<GS1 Innføring>

Overordnet design

IKT tjeneste for RFID

Versjonskontroll:

Versjon	Dato	Forklaring	Utført av
0.1	01.06.2020	Dokument opprettet	Bjørn Ravnestad
0.4	15.06.2020	Revisjon av dokument	Bjørn Ravnestad
0.5	23.06.2020	Revisjon av dokumentet	Bjørn Ravnestad

Godkjent av:

Navn	Rolle	Stilling	Dato

Innholdsfortegnelse

1. Innledning

Dokumentet beskriver en ikt-tjeneste for RFID-system som understøtter etablering av RFID-løsninger på ulike bruksområder. Systemet som skal anskaffes er kontrollsystemet for en RFID-løsning.

Dokumentet er bygget opp med følgende struktur:

Forretning – i dette kapittelet beskrives hvilke bruksområder og brukstilfeller IKT-tjenesten skal dekke, samt hvordan forvaltning av denne kan organiseres.

Informasjon – I dette kapittelet beskrives hvilken informasjon som IKT-tjenesten skal behandle.

Applikasjon – I dette kapittelet beskrives applikasjonsfunksjonalitet og -tjenester IKT-tjenesten må tilby, og mulige implementeringsstrategier.

Teknologi – I dette kapittelet beskrives tekniske kapabiliteter, inkludert sikkerhet og avhengighet til plattformtjenester.

2. Forretning

2.1. Innledning

RFID-systemet er beregnet for en rekke ulike bruksområder, det er i regi av de regionale byggeprosjektene blant annet utarbeidet brukstilfeller for følgende områder:

- Innkjøp og logistikk
- Medisinsk teknisk utstyr og forbruksmateriell
- Legemiddel

Ett RFID-system må understøtte automatisk identifikasjon og datafangst av innhold på RFID ID-brikker, filtrering og sammenstilling av denne informasjonen, og videreformidling av informasjonen til konsumentsystemer. .

2.2. Om RFID

For vareflyt finnes det frittstående logistikkløsninger basert på strekkodelesere integrert med dedikerte arbeidsstasjoner med vareforsyningssystemet for vareflyt. Tilsvarende finnes for medisinforsyning med frikoblede logistikkløsninger. Utfordringene med disse løsningene er at det ikke er etablert enhetlige løsninger for strekkodelesere og grunndata for lokasjon, produkt- og eiendelskataloger.

Ved å innføre en RFID løsning for automatisk datafangst og sporing i foretaksgruppen vil det kunne legges til rette for både grunndatakildene som i dag mangler, samt danne grunnlaget for mer effektiv logistikk og bruk og forvaltning av eiendeler. Dette gjennom blant annet harmonisering av logistikk på tvers av helseforetakene på områdene innkjøp og logistikk, medisinsk-teknisk utstyr, forbruksmateriell og legemiddel.

2.3. Brukstilfeller

I avsnittene under beskrives brukstilfeller for ulike forslagsvise brukerroller som benytter IKT-tjenesten RFID system. Brukerrollene og aktører som er beskrevet er:

- Bruker med utvidede rettigheter (tjenesteleverandør) - Dette er en superbruker som har mulighet til å administrere applikasjonen og tilordne rettigheter til brukere, og er en rolle som tjenesteleverandør benytter i sin forvaltning av applikasjonen.
- Bruker med utvidede rettigheter (intern administrasjon) – Dette er en superbruker som har muligheter til å administrere ID-brikker og informasjonsbasen. Dette er en rolle som virksomheten benytter i sin forvaltning av RFID merkingen.
- Bruker med utvidede rettigheter (integrasjon) – Dette er en superbruker som har muligheter til å administrere integrasjoner, og er en rolle som tjenesteleverandør benytter i sin forvaltning av applikasjonen.

2.3.1. Bruker med utvidede rettigheter (tjenesteleverandør)

Opprette brukere av tjenesten (provisjonere / on-demand)
Det skal være mulig å provisjonere brukere av ikt-tjenesten automatisk ved hjelp av et system for identitetshåndtering. Dette for å sikre at brukere opprettes og fjernes automatisk i tråd med foretakets policy for identitetsforvaltning.

2.3.1. Bruker med rettigheter (lokal forvalter)

Opprette ID-brikker og registrere disse i RFID system
Det skal være mulig å provisjonere ID-brikker av ikt-tjenesten automatisk ved import av data og via bruk av avlesingsmekanisme. Dette for å sikre at ID-brikker på anskaffet utstyr opprettes og fjernes automatisk i tråd med foretakets policy.

2.4. Forvaltningsmodell

Når det kommer til forvaltning er det behov for forvaltning av IKT-løsning og forvaltning av data i løsningen, dataforvaltning.

