

Tekniske erfaringer



SES@m Tromsø

Telemedisin i pleie- og omsorgstjenesten
Fyrtårnsprosjekt for bedre samordning og
kontinuitet i helsesektoren

Det kan fritt kopieres fra denne publikasjonen hvis kilden oppgis. Brukeren oppfordres til å oppgi rapportens navn, forfatter, samt at den er utgitt av Nasjonalt senter for telemedisin og at den i sin helhet er tilgjengelig på www.telemed.no.

© 2006 Nasjonalt senter for telemedisin

Innhold

1	Innledning	4
1.1	Om dokumentet og målgruppen	4
1.2	Forfattere	4
2	Datatekniske utfordringer og erfaringer	5
2.1	Programvare	5
2.1.1	<i>Well Communicator - elektronisk samhandling</i>	5
2.1.2	<i>Safeboot – Harddiskkryptering og oppstartspærre</i>	6
2.1.3	<i>PKI og digitale sertifikater</i>	7
2.1.4	<i>Checkpoint Secure Client VPN</i>	7
2.1.5	<i>Checkpoint SSL Network Extender VPN</i>	8
2.1.6	<i>Internet Explorer</i>	8
2.1.7	<i>Fingeravlesningsteknologi fra IBM</i>	8
2.1.8	<i>SkaniX® Illusion</i>	9
2.1.9	<i>Programvare fra Thales Communication</i>	9
2.1.10	<i>Unique Profil (fagsystem for pleie- og omsorgssektoren)</i>	10
2.1.11	<i>Citrix Metaframe</i>	11
2.1.12	<i>Powerfuse</i>	11
2.2	Maskinvare og nettverk	11
2.2.1	<i>Tilkobling mellom Tromsø kommune og Norsk Helsenett AS (NHN)</i>	11
2.2.2	<i>Bærbar PC</i>	12
2.2.3	<i>Datalinjer til distriktssonene i Tromsø kommune</i>	13
2.2.4	<i>Digitalt kamera og diodelys</i>	14
2.2.5	<i>Mobiloperatører og mobilkort</i>	14
2.2.6	<i>Autentiseringsenheter til mobil tilgang</i>	16
2.3	Forsinkelser og låste skjermbilder	16
2.3.1	<i>Fra stasjonær PC i LAN</i>	16
2.3.2	<i>Fra mobil PC</i>	17
3	Organisatoriske erfaringer i prosjektet	18
3.1	Opplæring og brukerstøtte i fokus	18
3.2	Drift av prosjektet	18
4	Tromsø kommunes erfaringer fra prosjektet	20
4.1	Bruk av frontteknologi i miljøer med lav datakompetanse blant brukerne	20
4.2	Etablere pilotprosjekter i eksisterende driftsmiljø	20
4.3	Andre organisatoriske utfordringer	21
5	Oppsummering av erfaringer	22
5.1	Tekniske erfaringer	22
5.2	Organisatoriske erfaringer	22
5.3	Erfaringer med support og oppfølging	23
5.4	Erfaringer gjort med tanke på ressursplanlegging	23
6	Forkortelser	24
7	Referanser	25
8	Vedlegg 1 - Test av Option GlobeTrotter Fusion med Telenors Mobilt Kontor	26
9	Vedlegg 2 – Test av nedlastningshastighet på EDGE- og UMTS-kort i Tromsø by	29

1. Innledning

1.1 Om dokumentet og målgruppen

Dette dokumentet består av en samling erfaringer som ble gjort i forbindelse med design og implementering av de tekniske løsningene i SES@m Tromsø-prosjektet.

Målgruppen er personell som er involvert i beslutningstaking, design av eller implementering av IKT-systemer i en kommune.

I dette dokumentet vil det ikke bli gitt noen utdypende forklaring på produkter, tjenester og samarbeidsparter i SES@m Tromsø. Dette er omtalt i dokumentet "Teknisk dokumentasjon". Se kapittel 7 "Referanser".

Det er i dette dokumentet benyttet noen symboler som trenger en forklaring:

☺ Brukes for å markere en positiv erfaring eller forhold som fortjener ros.

☹ Brukes for å markere en negativ erfaring eller kritikkverdige forhold.

→ Brukes for å markere et konkret tips eller teknisk råd.

1.2 Forfattere

Nasjonalt Senter for Telemedisin (NST) har utarbeidet dette dokumentet i samarbeid med Tromsø kommune. Forfatter: Harald Øverli Eriksen. I tillegg har følgende bidratt fra NST: Daniel Nygård, Lisbeth Remlo Abelsen og Eva Skipenes.

Kapittel 4. "Tromsø kommunes erfaringer fra projektet" er skrevet av Vidar Størkersen, Frank Johansen og Roger Hansen fra Tromsø kommune.

2. Datatekniske utfordringer og erfaringer

2.1 Introduksjon

Dette kapitlet beskriver hvilke tekniske løsninger som ble valgt og erfaringer gjort underveis i prosjektet. Det blir gjort rede for programvare-, maskinvare- og nettverkløsninger. Til slutt i kapitlet drøftes grunnene til forsinkelser og problemer med låste skjermbilder.

2.1 Programvare

2.1.1 *Well Communicator - elektronisk samhandling*

Well Communicator er et av produktene til firmaet Well Diagnostics AS (Well). Well Communicator hadde aldri før blitt benyttet som sluttbrukerapplikasjon i en kommune, og Well gjorde mange tilpassninger i Well Communicator underveis i prosjektet. Den versjonen av Well Communicator som kjørte hos kommunen ved SES@m Tromsø-prosjektets slutt var et resultat av gjentatte iterasjoner med tilpasning, testing, installasjon og drift.

Det ble jobbet tett med Well gjennom hele prosjektperioden for å få tilpasset programvaren slik at den ville fungere i en kommune. Programvaren ble så testet i et testnettverk hos NST før den ble installert og rullet ut til utvalgte institusjoner hos kommunen. Denne prosessen gjentok seg når feil ble oppdaget og nye krav fra brukerne krevde det.

Under kommer noen utfordringer forbundet med bruk av Well Communicator som ikke hadde sitt opphav i selve programvaren.

Well Communicator ikon ikke tilgjengelig eller fungerte ikke

Etter å ha logget inn i Citrix Metaframe ble de programmene brukerne hadde tilgang til vist som ikoner. Det forekom at brukere ikke fikk vist Well Communicator ikonet fordi deres rettigheter ikke var riktig satt opp i Active Directory i kommunens datanettverk. Det forekom også at ikonet ble vist men at Well Communicator ikke startet når brukerne klikket på ikonet.

Feilmeldinger fra databasen

Hvis man installerte Well Communicator på standard måte brukte den en flatfilddatabase for å lagre alle sine opplysninger i. Well Communicator med flatfilddatabase er kun anbefalt fra Well å bruke på legekontorer og andre steder der antall lagrede meldinger og antall brukere ikke blir for stort. Installasjonen av Well Communicator i kommunen involverte mange brukere og eksterne partnere, og mengden meldinger i databasen ble mye større enn anbefalt fra Well. Det ble derfor observert mange feilmeldinger i Well Communicator som var relatert til flatfilddatabasen. Etter hvert ble flatfilddatabasen byttet ut til fordel for Microsoft SQL server 2005. Det ble vurdert å bruke en lettvektsgutgave og gratisversjon av MS-SQL, SQL Server 2005 Express Edition. Denne ble ikke benyttet fordi kommunen ikke ville bygge seg opp kompetanse på et "nytt" produkt som i fremtiden ikke ville vise seg å være dimensjonert for kommunen (utilstrekkelig ytelsen, støtte for et for lite antall brukere etc.)

Utskrift

Da Well Communicator ikke var integrert med fagapplikasjonen Unique Profil, var det veldig viktig å få skrevet ut meldinger som ble mottatt i Well Communicator for å få samlet all pasientinformasjon på ett sted. Det hendte ofte at brukerne ikke fikk skrevet ut fra Well Communicator, eller at utskrifter havnet på en annen skriver enn den brukeren forventet å finne utskriften på. Well Communicator benyttet standardskriver definert i Windows. Kommunen benyttet en programvare som heter Thinprint for å ta seg av utskrift fra Citrix Metaframe. Utskriftproblemene i forbindelse med Well Communicator kom av at:

- Thinprint var ikke konfigurert på riktig måte eller ikke installert
- Det var ikke valgt lokal printer på PC
- Brukerprofilen til brukerne ikke hadde fått tilstrekkelige rettigheter.

Forsinkelse på skjermoppdatering, mus- og tastaturkommandoer

Brukerne på stasjonære PCer på de distriktsonene som hadde underdimensjonerte linjer inn til servere sentralt hos kommunen, og bruker på bærbare PCer med dårlig dekning, opplevde lang forsinkelse på skjermoppdatering, mus- og tastaturkommandoer når de brukte Well Communicator og Unique Profil.

Problemer med meldingsutvekslingen som følge av

- IP-konflikt mellom Norsk Helsenett AS og kommunen. Se kapittel 2.2.1 "Tilkobling mellom Tromsø kommune og Norsk Helsenett AS (NHN)" for mer informasjon.
- Feilkonfigurering og vedlikehold. Det hendte at det ble gjort endringer internt i kommunen som gjorde at meldingsutvekslingen stoppet opp i kortere eller lengre tidsrom.

