Microsoft Kommundesign MSKD

Version 4.0

people ready

Microsoft

Innehåll

1 Versionskommentarer 1
1.1 Författare 4.0 1
1.2 Medförfattare 4.0 1
2 Kort sammanfattning 2
2.1 Infrastruktur 2
2.2 Kärnvärden 2
2.3 Vinster 2
2.4 Utmaningar 2
3 Historik 4
3.1 MSKD 1.0, juni 2004 4
3.2 MSKD 2.0, mars 2005 4
3.3 MSKD 3.0, juni 2007 5
3.4 Sammanfattning tidigare MSKD versioner 6
3.5 Citizen Service Platform 6
4 Kärnvärden MSKD 8
4.1 Kärnvärden 8
4.2 Exempel på vinster med konsolidering och standardisering 8
4.3 Miljöanpassning – Grön IT 9
4.3.1 Konsolidering och virtualisering 9
4.3.2 Modern teknik drar mindre ström 9
4.3.3 Minskat resande minskar utsläppen 9
5 Vision och omfattning 11
5.1 Förutsättningar inför MSKD 4.0 11
5.1.1 Avgränsa mot CSP:s övre lager 11
5.1.2 Stort intresse 11
5.1.3 Myterna i MSKD 11
5.2 Primära teman version 4.0 12
5.2.1 Server and Domain Isolation 12
5.2.2 Windows 7 och Windows Server 2008 R2 12
5.2.3 Cloud Computing Single Sign-On och ADFS 2.0 13
5.3 Sekundära teman 13
5.4 MSKD Versioner 13
5.5 MSKD 4.0 Nivåer 14
5.6 Avgränsning 14
6 Införande - Projektmetodik 15

6.1 Projektstyrningsmodell 15
6.1.1 Kända projektstyrningsmodeller 15
6.2 Vattenfallsmodellen 15
6.3 Iterativ utveckling 16
6.4 Microsoft Solutions Framework 16
6.5 PROPS 17
6.6 Scrum 17
6.7 Kompetensuppbyggnad 17
6.8 Projekt och aktiviteter 18
6.8.1 Projekt 18
6.8.2 Aktiviteter 18
7 Drift - Processer och organisation 20
7.1 Processer 20
7.1.1 MOF/ITIL och ITSM 20
7.1.2 Kommunen och MOF/ITIL 21
7.1.3 Exempel på processer och rutiner 22
7.2 Organisation 24
7.2.1 Roller och kompetens inom IT-organisationen 24
7.2.2 IT-mognadsgrad 25
7.2.3 Standardisering 26
7.2.4 Centralisering 26
7.2.5 Service Desk 27
7.2.6 SLA 27
7.2.7 IT-strategi 27
7.2.8 Egen IT-drift/Beställarorganisation 27
7.2.9 Outsourcing/Cloud Computing 27
8 Referensdesign 28
8.1 Katalogtjänst – Active Directory 28
8.1.1 Active Directory Domain Services Design 28
8.1.2 Namnstandard 31
8.2 Public Key Infrastructure (PKI) 31
8.2.1 Användningsområden PKI 32
8.2.2 Alternativ till intern PKI 32
8.2.3 Active Directory Certificate Services (ADCS) 32
8.3 Single Sign On (SSO) 33
8.3.1 Active Directory Federation Services (ADFS) 33
8.4 Identitets- och åtkomsthantering 33
8.4.1 Vad menar vi med identitetshantering? 34

8.4.2 Identity Lifecycle Manager (ILM) 2007 35
8.4.3 Forefront Identity Manager 2010 35
8.4.4 Utveckling 35
8.5 Nätverksdesign 36
8.5.1 Ett fysiskt nätverk 36
8.5.2 Åtkomst: hanterade klienter 36
8.5.3 Åtkomst: icke hanterade klienter 40
8.5.4 Trådlösa nätverk 41
8.5.5 Utgående Internetåtkomst 41
8.6 Hanterad standardklient 41
8.6.1 Windows 7 41
8.6.2 Microsoft Deployment Toolkit 2010 42
8.6.3 Applikationspaketering 43
8.6.4 Datortyper 45
8.7 Servervirtualisering 47
8.7.1 Inledning 47
8.7.2 Private Cloud 47
8.7.3 Vilka system ska virtualiseras? 47
8.7.4 Hantering av virtualiserade system 48
8.8 Säkerhet 48
8.8.1 Patchhantering 49
8.8.2 Windows Server Security Guide 49
8.8.3 Windows 7 Security Guide 49
8.8.4 Windows BitLocker Drive Encryption 49
8.8.5 AppLocker 49
8.8.6 Stark autentisering 50
8.8.7 CLM (ILM) 50
8.8.8 DirectAccess 50
8.8.9 NAP (Network Access Protection) 50
8.8.10 RMS (Rights Management Services) 51
8.8.11 Forefront 51
8.8.12 Förslag och tips på lösenordspolicy 52
8.9 Management 52
8.9.1 System Center 53
8.9.2 Server Management Suite Licensing 57
8.9.3 MDOP 58
8.10 Unified Communications och samarbete 59
8.10.1 Snabbmeddelande och närvarohantering 59

8.10.2 Collaboration; SharePoint 2007 60
8.10.3 Exchange Server 63
8.11 Microsoft Online Services 64
8.11.1 Business Productivity Online Suite (BPOS) 64
8.11.2 Referensdesign för BPOS 65
8.11.3 Live@edu 65
8.11.4 Single Sign On/Federation 65
8.11.5 Lagring utomlands 66
8.12 Verksamhetslösningar 66
8.12.1 Microsoft Citizen Service Platform 66
8.12.2 Arkitekturer som stöds av infrastrukturen i MSKD 4.0 67
8.13 Migrering 68
8.13.1 Vad är migrering? 68
8.13.2 Migrering från befintlig Active Directory-domän 69
8.13.3 Novell NDS-migrering 70
8.13.4 Migrering från Exchange 72
8.13.5 Migrering från Lotus Notes/Domino 73
8.13.6 Migrering från Groupwise 73
8.13.7 FirstClass 74
9 Licensiering 75
9.1 Nivåer 75
9.2 Licenser 75
9.3 Volymlicensiering 76
9.3.1 Enterprise Agreement 76
9.3.2 Software Assurance 76
9.3.3 Enrollment for Enterprise Agreement 77
9.4 Licensing Management Suites 78
9.1 Professional Desktop 78
9.2 Enterprise Desktop 78
9.3 Per User/Per Device 79
9.4 Windows Server 79
9.4.1 Virtualisering 79
9.4.2 VDI 80
9.5 Threat Management Gateway 2010 80
9.6 Exchange Server 2010 80
9.7 Office 80
9.8 Windows Client 80
9.9 Skola 80

10 Appendix 1: Samarbete mellan kommuner 81
10.1 Infrastrukturdesign i ett kommunsamarbete 81
10.1.1 Active Directory-design 81
10.1.2 Federation 81
11 Appendix 2 - Namnstandard 82
11.1 OU 82
11.2 GPO 82
11.3 Grupper 82
11.4 Användarkonton 83
11.5 IT-Administrativa konton, interna 83
11.6 IT-Administrativa konton, externa 83
11.7 Elevkonton 84
11.8 Konsultkonton 84
11.9 Servicekonton 84
11.10 AD-Sitenamn 85
11.11 Location 85
11.12 Root CA 85
11.13 Utgivade CA 85
11.14 Certifikatmallar/PKI 86
11.15 Skrivarnamn 86
11.16 Skrivarkönamn 86
11.17 DHCP-scopenamn 87
11.18 Klientnamn 87
11.19 Servernamn 87
11.20 WLAN-accesspunkt 87
11.21 LAN-nätverksutrustning 88
12 Appendix 3: Offentlig sektor och säker e-post 89
12.1 Sammanfattning 89
12.2 Inledning 89
12.3 Uppfylla regelkrav – Microsoft Exchange Server 2007 90
12.4 Nya funktioner för regelefterlevnad inom Exchange Server 2007 90
12.5 Tänkbara scenarier 93
12.5.1 E-postarkivering och sökning 93
12.5.2 Säker leverans 94
12.5.3 Kontroll av policys 94
12.5.4 Microsoft Exchange Hosted Services 94
12.6 Välja rätt lösning för regelefterlevnad 96
13 Appendix 4: FirstClass-migrering 97

13.1 Sammanfattning 97
13.2 Strategier för att migrera 97
13.3 Mailbox-migrering med Exchange 2003 Migration Wizard 97
13.3.1 Inledning 97
13.4 Mailbox migrering utan att använda sig av Mailbox migreringsverktyg 103
13.4.1 Mailbox Migrering 103
13.4.2 Migrering av övrig Brevlådedata 105
13.4.3 Migrering av Konferensdata 108

1 Versionskommentarer

Microsofts kommundesign är ett ”levande” dokument, vilket innebär att kunder och partners har möjlighet att lämna synpunkter och önskemål på innehållet som sedan kan leda till att dokumentet förändras med tiden. Målet är att kommundesignen utvecklas i en riktning som gagnar både Sveriges kommuner och partners och de föreslagna förändringarna och tilläggen kommer att publiceras i senare versioner.

Kommentarer och synpunkter kan skickas till: mskd@microsoft.com

1.1 Författare 4.0

Magnus Jungåker, magnusj@microsoft.com
Magnus Holmér, magnus.holmer@microsoft.com
Anders Bjurström, anders.bjurstrom@microsoft.com

1.2 Medförfattare 4.0

Jesper Ståhle, Bradata
Magnus Göransson, Bradata
Fredrik Pålerud, Bradata
Anders Wallgård, Addition IT
Magnus Haglund, Kerfi
Patrick Aune, Kerfi
Berit Pehrsson, Microsoft
Anders Björling, Microsoft
Christer Olsson, Microsoft
Henrik Byström, Microsoft
Niclas Engström, Microsoft

2 Kort sammanfattning

MSKD version 4.0 är den senaste versionen av en referensdesign som beskriver en Microsoft-infrastruktur optimerad för en svensk kommun. Utvecklingen av MSKD började 2004 som ett samarbete mellan Microsoft Sverige och olika svenska kommuner.

2.1 Infrastruktur

MSKD är en lösning som är en del av ett större ramverk som kallas ”Citizen Service Platform, CSP”. MSKD omfattar och fokuserar på infrastrukturen och motsvarar det understa lagret av CSP:s fyra lager.

Version 4.0 lyfter MSKD från den förra gyllene generationens infrastrukturprodukter Windows XP och Windows Server 2003 (årsmodell 2001/2003) till nästa gyllene generation Windows 7 och Windows Server 2008 R2 (årsmodell 2010).

2.2 Kärnvärden

De bestående kärnvärdena i Microsoft Kommundesign (MSKD) har alltid varit följande:

1. En **logisk säkerhetsmodell** istället för en fysisk. Användarautentisering är en viktigare säkerhetsmekanism än nätverksåtkomst.
2. **Konsolidering**. Vi behöver inte längre dubblerade infrastrukturer för administration och skola.
3. En **standardisering** på så få produkter, kompetenser och leverantörer som möjligt.

2.3 Vinster

En av huvudvinsterna med MSKD är att konsolidera (eller reducera) antalet produkter, kompetenser och leverantörer. Största ekonomiska vinsten med denna konsolidering ligger inte nödvändigtvis i inköp av hård- och mjukvara, utan vanligtvis i minskad åtgång av resurser för att utvärdera, designa, implementera, drifta och inte minst integrera de utvalda produkter och lösningarna.

En standardiserad och konsoliderad lösning blir naturligtvis mindre komplex. Mindre komplexitet innebär både högre säkerhet (attackytan minskar) och högre flexibilitet (lättare att genomföra förändringar och nya lösningar).

En modern plattform som MSKD 4.0 möjliggör också säkra lösningar enligt nya arkitekturer, såsom mobilitet och distansarbete, tjänsteorienterad arkitektur (SOA) och inte minst ”Software + Services” där en del lösningar levereras med egen infrastruktur medan andra kan levereras som molntjänster.

Infrastrukturen blir på så vis en möjliggörare för de e-tjänster som medborgarna efterfrågar.

Ytterligare ett av de grundläggande målen med MSKD är att ge kommuner goda förutsättningar att ta större ansvar för miljöförbättrande åtgärder. Såväl kommuner som samhället i stort har krav på sig att ständigt förbättra miljöarbetet, och MSKD är genom konsolidering, virtualisering, ny strömsparande teknik och möjliggörare för minskat resande en naturlig del i detta.

2.4 Utmaningar

Största utmaningen med de flesta infrastrukturprojekt är att inte bara lägga till något nytt utan att också ta bort något gammalt. Det är viktigt att driva MSKD-projekt strukturerat där man inventerar

existerande lösningar och behov för att kunna ersätta dem smärtfritt och effektivt. Införandet blir nästan alltid i form av ett migreringsprojekt. Möjligen kan man på skolsidan i vissa fall införa nya lösningar utan hänsyn till de tidigare.

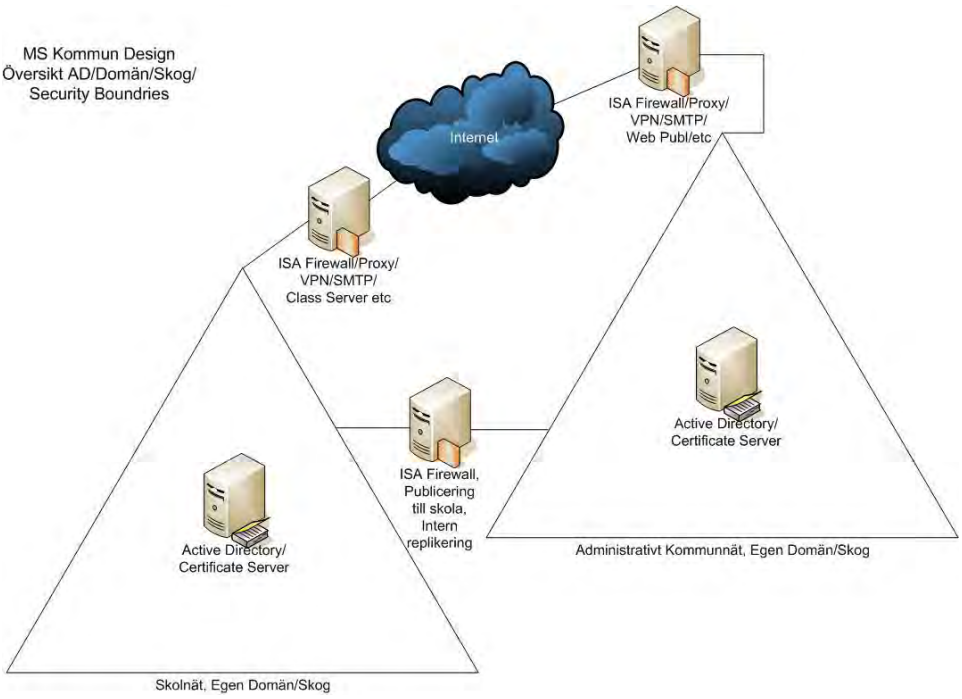
3 Historik

Microsoft Kommundesign, ”MSKD” har från början (och därefter löpande) utvecklats som en lösning på de unika behov som en svensk kommun har på sin IT-lösning. Det förhärskande designmönstret för svenska kommuner vid den här tiden byggde på två helt separerade nätverk, ett för ”administrationen” och ett för ”skolan”. Detta designmönster löste ett säkerhetsproblem, men skapade samtidigt ett (med tiden allt tydligare) åtkomstproblem. Det innebar också att man behövde dubbla infrastrukturer, en för varje nätverk.

3.1 MSKD 1.0, juni 2004

Under år 2004 började Microsoft Sverige att utveckla Microsoft Kommundesign, ”MSKD”. Målet med den första versionen av MSKD var att möjliggöra för skol- och administrativ- personal som var anslutna till ”skolnätet” att kunna komma åt lösningar och tjänster på ”adminnätet”. Lösningen på problemet blev att placera Microsoft ISA Server mellan de två nätverken och bara släppa igenom de användare som (efter autentisering) hade behörighet att komma tjänster på ”adminnätet”.

Ett genomgående tema i MSKD 1.0 var även säkerhet på djupet eller ”Defense In Depth”. Detta innebär att man använder flera lager av säkerhetslösningar och kan på så vis höja förtroendet för lösningen som helhet.

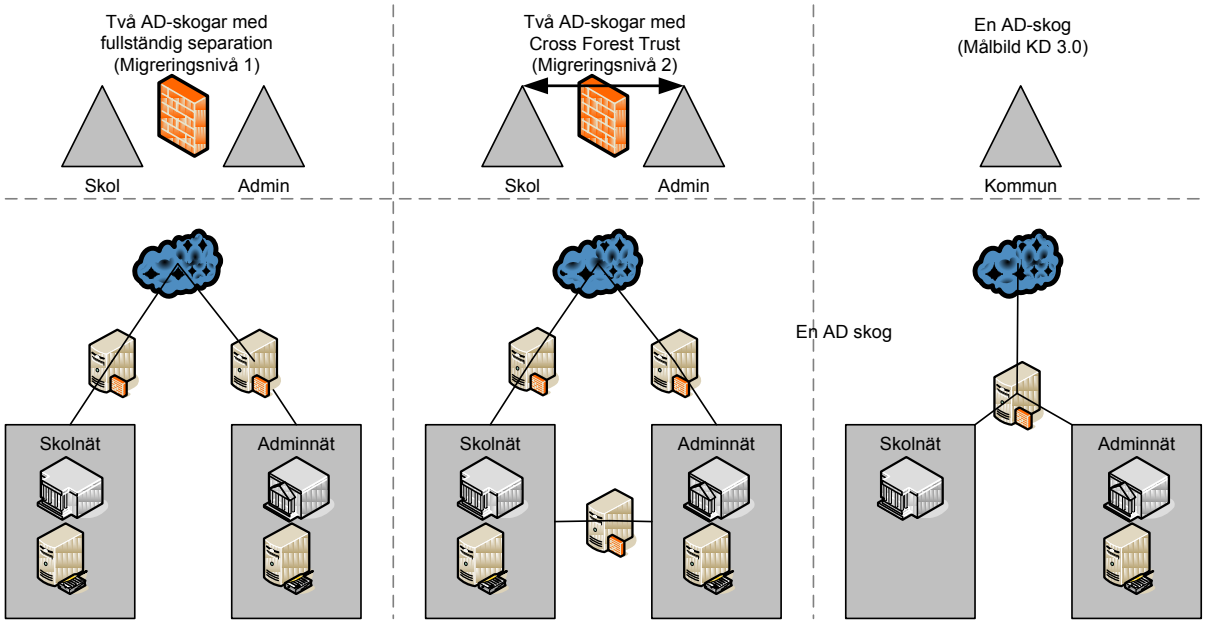


3.2 MSKD 2.0, mars 2005

När åtkomstproblemet mellan nätverken var hanterat med hjälp av MSKD 1.0 flyttades fokus till katalogtjänsten. Eftersom de dubbla infrastrukturerna innebar separata katalogtjänster för ”skola” och ”administration” blev nästa problem; dubbla användarkonton för de användare som hade behov att komma åt tjänster på båda nätverken. Dubbla användarkonton innebär att användarna utsätts för förvirrande dubbel administration av lösenordsuppdateringar och i förlängningen sänks säkerhets-nivån på lösningen som helhet.

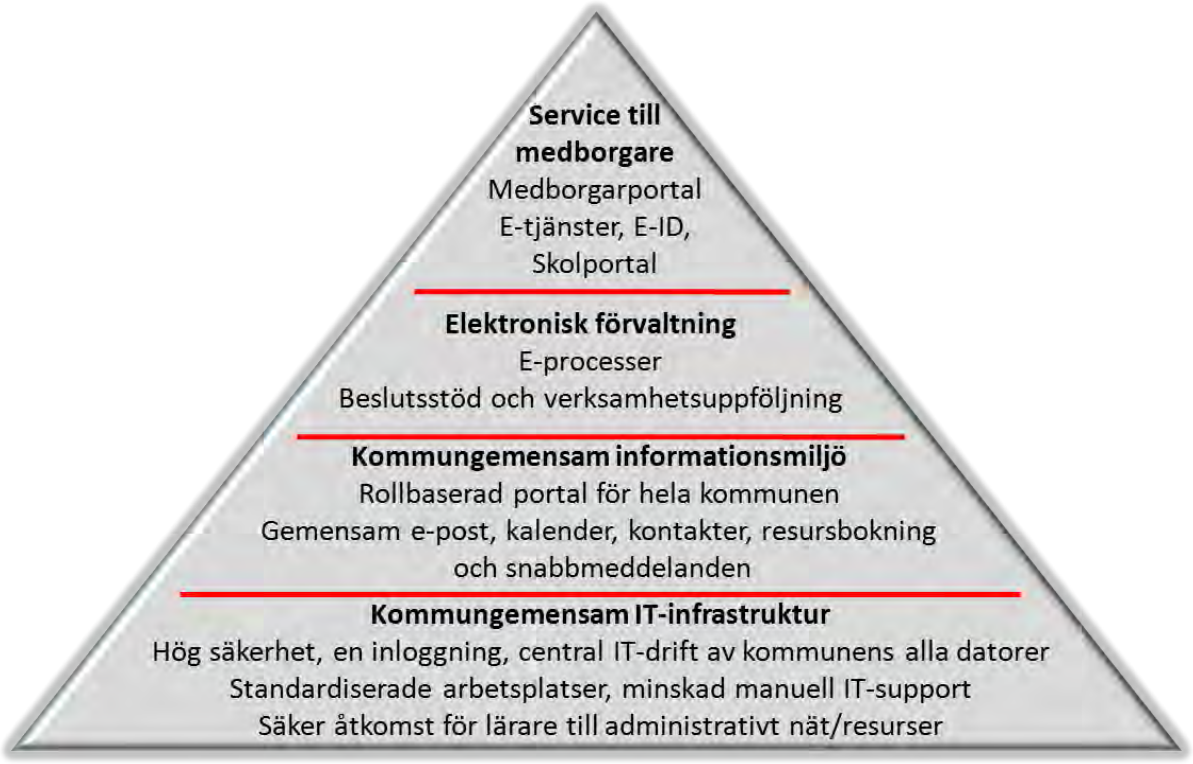
Första lösningsförslaget (och egentligen en del av MSKD 1.0) var att etablera en ”trust” mellan de två katalogtjänsterna. Trusten möjliggör att användarna endast behöver ett konto för att komma åt tjänster från båda nätverken. En djupare analys av lösningen avslöjar dock att den är onödigt dyr och komplex. Samma säkerhetsnivå kan nämligen uppnås om man konsoliderar de två katalogtjänsterna till en. Det går på så vis åt hälften så många servrar och lösningen blir mycket enklare att bygga och administrera.

Den rekommenderade AD-designen blev därför att bygga ett gemensamt AD för ”administration” och ”skola”. Vi beskrev dock både separerade och trust-sammankopplade AD-designer som alternativa lösningar.



3.3 MSKD 3.0, juni 2007

I version 3.0 uppdaterades MSKD med de senaste versionerna av Microsoft-programvaror, men framförallt utvecklades designen på Information Worker ”IW”-sidan. Mycket fokus lades på portaler och samarbetslösningar. Man beskrev också en komplett IT-hierarki (se pyramiden nedan). E-förvaltning och e-tjänster lades ovanpå infrastrukturen för att visa hur plattformen kan utnyttjas fullt ut.



