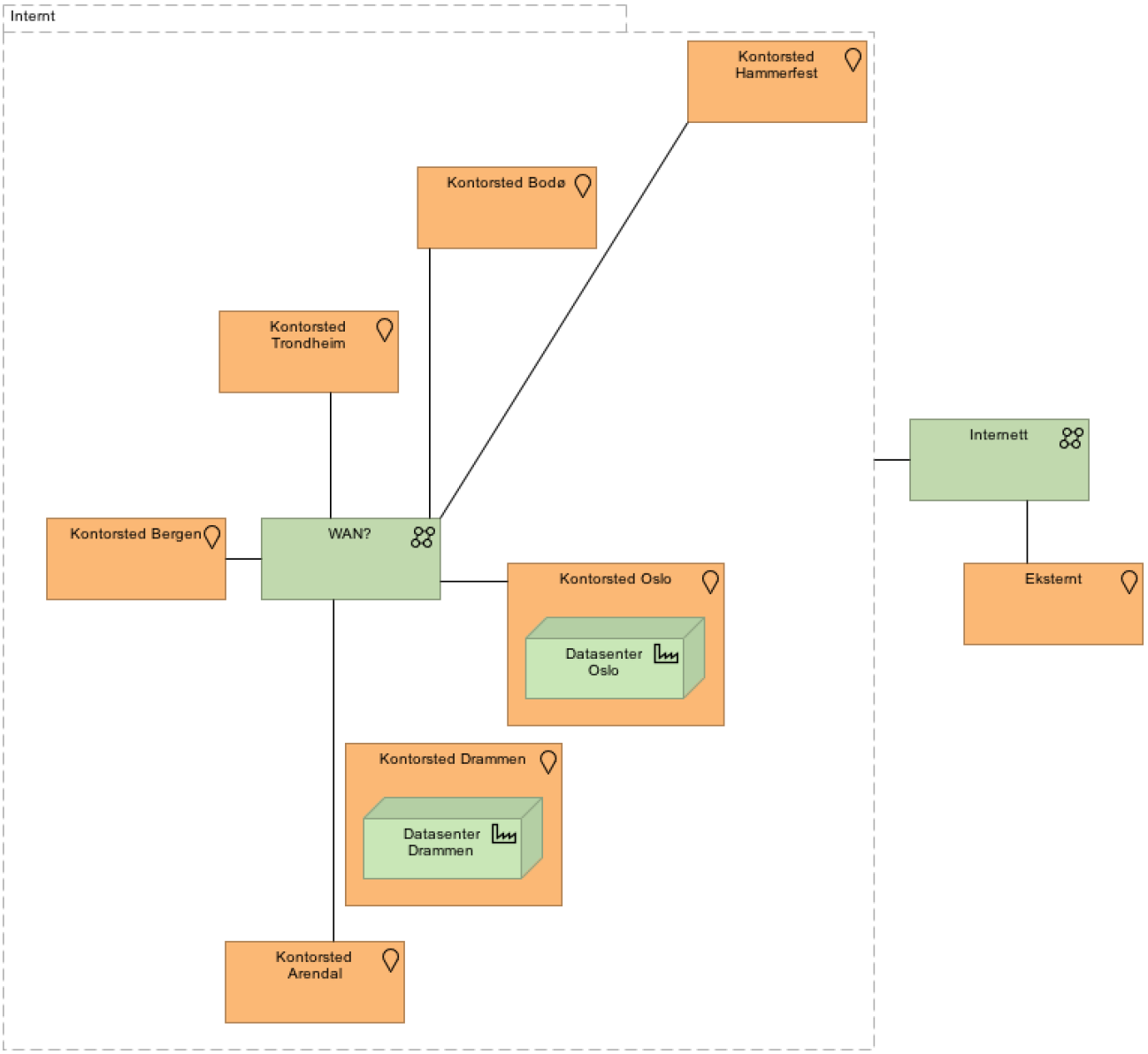
Husbanken

Kundens tekniske plattform

Bilag 3 til tilpasningsavtalen for lånesystem

INNHOLD

1. FYSISK



Brukersteder

Husbanken har flere kontorsteder som alle ligger i Norge:

- Kystveien 2, Arendal
- Solheimsgaten 11, Bergen
- Torvgata 2, Bodø
- Grønland 53, Drammen
- Sjøgata 6, Hammerfest
- Kirkegata 15, Oslo
- Petter Egges plass 2, Trondheim

Husbankens personell har anledning til å arbeide fra andre steder over et virtuelt privat nettverk (VPN).

