

## Trenger du en epost-arkitektur?

*Vi har epost-systemer – tjenere, klienter, kanskje sågar filtre og arkiver. Men har vi en arkitektur? Og trenger vi det? For de fleste miljøer som håndterer sin egen epost, er svaret ja – på grunn av det voksende volumet, viktigheten av epost i virksomheten, og ikke minst på grunn av truslene. De fortsetter å vokse, og det er ingen grunn til å tro at utviklingen vil snu.*

### Handling på overtid?

Prinsippet om at “if it ain't broken, don't fix it” fungerer ofte – men ikke alltid. Tilsvarende kan sies om “det vi ikke vet, har vi ikke vondt av”. For epostens vedkommende er begge deler feil: Den er ofte ute av kontroll uten at noen er klar over det før det er for sent. Likeledes trenger den ikke å være ‘ødelagt’ i betydningen ute av funksjon for å ha stor nytte av en vesentlig overhaling eller oppgradering.

Nå er forholdet slik – som vi har vært inne på ved en rekke anledninger tidligere – at teknisk håndtering av epost egentlig ikke hører hjemme i noen organisasjon. Knappt noen tjeneste er bedre egnet til *outsourcing* enn nettopp epost. For de fleste miljøer er det faktisk slik at det neppe noen gang blir skikkelig orden på eposten før den er overlatt til spesialister. Årsaken til at vi ikke kan sende stafettpinnen videre med det samme, er at det finnes altfor få av dem der ute, og våre sjanser til å skaffe eller lære opp lokal ekspertise er beskjedne. At enkelte lykkes med nettopp dette (se for eksempel artikkelen om Sandefjord Kommune på side 19), betyr ikke at det er mulig for miljøer flest å gå samme vei.

### Fra støttefunksjon til virksomhetskritisk tjeneste

Også den generelt stemoderlige behandlingen epost har blitt tildelt i organisasjoner flest, har vært gjenstand for diskusjoner i Mellvik-Rapporten. Nå er denne situasjonen stort sett tilbakelagt – i oppmerksomhetsmessig forstand: Verken styrer eller toppledere vinker lenger avfeiende med hånden når epost kommer på bane, og de fleste er i stand til å se både avhengighetsforhold og sikkerhetsmessige sider. Derfra til å akseptere nødvendigheten av for eksempel opplæring, juridiske avklaringer, retningslinjer for bruk og så videre, er det imidlertid et drøyt stykke. Lerretet som skal blekes er med andre ord fortsatt av betydelig størrelse.

Mens jobben med å flytte tjenesten inn i en ryddigere setting fortsetter, må de av oss som har teknisk ansvar, legge forholdene til rette for at denne virksomhetskritiske tjenesten fungerer og er pålitelig. At den har oppfylt begge kravene over lang tid, er ingen garanti for at situasjonen vil vedvare. Ofte er det motsatte tilfelle: Systemet har ikke vært utsatt for tilstrekkelig store påkjenninger til at svakhetene er kommet

til syne. Her er noen av momentene som indikerer at 'hvetebrødsdagene' nærmer seg slutten:

- ✓ Epost-systemet og grensesnittet er – tilfeldig eller planlagt – blitt et konvergeringspunkt for stadig flere såkalte meldingstjenester. De lettest synlige er telefaks, talepost og SMS.
- ✓ Tilgangen til epost er blitt like kritisk som tilgangen til telefon. I enkelte tilfeller går de over i hverandre, og telefonen blir epost-klient.
- ✓ Med stadig flere klient-typer som skal støttes og krav om 100% tilgjengelighet, blir monolittiske produktarkitekturer som var tilfredsstillende for 5 og 3 år siden, ikke lenger akseptable.
- ✓ Kravene til sikkerhet følger de andre forholdene vi har nevnt ovenfor, og sørger for at tradisjonell 'etterpå-sikring' ikke lenger er akseptabelt. Sikkerheten må inn i arkitekturen, være dokumentert og etterprøvbart. Det faktum at langt over 90% av alle virus blir distribuert via epost, er mer enn nok til å bringe nettopp dette forholdet i fokus.
- ✓ Lagring og arkivering er blitt et område og en utfordring for seg selv, som vi diskuterte i forrige utgave (nr. 114).
- ✓ LDAP-baserte katalogtjenester og *Identity Management* systemer<sup>3</sup> sentraliserer brukerinformasjon, og skal være effektivt koblet til epost-systemet – som på sin side ikke skal ha eller administrere brukerspesifikk informasjon.
- ✓ Epost er blitt en synlig kostnad i budsjettene, hvilket i mange tilfeller har forårsaket en overmoden diskusjon om behov, løsninger og muligheter for optimalisering. Praktisk talt uten unntak har kostnadenes omfang kommet som en overraskelse.