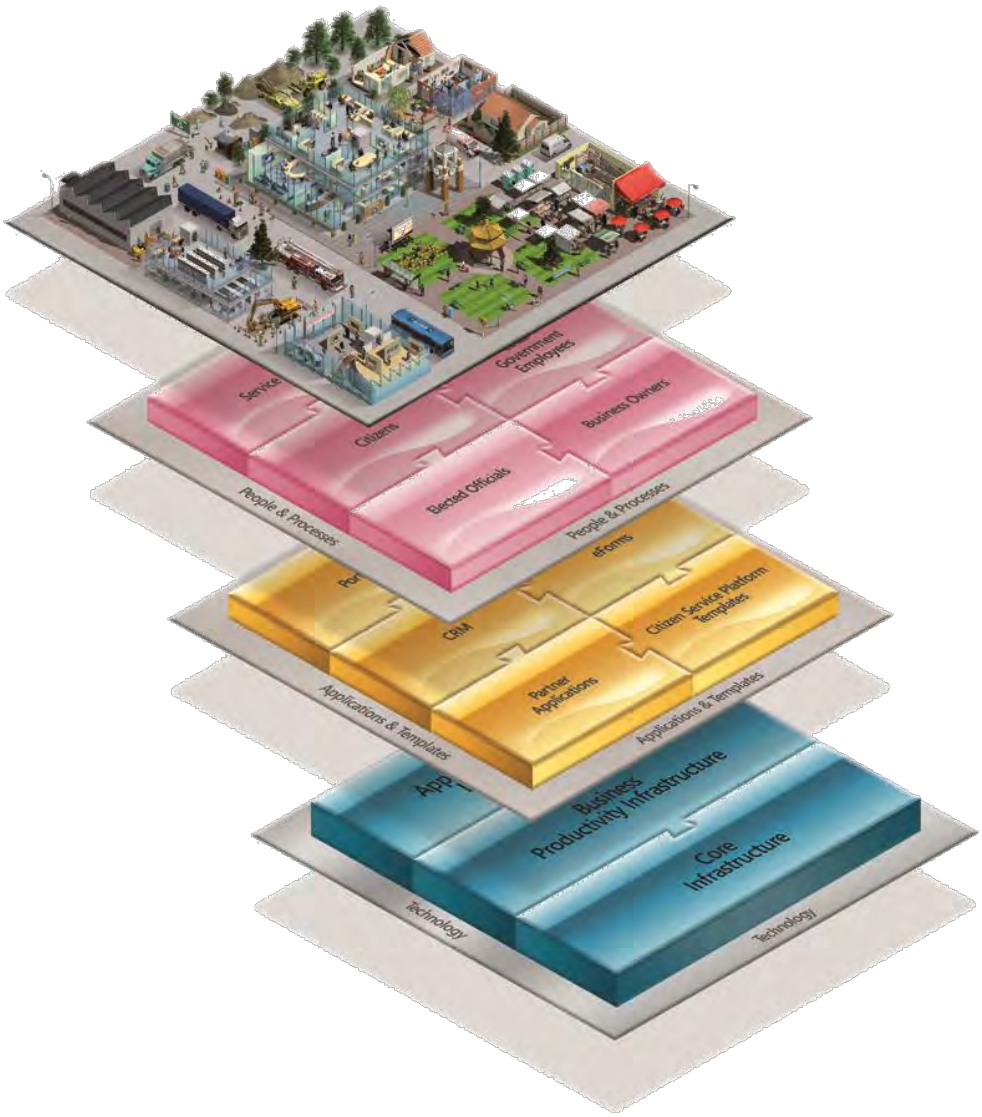
3.4 Sammanfattning tidigare MSKD versioner

MSKD version	Tema	Release	Windows Server	Windows Client	Nätverk	AD
1.0	Säkerhet på djupet	2004-06	2003	XP	Fysisk sep ISA 2004	2 AD
2.0	Integration skol och adminnät	2005-03	2003	XP	Fysisk sep ISA 2004	Rek 1 AD
3.0	Portaler E-förvaltning E-tjänster	2007-06	2003 2003 R2	XP Vista	Fysisk sep/ SDI ISA 2006	Stark rek 1 AD

3.5 Citizen Service Platform

Under 2008 introducerade Microsoft centralt ”Citizen Service Platform” (CSP), som är ett ramverk för offentlig verksamhet och hur denna verksamhet stöds av en IT-plattform. Detta ramverk tar över den del av MSKD 3.0 som handlade de övre lagren i IT-pyramiden.

CSP består av en fyrskiktsmodell där det fjärde skiktet beskriver den tekniska plattform på vilken man bygger verksamhetslösningar och e-tjänster mm och där kan vi nu placera in MSKD 4.0 som en infrastrukturlösning.



4 Kärnvärden MSKD

4.1 Kärnvärden

De bestående kärnvärdena i Microsoft Kommundesign (MSKD) har alltid varit följande:

1. En **logisk säkerhetsmodell** som ersätter den tidigare förhärskande fysiska säkerhetsmodellen (med en uppdelning i skolnät och adminnät). Behovet har blivit mer och mer uppenbart när kommuner efterfrågar möjlighet för administrativ personal som är anslutna till ett skolnät att komma åt lösningar som bara finns tillgängliga på ett adminnät. Detta sammanfaller även med andra megatrender inom IT såsom: bredband, mobilitet, distansarbete och individbaserad åtkomst. Man skall dock inte se detta skifte av säkerhetsmodell som riskfyllt eller som att avsägande av skyddsmekanismer. Vi kombinerar nämligen den logiska säkerhetsmodellen med ”säkerhet på djupet”, där vi mycket väl kan använda fysisk säkerhet som ett extra säkerhetslager. Den logiska säkerhetsmodellen är dock den mest grundläggande. Man kan fråga sig, vad kommer först, användarautentisering eller nätverksåtkomst. I den fysiska säkerhetsmodellen behövs nätverksåtkomst innan man kan göra användarautentisering. I den logiska säkerhetsmodellen behövs användarautentisering innan man får nätverksåtkomst.
   Jämför med telefoni; förr med fast telefoni var det avgörande vilket telefonjack man kopplade in sig i, idag med mobiltelefoni är det din identitet på telefonens sim-kort som avgör. Likaledes skall det idag inte spela någon större roll vilket nätverksjack eller trådlöst nät du råkar ansluta till, utan din användarautentisering borde vara huvudsakligen avgörande för vilken behörighet du får. Säkerhetslösningarna måste stödja denna logiska säkerhetsmodell.
2. När man väl har börjat bygga en infrastruktur baserat på en logisk säkerhetsmodell blir en **konsolidering** uppenbar och självklar. Vi behöver inte längre en dubblerad infrastruktur bara för att vi har fysiskt separerade nätverk som säkerhetsmodell. Konsolideringsmöjligheterna är dock större än en halvering av infrastrukturen eftersom vi inte längre behöver integrationslösningar och besvärlig undantagshantering. I vissa fall går man ännu längre och slår ihop flera kommuners infrastruktur till en gemensam.
3. En **standardisering** av infrastrukturlösningar och klientkomponenter medger effektiv IT-drift. Drift, support samt egen integration och utveckling är kostsamt. En insikt att standardisering på Microsofts infrastruktur och klientplattform ger inte bara kostnadsfördelar utan även produktivitetsvinster och möjlighet till verksamhetsutveckling och kvalitetssäkring är naturligtvis också central för MSKD.

4.2 Exempel på vinster med konsolidering och standardisering

För att uppnå de potentiella vinsterna med konsolidering och standardisering bör man inte välja produkter och lösningar efter ett ”Best of Breed”-tänkande. Då kommer man i förlängningen ha ett stort antal produkter och leverantörer, men själv få ta ansvaret för integration och helhetsfunktion. Kan man standardisera och konsolidera antalet produkter, tekniker och leverantörer blir IT-verksamheten effektivare och kan ägna mer tid och resurser åt utveckling och mindre åt drift och underhåll.

Exempel på lösningar som Microsoft kan leverera inom MSKD:

- Antivirus
- Spamhantering (lokalt och online)
- Brandvägg (klient, server och nätverk)
- VPN
- NAP (hygienkontroll för nätverksåtkomst)
- Trådlöst
- Radius
- DNS
- PKI
- Klientutrullning/imagehantering
- Övervakning
- Virtualisering
- Webb
- Intranät
- Katalogsynkronisering
- Single Sign On

4.3 Miljöanpassning – Grön IT

Ett av de grundläggande målen med MSKD är att ge kommuner goda förutsättningar att genom en modern infrastruktur ta större ansvar för miljöförbättrande åtgärder. Såväl kommuner som samhället i stort har krav på sig att ständigt förbättra miljöarbetet, och MSKD är en naturlig del i detta.

4.3.1 Konsolidering och virtualisering

Konsolidering och virtualisering ger en högre nyttjandegrad av kraften. Färre strömförbrukande enheter behövs eftersom vi kan använda de servrar som redan finns på ett effektivare sätt. Färre värmekällor minskar dessutom behovet av nedkylning i t.ex. en datahall, vilket i sin tur också leder till lägre energiförbrukning.

4.3.2 Modern teknik drar mindre ström

Både Windows 7 och Windows Server 2008 R2 har väl utvecklad teknik för att dra mindre ström, både under användning och i vila. Som exempel kan nämnas att Windows Server 2008 R2 har inbyggd funktionalitet som stänger av en eller flera processorer i en server när de inte används för att spara ström (t.ex. nattetid). Windows 7 har en liknande funktionalitet som tar ned all hårdvara till lägsta möjliga aktivitet när du går iväg från datorn en kort stund. Windows 7 sänker även ljusstyrkan på skärmen efter en kort stunds inaktivitet, och in- och utgångar såsom nätverksuttag stängs av ifall ingen sladd finns inkopplad.

4.3.3 Minskat resande minskar utsläppen

Oavsett hur långt man går i sin implementation av MSKD, går det alldeles utmärkt att spara in resurser redan från start. Windows 7 och Windows Server 2008 R2 DirectAccess ger användaren möjlighet att på ett helt nytt sätt arbeta på distans och slippa ta sig till olika platser rent fysiskt. För användaren innebär det ingen skillnad alls att öppna sin PC hemma eller på kontoret; samma upplevelse följer med oavsett plats utan krångliga VPN-förbindelser som avbryts gång på gång.

Med hjälp av Microsofts molntjänster, BPOS, som ingår som en del av MSKD, kan man snabbt och enkelt komma igång med videokonferenser med applikationsdelning efter behov. Medarbetarna slipper resa till möten när eller fjärran, och bidrar därmed till minskade utsläpp.

Office Communications Server 2007 R2, som ingår som en del av en utökad infrastrukturell lösning, erbjuder utökade möjligheter för samlad kommunikation för den som har lite större behov och vill ha lösningen lokalt installerad. Snabbmeddelanden, videokonferenser, applikationsdelning och telefoni ger utökade möjligheter till god kommunikation på ett miljömässigt sätt.

5 Vision och omfattning

Motiveringen för att utveckla en ny version av MSKD är att identifiera dels hur långt vi idag kan komma med ovanstående kärnvärden och dels att peka på de möjligheter som uppstår i nya och kommande produkter och lösningar.

Det finns också anledning att förtydliga MSKD genom att trycka just på dessa kärnvärden och identifiera de aktuella ”best practice” som bäst beskriver MSKD. Tidigare har MSKD varit relativt öppen för tolkning. Kan vi förtydliga de centrala principerna och tydligare formulera kraven för uppfyllande av en viss version av MSKD borde begreppet bli än mer relevant.

5.1 Förutsättningar inför MSKD 4.0

5.1.1 Avgränsa mot CSP:s övre lager

Med tillkomsten av ett centralt definierat ramverk (CSP) som fokuserar på just hur kommuner och myndigheter skall tillhandahålla e-förvaltning och e-tjänster blir det tydligt att MSKD är en infrastrukturlösning inom ramen för CSP lager 4: Teknik.

MSKD 4.0 kommer därför att fokusera på infrastruktur, men överlåta e-tjänster och e-förvaltning till andra CSP-lösningar.

5.1.2 Stort intresse

Så gott som alla svenska kommuner känner till MSKD och av de som bygger sin infrastruktur på Microsoft-teknologi hävdar de flesta kommuner att de bygger på MSKD.

Även bland Microsoft partners är MSKD populärt och att stå på listan som MSKD-partner är attraktivt.

5.1.3 Myterna i MSKD

MSKD har i sin framgångsrika spridning ibland blivit missförstått. För att ge några exempel på dessa missförstånd:

5.1.3.1 MSKD 1.0: ISA Server kan autentisera all trafik

När vi i MSKD 1.0 föreslog att ISA Server skulle autentisera och kontrollera vilka användare som skulle få åtkomst från skolnätet till adminnätet, var detta huvudsakligen en lösning för webbaserade tjänster som skulle publiceras. I de fall andra protokoll behövde göras tillgängliga fanns det en möjlighet att åstadkomma detta med VPN.

Det förekommer dock regelbundet att man missförstår ISA Servers roll och tror att den kan autentisera all trafik som den routar. *Faktum är* att ISA Server som reverse proxy endast kan autentisera web-protokoll och som forward proxy kan autentisera web-protokoll samt Windows sockets-applikationer.

5.1.3.2 MSKD 2.0: Ett eller två AD är två likvärdiga modeller

När vi i MSKD 2.0 beskrev nackdelarna med att ha olika AD för skola och admin och fördelarna med att ha ett gemensamt AD för hela kommunens verksamhet, beskrev vi dessa scenarion som tre olika alternativ. Detta har gjort att många har uppfattat dessa alternativ som likvärdiga. *Faktum är* att vi sedan MSKD 2.0 har argumenterat fördelarna med att konsolidera sin infrastruktur och bara ha ett AD.

5.1.3.3 MSKD 3.0: E-tjänster

Med informationspyramiden i MSKD 3.0 ställdes i vissa fall orimligt höga förväntningar på hur uppnåeliga de kommunala e-tjänsterna egentligen var. Pyramiden fyllde förvisso en pedagogisk funktion att visa på arkitekturens och infrastrukturens betydelse för att kunna leverera sagda tjänster. Vi (människor) tenderar att överskatta vad vi kan åstadkomma på ett år men samtidigt underskatta vad vi kan åstadkomma på 5-10 år. *Faktum är* att vi nu är närmare en komplett teknikplattform som kommer att både möjliggöra och förverkliga e-tjänster än någonsin.

5.1.3.4 MSKD 4.0: 802.1x och SDI kompletterar varandra

För att gå händelserna i förväg, kan vi även beskriva ett sätt som MSKD 4.0 riskerar att bli missuppfattat på. Med SDI kan vi centralt beskriva de brandväggsregler som skall gälla i Windows Firewall på alla klienter och servrar. Eftersom vi inte behöver definiera några skol- och adminnät på klientsidan utan använder den påloggade användaren för att styra åtkomsten till olika servrar blir den fysiska nätverksdesignen enkel.

Nätverksgruppen som har för vana att hantera nätverkssäkerhet kommer att vilja lösa samma problem (som vi löser med SDI) med hjälp av 802.1x. Denna teknik kommer dock inte att ge oss samma säkerhetsnivå och kommer dessutom att skapa en mer komplex nätverksdesign. Det värsta scenariot kommer att bli när man inför både SDI och 802.1x och försöker lösa samma problem två gånger. Man kommer då att behöva hantera nätverkssäkerhet både i Windows med SDI och i nätverksinfrastrukturen med interna brandväggar. Följden kommer att bli ett komplext och svårhanterat nätverk som mer hindrar än möjliggör nya lösningar. *Faktum är* att SDI är premiumlösningen för nätverkssäkerhet. Dessutom kräver den ingen specialmaskinvara utan fungerar på vanliga nätverksswitchar och PC:s.

5.2 Primära teman version 4.0

MSKD beskriver en modern infrastruktur baserat på Microsoft-teknologi för en svensk kommun. I detta perspektiv är samtliga Microsofts infrastrukturprodukter intressanta och relevanta. Men när vi tittar på vad som är specifikt och centralt för MSKD version 4.0 ser vi några teknologier som mer framstående än andra.

De centrala temana i MSKD 4.0 är:

- ”Server and Domain Isolation”
- ”Windows 7 och Windows Server 2008 R2”
- ”Cloud Computing Single Sign-On och ADFS 2.0”.

5.2.1 Server and Domain Isolation

Den logiska säkerhetsmodellen kan från och med Windows Vista enkelt implementeras och radikalt höja säkerhetsnivån utan att skapa icke önskade åtkomstproblem. Tekniken har visserligen funnits tillgänglig från och med Windows 2000, men enkelheten och användbarheten har inte materialiserats fullt ut förrän med Windows Vista. Då fick vi också möjlighet att styra varje klients nätverkssäkerhet baserat på den påloggade användaren och inte bara på maskinidentiteten.

5.2.2 Windows 7 och Windows Server 2008 R2

Även om redan Windows Vista och Windows Server 2008 ger många av de möjligheter som vi efterfrågar så är det inte förrän Windows 7 som vi ser en reell möjlighet för flertalet kommuner att överge Windows XP och äldre Windows-versioner för att istället helt standardisera på en modern Windows-version. Windows 7 medger tack vare sin optimering för netbooks och hårdvara med mer

begränsade resurser en genomgripande standardisering på en modern Windows-version. När vi väl standardiserar på en version kan vi börja utnyttja de nya funktioner och säkerhetsnivåer som denna version ger oss.

Tillsammans med Windows Server 2008 R2 får vi dessutom tillgång till funktioner som DirectAccess, AppLocker m fl.

5.2.2.1 Virtualisering

För att ytterligare driva konsolideringen samt att ta ansvar för sin energikonsumtion så använder vi Hyper-V för servervirtualisering. Servervirtualisering är också centralt för uppnå ”Dynamisk IT”-visionen.

Klientvirtualiseringstekniken i MDOP (App-V och MED-V) kan radikalt effektivisera applikations-paketering och förbättra applikationskompatibiliteten och därför möjliggöra en plattforms-uppgradering. På skolsidan blir det allt vanligare med egna elevdatorer. För att ändå ha en chans att kunna installera applikationer på en inte fullt kontrollerad elevdator är klientvirtualisering med App-V och MED-V goda möjliggörare.

5.2.3 Cloud Computing Single Sign-On och ADFS 2.0

Med tidigare MSKD-versioner har vi konsoliderat till *ett* Active Directory (AD) per kommun. Nästa steg i konsolideringen av identitetshantering är federation. Med ADFS 2.0 på plats som en del av MSKD infrastruktur får kommunen möjlighet att köpa lösningar och tjänster i molnet utan att behöva utsätta användarna för den belastning som hanterandet av multipla identiteter innebär. Single Sign-On blir med denna teknik och lösning en självklar rättighet och ett berättigat krav som alla kan ställa på så väl programvara som tjänster (software + services).

5.3 Sekundära teman

MSKD omfattar alla Microsofts relevanta infrastrukturteknologier, även sådana som inte är uppräknade som primära teman ovan. För att nämna några exempel:

- Forefront
- System Center
- Exchange
- OCS

5.4 MSKD Versioner

Lägger vi till version 4.0 i listan med MSKD versioner får vi följande sammanställning:

MSKD version	Tema	Release	Windows Server	Windows Client	Nätverk	AD
1.0	Säkerhet på djupet	2004-06	2003	XP	Fysisk sep ISA 2004	2 AD
2.0	Integration skol och adminnät	2005-03	2003	XP	Fysisk sep ISA 2004	Rek 1 AD
3.0	Portaler E-förvaltning E-tjänster	2007-06	2003 2003 R2	XP Vista	Fysisk sep/ SDI ISA 2006	Stark rek 1 AD

4.0	SDI Windows 7 Cloud Computing	2009-11	2008 R2	Windows 7	SDI TMG, UAG	1 AD + federation

5.5 MSKD 4.0 Nivåer

För att en kommun skall kunna hävda att den uppfyller kraven för MSKD version 4.0 Basic krävs att den följer de centrala designprinciperna: Ett AD och ”Server and Domain Isolation (SDI)” samt bygger på Windows 7-generation av Windows och infrastrukturprodukter.

Man kan dock välja hur långt man vill gå med Microsoft-lösningen. Antingen bygger man på Professional Desktop (Core CAL Suite) eller på Enterprise Desktop (Enterprise CAL Suite). Detta blir då ”MSKD 4.0 Core” och ”MSKD 4.0 Enterprise”. Har man inte rullat ut alla Core eller Enterprise-komponenterna kan man ändå uppfylla kraven för en underliggande nivå.

Nivå	Infrastruktur	Klient
Basic	Windows 2008 R2 Ett AD SDI TMG 2010	Hanterad standardklient Windows 7 MDT 2010 Lite Touch
Core	Exchange 2010 SharePoint 2007 SCCM 2007 SP2	MDT 2010 Zero Touch Office 2007 Professional Plus
Enterprise	OCS Forefront Client Security Forefront Server Security UAG	Forefront Client Security

5.6 Avgränsning

Det har nu uppstått ett behov att avgränsa MSKD till att beskriva infrastrukturdesign. I senaste versionen av MSKD beskrevs hela stacken upp till och inklusive medborgarportaler och e-tjänster. Med uppkomsten av Citizen Service Platform (CSP) kan vi överlämna de överliggande lösningslagren till andra CSP-lösningar.

- E-tjänster
- E-förvaltning
- Produktivitetsverktyg
- Office
- SharePoint
- CRM

6 Införande - Projektmetodik

Vid förändring av infrastrukturen inom en kommun bör en strukturerad modell användas för själva genomförandet, någon form av projektmodell eller metodik bör alltså användas. Vilken av modellerna som används är av mindre vikt utan värdet ligger i *att* man använder ett strukturerat tillvägagångssätt. Det finns idag ett stort antal etablerade modeller och många kommuner och organisationer har skapat en egen eller använder en befintlig. Här redogör vi för ett antal olika modeller.

6.1 Projektstyrningsmodell

En projektstyrningsmodell är en modell av det arbete som skall föregå inom ett projekt, inriktat mot konkreta lösningar i syfte att bryta ner, strukturera, förutsäga och tidsbestämma skeendet i ett projekt. De första projektstyrningsmodellerna utvecklades av USA:s Department of Defense under kalla kriget, i synnerhet efter sputnikkrisen. Målet med modellerna var hög styrbarhet, kontroll, planering och utvärdering av stora försvarsprojekt.

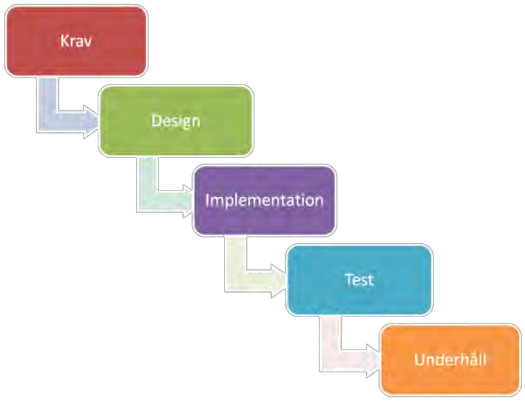
6.1.1 Kända projektstyrningsmodeller

- PRINCE2 Den internationellt sett största projektstyrningsmodellen.
- PERT Är en metod för att göra tidsbedömningar i projekt.
- CPM Critical Path Method är en metod för att prioritera åtgärder och styra upp projektaktiviteter.
- WBS Work Breakdown Structure är ett sätt att bryta ned ett projekt i leveranspaket.
- RUP Rational Unified Process är en systemutvecklingsmodell för design och implementering av IT-system. Utvecklingsmodellen ägs numera av IBM och utvecklas av IBM Rational Software.
- PROPS är en projektstyrningsmodell som utvecklats av Ericsson. Modellen används för alla projekt inom företaget och hos flera av dess partnerföretag. PROPS används också av många företag i andra branscher, liksom av flera svenska myndigheter. Modellen ägs och förvaltas nu av konsultföretaget Semcon.
- PPS Praktisk Projektstyrning är en projektstyrningsmodell som används främst i IT-projekt som är framtagen av TietoEnator.
- Scrum är en agil metod främst använd i programvaruprojekt.

För mer information om dessa exempel se här.

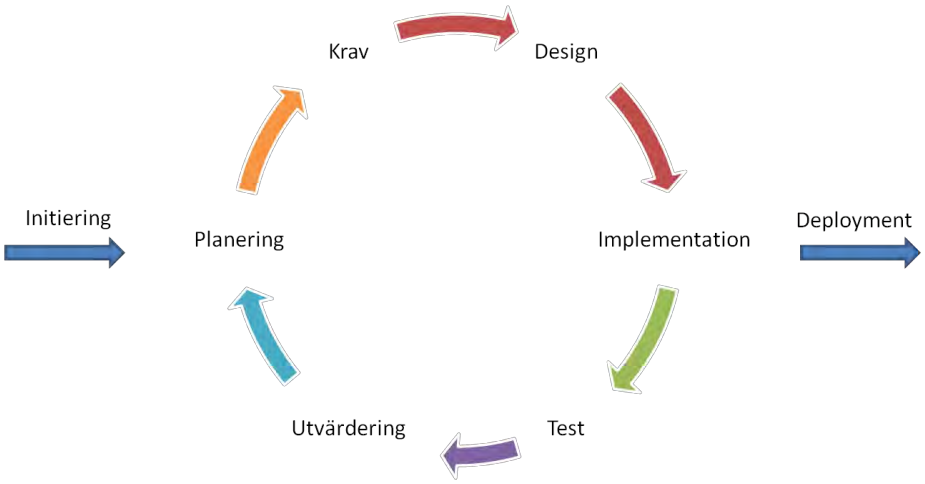
6.2 Vattenfallsmodellen

En traditionell modell är vattenfallsmodellen som är en sekventiell modell där varje steg i processen flödar ner till nästa process. Denna modell lämpar sig väl inom konstruktions- och tillverkningsbranschen där man fullt ut kan avsluta en process. Inom IT området där det många gånger är svårt att med säkerhet säga att en process verkligen är färdig lämpar sig denna inte fullt lika bra utan man bör då använda en mer iterativ modell.



6.3 Iterativ utveckling

En iterativ eller inkrementell modell baseras på en cyklisk utvecklingsmodell som skapats som ett svar på svagheterna med vattenfallsmodellen. Denna modell startas med initial planering och slutar med utrullning/deployment och under det steget pågår en fortsatt cyklisk modell som upprepas. De flesta projektmodeller som nämnts här baseras på någon form av iterativ modell, dvs arbetet fortsätter även efter att en del i processen avslutats.



