Teknisk kravspesifikasjon

For bruk ved anskaffelse og større oppgraderinger av SaaS-baserte og lokalt installerte IT-systemer og tjenester i Tromsø kommune.

Versjon 2.0

07.01.2013

Endringshistorikk

Versjon	Dato	Endringer	Navn
1.0	19.08.08	Første utgav dokumentet klar til bruk	Jan Holthe
1.1	21.08.08	Mindre justeringer	Jan Holthe
1.2	17.12.08	Justeringer i bl.a. kap. om sikkerhet og datautveksling samt sjekkliste.	Jan Holthe
1.3	22.12.08	Oppdatert WAI referanse til WCAG 2.0 og tatt med krav til universell utforming i kap.3	Jan Holthe
1.4	08.01.09	Oppdatert kap. 7 mht. tekniske krav for brukergrensesnitt på mobile enheter og fjernet kap. 3.5 om det samme.	Jan Holthe
1.4.1	02.03.09	Oppdatert kap. 5.3	Jan Holthe
1.5	25.08.09	Delt opp i 2 dokumenter og ajourført	Jan Holthe
1.6	16.09.09	Revidert etter gjennomgang med Vidar og Henning	Jan Holthe
1.7	28.09.09	Siste finpuss før ny versjon	Jan Holthe
1.8	01.11.2012	Diverse revideringer	Jan Holthe
2.0	07.01.2013	Oppdatert etter gjennomgang med IT-senteret. Slått sammen kravspek I og II til ett dokument.	Jan Holthe

Innholdsfortegnelse

Innledning

Tromsø kommune har som målsetting å være blant de beste kommunene i landet når det gjelder å etablere nye digitale tjenester for dialog mellom kommunen og innbyggerne. Målet er å kunne presentere helhetlig og tilpasset informasjon fra flere ulike baksystemer samt forenkle samhandlingen på tvers av sektorer og systemer.

For å oppnå dette, har Tromsø kommune utarbeidet en IT-strategi. Som en del av dette arbeidet, er det behov for å definere tekniske krav til nye systemer og tjenester slik at spesielt integrasjon og samspill med andre systemer forenkles.

1.1 Lokal installerte IT-systemer

Med lokalt installerte IT-systemer, mener vi her systemer som installeres lokalt på servere og klientmaskiner i Tromsø kommune. Dette kan være Windows-klient/tjener applikasjoner eller Web-baserte systemer som kjører mot en intern Web-server. Det vil i stadig sterkere grad også være snakk om hybrid-løsninger hvor lokalt installerte systemer benytter seg av eksterne Web-tjenester på utvalgte områder.

1.2 SaaS-baserte IT-tjenester

SaaS (Software as a Service) er en betegnelse på en forretningsmodell som innebærer at tjenester med tilhørende programvare og databaser, driftes eksternt hos 3.part og hvor tilgangen til tjenestene som regel skjer via et Web-grensesnitt (nettleser).

Dette dokumentet inneholder kravstillinger til leverandører av systemer basert på begge eller en av disse modellene.

1.3 Sjekkliste

De tekniske kravene er oppsummert og samlet i egen sjekkliste. Denne sjekklisten distribueres sammen med dette dokumentet.

2. Brukergrensesnitt

Dette kapitlet inneholder tekniske- og designmessige kravstillinger som skal bidra til at løsningen som anskaffes blir best mulig tilpasset de behov brukerne av kommunens løsninger måtte ha.

2.1 Web-klienter

World Wide Web Consortium (W3C) arbeider for at Web-teknologi skal utnyttes på best mulig måte og samtidig legge til rette for at mennesker med nedsatt funksjonsevne i størst mulig grad kan benytte teknologien. For å sørge for størst mulig tilgjengelighet på Web-baserte løsninger, skal disse derfor være utformet iht. retningslinjer definert i Web Content Accessibility Guidelines (WCAG) versjon 2.0.

2.1.1 Universell utforming

Regjeringens handlingsplan for økt tilgjengelighet for personer med nedsatt funksjonsevne, tar bl.a. sikte på å få fram standardiserte krav som kan gi en mer forutsigbar web (Universell utforming). WCAG kravene dekker ikke alle aspekter av dette.. Tromsø kommune ønsker at leverandører i størst mulig grad tar hensyn til krav om universell utforming ved levering av Web-baserte systemer.