Husbankens samarbeidspartnere og kunder er offentlige organer, foretak og fysiske personer i Norge som kan ha behov for å nå Husbankens selvbetjeningsløsninger fra de fleste steder i verden, men primært i Norge.

Datasentre

Husbanken hus sine egne datasentre i egne lokaler. Utstyret er nytt og har god kapasitet for Husbankens formål. Husbanken har to datasentre:

- Drammen
- Oslo

Datasenteret i Drammen er hoveddatasenteret. Datasenteret i Oslo inngår i kastrofeberedskap i tilfelle datasenteret i Drammen ikke lenger skulle være tilgjengelig i lengre tid. Datasenteret i Oslo huser også utviklings- og testmiljøer slik at man får utnyttet kapasiteten på senteret og sikrer at det fungerer og er tilgjengelig fra brukerstedene.

2. TEKNISK

2.1. Teknisk infrastruktur

Klient

Personlige datamaskiner

- Operativsystem: Microsoft Windows 10
- Nettleser: Edge (standard), Internet Explorer 11, Chrome
- Kontorstøtte: Microsoft Office 2016, Office 365 fra 1. april 2019

Kunden ønsker ikke Java eller Adobe Flash på klientene. Kunden foretrekker web fremfor installerte klienter.

Maskiner og lagring

Kunden bruker utelukkende virtuelle tjenere.

- Fysiske maskiner
- Virtualiseringsplattform: VMware vSphere
- Hypervisor: VMware ESXi 6.7
- Lagring: Compellent Enterprise SAN SC90000

Nettverk

- LAN: 1 Gbit til klient. 802.11 ac for trådløse klienter. Servere i datasenter har 10 Gbit aksess. Cisco 4507 kjerne.
- WAN: IP VPN (MPLS) fra TDC. Alle kontorer er tilknyttet MPLS ved egen fiber. Aksess mellom 200 Mbit og 2 Gbit avhengig av kontor.
- VPN: Microsoft Direct Access for alle klienter. Også egen Stonesoft VPN-løsning for eksterne klienter med midlertidig tilknytning til Husbankens tjenester.
- Brannmur: Stonesoft firewall i HA cluster (10 Gbit)
- Omvendt proxy: Apache HTTP Server med ModSecurity

Applikasjonstjener

Kunden støtter to ulike konfigurasjoner for applikasjonstjenere: en basert på Microsoft og en basert på Red Hat.

Microsoft

Kunden har applikasjonstjenere basert på Microsoft-teknologi. Disse brukes til å kjøre standard programvare som blant annet Microsoft SQL Server 2017, Microsoft Exchange 2016, Microsoft Skype for Business Server 2015, Microsoft SharePoint 2013 og Active Directory.

Applikasjonstjenerne kjører på virtuelle maskiner uten bruk av container-teknologi og består av:

- Operativsystem: Microsoft Windows Server 2016
- Web-server: Internet Information Server 10
- Kjøretidsmiljø: .NET 4.7.1

Red Hat

Kunden har applikasjonstjenere basert på Red Hat-teknologi. Disse brukes blant annet til å kjøre egenutviklet programvare. Kunden utvikler egen programvare som mikrotjenester implementert i Java.

Applikasjonstjenerne kjører i Docker-containere på virtuelle maskiner. Orkestrering gjøres ved hjelp av Red Hat OpenShift, en Kubernetes-distribusjon.

- Operativsystem: Red Hat Enterprise Linux 7
- Containere: Docker
- Orkestrering: Red Hat OpenShift
- Kjøretidsmiljø: OpenJDK 8 eller 9

Database

Kunden bruker Microsoft SQL Server 2017 som databasetjener.

Driftstyring, overvåking og logging,

Kunden bruker Splunk til logging.

Test

Kunden bruker Cucumber til automatisert akseptansetesting. Kunden bruker Selenium til automatisering av tester gjennom grafiske brukergrensesnitt.

Kunden bruker Jira for å følge krav knyttet til utvikling og endring gjennom verifisering, utvikling og testnivåer frem til produksjonssetting. Det vil være aktuelt å overføre krav knyttet til forberedelser til akseptansetest og akseptansetest til Jira for detaljspesifisering og oppfølging av test.