Feil oppsett av krypteringsnøkler

Meldingsutvekslingen i Well Communicator krypterte meldinger med symmetriske nøkkel-par. Dette betyr at den samme nøkkelen brukes for å kryptere og dekryptere. På grunn av feil oppsett av krypteringsnøkler i en av partenes installasjoner hendte det at meldinger ikke ble mottatt korrekt.

Kompatibilitetsproblemer mellom nye og gamle versjoner

På Hudavdelingen på UNN ble en eldre versjon av Well Communicator, kalt Doris Professional, brukt. Doris hadde fungert godt i flere år, men vi opplevde at sårmeldinger sendt fra kommunen plutselig ikke kunne hentes inn i Doris. Årsaken til dette var sannsynligvis at nye maler i Well Communicator ikke var kompatible med Doris. Ved overgang til Well Communicator på Hudavdelingen ble problemet løst.

2.1.2 Safeboot – Harddiskkryptering og oppstartspærre

Safeboot er et produkt som kan settes opp til å kryptere harddisken og kreve autentisering før oppstart av pc tillates. Vi kjørte dette produktet på de bærbare PCene i test en periode og benyttet det på en institusjon en tid. Det var aldri meningen at noen sensitive data skulle lagres på de bærbare PCene, men etter å ha kjørt risikoanalyse av den mobile oppkoblingen ble det besluttet å sikre de bærbare PCene med Safeboot. Hvis det mot formodning allikevel skulle finnes sensitive opplysninger på de bærbare og de skulle komme på avveie ville dataene være uleselig.

Det var flere ting med Safeboot som ikke var tilfredsstillende:

- Safeboot var ikke helt stabilt og vi opplevde at den bærbare PCen låste seg som følge av Safeboot
- Dette var et nytt produkt for leverandøren og det var derfor vanskelig å få hjelp og support
- Det var meget enkelt for brukerne å fjerne Safeboot fra de bærbare PCene. Dette gjorde det enkelt å omgå hele sikkerhetsmekanismen.

Det ble derfor bestemt å ikke bruke Safeboot eller harddiskkryptering men heller fjerne alle muligheter for å lagre, registrere og editere pasientinformasjon på lokal harddisk på de bærbare PCene. Dette ble gjort ved å fjerne alle programmene som kunne benyttes for å legge inn mulige sensitive data (MS Word, Notepad, Wordpad). Programmer som benyttes til å behandle sensitive data kjøres på kommunens server med tynn klient ut til de mobile PCene.

- ⊕ Prosjektet kjøpte inn et produkt det ikke var behov for og som ikke holdt mål. Leverandøren kunne ikke yte tilstrekkelig support.

→ Mulig løsning: Bruk tilstrekkelig tid til å teste ut produkter før innkjøp blir vurdert. Snakk med andre som har benyttet produktene over tid.

2.1.3 PKI og digitale sertifikater

Det var et mål i prosjektet å benytte PKI og digitale sertifikater for å kryptere EDI-trafikk mellom de involverte kommunikasjonspartnerne. Dette ble det ikke noe av fordi prosjektet anså det som en forutsetning at HER-registeret var på plass før det ville lønne seg å ta i bruk PKI. HER-registeret (Helse-enhets-registeret skal være en adressekatalog som viser adresser til de ulike enhetene innen helsevesenet som man kan kommunisere med). Det hersker en viss usikkerhet om HER-registeret faktisk tar høyde for kommunal sektor fordi HER i utgangspunktet er tilrettelagt for spesialisthelsetjenesten. Det ble i stedet benyttet symmetriske nøkkelpar for å kryptere trafikken.

- ⊕ Det er mye arbeid å publisere og vedlikeholde symmetriske nøkkel når antall parter som skal kommunisere øker.

→ Mulig løsning: Benytt PKI, digitale sertifikater og HER-registeret.

2.1.4 Checkpoint Secure Client VPN

Vi benyttet Checkpoint Secure Client VPN for å sikre en kryptert tunnel fra bærbar PC til sentral server hos kommunen. Dette produktet passet ikke helt bra i dette prosjektet. Checkpoint Secure Client VPN etablerte en tunnel fra en programvare på klienten til brannmuren hos kommunen. I dette prosjektet brukte mange brukere de samme bærbare PCene. I Checkpoint Secure Client VPN var det ikke tatt høyde for å ivareta brukervennligheten på en god nok måte for dette scenarioet. Når en ny bruker skulle overta en bærbare PC etter en annen, var det nødvendig å gjøre noen konfigureringsendringer i Checkpoint Secure Client VPN. Dette ble rett og slett en for stor terskel for brukerne med begrenset datakompetanse. Med tanke på vedlikehold var det heller ikke ønskelig å ha en klientinstallasjon på de bærbare PCene som var plassert ute i distriktet.

☹ Checkpoint Secure Client VPN er lite brukervennlig når flere brukere skal bruke den samme PCen.

→ Mulig løsning: Benytt annen løsning. For eksempel Checkpoint SSL Network Extender (se eget kapittel)

☹ Det krever mer arbeid å vedlikeholde VPN-løsninger der man må ha en programvare installert på klienten

→ Mulig løsning: Benytt klientløs VPN. For eksempel Checkpoint SSL Network Extender (se eget kapittel)

2.1.5 *Checkpoint SSL Network Extender VPN*

Vi gikk over til Checkpoint SSL Network Extender etter å ha benyttet Checkpoint Secure Client VPN på en distriktssone i to måneder. Checkpoint SSL Network Extender er en klientløs VPN-løsning der en applet på 7-800 Kb lastes ned fra serveren ved hver pålogging.

☺ Ingen klientinstallasjon lokalt, og skaper derfor ikke vedlikehold på klientene

2.1.6 *Internet Explorer*

I Tromsø kommune benyttet brukerne Internet Explorer for å logg inn i Citrix Metaframe og få tilgang til sine applikasjoner. Dette fungerte bra. På de stasjonære PCene i kommunen foregikk surfing på Internett på en kontrollert måte ved at dette skjedde i en egen Citrix-sesjon. De bærbare PCene som er utstyrt med mobilkort hadde en mer "direkte" tilgang til Internett. For å unngå nedlastning av uønsket programvare og virus til de bærbare PCene ble sensurmekanismen i Internet Explorer benyttet. Kun nødvendige servere hos kommunen ble tillatt aksessert. Brukerne hadde allikevel tilgang til Internett, men måtte da gjøre dette gjennom en Citrix-sesjon, og da gjennom kommunens brannmur. Dette fungerte også bra. Konfigurering av hva som skulle sensureres ble passordbeskyttet slik at det kun var IT-avdelingen som kunne gjøre endringer.

☺ Bruk av Internet Explorer for å logg inn i Citrix Metaframe fungerer bra.

☺ Sensurmekanismen i Internet Explorer fungerer bra for å kun tillate brukerne tilgang til bestemte sider på Internett. Denne tilgangskontrollen er ikke aktiv ved bruk av andre Internett browser programmer.

2.1.7 *Fingeravlesningsteknologi fra IBM*

Vi hadde en del møter med IBM og vurderte å benytte deres løsning for fingeravlesning. Dette kunne være et godt alternativ til Aladdins eToken og RSA SecureID som ble benyttet for å sikre tilgang fra de bærbare PCene til sentrale servere hos kommunen. eTokenet kunne blitt gjenglemt, mistet eller skadet slik at det ikke fungerte. Med fingeravlesning slipper vi muligens dette problemet, men fingeravlesning er sensitiv for rifter/sår/malingsflekker/kalde fingre osv., som kan utgjøre et problem.

Det ble reist juridiske spørsmål rundt det å oppbevare ansattes fingeravtrykk i en sentral database. Dette var noe datatilsynet var skeptisk til. Fingeravlesning fra IBM som autenti-

seringsmetode ville kreve en del ekstra lisenser/servere for å få til en single sign-on løsning. Kommunen ønsket å benytte RSA SecureID som autentiseringsmekanisme da de kunne levere den mest komplette løsningen.

2.1.8 Skanix® Illusion

Det er veldig ressurskrevende å holde bærbare PCer lokalisert ute i distriktet oppdatert og fungerende. For å redusere denne jobben ble et produkt fra Skanix AS som heter Skanix® Illusion prøvd ut. Skanix® Illusion er et program som installeres på den PCen som skal beskyttes mot endringer. Det fungerer slik at alle endringer som blir gjort på PCen blir overvåket og tilbakestilt når PCen slås av og på. Dette betyr at alle feil som skyldes at brukerne har gjort endringer på systeminnstillinger, installert programmer, introdusert virus og uønskede programmer etc. blir fjernet bare ved å slå PCen av og på.

2.1.9 Programvare fra Thales Communication

2.1.9.1 Thales Trusted Mail Plug-in (TMP)

Thales Trusted Mail Plug-in (TMP) er en plug-in til Microsoft Outlook og skal forhindre uforsettlig/ufrivillig sending av sensitiv e-post. Brukeren lager og sender e-post med MS Outlook og TMP overvåker flere ting; ekstensjonen på filer som legges ved en e-post, hvilke område på serveren vedlagte filer stammer fra, opprinnelsen til innhold som er kopiert og limt inn i e-posten. Avhengig av innholdet i e-posten eller hvor innholdet stammer fra vil TMP merke e-posten som sensitiv eller ikke sensitiv. E-post som er markert som sensitiv vil bare kunne bli sent til forhåndsgodkjente mottakere. Skal e-posten sendes til andre vil den bli markert som blålystrafikk og brukeren må begrunne utsendelsen. Dette blir loggført. Kun brukere som er godkjent for å sende blålystrafikk kan gjøre det.