Epost er med andre ord ikke lenger et spørsmål om tjenester og funksjonalitet, men også om økonomi: Hvor mye koster herligheten, og hva får vi igjen for pengene?

## På tide å tenke nytt

Den mest nærliggende og samtidig viktigste observasjonen vi kan gjøre i kjølvannet av punktene ovenfor, er at tradisjonelle monolittiske 'alle-funksjoner-i-én-boks' løsninger har gått ut på dato. Den mest fundamentale forutsetningen for egenskaper som skalerbarhet, pålitelighet og sikkerhet er at løsningens bestanddeler er identifiserbare. De skal ikke bare være bokser i en brosjyre eller en presentasjon, men moduler som etter behov kan flyttes mellom fysiske bokser og om nødvendig fordeles over flere.

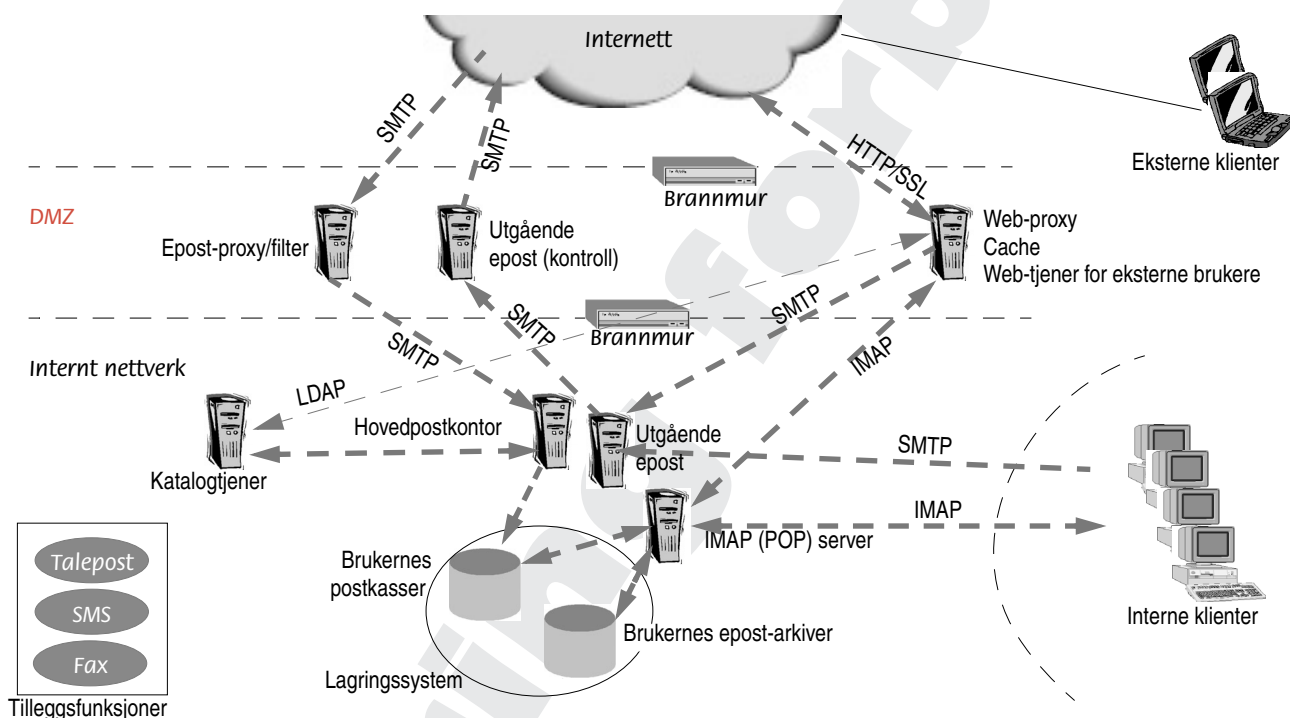
Det betyr i sin tur at grensesnittene må være veldefinerte, stabile og standardiserte, et krav vi har poengtert ved en rekke tidligere anledninger i Mellvik-Rapporten, og som er viktigere enn noen gang. Årsaken til at vi diskuterer epost-arkitektur er jo nettopp at mange av