Utskrift

Kunden bruker Windows print på eventuelle lokale klienter og Lexmark sikker utskriftssystem slik at konfidensielle utskrifter ikke kommer på avveie.

2.2. Informasjonssikkerhet

Pålogging og føderasjon av identitet

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.

Husbanken brukte tidligere OpenAM, men migrer nå vekk fra denne.

Brukerkataloger og autentisering

Kunden benytter to ulike løsninger for brukerkatalog og autentisering:

- ID-porten – felles innloggingsløsning til offentlige tjenester på internett utviklet og forvaltet av Direktoratet for forvaltning og IKT (Difi).
- Active Directory - Kundens egen brukerkatalog for Kundens personell og personell i kommuneforvaltningen.

Kundens egne brukerkataloger vedlikeholdes separat og manuelt. Brukerkatalogene er implementert som to ulike instanser, ikke som ulike domener i samme instans. Det er ingen provisjonering av brukerkontoer og tilganger fra personalsystem eller lignende ved hjelp av løsning for identitet og tilgangsstyring. Tilgangsstyring gjøres ved hjelp av grupper i Active Directory.

Kunden skal bruke ID-porten for digitale tjenester som krever innlogging og autentisering av eksterne brukere.[1] Kunden benytter RedHat Single Sign-On (RH SSO) som intern identitetstilbyder for ID-porten basert på OpenID Connect standarden. I dag støttes autentisering av følgende brukergrupper:

- Privat – Brukere som autentiseres via ID-porten og som representerer seg selv i kontakt med Kunden

[1] H-7/17 Digitaliseringsrundskrivet 1.6 Bruk nasjonale felleskomponenter og fellesløsninger

- Proff – Brukere som autentiseres via ID-porten og som via Autorisasjonskomponenten i Altinn har en rolle for en eller flere organisasjoner (privat eller offentlig) som man velger å representere i dialog med Kunden

I tillegg benytter Kunden også her RH SSO som identitetstilbyder for egenutviklede løsninger basert på OpenID Connect standarden for følgende brukergrupper:

- Partner – Eksterne brukere som administreres i en egen katalogtjener og som typisk brukes i forbindelse med administrasjon av tilgang til fagsystemer der hvor brukere tilhører andre offentlige organisasjoner.
- Husbanken – Gir mulighet for å administrere tilgang for Kundens egne ansatte i AD og sikre disse Single Sign-On til web baserte løsninger. Brukes også for å administrere system-til-system tilgang hvor nødvendig. Eksempler kan være at Kundens egne tjenester krever en autentisering for å autorisere en forespørsel.

Autorisering

Tilgangsstyring for interne brukere gjøres ved hjelp av grupper i Active Directory.

Tilgangsstyring i selvbetjeningsløsningen gjøres ved hjelp av regler i applikasjonene basert på roller i Altinn.

Ved autentisering mot RH SSO mottar klienten JSON Web Token (JWT) som inneholder informasjon om pålogget bruker, eventuelt hvilken organisasjon denne representerer og samsvarende roller.

JWT-token benyttes også til autorisasjon i Kundens eget tjeneste lag. Dette betyr at dersom ikke bruker er autentisert ved RH SSO (men i stedet direkte mot AD) så må systemet autentiseres mot RH SSO for å få nødvendig tilgang til disse tjenestene.

Skadevare

Kunden bruker Microsoft Windows Defender ATP til å beskytte mot skadevare, både på klienter og tjenere med Windows som operativsystem. Innkommende filer skannes ved hjelp av Windows Defender via en egen fellestjeneste.

2.3. Generelle system og tjenester

Kundeportal - Husbankens innloggede tjenester

Husbankens Innloggede Tjenester (HIT) er en løsning som tilbyr «Min Side» funksjonalitet til alle Kundens brukergrupper; Privat, Proff og Partner. Avhengig av brukergruppe og rolle vil forskjellig funksjonalitet tilbys på denne flaten, for eksempel lenker til brukers tilgjengelige verktøy som nettbank og elektronisk søknad om lån og tilskudd, informasjonsmeldinger og direktemeldinger.

Husbankens Innloggede Tjenester er implementert som en Single Page Application (SPA) basert på Angular som frontend rammeverk. Løsningen benytter flere av Kundens mikrotjenester i bakkant for å tilby nødvendig funksjonalitet. Sentralt er også Kundens løsning for pålogging og føderasjon av identitet for å sikre sømløs integrasjon mellom forskjellige web applikasjoner bruker har tilgang til.