6.4 Microsoft Solutions Framework

Microsoft Solutions Framework, MSF 4.0 är ett ramverk som beskriver hur programvaruutvecklings-processen kan bedrivas i allmänhet och innehåller även konkreta modeller för hur man praktiskt ska gå till väga, dvs implementera Agile (Agile Software Development) och CMMI (CMMI Process Improvement).

Mer information om MSF finner ni här.

6.5 PROPS

PROPS är en projektstyrningsmodell som utvecklats av Ericsson. Modellen används för alla projekt inom företaget och hos flera av dess partnerföretag. PROPS används också av många företag i andra branscher, liksom av flera svenska myndigheter. Modellen ägs och förvaltas nu av konsultföretaget Semcon.

PROPS delar in projekt i tre olika områden, det styrande (affären), det ledande (projektledningen) samt det utförande (arbetsmodellen). Dessa symboliseras av olika färger, rött är styrande, blått är ledande och gult är liktydigt med arbetsmodellen.

PROPS har sex olika toll-gates. Dessa TGn benämns:

Förstudie

TG0 Start av förstudie

Utredning

TG1 Start av utredningsfas

Genomförande

TG2 Start av genomförandet
TG3 Beslut om fortsatt genomförande
TG4 Beslut om start av överlämning

Avslut

TG5 Beslut om projektnedläggning

6.6 Scrum

Scrum är en metodik för systemutveckling skapad av Jeff Sutherland och Ken Schwaber. Ordet "Scrum" kommer från rugbyn, och är ett moment när bollen sätts i spel. Rugby användes som en liknelse av de japanska managementforskarna Hirotaka Takeuchi och Ikujiro Nonaka för att beskriva en speciell stil av utveckling. I rugbyliknande utveckling samarbetar ett tvärfunktionellt team för att göra klart produkten på samma sätt som ett rugbylag spelar tillsammans för att föra bollen uppför planen. Denna typ av arbetsform kontrasterade Nonaka och Takeuchi med mer stafettliknande processer. I dessa färdigställs arbete i funktionella faser, med tydliga överlämningar mellan grupper när arbetet går från en fas till en annan.

Scrum har tillämpats sedan tidigt 1990-tal och formaliserades 1995. Scrum är ett kraftfullt sätt att fördela arbetsuppgifter i tiden med bibehållet fokus på levererad affärsnytta.

6.7 Kompetensuppbyggnad

När man inför en ny eller uppdaterad plattform inom en organisation är det viktigt att man stöder denna med att ha personal med rätt kompetens som kan förvalta och hantera plattformen. Kunskapen eller kompetensen kan erhållas genom att utbilda personalen inom ett eller flera områden som täcker plattformen. Utbildning kan ske på olika sätt. Olika individer tillgodoser sig utbildning bättre med olika metoder (lärstilar). En del tekniker föredrar att testa tekniken praktiskt i labb, andra föredrar teoretisk inläsning eller muntlig föredragning. Det är dock för organisationen ofta viktigt att belysa och premiera den individuella kompetensuppbyggnaden.

För information om olika utbildningsområden på Microsoft-teknologier se följande länk.

För att verifiera kompetensen kan det också vara klokt att genomföra en certifiering. Dessa certifieringar kan vara rent produkt- eller områdesspecifika som t.ex. för Windows Server eller Exchange eller omfatta ett certifieringsprogram som t ex MCM eller MCITP.

Här hittar du mer information om certifieringsprogram respektive produktcertifieringar.

6.8 Projekt och aktiviteter

Under arbetet med denna version av MSKD har vi diskuterat vilka projekt som är vanliga i samband med en förändring i infrastrukturen. Därför listar vi här ett flertal exempel på några projekt och aktiviteter som man kan behöva genomföra. Det vore dock orimligt att försöka beskriva en generell projektplan eller ”att göra”-lista. Dels varierar förutsättningar och utgångsläge kommun för kommun och dels skulle MSKD-projektet i sig växa och bli ohanterligt stort för de tillgängliga och inblandade resurserna.

6.8.1 Projekt

Följande lista av projekt är vanligt förekommande vid införande och eller migrering till MSKD. Observera att beroenden kan finnas mellan projekten, till exempel vill man antagligen genomföra AD-migrering, klientmigrering och servermigrering innan man genomför ”Domain Isolation” för hela miljön.

- AD-migrering
- Mailmigrering
- Klientmigrering
- Servermigrering
- Skrivarmigrering
- Nätverksmigrering (”Server & Domain Isolation”)
- Övervakning
- Realtidskommunikation
- Samarbetsplattform

6.8.2 Aktiviteter

Under införandet av en ny plattform som genomförs med stöd av projekten ovan kan följande lista utgöra några av de centrala och viktiga aktiviteterna som man bör hantera.

- Koordinering/projektledning
- Inventering applikations-/systemägare
- Design/Namnstandard
- Riskanalys
- Standardisering
- Informationsklassificering
- Kommunikation och information till användare
- Applikationspaketering
- Datamigrering
- Behörighetsstrukturer
- Processrutiner och drift
- Överlämning
- Konsolidering/rensning
- Utrullning

- Avveckling
- Samexistens

7 Drift - Processer och organisation

7.1 Processer

Från att många gånger varit driven av teknik eller hantering av tekniska problemställningar har många IT-organisationer rört sig mot ett mer standardiserat sätt att stödja organisationernas olika verksamheter. I linje med Microsofts IO-modell finns det kring ägande av en IT-miljö ett antal definierade steg att ta sikte på eller mellanlanda vid. Traditionellt har man talat kring att skapa ett ekosystem som inte bara rent tekniskt stödjer de införda lösningarna, man har även skapat strukturerade processer som verkat för att upprätthålla lösningen under hela dess livslängd; processer och rutiner som beskriver vad som skall ske vid en given händelse eller under ett givet händelseförlopp.

En standardiserad lösning är många gånger bra ur ett IT-tekniskt perspektiv. Rutiner kan, om de följs och upprätthålls, ses som en garant för att miljön ser likadan ut imorgon som den gjorde igår. Genom att fortsätta röra sig åt höger i IO-modellen mot en rationaliserad miljö kan IT inte bara upprätthålla funktionerna utan även förbättra kvaliteten kring tjänsterna och samtidigt minska kostnaderna för sina tjänsteleveranser.

Tar man sikte på en dynamisk miljö så blir uppgiften för IT-organisationen, både för sin egen verksamhet och för kundernas, att utforma IT-tjänster för befintliga och framtida behov.
Att "*IT är Verksamheten och Verksamheten är IT*" slås fast i itSMFs handbok kring "Ledning och styrning av IT-tjänster", till vårt stöd har vi ramverk som MOF och ITIL bland andra.

7.1.1 MOF/ITIL och ITSM

Microsoft Operations Framework (MOF), är ett ramverk eller en Best Practice som tillhandahåller riktlinjer för att bedöma vad en IT-organisation behöver och hur en IT-organisation framgångsrikt tillämpar IT Service Management. Verktyget är framtaget och upprätthålls av Microsoft och det har en god förståelse för tekniken som används.

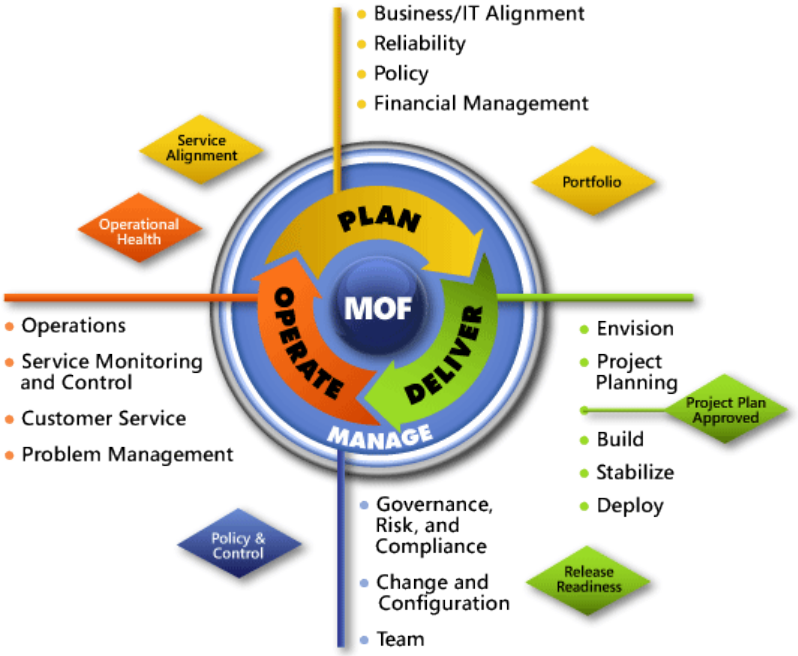
Information Technology Infrastructure Library (ITIL) som har sammanställts av brittiska Office of Government Commerce är även det ett ramverk för att hantera IT-infrastruktur. ITIL innehåller beskrivningar av hur olika IT-relaterade uppgifter kan utföras och sätter formatet för vad som skall göras snarare än att ge svar på hur arbetet skall utföras. ITILs hjärta kan sägas vara IT Service Management.

Information Technology Service Management (ITSM), har som övergripande mål just att hjälpa till att utforma IT-tjänster efter de befintliga och framtida behoven i verksamheten och hos kunderna, att förbättra kvaliteten på de levererade IT-tjänsterna och att minska kostnaderna för tjänsteleveranser. Vanligtvis delas Service Management upp i *Service Support* som fokuserar på den dagliga driften och stödet för IT-tjänsterna och *Service Delivery* som omfattar den långsiktiga planeringen, uppföljningen och förbättringen av IT-tjänsterna.

MOF och ITIL ställs många gånger felaktigt mot varandra som konkurrenter men de är egentligen två begrepp eller funktioner som levererar mot samma sak. De båda ramverken baseras på ett processdrivet arbetssätt som är skalbart för att passa såväl stora som mindre organisationer. Utkomsten av de båda synsätten är att åstadkomma och upprätthålla högkvalitativa och innovativa IT-tjänster utformade efter verksamhetens behov.

MOF och ITIL utgår från en tjänstelivscykel som beskriver IT-tjänstens liv från planering och optimering utifrån affärsverksamhetens behov genom design och leverans av IT-tjänsten till den

löpande driften och supporten av samma tjänst. Tjänstelivscykeln vilar på en bas av IT-styrning, riskhantering, organisation och förändringsledning.



7.1.2 Kommunen och MOF/ITIL

Kommunens IT-avdelning bör ta stöd ur MOF och/eller ITIL för att hjälpa till att sköta och optimera systemdrift samt system- och tjänstetillgänglighet. Ur ett Service Delivery-perspektiv används bland annat termer som Service Level Management, Capacity Management och Availability Management för att reglera leveransnivåer. Som stöd för leveransen används bland annat basprocesser för Incident-, Problem- och Förändrings-hantering.

Genom att anamma ett mer kontrollerat ägande på ett sätt som MOF/ITIL ger kommer man inte bara att kunna ge en säkrare leverans i sina lösningar, IT kan samtidigt bli en mer aktiv del i organisationens utveckling och tillföra funktionalitet utan att riskera ökade drifts- eller ägandekostnader. Som stöd för denna utveckling används en gemensam basinfrastruktur tillsammans med definierade processer för Service Support och Service Delivery. Som exempel kan nämnas OLA och SLAer där både leverantör och konsument av en tjänst kan se och mäta kvalitén på de tjänster som levereras. Inom MSKD kan med fördel verktyg ur System Center-familjen användas; System Center Operations Manager (SCOM), System Center Configuration Manager (SCCM) och System Center Capacity Planner finns redan på marknaden sedan flera år och kommer inom en snar framtid att kompletteras med System Center Service Manager (SCSM). System Center-verktygen är framtagna just för att samla in information om miljön och ge stöd till IT för att effektivt kunna äga den.

För att kunna flytta sin organisation från vänster till höger i IO-modellen nämns ofta de "tre P:na": *Personer*, *Processer* och *Produkter*. Personer med rätt kunskap och förståelse, Processer som är framtagna och avpassade för verksamheten och Produkter i form av verktyg och teknik som stödjer organisationens verksamhet.

Kort kan man säga att om det råder ordning och reda genom förutsägbara processer och tydliga beslutsfattare kan en verksamhet skötas och följas upp snabbt och effektivt. Allt detta gör att ägandekostnaderna kan sänkas samtidigt som tillgänglighet, stabilitet och säkerheten (teknisk så väl som leveranssäkerhet) kan öka. Framför allt ger det att IT kan röra sig från att ha varit en reaktiv och

primärt stödjande eller felavhjälpande resurs till att bli en strategisk resurs, som relativt enkelt kan förändras och byggas ut/om på ett snabbt och kontrollerat vis, för att stödja verksamheten på effektivast möjliga sätt.

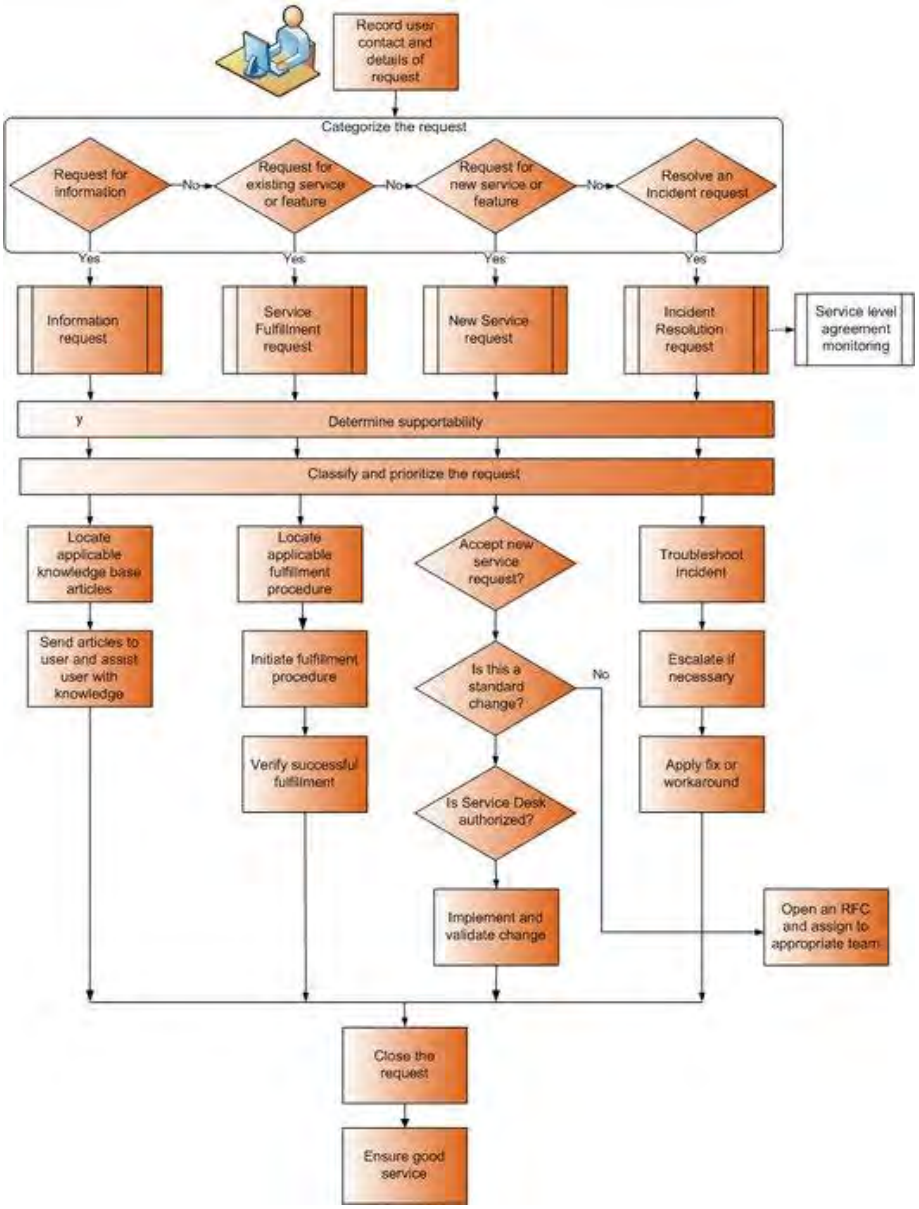
Till detta kan man koppla processer/rutiner samt teknik till standarder som DISC PD0005, ISO/IEC 20000, ISO17799/BS7799 och ISO27001 för att visa hur och på vilket sätt man lever upp till informationssäkerhetsstandarder (Regulatory Compliance), riskidentifiering, riskhantering, styrmodeller m.m. för säkerhetsarbetet inom organisationen. Detta dokument ämnar inte fördjupa sig i dessa standarder men vi rekommenderar vidareläsning inom området.

7.1.3 Exempel på processer och rutiner

7.1.3.1 Incident management

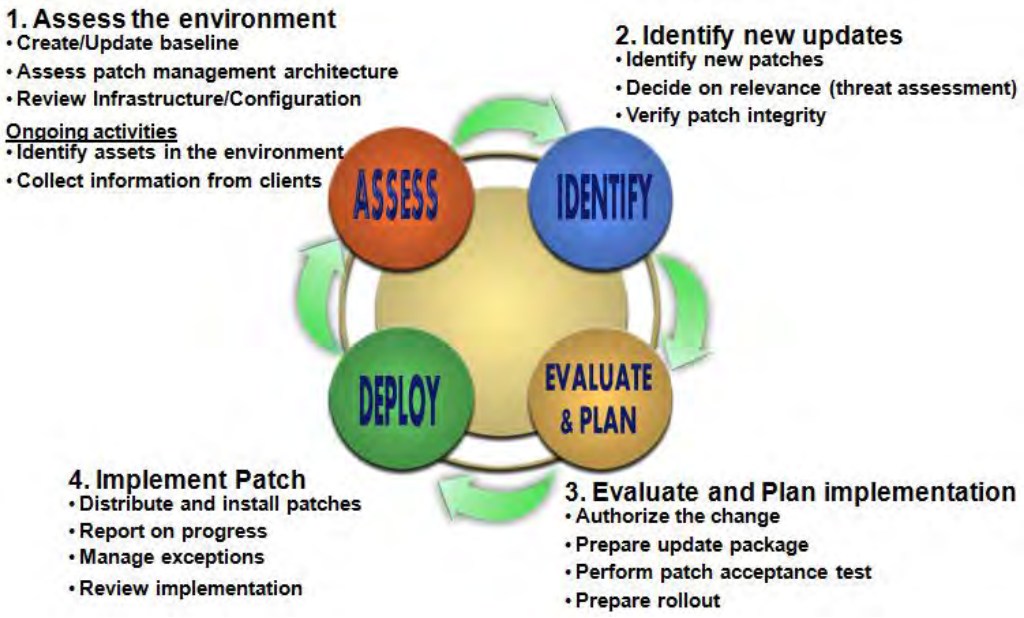
Incident Management är ett bra exempel på hur MOF och ITIL pratar om samma sak och har samma syfte ut mot verksamheten. Incident Management är en process inom de båda ramverken; under MOF är det en del av *Customer Service* och under ITIL och ITSM är det en del av *Service Support.* I båda fallen adresseras användarnas förfrågningar och driftsstörningar av IT tjänster. De övergripande aktiviteterna består av:

- *Registrering och klassificering av inkommande förfrågningar*
- *Felsökning och lösande av incidenter, via workarounds*
- *Säkerställa god kundservice*



7.1.3.2 Update Management

Microsofts Update management (Patch management) process beskriver hela flödet från att de månatliga säkerhetsbulletinerna släpps till att berörda system är patchade och verifierade.



7.2 Organisation

7.2.1 Roller och kompetens inom IT-organisationen

Organisations uppdelning baseras på principer från MOF/ITIL och kan delas in i fyra nivåer:

1. Central Servicedesk (SPOC)
2. Central drift
3. Central systemförvaltning
4. Leverantör och industri

De tre första nivåer återfinns oftast inom organisationen om inte miljön är ”outsourcad”. Nivå fyra återfinns normalt hos leverantör/industrin. Till dessa nivåer och roller knyts administrativa behörigheter i systemet. Notera att nödvändig auditing/loggning måste införas så att man både i realtid kan följa upp användning av behörigheter såväl som för logguppföljning/forensic. Dessa nivåer är ett antal utgångsförslag som kan behöva anpassas för gällande organisation.

Information om Microsoft utbildningar och certifieringar hittar ni här.

CompTIA är en oberoende industristandard för certifieringar för supporttekniker och lämpar sig väl för driftspersonal.

7.2.1.1 Central Service Desk – Nivå 1

Utbilding/Certifiering/Erfarenhet motsvarande:

- CompTIA A+
- MCITP: Enterprise Desktop Administrator 7
- MCITP: Enterprise Support Technician
- Microsoft Office
- MOF/ITIL Awareness - grundförståelse kring ramverken, deras uppbyggnad och syfte

- Kännedom eller kunskap om andra verksamhets- och affärsapplikationer som använd inom organisationen

7.2.1.2 Central drift – Nivå 2

Utbilding/Certifiering/Erfarenhet minst motsvarande:

- CompTIA A+
- MCITP: Enterprise Administrator
- MCITP: Server Administrator
- MCITP: Enterprise Messaging Administrator
- MOF/ITIL Awareness - grundförståelse kring ramverken, deras uppbyggnad och syfte Mellandjup kunskap på andra infrastruktur- samt affärsapplikationer som använd inom organisationen

7.2.1.3 Central systemförvalting- Nivå 3

Utbilding/Certifiering/Erfarenhet minst motsvarande:

- CompTIA A+
- MCSE Windows 7
- MCSE + Security Windows Server 2008 R2
- MOF/ITIL Foundation - fördjupad kunskap kring ramverken, deras uppbyggnad och syfte
- Djup kunskap på andra infrastruktur- samt affärsapplikationer som använd inom organisationen

7.2.1.4 Leverantör och Industri – Nivå 4

Utbilding/Certifiering/Erfarenhet minst motsvarande:

- MCSE + Security Windows Server 2008 R2
- MOF/ITIL Foundation - fördjupad kunskap kring ramverken, deras uppbyggnad och syfte
- Specialistkompetens på sålda produkter (COTS) eller specialanpassade/specialutvecklade produkter för kunden

7.2.2 IT-mognadsgrad

IO-modellen (Infrastructure Optimization) är en modell utvecklad av Microsoft som baseras på Gartners modell IMM (Infrastructure Maturity Model). Modellen går i korthet ut på att hjälpa företag att utvärdera sin infrastruktur för att bli mer dynamisk. MSKD strävar i alla avseenden att höja våra kunders mognad från en enkel nivå där mycket tid och kostnad läggs på att underhålla IT till att istället skapa en effektiv IT miljö med en hög grad av automatisering och hög kostnadseffektivitet.

IO modellen definierar fyra nivåer av systemmognad i ett företag, samt vad som krävs för att ta steget från nuläget till ett snabbare och mer flexibelt IT-system. Modellen är produktoberoende och har som övergripande syfte att förädla kundens IT miljö med hänsyn till befintliga produkter och lösningar.

- *Basic:* Låg grad av automatisering, individuell desktop-anpassning.
- *Standardized:* Styrd infrastruktur med visst mått av automatisering.
- *Rationalized:* Styrd och befäst infrastruktur.
- *Dynamic:* Fullt automatiserad systemövervakning, dynamiskt resursutnyttjande.

IO-modellen delas vidare in i tre olika områden: Core-IO (infrastruktur), BPIO (verksamhetseffektivitet) och APO (applikationsutveckling), för vilka vi identifierar kundens mognad enlig nivåerna ovan.

7.2.2.1 Core-IO

Inom Core-IO eller infrastruktur är fokus på att kartlägga hur moget ett företag är inom följande sex kärnområden:

1. Identitetshantering
2. Standardklienthantering
3. Säkerhet, nätverk och övervakning
4. Backup och återställning
5. Säkerhets process
6. ITL/COBIT process

7.2.2.2 BPIO

Inom BPIO eller verksamhetseffektivitet är fokus på att kartlägga hur moget ett företag är inom följande kärnområden:

1. Samarbete
2. Unified Communications
3. Enterprise Content Management (ECM)
4. Beslutsstöd
5. Enterprise Search

7.2.2.3 APO

Inom APO eller applikationsutveckling är fokus på att kartlägga hur moget ett företag är inom följande kärnområden:

1. Utveckling
2. SOA och affärsprocess (SOA and Business process)
3. Datahantering (Data Management)
4. Användbarhet (User experience)
5. Beslutsstöd (Business Intelligence)

7.2.3 Standardisering

En av de viktigaste principerna för en IT-organisation bör vara att sträva efter standardisering inom plattformen. Detta är ett av de tre kärnvärdena i denna version av MSKD och det gäller även för processer och organisationen.

En standardiserad och konsoliderad lösning blir naturligtvis mindre komplex. Mindre komplexitet innebär både högre säkerhet (attackytan minskar) och högre flexibilitet (lättare att genomföra förändringar och nya lösningar).

