Leverandørtilganger

Pål-Øivind Kjeserud

Enhetsleder Sykehuspartner

24.01.2014

LIVSVIKTIG

Sykehuspartner

Agenda

- Hvem og hva er Sykehuspartner
- Leverandørtilgang
- Leverandørtilgang i praksis

SYKEHUSPARTNER

Hvem og hva er Sykehuspartner?

SYKEHUSPARTNER

Helse Sør-Øst RHF - det regionale helseforetaket

Norge er delt i fire helseregioner. I hver av dem har et regionalt helseforetak ansvar for å sørge for at befolkningen blir tilbudt spesialiserte helsetjenester. Staten eier de regionale helseforetakene.

Helse Sør-Øst RHF Helse Sør-Øst RHF eier 10 helseforetak og har hovedkontor på Hamar

Ansvar for sykehustjenester til befolkningen i Østfold, Akershus, Oslo, Hedmark, Oppland, Buskerud, Vestfold, Telemark, Aust-Agder og Vest-Agder.

Virksomheten omfatter:

- sykehus
- institusjoner i psykiatrien og innen rusbehandling
- ambulansetjenesten
- nødmeldingstjenesten
- pasienttransport
- opptreningsinstitusjoner
- sykehusapotek
- laboratorier

SYKEHUSPARTNER

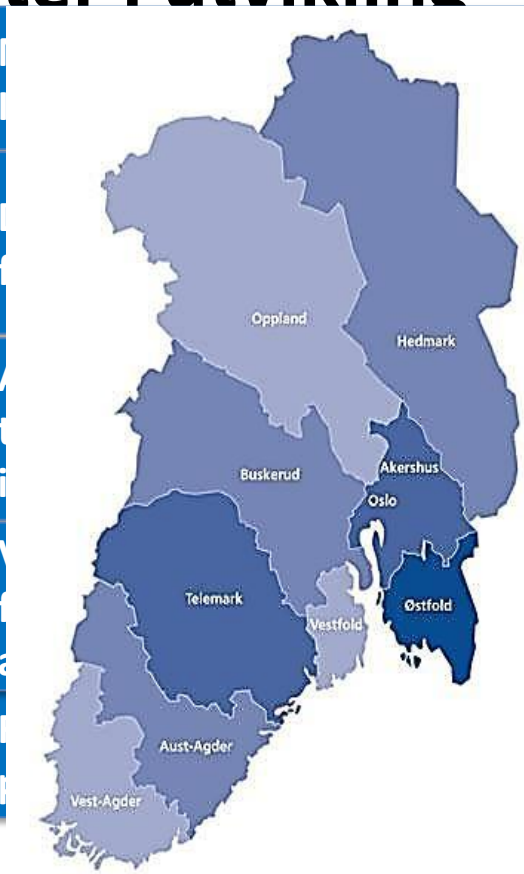
Hvem er Sykehuspartner

“En partner for helsetjenester i utvikling”

Felles tjenesteleverandør av ikke-medisinske støttetjenester til helseforetakene i Helse Sør-Øst

Ca. 1050 ansatte fordelt på hovedkontor i Drammen og avdelingskontorer i Oslo, Grimstad, Fredrikstad, Porsgrunn, Innlandet og ulike helseforetak

Vi leverer samordnede løsninger innen IKT, HR, brukerservice og innkjøp/logistikk



SYKEHUSPARTNER

Våre kunder er helseforetakene i Helse Sør-Øst

Oslo universitetssykehus

Vestre Viken HF

Sørlandet sykehus HF

Sykehuset Innlandet HF

Akershus universitetssykehus

Sunnaas sykehus HF

SYKEHUSET ØSTFOLD

Sykehuset i Vestfold

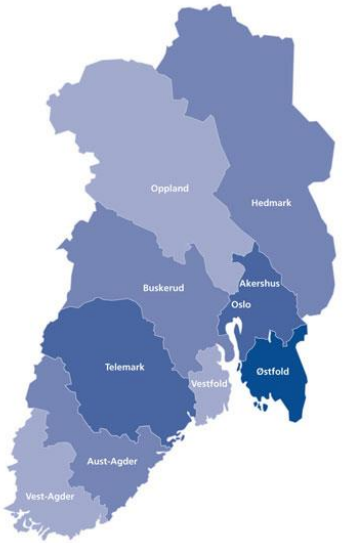
Revmatismesykehuset
LILLEHAMMER – NORWAY

BETANIEN

MHH 1936

SYKEHUS APOTEKENE

Sykehuset Telemark



SYKEHUSPARTNER

Sykehuspartner - IKT

- Overordnet mål å
  - levere stabil og høy tilgjengelighet på IKT-systemer i helseregionen
    - levere tjenester til avtalt kvalitet og effektivitet

    for å

    - redusere kostnader og ressursbruk til IKT

    ved

    - samordning, standardisering og sentralisering

SYKEHUSPARTNER

Sykehuspartner - IKT

er bare et av verktøyene for å støtte opp under Helse Sør-Østs oppgave

Å GI ET GODT HELSETILBUD TIL DEN ENKELTE MED GOD KVALITET

SYKEHUSPARTNER

Basis for «Godt helsetilbud»

Avhengig av

TILLIT

SYKEHUSPARTNER

Helse Sør-Øst

VERDIFILMEN

Hva sier informasjonsvideo?

- Et godt helsetilbud er avhengig av tillit til helseforetakene
- Pasientsikkeret i fokus
- Helseforetakene forvalter meget sensitiv informasjon
- Teknologi alene gir ikke tillit

SYKEHUSPARTNER

Hva sier ikke informasjonsvideo?

Lovverket legger ***strenge føringer*** for sikring av personopplysninger.

Forskrift om behandling av personopplysninger

http://lovdata.no/dokument/SF/forskrift/2000-12-15-1265

SYKEHUSPARTNER

Personopplysningsloven

Databehandleravtalen mellom Sykehuspartner og Helseforetakene i Helse Sør-Øst:

- Tilgang til tjenester og opplysninger i nettverket skal være basert på individuelle brukerkoder og passord.

- Det skal benyttes personlige brukerkonti for all tilgang knyttet til gjennomføring av leveransen.

Disse to kapitlene er forankret i følgende lovbestemmelse; Personopplysningsforskriftens sikkerhetsbestemmelser:

[§ 2-14 Sikkerhetstiltak]

- Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og ikke være begrenset til handlinger som den enkelte forutsettes å utføre.