2.4.1. Forvaltning av IKT-løsning

Forvaltningsmodellen for IKT-løsningen skal understøtte løsningen i foretaksgruppen. Det forvaltnings- og driftsmessige hovedansvaret for eierskap til IKT-løsningen forutsettes å ligge hos det regionale helseforetaket (RHF) siden IKT-løsningen har et regionalt bruksområde i foretaksgruppen.

Forvaltningsmodellen beskriver rollen «Tjenesteleverandør» som skal leveres som en tjeneste av den til enhver tid aktuelle leverandør. Rollen skal på vegne av et regionalt forvaltningsråd (hovedansvarlig) ha ansvar for (utøvende og på vegne av), og sikre, koordinering mellom alle aktører i den tekniske leveransekjeden i IKT-løsningen, ved alle endrings- og hendelsesrelaterte aktiviteter. Ansvaret forpliktes gjennom kontrakter og avtaleverk.

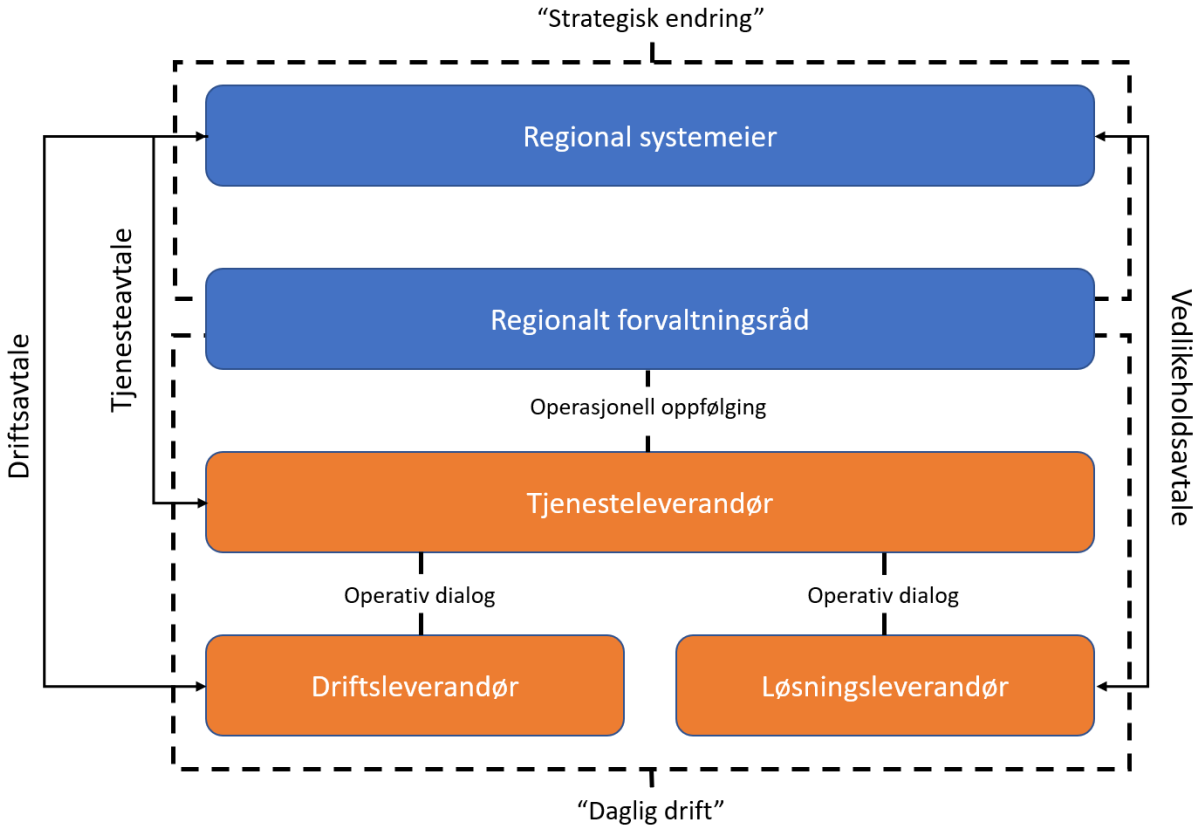
Drift og forvaltning av en regional IKT-løsning krever representasjon og involvering i en «Regional Systemeiergruppe» og et «Regionalt Forvaltningsråd» fra de helseforetak som er interessenter i, og brukere av, IKT-tjenesten.

Denne modellen skisserer roller som er nødvendig for å sikre en god og sikker drift og forvaltning av en slik regional IKT-løsning. En drifts- eller løsningsleverandør kan ivareta flere roller.

Forvaltningsmodellen brukes ved etablering av nye IKT løsninger som skal fungere på tvers av to eller flere foretak. I tabellen under er det definert noen begreper. Definisjonene er hentet fra «Kilden»[1].

