at det skal være gjort tiltak som sikrer at autentiseringsfaktoren har blitt tildelt rett person; se Tabell 1 nedenfor. ID-porten tilbyr både sikkerhetsnivå 3 og 4. Det høyeste nivået oppnås med Bank ID, Bank ID på mobil, Buypass og Commfides.

Nivå	Krav til autentiserings-faktor(er)	Utlevering til bruker		Sikring av autentiserings-faktorer ved lagring	Krav til offentlig godkjenning	Krav til uavviselighet
		Fysiske personer	Juridiske personer			
1	Ingen krav	Ingen krav.	Ingen krav.	Ingen krav.	Ingen krav.	Ingen krav.
2	Enfaktor	Post til folkeregistrerte adresse.	Post til enhetsregisterets registrerte adresse. Navnet til den fysiske personen som kan tegne for den juridiske personen, skal stå først på forsendelsen. Alternativt kan det sendes til den som tegners folkeregistrerte adresse.	Både statiske og dynamiske kan være kopierbare.	Ingen krav.	Det skal foreligge rutiner og logger, som gjør at det er rimelig sikkert at kommunika-sjonsparten står bak en handling eller et informasjons-element.
3	Tofaktor, hvorav en er dynamisk	Samme krav som i 2, men med ett tilleggskrav om at utsendelsesprosedyren skal ha integrert tilleggssikring som sørger for at sannsynligheten for at feil person tar løsningen i bruk minimaliseres. Det er ikke krav om personlig oppmøte.	Samme krav som i 2, 3men med ett tilleggskrav om at utsendelsesprosedyren skal ha integrert tilleggssikring som sørger for at sannsynligheten for at feil person tar løsningen i bruk minimaliseres. Det er ikke krav om personlig oppmøte.	Dynamiske kan være kopierbare. Statiske kan ikke være kopierbare.	Ingen krav.	Det skal foreligge rutiner og logger, som gjør at det er rimelig sikkert at kommunika-sjonsparten står bak en handling eller et informasjons-element.

[18] H-7/17 Digitaliseringsrundskrivet 1.6 Bruk nasjonale felleskomponenter og fellesløsninger
[19] Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, Fornyings- og administrasjonsdepartementet, April 2008

Nivå	Krav til autentiserings-faktor(er)	Utlevering til bruker		Sikring av autentiserings-faktorer ved lagring	Krav til offentlig godkjenning	Krav til uavviselighet
		Fysiske personer	Juridiske personer			
4	Tofaktor, hvorav en er dynamisk	Kravene til registrering og utleveringsprosedyrer er tilsvarende Kravspesifikasjonen for PKI, Person Høyt. Personlig oppmøte med legitimering, minst én gang.	For juridiske personer skal den fysiske personen som tegner for den juridiske, enten møte opp personlig, eller gi fullmakt til en annen som kan møte personlig på personens vegne. Det skal fremlegges legitimasjon for begge, samt sjekkes mot enhetsregisteret. Krav tilsvarende for PKI, nivå Virksomhet.	Ikke-kopierbare.	Løsningen skal være deklarert i henhold til offentlige krav.	En kommunikasjons-part skal kunne verifisere at den andre part står bake en handling eller et informasjons-element, den skal ikke selv kunne produsere eller endre på slike bevis i etterkant.

Tabell 1 Sikkerhetsnivåer for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor.