[§ 2-16 Dokumentasjon]

- Registrering av autorisert bruk av informasjonssystemet og av forsøk på uautorisert bruk, skal lagres minst 3 måneder. Det samme gjelder registreringer av alle andre hendelser med betydning for informasjonssikkerheten

SYKEHUSPARTNER

Leverandørtilgang

SYKEHUSPARTNER

Leverandørtilgang

Leverandøren er det samme som en bruker

minus

Ansattforhold regulert gjennom ansettelsesavtaler og andre kontrakter

Altså, det krever ennå større behov for tilgangskontroll

- Avtaler sikrer:
  - Sikkerhet
  - Stabil drift på IKT systemene

SYKEHUSPARTNER

Leverandørtilgang

- Helseforetakene er avhengig av leverandører av medisinteknisk utstyr (MTU) og programvare for pasientbehandling
- Leverandører trenger tilgang til «sine» systemer for
  - Feilretting
  - Vedlikehold
  - Konfigurasjon
- Forventning fra «alle» om online tilgang til systemer

SYKEHUSPARTNER

Leverandørtilgang

De fleste systemer er av en slik art at de inneholder ***sensitiv informasjon*** om pasienter

Konsekvensen av dette er at leverandørtilgang ikke er trivielt

SYKEHUSPARTNER

Leverandørtilgang – kontroll og sporbarhet

Tilgang til interne systemer må

- Kontrolleres
- Være sikker
- Handlinger må kunne spores

Tiden med
«kan vi ikke bare får et VPN»
er forbi!

SYKEHUSPARTNER

Kontroll, sikkerhet og sporbarhet

- Leverandøraksess gis personlig
  - Ikke tillatt å overdra tilgang til andre eller bruke andres identitet
  - Teknologi begrenser mulighet for dette, men ikke absolutt

- Databehandlingsavtale mellom SP eller leverandør og helseforetak
  - Underleverandører er omfattet av denne avtalen

SYKEHUSPARTNER

Kontroll, sikkerhet og sporbarhet

- Teknisk sikring av informasjon
  - Begrensning av tilganger
  - Begrensning av muligheter
    - Direkte Copy/Paste er umuliggjort
    - Sterke begrensninger på hva som er mulig å utføre
  - Aldri direkte kontakt mellom administrert system og klient som aksesserer systemet

SYKEHUSPARTNER

Kontroll, sikkerhet og sporbarhet

- Intensjonen er ikke å overvåke leverandører
- Alle aksjoner må være sporbare
  - Inn- og utlogging
  - Handlinger og aksjoner logges
- Leverandører må underlegge seg SP's regime for endringshåndtering
  - Endringer skal godkjennes av SP og helseforetak
  - Ingen «skal bare» er tillatt
- For enkelte systemer vil ikke leverandørtilgang kunne gis
  - Spesielt sensitive systemer
  - Legacysystemer i isolerte nett

SYKEHUSPARTNER

Misbruk av leverandørtilgang

«***Teknologi alene gir ikke tillit***»

- Alle systemer kan misbrukes
- Underleverandører signerer personlig på
  - Taushetserklæring
  - Retningslinjer for bruk av tjeneste

Det vil alltid være mulig å komme rundt sikkerhetsforanstaltningene

- En utro underleverandør kan avfototgrafere/ta skjermdump av et skjermbilde
- En bruker kan bevisst gi fra seg påloggingsinformasjon

SYKEHUSPARTNER

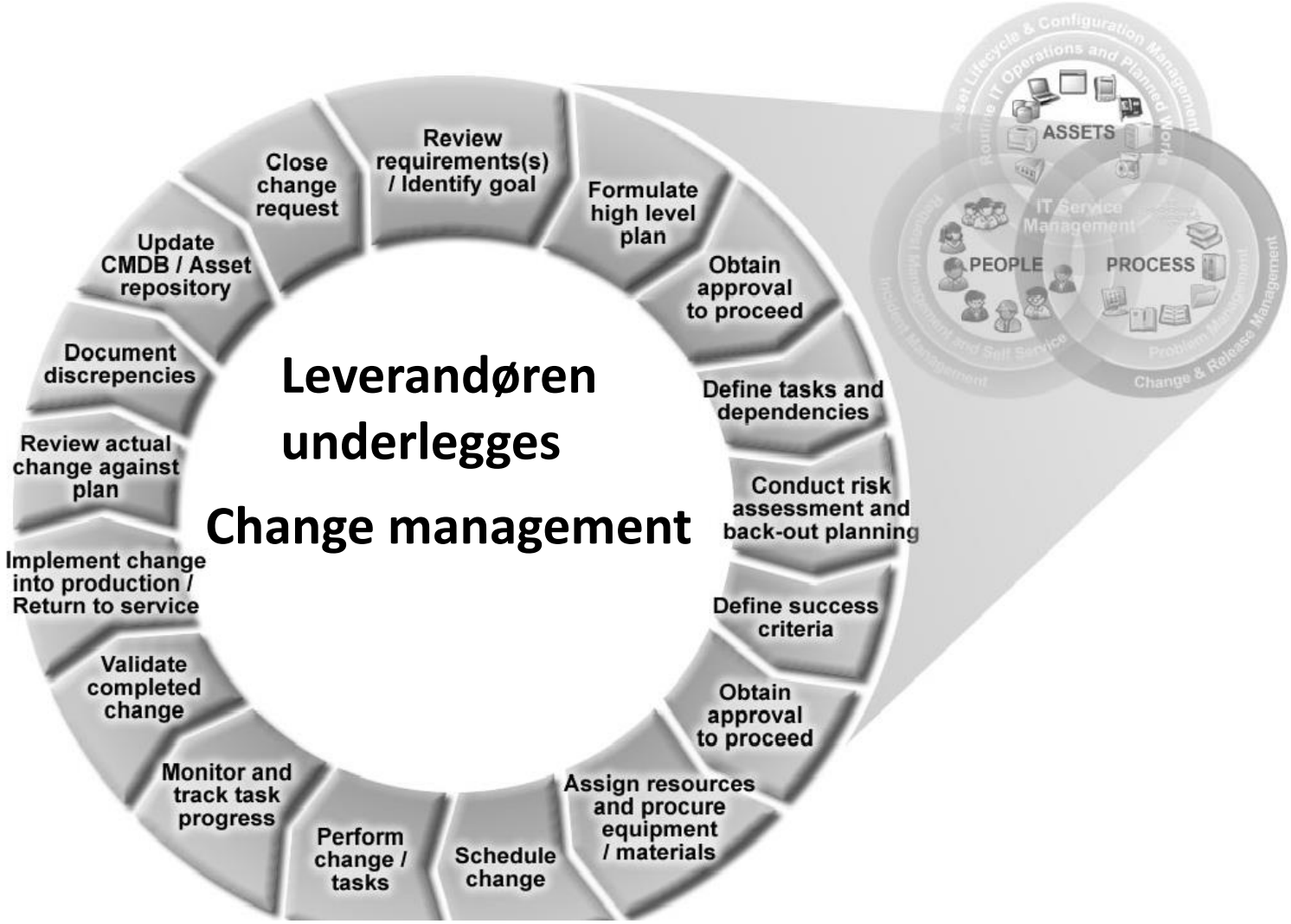
Hvordan sikrer man systemer?