[1] https://kilden.sykehusene.no/pages/viewpage.action?pageId=51511559

Begrep	Definisjon
IKT-tjeneste	En IKT-tjeneste er en IKT-løsning inkludert tilhørende drift og forvaltning av IKT-løsningen. En IKT-tjeneste er basert på informasjonsteknologi og støtter fagsidens arbeidsprosesser. Tjenesten inneholder personellressurser, produksjonsprosesser, teknologi, samt drift og forvaltning av tjenesten
IKT-løsning	Ett eller flere tekniske IKT-system som til sammen støtter virksomheten
IKT-system	En enkeltstående applikasjon eller en applikasjon med flere integrasjoner inkludert tilhørende infrastruktur. Et IKT-system behandler, lagrer og overfører data og kan sees på som den tekniske delen av en IKT-løsning.
Drift	Summen av alle styrings- og arbeidsprosesser som er nødvendige for å sikre brukerne tilgang til et IKT-system med avtalt kvalitet. Det være seg basis drift (nettverk, datasenter, servere overvåking, databaser, OS, lisenser m.m uten noen form for forretningslogikk), samt applikasjonsdrift (tilgjengeliggjøring av programvare for sluttbrukere med tilhørende overvåking, kapasitetsplanlegging, proaktiv drift, vedlikehold, patching og oppgradering av applikasjonen)
Forvaltning	Summen av alle styrings- og arbeidsprosesser som er nødvendige for å opprettholde krav til kvalitet i en IKT-tjeneste (IKT-løsning, metode, prosess etc) over tid. Forvaltning kan deles inn i Funksjonell forvaltning, Applikasjonsforvaltning og Teknisk forvaltning. Se også Systemforvaltning



Figur 1 - Forvaltning av IKT-løsning

Regional systemeier skal:

- Prioritere endringsbehov, sikre finansiering og beslutte andre strategiske valg relatert til endringer i arbeidsprosesser, rutiner, prosedyrer og opplæringsmateriell
- Sikre at IKT-løsning er i henhold til vedtatt IKT-strategi og målarkitektur
- Ha strategisk dialog med leverandører

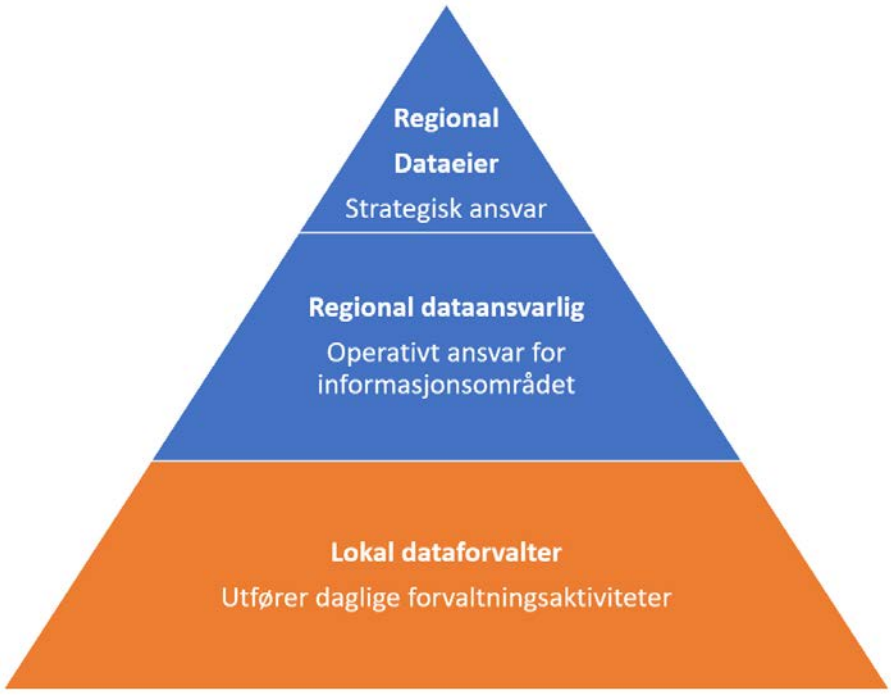
Regionalt forvaltningsråd skal:

- Ivareta og forbedre aktuelle arbeidsprosesser
- Definere rutiner, prosedyrer og opplæringsmateriell
- Sikre synkroniserte utviklings, vedlikeholds- og veikart med helseforetak og tjenesteleverandør
- Tilrettelegge for og utarbeide beslutningsgrunnlag for systemeiers ansvarsområder
- Forvalte oppgaver i et utviklingsperspektiv
- Være operativt nivå for lokale innspill, erfaringer og involvering i helseregionen rundt beslutninger på prioritering av endrings- og feilrettingsønsker

Drifts- og løsningsleverandør skal:

- Gjennomføre prioriterte tiltak ihht definerte prosesser for feil- og endringshåndtering
- Utføre operativ leverandørstyring og operativ avtalehåndtering

2.4.2. Forvaltning av Data



Figur 2 - Forvaltning av data

I modellen over skal de ulike rollene ha følgende ansvar.