TMP var en relativt ung programvare og hadde ikke blitt brukt i en kommune før. Well og Thales Communications AS modifiserte sine produkter slik at de kunne sende meldinger seg i mellom. Denne integrasjonen ble bare testet i småskalamiljø og TMP ble ikke tatt i bruk i prosjekt slik det først var tenkt. I stedet ble Well Communicator benyttet. En av grunnene til dette var at det å ferdigstille integrasjonen mellom Well Communicator og TMP innebar mye mer utvikling enn først antatt. I tillegg var det nødvendig å kjøpe eller lage en programvare som kunne filtrere e-postmeldinger. Thales hadde erfaringer med og lagt opp til å bruke Clearswift Mailsweeper til denne jobben. Clearswift Mailsweeper kostet mye, NOK 75.000 for 500 brukere det første året og NOK 15000 de neste årene. Tromsø kommune ville komme til kun å bruke en brøkdel av Mailsweepers funksjonalitet. Det var derfor uaktuelt å gå til innkjøp av Clearswift Mailsweeper. Det å lage denne programvaren selv var det ikke rom for i prosjektet. Det at et produkt som Clearswift Mailsweeper var nødvendig for å få TMP opp å kjøre ble aldri kommunisert til prosjektet fra Thales. Dette kom som en stor overraskelse på prosjektet og ble oppdaget i arbeidet med integreringsprosessen mellom Well Communicator og TMP.

⊕ Alle aspekter ved TMP ble ikke tilstrekkelig belyst før det ble bestemt å benytte dette produktet i prosjektet.

→ Mulig løsning: Bruke tilstrekkelig tid til å undersøke produkter og hvor ferdigutviklede utprøvde de er før de velges ut til å være bærebjelker i teknisk løsning. Snakk med andre som har benyttet produktene over tid.

- ☺ Konseptet til TMP med å forhindre uforsettlig/ufrivillig sending av sensitiv e-post er interessant, men TMP som produkt var ikke kommet mer enn til prototyp-nivået.

2.1.9.2 *Trusted VPN (TVPN)*

Med Thales Trusted VPN solution (TVPN) kan man sette opp en sikker tunnel fra bærbar PC til sentral server på innsiden av en brannmur i et privat nett. Det er et PCMCIA-innstikkskort (TVPN-kort) i den bærbare PCen som tar seg av dekrypterings-/krypteringsjobben på klientsiden. Når man benytter TVPN-kortet stenges alle andre datanettverkskoblinger enn den som går gjennom TVPN-kortet. Ulempen med TVPN-kortet er at det bare kan kommunisere til omverdenen ved hjelp av infrarød-port (IR) eller TCP/IP-port. Skal man bruke TVPN-kortet i en mobil kontekst medfører dette at man må ha en mobiltelefon med IR-grensesnitt for å få til koblingen mellom TVPN-kortet og Internett.

Da teknisk løsning ble designet første gang var ikke EDGE- og UMTS-nettene godt nok utbygd, derfor var vi fast bestemt på å bruke TVPN-løsningen til Thales. Det viste seg etter hvert at TVPN-løsningen inneholder en del fallgruver for en lite datakyndig bruker og det ble derfor besluttet å bruke EDGE- og UMTS-nett og tenkologi. Det å bruke en mobiltelefon som skal kommunisere via IR mens du er på farten i en bil er vanskelig å gjennomføre og kan føre til mange brudd i kommunikasjonen. Både mobiltelefonen og den mobile enheten må være i samme posisjon uten hinder imellom for at IR-kommunikasjonen ikke skal bli brutt. Thales TVPN-løsningen binder oss også til å kommunisere over GPRS-mobilnettet uten mulighet til å benytte de raskere EDGE- eller UMTS-mobilnettene.

- ☹ Kommunikasjon over IR-port. Dette medfører stor fare for brudd i kommunikasjonen for mobile brukere som skal bruke løsningen fra bil eller andre steder der man ikke har tilgang til å sette den bærbare PCen fra seg på et stabilt underlag.
- ☹ Ikke mulig å benytte EDGE- eller UMTS-mobilnettene uten å koble til ekstra hardware. Dette vil gjøre løsningen mindre mobil.
- ☹ TVPN er kostbart.
- ☹ TVPN er en VPN-løsning med meget høy sikkerhet med tanke på hacking/innbrudd. Grunnen er at kryptering/dekryptering skjer i PCMCIA-innstikkskortet på den bærbare PCen uten hjelp eller kontakt med operativsystemet. Det er derfor ikke mulig å utnytte feil eller mangler i operativsystemet for å lage bakveier inn i systemet. Kunder med meget høy krav til sikkerhet har valgt TVPN (forsvaret og politi)

2.1.10 *Unique Profil (fagsystem for pleie- og omsorgssektoren)*

Tromsø kommune bruker programvaren Unique Profil som sitt pleie- og omsorgssystem. Kommune har foreløpig valgt å ikke gå til anskaffelse av den ekstramodulen til programmet som skal gjøre det mulig å motta elektroniske meldinger fra blant annet Well Communicator. Pasientinformasjonen som kom inn til sykehjemmet eller hjemmetjenesten (i Well Communicator) ble derfor skrevet ut og lagret i papirjournalen.

Visma Unique kom med tilbud på modulen, men da den var relativt dyr og heller ikke var ferdig pilotert var det uaktuelt for kommunen å gå til innkjøp av den på nåværende tidspunkt. Det var meget beklagelig fordi en integrering mellom Well Communicator og Unique Profil

ville ført til at brukerne ble tvunget til å bruke journalsystemet til å lese meldinger fra sykehuset, noe som kanskje ville vært et incitament til ytterligere bruk av elektronisk pasientjournal. I tillegg ville brukerne da kun hatt ett brukergrensesnitt å forholde seg til. Da ville det heller ikke vært nødvendig å skrive ut labsvarene og epikrisene fra Well Communicator for så å lagre det i papirjournal. For å kunne sende meldinger ville brukerne imidlertid måtte forholde seg til Well Communicator, da Visma Unique ikke hadde utviklet en modul for sending av meldinger før prosjektet ble avsluttet.

2.1.11 Citrix Metaframe

Isolert sett har Citrix Metaframe fungert meget godt både stasjonært og mobilt. De problemene vi erfarte med Citrix Metaframe kan relateres til at systemet ikke var riktig konfigurert. Det hendte blant annet ved flere anledninger at brukere ikke var blitt tildelt nok rettigheter slik at de derfor ikke fikk tilgang til sine applikasjoner.

2.1.12 Powerfuse

I Citrix Metaframe miljø er det vanligvis ønskelig å hindre brukere fra å overføre filer fram og tilbake mellom klient og server. Ved å benytte et produkt som heter Powerfuse var det mulig å overføre bilder fra digitalkamera eller kameraminnekort-leser tilkoblet klientmaskinen ved hjelp av USB-grensesnitt til EDI-server. Da vi gikk til innkjøp av Powerfuse ble vi forespeilet at dette var en programvare som var i stand til å gjøre en enda mer detaljert filtrering på datatrafikken enn det som viste seg å være mulig. Det skulle blant annet være mulig å sette opp Powerfuse til å bare slippe gjennom filer med forhåndsdefinerte filtyper, fra forhåndsdefinerte tynne klienter. Dette vist seg å ikke være tilfelle. Det Powerfuse kunne bidra med for å øke sikkerheten var å kun tillate overføring av data en vei, dvs fra bærbare Pcer til EDI-serveren i kommunens nett.

⊕ Prosjektet kjøpte inn dette produkt i den tro at det ville høyne sikkerheten mer enn det faktisk gjorde.

→ Mulig løsning: Bruk tilstrekkelig tid til å teste ut produkter før innkjøp blir vurdert. Snakk med andre som har benyttet produktene over tid.

2.2 Maskinvare og nettverk

2.2.1 Tilkobling mellom Tromsø kommune og Norsk Helsenett AS (NHN)

Denne tilkoblingen var på plass da prosjektet startet. Dette var en jobb kommunen hadde gjort i samarbeid med NHN. Se dokumentet "Teknisk dokumentasjon" for tekniske detaljer.

Sommeren 2005 gikk NHN over til å bruke private IP-adresser i kommunikasjonen med kommunen. Det ble i ca to måneder umulig å kjøre meldingsutveksling i Well Communicator for enkelte av kommunens institusjoner. Problemet oppstod fordi kommunen og NHN brukte de samme private IP-nettadressene. Dette ble løst ved at kommunen byttet IP-nettadresser.

⊕ Det er meget bekymringsverdig at NHN som landsdekkende nettverksaktør og tjenestetilbyder i helsevesenet benytter seg av private IP-adresser. Private IP-adresser brukes normalt kun internt i en organisasjon mens man bruker offentlige adresser når man skal

kommunisere med eksterne parter. Problemene ble løst ved at kommunen gikk over til et annet IP-nett. I løpet av de kommende årene vil alle kommuner i Norge bli koblet til NHN. Da vil det være lettere at NHN tar i bruk offentlige adresser i stedet for å presse alle Norges kommuner til å endre IP-nett.