Fokus må være

- Å gjøre tilgang pr bruker/leverandør så spesifikk som mulig
- Bevisstgjøring av brukere
- Bevissthet på hva er «Sikkert nok»

SYKEHUSPARTNER

Hvordan sikrer man systemer?



SYKEHUSPARTNER

Leverandøraksess i praksis

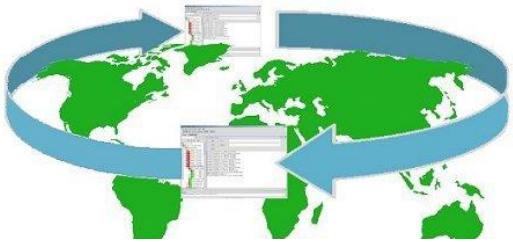
SYKEHUSPARTNER

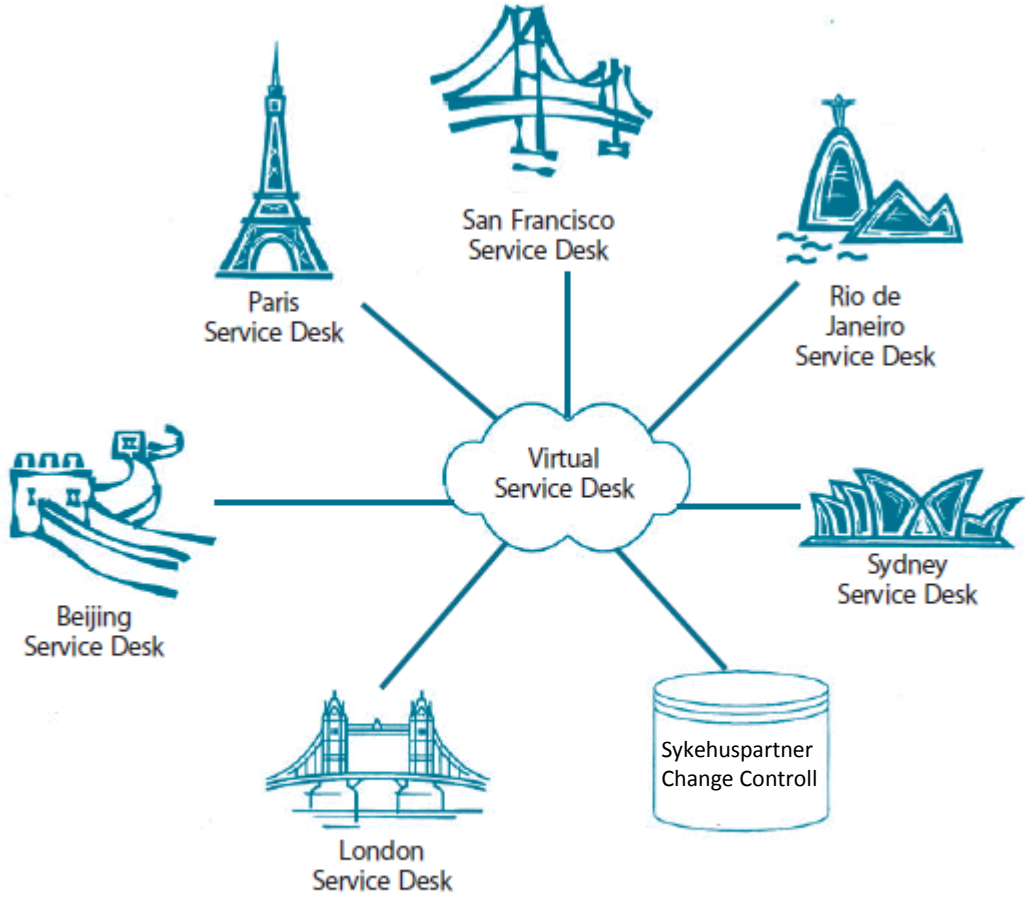
Konkrete sikkerhetsmekanismer i Sykehuspartners leverandøraksess

- Bruker må godkjennes for leverandørtilgang
  - Signering av taushetserklæring og instruks
- Bruker må være definert i AD
- 2-faktor autentisering
- Logging av aktivitet
- Bruker er kun autorisert og gis tilgang til gitte systemer, intet annet
- Copy/paste er umuliggjort
- Leverandør kan laste opp filer til filserver
  - Sykehuspartenerpersonell må håndtere derfra
- Leverandør kan ikke hente ut data fra foretakene
  - Sykehuspartenerpersonell må utføre. Oppgaven må initieres innenifra

SYKEHUSPARTNER

Follow the sun er en utfordring





SYKEHUSPARTNER

Fremtidige og delvis innførte sikkerhetsmekanismer

- Key-logging funksjoner
- Leverandøraksess er stengt, tilgang gis tidsbegrenset ved behov og personlig identifikasjon
- Enkelte systemer gis det ikke leveransdøraksess på
- Overgang fra adminservere til VDI