<sup>3</sup> Vi kommer tilbake til katalogtjenester og IDENTITY MANAGEMENT i en egen hovedartikkel senere i år.

produktene som har vært dominante i markedet i en periode, ikke lenger strekker til – utover de minste og enkleste miljøene. Og selv der svikter det med voksende hyppighet, ikke funksjonelt, men med hensyn til sikkerhet og stabilitet.

### En åpen arkitektur

Figur 1 viser en prinsippskisse for en moderne epost-arkitektur. Hovedvekten er lagt på å få frem de funksjonelle elementene som inngår og protokollene som knytter dem sammen. Vi har videre holdt oss strengt til meldingsformidling i denne omgang, og skal kommentere tilleggsfunksjoner (typisk kalender) nedenfor.



**Figur 1** En epost-arkitektur skal identifisere alle funksjonelle elementer som inngår i systemet, og plassere dem i forhold til viktige infrastrukturkomponenter som brannmurer, DMZ, lagringssystemer, katalogtjeneste og så videre.

De viktigste funksjonelle elementene i arkitekturen kan kort beskrives slik:

- ✓ **Hovedpostkontoret** er selve fordelingsentralen for innkommende epost, og i utgangspunktet det mest kompliserte element – med hovedoppgave å levere innkommende post til brukernes postkasser. Grensesnittet mot disse postkassene er et kritisk valg som blant annet påvirker fleksibiliteten med hensyn til valg av IMAP-tjenere (se neste punkt). Her er det flere *de facto* og ingen *de jure* standarder å velge mellom.<sup>4</sup> Det viktigste er at formatet gjør postkassene tilgjengelige for andre, og ikke låser meldingene inne i en database eller et leverandørspesifikt spesialformat.

<sup>4</sup> Vi kommer tilbake til denne problemstillingen i gjennomgangen av ulike leverandørstrategier i neste utgave, se baksiden for detaljer.