2.2.2 Bærbar PC

I utvelgelsesprosessen ble det vurdert en rekke ulike mobile enheter: iPac, PDA, OQO ultra-bærbar PC, bærbar PC. Valget falt på en bærbar PC fra IBM, X40. Vi valgte denne bærbare PCen fordi:

- ☺ Den er liten, lett og kompakt. Den er ikke større enn at man får den med seg i en liten sekk eller veske.
- ☺ Tastaturet på IBM X40 er nesten like stort som på et vanlig tastatur. Dette gir høy grad av gjenkjenneelse for brukerne.
- ☺ IBM X40 er, som de fleste andre bærbare datamaskinene fra IBM, robuste og solide. De er pakket inn i en kasse av aluminium, har solide hengsler og en mekanisme som låser lesehodet på harddisken hvis PCen skulle bli utsatt for støt eller slag.
- ☺ Ved å velge en mobil enhet med stor skjerm kunne alle applikasjonene som ble brukt på de stasjonære PCene på vaktrommene på institusjonene også kjøres på de bærbare PCene uten at scrolling i horisontalplanet var nødvendig.
- ☺ Med en 12.1 tommers skjerm forblir teksten fortsatt lesbar ved 1024 x 768 oppløsning.

For å gjøre løsingen mer brukervennlig kunne følgende vært gjort med IBM X40:

- ☹ Oppstarttiden kunne vært kortere. Skulle man fått ned oppstarttiden merkbart kunne Windows Mobile operativsystemet vært et alternativ.
- ☹ Batterilevetiden kunne vært bedre. Vi brukte ekstra batteripakke på denne PCen, men det var ikke nok til å holde en hel arbeidsdag på farten. Særlig ikke når PCen ble brukt utendørs eller i bil der temperaturen var lavere. For å bøte på dette, ble brukerne utstyrt med billadere til IBM X40. Dette gjorde at den bærbare PCen hadde strøm nok for en hel arbeidsdag, men medførte noe ekstra plunder og heft for brukerne.

2.2.2.1 Vedlikehold av bærbare PCer

IBM X40ene ble benyttet som tynne klienter. Dette betyr at all dataprosessering foregikk på sentral server. Dette sikret at ingen helseopplysninger ble lagret på IBM X40ene. Etter å ha kjørt en risikovurdering av den mobil tilgangen kom vi fram til at det som en ekstra sikkerhetsforanstaltning ville være lurt å fjerne de grensesnitt vi kunne der virus og uønskede programmer kunne få innpass til de bærbare PCene. Vi ønsket at brukerne bare skulle bruke de linjene ut fra de bærbare PCene som vi hadde satt opp. Derfor ble det innebygde trådløskortet, seriell-, parallell- og IR-porten deaktivert. For å unngå at brukerne selv registrerte sensitive opplysninger på de bærbare PCen ved hjelp tekstbehandlingssystemer, ble alle slike unødvendige programmer fjernet. Det ble lagt inn et sensurfilter i Internet Explorer slik at bare kommunens servere var tilgjengelig fra de bærbare PCene. Endringer

i tilkoblingsmåte og andre konfigureringer av de bærbare PCene forekom ofte. Derfor var oppsettet av de bærbare PCene i stadig endring, også etter at de var blitt plassert ut i distriktsonene. Vi brukte mye tid på å holde de bærbare PCene i en tilstand der de fungerte optimalt. Dette innebar mye mer arbeid enn vi hadde forestilt oss. Det ble ekstra tungvint å administrere de bærbare PCene fordi de geografiske avstandene til distriktsonene var så store.

Virusoppdateringer og driveroppdateringer ble overført til de bærbare PCene ved at brukerne koblet dem til Tromsø kommunes faste datanettverk (LAN) en gang i uken.

- ⊕ Det er veldig ressurskrevende å gjøre endringer på bærbare PCer lokalisert ute i distriktet. Dette problemet kunne vært begrenset ved å bruke programvarer for fjernadministrasjon av bærbare PCer (for eksempel PCanywhere og lignende) eller programvare som gjenoppretter og rydder på PCen når den blir slått av og på (for eksempel Skanix® Illusion, se kapittel 2.1.8 ”Skanix® Illusion”). Hvis det er mobiltelefoner eller Smartphones som skal fjernadministreres kan produkter fra Synchronica være grei å sjekke ut. Her kan det være mye å spare.

2.2.2.2 Innlogging på bærbare PCer

For å gjøre oppkoblingsprosessen fra de bærbare PCene til fagapplikasjon så brukervennlig som mulig, var det nødvendig å gjøre en del konfigurering på hver enkelt PC. Disse konfigureringene ble dessverre bare lagret i windows-brukerens profilen og var derfor bare gyldig for denne brukeren. Dette medførte at en slik konfigureringsjobb ville måtte gjøres for hver bruker som skulle ha tilgang til bærbar PC. For hver ny ansatt eller ny bruker ville det kreve at en tekniker tok en kjøretur ut i distriktsonen for å gjøre disse endringene. Dette ble simpelthen for mye vedlikehold. Løsningen ble derfor å sette opp en felles windows-bruker for hver avdeling. Alle brukerne på en avdeling brukte altså det samme brukernavnet og det samme passordet for å logge inn på de bærbare PCene som tilhørte deres avdeling. Denne første barrieren gjør maskinen mindre attraktiv å stjele og skulle det mot formodning være lagt inn noe sensitivt materiale på PCen, vil dette være beskyttet. For å få logge videre inn mot kommunen var det nødvendig med individuell pålogging.

2.2.3 Datalinjer til distriktssonene i Tromsø kommune

Da prosjektet startet hadde samtlige distriktssoner i kommunen, som skulle få utplassert bærbare PCer, dedikerte datalinjer som knyttet dem til kommunens datanettverk. Kapasiteten på disse linjene var på 128 Kbit/s. De var dimensjonert for en, maks to, PCer. På flere distriktssoner var det satt opp langt flere PCer og linjene var derfor i utgangspunktet underdimensjonert. Brukernes tilgang til fagapplikasjoner var lite tilfredsstillende og kunne til tider være totalt fraværende. Dette førte til fortvilelse og maktesløshet blant de ansatte som var innstilt på å benytte fagapplikasjoner. Bruken av disse systemene ble sterkt redusert. For å få opp bruken av IKT og elektronisk samhandling i distriktssonene ble det jobbet iherdig fra NSTs side for å få kommunen til å gå til innkjøp av større båndbredde på disse datalinjene. Dette var både et kostnadsspørsmål for kommunen og et spørsmål om oppgradering av sentraler hos Telenor, men etter hvert fikk en av distriktssonene oppgradert sine linjer. Dette førte til økt bruk av fagsystemene både fra stasjonære PCer og bærbare PCer.

- ⊕ Det er veldig viktig å sette seg inn i hvordan tilstanden/belastning er i det datanettverket man skal plassere ut nye tjenester/PCer i, og hvilke grep som eventuelt må gjøres for å gi rom for de nye tjenestene/PCene.

2.2.4 Digitalt kamera og diodelys

Digitalkameraet som helsepersonell i dette prosjektet benyttet var Nikon Coolpix 4500. Sammen med kameraet ble det benyttet en diodelyskilde, Nikon Cool Light, som kan skrues fast på objektivet på kameraet og gir et konstant og fargenøytralt kortdistanselys som sikrer jevne lysforhold ved nærfotografering. NST har gode erfaring med kameraet fra foregående prosjekter.

Fordeler med Nikon Coolpix 4500:

- ☺ Robust
- ☺ Har kort nærgrense. Dette betyr at man kan ta nærbilder på inntil to cm. Dette kan være en fordel hvis man skal ta hud- eller sårbilder.
- ☺ Skjerm og objektiv kan vris i forskjellige retninger. Dette gjør at man kan se motivet på skjermen selv under fotografering i vanskelige vinkler.
- ☺ Ikke for lite. Ligger godt i hånda. Lettere å holde stødig og få klare bilder ved fotografering i dårlig lys.
- ☺ Kameraet kan brukes med annet medisinsk utstyr som skrues på linsen, blant annet dermatoskop.
- ☺ Kameraet har lang batterilevetid.

Ulemper med Nikon Coolpix 4500:

- ☹ Hver gang kameraet skulle brukes for å ta sårbilder var det nødvendig å gjøre mange innstillinger. Disse innstillingene ble ikke lagret når kameraet ble slått av og på igjen. Dette førte til en høyere brukerterskel.
- ☹ Prisen på kameraet er høy.
- ☹ Kameraet har et spesialbatteri som ikke kan kjøpes i vanlige butikker, og tiden fra man får indikasjon på lav batterikapasitet til kameraet dør er meget kort.

2.2.5 Mobiloperatører og mobilkort

2.2.5.1 Dekning

Vi har benyttet mobilnettene til både Telenor og Netcom i dette prosjektet. Dekningsgraden til både Telenor og Netcom endret seg mye i prosjektperioden. Derfor ble dekningskartene, opplysninger fra teleoperatørene om hvordan dekningsområdet kom til å bli sendt ut, opplysninger om dekningsgraden fra de lokale brukerne og kjøreturer der dekningsgraden ble testet lagt til grunn for valg av hvilke operatører som ble valgt i hvilke områder.