SYKEHUSPARTNER

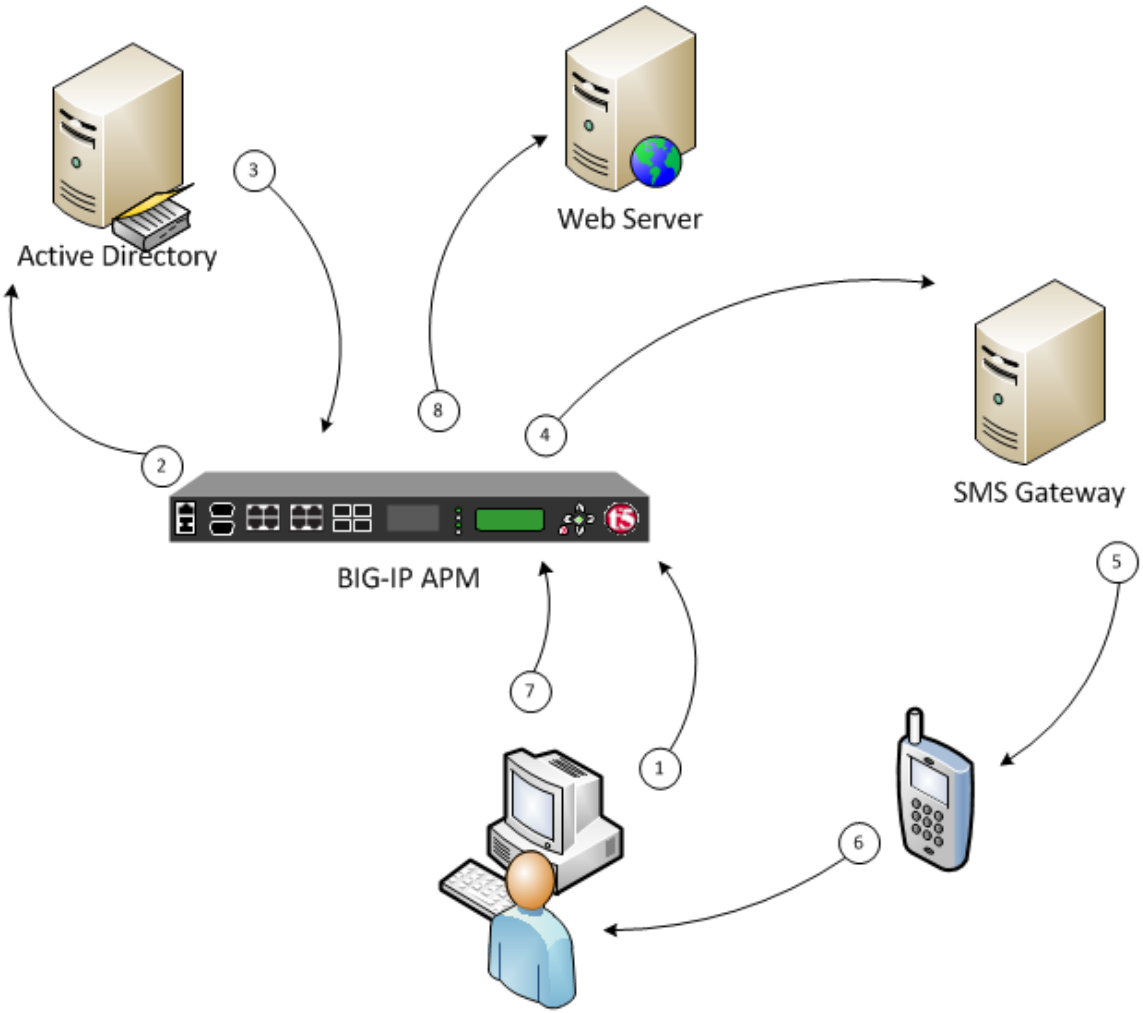
Leverandøraksess i praksis

- Leverandør sitter off-site med egen klient
- Citrix online plugin installert på klient
- Aksesserer portal