2.1.2 Nettleserstøtte

For systemer som er basert på tilgang via nettleser, må systemet være testet på og tilby støtte for følgende utgaver:

Nettleser	Versjon
Microsoft Internet Explorer	9.0 eller høyere
Firefox	15 eller høyere
Chrome	22 eller høyere

2.2 Skjermoppløsning

Løsningen som anskaffes må støtte og tilpasse seg følgende skjermoppløsninger:

Standardproporsjoner:
- 1280 x 1024 piksler
- 1600 x 1200 piksler

WideScreen:
- 1680 x 1050 piksler
- 1900 x 1200 piksler

2.3 Mobile enheter

Web-baserte systemer bør i størst mulig grad også kunne benyttes på mobile håndholdte enheter. W3C har utarbeidet et sett med retningslinjer for hvordan Websider skal tilpasses mobile enheter på best mulig måte. Til disse retningslinjene (W3C MobileOK Basic Test) er det også utviklet en egen test som gir en bedømming av hvor mobilvennlig en nettside er og gir tips om hvordan manglende kan rettes opp.

Tromsø kommune ønsker at leverandørene tar hensyn til disse retningslinjene i forbindelse med utvikling av systemer med Web-basert brukergrensesnitt slik at løsningene også kan benyttes i de mest brukte nettleserne på de mobile plattformer.

2.3.1 App's

Det blir stadig mer vanlig at leverandører tilbyr spesialutviklede løsninger for hele eller deler av funksjonaliteten i form av app'er for smarttelefoner og nettbrett. Tromsø kommune ønsker å ta i bruk mobile enheter innenfor områder der dette kan være hensiktsmessig og vurderer det derfor som positivt om en leverandør kan tilby slike løsninger som tillegg til basisfunksjonaliteten.

2.4 Terminalservermiljø

Det er krav at alle applikasjoner skal være designet og utformet for å kunne kjøre problemfritt i et flerbruker terminalservermiljø som for eksempel Citrix.

2.5 Språkstøtte

Som et minimum, skal systemet ha støtte for norsk bokmål i menyer, ledetekster og hjelpesystem. Dersom systemet tilbyr flere språk, må det være mulig for brukeren selv å skifte til ønsket språk.

2.6 Skjemaløsninger

Forenkling av offentlige skjemaer er en viktig oppgave for å bedre kommunikasjonen mellom brukerne og offentlig sektor. Ved å følge gode pedagogiske prinsipper kan elektroniske skjemaer også sikre bedre

oppgaveforståelse, bedre kontroll av data før innsending, og dermed bedre svarkvalitet og mer effektiv saksbehandling hos den myndigheten som skal bruke svarene.

Nærings- og handelsdepartementet har vedtatt at ***Elmer 2*** standarden skal være felles retningslinjer for brukergrensesnitt i offentlige skjemaer på Internett. Dette er et helhetlig sett med prinsipper og spesifikasjoner for utforming av nettbaserte skjemaer. Leverandører som ønsker å levere skjemaløsninger til Tromsø kommune bør derfor støtte versjon 2.1 av denne standarden.

3. Plattform, integrasjon og arkitektur

Tromsø kommune stiller seg bak de overordnede arkitekturprinsippene for offentlig sektor slik de er formulert av Difi. Det innebærer følgende:

- Ved nyanskaffelser og/eller større oppgraderinger av eksisterende løsninger er det et krav at systemet og komponentene dette består av, er tilstrekkelig modularisert, løst koblet og benytter veldefinerte grensesnitt basert på felles begrepsmodeller (se kap.6).
- Løsningene skal være utformet og bygget slik at leverandøren enkelt og rimelig kan tilpasse systemet f.eks. i forbindelse med lovendringer.

.

3.1 Plattform

For systemer som skal installeres og driftes lokalt i kommunen, er det et krav at disse skal kunne kjøres på en plattform som er standard i Tromsø kommune. Følgende plattformer støttes:

System	Spesifikasjon
Klienter	Windows 7
Web-server	Apache/Tomcat Microsoft IIS versjon 7 eller høyere
Applikasjonsserver	Microsoft Windows 2008 Server R2 eller høyere
Databaseserver	Microsoft SQL Server 2008 R2 eller høyere Oracle 11
Operativsystem	MS Windows Server 2008 R2 eller høyere Ubuntu (alt. Linux kernel 3.2 eller høyere)

3.2 Datautveksling og kommunikasjon med andre systemer

En tjenesteorientert arkitektur krever fokus på integrasjon og standardisering. Data og funksjonalitet deles i stedet for å dupliseres. Dette gjelder både innenfor en enkelt sektor, på tvers av sektorer samt mot eksterne aktører og systemer. I en ny arkitektur er Web Services og XML sentrale teknologier for å få dette til.