Resultatet ble at EDGE/GPRS-nettverk fra både Netcom og Telenor ble brukt, men i forskjellige distriktssoner. Etter å ha kjørt og testet både Telenors og Netcoms UMTS-dekning viste det seg at Netcom hadde bedre og mer stabil dekning i bysonene i Tromsø.

2.2.5.2 Mobilkort

Under følger noen erfaringer gjort med mobilkort.

Mobilkort brukt i distriktssoner

- Sierra Wireless AirCard® 775 EDGE PCMCIA-innstikkskort (med SIM-kort fra Netcom)
- Sony Ericsson GC85 EDGE/GPRS PCMCIA-innstikkskort (med SIM-kort fra Telenor)

Mobilkort brukt i bysonen

- HUAWEI E620 Mobile Connect UMTS/EDGE/GPRS PCMCIA-innstikkskort (med SIM-kort fra Netcom)

Mobilkort som ble testet men ikke brukt

- Option GlobeTrotter Fusion med Telenors Mobilt Kontor-programvare

2.2.5.2.1 Sierra Wireless AirCard®775 EDGE (med SIM-kort fra Netcom)

Dette er et PCMCIA-innstikkskort som ikke er låst på operatør. Vi valgte å bruke SIM-kort fra Netcom fordi de hadde best dekning ved Kvaløya hjemmetjeneste avdeling Brensholmen. Sierra Wireless AirCard®775 EDGE kortet var det EDGE kortet av dem vi testet som hadde den beste opplastningskapasiteten. Det hadde dynamisk allokering av time-slottet til nedlastning og opplastning. Det betyr at hvis det var mest trafikk som gikk ut fra kortet, for eksempel sending av sårbilder til spesialist, så brukte kortet fire av seks time-slottet på opplastning (sending). Hvis det derimot skulle laste ned en større datamengde, for eksempel vise et sårbilde på skjermen, brukte det fire av seks time-slottet til nedlastning.

- ☺ God opplastningskapasitet.
- ☺ Dynamisk allokering av time-slottet.
- ☺ Brukte lite strøm.
- ☺ Kjapp oppkobling.

2.2.5.2.2 Sony Ericsson GC85 EDGE/GPRS PCMCIA-innstikkskort (Med SIM-kort fra Telenor)

Fordi SES@m Tromsø-prosjektet er et fyrtårnsprosjekt var det ønskelig å prøve ut forskjellige kort og forskjellige mobiloperatører. Dette kortet som er låst til å bruk i Telenor sitt mobilnett ble derfor brukt i distriktet der Telenor hadde best dekning. Dette var ved Om-sorgstjenesten Fastlandet avdeling Lakselvbukt. Kortet fungerte meget bra og hadde et lettfattelig brukergrensesnitt med en god del konfigureringsmuligheter. Det var blant annet mulig å lage snarvei til andre applikasjoner fra kortets tilkoblingsapplikasjon.

- ☺ Fungerte bra.
- ☺ Lettfattelig brukergrensesnitt på medfølgende programvare.
- ☺ Kjapp oppkobling.

2.2.5.2.3 Option GlobeTrotter Fusion med Telenors Mobilt Kontor-programvare

Dette var opprinnelig det kortet vi tenkte å bruke i bysonen, men etter å ha hatt en del problemer med det valgte vi å se etter alternativer. Det er vanskelig å fastslå om problemene vi opplevde på testturen skyldes dårlig dekning eller feil/svakheter i kortet. Vi opplevde 8 brudd på sambandet fra vestsiden av Tromsøya til Tromsdalen. Dette er ikke forenelig med autentiseringsmekanismen som brukes for mobil tilgang til datanettet i kommunen. Dette fordi det hver gang det oppstår brudd på sambandet, må påregnes 7-8 minutters påloggingstid for å få logget inn så man får tilgang til pasientopplysninger igjen.

Denne løsningen som benytter UMTS/GPRS er for øyeblikket for ustabil med tanke på oppetid når man er i bevegelse for at den kan brukes i SES@m Tromsø-prosjektet. Se Vedlegg 1 "Test av Telenor Mobilt Kontor - Oppetid - Brudd - Tilkoblingstid - Dekning" for flere detaljer.

- ☹ Opplevde mange brudd.
- ☹ Lang oppkoblingstid.

2.2.5.2.4 HUAWEI E620 Mobile Connect UMTS/EDGE/GPRS PCMCIA-innstikkskort (med SIM-kort fra Netcom)

Dette kortet var låst på operatør. Man måtte bruke SIM-kort fra Netcom. Dette var det kortet som var mest stabilt av de UMTS-kortene vi testet. Kortet ble derfor brukt i den eneste bysonen som vi ga mobil tilgang, Natttjenesten. Tiden kortet brukte på å koble opp var kortere enn Option GlobeTrotter Fusion-kortet med Telenors Mobilt Kontor-programvare. Kortet vekslet mellom UMTS og EDGE uten at dette var merkbart for brukeren.

- ☺ Fungerte bra.
- ☺ Lettfattelig brukergrensesnitt på medfølgende programvare.
- ☺ Profesjonelt brukergrensesnitt.

2.2.6 Autentiseringsenheter til mobil tilgang

Tilgang til sensitive helseopplysninger initiert fra utsiden og inn i sikker sone var noe som krevde sterk autentisering av brukerne. Det ble benyttet to-faktor-autentisering i form av to forskjellige systemer. Vi brukte to systemer for å autentisere brukerne, eToken fra Aladdin og SecureID fra RSA.

2.2.6.1 eToken – lagringsenhet for personlig sertifikat

Den løsningen ble brukt på tre avdelinger i kommunen. eToken fra Aladdin ble utstyrt med et personlig sertifikat utstedet fra kommunen til de brukerne som skulle ha mobil tilgang. Dette fungerte bra. For å få tilgang måtte brukerne sette sitt personlig eToken inn i USB-porten på den bærbare PCen og oppgi brukernavn og passord.

2.2.6.2 RSA SecureID

RSA SecureID brukes for å autentisere brukerne. Det ble benyttet RSA tokens sammen med Netcom sitt UMTS kort HUAWEI på en av avdelingene som hadde mobil tilgang. RSA SecureID autentiserte brukere basert på noe de visste (passord) og noe de hadde (kode på RSA Kalkulator).

RSA SecureID er en kodegenerator som genererer en 6 sifret kode som vises i et lite display på enheten. Denne koden måtte brukeren oppgi ved innlogging i tillegg til personlig brukernavn og passord. RSA SecureID genererte ny kode ofte og kommunens autentiserings-server genererte en tilsvarende kode eksakt samtidig. Ved innlogging ble disse kodene sjekket mot hverandre for å identifisere brukeren. RSA SecureID fungerte uten problemer.

2.3 Forsinkelser og låste skjermbilder

Brukerne opplevde fra tid til annen forsinkelser og låste skjermbilder når de arbeidet inn mot kommunens sentrale Citrix Metaframe park.

2.3.1 Fra stasjonær PC i LAN

Tiden det tok fra stasjonær PC i kommunens LAN startet til brukeren var autentisert og klar til å arbeide med sensitiv informasjon varierte.

Faktorer som påvirket innloggingstid, oppdatering av skjermbildet og reaksjonstid på tastatur- og musesignaler:

- Linjekapasitet på datalinje fra kommunens sentrale servere til institusjonen
- Linjekapasitet inne på institusjonen
- Spesifikasjoner på den stasjonære PCen
- Spesifikasjoner på EDI-serveren sentralt hos kommunen
- Belasting. Hvor mange brukere som var logget på fra den samme institusjonen

⊕ Brukerne klarte fra tid til annen ikke å logg på grunn av overbelastede datalinjer

→ Mulig løsning: Oppgrader til datalinjer med mer båndbredde, både internt i institusjonene og mellom institusjonene og kommunens sentrale serverrom.

→ Bruk tid på å kartlegge alle tekniske begrensninger og flaskehalsen som kan få konsekvenser ved innføring av nye løsninger.

2.3.2 Fra mobil PC

Løsningen som ble implementert hadde konsekvenser for hvor lang tid det tok fra bærbar PC ble slått på til brukeren var logget på og klar til å arbeide. Kommunens infrastruktur og sikkerhetskrav fra ”Lov om helseregistre og behandling av helseopplysninger” og ”Lov om behandling av personopplysninger” la premisser for hvilke valg som ble foretatt i prosjektet når det gjaldt autentiseringsløsninger. Dette medførte at oppkoblingstiden fra brukeren slo på maskinen til hun/han hadde tilgang til fagapplikasjoner med sensitive opplysninger var ca 7-8 minutter. Skulle kontakten mellom bærbar PC og kommunens servere bli brutt som følge av for eksempel dårlig mobildekning, måtte innloggingsprosessen startes fra begynnelsen igjen.

Faktorer som påvirket innloggingstid, oppdatering av skjermbildet og reaksjonstid på tastatur- og musesignaler:

- Mobildekningen på stedet
- Spesifikasjoner på den bærbare PCen
- Spesifikasjoner på EDI-serveren sentralt hos kommunen
- Belastingen på basestasjonen. Hvor mange aktive brukere som befant seg i samme området

⊕ Ved brudd på oppkoblingen må brukerne logge inn på nytt.