Integrasjon med HIT kan gjøres ved:

- standard komponenter som kan integreres i Kundens Angular baserte SPA
- en eller flere applikasjoner som integreres sømløst gjennom Kundens løsning for pålogging og føderasjon
- Standard APIer

Analyse og rapportering

- Datavarehus: Microsoft SQL Server Analysis Services (SSAS)
- ETL (extract, transform, load): Microsoft SQL Server Integration Services

- Analyse: Microsoft Excel og Power Pivot. Husbanken vil ta i bruk Microsoft Power BI Pro i løpet av 2019.

For styringsparametere, statistikkbank og offentlige data brukes Qlik Sense og Qlik Analytics Platform.

Dokument og arkiv

Kunden har en egen dokumenttjeneste som håndterer generering, formidling og arkivering av dokumenter. Tjenesten bruker følgende

- Generering: Docmosis
- Fysisk formidling: PostNord Strålfors
- Elektronisk formidling: Difi eFormidling
- Arkiv: ePhorte

Kontorstøtte

Kunden benytter flere samhandlingsløsninger på tvers av hele organisasjonen:

- E-post, kalender osv: Microsoft Exhange 2016
- Intranett, samskriving: Microsoft SharePoint 2013 og OneDrive for Business
- Lynmeldinger og telekonferanse: Skype for Business Server 2015
- Sosialt nettverk: Yammer (Office 365)

Utvikling

Kunden benytter i tillegg noen andre samhandlingsløsninger for utvalgte brukere. Innen digitalisering gjelder dette spesielt:

- Konfigurasjonsstyring: Bitbucket
- Wiki: Atlassian Confluence
- Issue-håndtering (inkl. testadministrasjon og -dokumentasjon) og prosjektledelse: Atlassian Jira
- Chat: Slack og Rocket Chat

2.4. Grunndata

Part

Som offentlig virksomhet skal Kunden bruke felleskomponenter som kilde til opplysninger om fysiske og juridiske personer:

- Det sentrale folkeregister (Skatteetaten)
- Kontakt- og reservasjonsregisteret (Difi)
- Enhetsregisteret (Brønnøysundregistrene)

Eiendom

Som offentlige virksomhet skal Kunden bruke felleskomponenter som kilde til opplysninger om eiendommer og boliger:

- Matrikkelen (Statens kartverk)
- Grunnbok (Statens kartverk)

I tillegg har kunden en avtale med leverandør av verdivurdering av eiendommer:

- Eiendomsverdi. I dag er dette bare en frittstående løsning.

2.5. Økonomisystemer og -tjenester

Kredittvurdering

Kunden bruker Bisnode for kredittvurderingen og Innrapportert inntekt fra Skatteetaten[2] for å innhente opplysninger om økonomiske forhold.

Faktura

Kunden bruker Nets for eFaktura og AvtaleGiro. Flere låntakere er offentlig virksomheter og skal kunne ta imot elektronisk faktura og kreditnota på Elektronisk handelsformat versjon 3.0 fra 1. januar 2019. Det anbefales også at de skal ta imot purring på Elektronisk handelsformat – purring.

Betaling

Kunden bruker Nordea som betalingsformidler. Statens konsernkontobanker skal kunne ta imot ISO 20022 Pain.001 og sende ISO 20022 Pain.002 og ISO 20022 Camt.054. Direktoratet for forvaltning og IKT (Difi) anbefaler at offentlige virksomheter bruker PEPPOL eDelivery-nettverket i kunde-bank grensesnittet.

Regnskap

Kunden bruker Unit 4 Business World M7 (tidligere kjent som Agresso) til hovedbok. Kunden har egen installasjon. Systemet supporteres av Evry.

Innkreving

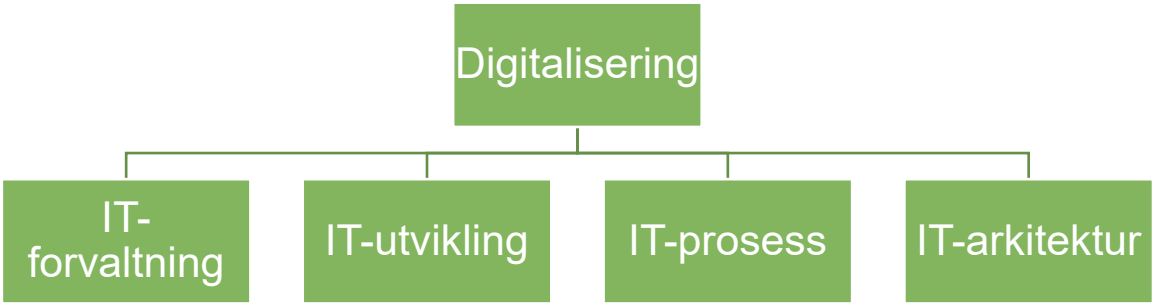
Kunden har satt ut innkreving av misligholdte lån til Statens innkrevingssentral som er del av Skatteetaten.