- ✓ **Epost-proxy/filter** er et kritisk element for både sikkerheten og effektiviteten i systemet. En slik proxy kan gjerne være usynlig for det interne hovedpostkontoret, og har som hovedoppgave å kontrollere innkommende meldinger før de slippes videre eller eventuelt avvises. De viktigste oppgavene er SPAM-kontroll, viruskontroll og eventuelt kontroll av at mottakerne finnes.<sup>5</sup> Dersom også sistnevnte oppgave er med, må tjenesten ha tilgang til LDAP-katalogen direkte eller eventuelt en speilet utgave av denne (av sikkerhetsmessige årsaker). En slik mottaks-kontroll representerer en betydelig avlastning av hovedpostkontoret, som slipper å beskjefte seg med returere, og for nettverket – siden meldinger som ikke er akseptable, avvises 'i døren'.
- ✓ **IMAP-tjeneren** betjener brukerne og har den tyngste jobben i arkitekturen. All brukerinteraksjon mot postkasser og arkivbokser går via denne, som forutsetningsvis må håndtere det samme postkasseformatet som hovedpostkontoret. Mange, kanskje de fleste kommersielle produkter har denne tjenesten inkludert i nettopp hovedpostkontoret, hvilket også er hovedårsaken til deres karakteristiske ytelses- og skaleringsproblemer. Det finnes ingen tekniske argumenter for – men mange imot – å koble disse tjenestene tett sammen. Siden en rekke miljøer fortsatt bruker POP-protokollen for klient-aksess (hvilket frarådes), er det naturlig at denne tjeneren også kan levere POP-tjenester.
- ✓ **Utgående epost** håndteres som regel i første ledd av hovedpostkontoret, hvilket er OK så lenge kapasiteten finnes. Oppgaven er enkel nok: Å sende internpost direkte til hovedpostkontoret, og dirigere eksterntpost videre – enten til en ekstra kontrollpost eller direkte til mottaker. Det siste er mest vanlig, men det er ikke lenger akseptabelt å sende epost ut fra organisasjonen uten at den har vært kontrollert. Det aller meste av Internettets SPAM og virus kommer fra intetanende personer og organisasjoner som er blitt infisert. Denne strømmen kan og bør stoppes av et utgående filter. Om filtreringen skal gjøres av tjeneren for utgående post eller en egen filtreringstjener (i DMZ), er et spørsmål om sikkerhet og kapasitet. Vår anbefaling – i henhold til figuren – er å prioritere sikkerheten og velge en todelt løsning. Videre er det rimelig å stille spørsmål om den sendende epost-tjeneren skal være synlig for eksterne mottakere, eller om vår eksterne brannmur skal stå som avsender. Å la brannmuren stå som avsender er en grei hovedregel. Imidlertid er det viktig å sørge for at avsenderen – uansett om det er den ene eller den andre 'boksen' – har en registrert IP-adresse med tilgjengelig reversopp-slag, slik at mottakerne kan verifisere at vi er en legitim avsender. Selv store og antatt profesjonelle organisasjoner – i inn- og utland – syndrer stort på dette punktet.

<sup>5</sup> Vi gjennomgikk disse funksjonene i detalj i SPAM-artiklene i Mellvik-Rapporten nr. 106 og 107.

- ✓ **Web-mail:** Bruk av nettleser-baserte epost-grensesnitt viser med god grunn voksende popularitet. Med SSL-sikring sørger slik aksess til postkasser og arkiv for effektiv og lettvinntilgang til eposten nærmest uansett hvor brukeren er, upåvirket av brannmurer, pakkefiltre og utstysrestriksjoner. Vi skal ikke komme inn på egenskaper i selve Web-mail løsningen i denne omgang, men påpeke at Web-tjenerens plassering i forhold til IMAP-tjener og LDAP-tjener er viktig både for effektivitet og sikkerhet. Den sikreste og dermed foretrukne varianten er å benytte en intern Web-tjener via en proxy som samtidig terminerer SSL-forbindelsen.

### **Enkel skalering**

For små og mellomstore miljøer kan en slik arkitektur virke unødig komplisert – og vil alltid være mer kompleks i driftsmessig forstand enn en tradisjonell alt-i-ett løsning. At enkeltfunksjonene i løsningen er separate, betyr imidlertid ikke at de krever sin egen maskin. Tvert imot vil det være naturlig for små og mellomstore miljøer å plassere alle eller de fleste interne epost-funksjoner på én og samme maskin. Kontrollfunksjonene i DMZ forutsetter egen hardware, men er ikke spesielt ressurskrevende. Med en optimal arkitektur og ditto produkter, kan sågar flere titusen brukere håndteres av én eller to maskiner og fortsatt ha rikelig reservekapasitet.<sup>6</sup> Arkitekturen forteller først og fremst hvordan systemet skal settes sammen, ikke hvordan oppgavene fordeles på maskinutstyret.