→ Mulig løsning: Gå over til Citrix Metaframe 4.0 som inneholder funksjonalitet for å håndtere mobile tilkoblinger.

⊕ 4 pålogginger er for mye og tar for lang tid.

→ Mulig løsning: Benytt en singel sign-on løsning for å automatisere 2 av de 4 påloggingene, og dermed komme ned i 2 pålogginger. RSA som kommunen benytter i dag kan muligens brukes.

⊕ Tid fra bærbar PC slås på til sensitive opplysninger er tilgjengelig er for lang.

→ Mulig løsning: Benytt bærbare PCer med lettvektoperativsystem, for eksempel Windows mobile.

3. Organisatoriske erfaringer i prosjektet

3.1 Opplæring og brukerstøtte i fokus

Tjenestene og løsningene i SES@m Tromsø-prosjektet (pilot) ble plassert ut i Tromsø kommunes ordinære datanettverk og benyttet av ansatte i kommunens pleie- og omsorgstjeneste.

Ved implementering av IT-løsninger er det viktig å ta hensyn til ulikt kompetansenivå blant brukere, og gi disse nødvendig opplæring, oppfølging og support. Det er derfor viktig at prosjektet har et apparat som kan sørge for lett tilgang til støtte og support for sluttbrukerne. Vår erfaring er at dette er kritisk.

Noen konkrete erfaringer fra SES@m Tromsø-prosjektet er:

- Ikke undervurder behovet for støtte, support og oppfølging av brukere. Det er viktig å sette mye ressurser til dette.
- Det å belage seg ensidig på kommunens interne brukerstøtteapparat har ikke fungert tilfredsstillende i vårt pilotprosjekt. Brukerstøtteapparatet har kompetanse på allerede etablerte løsninger og er ressursmessig dedikert til den ordinære kommunale hverdagen. I prosjektsammenheng er endringshastigheten stor og behovet for ressurser kan oppstå spontant. Det bør derfor settes av egne ressurser i prosjektet som tar seg spesielt av konkrete oppgaver relatert til pilotprosjektet.

→ Det er viktig å sette av nok ressurser til å drive oppfølging av brukerne.

→ Endring av arbeidsmåter og rutiner krever utrolig mye ressurser, økonomisk, tidsmessig og menneskelig.

3.2 Drift av prosjektet

SES@m Tromsø-prosjektet var initiert og ledet av Nasjonalt senter for telemedisin og løsningene ble innført i Tromsø kommunes nettverk. En erfaring etter prosjektet er at det er viktig at nye prosjekter blir godt forankret på alle nivå i kommunen. Med en slik organisering er det også utrolig viktig å koordinere med interne it-ressurser med tanke på "timing" av milepæler og lignende.

SES@m Tromsø-prosjektet ble utviklet av NST og ikke av kommunen. NST fikk kommunen med på laget på overordnet nivå mens detaljplanleggingen ble foretatt av NST. Etter hvert som prosjektet skred fram ble det gradvis forankret på ulike enheter i PLO-tjenesten. Mye av forankring og eierskap er vokst fram gjennom prosessen med gjennomføringen av prosjektet. Ideelt sett kan man tenke seg at prosjektinitiativet kom fra kommunen og at kommunen ledet prosjektet.

Hvis ledelsen på sykehjem og i hjemmetjeneste hadde vært mer informert om hva det ville kreve av deres ansatte for å ta i bruk tjenestene i prosjektet, ville dette kanskje ført til at hverdagen ble bedre tilrettelagt i forhold til bruk av tjenestene. Dette ville kanskje igjen føre til at tjenestene ble mer brukt. Hadde det vært etablert sterkere eierskap til

prosjektet hos ledelsen på sykehjem og i hjemmetjeneste ville nok dette ført til økt prioritet på å ruste opp gamle datamaskiner og datanettverk på institusjonene. Det er viktig å forankre et slikt pilotprosjekt helt ned til brukernivå og at brukerne får satt av tid til å delta i selve prosjektet.

Prosjektet har hatt mange ulike aktører i både privat og offentlig sektor. Det har vært organisatoriske utfordringer for å opprettholde den ønskede progresjonen. Som ledere av prosjektet har vi erfart at til tross for gode prosjektplaner, så handler det mye om å takle det uforutsette.

Prosjektleder-rollen innebærer å være pådrivere og styre prosjektet etter oppsatte milepæler og tidsfrister. Pådriverrollen kan være vanskelig, og tett oppfølging av aktørene kan være nødvendig. Dette både for å unngå forsinkelser og for å holde progresjonen oppe. Opplever man mindre framdrift hos enkelte enheter enn ønsket, så er det hensiktsmessig å kjøre regelmessige møter.

Når en planlegger prosjektet er det viktig å gjøre en grundig kartlegging av infrastruktur og maskinvare. Dette for å kunne si noe om hvilke investeringer prosjektet må regne med for å få den tekniske plattformen opp på et tilstrekkelig nivå

Det er ingen enkel jobb å kartlegge nødvendig maskinvare og programvare i prosjekter og en bransje der den teknologiske endringshastigheten er stor. Teknologien som blir benyttet er kanskje helt nyutviklet eller blir utviklet underveis i prosjektet. Få eller ingen kan si noe sikkert om hvordan den endelige løsningen blir i detalj når prosjektet planlegges. Veien blir til mens man går. Dette må man ta høyde for.

Det er oftest satt av for lite ressurser til oppfølging av brukerne når man skal implementere IT-løsninger. Dette tok vi etter hvert til følge, og prosjektet ansatte en person fra pleie- og omsorgstjenesten i kommunen til å ta seg spesielt av opplæring og oppfølging.

- Ansatte vil ha kontinuerlig behov for oppfølging etter at de har tatt i bruk nye tjenester. Mange trenger også repetisjon av opplæring.
- Når man implementerer en ny løsning vil det alltid måtte gjøres endringer/utvidelser i etterkant.
- Det er viktig å avklare hvem som er ansvarlig for disse aktivitetene etter at prosjektet er over.
- Det er viktig å være klar over utfordringene forbundet å jobbe i en driftsorganisasjon samtidig som man er deltaker i et prosjekt som krever kontinuerlig oppfølging.

4. Tromsø kommunes erfaringer fra prosjektet

SES@m Tromsø er et nasjonalt fyrårnsprosjekt og samtidig et pilotprosjekt. Å etablere pilotprosjekter i en driftsorganisasjon kan være en stor utfordring. Følgende spenningssområder/motsetninger kan oppstå:

- Bruk av frontteknologi i miljøer med lav datakompetanse blant brukerne
- Teknologi med høy endringstakt i et etablert driftsmiljø
- Sikkerhetsspørsmål som bryter med prinsippene i Datatilsynets veiledning for kommuner og fylker

4.1. Bruk av frontteknologi i miljøer med lav datakompetanse blant brukerne

Pilotprosjektet SES@m Tromsø forsøkte å etablere frontteknologi i et miljø der IT-kompetanse blant brukerne er lav. Utfordringene er flere. Frontteknologi er sjelden brukervennlig. Har gjerne kompliserte konfigureringer og brukergrensesnitt. Slik teknologi innført i miljøer med lav IT-kompetanse blant brukerne, gir gjerne store utfordringer.

Forslag til løsninger

1. Senke ambisjonsnivået med tank på teknologi
2. Velge enkle og mer brukervennlige teknologi
3. Prosjektet må gi brukerne tett "på fanget" oppfølging m.h.p bruk av system
4. Gi opplæring til brukere etter hvert som teknologi endrer seg i prosjektet
5. Ha så lite utvalg av brukere som mulig, for å minke brukerstøttebehovet
6. Velge ut superbrukere som har IT-kompetanse (se dokumentet "Opplæring Oppfølging - Erfaringer fra opplærings- og oppfølgingsarbeidet ved implementeringen av de telemedisinske samhandlingstjenestene i SES@m Tromsø." for mer info om superbrukere).

4.2 Etablere pilotprosjekter i eksisterende driftsmiljø

Det er ei utfordring å gjennomføre pilotprosjekter i eksisterende driftsmiljø. Pilotprosjekter har gjerne en del prøving og feiling av ny teknologi som ikke har samme stabilitet som etablert teknologi. Ny teknologi har gjerne høy brukerterskel. Den kommunale IT driftsorganisasjonen er ikke dimensjonert eller tilpasset utfordringene som et pilotprosjekt medfører. Den vanlige brukerstøttefunksjonen vil ikke ha mulighet til å hjelpe brukere rundt et pilotprosjekt. Til det er endringstakten for stor til at brukerstøttefunksjonen klarer å fange det opp.