Nr.	Krav
2.2	Systemet skal sikre at brukere ikke får tilgang til systemet uten at de er korrekt identifisert, sikkert autentisert og eksplisitt autorisert til den tilgangen de får. Dette gjelder både interne og eksterne brukere av løsningen, brukere som bruker løsningen direkte og brukere som bruker den via API-er. Leverandøren skal beskrive sin løsning for identitet- og tilgangskontroll og hvilke brukerkataloger og single sign-on løsninger de støtter og hvilke begrensinger som finnes i støtten i Bilag 2B.
2.2.1	Systemet skal gjøre det mulig for brukere å logge på ved hjelp av brukernavn og passord som definert i Kundens interne brukerkatalog, slik at brukerne slipper å forholde seg til så mange brukernavn og passord, noe som bidrar til bedre passordskikk.
2.2.2	I eventuell selvbetjeningsløsning skal autentisering skje på sikkerhetsnivå 3 eller 4.
2.2.3	I eventuell selvbetjeningsløsning skal autentisering skje ved hjelp av Husbankens egen Identity Provider (RH SSO) og ID-porten.
2.2.4	Systemet skal ha single sign-on for brukere slik at brukerne slipper å logge seg inn så ofte.
2.2.5	Systemet skal ha single sign-on ved hjelp av OpenID Connect.
2.2.6	Systemets API-er nødvendig for selvbetjeningsportal skal tilby single sign-on for personell i kommuneforvaltningen autentisert i Husbankens brukerkatalog for disse brukerne.
2.2.7	Systemet skal gjøre det mulig å begrense varighet av sesjoner til en konfigurerbar verdi, slik at det blir mindre sannsynlig at noen får tilgang til systemet fra en ulåst PC eller lignende.
2.2.8	Systemet skal gjøre det mulig å begrense tilgang til kun de funksjoner og data brukeren har tjenstlig behov for.
2.2.9	Systemet skal gjøre det mulig å administrere tilganger og sett av tilganger i et grafisk brukergrensesnitt, slik at driftspersonell kan vedlikeholde strukturer i forbindelse med omorganiseringer og lignende.
2.2.10	Systemet skal gjøre det mulig å hindre at samme bruker har spesielle kombinasjoner av rettigheter på samme tid, slik at man for eksempel kan hindre at en person alene kan gjennomføre samtlige transaksjoner nødvendig i et underslag.
2.2.11	Systemet skal gi tilganger til brukere basert på grupper brukeren tilhører i Kundens interne brukerkatalog.

Nr.	Krav
2.2.12	I eventuell selvbetjeningsløsning skal brukere som er logget inn på egne vegne kun få tilgang til egne data.
2.2.13	I eventuell selvbetjeningsløsning skal brukere som er logget inn på andres vegne kun få tilgang til data til den parten de representerer.
2.2.14	Systemets API-er nødvendig for selvbetjeningsportal skal bare gi tilgang til egne data hvis brukeren er logget inn på egne vegne.
2.2.15	Systemets API-er nødvendig for selvbetjeningsportal skal bare gi tilgang til data til parten brukeren representerer når brukeren er logget inn på andres vegne.
2.2.16	I en eventuell selvbetjeningsløsning skal brukere som representerer en annen part bare få tilgang til de funksjoner som er tilordnet den rollen de innehar for parten de representerer.
2.2.17	Systemets API-er nødvendig for selvbetjeningsportal skal bare gi tilgang til de funksjoner som er tilordnet den rollen brukeren innehar når brukeren representerer en annen part.
2.2.18	Systemet skal gjøre det mulig å avslutte tilganger som ikke har vært benyttet i et tidsintervall av konfigurerbar lengde, slik at det blir mindre sannsynlig at brukere beholder tilganger de ikke lenger har tjenstlig behov for.
2.2.19	Systemet skal gjøre det mulig å vite om alle mislykkede forsøk på logge inn.
2.2.20	Systemet skal gjøre det mulig å vite hvem som var pålogget når og hvor lenge.
2.2.21	Systemet skal gjøre det mulig å vite hvem som hadde hvilke tilganger når.

2.3. Sporbarhet og uavviselighet

Systemet skal sikre at det er mulig å vite hvem som har gjort hva, slik at revisjon og etterforskning blir enklere.

Uavviselighet er å bekrefte at en handling eller et informasjonselement er uendret og at det kan knyttes til en bestemt identitet. Uavviselighet er i mange sammenhenger også omtalt som ikke-benekting.

Kunden, som offentlig forvaltningsorgan, bør bruke eSignering for elektronisk signering. eSignering er en felles tjeneste for elektronisk signering etablert av Difi. Signeringstjenesten er en frittstående tjeneste som er tilgjengelig for offentlige virksomheter. Tjenesten gjør det mulig for innbyggere å signere dokument fra det offentlige digitalt ved påføring av digital personsignatur.[20]