3.2.1 Datautveksling / tjenestegrensesnitt

En av de største utfordringene i forhold til dagens systemer og samhandling, er mangel på standardiserte grensesnitt, semantikk og universelle transport protokoller.

I forbindelse med anskaffelser av nye systemer er det et krav at leverandøren kan tilby et veldefinert og dokumentert tjenestegrensesnitt basert på Web Services og at tjenestene er implementert i henhold til

protokoller og standarder som er vedtatt benyttet i offentlig forvaltning.

Det er ikke akseptabelt at leverandører kun tilbyr manuelt initiert filoverføring (import/eksport) som eneste eksterne grensesnitt for tilbudt system.

3.3 Integrasjon med MS Office

Der det er relevant, er det et krav at systemet skal tilby integrasjonsmulighet med den til enhver tid gjeldende kontorstøtteplattform. I Tromsø kommune gjelder dette for øyeblikket Microsoft Office produktene.

3.4 Integrasjon med Sak/Arkiv system

Der det er relevant, skal løsningen kunne integreres mot kommunens saksbehandlingssystem (EDB eSak).

3.5 Integrasjon med økonomisystem

Der det er relevant, er det et krav at systemet skal være klargjort for integrasjon mot Agresso.

3.6 Integrasjon med Lønns- og Personalsystem

Der det er relevant, er det et krav at systemet skal være klargjort for integrasjon Visma Enterprise HRM

4. Avbruddshåndtering

Systemet bør kunne håndtere følgende feil:

- nettverksbrudd, dvs. at det ikke oppnås kontakt over nettverket mot underliggende lag (eks. database/fagsystem/forretningslag/tjenester)
- underliggende lag er ”nede”, dvs. at det oppnås nettverkskontakt
- unormalt lange responstider fra underliggende lag

Når slike feil inntreffer bør brukeren få beskjed om dette. Dersom systemet består av flere funksjonelt separate komponenter, bør de delene av applikasjonen som ikke er avhengig av det aktuelle tjenestelaget fortsatt være tilgjengelig. Det er også en fordel at systemet selv automatisk overvåker og kan reetablere forbindelsen til underliggende lag.

5. Tilgangskontroll og sikkerhet

Personopplysningslovens m/forskrifter, inneholder forventninger om tilfredsstillende sikring av informasjonssystemer. Det er et absolutt krav at systemer som anskaffes, skal være utviklet på en måte som ivaretar de krav og føringer som her framkommer. Gjennom dette ønsker man i størst mulig grad å forhindre uautorisert adgang og tilgang til informasjon.

På tilsvarende måte gir Helseregisterloven og Norm for informasjonssikkerhet i helse-, omsorgs- og sosialsektoren (Normen) føringer for behandlinger av helseopplysninger i helseforvaltningen.

Disse kravene gjelder både i forhold til oppbevaring og behandling av informasjon. Det er her et viktig prinsipp at sensitive personopplysninger bare skal kunne være tilgjengelig for de som er spesielt autorisert for det, og at det skal være separasjon både i forhold til andre systemer i kommunen og spesielt i forhold til andre organisasjoner.

5.1 Sårbarhet i Web-applikasjoner

Leverandøren må kunne svare bekreftende på at sårbarhetene under (*Top Vulnerabilities in Web Applications*) er håndtert og at ingen slike feil finnes i applikasjonen. Feilene er listet opp i tabellen nedenfor:

A1 - Cross Site Scripting (XSS)	XSS feil opptrer når en applikasjon sender brukerinnmeldte data til en nettleser uten først å validere eller kryptere innholdet. XSS tillater angripere å utføre script i offerets nettleser som bl.a. kan resultere i sesjonsovertakelse, installering av virus og spionprogram osv.
A2 - Injection Flaws	Spesielt SQL injection er en vanlig sårbarhet i mange Web-applikasjoner. Angriperen modifiserer eller legger til kommandoer som en del av en eksisterende spørring eller kommando og kan på den måten få utført ulovlige kommandoer og/eller endret på grunndata i systemet.
A3 - Malicious File Execution	Kode som er sårbar for RFI(Remote File Inclusion) kan tillate angripere å inkludere fiendtlig kode og data som kan føre til ødeleggende angrep hvor f.eks. en hel server kompromitteres. PHP, XML og alle frameworks som aksepterer filnavn/filer fra brukere er sårbare ift. denne type angrep.
A4 - Insecure Direct Object Reference	Oppstår når en utvikler eksponerer en referanse til ett internt object som f.eks. en fil, en katalog, databaserekords eller databasenøkkel gjennom en URL eller et parameter. En angriper kan manipulere disse referansene og dermed få uautorisert tilgang til andre objekter/dataelementer.
A5 - Cross Site Request Forgery (CSRF)	Ett CSRF angrep tvinger nettleseren til en pålogget bruker å sende en pre-autorisert forespørsel til en sårbar Web-applikasjon. På denne måten tvinges offerets nettleser til å utføre en fiendtlige operasjon på vegne av angriperen.
A6 - Information Leakage and Improper Error Handling	Applikasjoner kan uten å ville det lekke informasjon om systemets konfigurasjon eller data gjennom en rekke forskjellige applikasjonsproblemer. En vanlig feil er f.eks. dårlig feilhåndtering som resulterer i at systemspesifikke feilmeldinger og data vises for brukeren. Angripere kan bruke denne informasjonen til å stjele sensitiv informasjon eller utføre andre mer alvorlige angrep.
A7 - Broken Authentication and Session Management	Konto kredentialer eller sesjons token er ofte ikke godt nok beskyttet. Angripere kan dermed kompromittere passord eller autentiseringsnøkler og gjennom dette operere med andre brukeres identitet.
A8 - Insecure Cryptographic Storage	Web applikasjoner gjør sjelden bruk av kryptografi for å beskytte data og kredentialer. Angripere utnytter en slik svak beskyttelse til å utføre identitets tyveri og/eller andre straffbare handlinger som f.eks. kredittkort svindel.
A9 - Insecure Communications	Mangelfull kryptering av nettverkstrafikk for å beskytte sensitive data.
A10 - Failure to Restrict URL Access	Ofte beskytter en applikasjon tilgangen til sensitive funksjonalitet kun ved å skjule lenker eller URL-er for ikke-autoriserte brukere. En angriper som kjenner funksjonen, kan aksessere og utføre ikke-autoriserte operasjoner ved å bruke disse URL-ene direkte.

5.2 Autentisering

Fornyings- og Administrasjonsdepartementet har definert 4 ulike risikonivå:

- Risikonivå 1 - Ingen
- Risikonivå 2 – Liten
- Risikonivå 3 – Moderat
- Risikonivå 4 - Stor

”Risikonivå 1 – ingen”, er beregnet på åpen informasjon. Funksjoner og informasjonsutveksling i tilknytning til informasjon som er konfidensiell, taushetsbelagt eller personsensitiv, må legges på de andre risikonivåene iht. hvilke sannsynlige konsekvenser som kan oppstå hvis uheldige hendelser finner sted. Plasseringen av en tjeneste i et gitt risikonivå peker direkte mot hvilket sikkerhetsnivå som må velges.

Sikkerhetsnivå 1

Dette sikkerhetsnivået gir liten eller ingen sikkerhet. Her fungerer helt åpne løsninger. Det finnes også sikkerhetsløsninger som vil havne i denne kategorien fordi de ikke tilfredsstiller kravene til sikkerhetsnivå 2. Dette gjelder løsninger som for eksempel:

- Selvvalgt passord og brukernavn over nettet.
- Identifisering kun vha. fødselsnummer

Sikkerhetsnivå 2
På dette sikkerhetsnivået fungerer alle løsninger som tilfredsstiller kravene til sikkerhetsnivå 2, men som ikke tilfredsstiller kravene til sikkerhetsnivå 3. Eksempler på sikkerhetsløsninger som havner i denne kategorien er:

- Fast passord, sendt ut i brev til folkeregisterregistrert adresse.
- Passordkalkulatorer uten passordbeskyttelse, minimum distribuert gjennom folkeregisterregistrert adresse.
- Engangspassordlister distribuert til folkeregisterregistrert adresse.