Mulige tiltak:

1. Sett av egne ressurser i prosjektet som tar seg av brukerstøtte. Disse ressursene må være "IT-kyndige folk", som hvis det er nødvendig tar kontakt med det normale brukerstøtteapparatet
2. Sett av personer i det normale brukerstøtteapparatet som prosjektets IT-kyndige kan ha direkte kontakt med

3. Teknologisk sett så bør pilotprosjektet skilles fra driftsmiljø, slik at ikke problemer i pilotprosjektet berører stabilitet og ytelse i produksjonsmiljø
4. Før igangsetting av pilotprosjektet, så bør den kommunale IT driftsorganisasjonen tas med på et tidlig stadium. Slik vil en finne ut om eksisterende infrastruktur lar seg benytte i piloteringen. Viser dette seg å være tilfelle, vil en bl.a. slippe å bruke mye tid på å utrede løsninger som senere kan bli forkastet

4.3 Andre organisatoriske utfordringer

- Få med alle involverte parter i den organisasjonen som blir berørt av prosjektet. Prøv å oppnå konsensus blant de involverte partene m.h.p mål, gjennomføring, tidsforbruk, milepæler, osv.
- Sørg for å “time” innføringen slik at den ikke kolliderer med andre prosjekter som påvirker den daglige drift
- Prosjektet bør og må være forankret fra topp og helt ned til sluttbruker. Ved at deltakere i prosjektet føler at noe ”tvunget” inn, vil man komme skeivt ut allerede fra starten av

5. Oppsummering av erfaringer

I dette kapitlet presenteres en oppsummering av alle erfaringene gjort i den tekniske implementeringen i SES@m Tromsø-prosjektet.

5.1 Tekniske erfaringer

- Bruk tid på å kartlegge de tekniske omgivelsene og deres begrensninger og flaskehalsar som kan få konsekvenser ved innføring av nye løsningsar
- Singel sign-on løsningsar kan vurderes for å redusere antall innloggingar
- Bruk tilstrekkelig tid til å teste ut produkter før innkjøp av dem blir vurdert. Snakk med andre som har benyttet produktene over tid
- Det er mye arbeid å publisere og vedlikeholde symmetriske nøkkel når antall parter som skal kommunisere øker. Benytt PKI, digitale sertifikater og HER-registeret
- Det krever mye arbeid å vedlikeholde VPN-løsningsar der man må ha en programvare installert på klienten. Benytt klientløs VPN
- IPsec er lite brukervennlig når flere brukere skal bruke den samme PCen
- Sensurmekanismen i Internet Explorer fungerer bra for å kun tillate brukerne tilgang til bestemte sider på Internett. Denne tilgangskontrollen er ikke aktiv ved bruk av andre Internett browser programmer
- Bruke tilstrekkelig tid til å undersøke hvor ferdigutviklet og utprøvde produkter er før de velges ut til å være bærebjelker i den tekniske løsningen. Snakk med andre som har benyttet produktene over tid
- Det er veldig ressurskrevende å holde bærbare PCer lokalisert ute i distriktet oppdatert. Bruk systemer som gjør fjernadministrasjon av bærbare PCer enklere.
- Senk ambisjonsnivået m.h.p teknologi. Velg enkle og derfor mer brukervennlig teknologi
- Teknologisk sett så bør pilotprosjektet skilles fra driftsmiljø, slik at ikke problemer i pilotprosjektet berører stabilitet og ytelse i produksjonsmiljø

5.2 Organisatoriske erfaringer

- Etablere eierskap hos IT-avdeling, ansatte og ledelsen på avdelingene i kommunen. Ta parter med på råd når prosjektet planlegges

- Det er viktig å være klar over utfordringene forbundet med å jobbe i en driftsorganisasjon samtidig som man er deltaker i et prosjekt som krever kontinuerlig oppfølging
- Før igangsetting av pilotprosjektet, så bør den kommunale IT driftsorganisasjonen tas med på et tidlig stadium. Slik vil en finne ut om eksisterende infrastruktur lar seg benytte i piloteringen. Viser dette seg å være tilfelle, vil en bl.a. slippe å bruke mye tid på å utrede løsninger som senere kan bli forkastet
- Få med alle involverte parter i den organisasjonen som blir berørt av prosjektet. Prøv å oppnå konsensus blant de involverte partene m.h.p mål, gjennomføring, tidsforbruk, milepæler, osv.
- Sørg for å “time” innføringen slik at den ikke kolliderer med andre prosjekter som påvirker den daglige drift
- Prosjektet bør og må være forankret fra topp og helt ned til sluttbruker. Ved at deltakere i prosjektet føler at noe “tvunget” inn, vil man komme skeivt ut allerede fra starten av.

5.3 Erfaringer med support og oppfølging

- Ansatte vil ha kontinuerlig behov for oppfølging etter at de har tatt i bruk nye tjenester. Mange trenger også repetisjon av opplæring. Dette krever mye ressurser
- Prosjektet må gi brukerne tett “på fanget” oppfølging m.h.p bruk av system
- Gi opplæring til brukere etter hvert som teknologi endrer seg i prosjektet
- Ha så lite utvalg av brukere som mulig, for å minke brukerstøttebehovet
- Velge ut superbrukere som har IT-kompetanse (se dokumentet “Opplæring Oppfølging - Erfaringer fra opplærings- og oppfølgingsarbeidet ved implementeringen av de telemedisinske samhandlingstjenestene i SES@m Tromsø.” for mer info om superbrukere).

5.4 Erfaringer gjort med tanke på ressursplanlegging

- Når man implementerer en ny løsning vil det alltid måtte gjøres endringer/utvidelser i etterkant. Det er viktig å avklare hvem som er ansvarlig for disse aktivitetene etter at prosjektet er over
- Sett av egne ressurser i prosjektet som tar seg av brukerstøtte. Disse ressursene må være “IT-kyndige folk”, som hvis det er nødvendig tar kontakt med det normale brukerstøtteapparatet
- Sett av personer i det normale brukerstøtteapparatet som prosjektets IT-kyndige kan ha direkte kontakt med

6. Forkortelser

EDGE	Står for Enhanced Data GSM Environment og er et mobilnett basert på en oppgradering av GSM-mobilnettet. Gjør at overføringshastigheten av data øker sammenlignet med det som oppnås på tradisjonell GSM. Har en maksimal teoretisk overføringshastighet på 200 Kbps
EDI-meldinger	Står for Electronic Data Interchange , eller på norsk Elektronisk Data Utsveksling . Innebærer utveksling av informasjon mellom forskjellige programmer og systemer
GPRS	Står for General Packet Radio Service . Bruker mobilnettet og gir dataoverføring med maksimal teoretisk hastigheter på inntil 114 Kbps
HER-registeret	Helse-Enhets-Registeret er en adressekatalog som viser adresser til de ulike enhetene innen helsevesenet som man kan kommunisere med
LAN	Står for Local Area Network . Med LAN menes firmaets eller organisasjonens private kablede datanettverk
PCMCIA	Står for Personal Computer Memory Card International Association . Dette er en organisasjon som lager standarder for ekstrautstyr til bærbare PCer. PCMCIA-ekstrautstyr er en type maskinvare som kan kobles til en bærbar PC hvis den har en PCMCIA-port
SSL	Står for Secure Sockets Layer . Dette er en protokoll for å overføre sensitiv informasjon over Internett. SSL bruker et krypteringssystem som bruker en privat nøkkel og en offentlig nøkkel.
UMTS	Står for Universal Mobile Telecommunications System . Mobilnett som gjør at data kan overføres 8-10 ganger raskere enn i GSM-nettet, maksimal teoretisk overføringshastighet på 384 Kbps.

Referanser

1. Daniel Nygård og Harald Øverli Eriksen m. fl. : *"Tekniske dokumentasjon"*
2. Ann Theres Lotherington m. fl.: *"Telemedisin i pleie- og omsorgssektoren: Forventninger og utfordringer"*
3. Ann Theres Lotherington m. fl.: *"Telemedisin i pleie- og omsorgstjenesten: Om å takle det uforutsette"*
4. Ann Theres Lotherington m. fl.: *"Telemedisin i pleie- og omsorgstjenesten: Sluttrapport fra prosjektet SES@m Tromsø"*
5. Eva Skipenes, NST, og Arnstein Vestad, KITH: *"Risikovurdering av mobil tilgang til fagapplikasjoner i SES@m-prosjektet"*
6. Eva Skipenes, NST, og Arnstein Vestad, KITH: *"Risikovurdering av løsningene i SES@m-prosjektet fra et brukerperspektiv"*
7. Eva Skipenes, NST, og Arnstein Vestad, KITH: *"Risikovurdering av tekniske løsninger i SES@m-prosjektet"*
8. Eva Skipenes, NST, og Arnstein Vestad, KITH: *"Oppsummering av sikkerhetskritiske aspekter i SES@m-prosjektet"*
9. Line Nordgård, NST: *"Opplæring Oppfølging - Erfaringer fra opplærings- og oppfølgingsarbeidet ved implementeringen av de telemedisinske samhandlings-tjenestene i SES@m Tromsø."*

Disse dokumentene er publisert på SES@m Tromsø-prosjektet web side:

<http://www.telemed.no/index.php?cat=31253>

8. Vedlegg 1 - Test av *Option GlobeTrotter Fusion* med Telenors Mobilt Kontor

Denne testen ble utført 10.01.06 i Tromsø by. Formålet var å finne ut om dette kortet kunne brukes sammen med bærbare Pcer som skulle plasseres ut hos Nattjenesten i Tromsø kommune. Det som ble testet var oppetid, brudd, tilkoblingstid og dekning. I denne testen ble det benyttet tre stk IMB X40 bærbare Pcer med Option GlobeTrotter Fusion og med Telenors Mobilt Kontor applikasjon installert.