[2] https://fellesdatakatalog.brreg.no/datasets/59d42d56-9769-4de8-8f19-df6e97c68476

3. ORGANISATORISK

3.1. Organisasjon

Digitalisering er et kontor i Husbanken og er totalleverandør av digitale verktøy og tjenester i Husbanken. Kontoret består av fire avdelinger og har et personell bestående av i alt 44 ansatte og 35 innleide.



IT-forvaltning

IT-forvaltning har 19 ansatte og har ansvar for:

- Anskaffelser og resepsjon, adgangskontroll
- Brukerservice
- Infrastrukturarkitektur
- Kjøringer (batch) knyttet til virkemidlene
- Drift av applikasjoner
- PC, printer og telefoni
- Back-up
- Nettverk, brannmur og lagring
- Kontorstøtteverktøy
- AV-utstyr møterom
- Fysisk sikkerhet
- CMS-løsninger (Veiviser, hb.no, Husnettet)
- Sikkerhet på klient, servere, autentisering interne tjenester (Active Directory)

IT-utvikling

IT-utvikling har 11 ansatte og omtrent 35 innleide og har ansvar for:

- Interaksjonsdesign og lede designforum
- Faglig utvikling innenfor teknologier brukt på egne fagsystemer
- Kompetanseoverføring fra konsulenter til egne ansatte
- Ressurseier mot prosjekter og tverrfaglige team

IT-prosess

IT-prosess har 7 ansatte og har ansvar for:

- Metodikk for prosjektledelse og testledelse
- Kvalitet i leveransene fra tjenesteteamene
- Å ha kompetanse på kartlegging og effektivisering av arbeidsprosesser (f.eks. LEAN) ut fra et digitalt perspektiv
- Å lede forum for informasjonssikkerhet
- Budsjett for utviklingsporteføljen (45-post)
- Metodikk for gjennomføring av risikoanalyser

- Kompetanse på å omdanne fag-krav til system-krav (funksjonell arkitektur)

IT-arkitektur

IT-arkitektur har 10 ansatte og har ansvar for:

- Systemarkitektur knyttet til Kundens egenutviklede systemer
- Kundens Fellestjenester
- Felles ekstern datakatalog og API (hvordan åpne datasett og tjenester eksternt)
- Kontakt og samarbeid med offentlige felleskomponenter, herunder Difi og Altinn
- Arkitektur- og designprinsipper
- Retningslinjer for arkitektur
- Systemsikkerhet (pålogging etc.)

3.2. Prosesser

Tilgangsstyring

Disse prosessene gjelder tilganger til Kundens eget personell og til andre Kunden styrer tilganger til i egne brukerkataloger.

Håndtere tilganger

Ansettelser, oppsigelser og endringer i arbeidsoppgaver gir endringer i behov for tilganger. Linjeleder melder fra til IT-forvaltning om de nødvendige endringene for sine ansatte og IT-forvaltning gjennomfører de nødvendige endringene.

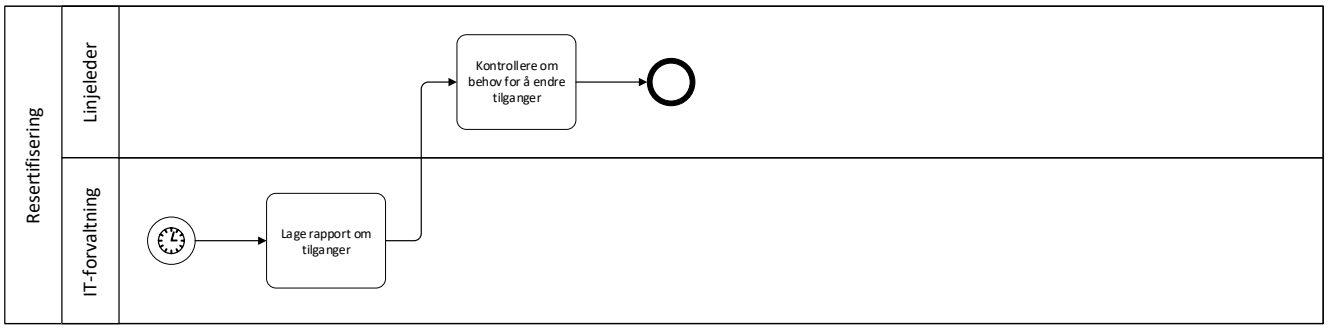
Annen informasjon:

- Dette er en manuell prosess. Husbanken har ingen løsning for identitet- og tilgangsstyring som tilordner rettigheter basert på ansattforhold.

Åpne punkter:

Resertifisering

Selv om man skal fjerne tilganger når det skjer endringer som gjør at man ikke lenger har behov for tilgangene, er det ikke alltid dette skjer. Det er derfor nødvendig med en periodisk gjennomgang av tilganger for å sikre at personell bare har de tilgangene de har behov for.



Annen informasjon:

- Dette er en manuell prosess.

Åpne punkter:

4. ARKITEKTUR

4.1. Prinsipper

Generelle prinsipper

Prinsipp	Type	Beskrivelse	Konsekvens
Mikrotjenester	Veiledende	Applikasjoner skal bestå av løst koblede, samarbeidende tjenester. Hver tjeneste implementerer et sett med nært relaterte funksjoner. Tjenestene kommuniserer enten ved hjelp av synkrone protokoller som HTTP/REST eller asynkrone tjenester som AMQP. Tjenester kan utvikles og produksjonssettes uavhengig av hverandre. Hver tjeneste har sin egen database slik at de er dekoblet fra andre tjenester. Datakonsistens ivaretas ved hjelp av Saga-mønsteret.	
Kontrakt først	Styrende		Vi starter ikke arbeid på interne forhold i tjenester før de funksjonelle og ikke-funksjonelle kravene til tjenesten er bestemt.
Grensesnitt før implementasjon	Styrende	Grensesnittet har høyere verdi enn implementasjonen. Fokus skal være på design av tjenester, ikke på implementeringen.	Grensesnitt holdes adskilt fra implementasjonen i alle lag og styres i egen prosess.
Tjenester leveres i løsninger	Veiledende	Tjenester skal leveres i løsninger. Løsningen skal planlegges. Ingen tjenester skal leveres med mindre de er del av løsningen på et forretningsproblem.	Alle tjenester skal være knyttet mot et forretningsmessig behov og skal være del av en løsning (ha separat livssyklus).
Tjenester skal bruke standard eller eksisterende datamodeller	Veiledende	Eksisterende og etablerte datamodeller skal benyttes når mulig. Hvis tjenesten skal utvides til å tilby data fra flere systemer eller kilder, er det behov for grundigere design.	
Minimal konsekvens for eksisterende brukere	Veiledende	Endringer i tjenester skal leveres med minimal konsekvens for eksisterende brukere av tjenestene.	
Innebygd personvern	Veiledende	Det skal tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning.	

Integrasjonsprinsipper

Prinsipp	Type	Beskrivelse	Konsekvens
Applikasjoner skal ikke trenge å ta hensyn til integrasjonstjenester	Styrende	Tjenester/meldinger skal leveres i format definert i tjenestearkitekturen. De skal mottas i formater som avgjøres av hver enkelt tilbyder.	Integrasjonstjenesten har ansvar for omforming til felles format.
Minimal konsekvens for eksisterende brukere	Styrende	Endringer i tjenester skal leveres med minimal konsekvens for eksisterende brukere av tjenestene.	

Prinsipp	Type	Beskrivelse	Konsekvens
Logisk datamodell	Veiledende	Meldinger og dataformat skal baseres på logiske representasjonen av forretningsobjekter og ikke fysiske datastrukturer i applikasjoner.	

Sikkerhetsprinsipper

Prinsipp	Type	Beskrivelse	Konsekvens
Alltid SSL	Veiledende	SSL skal alltid benyttes. Våre eksterne API-er kan benyttes fra ethvert sted med internett-tilgang som biblioteker, kaféer og lignende. Mange av disse nettverkene er ikke tilstrekkelig sikret. Dette medfører risiko for avlytning og falsk identitet.	SSL forenkler autentisering. Det kan benyttes enkle tokens i stedet for å signere hvert API-.kall.