7.2.4 Centralisering

En av huvudvinsterna med MSKD är att konsolidera (eller reducera) antalet produkter, kompetenser och leverantörer. Största ekonomiska vinsten med denna konsolidering ligger inte nödvändigtvis i inköp av hård- och mjukvara, utan vanligtvis i åtgången av resurser för att utvärdera, designa, implementera, drifta och inte minst integrera de utvalda produkter och lösningarna. Detta går hand i

hand med standardisering eftersom det är enklare att centralisera och konsolidera miljön om det finns färre olika komponenter att hantera.

Genom att centralisera tekniken blir det också enklare för driftsorganisationen att samlas centralt och utöva administration och drift från en eller från färre platser än tidigare.

7.2.5 Service Desk

Målet för en Service Desk är att vara en central kontaktpunkt för användarna då de vill ha hjälp att hantera Incidenter och Förfrågningar och samtidigt vara ett gränssnitt för andra processer under IT Service Management organisationen (exempelvis Change, Problem, Configuration med flera). Namnändringen från Helpdesk till Service Desk syftar på den utvidgade rollen ovan som denna funktion fått, ofta blir den en Single Point of Contact (SPOC) för organisationens basleveranser och med det ställs höga krav på förmåga, uppträdande och inställning. En väl fungerande Service Desk är central för att kunna etablera en effektiv Service Management.

7.2.6 SLA

Inom ramen för MOF/ITIL ingår som vi nämnt tidigare i dokumentet att IT-organisationen etablerar OLA och SLA med sina kunder så att både producent och kund kan se och mäta kvalitén på levererade tjänster. För att göra detta används produkterna i System Center och data och statistik som finns i dessa system för att kunna presentera faktisk statistik och mätetal.

7.2.7 IT-strategi

IT-strategi är ett begrepp för att säkerställa och utveckla verksamhet med IT eller som relaterar till IKT-frågor (informations- och kommunikationsteknik). Omfattningen är informations- och informationsteknologi för organisation som helhet eller avgränsade delar med olika utvecklings-områden. Vanligtvis omfattas vision, policy och handlingsplan samt konkreta eller mätbara mål.

IT-strategier blev först populär i affärsverksamheter och stora IT-organisationer och växte fram på 1990-talet då den från början tillämpades på IT-verksamhet och deras IT-projekt och IT-leveranser. Målet med IT-strategin är en *effektiviserad* verksamhetsstyrning, *snabbare* möjligheter eller *tydligare* fördelar för organisationen. Exempel på resultat är ökad effektivitet eller stärkt överlevnads- och framgångsfaktor med stöd av IT. Ett annat exempel är IT-styrning.

IT strategin utövas som intern ledningsförmåga efter verksamhetsplan eller affärsplan av den IT-strateg som ansvarar för IT-strategin och CIO-planerna. IT-chefen äger ansvar för de dagliga IT-operationerna och leveranserna.

Varje kommun bör definiera en IT-strategi som ökar effektiviteten av IT inom kommunen.

7.2.8 Egen IT-drift/Beställarorganisation

Det finns två generella sätt på vilken en kommun kan välj att hantera sin IT drift, antingen äger man drift och personal själv eller också ställer man krav på en intern eller extern leverantör.

7.2.9 Outsourcing/Cloud Computing

En modern plattform som MSKD 4.0 möjliggör också säkra lösningar enligt nya arkitekturer, såsom mobilitet och distansarbete, tjänsteorienterad arkitektur (SOA) och inte minst ”Software + Services” där en del lösningar levereras med egen infrastruktur medan andra kan levereras som molntjänster.

8 Referensdesign

8.1 Katalogtjänst – Active Directory

Microsofts katalogtjänst Active Directory Domain Services (ADDS) utgör grunden för säkerhet i en Windows-baserad infrastruktur eftersom den används för all autentisering och auktorisering. AD medger även ”single sign on” för övriga komponenter i referensdesignen såväl som för många tredje-partslösningar som implementeras på infrastrukturen. Med Active Directory Federation Services (ADFS) expanderas "single sign on"-konceptet även ut över Internet och in i molnet. Active Directory stöder många olika säkerhetsnivåer såsom lösenord med olika krav och protokoll, PKI (tillsammans med Active Directory Certificate Services, ADCS) men även stark autentisering som t ex smarta kort.

8.1.1 Active Directory Domain Services Design

Hur Windows Server 2008 (R2) ADDS bör designas, beskrivs i AD DS Design Guide som finns fritt tillgänglig på TechNet. I vissa fall är dock Designing and Deploying Directory and Security Services från Windows Server 2003 Deployment Guide mer omfattande och komplett.

För att förenkla design- och migreringsprocessen för en kommun har nedanstående referensdesign tagits fram. För en kommun kan en AD-design alltså se ut som beskriv i nedanstående avsnitt.

8.1.1.1 Skogdesign

Traditionellt har svenska kommuner separerade nätverk för administration och skola. Denna design leder till separerade infrastrukturer och i AD-fallet till varsin skog (forest) för administration och skola. Man har helt enkelt låtit nätverksdesignen bli en designparameter för övrig infrastruktur.

MSKD har från början fokuserat på att tillhandahålla en säkerhetsdesign som tillmötesgår de funktionalitets- och åtkomstbehov som finns. Från och med MSKD 2.0, 2005 har vi pekat på fördelarna med ett gemensamt AD istället för separerade.

Enligt Creating a Forest Design är det viktigaste designkriteriet om organisationen kan ha förtroende för de som äger och administrerar AD-skogen. En typisk svensk kommun har idag ***en*** IT-avdelning och ***en*** IT-chef för hela kommunens verksamhet. Detta blir då ett tydligt bevis på att hela organisationen kan ha förtroende för ***en*** gemensam administration och därmed ***ett*** gemensamt AD. Ett annat design-kriterium är att man har fungerande nätverkskommunikation. Det finns dock ingen anledning att begränsa möjligheten till fysisk nätverkskommunikation inom en kommun som använder MSKDs säkerhetslösning. En MSKD 4.0 design använder sig därför av **en AD-skog**.

8.1.1.2 Domändesign

Domäner är partitioner för replikering i AD. Eftersom en kommun av naturliga skäl är geografiskt begränsad och ingen kommun är större än att den ryms i en domän, finns det heller ingen anledning att designa fler domäner än skogar. Det finns inte heller längre någon anledning att designa AD skogar med en ”empty root domain” eftersom det numera går att döpa om en domän. En MSKD 4.0 design använder sig därför av **en AD-domän**.

8.1.1.2.1 Domännamn

Vad man bör tänka på när man väljer domännamn finns beskrivet i Assigning Domain Names och Selecting the Forest Root Domain. Sammanfattat bör man hitta ett namn som kan användas både till DNS och NetBIOS. NetBIOS-namnet och DNS-prefixet som alltså bör vara identiskt skall bestå av max 15 tecken (A-Z, a-z, 0-9, and (-), men inte enbart siffror). NetBIOS-namnet måste även vara ledigt på hela nätverket.

DNS-suffixet bör skyddas genom att vara registrerat på Internet. Använd aldrig single-label, dvs DNS-namn utan suffix. Även om det aldrig har blivit skyddat i RFC 2606 Reserved Top Level DNS Names så är det vanligt förekommande att man använder ".local" som DNS-suffix.

Se nedanstående tabell för exempel på domännamn (byt ut "*kommun*" i nedanstående exempel mot kommunens faktiska namn, men bara med bokstäverna a-z). DS i nedanstående exempel skall uttydas "Domain Services".

DNS	Exempel DNS	NetBIOS	Exempel NetBIOS
***kommun*-ds.*kommun*.se**	goteborg-ds.goteborg.se	*KOMMUN*-DS	GOTEBORG-DS
ds.*kommun*.se	ds.goteborg.se	DS	DS
***kommun*.local**	goteborg.local	*KOMMUN*	GOTEBORG

8.1.1.2.2 Uppgradering eller migrering

Hur AD implementeras beskrivs i AD DS Deployment Guide.

Om man redan har en tidigare version av Active Directory installerat behöver man uppgradera eller migrera. Uppgradering är enkelt, migrering är ett mer omfattande projekt. Har man flera skogar eller domäner idag och vill konsolidera till en skog och en domän behöver alla användare, datorer och resurser migreras in till en och samma domän. Kostnaden för detta migreringsprojekt får då vägas mot vinsterna med en konsoliderad infrastruktur. Det går naturligtvis att bygga samma lösning och funktionalitet med flera AD-skogar och -domäner som sammankopplas med "trusts". Det blir dock mer komplext och dyrare att bygga, äga och drifta denna infrastruktur.

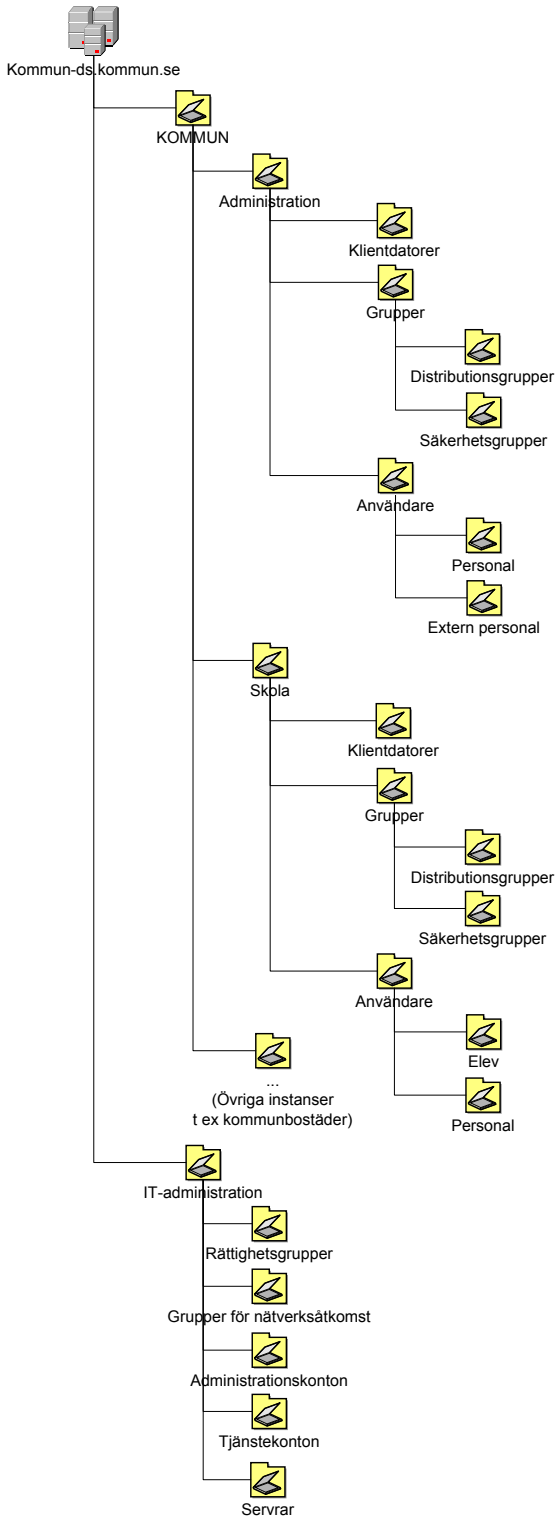
8.1.1.3 DNS-design

Normalt installerar man DNS-serverrollen på alla ADDS-servrar och använder AD-integrerad replikering av DNS-zon-information och får därmed multimaster-uppdateringsstöd och säkra dynamiska uppdateringar.

8.1.1.4 OU-design

OU-designens primära syfte är att möjliggöra delegerad administration. Sekundärt kan OU-designen användas för att tilldela GPO:er (grupprincipobjekt). Det finns alltså ingen anledning till att försöka beskriva organisationen (utöver hur den administreras IT-mässigt) med hjälp av OU-strukturen. I MSKD används OU-designen dessutom för att separera administration och skola. Syftet här är t ex att kunna begränsa elevers rättigheter att göra uppslag om personal på administrationen och att kunna lägga upp separata adresslistor.

Ett exempel på en OU-design är följande:



MSKD 4.0 - Grundläggande OU-design

Denna design är avsedd att ligga som grund för domänens OU-struktur.

Under domänen skapas två rotenheter; IT-administration och KOMMUN.

Under IT-administration hamnar objekt som inte lämpar sig att delegera rättigheter till för annan personal än IT-personal. Till exempel, enheten kallad Rättighetsgrupper innehåller grupper som delger rättigheter i AD:t. Om denna enhet låg under, exempelvis, enheten för Administration, skulle en delegerad rättighet att hantera gruppmedlemskap under Administration innebära att användaren kan ge sig själv mer delegerade rättigheter i AD:t. Detsamma gäller Grupper för nätverksåtkomst, Administrationskonton, Tjänstekonton och Servrar. Rättigheter till objekt under dessa enheter skall inte delegeras till någon annan del i organisationen än IT-personalen.

Under KOMMUN hamnar enheter med objekt för kommunens olika organisationer. Här hamnar alltid Administration (för administrativ personal inom kommunen) och Skola (för pedagogisk personal och elever inom kommunen).
Under KOMMUN kan man även lägga övriga organisationer, till exempel Kommunbostäder, räddningstjänst och liknande.

Under respektive organisationsenhet finns en grundstruktur bestående av huvudenheter för Klientdatorer, Grupper och Användare.
Dessa huvudenheter möjliggör enkel delegation av rättigheter och GPO-länkning. De är också anpassade för att man enkelt skall kunna skapa MMC-konsoler för administratörer, till exempel kan en användare som hanterar användarkonton för både lärare och elever skapa en ADUC-konsol från och med nivån Skola\Användare.

Under Klientdatorer placeras alla klienter för gällande organisation. Vill man dela in datorerna i ytterligare organisationsenheter kan man göra så, men det är att föredra att kategorisera datorerna genom attribut eller gruppmedlemskap för exempelvis GPO-filtrering.

Under Grupper placeras gruppobjekt för gällande organisation. Här finns en enhet för Distributionsgrupper och en för Säkerhetsgrupper. Tanken med denna indelning är att förenkla rättighetsdelegeringen då, exempelvis, en administratör som hanterar distributionslistor inte nödvändigtvis skall hantera Säkerhetsgrupper.

Under Användare placeras användarkonton för gällande organisation. Indelningen här är valfri, men som förslag kan enheten under Skola delas in i enheterna Elev och Personal. Ytterligare enheter kan skapas under dessa, men det är att föredra att låta attribut eller gruppmedlemskap kategorisera användarkonton för exempelvis GPO-filtrering.

8.1.1.5 AD Site-design

Hur "Site Topology" bör designas beskrivs i Designing the Site Topology for Windows Server 2008 AD DS.

Site-topologin används för:

- ADDS domänkontrollantsreplikering.

- För att klienter skall hitta närmsta domänkontrollant.
- För att klienter skall hitta närmsta DFS-replika.
- För att klienter skall hitta närmsta tillhandahållare av olika slags tjänster som använder ADDS för att publicera dessa tjänster.
- För att hitta närmsta skrivare.
- GPO-tilldelning kan ske styrt med site-tillhörighet.
- Applikationstilldelning kan i vissa lösningar ske site-styrt.

Det är alltså ovanstående behov som styr vilka siter som behövs. Normalt sett har man inom en kommun centraliserat alla servrar till en datahall och behöver för AD-replikering och klienters server-närhet bara definiera en site. Behovet att definiera flera siter uppstår oftast när de används för att styra skrivartilldelning.

8.1.1.5.1 Placering av domänkontrollanter

Som en del av site-designen placeras domänkontrollanter ut i infrastrukturen. Men har vi bara en central serverhall så är ju detta enkelt. Best practice är dock att man alltid har minst två domän-kontrollanter av tillgänglighetsskäl. Alla domänkontrollanter skall också vara "Global Catalog".

Det bör också nämnas att det är kritiskt med fysisk säkerhet för domänkontrollanter. Kan någon som vill attackera nätverket, få fysisk åtkomst till en domänkontrollant har den personen möjlighet att få fullständig åtkomst till hela miljön. Därför skall alla domänkontrollanter placeras i en säker och skyddad datahall. Skulle behovet finnas att placera ut en domänkontrollant i en fysiskt mindre skyddad miljö finns nu read-only domain controller (RODC) som alternativ.

8.1.2 Namnstandard

I MSKD version 3 fanns ett utförligt avsnitt om namnstandard och responsen från våra kunder och partners har varit tydligt att det är bra att ha denna med. Därför så medföljer en något uppdaterad namnstandard som bilaga till detta dokument, se Appendix 2 ”Namnstandard”.

För att standardisera men också göra det möjligt att maskinellt genomföra olika saker i sin miljö som t.ex. i verktyg som MDT, ILM och i scripts, logganalys, sortering i verktyg, uppföljning etc. är det viktigt att införa enhetliga namnstandarder överallt där det är möjligt. Det finns naturligtvis fler namn att standardisera på i en lösning för att få överblickbarhet och enkelhet bl.a. inför administration och övervakning, men framförallt för att på ett enklare sätt kunna bygga ut och bygga om miljön vart efter tiden går. Försök samla denna namnstandard i centralt underhållna dokument. Det är viktigare att man har central kontroll än att namnstandarden är helt perfekt.

8.2 Public Key Infrastructure (PKI)

En många gånger överdramatiserad och underutnyttjad teknologi är PKI och Active Directory Certificate Services (ADCS). Det är synd då det är teknologi som är väldigt användbar både för att höja säkerheten och för möjliggöra interoperabilitet. PKI kan med hjälp av Active Directory Domain Services och Active Directory Certificate Services införas med ett minimum av ansträngning. Till exempel kan certifikat både begäras och utfärdas helt automatiskt till både maskiner och användare. Det enda som krävs är att rättigheter sätts på det önskade viset.

Anledningen till att PKI ofta överdramatiseras är att i stora applikationer där PKI är den bärande identitets- och säkerhetslösningen blir lösningen ofta både komplex och dyr, med stora hierarkier och extrema säkerhetsprocedurer. De huvudsakliga användningsområdena för PKI inom MSKD ligger snarare inom vad som kan betecknas som infrastruktur-PKI. En intern infrastruktur-PKI-lösning etablerar normalt sitt förtroende genom ADDS. ADDS blir på så vis det översta lagret i PKI-hierarkin.

8.2.1 Användningsområden PKI

I lösningen används certifikat inom många områden för att realisera funktionalitet såsom:

- Dator- och användarautentisering m h a certifikat
- Smarta kort (SC) autentisering för exempelvis användar-, WLAN- och VPN-autentisering
- DirectAccess
- EFS-filkryptering på klienter
- SSL (autentisering och kryptering)
- S/MIME (signerad och krypterad epost)
- IPsec Server and Domain Isolation (SDI)
- IAS/Radius autentisering (t ex 802.1x) för VPN, WLAN och LAN
- Kodsignering
- Mobiltelefonsäkerhet
- SCCM
- SCOM
- OCS

8.2.2 Alternativ till intern PKI

I många fall kan man välja mellan PKI och andra metoder. För till exempel säkra trådlösa nätverk kan man använda antingen certifikat med 802.1x EAP-TLS eller lösenord med 802.1x PEAP. Båda är säkra metoder som använder SSL för att bevisa att man känner till en hemlighet som dock aldrig kommuniceras. Självfallet är dock kvaliteten på en privat nyckel (PKI) högre än ett användarlösenord. Likaså kan man för SDI välja mellan Kerberos och PKI för IPsec autentisering. Kerberos är i allmänhet att föredra eftersom allt som behövs redan finns på plats och används i och med ADDS. PKI blir dock ofta ett krav om man har behov av att stödja och ta med heterogena miljöer i lösningen.

För externa kommunikationsbehov föredrar man oftast "köpta certifikat" från en extern och allmänt betrodd certifikatutfärdare.

8.2.3 Active Directory Certificate Services (ADCS)

Som CA (Certificate Authority) används i denna lösning Windows Server 2008 R2 **Enterprise Edition** för att fullt ut kunna använda inbyggd funktionalitet för automatisk certifikatshantering. Windows Server Standard Edition har förvisso en ADCS-roll, men den är starkt begränsad då den inte stöder version 2 och 3 certifikat-mallar och därmed varken automatiskt utfärdande av användarcertifikat eller de senaste kryptoalgoritmerna.

Observera att vi även kan hantera Windows Phone. Att kunna utfärda certifikat kan hjälpa till att höja säkerhetsnivån på flera nivåer. För viss funktionalitet är den t o m nödvändig. Eftersom en certifikatserver med stöd för automatisk utrullning av certifikat ingår i Windows Server 2008 R2 Enterprise Edition är detta dock inte speciellt komplicerat.

CA-strukturen bör enligt best practice byggas i en 2-lagerslösning vilket innebär att en CA Root bör installeras som lager samt ett lager 2 med AD-integrerade utgivande CA. För effektiv drift och underhåll av lösningen rekommenderar vi en lösning med Forefront Identity Manager som kan hantera certifikatprocesserna.

8.3 Single Sign On (SSO)

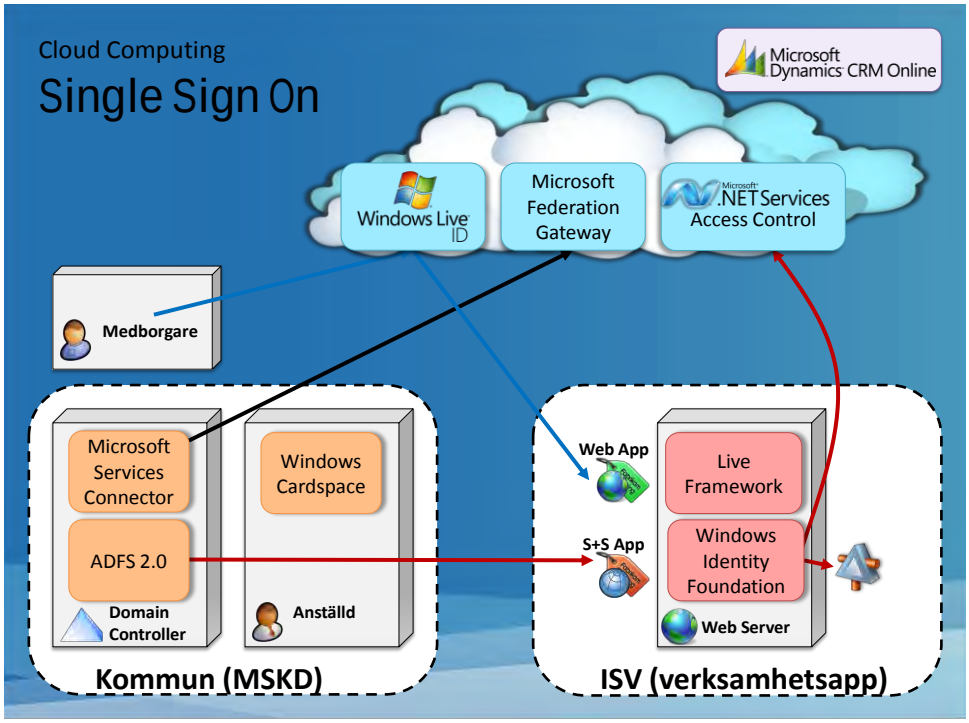
En lösning baserad på AD innebär att all nödvändig grund är lagd för att erbjuda SSO inom kommunens alla IT-system. Alla Microsoft-baserade lösningar som presenteras i denna lösning har fullt stöd för SSO och detta implementeras fullt ut i MSKD av både säkerhets- och auditing-/loggningsskäl för att bl.a. uppfylla uppföljningskrav ex från standards som ISO17799/ISO27001.

8.3.1 Active Directory Federation Services (ADFS)

Det finns 290 kommuner i Sverige. Varje kommun har åtminstone ett 20-tal olika verksamheter som var och en behöver olika verksamhetsanpassade IT-system. Dessa förutsättningar gör att dessa IT-system är synnerligen lämpade att levereras som s k molntjänster. Som molntjänster istället för lokalt installerade system, kommer de att kunna utvecklas, driftas och ägas betydligt effektivare, säkrare och billigare.

En nackdel med molntjänster har länge varit att man förlorar möjligheten till single sign on. Med ADFS och de standardprotokoll som den implementerar får vi nu möjlighet att använda det lokala AD:t även för inloggning till molntjänster. För en användare som har nätverkskontakt med AD, används dennes kerberosbiljett. För en användare som inte har kontakt med AD, kommer denne att få autentisera sig med sitt AD-konto och lösenord vid anslutningen till tjänsten.

För att en molntjänst skall kunna använda sig av ADFS, behöver den vara utvecklad med Windows Identity Framework eller stödja de protokoll som används.



8.4 Identitets- och åtkomsthantering

Med en strukturerad IT-miljö byggd utifrån MSKD 4.0 finns också stora möjligheter att både effektivisera och höja kvaliteten inom identitets-, rättighets- och åtkomsthantering.