Maskinnr.	Kortnr.	Tid	Posisjonsnummer	Tilkoblingstid i sekunder	Oppetid før brudd i min.	Dekning (ant streker)	Feilmeldingsnr.	Bil i fart
G	I	13:24	1	-	-	-	1	Ja
G	I	13:29	2	10	1	3	-	Ja
G	I	13:31	2	10	1	2	-	Nei
H	II	13:32 - 13:48	2	10	16	3	-	Nei
G	I	13:33 - 13:35	2	15	2 forsøk a 1	3	-	Nei
U	III	13:34 - 13:53	2	15	19	3	-	Nei
H	II	13:50	2	-	-	3	1	Nei
H	II	13:51	2	-	-	3	1	Nei
H	II	13:51	2	-	-	3	1	Nei
H	II	13:53	2	-	-	3	1	Nei
U	III	13:55	2	10	20	3	-	Nei
G	I	13:47	2 og 3	10	49	3 og 4	-	Nei -Ja - Nei ¹
U	III	14:11	3	-	-	4	2	
U	III	14:12	3	-	-	4	3	
U	III	14:39	3	10		4	-	
U	III	14:39	3	10			-	
G	I	14:38	3	10			-	
U	III	15:09	4	10	31		-	
G	I	15:04	4					
G	I	15:10	4		18 brøt selv	4 - 5		
G	I	15:35	5 - 7		29 brøt selv	4		
U	III	15:35	5 - 6	10	19	4		
U	III	15:54	6 - 7	10	10 brøt selv	4		
G	I	16:05	7 -	10		3 -		Se ² under
U	III	16:05	7 -	10		3 -		Se ² under

¹ - Kjørte fra posisjon 2 til posisjon 3. Maskin G var koblet på nett da vi startet å kjøre fra posisjon 2 og lenge etter at vi kom fram til posisjon 3. Valgte å koble fra maskin G i posisjon 3 etter å ha vært på nett i 49 minutter fordi vi ønsket å teste om maskinen klarte å koble på nett igjen i den nye posisjon 3. Den andre maskinen klarte nemlig ikke dette. Maskin G klarte å koble på i posisjon 3 uten problemer, også etter å ha restartet Mobil kontor-applikasjonen.

Maskin U som ikke var på nett da vi kjørte fra posisjon 2 til posisjon 3 klarte ikke å komme på nett i posisjon 3 før vi restartet maskinen.

Vi trekker den konklusjonen at et Option GlobeTrotter Fusion med Telenors Mobilt Kontor som har tilgang til nettverk når det beveger seg inn i en sone der det må konkurrere med flere UMTS-brukere om båndbredden eller en sone der det er dårligere dekning, lettere vil kunne koble seg av og på i den nye sonen til forskjell fra et kort som ikke hadde tilgang til nettverk under transporten til den nye sonen.

² - Mistet kontakten på maskin G og U i posisjon 8, 9, 10, 11, 12 og 13. Se kart.

Feilmeldinger	
Nr.	Feilmeldingstekst fra Mobil Kontor-applikasjonen
1	Tilkoblingsforsøk feilet. Ønsker du å forsøke igjen.
2	Mobilt kontor finner ingen forhåndsdefinerte Trådløse nett eller Mobilnett. For å finne tilgjengelige nett, trykk SØK under Trådløse Nett eller trykk SØK under Mobilnett. Sjekk også at SIM-kort er satt inn i ditt datakort og at datakortet er satt ordentlig inn i datamaskinen.
3	Det oppstod en feil i Mobilt Kontor. Sjekk at SIM-kort er satt inn i ditt datakort og at datakortet er satt ordentlig inn i datamaskinen.

Kjørerute

Vi startet kjøreturen i posisjon 1 og avsluttet i posisjon 13.



Mange brudd på sambandet

Før vi kjørte fra posisjon 3 koblet vi opp maskin U og G. På veien mellom posisjon 3 og posisjon 4 gikk maskin U og G av nett hele 8 ganger.

U og G gikk av nett:

Sted	Tid
Rundkjøringen på Langnes	14:54
Langnesbakken	14:57
Ved Prestvannet	15:02
Ved værvarslinga	15:03
Ved Kongsbakken videregående skole	15:04
Ved Fokuskvartalet i Grønnegata	15:06
Midt på Tromsøbrua	15:09

Konklusjon

Vi opplevde 8 brudd på sambandet fra vestsiden av Tromsøya til Tromsdalen. Dette er ikke forenelig med autentiseringsmekanismen som brukes for mobil tilgang til datanettet i kommunen. Dette fordi det hver gang det oppstår brudd på sambandet, må påregnes 7-8 minutters påloggingstid for å få logget inn i så man får tilgang til pasientopplysninger igjen.

Denne løsningen som benytter UMTS/GPRS er for øyeblikket for ustabil med tanke på oppetid når man er i bevegelse for at den kan brukes i SES@m Tromsø-prosjektet.

9. Vedlegg 2 – Test av nedlastningshastighet på EDGE- og UMTS-kort i Tromsø by

Dette dokumentet beskriver en test av nedlastningshastighet. Testen var en del av arbeidet som ble gjort for å finne fram til teknisk løsning i SES@m Tromsø-prosjektet. Målgruppen er personell som er involvert i beslutningstaking, design av eller implementering av IKT-systemer i en kommune. For mer informasjon om prosjektet, tjenester og samarbeidsparter i SES@m Tromsø kapittel 7 "Referanser".

Testen ble gjort i Tromsø by 17. januar kl 12:30 og utover ettermiddagen.

Formålet var å finne hvilket EDGE- og/eller UMTS-kort som skulle bli brukt sammen med bærbare Pcer som skulle brukes av Natttjenesten i Tromsø kommune. I denne testen konsentrerte vi oss om å teste nedlastningshastighet. Det ble benyttet fire stk IMB X40 bærbare Pcer med hvert sitt EDGE- og/eller UMTS-kort kort installert.

Kortene som ble testet var:

Kort 1- Sierra Wireless AirCard® 775 EDGE PCMCIA-innstikkskort med Netcom SIM-kort

Kort 2 - Sony Ericsson GC85 EDGE/GPRS PCMCIA-innstikkskort med Telenor SIM-kort

Kort 3 - GlobeTrotter 3G QUAD med Netcom SIM-kort

Kort 4 - HUAWEI E620 Mobile Connect UMTS/EDGE/GPRS PCMCIA-innstikkskort med Netcom SIM-kort

Kjørerute

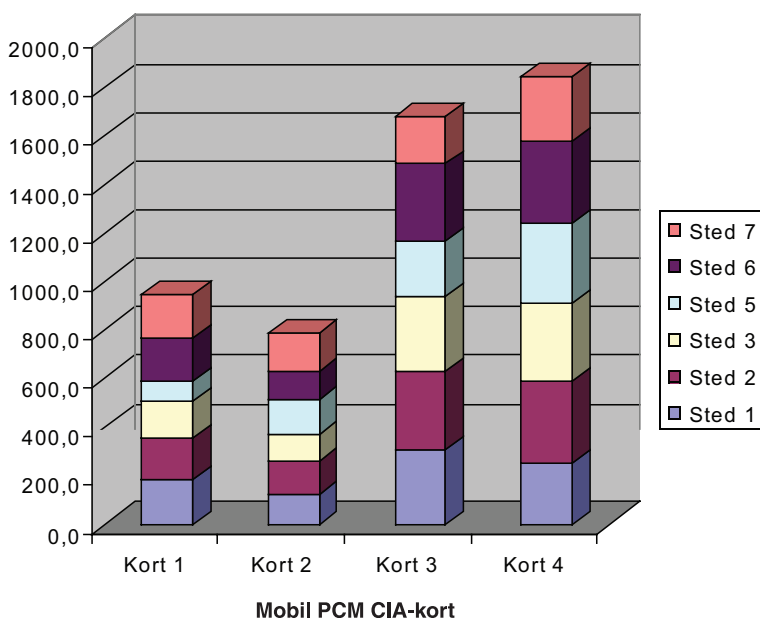
Vi startet kjøreturen i posisjon 1 og avsluttet i posisjon 7.



Testresultat

Gjennomsnittlig nedlastingshastighet:				
Sted\Kort	Kort 1	Kort 2	Kort 3	Kort 4
Sted 1	184,6	123,9	308,3	252,7
Sted 2	167,8	132,3	321,0	333,7
Sted 3	154,0	115,5	308,7	327,0
Sted 5	80,7	141,7	227,7	328,7
Sted 6	178,0	118,0	318,0	337,5
Sted 7	179,8	156,3	198,3	266,3
Snitt ned i Kpbs	157,5	131,3	280,3	307,6

Samlet nedlastningshastighet



Konklusjon

Av de kortene vi testet var det HUAWEI E620 Mobile Connect UMTS/EDGE/GPRS PCMCIA-innstikkskort med Netcom SIM-kort som ga best nedlastningshastighet av de to kortene som støttet UMTS. Dette kortet mistet heller ikke kontakten med Netcoms UMTS-basestasjon en eneste gang i løpet av testrunden. Vi valgte derfor å bruke dette kortet i Natttjenesten. Av de to kortene som støttet EDGE-nettet var det kort 1- Sierra Wireless AirCard® 775 som kom best ut. Dette kan komme av at Sierra Wireless har flere tilgjengelig slotter for nedlastning enn kort 2 - Sony Ericsson GC85.