Dataeier skal:

- Ha strategisk ansvar for et informasjonsområde
- Representere lokale og regionale interesser
- Ha interesse og myndighet til å fatte beslutninger knyttet til informasjonsforvaltning
- Godkjenne retningslinjer, standarder og måleparameter

Dataansvarlig skal:

- Koordinere dataforvaltere
- Ha operativt ansvar for informasjonsområdet
- Arbeide tett med systemansvarlige og dataforvaltere
- Følge opp at krav, standarder og retningslinjer etterleves

Dataforvalter skal:

- Være en anerkjent fagsekspert
- Utfører daglige forvaltningsaktiviteter i henhold til krav, standarder og retningslinjer

- Ha stor interesse i at datakvaliteten ivaretas på en god måte

3. Informasjon

Dette kapittelet beskriver overordnet hvilken informasjon som vil bli behandlet av IKT-tjenesten.

3.1. Om RFID

RadioFrekvensIDentifikasjon (RFID) gjør det mulig å overføre data fra en ID-brikke som er en elektronisk enhet (RFID brikke), som kommuniserer via radiofrekvenssignaler over RFID antenner med en RFID leser. RFID-systemet sender instruksjoner og mottar respons tilbake.

Det vil være ulike anvendelser av RFID i applikasjoner, og det er disse applikasjonene som vil behandle data som er avlest fra ID-brikkene.

3.1.1. Grunndata

I det regionale GS1 prosjektet er det identifisert to klasser av grunndata som det er aktuelt å representere på ID-brikker i et RFID-system. Dette er:

- Produkt – I helseforetakene benyttes det en rekke produkter for produksjon av helsetjenester. Åpenbare eksempel er legemiddel, medisinsk utstyr (eks implantat), medisinsk forbruksmateriell m.m. I økende grad er slike produkt merket med RFID ID-brikker inneholdende elektroniske produktkoder, EPC. Gjennom å kunne avlese og dekode produktkoder fra ID-brikker påsatt fysiske produkt etablerer man sporbarhet i logistikkkjeder og gjør det mulig å avdekke avvik og forfalskede produkt som kommer inn i forsyningskjedene. I økende grad brukes også sensorikk for å understøtte kjølekjeder.
- Eiendeler – Helseforetakene har mange ulike eiendeler som forvaltes. Ved at disse merkes med ID-brikker som inneholder unike nummer for hver enkelt instans blir det mulig å spore og lokalisere eiendelene i helseforetakene. Dette øker kontroll og utnyttelsesgrad for utstyret, reduserer svinn, og reduserer medgått tid til å lete etter utstyr.

Automatisk identifikasjon og datafangst av innhold på RFID ID-brikker påsatt produkt og eiendeler er ikke isolert sett kontroversielt, men dersom ID-brikkene bæres av personer og på denne måten indirekte sporer personer er det behov for å vurdere personvernkonsekvens.

Det er også mulig å utstede ID-brikker med nummer som direkte eller indirekte identifiserer personer, eksempelvis pasienter eller helsepersonell. Et eksempel på dette kan være pasientarmbånd med integrert RFID ID-brikke. Ved implementering av en slik anvendelse av et RFID-system må lovlighet vurderes og det må utføres en personvernkonsekvensutredning for den planlagte RFID-applikasjonen. GS1 prosjektet har ikke planlagt RFID-applikasjoner

som skal behandle persondata. Se forøvrig avsnitt i kapittel 5 om behov for personvernkonsekvensutredning for RFID applikasjoner.

3.1.2. Transaksjonsdata

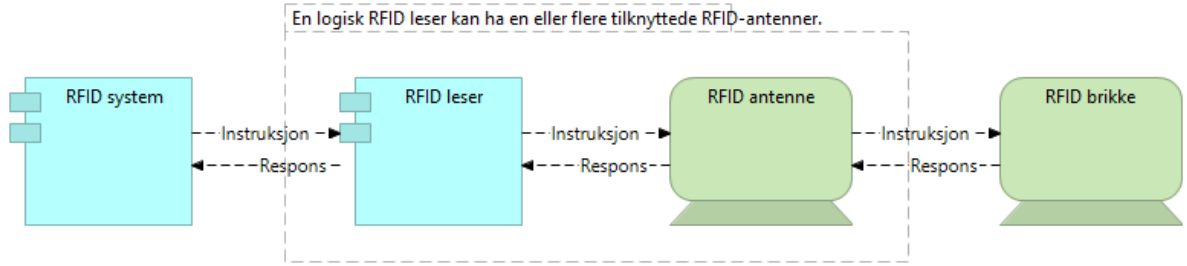
Datafangsthendelser som samles inn av RFID infrastrukturen utgjør transaksjonsdata som typisk beskriver «hva», «hvor» og «når» for ID-brikker. Det kan dreie seg om høye volum av data, og derfor gjør RFID-systemet en filtrering og sammenstilling transaksjoner før disse sendes videre til konsumenter av datafangsthendelsene.