Nr.	Krav
2.3.1	Systemet skal sikre at det er mulig å vite hvem som utførte hvilke transaksjoner. Dette gjelder både interne og eksterne brukere av løsningen, brukere som bruker løsningen direkte og brukere som bruker den via API-er. Leverandøren skal beskrive sin løsning for sporing og uavviselighet i støtten i Bilag 2B.
2.3.2	Systemet skal sikre at det er mulig å vite hvem som har sett hva av fortrolig informasjon som for eksempel personopplysninger. Leverandøren skal beskrive sin løsning for sporing av lesing av fortrolig informasjon i støtten i Bilag 2B.
2.3.3	I eventuell selvbetjeningsløsning skal transaksjoner som kan medføre økonomisk tap være uavviselige på minimum sikkerhetsnivå 4.
2.3.4	I eventuell selvbetjeningsløsning skal transaksjoner som kan medføre økonomisk tap signeres ved hjelp av tjenesten eSignering fra Difi.

[20] https://www.difi.no/fagomrader-og-tjenester/digitale-felleslosninger/esignering

2.4. Tilgjengelighet

Systemet skal være tilgjengelig 24/7/365. Kunden tilbyr fleksitid til sitt personell som medfører at personell kan ha behov for systemet når som helst, men for de fleste kun i perioden mellom kl. 06.00 og 21.00 mandag - lørdag[21]. Systemet skal legge til rette for selvbetjening og kunder og partnere kan også ha behov for systemet når som helst.

Kunden har imidlertid begrensninger i sin tekniske plattform og beredskap som medfører at det kan være noe nedetid. Kunden har ikke personell på vakt utenom normal åpningstid.

Oppetidskrav med utgangspunkt i 24/7/365 tilgjengelighet med unntak av planlagte oppdateringer en kveld per måned.

Ved katastrofe som gjør datasenter i Drammen utilgjengelig, skal Husbanken kunne gjenopprette systemer innen 8 timer til 2 døgn avhengig av kritikalitet av systemene. Husbanken har derfor et ekstra datasenter i Oslo og replikerer over en gang hvert døgn. Dette betyr at det kan være noe datatap.

Nr.	Krav
2.4	Systemet skal være tilgjengelig 24/7/365 bortsett fra eventuell planlagt nedetid i perioden mellom kl. 16.00 og 23.00 forbindelse med månedlige driftsdager, Leverandøren skal i Bilag 2B beskrive hvordan systemet sikrer høy tilgjengelighet gitt Kundens tekniske plattform og beredskap.
2.4.1	Løsningen skal ha 99,9 prosent oppetid i åpningstiden over et år.
2.4.2	Løsningen skal ha 99 prosent oppetid utenom åpningstiden fratrukket planlagt nedetid over et år.
2.4.3	Løsningen skal kunne gjenopprettes innen åtte timer etter en katastrofe som gjør det primære datasenteret utilgjengelig.

2.5. Personvern

Systemet skal til enhver tid tilfredsstille gjeldende lovpålagte krav som gjelder personvern. Systemet skal også være tilrettelagt for at Kunden kan oppfylle sine forpliktelser etter personvernregelverket.

Kunden har hjemmel i Husbankloven til å behandle følgende opplysninger:

- opplysninger om navn, adresse, telefonnummer, e-postadresse, kundenummer, reservasjonsstatus for digital post, kontonummer, målform og fødselsnummer
- opplysninger om eventuell verge og den rettslige handleevnen til søkeren i økonomiske forhold
- opplysninger om inntekt, formue, skatt og gjeld, herunder opplysninger om inntekt fra Arbeids- og velferdsetaten
- andre opplysning økonomiske forhold
- opplysninger om offentlige ytelser
- opplysninger om arbeidsforhold
- opplysninger om oppholdstillatelse og -rett, og bakgrunnen for gitte tillatelser og retter
- opplysninger om bosted, bo- og sosial tilhørighet
- opplysninger om utdannelse

[21] Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. §§ 10-10 – 10.11

Tilgangen gjelder også for ektefelle, samboer, hjemmeboende barn og andre husstandsmedlemmer. I tillegg kan Kunden ved samtykke innhente helseopplysninger. [22] Det må legges til grunn at det vil bli behandlet særlige kategorier personopplysninger.