Sikkerhetsnivå 3
Middels sikkerhetsnivå hvor sensitive opplysninger ikke behandles. ”MinId” tilhører foreløpig dette nivået. Andre løsninger på dette nivået kan være:

- Passordkalkulatorer beskyttet med PIN-kode, der første PIN-kode er sendt i separat forsendelse
- Engangspassord på mobiltelefon, der mobiltelefonen er registrert med en egen registreringskode distribuert til folkeregisterregistrert adresse.
- Engangspassordlister benyttet sammen med fast passord og brukernavn. Valg av fast passord skal skje på bakgrunn av en engangskode sendt til folkeregisterregistrert adresse (eventuelt første kode på engangspassordlisten)

Sikkerhetsnivå 4
I praksis er det bare PKI-baserte løsninger som tilfredsstiller dette nivået. Omfatter behandling av sensitive opplysninger og behov for høyeste sikkerhetsnivå. I henhold til gjeldende regelverk må løsningene være selvdeklarert i Post- og teletilsynet i forhold til om de oppfyller krav i «Kravspesifikasjon for PKI i offentlig sektor».

Pr. i dag tilbyr ID-porten innlogging på dette sikkerhetsnivået ved hjelp av løsninger fra BuyPass, Commfides og BankID.

5.2.1 Integrasjon mot ID-porten

ID-porten gir tilgang til nettjenester i mer enn 240 offentlige virksomheter og er en offentlig fellesløsning driftet av Direktoratet for forvaltning og IKT (Difi). ID-porten gir i dag innbyggerne valget mellom tre elektroniske ID-er: det offentliges egen MinID og de private løsningene Buypass, Commfides eID og BankID.

Der dette er hensiktsmessig, skal nye systemer som anskaffes – helt eller delvis - tilbyr autentisering via integrasjon mot ID-porten.

5.2.2 Integrasjon mot FEIDE

Feide - Felles Elektronisk IDEntitet - er Kunnskapsdepartementets valgte løsning for sikker identifisering i utdanningssektoren. FEIDE er basert på føderert identitetshåndtering noe som innebærer at tjenester stoler på den autentiseringen som gjøres av brukernes vertsorganisasjoner. Tjenestene gjør seg nytte av de opplysninger vertsorganisasjonene sitter på når det gjelder tilgangskontroll, personifisering osv.

Alle nye systemer som anskaffes innenfor skolesektoren i Tromsø kommune, skal der det er hensiktsmessig, tilby FEIDE-pålogging

5.2.3 Autentisering og bruk av fødselsnummer

- Fødselsnummer skal bare brukes når det er saklig behov, og når det er umulig å oppnå

tilfredsstillende identifikasjon ved bruk av andre metoder, som for eksempel navn, adresse, fødselsdato, medlems- eller kundenummer.
- Overføring av fødselsnummer skal alltid krypteres.
- Fødselsnummer skal aldri brukes til autentisering alene, men kan kun eventuelt brukes som brukerident i en autentiseringsløsning.

5.2.4 Integrasjon mot AD

Systemet må, der dette er relevant, ha støtte for integrasjon med Microsoft Active Directory(AD) slik at autentisering/pålogging skjer automatisk basert på gjeldende AD innlogging...

5.2.5 Citrix

Ved distribusjon av systemet som tynnklient(Citrix), *bør* det være mulig å automatisk overføre credentials fra Citrix sesjonen til systemet og derved gjøre dedikert innlogging unødvendig.

5.3 Autorisering

Systemet bør tilby rollebasert tilgangsstyring med minimum tre ulike tilgangsnivå i form av for eksempel rollene Administrator, Superbruker og Bruker. Det kan også i større systemer være behov for at administrator kan sette opp egne roller og tildele rettigheter til disse.

5.3.1 Administrasjonsrettigheter

Det er et absolutt krav at nye systemer ikke skal kreve administrasjonsrettigheter på klientmaskiner i daglig bruk.

5.4 Logging/sporbarhet

Systemet bør ha funksjonalitet for logging av viktige hendelser. Følgende system spesifikke loggfiler (eller tilsvarende) bør være etablert:

Loggnavn	Beskrivelse
Transaksjonslogg	Logger alle transaksjoner som skjer i systemet. Spesielt viktig i forhold til kommunikasjon med delsystemer og eksterne system i forbindelse overføringer av pengebeløp.
Sikkerhetslogg	Inneholder informasjon om av/påloginger samt forsøk på inntrenging og kompromittering av sikkerheten i systemet. Omtales også som «Hendelsesregister» (ref. Normen) i forbindelse med systemer i helse- og omsorgssektoren.
Brukerfeillogg	Kritiske brukerfeil som har skjedd i systemet.
Systemfeillogg	Informasjon om systemspesifikke feil som har oppstått. Viktig at dette ikke logges sammen med brukerfeil.
Batch logg	Aktuelt dersom systemet benytter seg av satsvise (batch) operasjoner i bakgrunnen. Logger tidspunkt for start/stopp samt resultater eller evt. feil som har oppstått.