4. Applikasjon

Dette kapittelet beskriver konseptuelt applikasjonstjenester som skal gjøres tilgjengelig som en IKT-tjeneste.

4.1. Konseptuelt design

RadioFrekvensIDentifikasjon (RFID) gjør det mulig å overføre data fra en ID-brikke som er en elektronisk enhet (RFID brikke), som kommuniserer via radiofrekvenssignaler over RFID antenner med en RFID leser. RFID-systemet sender instruksjoner og mottar respons tilbake.



Figur 3 – RFID system

RFID-koder har flere funksjoner og egenskaper. Noen av disse er:

- RFID-brikker kan leses selv når det ikke er en direkte optisk synslinje fra RFID-brikken til RFID-leser.
- En enkelt RFID-leser kan lese mange RFID-brikker samtidig.
- Data på RFID-brikker er organisert i flere minnebanker, som hver har separat tilgang.
- Dataene i RFID-brikker kan oppdateres og endres.
- Ulike typer RFID-brikker kan tilby ekstra funksjonalitet i tillegg til datalagring og dataaksess; for eksempel: kryptering, autentisering, tilgangskontroll, elektronisk deaktivering av RFID-brikke, sensorikk, aktuering, etc. Grensesnittene gir også muligheten til å utføre disse operasjonene.

RFID-systemer bruker et ekstra lag med programvare mellom datafangstprogrammet og individuelle RFID-maskinvareenheter. De to vanlige grensesnittene mellom et datafangstprogram, og RFID-leseren som den samhandler med, er:

- **Application Level Events (ALE)[2] grensesnitt:** ALE, som kan oversettes til Applikasjonsnivåhendelser**,** er en GS1 standard som er et standardisert grensesnitt mellom et datafangstprogram og RFID-lesere. ALE utstyrer datafangstprogrammer

[2] *GS1 Application Level Events (ALE) Standard*

med et grensesnitt der data fra mer enn én RFID leser kan aggregeres sammen og der data filtreres for å unngå flere duplikate avlesninger, uønskede avlesninger, etc. ALE gjør det også mulig for flere applikasjoner å samhandle samtidig med de samme RFID-leserene. ALE er utformet for å la et datafangstprogram fokusere på *hvilke* data og operasjoner de ønsker å bruke i samspill med RFID-brikker, uten å eksponere detaljene om *hvordan* dette er implementert i samspillet mellom leser og brikke.

- **Low Level Reader Protocol (LLRP)[3] grensesnittet:** LLRP er en GS1-standard som beskriver grensesnitt til en enkelt RFID-leser. Dette er et grensesnitt på et lavere nivå enn ALE. Det gir full kontroll over operativ drift av en RFID-leser inkludert detaljer om samhandling melllom RFID-leser og RFID-brikke. Data på LLRP-nivå er representert i det samme rå, kodede formatet som brukes i selve RFID-brikkens minne. LLRP gjør det mulig for en enkelt klient å ha full kontroll over en enkelt leser.

Når ALE og LLRP brukes sammen, er det vanligvis et lag med programvare mellom LLRP- og ALE-grensesnittene. Denne programvaren kalles filtrering- og innsamlingsprogramvare. Filtrering- og innsamlingsprogramvaren er ansvarlig for å motta instruksjoner på høyt nivå fra ett eller flere datafangstprogrammer som kommuniserer gjennom ALE-grensesnittet, bestemme hvordan best utføre disse instruksjonene ved hjelp av individuelle RFID-lesere, og deretter utføre instruksjonene overfor RFID-leseren gjennom LLRP. Filtrerings- og innsamlingsprogramvaren oversetter også mellom rå, kodede dataformater som avleses fra RFID-brikke, til «applikasjonsvennlige» dekodede format som kan brukes av datafangstprogrammer.

ALE og LLRP er en del av "dataflyten" i en RFID-datafangstarkitektur - de er ansvarlige for kommunikasjon av applikasjonsdata mellom RFID-brikker og applikasjonslaget. Komplekse RFID-installasjoner som involverer mange RFID-lesere har vanligvis også en "kontrollflyt" som brukes til å konfigurere, administreres og overvåke RFID-maskinvare for optimal drift. Dette er særlig viktig når RFID-enheter ikke styres direkte av menneskelige operatører. Det finnes to GS1-standarder som beskriver grensesnitt for å etablere en «kontrollflyt» for RFID-infrastruktur:

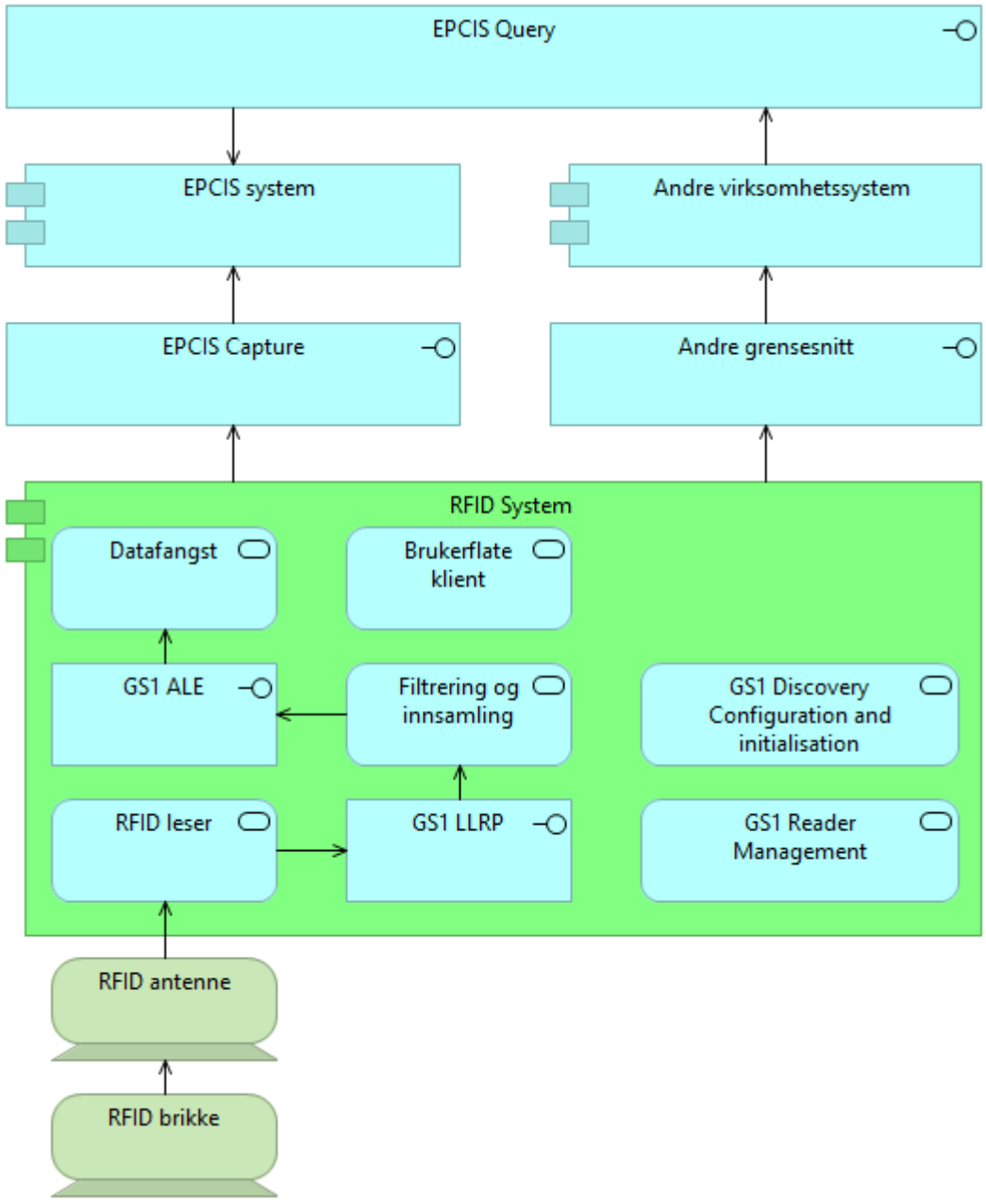
Reader Management (RM)[4] grensesnitt: RM er en GS1-standard for et grensesnitt der et overvåkingsprogram kan få informasjon om statusen til en RFID-leser, inkludert om det er operativt, hvor mange ID-brikker som leses, og så videre.

RFID Discovery, Configuration, and Initialisation (DCI)[5] grensesnitt: **DCI** er en GS1-standard for et grensesnitt for hvordan en RFID-leser automatisk kan gjøre seg kjent for et nettverk,

[3] *Low Level Reader Protocol (LLRP)*
[4] *GS1 Reader Management (RM)*
[5] *GS1 Diccovery, Configuration and Initialisation (DCI)*

innhente konfigurasjonsinformasjon og initialisere seg selv slik at den kan kommunisere med filtrering- og innsamling- eller applikasjonsprogramvare.

Figuren under illustrerer komponentene som inngår i en arkitektur for et RFID-system.