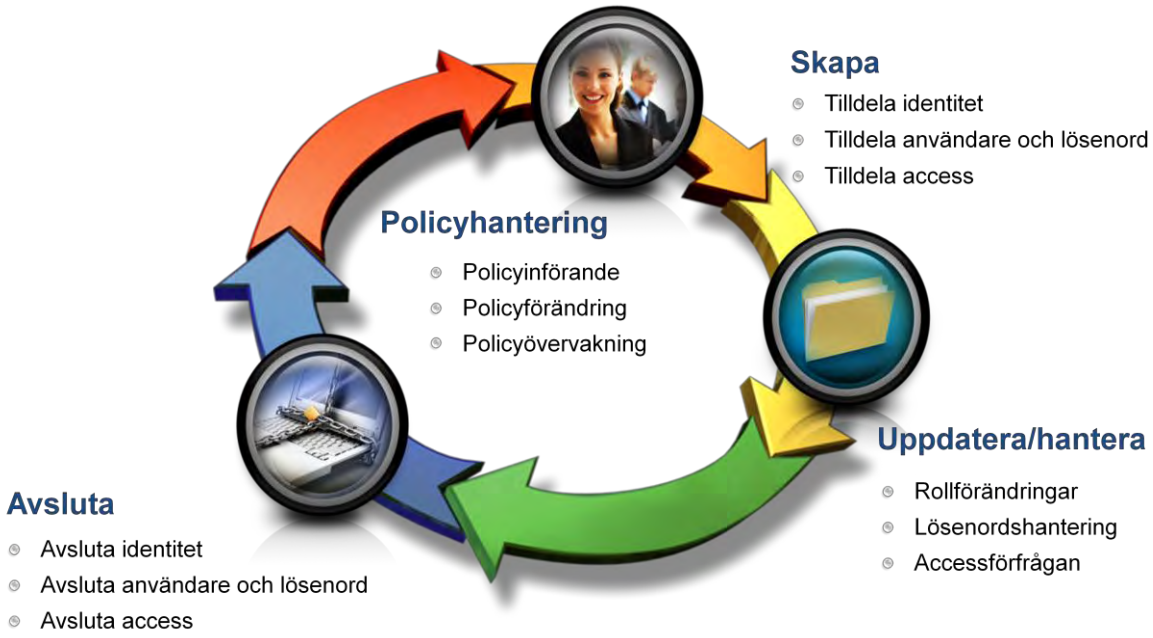
Genom att utnyttja redan befintliga system inom kommunen kan flöden för att skapa, underhålla och avsluta konton och medlemskap i grupper.

Detta avsnitt handlar om hur man kan hantera källdata från exempelvis personal- och elevsystem för att skapa en automatiserad process inom området.

8.4.1 Vad menar vi med identitetshantering?

I många kommuner hanteras fortfarande användarkonton och gruppmedlemskap i AD genom manuella eller halvmanuella flöden och kommunen har inte satt upp en tydlig policy för identitetshanteringen.

En policy för identitetshantering det nödvändiga regelverk som behövs för att skapa, uppdatera/hantera samt avsluta identiteter inom kommunen.



När det gäller personal är det oftast upp till närmast överordnad chef att beställa användarkonton för nyanställda. Detta brukar inte vara ett stort problem då det är uppenbart att en nyanställd måste få ett användarkonto för att kunna använda datorer kopplade till kommunens IT-miljö. Kvaliteten på de lämnade uppgifterna kan inte verifieras, t ex kan en anställd ha ett smeknamn som används och detta kommer sedan inte stämma överens uppgifter i andra system som t ex använder folkbokföringsuppgifter.

Vid underhåll av konton, t ex att en anställd byter av avdelning är det inte lika självklart att IT-avdelningen överhuvudtaget får denna uppgift. Oftast blir det uppenbart då den anställde inte kommer åt gemensamma mappar på den nya avdelningen och IT-avdelningen måste i all hast flytta in den anställde i AD-grupper utan att ha någon beställning från ansvarig chef. I många fall måste tillgängligheten prioriteras och det nödvändiga arbetet med att ta bort åtkomsten för den anställde till den gamla avdelningens gemensamma mappar riskerar att glömmas bort.

När den anställde slutar finns det stor risk att användarkontot överhuvudtaget inte avslutas på grund av att närmaste chef glömmer bort att meddela IT-avdelningen att detta sker och den före detta anställde kommer fortfarande ha access till den IT-miljö.

Gemensamt i samtliga scenarior ovan är att de riktiga uppgifterna finns att hämta i kommunens personalsystem. Där hanteras start på anställning, förändringar i anställning samt avslut av anställning. För elever i kommunens skolor finns motsvarande uppgifter hanterade i ett elevsystem.

Genom att skapa en automatiserad process mellan personalsystem och AD samt elevsystem och AD vinner man flera saker såsom:

- Rätt information om användarna
- Tydlig ansvarsfördelning
- Mindre tid behöver ägnas åt kontofrågor
- Rätt behörighet och åtkomst för användarna

8.4.2 Identity Lifecycle Manager (ILM) 2007

När man startar att använda automatiska processer för identitetshanteringen startar man lämpligtvis med att utse ett källdatasystem för personal och elever som är de stora användargrupperna i en kommun.

Mellan källsystem och AD sätts Microsoft ILM 2007 upp. ILM innehåller både flödesmotor och metadatabas. De första automatiska processerna flödar attribut från källsystem till metadatabas till AD, men kan i en fortsatt utveckling hantera fler källdatasystem som t ex telefonisystem för attribut rörande telefonnummer och anknytningsnummer. De automatiska processerna kan vara envägs- eller tvåvägs-riktade och t ex flöda attributinformation mellan källsystem.

Kommunen bör sätta upp en policy för identitetshanteringen där exempelvis standarder för namnsättning, e-postadresser, lösenord fastställs. Denna policy används vid uppsättning av de automatiska processerna. Vilka attribut i användarkontot i AD som ska flödas med automatik från källdatasystemet fastställs. Detta innebär också att ansvaret för innehåll och kvalitet på dessa attribut flyttas från IT-avdelning till förvaltare av personal- och skolsystem.
Attribut som flödas med automatik mellan källsystem och AD hanteras alltid i källsystemet.

En kompetent produkt med Microsoft ILM 2007 som bas ska kunna i ett startskede kunna:

- Skapa, underhålla och avsluta användarkonton i AD
- Skapa, underhålla och avsluta e-postkonto i Exchange eller Live@edu
- Skapa, underhålla och avsluta grupper i AD
- Skapa, underhålla och avsluta medlemskap i grupper i AD

8.4.3 Forefront Identity Manager 2010

Forefront Identity Manager 2010 möjliggör för IT-organisationer att minska kostnader för att administrera och hantera identiteter och rättighetsprocesser genom att ur en vy presentera användarnas identitet i kommunen samt att automatisera vanligt förekommande rutinuppgifter.

Forefront Identity Manager stödjer bl.a. hantering av “User provisioning” samt administration av certifikat och smarta kort för hela Windowsplattformen, men även till andra icke-Windowsbaserade system. Forefront Identity Manager är en vidareutveckling av Identity Lifecycle Manager ILM/Certificate Lifecycle Manager CLM med ett mycket bättre stöd för processflöden och hantering av användare.

8.4.4 Utveckling

Möjligheterna till utveckling av ett system för identitets- och accesshantering är stora. Ökade krav på hantering av användaridentiteter, både avseende interna roller som anställda och elever och externa roller som medborgare kräver automatiska processer då hantering av stora kataloger inte går manuellt utan att kostnaderna ökar för mycket.

Ett exempel på utveckling för en kommun kan vara att flöda in folkbokföringsuppgifter från Skatteverket via tjänsten Navet. Dessa uppgifter kan sedan sättas upp som flödesprocesser mot kommunens samtliga system som har behov av detta.

8.5 Nätverksdesign

Nätverk och kommunikation är tekniken som ligger bakom både intranät och Internet. I denna roll har tekniken revolutionerat samarbetet både internt och externt för såväl företag som individer. I den tidiga IT-utvecklingen sågs nätverksåtkomst som den grundläggande säkerhetsmekanismen (”fysisk säkerhetsmodell”). Idag (tack vare Internet, bredband och trådlösa nätverk) förväntar sig alla full nätverksåtkomst överallt och alltid. Vi behöver inte fysiskt åka till en arbetsplats med ett lokalt nätverk för att kunna kommunicera och använda de IT-tjänster vi behöver i vår verksamhet. Samtidigt som åtkomsten har expanderat, har naturligtvis exponeringen och säkerhetsbehovet ökat. Vi behöver alltså en ny säkerhetsmodell som stöder dagens kommunikationsbehov. Vi kallar denna för en ”logisk säkerhetsmodell”. I den logiska säkerhetsmodellen är den grundläggande säkerhets-mekanismen autentisering (av maskiner, tjänster och användare). I princip spelar det ingen roll var eller på vilket nätverk du är inkopplad. Observera dock att den logiska säkerhetsmodellens eventuella risker hanteras med ”säkerhet på djupet”. Nätverkssäkerhet och inte minst klientens hygien med mera kan spela in och vara en faktor i auktoriseringen av åtkomst till system och tjänster.

8.5.1 Ett fysiskt nätverk

8.5.1.1 Fysisk säkerhetsmodell

Det traditionella designmönstret för en svensk kommun har länge varit fysiskt separerade nätverk för skola (edu) och administration (adm). Verksamheterna har setts som så åtskilda att inget kommunikationsbehov har funnits. Tvärtom har riskerna med att exponera känsliga verksamhetssystem på samma nätverk som nyfikna och djupt datakunniga elever övervägt vid nätverksdesignen. Även om tekniken för traditionell nätverksdesign har gått framåt med lösningar som t ex 802.1x, är det fortfarande nätverkslösningar som förutsätter en central brandvägg som bestämmer vilken nätverkstrafik som skall tillåtas. Klienter måste sorteras upp i olika virtuella nätverk (VLAN). Med flera fysiska nätverk (adm, edu), trådlöst och fjärråtkomst med mera blir nätverks- och säkerhetsdesignen komplex och kostsam att bygga och underhålla.

8.5.1.2 Logisk säkerhetsmodell

MSKD har från början tagit fasta på det accelererande behovet av integration och konsekvenserna av centralisering och konsolidering och därför sökt möjliggöra säker åtkomst mellan nätverken. Tekniken är nu mogen för att konsolidera de två fysiska nätverken till ett och istället applicera en logisk säkerhetsmodell på nätverksdesignen. Specifikt kan vi med ”Windows Firewall with Advanced Security” och ”IPsec” införa ett koncept som kallas ”Server and Domain Isolation (SDI)”. Med SDI kan en användares autentisering och auktorisering styra brandväggsreglerna för varje enskild inblandad dator. Istället för en central brandvägg blir varje enskild dator del av en logisk distribuerad brandvägg. Denna logiska distribuerade brandvägg konfigureras dock ändå centralt med hjälp av Active Directory Domain Services och Group Policy. Lägger vi sedan till DirectAccess har vi förlängt säkerhetslösningen hela vägen ut till Internet.

8.5.2 Åtkomst: hanterade klienter

Hanterade klienter är medlemmar i Active Directory (AD) och står därmed under IT-avdelningens styrning och kontroll. Detta innebär att även om användaren är lokal administratör på sin PC, kan IT-avdelningen med hjälp av grupprinciper (GPO) styra PC:ns säkerhetskonfiguration. Det spelar alltså ingen roll om användaren är lokal administratör eller inte, det avgörande är om klienten är medlem i AD. Om användaren är lokal administratör eller inte har dock andra konsekvenser (såsom applikationshantering mm) som vi återkommer till i avsnittet om klienthantering. Typiskt är alla PC:s som organisationen äger hanterade klienter, medan privata klienter är ohanterade.

En hanterad klient kan dra fördel av moderna och säkra åtkomstmetoder som SDI och DirectAccess.

8.5.2.1 Server and Domain Isolation (SDI)

Server and Domain Isolation är en logisk säkerhetsmodell som innebär att nätverksresurser isoleras med hjälp av den lokala brandväggen och autentisering med IPsec. För att få kommunicera med isolerade resurser krävs autentisering. Autentisering sker normalt med Kerberos vilket då förutsätter AD-medlemsskap, men kan också åstadkommas med PKI vilket är flexiblare och möjliggör att en mer heterogen miljö kan delta i SDI.

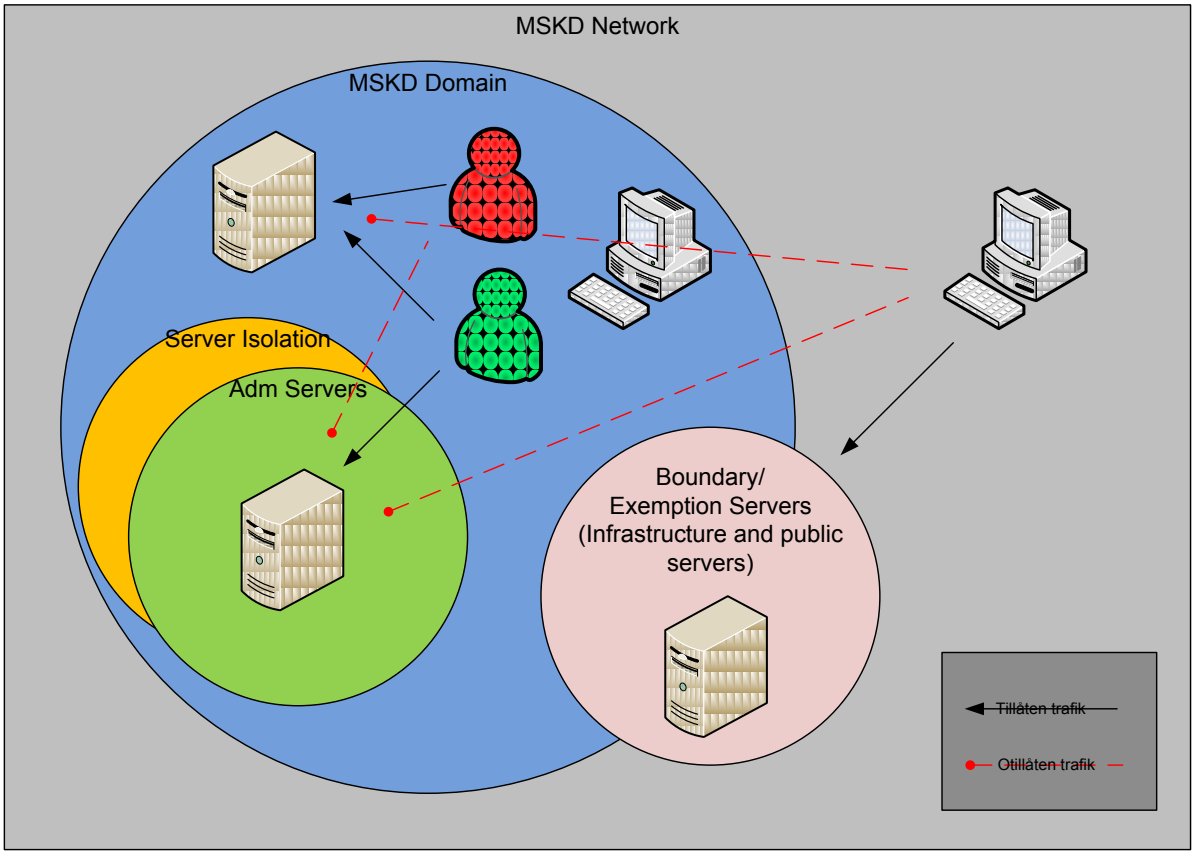
8.5.2.1.1 Vinster med en logisk säkerhetsmodell och SDI

Med en logisk säkerhetsmodell och SDI istället för en fysisk säkerhetsmodell vinner vi:

1. **Dynamisk IT**. Elever, lärare och administrativ personal kommer åt de system och tjänster de har behörighet till, oberoende av fysisk nätverksanslutning. Det spelar ingen roll om man ansluter till nätverket från kommunhuset, skolan, trådlöst eller utifrån Internet man kommer fortfarande åt just de lösningar man borde.
2. **Isolering och hygien**. Alla klienter är medlemmar i domänen och hanterade säkerhetsmässigt av IT-avdelningen. Lokala brandväggen, skyddet mot skadlig kod och uppdateringar mm är styrt av IT-avdelningen och kommunens säkerhetspolicy.
3. **Konsolidering**. Vi kan använda en gemensam infrastruktur för skola och administration. Vi kan dessutom distribuera nätverkssäkerhet från centrala brandväggar till enskilda servrar och klienter. Antalet ingående komponenter och komplexiteten minskar.

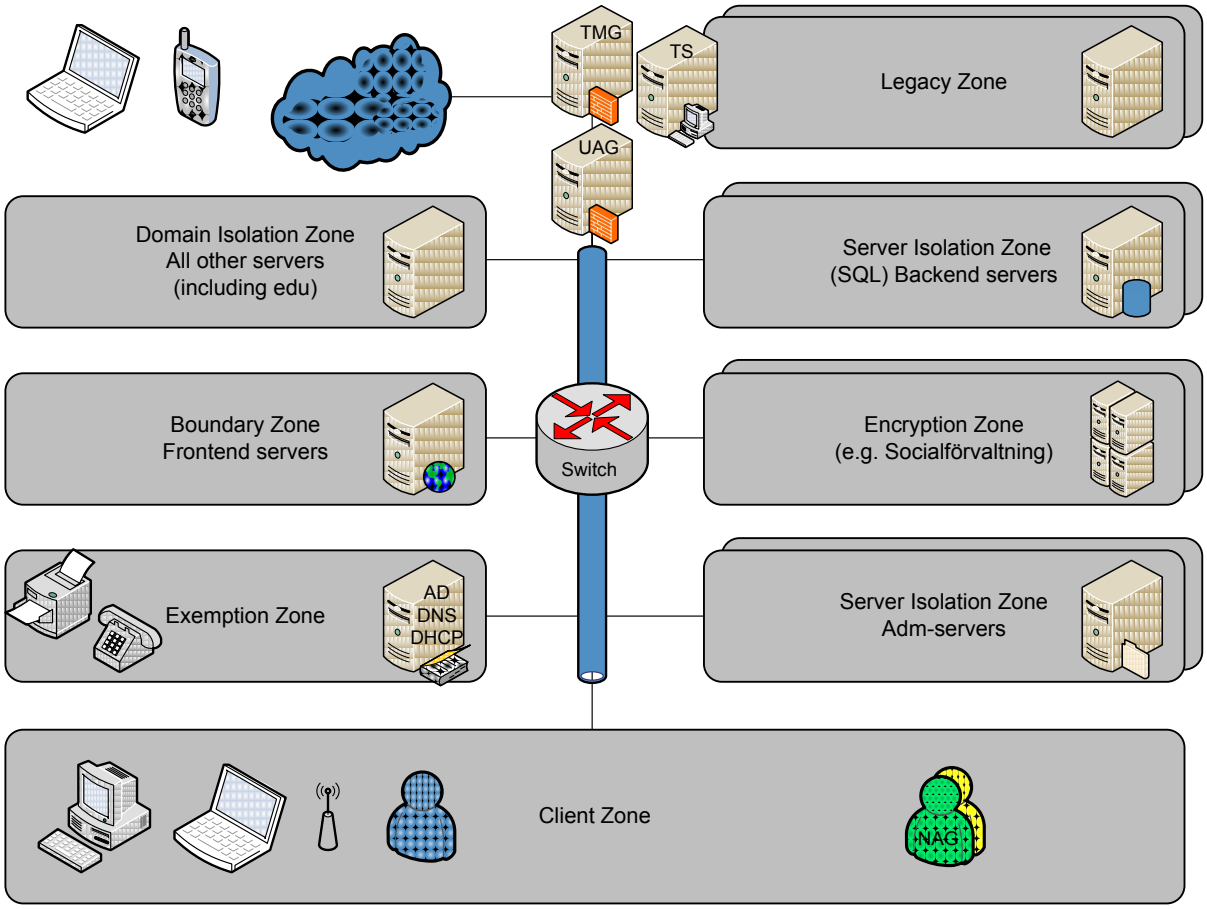
8.5.2.1.2 Konceptuell design

Med SDI isoleras domänen och trafik tillåts bara om den är autentiserad. Vissa resurser såsom grundläggande infrastruktur (DHCP, DNS, AD) kan inte isoleras utan måste göras tillgänglig för att kunna släppa in behöriga klienter i SDI-konceptet. Vissa resurser skall vara ännu mer skyddade och server-isoleras. Detta innebär att det inte räcker med framgångsrik autentisering, det krävs även auktorisering (klienten eller användaren är med i speciell grupp (NAG)). Ett exempel kan vara administrationens servrar som skall skyddas från elever.



8.5.2.1.3 Nätverkszoner

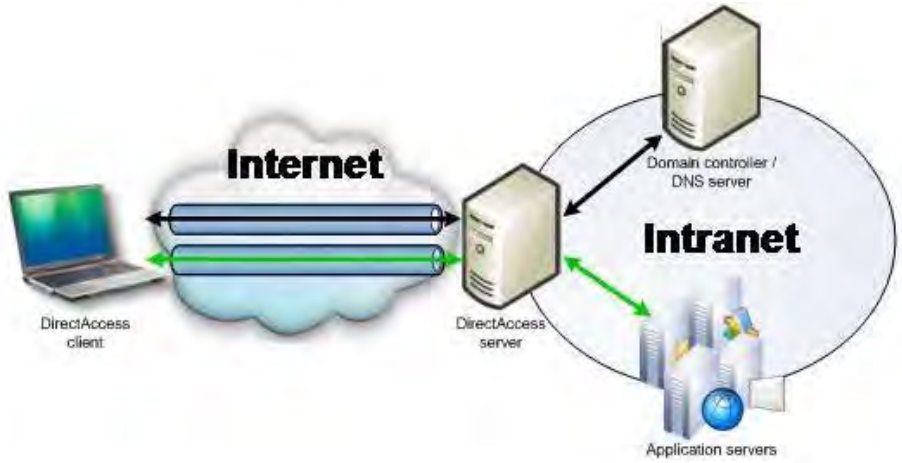
Med Windows Vista och Windows Server 2008 och senare versioner är SDI väsentligt förbättrat och integrerat med den lokala brandväggen. Dessa versioner tillåter också att nätverksåtkomst kan styras på användarnivå och inte bara klientnivå. Det blir då naturligt att designa nätverket med ***en*** klientzon. Däremot är det både rimligt och fördelaktigt att designa flera servernätverkszoner. Att gruppera servrar i zoner efter åtkomstklass förenklar konfigurationen av SDI.



Speciella zoner kan användas både för extra isolering, men även för undantagshantering där SDI inte kan användas. När vi talar om IPsec i SDI avser vi normalt bara autentisering av nätverkstrafiken. Det finns även möjlighet att använda IPsec för kryptering. Kryptering drar extra processorkraft och bör bara användas där det är motiverat.

8.5.2.2 DirectAccess

Med DirectAccess kan hanterade klienter alltid vara uppkopplade till intranätet. DirectAccess fungerar som ett konstant automatiskt VPN.



Den underliggande tekniken i DirectAccess är IPsec och IPv6. IPv6-trafiken tunnlas över Internet och IPv4, men på intranätet ger protokollet tillgång till IPv6-baserade servrar. Finns behov av kommunikation med IPv4-baserade servrar (t ex Windows Server 2003 och tidigare) måste bryggningsteknik användas. Microsoft tillhandahåller denna bryggningsteknik som en del av Unified Access Gateway (UAG) 2010.

8.5.3 Åtkomst: icke hanterade klienter

En icke hanterad klient är inte medlem i AD:t. IT-avdelningen har ingen kontroll på denna klient. Säkerhetsmässigt behöver en sådan klient hanteras med större försiktighet. Exempel på icke hanterade klienter är en lånad dator på ett Internet-café eller en anställds/elevs privata hemdator. Detta gäller oberoende av om klienten ansluter utifrån Internet eller lokalt på kommunens nätverk. I skolan talas om ”bring your own PC” som är ett typexempel på en icke hanterad klient. Många skolor inför också 1:1-koncept där varje elev får en egen (bärbar) dator. Dessa bör vara hanterade klienter, men kan i en del fall även vara icke hanterade klienter.

Icke hanterade klienter får med MSKD inte samma nätverksåtkomst som hanterade klienter eftersom de varken kan använda SDI eller DirectAccess. När en icke hanterad klient ansluts till det lokala nätverk ges den endast åtkomst till grundläggande nätverksinfrastruktur som medger anslutning till AD (för att bli hanterad klient om man så önskar) samt åtkomst till Internet. En icke hanterad klient får därefter åtkomst till lämpliga system och tjänster via de mekanismer som används för Internet-publicering av interna system och tjänster.

8.5.3.1 Internetpublicering

Grundläggande Internetpublicering kan tillhandahållas med hjälp av Threat Management Gateway (TMG). En ännu bättre lösning är dock Unified Access Gateway (UAG). UAG har en mycket rikare funktionalitet och kan publicera i princip vilken applikation som helst medan TMG är begränsad till i huvudsak webbapplikationer. UAG har dessutom en åtkomstportal och klientdetektering för att avgöra klientens säkerhetsnivå och även ta åtkomstbeslut baserat på detta.

För hanterade klienter kan man använda DirectAccess istället för Internetpublicering.