- Alle logginnslag bør være tidsstemplet basert på lokal tid og formattert i henhold til ISO 8601 standarden (2008-09-15T13:01:01) eller tilsvarende.
- Innslagene må inneholde nødvendig transaksjons- og/eller kunde/klient id.
- Dersom loggfilene kan tenkes å vokse raskt i størrelse, bør systemet logge kjente feil basert på dokumenterte feilkoder i stedet for å benytte hele feilmeldingen.
- Loggfiler bør navngis med YYYY-MM-DD som en del av filnavnet.
- Større systemer bør ha på plass funksjonalitet for automatisk rotering av loggfiler ved midnatt.
- Muligheter for av/på slåing av ulike loggnivå (Utfyllende feilsøkingsinformasjon)

5.5 Kryptering

All informasjon som opptrer i systemet og som iht. Personopplysningsloven eller Norm for informasjonssikkerhet i helse og omsorgsektoren, betraktes som sensitiv og/eller konfidensiell, skal beskyttes ved kryptering under transport. Transportkrypteringen skal være basert på SSL v.3/TLS v.1 eller bedre.

Det er også ønskelig at systemet kan konfigureres til å lagre overnevnte informasjon i kryptert tilstand.

5.5.1 Helse- og omsorgssektoren

Norsk Helsenett er et lukket nettverk for elektronisk kommunikasjon og samhandling i helse- og omsorgssektoren i Norge. Norsk Helsenett tilbyr infrastruktur og basistjenester. Sensitiv informasjon skal ikke gå i klartekst over Norsk Helsenett, og må derfor krypteres før den går ut av virksomheten.. Virksomhetssertifikater fra godkjent PKI-tjeneste på tilstrekkelig sikkerhetsnivå må benyttes for signering og kryptering på virksomhetsnivå.

6. Standarder

Både Fornyings- og administrasjonsdepartementet (FAD), Difi, KS og K10-kommunene arbeider for å ta fram IT-standarder for offentlig forvaltning som skal bedre samhandlingen, redusere bindinger til enkeltleverandører og sørge for likebehandling og inkludering av alle innbyggere uavhengig av hvilken programvare eller plattform hver enkelt benytter.

6.1.1 Referansekatalogen for IT-standarder i offentlig forvaltning

Det er foretatt en justering av rollene for FAD, Difi og Standardiseringsrådet i forhold til tidligere når det gjelder fastsetting av obligatoriske og anbefalte forvaltningsstandarder innenfor offentlig sektor.

FAD stiller gjennom «Referansekatalogen for IT-standarder i offentlig forvaltning» de obligatoriske krav som statlige og kommunale virksomheter skal forholde seg til ved utvikling av sine IT-tjenester. Gjeldende versjon av referansekatalogen er versjon 3.0, men det er forventet at det vil foreligge en revidert utgave som gjøres gjeldende fra januar 2013.

Difi har fått myndighet til å fastsette anbefalte forvaltningsstandarder som også skal gjelde for kommunene.

Tromsø kommune vil sørge for å til enhver tid oppfylle de obligatoriske krav - og i størst mulig grad også støtte de anbefalte standardene - som stilles i gjeldende versjoner av forvaltningsstandardene. . Vi ønsker derfor at leverandører av nye systemer og tjenester gjør seg kjent med de krav og anbefalinger som stilles i disse standardene og følger opp i forhold til egne løsninger...

6.1.2 Resultat XML

KS har gjennomført et prosjekt for utvikling av standardisert grensesnitt mellom skjemaløsninger, fagsystemer og sak-/arkivsystemer i kommunesektoren. Hovedformålet med standarden er å hindre leverandørbindinger og sikre teknisk og semantisk interoperabilitet. Standarden er generell for kommunesektoren uavhengig av fagområde. Med standard forstås i denne sammenheng en teknisk anbefaling/forvaltningsstandard for kommunesektoren.