Figur 4 – RFID-system

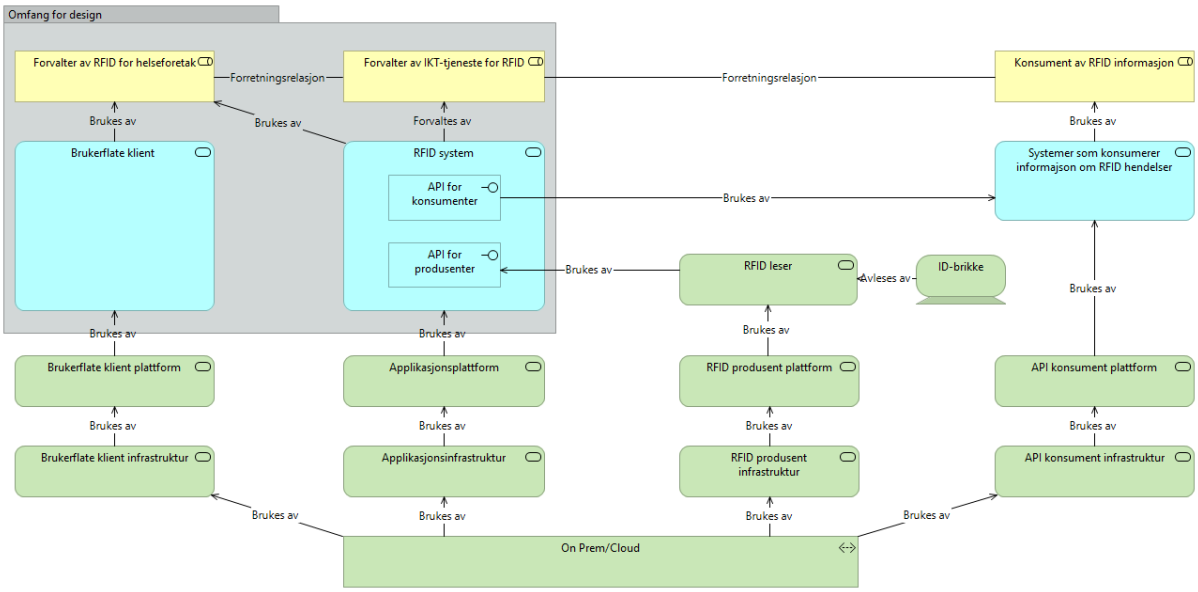
4.2. Mulige Implementeringsstrategier

RFID-system vil først implementeres i de to helseforetakene som er i gang med større byggeprosjekt. Dette gjelder VVHF og OUS HF. Anbefalingen fra Sykehuset i Århus i Danmark er å implementere datafangstinfrastrukturen gradvis slik at den fortløpende understøtter forretningsmessige behov, og at man ikke på forhånd bygger ut en omfattende infrastruktur

uten å ha planlagt hvordan den skal utnyttes. Både VVHF og OUS ønsker å fokusere på varelogistikk og lokalisering og sporing av medisinsk-teknisk utstyr. RFID-systemet må kunne skaleres opp etter hvert som ibruktakelsen øker og RFID-infrastrukturen utvides.

5. Teknologi

Figuren under illustrerer et overordnet teknisk design, og det er områdene innenfor «Omfang for design» (grå bakgrunn) som skal etableres som en IKT-tjeneste. Det forutsettes at plattform og infrastruktur for å etablere, drifte og forvalte en applikasjonstjeneste eksisterer.



Figur 5 – Løsningskonsept for RFID

5.1. Sikkerhet

Et RFID system vil ikke inneholde pasientsensitiv informasjon så fremt det ikke benyttes ID-brikker med personinformasjon

Sikkerhetsmessige bruksscenario fra regional målarkitektur IAM[6] som er relevant for IKT-løsningen RFID-system er:

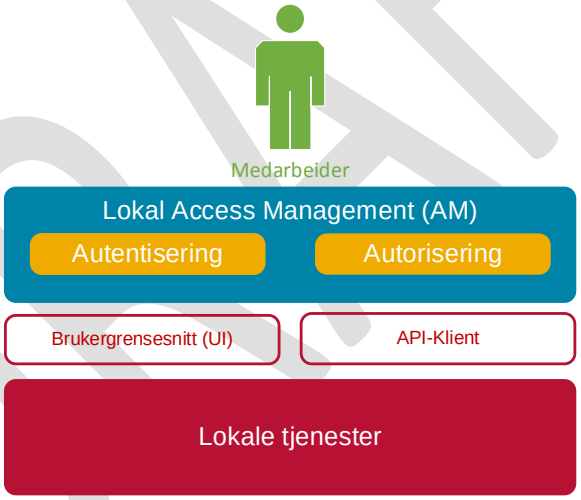
- Sikker tilgang til egne tjenester for eget personell (lokalt HF)

5.1.1. Sikker tilgang til egne tjenester for eget personell (lokalt HF)

Bruksscenarioet er aktuelt for systemer og brukere som skal ha tilgang til RFID system for å administrere løsningen. Dette overordnede designet antar at RFID-system etableres som en regional IKT-tjeneste, men dette kan realiseres på forskjellige tekniske måter.