### **Tid for konsolidering og oppgradering**

En gjennomgang av epost-arkitekturen er spesielt aktuell for miljøer som i disse dager vurderer oppgraderinger av Lotus Notes/Domino, Exchange 5.x eller enda eldre stormaskinbaserte epost-systemer. Selv de nyeste utgavene av disse produktene har en tradisjonell monolitisk arkitektur, og første kritiske valg er om dette er akseptabelt eller ikke. I løpet av de siste årene har det dukket opp produkter som er pluggkompatible med MS Exchange og i noen tilfeller Domino og GroupWise, hvilket gir flere valgmuligheter med hensyn til såvel arkitektur som system. Hva som karakteriserer disse alternativene skal vi komme tilbake til i neste utgave (se baksiden for detaljer).

Selv om kjernen i meldingssystemet er gitt – og for eksempel er nettopp Domino, GroupWise eller Exchange – finnes det fortsatt betydelige muligheter for å optimalisere arkitekturen. De eksterne filtreringsmodulene kan introduseres på samme måte som vi har beskrevet, uten å påvirke det sentrale systemet på annen måte enn å redusere belastningen. Likeledes kan en separat IMAP-tjener bidra til å optimalisere ytelsesbildet vesentlig.

<sup>6</sup> En ISP vi kjenner til, har 200.000 brukere per epost-tjener som 'tommelfingerregel'. Det sier seg selv at disse brukerne aldri er aktive samtidig, og situasjonen er ikke direkte sammenlignbar med et typisk kontormiljø. Tallet sier imidlertid mye om spennvidden i tilgjengelige kommersielle meldingsformidlingsløsninger, der anbefalt antall brukere per fysisk system strekker seg over flere størrelsesordener.

### Tilleggstjenester

Vi har så langt ikke nevnt tilleggstjenester, der kalender er det mest fremtredende element. At kalendertjenesten ikke har noe med meldinger eller epost å gjøre, er på den ene siden et faktum, og på den andre siden av underordnet betydning. Inntil portal-baserte brukergrensesnitt løser opp denne koblingen, er den et faktum vi må forholde oss til.

I teknisk forstand er dette relativt trivielt. Vi har valget mellom å bruke leverandørens proprietære protokoller (for eksempel MAPI for MS Exchanges vedkommende) eller standardprotokoller med tilsvarende funksjonalitet (iCalendar). De mest populære brukergrensesnittene kan forholde seg til flere varianter, hvilket gir et visst spillerom. Imidlertid viser erfaring at det er et drøyt stykke fra leverandørens brosjyrer til hva som fungerer i praksis. Derfor er det praktiske tester og demonstrasjoner som avgjør hva som er reelle alternativer.

Leverandørene som har kastet seg inn i meldingssegmentet de siste årene – for eksempel Sun og Oracle, er avhengige av god kompatibilitet med eksisterende brukergrensesnitt for å kunne hevde seg i markedet. Derfor burde slik tilleggsfunksjonalitet ikke representere noen stor utfordring, uansett hvilken løsning vi velger.

## Oppsummering

Mens epost- og meldingssystemer i sin alminnelighet er på full fart ut av sin skyggefulle tilværelse, er det et betydelig stykke igjen til tjenestene er under tilfredsstillende kontroll – sikkerhetsmessig og ytelsesmessig. Kravene til skalerbarhet og pålitelighet hører hjemme øverst på prioriteringslisten, og forutsetter en arkitektur som plasserer funksjonene der de hører hjemme.

En slik arkitektur er verken komplisert eller tidkrevende, og danner et solid grunnlag for i første omgang å få oversikt over organisasjonens reelle behov, og dernest stille krav til potensielle leverandører. Hva de ulike leverandørene i segmentet har på tapetet, kommer vi tilbake til i neste utgave. Hvordan forholder de seg til markedets praktiske utfordringer, og hvilken grad av åpenhet kan de tilby i forhold til blanding av løsninger, tilleggsfunksjonalitet og ikke minst standarder? ■