8.5.4 Trådlösa nätverk

Det säkraste sättet att tillhandahålla trådlös nätverksfunktionalitet är att koppla de trådlösa accesspunkterna till Active Directory via Radius-protokollet som implementeras av "Network Policy and Access Services" (NPS). Detta tillåter då användare och klienter som är med i AD att använda det trådlösa nätverket. Autentiseringsmekanismen kan vara antingen certifikat med EAP-TLS eller lösenord med PEAP.

Andra säkerhetsmetoder som bygger på accesspunktens egna säkerhetsmetoder såsom delat lösenord, användarlistor med lösenord eller MAC-adresser är inte att rekommendera både på grund av sämre säkerhet, men lika mycket på grund av stora utmaningar i hanteringen av dessa säkerhets-metoder.

Ett möjligt alternativ är att ha ett oskyddat trådlöst nätverk som inte kräver någon autentisering för trådlös nätverksåtkomst utan istället kräver autentisering på nästa åtkomstnivå. För åtkomst till lokala resurser används SDI och för Internetåtkomst används TMG och autentisering med hjälp av Web Proxy eller "Firewall Client". En användare eller klient som inte har ett AD-konto, kommer då varken åt lokala maskiner eller Internet.

8.5.5 Utgående Internetåtkomst

För utgående Internetåtkomst används Threat Management Gateway (TMG) 2010. TMG är en betydande uppgradering från ISA Server med nya funktioner som: URL-filtrering, Virusscanning och Network Inspection System (NIS).

8.6 Hanterad standardklient

Ett kärnvärde i MSKD är standardisering. En standardklient är en förutsättning för att effektivt kunna leverera en konsekvent användarupplevelse. Men en standardklient är framförallt en förutsättning för att löpande driva ned kostnaden för att supporta användarna genom att styra investeringarna i klientinstallationen mot just en kontinuerligt förbättrad standardklient.

8.6.1 Windows 7

I Windows 7-projektet har utvecklarna fokuserat på kärnvärdena för ett operativsystem såsom: stabilitet, prestanda, säkerhet och kompatibilitet. Windows 7 är precis som Windows XP en evolutionär version som bygger på de revolutionära framstegen i den förra versionen.

Windows 7 är ett primärt tema i MSKD 4.0. Anledningen till att vi ser Windows 7 som en central del av MSKD 4.0-lösningen är dels att man möjliggör säkerhetslösningar som SDI och DirectAccess dels att Windows 7 med sina minska maskinvarukrav medger en fullskalig utrullning och standardisering på ett modernt operativsystem.

Med Software Assurance (SA) erhåller man Windows 7 Enterprise som är en komplett och fullständig version och medger funktioner:

- Enterprise Search – publicera sökområden direkt till startmenyn för effektiv sökning
- BitLocker och BitLocker To Go – skydda löstagbara minnesenheter
- AppLocker – säkerställ vilka applikationer som får startas på en PC
- DirectAccess – åtkomst till företagsnätet utan VPN
- BrancheCache – minska datatrafiken mellan olika kontor

8.6.1.1 Software Assurance

När man anskaffar operativsystemet kan man teckna det med s.k. Software Assurance vilket bl.a. ger rätten till att uppgradera till senaste versionen av programvaran (för övriga SA-förmåner se här). Kunder som väljer att köpa Windows med SA har dessutom rätt till att prenumerera på programpaketet Microsoft Desktop Optimization Package MDOP.

8.6.1.2 MDOP

Microsoft Desktop Optimization Pack (MDOP) är en förpackning med sex olika verktyg för att ge bättre stöd för distribution och underhålla av datorer och applikationer. Den senaste versionen av MDOP kallas MDOP 2009 R2 och krävs för Windows 7. Kunder som har köpt Windows med Software Assurance enligt ovan kan prenumerera på MDOP.

Följande verktyg ingår i MDOP:

- Microsoft Application Virtualization (App-V). Med denna teknik kan virtuella applikationer som skyddas av en egen "bubbla" distribueras via streaming till klienten och konflikter med andra applikationer kan undvikas.
- Microsoft Enterprise Desktop Virtualization (MED-V). Tekniken gör det möjligt att distribuera virtuella klienter (Virtual PC) till datorer som kan hanterad och konfigureras central. Används framförallt för att ge tillgång till applikationer som inte är kompatibla med Windows 7.
- Microsoft Advanced Group Policy Management (AGPM). Möjlighet till granulär kontroll genom change management, rollbasering och rollback.
- Microsoft Diagnostics and Recovery Toolset (DaRT). Verktyg för att reparera PCs, återställning och felsökning även om de inte går att starta.
- Microsoft System Center Desktop Error Monitoring (DEM). Agentlös rapportering av problem och systemkrascher från PC:s för analys och uppföljning med centrala verktyg.
- Microsoft Asset Inventory Service (AIS). Verktyg för att samla in information om applikationer som finns installerade i miljön.

Se TechNet för mer information och djupare teknisk beskrivning av MDOP.

8.6.2 Microsoft Deployment Toolkit 2010

Microsoft Deployment Toolkit 2010 (MDT 2010) är en s.k. Solution Accelerator som innehåller verktyg och riktlinjer för hur man sköter distribution av Windows-servrar och -klienter. Traditionellt så är många bra på att hantera distribution av användardatorer men serverar brukar hanteras manuellt och vi vill påpeka att det finns stora vinster i att också automatisera distribution av servrar.

På Microsofts Desktop Deployment TechCenter hittar du all information om hur du distribuerar klienter och specifik information om MDT 2010 finns här.

När det gäller distribution av operativsystem, nya som befintliga, med MDT 2010 finns två olika lösningar:

1. Lite Touch.
2. Zero Touch

8.6.2.1 Lite touch

Konceptet Lite touch innebär att *det krävs fysiskt kontakt* med den dator som ska installeras, vanligen att man trycker F12 för att bota från nätverk, DVD eller USB för att få igång installationen. Lite touch kan användas utan System Center Configuration Manager.

Vi kan rekommendera Lite touch-lösningen för organisationer med upp till 500 datorer, därefter rekommenderar vi att man implementerar Zero touch för bästa effektivitet och smidighet.

8.6.2.2 Zero touch

Zero touch betyder som namnet antyder att man *inte behöver ha någon fysisk kontakt* med den dator som ska installeras. Zero touch kräver System Center Configuration Manager och är den lösning vi rekommenderar för större organisationer.

8.6.2.3 Operativsystem

Följande operativsystem kan distribueras med MDT 2010:

Operating system	LTI	ZTI
Windows 7	●	●
Window Server 2008 R2	●	●
Windows PE version 3.0	●	●
Windows Vista (with Service Pack 1 [SP1] and later)	●	●
Windows Server 2008 (all service pack levels)	●	●
Windows XP (with SP3)	●	●
Windows Server 2003 R2	●	●
Windows PE version 2.1		●

OBS: För ZTI med MDT 2010 krävs System Center Configuration Manager 2007

8.6.3 Applikationspaketering

För programdistribution använder vi Microsoft System Center Configuration Manager – för alla typer av applikationer och paket, enda undantaget är MED-V packet som idag har en egen mekanism för distribution av virtuella PC:s. Med System Center kontrollerar vi användargrupper, datorer och enheter samt tillför sekvenser och flöden hur installation ska gå till.

För mer information om programvarudistribution med System Center Configuration Manager på TechNet här.

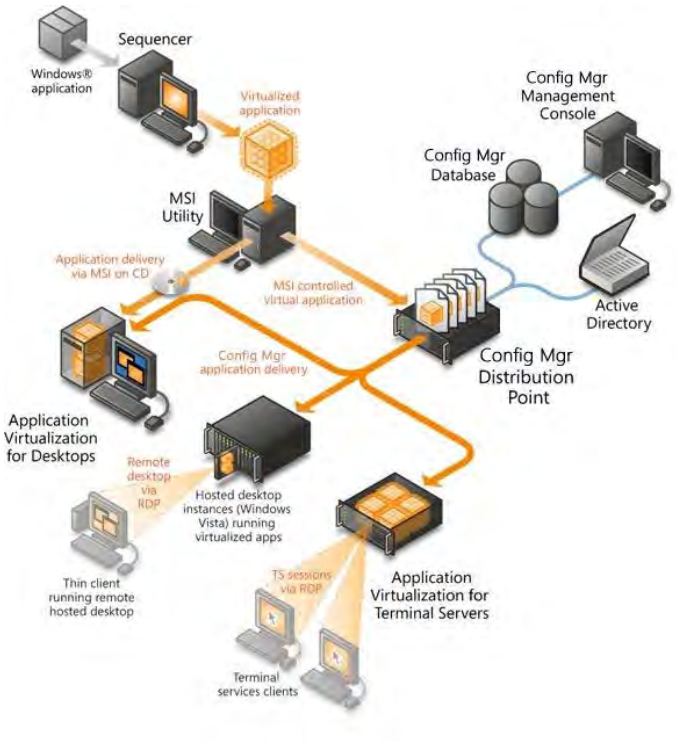
Applikationer kan idag paketeras på olika sätt och i olika kombinationer som gör att man kan få en flexibel och effektiv applikationsmiljö. Som alternativ till traditionell paketering av applikationer i form av installationsfiler så är virtuell paketering det nya sättet att göra denna process både effektivera, stabilare och mer ekonomisk. Microsoft har idag flera tekniker för att paketera och distribuera applikationer:

- App-V – Application Virtualization
- MED-V – Microsoft Enterprise Desktop Virtualization
- RDS – Remote Desktop Services (tidigare Terminal Services)
- Windows Installer

Vi rekommenderar för våra kommuner som bygger sin plattform på Microsofts servrar och klienter att man använder och utgår från System Center Configuration Manager som motor för distribution.

8.6.3.1 App-V

Microsoft Application Virtualization App-V gör det möjligt att skapa applikationer som inte behöver installeras på operativsystemet i traditionell mening utan kan hållas separerade från OS och andra applikationer genom att virtualisera dem. Detta resulterar i minskade konflikter och minskat behov av testning som i sin tur gör det möjligt att snabbare få skaffa och distribuera applikationer till kommunens anställda och personal. Följande bild visar hur arkitekturen för App-V kan se ut.

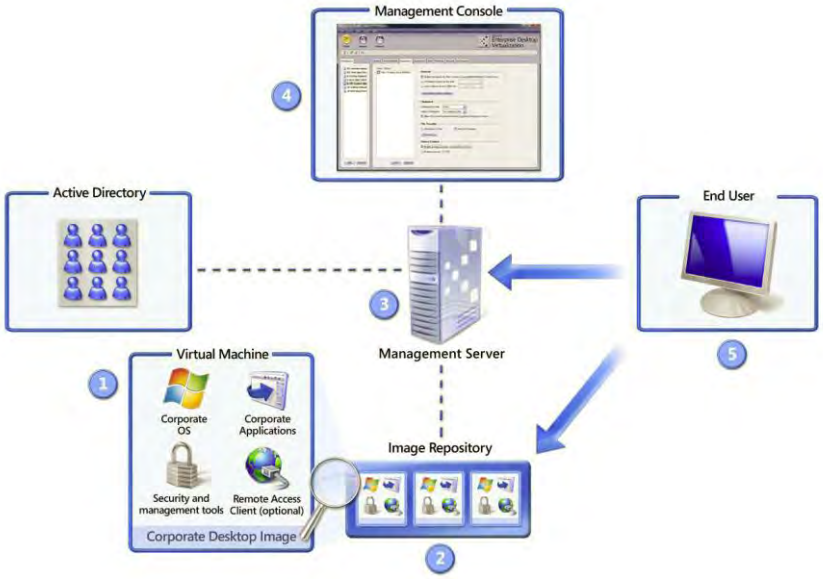


För Microsoft Best Practices kring virtuell applikationspaketering se följande länk.

Information om hur man importerar virtuella applikationer till Configuration Manager finns här.

8.6.3.2 MED-V

För att införa MED-V krävs att en Management-server installeras och att man definierar och skapar ett bibliotek av paket/images. Dessa virtuella PC-paket kallar vi hädanefter för VPC (virtuell PC). Följande bild visar en MED-V arkitektur.



1. Administratören definierar VPC:er – Skapar VPC som en full desktop med OS, applikationer, antivirus, uppdateringar, övervakning/managementklient etc.
2. Paketbibliotek – Innehåller alla VPC:er på en IIS-server med versions- och rättighetshantering och effektiva styrmekanismer för att hantera distribution av nya paket och uppdateringar för att minimera bandbreddsutnyttjandet och ge bra användarupplevelser (via ”Trim Transfer” teknik).
3. Management server – Styr tilldelning av VPC till användare i AD via policy och lagrar händelser i en SQL-databas för övervakning, loggning och rapportering.
4. Management console – Adminstratörens verktyg för att hantera management-server och paketbibliotek.
5. Användar-PC
    - Livscykelhantering av VPC– Autentisering, distribution, rättighetshantering och policy-inställningar.
    - Sessionshantering – Start, stop och låsning av VPC.
    - Normal PC – MED-V-applikationer är tillgängliga som vanligt på PC:n och nås via Start-menyn och integrerar med andra befintliga applikationer.

All kommunikation mellan klient och server (management-server och VPC-bibliotek) sker via HTTP eller HTTPS.

För att planera och implementera MED-V följ Microsoft best practices på TechNet här.

8.6.4 Datortyper

Då vi undersökt vilka typer av datorer som finns ute i kommunerna så varierar detta stort. Därför vill vi här ta upp ett antal scenarion.

8.6.4.1 Admin/User

Denna fråga rör huruvida man ska tillåta användare vara administratörer på sin dator för att kunna installera eller exekvera applikationer. Detta kan bero på flera saker som t.ex. att applikationen är skriven på ett sånt sätt att det krävs. Rekommendationen är att alla användare ska ha rollen User och

att applikationerna måste anpassas eller hanteras utifrån det perspektivet. För att hantera applikationer som kräver något annat bör man därför överväga alternativa sätt att distribuera dem:

- Skriva om applikationen eller skaffa en version med korrekt stöd
- Paketera applikationen virtuellt eller via Remote Desktop Service

8.6.4.2 Bärbart/Tablet PC/Stationärt

Idag finns flera olika datortyper att ta hänsyn till och vi måste vara beredda att kunna hantera alla. Stationära och ägda av skolan är kanske den enklaste typen medan bärbara blir svårare att underhålla då dessa inte alltid finns i nätet för t.ex. uppdateringar och säkerhetskontroller. Här kan funktioner som DirectAccess göra det möjligt att även från IT nå en dator som befinner sig utanför nätverket för säkerhetsuppdateringar och konfiguration.

8.6.4.3 Datasalar/Egen elevdator

För några år sen var det endast tal om att man hade datasalar som elever kunde använda medan man idag kanske delar ut datorer till varje elev eller att man får ta med en egen dator som kan användas i skolans nät. Vilka krav kan vi ställa på dessa olika typer?

Datorer kräver ett kontinuerligt underhåll och med tiden kommer förändringar att behöva genomföras, kanske ominstalleras eller uppdateras vilket förändrar dess utseende och beteende. Det finns förstås flera sätt att se på denna fråga. Det bästa vore förstås att alla datorer vore hanterade av kommunens IT och stödjer de inställningar och säkerhet som man enats om; uppdateringar, antivirus, brandväggar etc. Det finns dock ett behov av att även erbjuda s.k. pedagogisk frihet där eleverna får skapa och bygga egna lösningar. Här kan man förstås välja olika lösning men två alternativ skulle kunna vara:

1. Erbjuda en hanterad dator med en virtuell klient som eleven kan hantera på önskat sätt.
2. Erbjuda en dator som eleven kan hanterar som önskat och en central virtuell klient (VDI) för att nå skolans applikationer och system.

8.6.4.4 Kiosk-dator

Det finns ofta ett behov av en datortyp som alltid ser ut på samma sätt, t.ex. på ett bibliotek där man har en dator som man gör sökningar i och som man inte behöver spara inställningar i och där konfigurationer och lokalt lagrad information endast är temporär, en statisk PC. När denna typ av dator startas om så kommer den att ha samma utseende och konfiguration som då den installerades.

Denna typ av PC kan också vara ett alternativ för datasalar i den mån de finns. Via denna terminal skulle elever kunna få tillgång till elevsystem via Remote Desktop Services eller VDI, se nedan.

För denna typ av ”statiska” PC:s rekommenderar vi att Windows SteadyState används. Windows SteadyState, som namnet anger, gör det möjligt att skapa en statisk bild av en PC som man kan hantera m.h.a. användarprofiler och det går att låsa ner dem så att funktionerna blir begränsade. Läs mer om Windows SteadyState här.

8.6.4.5 Datasalar/Legacy-klient/Fjärråtkomst

I flera av de klientscenarion som finns inom en kommun och kanske särskilt på elevsidan finns det anledning att titta på lösningar som kan erbjuda tillgång till system på annat sätt än via den fysiska datorn. Dessa kan vara:

- Remote Desktop Services (Terminal Server) (user)

- VDI (admin)

Med dessa tekniker kan vi låta användarna komma åt system och applikationer utan att de installerats på den lokala datorn. Denna typ av lösningar kan också ge åtgång till äldre (legacy) applikationer som kanske inte fungerar i den nya moderna klientplattformen. Dessa tekniker gör det även möjligt att publicera ut tjänster utanför nätet som man t.ex. kan använda från ett Internetkafé, dvs via en icke hanterad klient.

8.7 Servervirtualisering

8.7.1 Inledning

Med servervirtualisering ökar vi hårdvarans nyttjandegrad och minskar antalet fysiska servrar i datacentret. Med servervirtualisering kan vi:

- Öka tillgängligheten på servrar
- Öka flexibiliteten i datahallen
- Lättare administrera servrar
- Lättare flytta last mellan olika servrar och mellan olika datahallar

8.7.2 Private Cloud

Cloud Computing använder virtualisering för att bygga en skalbar, elastisk och hanterbar infrastruktur. När företag ser på denna teknik vill de naturligtvis använda den själva. Och det oberoende av om de köper en molntjänst eller bygger egen infrastruktur. Microsoft inser detta behov och kommer att beskriva detta som en lösningsaccelerator ”**Dynamic Datacenter Toolkit for Enterprises**” i början av 2010. Se följande länk för mer information.

8.7.3 Vilka system ska virtualiseras?

En vanlig fråga gällande servervirtualisering är vilka system som rekommenderas att man virtualiserar. Det som man bör ta hänsyn till är:

- Supporterar systemleverantören virtualisering?
- Supporterar systemägaren virtualisering?

8.7.3.1 Supportade system

För system från Microsoft så är följande supportsida bra att utgå ifrån, där beskrivs vilka Microsoft server programvaror som supportas i en virtualiserad miljö (servervirtualisering baserad på Hyper-V).

För resp. produkter finns också specifika länkar till artiklar och dokument som beskriver hur dessa kan och bör virtualiseras. Nedan följer länkar till antal viktiga system och hur man bör virtualisera dessa.

- Active Directory domain
- Microsoft Exchange
- SQL
- BizTalk

Det finns även programvaruleverantörer som beskriver hur deras system kan virtualiseras. Exempel på detta är SAP.

8.7.3.2 Icke supporterade system

Exempel på system/roller man inte kan virtualisera är ”Unified messaging”-rollen i Exchange 2007. Ett annat är de roller i Office Communication Server som hanterar realtidsdata. Innan man virtualiserar någon last bör man säkerställa huruvida denna supporteras eller inte.

8.7.4 Hantering av virtualiserade system

För att hantera servrar i datahallen, såväl virtualiserade som fysiska, rekommenderar vi att man använder följande lösningar ur System Center-familjen.

8.7.4.1 System Center Configuration Manager

SCCM används i ett Datacenterscenario för att:

- Installera båda fysiska och virtuella servrar
- Hantera säkerhetsuppdateringar
- Inventera servermjukvara

8.7.4.2 System Center Virtual Machine Manager:

SCVMM används i ett datacenterscenario för att:

- Hantera samtliga virtuella maskiner, såväl i en Hyper-V-miljö som i en VMware ESX-miljö
- Installation av virtuella maskiner med hjälp av mallar och images
- Migrering av virtuella maskiner mellan olika fysiska system
- Migrering av fysiska maskiner till en virtuell miljö

8.7.4.3 System Center Operations Manager

SCOM används i ett datacenterscenario för:

- Maskinvaruövervakning
- Tjänsteövervakning av distribuerade tjänster som kan exekveras på olika fysiska och virtualiserade servrar

8.7.4.4 System Center Data Protection Manager

DPM används i ett datacenterscenario för att:

- Skydda Microsoft SQL Server
- Skydda Office SharePoint Server
- Skydda filer och kataloger på Microsoftbaserade filsystem
- Skydda Hyper-V-maskiner med sina virtuella maskiner

8.8 Säkerhet

Inom Microsoft lägger vi stor vikt och betydelse på tillförlitlig datahantering – sk ”Trustworthy Computing”. Vi vill fördjupa kundförtroendet genom kvaliteten på våra produkter och tjänster, vår tillgänglighet och tillförlitligheten i allt vi gör.

Den pågående utvecklingen idag av IT och IT- infrastruktur har två primära macro-nivåer som är under ständig utveckling: fler människor och företag förlitar sig på datorer i sitt dagliga arbete varje

dag samtidigt som de hot som kan underminera säkerheten i IT-miljön ökar och blir fler, större och mer avancerade för varje dag.

Trustworthy Computing är en långsiktig strategi för att leverera en säker och pålitlig IT- strategi för alla. Trustworthy Computing hos Microsoft började utformas i January 2002, när Bill Gates meddelade att företaget skulle göra en fundamental ändring i sin mission och strategi Inom nyckel områden såsom Security, Privacy, Reliability, och Business Practices.

I dag är Trustworthy Computing en av grundstenarna inom Microsoft och påverkar nästan allt vi gör. Det är inte bara frågan om att belysa dagens utmaningar utan även en förståelse för utvecklingen och hur användare kommer att använda sina datorer imorgon. Vi måste därför skapa möjligheterna för en säker miljö där användarna och företagen känner trygghet.

8.8.1 Patchhantering

8.8.1.1 SCCM (System Center Configuration Manager)

System Center är en familj av ledande IT management-lösningar som hjälper dig att proaktivt planera, installera, hantera och optimera din IT-miljö. System Center samlar och förenar kunskap om infrastrukturen, policy, processer och best practices så att IT-avdelningen kan bygga hanterliga system och arbeta på ett sätt som minskar kostnader, förbättrar tillgången till applikationer och höjer servicen.

Microsoft System Center Configuration Manager 2007, driver produktiviteten och effektiviteten i din IT-miljö genom minskade manuella ingrepp. Detta ger dig möjlighet att fokusera på high value-projekt, maximera investeringar gjorda i maskin- och programvara samt skapar möjlighet att effektivisera för slutanvändaren genom att leverera rätt programvara eller uppdatering vid rätt tillfälle. Configuration Manager bidrar till en effektivare IT-avdelning genom en säkrare och en bättre skalbarhet i utrullningen av operativsystem och applikationer, konfigurering, förbättrad system säkerhet, samt ger en tydlig och säker inventariehantering av servrar, klienter och mobila enheter.

8.8.2 Windows Server Security Guide

Windows Server Security Guide är en lösningsguide som hjälper organisationer att skapa, rulla ut och underhålla en säker Windows Server 2008 (R2) miljö.

8.8.3 Windows 7 Security Guide

Windows 7 Security Guide dokumenterar de större säkerhetsrelaterade motåtgärder som är tillgängliga i Windows 7, de sårbarheter som motåtgärderna hjälper till att hantera och de potentiella negativa konsekvenserna av att implementera de olika motåtgärderna

8.8.4 Windows BitLocker Drive Encryption

Windows BitLocker Drive Encryption krypterar data på interna hårddiskar, USB-stickor och externa hårddiskar. Allt går att styra med GPOer och för att låsa upp en enhet kan man använda en PassPhrase eller ett SmartCard. Recovery-nyckeln går självklart att spara i AD. BitLocker skyddar ditt data när en PC blir stulen eller oavsiktligt förlorad.

8.8.5 AppLocker

AppLocker tillåter system-administratörer att låsa vissa program och samtidigt tillåta vilka program som får köras på en dator, och detta via GPOer. Systemet bygger på att man pekar ut en .exe-fil och AppLocker läser in certifikat, utgivare, versionsnummer, hash, sökväg mm för att fastställa att just denna applikation är den man tillåter. Med AppLocker kan du kontrollera exakt vilka program som får

köras och inte köras, och på så vis kan du låta användare vara administratörer men ändå kontrollera vad de får installera och inte installera. Du kan exempelvis tillåta installationen av Adobe Reader, men endast om det är version 9 eller senare. AppLocker låter IT avdelningen ha kontroll över vad som installeras på företagets datorer och samtidigt undvika möjligheter för intrång, skadlig kod mm

8.8.6 Stark autentisering

För en bra identifiering och autentisering krävs ett AD där stark autentisering gärna sker med hjälp av flera faktorer (smarta kort, biometric, engångskoder etc).

8.8.6.1 Smarta kort

Smarta kort, ibland även kallat e-tjänstekort, är en del av en identifieringslösning som blir allt vanligare när man vill ha en säkrare inloggningsmetod.