Det er ønskelig at leverandører hensyntar de tekniske anbefalingene som framkommer gjennom «Resultat XML» og etter hvert innarbeider disse i sine løsninger.

6.1.3 NKXML

Bærum kommune har gjennom sitt SOA prosjekt utarbeidet et sett med navngivnings- og designregler for

utformingen av XML Schema og WSDL dokumenter. Hensikten er å sikre utviklingen av interoperabile Web Services og grensesnittdefinisjoner. K10 har vedtatt at BKXML standarden skal benyttes som grunnlag for en felles kommunal informasjonsmodell (NKXML).

NKXML-standarden er under utvikling, men det er ønskelig at leverandører av IT-systemer til kommunal sektor kjenner til standarden og i den grad det vil være aktuelt, tilpasser egne løsninger til de definisjoner standarden adresserer.

På sikt er det forventet at «Resultat XML» og «NKXML» smelter sammen og blir til en felles standard og informasjonsmodell.

7. Dokumentasjon og hjelpesystem

Det er ønskelig at systemet der det er relevant, leveres med følgende eller tilsvarende dokumentasjon:

Dokument	Beskrivelse
Systemdokumentasjon	• Systemet i seg selv og sammenhengen med andre systemer. • Overordnet arkitekturbeskrivelse • Grensesnitt og avhengigheter mellom interne og eksterne moduler og systemer.
Grensesnittbeskrivelse	• Detaljert teknisk og funksjonell beskrivelse av grensesnittet som systemet tilbyr eksternt.
Driftsdokumentasjon	• Maskinvarekrav og nødvendig konfigureringsinformasjon • Programvareinstallasjon og konfigureringsinformasjon • Plattformdriftsrutiner
Databasedokumentasjon	• Beskrivelse av databasestrukturen inkl. oppbygning og databaseobjekter(tabeller, roller, prosedyrer osv.)
Brukerdokumentasjon	• Beskrivelse av hvordan systemet brukes og administreres.
Hjelp	• Systemet skal ha integrert kontekst sensitiv hjelp. Hjelpesystemet bør være organisert slik at brukeren får hjelp mht. bruk av gjeldende funksjon eller skjermbilde. Tooltips og/eller felthjelp er også ønskelig.

8. Tilgjengelighet/oppetid

Systemet eller tjenesten skal som hovedregel kunne være tilgjengelig 24x7x365. Unntak er evt. planlagt nedetid ved nødvendig systemoppgradering og sikkerhetskopiering. Totalt sett bør tilgjengeligheten kunne ligge på 99.8 % innenfor definert oppetid.

Med definert oppetid mener vi her den oppetidsprosenten som måles mellom kl.08.00 og 16:00, mandag t.o.m. fredag gjennom en måned.

Oppetidskravene skal for øvrig reguleres gjennom dedikert SLA(Service Level Agreement) mellom tjenesteleverandør og kunde.

9. Support og vedlikehold

Det er et viktig kriterium ved vurdering av tilbudte systemer at potensielle leverandører kan vise til en god servicemodell. Spesifikke områder som er særlig viktige i vurderingen av de tekniske kvaliteter inkluderer følgende (i ikke-rangert rekkefølge):

- God tilgjengelighet av kvalifisert teknisk personell hos leverandør, og åpne kommunikasjonskanaler mellom disse og ansvarlig personell hos kunden.
- Generell feilhåndtering.
- Støttemekanismer ved innrapportering av feil i programvare, som for eksempel:
    - Tilgjengelighet av dedikert supportpersonell hos leverandør.
    - Tilgjengelighet av fullstendige oversikter over allerede kjente feil med beskrivelse av metoder for å unngå dem
    - Mekanismer for at kunde/driftspersonell skal fortløpende kunne følge status "online" på innrapporterte feil
- Teknikker for installasjon av feilfikser ("patching") etter at programvarefeil er eliminert hos leverandør
- Ansvarsfordeling for arbeidsoppgaver til driftspersonell hos kunde kontra leverandør
- Mekanismer for oppgraderinger av hovedsystemet, både ved mindre (inkrementell "patchlevel" utsending) og større (ved innføring av ny funksjonalitet).
- Brukervennlig administrasjonsgrensesnitt

9.1 ITIL sertifisering

Det er ønskelig at leverandører baserer sine kundestøtte- og leveranseprosesser på ITIL rammeverket og innehar gyldig sertifisering på området.