Nr.	Krav
2.5	Systemet skal til enhver tid tilfredsstille gjeldende lovpålagte krav som gjelder personvern. Systemet skal også være tilrettelagt for at Kunden kan oppfylle sine forpliktelser etter personvernregelverket. Leverandøren skal i Bilag 2B bekrefte at systemet er utviklet slik at Kunden kan oppfylle de registrertes rettigheter. Leverandøren skal beskrive systemets løsning for å håndtere innsynsbegjæringer, krav om begrensning av behandlingen samt retting og sletting av enkeltopplysninger. Videre skal det redegjøres for om systemet gir støtte for å underrette mottagere av personopplysninger om retting, sletting og begrensning av behandlingen. Dersom det er gjennomført en DPIA for systemet som kunden kan få tilgang til og benytte gis det opplysninger om det.
2.5.1	Systemet skal ha innebygget personvern og personvernvennlige standardinnstillinger. Leverandøren skal i Bilag 2B beskrive hvordan dette er ivaretatt.
2.5.2	Systemet skal gi mulighet til å slette personopplysninger. Både hele saker og saksopplysninger eldre enn en gitt dato må kunne slettes. Det vil være en fordel om også enkeltopplysninger kan slettes etter en angitt tid. Leverandøren skal i Bilag 2B beskrive mulighetene for sletting, avidentifisering, pseudonymisering og tilgangsbegrensing som finnes i systemet..
2.5.3	Systemet skal være utviklet slik at Kunden kan ivareta de registrertes rettigheter på en hensiktsmessig måte.
2.5.4	Systemet skal registrere kilden til personopplysninger som finnes i systemet.
2.5.5	Systemet skal gi mulighet for retting av personopplysninger som ikke er korrekte.
2.5.6	Systemet skal gi mulighet for å hente ut opplysninger knyttet til en enkelt registrert ved innsynsbegjæringer.
2.5.7	Systemet skal ikke behandle personopplysninger utover de opplysningstyper som er angitt ovenfor (de Husbankloven gir hjemmel til å behandle). Leverandøren skal i Bilag 2B oppgi eventuelle avvik og hvordan løsningen kan tilpasses slik at det ikke blir mulig å legge inn/generere opplysningene.
2.5.8	Systemet skal begrense bruken av informasjonskapsler. Leverandøren skal redegjøre for bruken, hvordan lovpålagte krav ivaretas og hva det er mulig å skru av/tilpasse
2.5.9	Systemet skal ikke ha fritekstfelt hvis formål er legge inn personopplysninger.

[22] Lov om Husbanken § 10

3. VEDLIKEHOLDBARHET OG DRIFTBARHET

3.1. Vedlikeholdbarhet

Nr.	Krav
3.1	Løsningen skal være vedlikeholdsvennlig. Leverandøren skal i Bilag 2B beskrive hvordan løsningen støtter dette kravet.
3.1.1	Løsningen skal ha en suite med dokumenterte, automatiserte akseptansetester som gjøre tilgjengelig for Kunden og som Kunden kan tilpasse og supplere slik at Kunden kan kjøre disse selv i en løsningen med Kundens konfigurasjon i forbindelse med regresjonstest ved nye utgaver.
3.1.2	Løsningen skal gjøre det mulig for Kunden å ha flere utviklings- og testmiljøer slik at Kunden kan teste flere utgaver samtidig og kan foreta ulike utviklings- og testaktiviteter samtidig.

3.2. Driftbarhet

Nr.	Krav
3.2	Løsningen skal ha gode driftsegenskaper. Leverandøren skal i Bilag 2B beskrive hvordan løsningen støtter dette kravet.
3.2.1	Løsningen skal kunne kjøre på Kundens tekniske plattform. Leverandøren skal i Bilag 2B beskrive den tekniske plattformen de anbefaler at løsningen skal kjøre på og også hvilke andre plattformer og hvilke versjoner av disse løsningen kan kjøre på. Leverandøren skal i Bilag 2B beskrive hvilke VM-er det er behov for med krav til antall prosessorkjerner og mengde med minne og lagring.
3.2.2	Systemet skal være slik at alle opplysninger som utgjør deler av regnskapet oppbevares i Norge, Danmark, Finland, Island eller Sverige.[23]
3.2.3	Systemet skal være slik at alle personopplysninger kun oppbevares og behandles i • EØS • stater, territorier eller sektorer i tredjestat som Kommisjonen har bestemt har et tilstrekkelig beskyttelsesnivå i henhold til personopplysningslovens artikkel 45 • i virksomheter omfattet av nødvendige garantier i henhold til personopplysningslovens artikkel 46
3.2.4	Systemet skal være slik at hvis personopplysninger oppbevares og behandles utenfor Norge så skal det ikke kreve mer enn tre måneder og 500 000 kroner å endre hvor personopplysninger oppbevares og behandles slik at man ikke kommer i strid med personopplysningslovens kapittel 5.
3.2.5	Alle applikasjonslogging skal skje i Splunk.
3.2.6	Systemet skal ikke logge personopplysninger i Splunk.