8.8.7 CLM (ILM)

Identity Lifecycle Management håller reda på större organisationers identiteter, t ex personuppgifter i HR-systemet, mailadresser och lösenord. Normalt sett finns sådana lagrade på olika håll och med olika standarder med en följd att olika applikationer baseras på olika indata. ILM 2007 löser de här problemen på ett smart sätt genom att kontinuerligt "lyssna" efter ändringar i databaser och replikerar samt sammanför dessa identiteter till olika katalogtjänster. Dessa har centralt underhåll och livscykelhantering av personuppgifter och rättigheter (smarta kort + certifikat på kortet) kopplade till ett användar-id.

ILM 2007 hanterar identitetsinformation tvärs över multipla lager genom att informationen samlas på en central plats som kallas Metaverse. Management-agenter agerar som kopplingar som översätter data från de sammankopplade systemen till metaversen. Exempelvis kan då e-post-systemet länkas till HR-systemet via ILM. När en anställd som börjar på ett företag och läggs till i HR systemet kan ILM automatiskt hantera den nyanställde i e-post-systemet . Varje anställds attribut, från e-post-systemet och HR-databasen, importeras in till kopplingsytan via management-agenter. E-postsystemet kan sedan använda de individuella attributen, som den information som lades in med den anställdes uppgifter i HR-databasen och då exempelvis dennes telefonnummer. Om den anställdes telefonnummer ändras i HR-systemet kommer detta att automatiskt slå igenom systemen och visas exempelvis i e-post-systemet.

8.8.8 DirectAccess

DirectAccess ändrar det traditionella sättet att komma åt nätverket när man är utanför jobbet vilket innebär att du enkelt kan etablera en internetförbindelse in till jobbet. Via denna kan man sedan arbeta som om man satt fysiskt på jobbet. IT-avdelningen kan enkelt hantera, uppdatera och kontrollera alla datorer i nätverket, oavsett om de är på interna nätverket eller uppkopplade utifrån. Detta underlättar framförallt i arbetet för att förhindra virusintrång eller andra säkerhetsattacker.

Funktionen DirectAccess innebär att klienten vid uppstart etablerar en VPN-förbindelse till nätet och beter sig i allt väsentligt som att den befann sig direkt på arbetets nätverk. GPO:er appliceras på klienten, uppdateringar installeras och användaren kan nå interna servrar precis som om denne befann sig fysiskt på jobbet.

8.8.9 NAP (Network Access Protection)

NAP är ett verktyg som nätverksadministratörer kan använda för att bidra till att öka säkerheten i ett nätverk. När du ansluter till ett företagsnätverk som utnyttjar NAP, kontrolleras om din dator har de programvaror och inställningar som krävs och att programvarorna och inställningarna är uppdaterade. Om något saknas eller är för gammalt, uppdateras datorn automatiskt. Under den

tiden kan tillgången till nätverket vara begränsad, men normalt sker den här processen utan att du behöver göra något och utan begränsningar i tillgången till nätverket.

8.8.10 RMS (Rights Management Services)

Microsoft Windows RMS är en teknik för informationsskydd som arbetar inifrån RMS-aktiverade program för att hjälpa till att skydda digital information från obehörig åtkomst. Det gäller såväl på webben som i frånkopplat läge och både innanför och utanför brandväggen.

Med hjälp av Windows Rights Management Services-tekniken kan författaren bestämma vad läsaren kan göra med de dokument han får genom att ge dokumenten begränsade behörigheter. Dessa begränsningar är anpassningsbara, dvs en författare kan ange att en person får visa dokumentet men inte skriva ut det, att en annan kan göra båda delarna och att en tredje person kan få visa och skriva ut dokumentet, men endast i fem dagar.

Innehåll med begränsad behörighet kan skapas med program som innehåller stöd för Windows Right Management Services, till exempel Microsoft Office Professional Edition 2003. När en författare skapar ett skyddat dokument, bäddar Office även in en behörighetsbegränsad HTML-version av innehållet i filen. Dessa begränsningar gör att författarna kan förhindra att känsliga dokument, webbaserad information och e-postmeddelanden vidarebefordras, redigeras eller kopieras av obehöriga. Begränsningarna ger skydd inte bara medan informationen överförs, utan också sedan mottagaren har fått den.

8.8.11 Forefront

Microsoft Forefront Security är en helhetslösning för skydd av IT-resurser, med ett fullständigt sortiment av säkerhetsprodukter och relaterade tjänster för arbetsstationer och bärbara datorer, servrar och plattformar för meddelandehantering och samarbete. Genom en kombination av interna och externa säkerhetsmetoder ger Forefront Security det fullständiga, integrerade och förenklade skydd för IT-infrastrukturen och kan på så sätt öka säkerheten, effektiviteten samt vinsterna för ett företag.

Forefront Endpoint Protection är Microsofts skadlig kod-skydd för ett företags klient- och server-operativsystem som är enkelt att styra och kontrollera. Forefront Endpoint Protection skyddar effektivt mot olika hot exempelvis spyware, rootkits, virus, maskar och trojanska hästar. Genom att Forefront Endpoint Protection integrerar med befintlig infrastruktur inklusive ett företags AD får man ett genomgående ökat säkert skydd och samtidigt större kontroll.

Forefront Protection för Exchange Server, Forefront Protection för SharePoint och Forefront Protection för OCS är antivirus, antispam och ämnesfiltrering på servernivå som hjälper till att skydda både e-post- och samarbetsmiljöer mot virus, maskar, skräppost mm.

Forefront Online Protection för Exchange är en tjänst för meddelandefiltrering som skyddar organisationens inkommande och utgående e-post från skräppost, virus, nätfiske och brott mot e-postregler.

8.8.11.1 Microsoft Forefront Protection Manager

Microsoft Forefront Protection Manager är en heltäckande lösning för att integrera säkerhets-teknologi så att den arbetar så effektivt och automatiserat som möjligt. Inte bara Microsofts egna produkter integreras utan även tredjepartsleverantörer. Microsoft Forefront Protection Manager täcker över alla väsentliga delar i infrastrukturen och har också en intressant dynamisk respons funktion som gör att den registrerar och rapporterar aktiviteter som händer. Det som sker i en del av

infrastrukturen triggar automatiskt andra delar av infrastrukturen. Microsoft Forefront Protection Manager (tidigare ”Stirling”) kommer att bli tillgängligt under 2010.

8.8.11.2 Threat Management Gateway

Threat Management Gateway (TMG) 2010 har två huvudfunktioner; agera brandvägg samt fungera som en Web proxy och cache-server. Brandväggens funktion är att scanna alla trafik på alla nivåer (paketnivå, kretsnivå och applikationsnivå). Web cach-servern mellanlagrar och servar all upprepad webbinformation i syfte att reducera nätverkstrafik och ge snabbare åtkomst till ofta besökta webbplatser. Detta sparar tid och pengar samt ökar slutanvändarens effektivitet.

8.8.11.3 Forefront Unified Access Gateway (UAG)

Forefront Unified Access Gateway hjälper att publicera och ge åtkomst till applikationer av anställda, partners och kunder oavsett nätverk och plats. Genom att integrera en komplett SSL-VPN-server och en stark säkerhetsmotor ger UAG en säker åtkomstkontroll med stöd för stark autentisering.

8.8.12 Förslag och tips på lösenordspolicy

Ett lösenord bör vara lätt att komma ihåg och svårt att gissa och bör inte kunna hänföras till användaren. Dessa krav är motsägelsefulla, men om man tänker på en hel mening, t.ex. ”5 Fula elefanter flög till de 7 månarna” och använder de första bokstäverna i varje ord och siffrorna blir lösenordet ”5Feftd7m”. Lösenordet blir då svårt att gissa för en utomstående, men lätt för innehavaren att komma ihåg.

Nedan följer Sveriges IT-incidentcentrums, Sitics, förslag på lösenordspolicy.

- Lösenord är personliga och får inte överlåtas.
- Ett lösenord ska bestå av minst åtta tecken och bestå av minst tre av de fyra teckenuppsättningarna versaler, gemener, siffror och icke alfanumeriska tecken (specialtecken).
- Lösenordet får inte vara detsamma som användarnamnet eller bestå av delar av användarnamnet.
- Lösenordet får inte vara knutet till personlig information som till exempel namn, personnummer och telefonnummer.
- Ett lösenord får inte vara en vanlig teckenkombination, ett ord eller en vanlig kombination av ord som finns i ordböcker eller används i dagligt språkbruk, oberoende av språk.
- Ett lösenord får inte vara ett ord som är skrivet baklänges.
- En användares lösenord som används inom organisationen får inte vara likadant som andra lösenord som används utanför organisationen.
- Lösenord ska bytas var tredje månad och får inte vara likadant som ett tidigare nyttjat lösenord.
- Lösenord bör inte skrivas ned. En anteckning om lösenordet ska behandlas som en värdehandling.

8.9 Management

Inom begreppet management rymmer vi *distribution, konfiguration, övervakning, säkerhetskopiering och återläsning* samt *ärendehantering*. Det är viktigt att se till att den infrastruktur man byggt upp hanteras på ett effektivt sätt för att leverera tjänster till organisationen med gott resultat.

Vi kan inte nog understryka vikten av att ha en bra hantering av ansluten datorutrustning såsom datorer, servrar och mobila enheter inom en organisation. Genom att ha en bra rutin och automatiserad hantering och distribution av datorer, servrar, applikationer, konfiguration, inventering mm så går det att höja kvaliteten, säkerheten och att få en kostnadseffektiv plattform.

Som exempel kan vi ta en organisation som har 1000 datorer. Om man för varje dator behöver gör en manuell ”uppdatering” under 1 minut till en kostnad av 10kr så krävs alltså att denna görs 1000 gånger vilket gör att det tar tid (16h), kostar pengar (10.000kr) och riskerar att man ”missar” någon dator och miljön blir inte enhetlig, den riskerar att divergera och få olika konfigurationer. Kanske behövs det dessutom flera administrativa resurser för genomförandet. Genom att automatisera denna uppdatering och ha en hög grad av systemhantering krävs en mycket kortare administrativ insats och kostnaden blir mycket lägre. Dessutom får alla datorer samma inställning och vi vet att miljön har en enhetlig konfiguration.

8.9.1 System Center

Microsofts lösningar för management samlas under namnet System Center och är till för att hjälpa IT-administrationen att hantera sin IT-infrastruktur.

Följande huvudprodukter ingår i System Center familjen:

- Configuration Manager
- Operations Manager
- Data Protection Manager
- Virtual Machine Manager
- Service Manager

Utförlig information om de olika komponenterna finns här.

8.9.1.1 Configuration Manager (SCCM)

Microsofts systemadministrationssystem heter System Center Configuration Manager (SCCM) och har bland annat stöd för installation, konfigurering och administration av servrar, klienter och Windows Phones. Detta gäller både fysiska och virtuella miljöer. Det är med SCCM som det går att automatiskt rulla ut relevanta programvaru- och säkerhetsuppdateringar till en hel eller del av organisation.

Med SCCM finns också stöd för Network Access Protection, NAP, som innebär att klienter och servrar som kopplar upp sig mot nätverket måste motsvara organisationens säkerhetskrav vad gäller exempelvis antivirus, installerade säkerhetsuppdateringar och konfiguration av brandväggen.

Kommunen bör implementera SCCM för att hantera utrullning av nya servrar och klienter, för distribution av applikationer, konfiguration, uppdateringar och säkerhetsuppdateringar samt för inventering och underhåll.

Läs om System Center Configuration Manager här och för Microsoft Best Practices kring införande av SCCM och dess olika områden hänvisar vi till TechNet.

8.9.1.1.1 Desired Configuration Management (DCM)

Med tiden kommer kommunens datormiljö att förändras, avsiktligt eller oavsiktligt, vilket innebär att den inte längre ser ut och beter sig som förväntat. På engelska pratar vi om compliance och på svenska kan man tala om regelefterlevnad, dvs uppfyller vår IT-miljö de krav som vi ställer på den. När IT-miljön förändras kan det uppstå säkerhetsproblem eller stabiliteten påverkas. Med Desired

Configuration Management (DCM) kan vi bestämma vilken grundnivå eller vilka grundkrav miljön ska uppfylla och utföra kontroller på att alla datorer uppfyller våra grundkrav. T ex kan vi kontrollera om:

- alla operativsystem har rätt version och är konfigurerade på korrekt sätt
- alla obligatoriska applikationer är installerade och korrekt konfigurerade
- alla frivilliga applikationer har rätt konfiguration
- det finns några otillåtna applikationer installerade
- rätt programvaru- och säkerhetuppdateringar är installerade.

Den grundnivå eller de grundkrav vi vill definiera kan importeras som SCCM 2007 *Configuration Packs,* vilka kan laddas ned från Microsofts webb eller från partner.

En översikt av DCM kan du läsa om här. För Microsofts Best Practices kring införande av DCM se följande länk.

8.9.1.2 Operations Manager (SCOM)

System Center Operations Manager är Microsofts produkt för att hantera övervakning och rapportering. Med System Center Operations Manager 2007 R2 kan vi övervaka både Microsoft-, Unix- och Linuxplattformar.

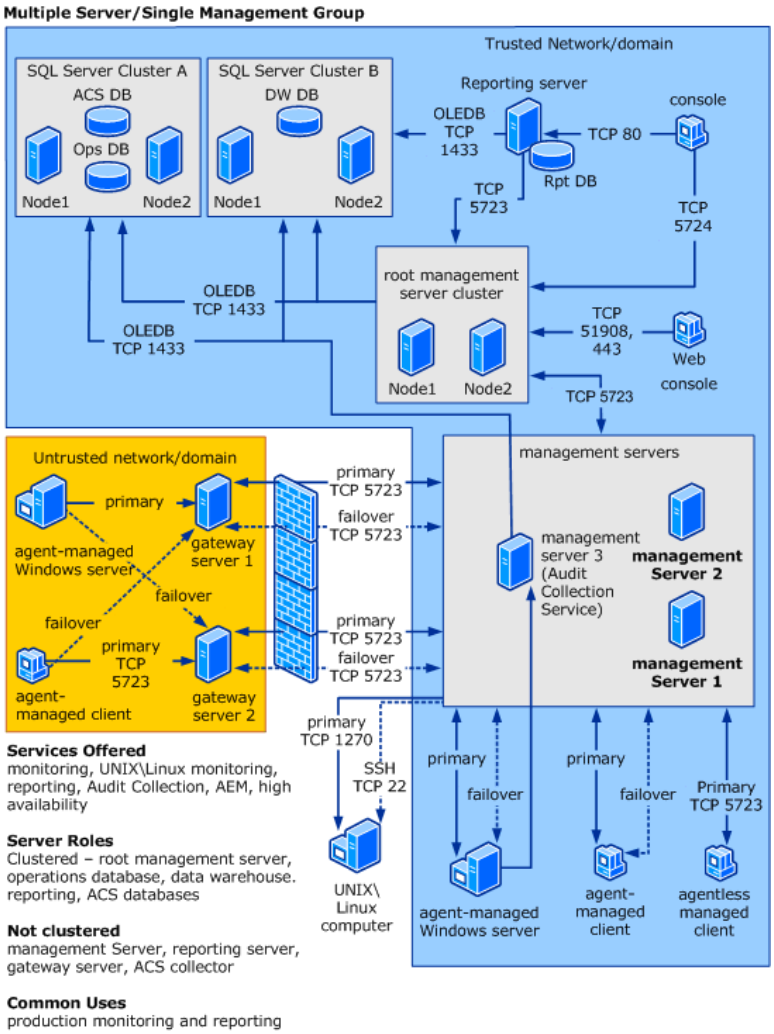
SCOM kan antingen installeras på en ensam server eller delar man upp de olika rollerna på olika servrar. Fördelarna med en installation där man delar upp rollerna på fler servrar är att man kan få ut mer funktionalitet samt att man får bättre tillgänglighet och redundans. Oberoende av arkitektur ger SCOM tillgång till tjänster som:

- Agentbaserad övervakning och larm
- Agentlös övervakning
- Rapportering
- Loggning (Audit Collection Service)
- Övervakning av klienter i olika AD (via trusts)

I en arkitektur med flera servrar får man dessutom redundans och högre tillgänglighet:

- Agent failover mellan management-servrar
- Gateway failover mellan management-servrar
- Hög tillgänglighet med klustring av databaser och root management-servrar

Bilden nedan visar en arkitektur för SCOM i en större installation:



Läs om System Center Operations Manager här och för Microsoft Best Practices kring införande av SCOM och dess olika områden hänvisar vi till TechNet.

8.9.1.3 Virtual Machine Manager (SCVMM)

Verktyget Microsoft System Center Virtual Machine Manager (SCVMM) ger omfattande stöd för hantering av virtualiserade miljöer i datacentret. Senaste versionen kallas SCVMM 2008 R2 och innehåller nya funktioner som:

- Live Migration av virtuella miljöer, dvs att flytta dem under drift och utan att det påverkar påloggade användare
- Möjlighet att utöka disklagring under drift
- Ny optimerad nätverksteknologi (Virtual Machine Queue (VMQ) and TCP Chimney)

Med VMM kan vi:

- Hantera olika typer av virtuella maskiner
  - Virtual Server 2005 R2
  - Hyper-V
  - VMware ESX
- Installera virtuella maskiner med hjälp av mallar och images

- Sköta migrering av virtuella maskiner mellan olika fysiska system
- Sköta migrering av fysiska maskiner till en virtuell miljö

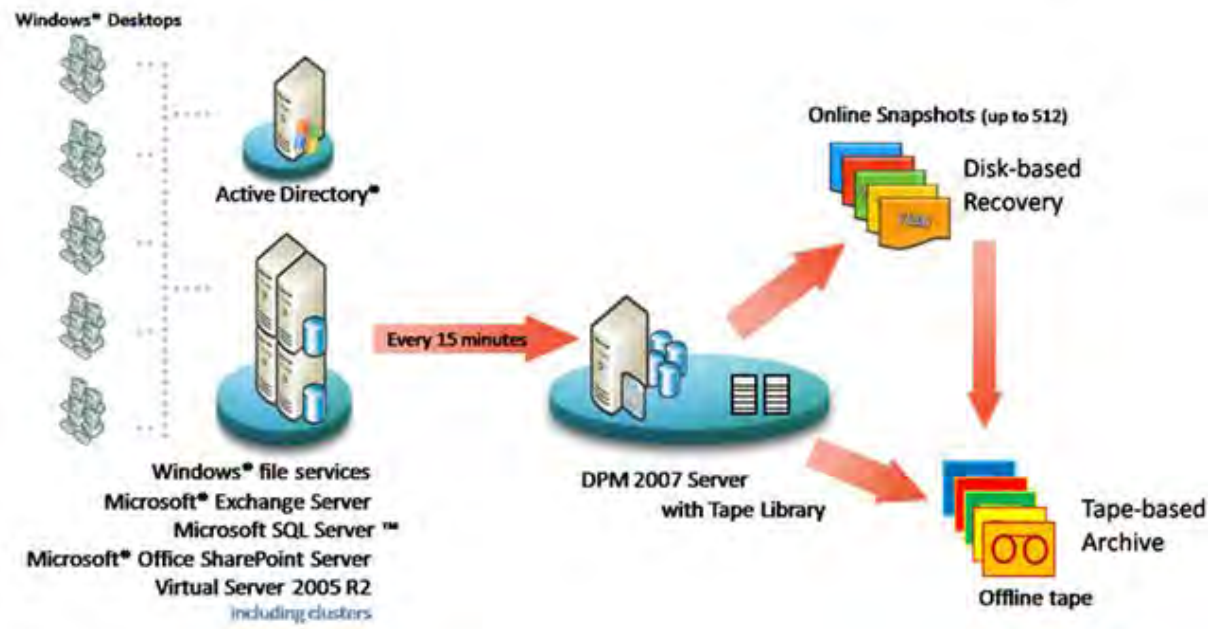
Läs om System Center Virtualization Machine Manager här och för Microsoft Best Practices kring införande av VMM och dess olika områden hänvisar vi till TechNet.

8.9.1.4 Data Protection Manager (DPM)

Data Protection Manager 2007 är namnet på Microsofts lösning för säkerhetskopiering och återläsning som kan skydda:

- Hyper-V
- SQL Server
- SharePoint
- Exchange
- System State (inklusive AD)
- filer och kataloger på Microsoft-baserade filsystem (alltså både server och PC)

På de datakällor som ska skyddas installeras en DPM protection agent. Genom att skapa olika grupper för backup styrs hur och vad agenten ska ta backup på. Backupen kan tas på upp till varje kvart till antingen disk, band eller båda. Denna backup som skapas kallas *replica* och genomförs antingen som en *disk*- eller *applikations*-backup beroende på vilken datakälla som ska skyddas. Agenten kan därefter tala om vilka förändringar som gjorts på datakällan och därefter görs endast inkrementella backuper vilket minskar tidsåtgång och datalagringsåtgång. Bilden nedan visar schematiskt hur backup går till.



Läs om System Center Data Protection Manager här och för Microsoft Best Practices kring införande av VMM och dess olika områden hänvisar vi till TechNet.

8.9.1.5 Service Manager (SCSM)

Microsoft System Center Service Manager är en integrerad plattform för att automatisera och hantera en organisations processer som t ex ITIL och MOF. SCSM stödjer ITIL-processer som:

- Incident Management
- Problem Management
- Change Control
- Asset Lifecycle Management

Genom sin CMDB kan SCSM kopplas till SCOM, SCCM och Active Directory för att hantera kunskap och information.

SCSM kan hjälpa till att reducera åtgärdstider genom att minska ledtiderna mellan larm, ärende, problem, förändring och åtgärd eftersom många steg kan automatiseras i större utsträckning. När t ex ett larm utlöses i SCOM skapas automatiskt ett ärende som kommer upp i portalen där användare och personal snabbt kan se status.

Ytterligare funktioner som gör SCSM till ett effektivt verktyg är möjligheterna till analys av snabba rapporter som automatiskt kan genereras och visa på incidenter, statistik och åtgärdstider.

SCSM har fått mycket uppmärksamhet redan idag och produkten kommer att finnas tillgängligt under första halvåret 2010.

8.9.1.5.1 Komponenter i Service Manager

Följande nyckelkomponenter finns i Service Manager:

- Workflow-motor för automatisering för processer kopplade till System Center-funktioner.
- En gemensam ”Data Warehouse” och rapporteringsplattform för System center och stöd för affärslogik (BI).
- Ett ramverk för att skapa kopplingar till System Center, andra Microsoft-produkter och tredjepartsverktyg.
- En CMDB som kan lagra information om organisationens olika IT-tjänster och komponenter och deras relation.
- En självbetjäningsportal där användarna får tillgång till tjänster i syfte att minska antal samtal och belastning på ”Service Desk”.
- En kunskapsdatabas som kan fånga, lagra och dela viktigt information som kan användas av IT-personal och användare.

Läs om System Center Service Manager här.

8.9.2 Server Management Suite Licensing

Microsoft har skapat licenspaket för de kunder som använder flera av komponenterna i System Center. Dessa paket ger en enkel och fördelaktig paketering av licenser för SCOM, SCCM, DPM och VMM. De två licenspaketen kallas Server Management Suites *Enterprise* SMSE och Server Management Suites *Datacenter* SMSD och de innehåller följande:

- Enterprise Server Management Licenses (SML) för
    - System Center Operations Manager 2007 R2
    - System Center Configuration Manager 2007 R2
    - System Center Data Protection Manager 2007
    - System Center Virtual Machine Manager 2008 R2
- System Center Virtual Machine Manager 2008 Management Server

Licenspaketen är speciellt förmånliga när man har en hög grad av virtualisering och de kan nyttjas så här:

- Server Management Suites Enterprise ger dig rätten att hantera upp till 4 virtuella instanser av OSE (Operating System Environments) på 1 fysisk server.
- Server Management Suites Datacenter ger dig rätten att hantera ett obegränsat antal OSE (Operating System Environments) på 1 fysisk server. SMSD licensieras per CPU (minimum 2 processorer).

Läs mer om licensiering i kapitel 9 Referensdesign – Licensiering.

8.9.3 MDOP

För att stödja ”Optimized Desktop” finns en paketering med managementteknologier som kallas Microsoft Desktop Optimization Pack (MDOP). För att stödja Windows 7 krävs MDOP 2009 R2.

MDOP 2009 R2 innehåller följande teknologier:

- Microsoft Application Virtualization (**App-V**) 4.5 SP1 omvandlar applikationer till centralt hanterade tjänster som inte behöver “installeras”, inte stör andra applikationer, och som strömmas vid behov till användaren.
- Microsoft Enterprise Desktop Virtualization (**MED-V**) 1.0 SP1 (tillgängligt Q1CY2010) erbjuder utrullning och hantering av Virtual PC-installationer som kan användas för att hantera applikationer som kräver ett annat operativsystem än användarens installerade.
- Microsoft Advanced Group Policy Management (**AGPM**) 4.0 erbjuder hantering och kontroll av grupprinciper (GPO) genom robust ändringshantering och rollbaserad administration.
- Microsoft Asset Inventory Service (**AIS**) är en molntjänst som samlar in inventeringsdata och översätter denna till affärsintelligens.
- Microsoft Diagnostics and Recovery Toolset (**DaRT**) 6.5 minskar stillestånd genom att påskynda klient-lagning, -återställning och -felsökning av Windowsinstallationer som inte startar korrekt.
- Microsoft System Center Desktop Error Monitoring (**DEM**) 3.5 möjliggör proaktiv problemhantering genom analys och rapportering av applikations- och systemkrascher.