  https://drift.sykehuspartner.no

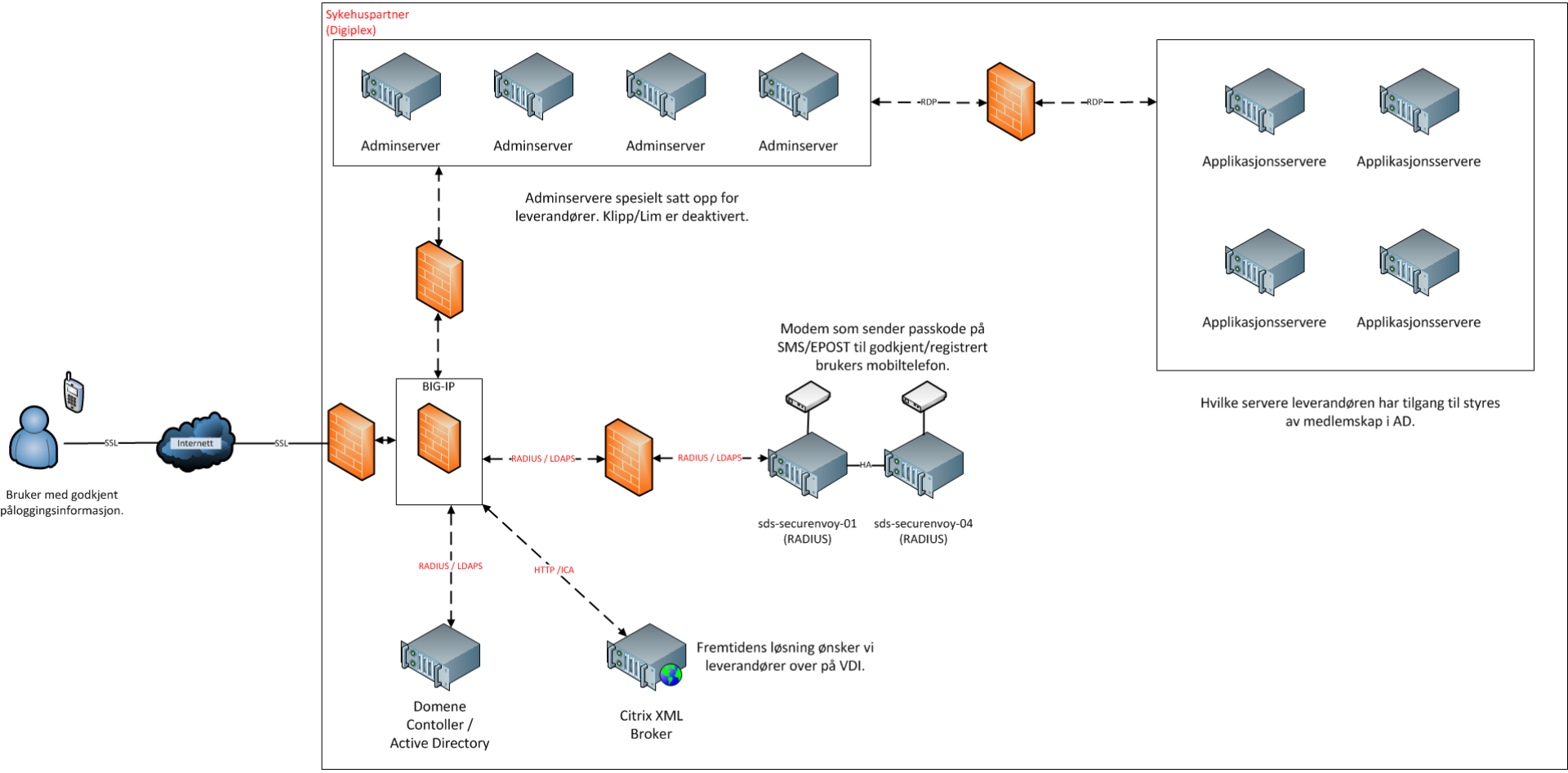
SYKEHUSPARTNER

Autentisering – konsept



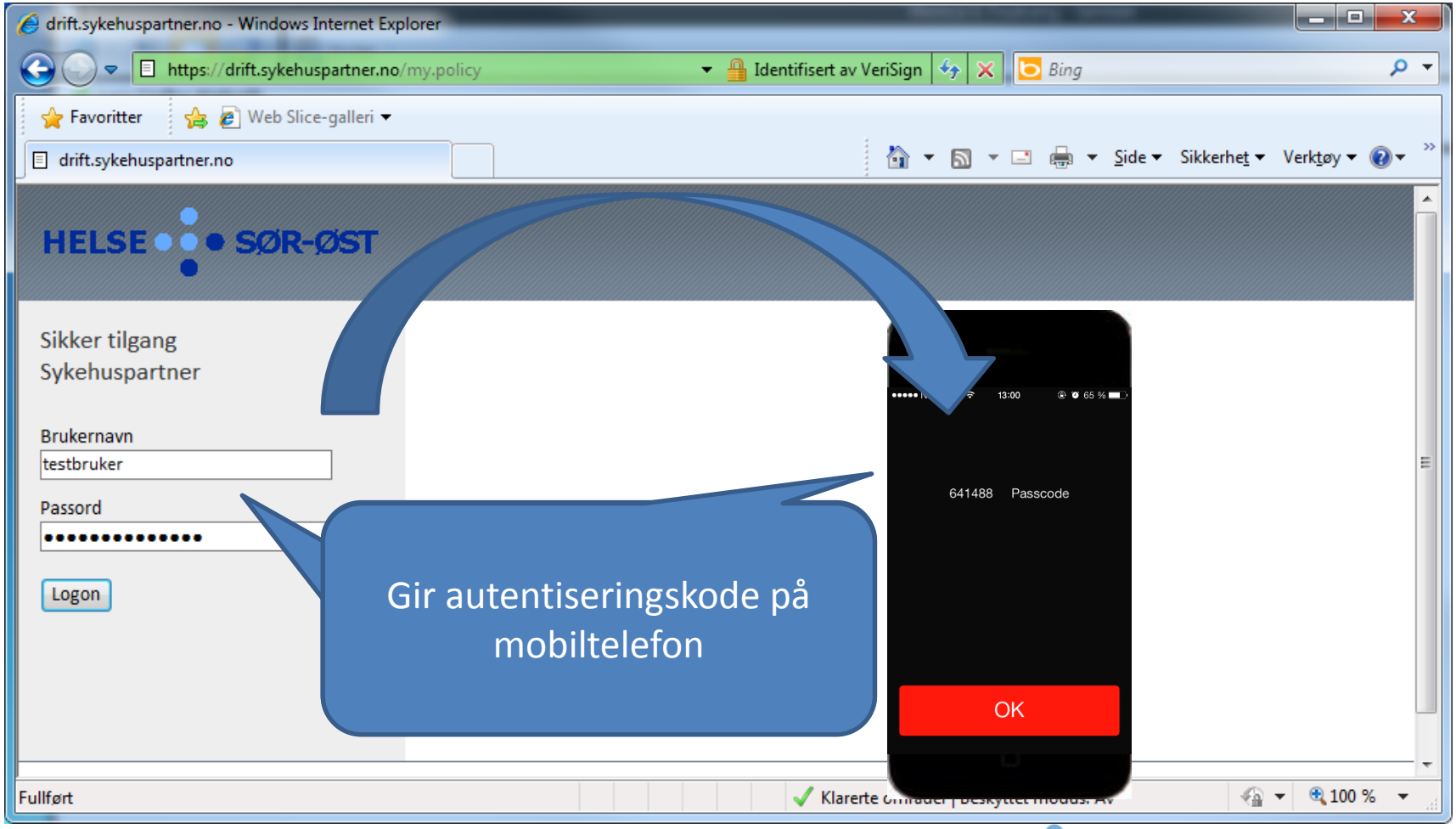
USPARTNER

Autentisering – HLD



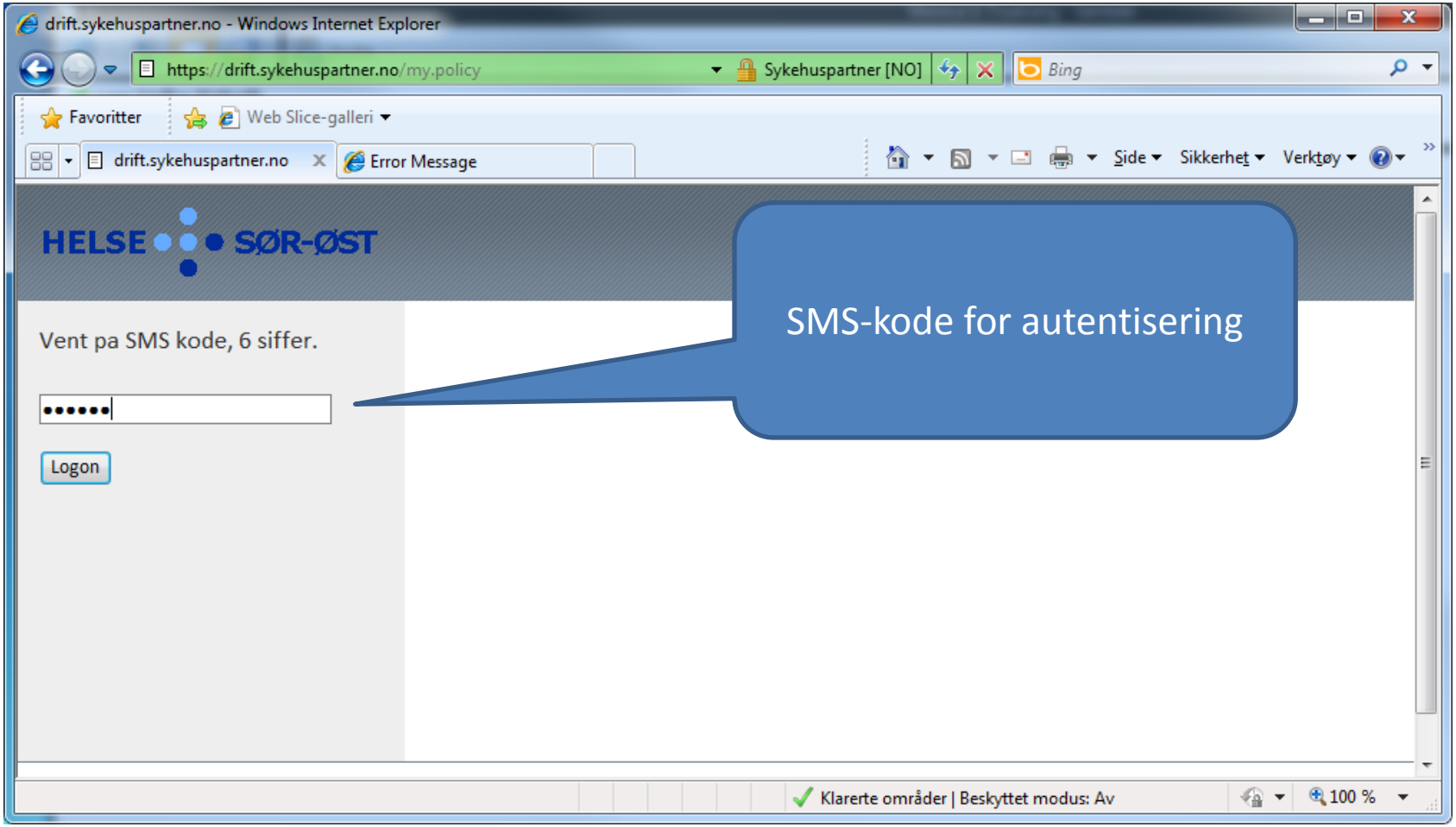
SYKEHUSPARTNER

Innlogging og autentisering



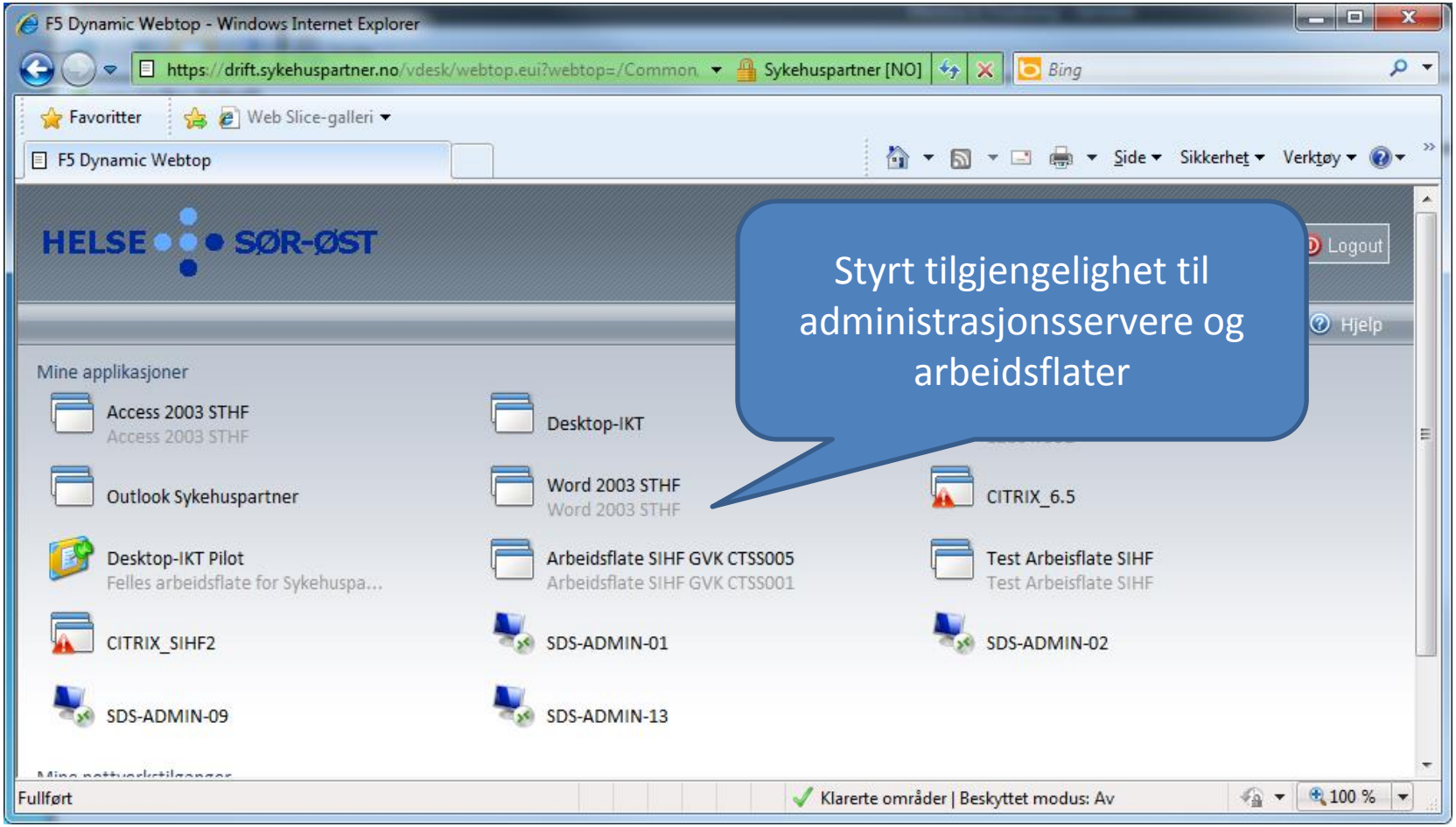
SYKEHUSPARTNER

Innlogging og autentisering



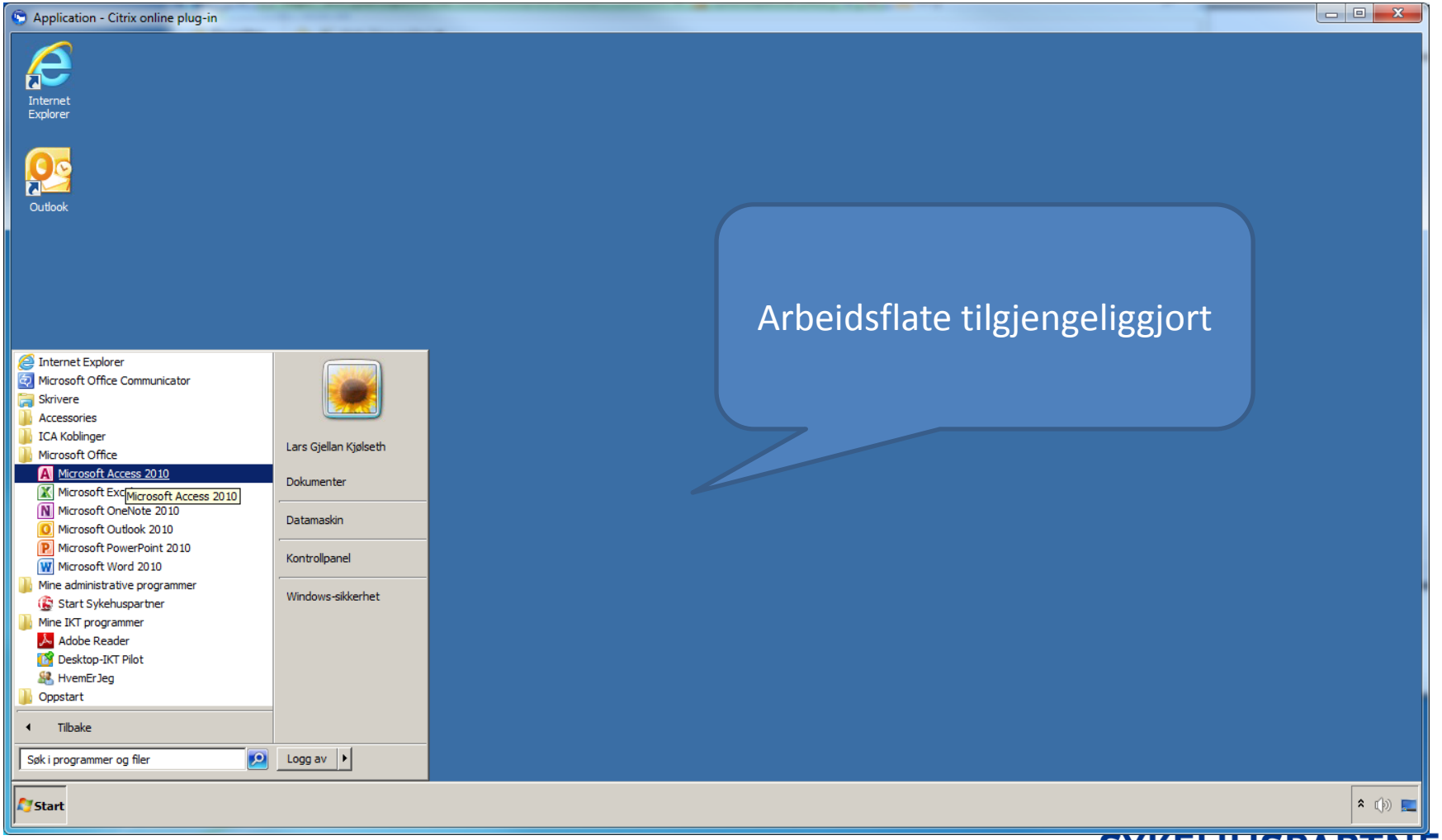
SYKEHUSPARTNER

Portal med tilgjengelige tjenester



SYKEHUSPARTNER

Arbeidsflate for leverandører



SYKEHUSPARTNER

Oppsummering

SYKEHUSPARTNER