[23] Forskrift om bokføring § 7-5, Forskrift om oppbevaring av elektronisk regnskapsmateriale i andre EØS-land § 1

4. PROSJEKTGJENNOMFØRING

4.1. Datakonvertering

Avtalens punkt 2.3.8

Grunndata, aktive saker og transaksjoner skal konverteres. Kunden har ansvar for å trekke ut, vaske, dokumentere og tilgjengeliggjøre data fra eksisterende systemer. Leverandøren har ansvar for omforming og lasting av data i systemet, samt prøvekonvertering.

Nr.	Krav
4.1	Leverandøren skal konvertere grunndata, aktive saker og transaksjoner inn i nytt system. Leverandøren skal i Bilag 2B beskrive hvordan konvertering vil bli gjennomført, inklusive Kundens leveranser og teststrategi.

4.2. Dokumentasjon

Avtalens punkt 2.3.6

Systemet skal leveres med dokumentasjon Kundens personell har behov for å kunne bruke, drifte og forvalte systemet.

Nr.	Krav
4.2.1	Systemet skal leveres med en innføring og håndbok for sluttbrukere slik at de kan sette seg inn i systemet og slå opp hvordan de kan gjennomføre arbeidsoppgavene sine.
4.2.2	Systemet skal leveres med en innføring og håndbok for driftspersonell slik at de kan sette seg inn i systemet og slå opp hvordan de kan gjennomføre arbeidsoppgavene sine.
4.2.3	Systemet skal leveres med håndbok for funksjonelle ressurser slik at de kan slå opp hvordan de kan gjennomføre endringer i funksjonelt oppsett.
4.2.4	Systemet skal leveres med dokumentasjon av samtlige API-er slik at utviklere kan integrere systemet med andre system og tjenester.
4.2.5	Systemet skal leveres med dokumentasjon av relevante deler av datamodellen slik at utviklere kan utarbeide rapporter og ETL til datavarehus.
4.2.6	Systemet skal leveres med dokumentasjon av alle felter i dokumenter som genereres i løsningen slik at utviklere kan utarbeide maler for fletting og formatering av dokumentene.
4.2.7	Systemet skal leveres med dokumentasjon av samtlige løsninger for å tilpasse systemet sik at utviklere kan utarbeide utvidelser i funksjonalitet.
4.2.8	Systemet skal leveres med dokumentasjon av eventuelle prosessmotororer og regelmotorer slik at Kundens personell kan foreta endringer i forretningsprosesser og -regler.
4.2.9	Systemet skal leveres med en ROS-analyse for informasjonssikkerhet og personvern.
4.2.10	Systemet skal leveres med dokumentasjon av dataflyt for personopplysninger inn og ut av systemet.

4.3. Opplæring

Avtalens punkt 2.3.7

Systemet skal leveres med den opplæring Kundens personell har behov for å kunne bruke, drifte og forvalte systemet.

Nr.	Krav
4.3.1	Systemet skal leveres med opplæring til sluttbrukere slik at de er i stand til å ta i bruk løsningen til å utføre sine arbeidsoppgaver. Leverandøren skal beskrive sitt opplegg i Bilag 2B.
4.3.2	Systemet skal leveres med opplæring til driftspersonell slik at de er i stand til å ta i drifte løsningen. Leverandøren skal beskrive sitt opplegg i Bilag 2B.
4.3.3	Systemet skal leveres med opplæring til forvaltningspersonell slik at de er i stand til å forvalte løsningen. Leverandøren skal beskrive sitt opplegg i Bilag 2B.

4.4. Deponering

Avtalens punkt 10.2.2

Systemet skal deponeres, jf. avtalens punkt 10.2.2.

Nr.	Krav
4.4	Systemet skal deponeres, jf. avtalens punkt 10.2.2.