Bruksscenarioet gjelder for personell i lokalt helseforetak som konsumerer egne tjenester.

Bruker aksesserer en intern applikasjon fra sin arbeidsstasjon (PC/laptop/tablet). Applikasjonen er sikret og tilgang gis kun til brukere med et tjenstlig behov.



Figur 6: Sikker tilgang til egne tjenester for eget personell (lokalt HF)

Ved aksessering av en beskyttet applikasjon må bruker autentisere seg (hvem er du), og det må foretas en autorisering (hva har du tilgang til). Bruker blir enten avvist eller godkjent og gitt tilganger basert på brukerlegitimasjon. Ved bruk av aksesstjenesten (Access Management, AM) blir brukersesjonen kontinuerlig kontrollert, slik at sikkerhetspolicy håndheves.

Applikasjonen kan også aksesseres direkte, men er beskyttet av autentiseringstjenesten. Dersom applikasjonen har behov for automatisert vedlikehold av intern brukerdatabase

[6] *Hentet fra versjon 1.0 av dokumentet «IAM Målarkitektur for Helse Sør-Øst 2023»*

benyttes provisjonering av brukere og nødvendige attributter, men disse attributtene kan også medfølge i token fra autentiseringstjenesten.

5.1.2. Personvernkonsekvensutredning for RFID applikasjoner

Europakommisjonen utstedte 12 mai 2009 en anbefaling om at det skulle utarbeides et bransjeforankret rammeverk for personopplysninger og personvernkonsekvensvurderinger av RFID-applikasjoner. Slike vurderingene kalles på norsk, etter ikrafttredelse av GDPR, vurderinger av personvernkonsekvenser, eller DPIAer.

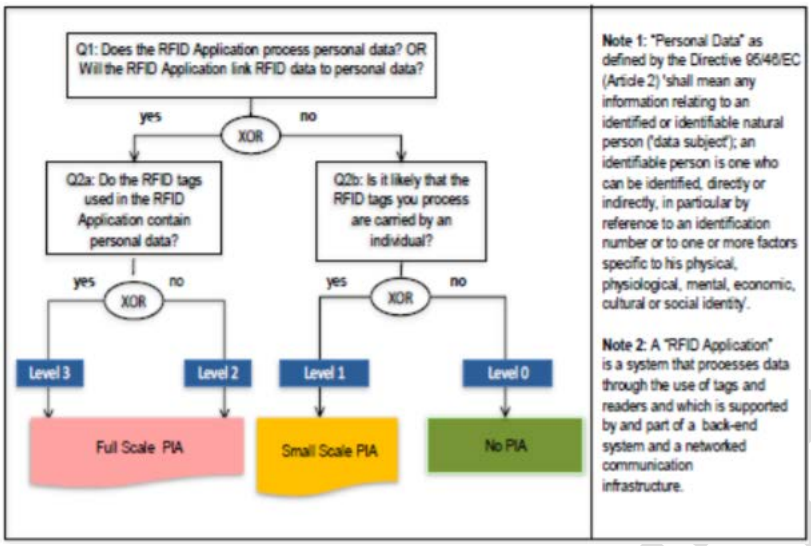
Ved å gjennomføre DPIAer for RFID-applikasjoner bistår man forvaltere av RFID-applikasjoner i å:

1. sikre og opprettholde overholdelse av lover og forskrifter for personvern og informasjonssikkerhet;
2. håndtere risiko for egen virksomhet og brukere av RFID-applikasjoner (både relatert til personvern- og informasjonssikkerhet); og
3. tilrettelegger for å kunne ta i bruk RFID-applikasjoner gjennom å bygge inn personvern allerede i tidlige stadier av spesifikasjons- og utviklingsprosesser.

DPIA-prosessen for RFID er basert på en tilnærming til risikostyring av personvern og databeskyttelse som hovedsakelig fokuserer på implementeringen av EUs RFID-rammeverk[7] og i samsvar med EUs øvrige juridiske rammeverk og beste praksis for informasjonssikkerhet og personvern. Man må blant annet vurdere:

- Systematisk behandling av personopplysninger inkludert vurdering av innebygd personvern
- Formål med behandlingen
- Behandlingens lovlighet
- Nødvendighet og forholdsmessighet av behandlingen
- Risiko for de registrertes rettigheter og friheter
- Planlagte tiltak for å håndtere risikoene (garantier, sikkerhetstiltak og mekanismer)

[7] *Privacy and Data Protection Impact Assessment Framework for RFID Applications*



Figur 7 – Beslutningstre for å vurdere om, og i hvilket omfang, det er behov for DPIA