Oppsummering

- ***Pasientsikkerhet*** i fokus
- Pasientopplysninger og sensitiv informasjon må under ***ingen omstendigheter*** komme på avveie
- Pasientsikkerhet er prioritert foran leverandørers tilgang
- Helsebehandling er avhengig av ***tillit!***
  - Tillit skapes gjennom sikkerhet i ***alle ledd***
- Systemets sensitivitet avgjør grad av leverandørtilgang

SYKEHUSPARTNER

Oppsummering

IKT, systemintegrator eller partner

som er hovedansvarlig for et selskap sine data

uansett form og farge på disse dataene

er

premissgiver for hvordan slike data skal aksesseres.

SYKEHUSPARTNER

Oppsummering

Leverandørene sier: Hvorfor er det så vanskelig å få tilgang her, ingen andre har det slik.

Viktig: Fortell og informer om prinsippene hvorfor man har et tilgangsregime.

Aksept hos leverandør begynner allerede i konkurransen under en anskaffelse:

Gi informasjon og still krav.

SYKEHUSPARTNER

Q & A

SYKEHUSPARTNER

Støtteslider

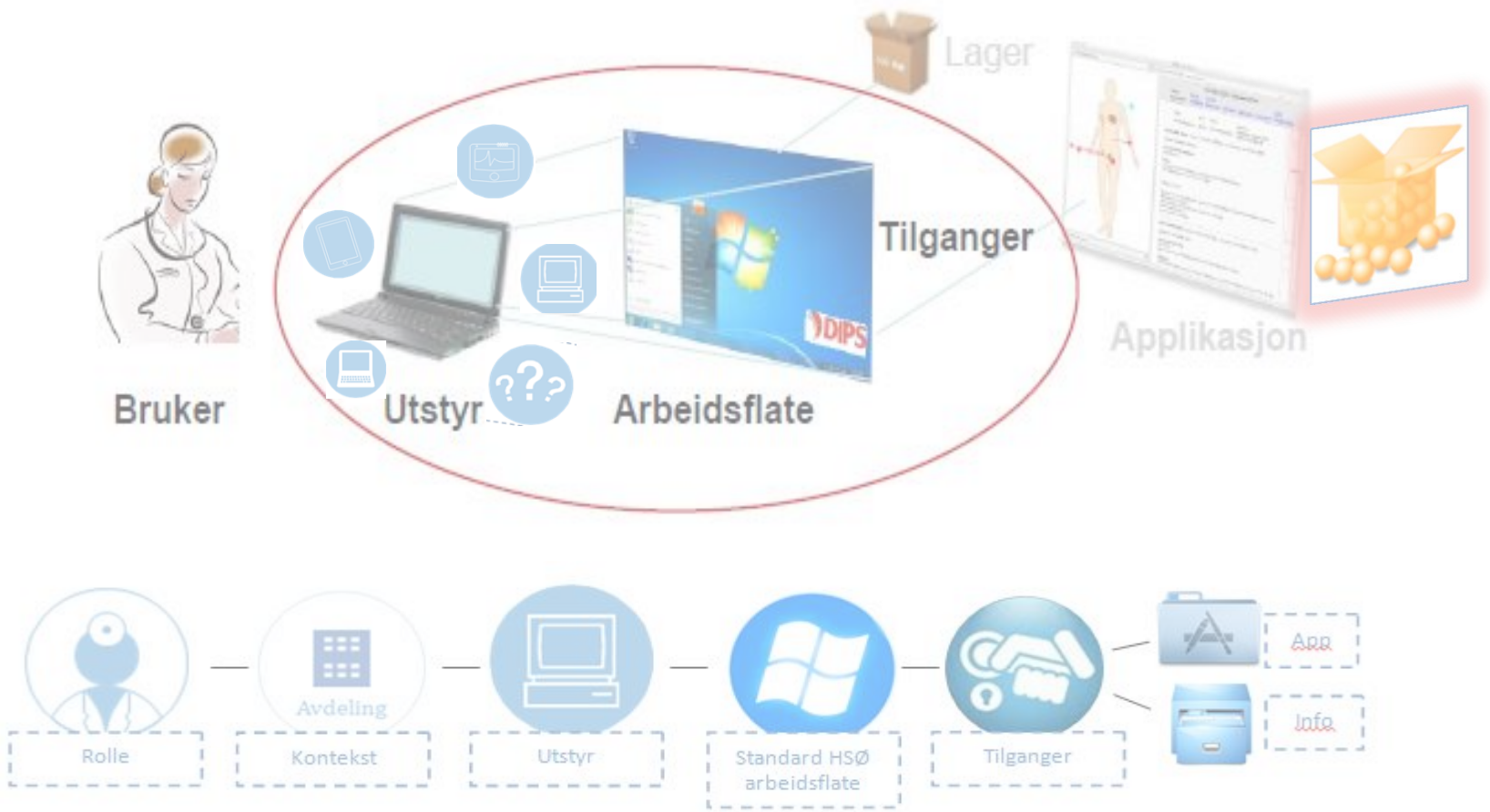
SYKEHUSPARTNER

Annet

- Vi sier intet om at
  - HF er juridiske enheter
  - Samspill og avtaleverk mellom leverandør, SP og HF

SYKEHUSPARTNER

Kontekststyrt tilgangskontroll



SYKEHUSPARTNER

Kontekststyrt tilgangskontroll

SYKEHUSPARTNER

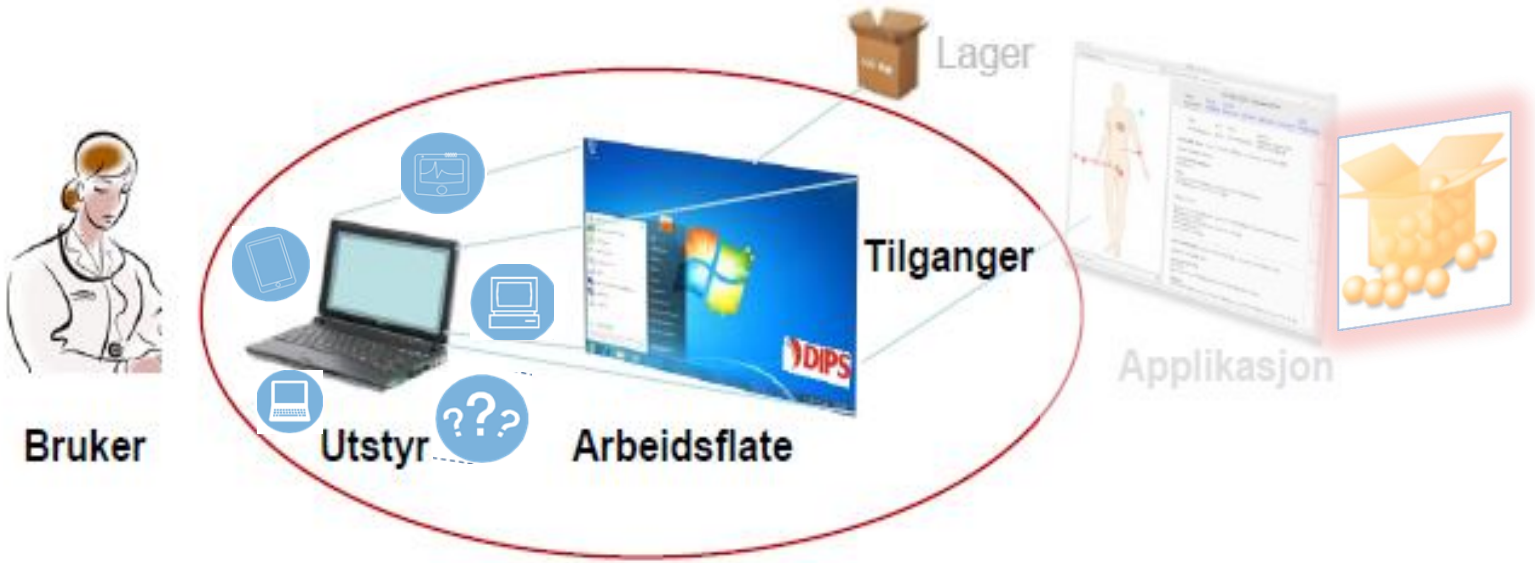
Kontekststyrt tilgangskontroll

SYKEHUSPARTNER

Kontekststyrt tilgangskontroll

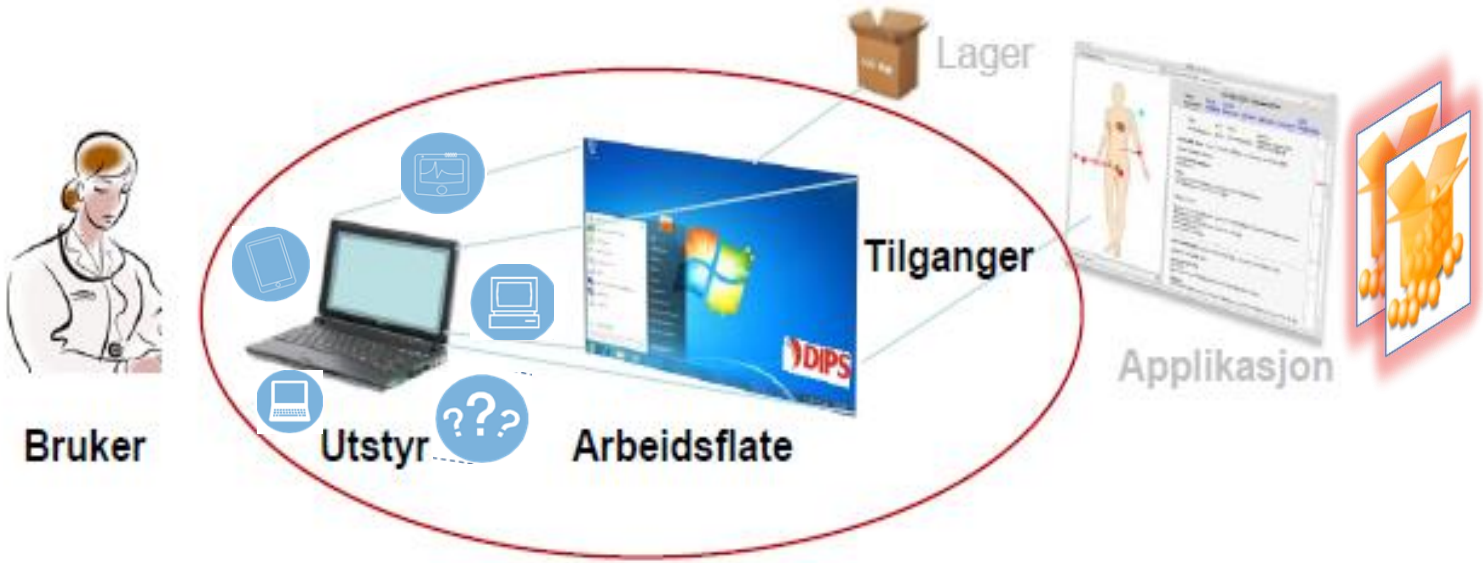
SYKEHUSPARTNER

Kontekststyrt tilgangskontroll



SYKEHUSPARTNER

Kontekststyrt tilgangskontroll



SYKEHUSPARTNER