Egentligen är alla ovanstående teknologier nyttiga inom ramen för MSKD. Det finns dock ett överlapp mellan molntjänsten AIS och infrastrukturlösningen SCCM där man bara behöver den ena. Likaså finns DEM både som separat komponent i MDOP likväl som inbyggd i SCOM.

App-V och MED-V är nyttiga verktyg och underlättar hanteringen av kompatibilitetsproblem vid applikationspaketering. De är dock inte nödvändigtvis en total ersättning för traditionell applikationspaketering inom ramen standardklienten (MDT) eller applikationsdistribution med SCCM utan oftast kompletterande verktyg. När App-V används för applikationspaketering har man fortfarande valet om applikationen skall distribueras som traditionellt Windows Installer-paket med SCCM eller strömmas från en App-V-server.

AGPM med sin robustare GPO-hantering är speciellt intressant för att hantera det ökade beroendet av GPO:er som följer med införandet av SDI.

8.10 Unified Communications och samarbete

8.10.1 Snabbmeddelande och närvarohantering

Med Microsoft Office Communications Server 2007 R2 och Microsoft Office Communicator 2007 R2 ger vi användarna möjligheten att på ett krypterat, snabbt och dynamiskt sätt kunna kontrollera sin in- och utgående kommunikation med t.ex. snabbmeddelanden eller VoIP. Genom närvarostatus kan användaren själv bestämma sin tillgänglighet och se andras. Till skillnad från e-posthantering erbjuder vi ett verktyg för realtidskommunikation, där användaren kan förvänta sig ett snabbt svar från motparten.

Microsoft Office Communications Server 2007 R2 kan sammanbindas (federeras) med t ex andra kommuner och organisationer, men också med Microsoft Live och andra publika IM-tjänster. Detta innebär att kommunen kan ge skolans elever och lärare möjligheten att kommunicera med varandra och externa parter med ett krypterat och kontrollerat verktyg.

Denna miljö kan också kompletteras med webbgränssnitt för internt och externt bruk, mobila användargränssnitt, telefonitjänster och webbkonferenser.

8.10.1.1 Genomförande och funktionalitet

Det är möjligt att separera skolans globala adresslistor från administrationens. En eventuell konfigurationsmodell skulle kunna vara att administrationen har elevernas adresser i sitt system, men inte tvärtom. En annan modell skulle kunna vara att lärare och skolpersonal ingår i både skolans och administrationens globala adresslistor.

Med hänsyn till spårbarhet och integritet bör man överväga att införa loggningsmöjligheter via en SQL Server, en s.k. Archiving Server. Detta ger organisationen möjlighet att i efterhand kunna ta fram dokumentation om vad som sagts och gjorts i ett visst ärende, något som är av yttersta vikt i hantering av människor inom offentlig sektor.

Inom såväl skola som administration är Live Messenger ett populärt verktyg, men det är inte den säkraste lösningen. Trafiken skickas med denna lösning okrypterad över Internet. Ett säkrare alternativ är att rulla ut Office Communicator till administrationen (och ev skolan) och sedan koppla den lokala OCS-lösningen mot PIC (Public IM Cloud). Användarna kan då lägga till sina Live Messenger-kontakter i Communicator-listan. All trafik förblir då krypterad internt och ända fram till Live-servrarna i molnet.

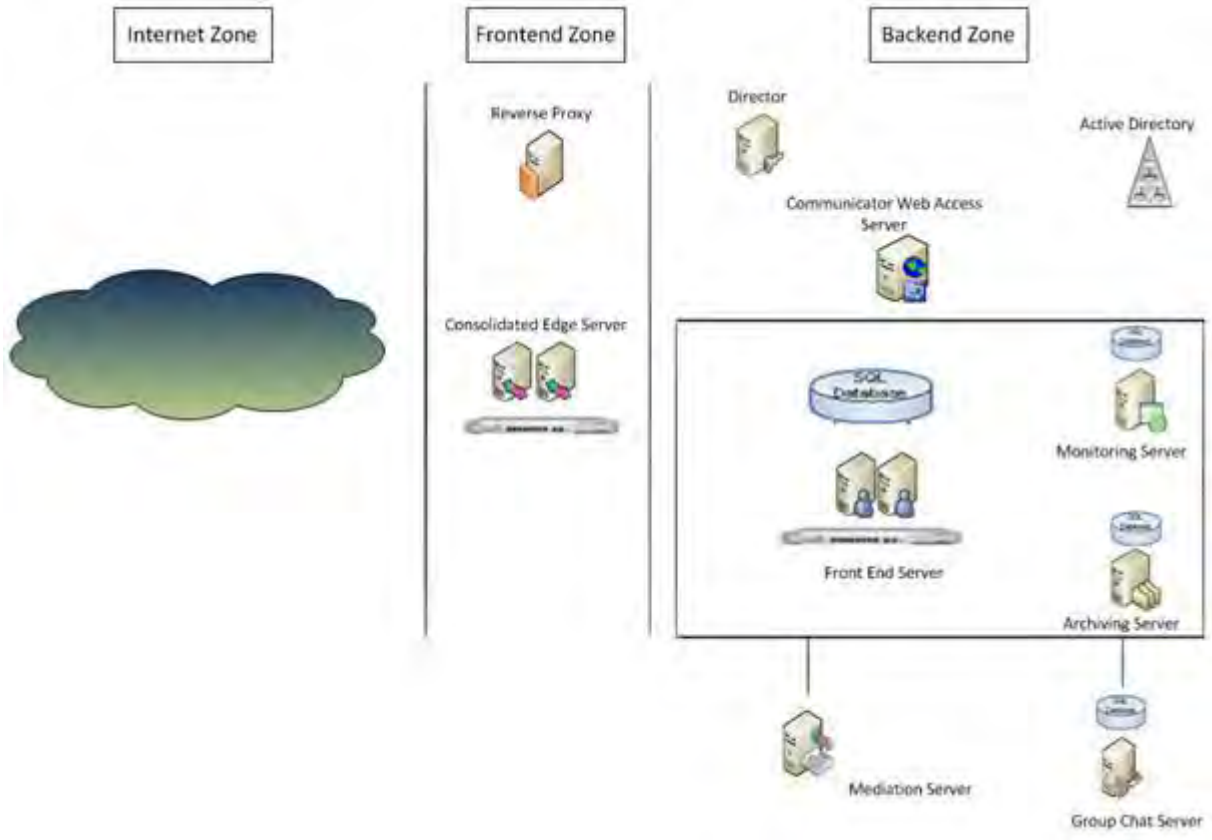
Läs mer om Microsoft Office Communications Server 2007 R2 här.
Läs om planering, utrullning och hantering av Microsoft Office Communications Server 2007 R2 här.
Notera också att under rubriken ”Microsoft Online Services” beskrivs hur kommunen kan använda sig av dessa tjänster i ett molnbaserat scenario.

8.10.1.2 OCS 2007 R2 Referensdesign

Planning Tool for Microsoft Office Communications Server 2007 R2 är ett bra stöd vid design av Unified Communications-lösningar. Det hjälper till att skala lösningen, presentera nödvändiga serverroller och annan infrastruktur och hur topologin skall se ut. Bilden nedan visar en referensdesign för en kommun med ca 1500 anställda som dagligen använder Unified Communications för snabbmeddelanden, audio- och videokonferens, grupp-chatt, övervakning och arkivering, VoIP (ca 30% av användarna), integration med SIP PBX och scenariot betjänar såväl interna som externa användare.

För att designen skall vara kompatibel med Server and Domain Isolation, har topologin som ritas upp i verktyget modifierats genom att brandväggarna mellan Internet, Edge-zonen och Backend-zonen

tagits bort från exemplet. Det enda som krävs är en Reverse Proxy och Windows som en distribuerad brandvägg.



Verktyget ger också svar på utrullningssteg, vilken maskinvarubestyckning som krävs, vilka nätverksportar som används m.m.

Ladda ned OCS 2007 R2 Planning Tool här.

Läs mer om Microsoft Office Communications Server 2007 R2 här.

Läs om planering, utrullning och hantering av Microsoft Office Communications Server 2007 R2 här.

Notera också att under rubriken ”Microsoft Online Services” beskrivs hur kommunen kan använda sig av dessa tjänster i ett molnbaserat scenario.

8.10.2 Collaboration; SharePoint 2007

Collaboration handlar om möjligheterna att etablera samarbetslösningar och portaler för att därigenom skapa verksamhetseffektivitet. Att kunna tillvarata medarbetarnas kunskapskapital är en kritisk framgångsfaktor för dagens organisationer. Detta ger inte bara kostnadseffektivitet utan också allmän kompetenshöjning och arbetsglädje. Då dagens organisationer i mycket stor utsträckning är kunskapsorienterade, så finns det också en stor risk att, för organisation viktig kompetens, försvinner om en enskild person ex vis väljer att sluta. Med väl fungerande samarbetslösningar och arbetssätt så kan risken minimeras samtidigt som kompetensspridningen ökas och effektiviseras markant.

Samarbetslösningarna ger möjligheter att etablera arbetsytor för möten, projekt, team och andra grupperingar. Möjligheter ges att hantera aktiviteter, forum, wikkis, bloggar, etc. Alla medarbetare hittar till och kan dela information på ett enkelt sätt och tillämpar ”social computing”, d v s att aktivt bidra med att dela med sig av information genom att vara med i virtuella grupper (communities),

blogga, bidra till idébanker, delta i forum, prenumerera på informationstjänster etc. Plattformen erbjuder också möjligheter till distribution av podcasts och av video exempelvis så att personal kan erbjudas utbildning när som helst och var som helst.

Genom att etablera samarbetslösningar och portaler som integreras med befintliga verksamhetssystem så utökas också värdet av redan gjorda investeringar samtidigt som utrymme och stöd skapas för en kreativ arbetsmiljö. Detta i synnerhet som användarna interagerar med samarbetslösningarna genom för dem bekanta verktyg såsom Office eller portaler baserade på exempelvis MOSS.

Referensdesign och information kring planering och arkitektur av MOSS 2007 hittar du här.
Information kring hur MOSS 2007 enklast rullas ut hittar du här.

8.10.2.1 Referensdesign satt i ett sammanhang

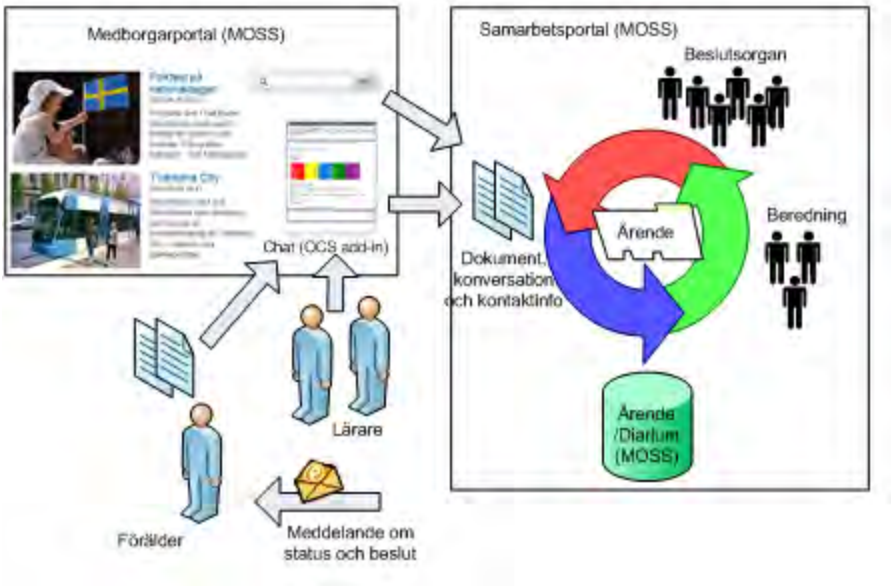
I ett framtidsscenario kommer medborgare att till mycket stor del sköta sin kommunikation med staden via elektroniska medier. Detta skulle kunna vara genom medborgarportaler på internet, kontaktcenter, skolportaler, e-blanketter etc.

Ett exempel skulle kunna vara en förälder som tar kontakt med en lärare via en *chattfunktion* i en *skolportal* för att diskutera barnets utbildning. Under dialogen så behöver ytterligare en lärare konsulteras som då bjuds in i kommunikationen. Under dialogen skickas ett antal *digitala blanketter och dokument* mellan lärarna och föräldern. Då detta har varit en mycket konstruktiv dialog, så har blanketterna skickats in i stadens system där flera *arbetsflöden* har dragits igång kring aktiviteter för barnet, men det var också så att föräldern bidrog med ett förslag på hur skolmiljön skulle kunna förbättras, vilket var något som ansågs tillämpligt på fler skolor som en generell idé. Denna idé skickades direkt vidare till ett *ärendehanteringssystem* med *hela dialogen inkl dokument och kontaktuppgifter* för de inblandade lagda som bilagor. Detta ärende gick via administrationen vidare till den *politiska processen* som ett förslag till beslut för Stadsledningen eller Stadsfullmäktige. Löpande under processen uppdateras de bidragande lärarna och föräldern om hur deras idé framskrider i den politiska processen samt slutligen det tagna beslutet.

Om någon annan parallellt med den pågående processen skulle komma på samma idé så kan denna söka via ett intelligent söksystem från portalen. Denna söklösning är också integrerad med registreringsprocessen så att inte flera ärenden dubbelregistreras utan att denna medborgare istället kan anmäla sitt engagemang till det pågående ärendet.

Scenariot visar inte bara på förändrad dialog i skolvärlden utan också hur medborgarengagemanget kan ökas genom att medborgaren på ett så enkelt sätt som från en daglig dialog där utsagan ”tänk om man istället kunde…” inte bara blir något som sägs utan att idén kan fångas och bli till ett förbättringsförslag genom ett enkelt klick. Detta samtidigt som dialogen, som förenklats och gjorts åtkomlig genom digitala medier, egentligen handlade om ett barns utbildningssituation.

8.10.2.2 Hur kan då detta realiseras?



Via en portal baserad på MOSS med ett add-in för Office Communicator, så sker dialogen. Denna konversation och dess tillhörande dokument skickas via arbetsflöden in till ett ärendehanteringssystem och samarbetsytor i MOSS. Via denna skaps aktiviteter och ytterligare dokument och handlingar relaterade till ärendet. Med regelbunden automatik skickas e-post tillbaka till förälder och lärare med status på ärendet och slutligen med beslutet.

Naturligtvis kan scenariot tillämpas inom många andra områden. Äldreomsorgen med anhöriga och vårdare, parkförvaltningen med boende och entreprenörer etc.

Observera att det inte under något steg ovan har behövts någon manuell process, förutom ev i det faktiska genomförandet. I chat-fönstret kan man naturligtvis övergå till röstbaserad kommunikation via mikrofon och hörlurar om så önskas, men ändå kunna behålla och registrera konversationen om så önskas.

8.10.2.3 Omsorg med delaktiga anhöriga

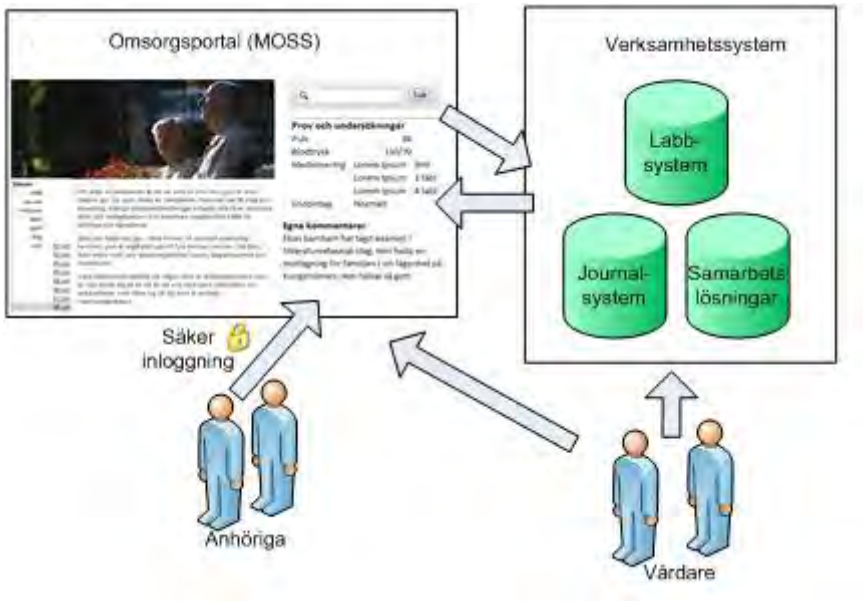
Av och till hör vi om människor som har synpunkter på omsorgen av deras äldre anhöriga. Ofta relaterar dessa synpunkter och upplevda problem till brist på information. Dagliga samtal mellan äldreomsorgen och anhöriga är inget som varken personalen eller den anhöriga har tid med även om båda parter skulle önska det. Dock behöver inte detta vara enda sättet till ökat engagemang och förbättrad information och interaktion.

Ett sätt att förbättra detta kunde vara genom en omsorgsportal där den anhöriga ges access via en säker inloggning ex vis baserad på e-id. I portalen kan den anhöriga ges information om hur läget är med dess anhörige. Viktig information och resultat från undersökningar kan delges direkt via uppdateringar från underliggande system.

En del på anhörigwebben kan också vara en wikki där personalen på ett enkelt sätt kan skapa nya inlägg på ett enkelt sätt. Basen för wikkin skulle kunna läsas upp från kommentarer o d i underliggande system för att underlätta för personalen.

Med några få rader om dagens händelser och tillstånd för den äldre omvårdade skulle informationen och interaktionen kunna ökas markant. Genom denna skulle också den anhörige kunna bidra med information och kunskap som positivt kan bidra i vården.

8.10.2.4 Hur kan då detta realiseras?



Via en portal baserad på MOSS med en webbsida uppsatt för varje åldring, så sker dialog och interaktion. Webbsiten integreras mot underliggande system där vårdarna för in kommentarer och resultat från provtagningar löpande. I Wikkin förs sedan en daglig loggbok med kort information om dagen. Till denna har också den anhöriga möjligheten att redigera och föra till information. Det kan vara information från det dagliga livet i hemmet eller andra kommentarer t ex relaterade till den direkta vården.

8.10.3 Exchange Server

Att införa, upprätthålla och bevisa regelefterlevnad för e-post är ett nyckelkrav för de flesta delarna i den offentliga sektorn.

I Microsoft Exchange Server 2007 finns nya, inbyggda funktioner som är utformade för att olika instanser ska få hjälp att kostnadseffektivt kunna följa gällande föreskrifter. Med början i den nya policymotorn har den här versionen funktioner för regelefterlevnad som till exempel förbättrad journalföring, sökning i flera postlådor, meddelandekategorisering, automatisk arkivering och radering av meddelanden samt redovisningsspårning. Organisationer kan skapa och upprätthålla de policys de behöver för sina specifika verksamhetskrav.

Microsoft Exchange Hosted Services kompletterar Exchange e-postservrar genom att hantera specifika områden inom regelefterlevnad, till exempel kryptering och arkivering.

Enkelhet vid regelefterlevnad är ett övertygande skäl att uppgradera till Exchange Server 2007.

I Appendix 3: Offentlig sektor och säker e-post, behandlas de problem med att uppfylla de krav som till exempel kommuner, landsting och myndigheter står inför. Dokumentet är skrivet utifrån intervjuer med ett flertal olika organisationer inom svensk offentlig sektor. Här visas hur offentlig sektor kan använda Microsoft Exchange Server 2007 för att snabbt införa omfattande åtgärder som uppfyller deras krav.

Exchange Server har också en betydande roll för samlad kommunikation än enbart traditionell leverans av e-post till en dator. Som exempel kan nämnas att Exchange Server 2007 kan

- Agera telefonsvarare och presentera dina röstmeddelanden direkt i inboxen

- Synkronisera e-post, kalenderuppgifter och kontakter med din smartphone
- Erbjuda Outlook Anywhere som innebär att användare kan använda den fulla Outlook-klienten för åtkomst av e-postlådan oavsett var de sitter
- Erbjuda ett rikt och dynamiskt gränssnitt för webbaserade användare (Outlook Web Access)

För planering och arkitektur av en Exchange Server 2007-lösning, läs mer här.
För utrullning och migrering till Exchange Server 2007, läs mer här och i Appendix 4.

8.10.3.1 Exchange 2010

I den senaste versionen, Exchange Server 2010, märks följande förbättringar (ett urval):

- Kraftigt förbättrad funktionalitet för e-postarkivering
- Mail Tips: få information om mottagarens status (OOF, mottagaren är en extern part m.m.) innan meddelandet skickas
- E-post kan grupperas i konversationsvyer där hela konversationer kan ignoreras
- Förhandstitt på röstmeddelanden (röst till text)
- Free/Busy-detaljer i kalendern mot externa parter

En rad förbättringar återfinns även på administrationssidan. Bl.a. optimeras Exchange Server 2010 för DAS (Direct Attached Storage), vilket möjliggör användning av större, billigare diskar, utan att äventyra lagringssäkerheten. En annan nyhet är att 2010 optimeras för Software + Services, vilket innebär att du kan komplettera din egna miljö med Exchange 2010-tjänster från molnet (BPOS), utan att användarna ser någon skillnad i var servern står.

Komplett information om Exchange Server 2010 finner du här.
Planering och utrullning av Exchange 2010 finner du här.

8.11 Microsoft Online Services

8.11.1 Business Productivity Online Suite (BPOS)

Som en komplettering till den IT-miljö som administreras i eget datacenter, finns möjligheten att på ett flexibelt sätt använda olika typer av molntjänster. Behov som med tiden växer fram, eller för tillfälliga projekt som kräver annan eller utökad kapacitet, kan tillgodoses på ett snabbt och flexibelt sätt. Molntjänsterna kan ses som en kran som öppnas eller stängs utefter de behov som finns för tillfället. I det som kallas BPOS, Business Productivity Online Suite, finns idag följande tjänster.

Microsoft Exchange Online
Microsoft Exchange Online bygger på Microsoft Exchange Server 2010 och har företagstjänster för e-post, kalendrar, övriga meddelandebaserade funktioner samt arkivering. Nya onlineanvändare kan interagera med användare på lokala servrar.
Microsoft Exchange Hosted Services (EHS) innehåller onlineverktyg som hjälper organisationer att skydda sig mot skräppost och skadlig programvara, uppfylla krav på lagring för regelefterlevnad och identifiering, kryptera data och därmed skydda konfidentialitet samt bibehålla åtkomst till e-post under och efter nödsituationer.
Microsoft SharePoint Online
Microsoft SharePoint Online bygger på Microsoft Office SharePoint Server 2010 och tillhandahåller en samlad, integrerad plats där anställda effektivt kan samarbeta med sina gruppmedlemmar, få tag i företagsresurser, söka och hantera innehåll och arbetsflöden.
Microsoft Office Communications Online

Med Microsoft Office Communications Online kan de anställda kommunicera enkelt med sina kollegor på andra kontor och i andra tidszoner via snabbmeddelanden (text), röstmeddelanden och videomeddelanden.

Microsoft Office Live Meeting

Microsoft Office Live Meeting är en webbkonferenstjänst för möten, utbildning och evenemang online via en tillförlitlig värdbaserad tjänst på företagsnivå.

8.11.2 Referensdesign för BPOS

Stegen nedan anger den allmänna ordningen för hur du går till väga. Mer information finns i dokumentationen som du når via Microsoft Online Services Administrationscenter.

- **Steg ett:** Logga in på Administrationscenter
- **Steg två:** Konfigurera tjänsterna
- **Steg tre:** Lägg till användare
- **Steg fyra:** Hämta och distribuera programmet Inloggning
- **Steg fem:** Ge slutanvändarna support

För information om säkerhet, migrering, white papers m.m., se följande biblioteksavsnitt på Microsoft TechNet

8.11.3 Live@edu

Skolan med dess elever innebär alldeles särskilda utmaningar, även bortom de rent infrastrukturella. Varje år slutar en stor kull barn och en annan kull kommer in. Ett sort antal konton försvinner och nya skall skapas. Applikationer, stödprogram och kommunikationsverktyg skall publiceras och distribueras. Barn och ungdomar som är vana med elektronisk kommunikation och stort lagringsutrymme för text, bilder, musik och video. Detta innebär mycket arbete för IT-avdelningen och kan innebära omfattande investeringar som landar i IT-budgeten.

Microsoft Live@edu erbjuder skolans samtliga elever en rad olika online-tjänster, såsom

- En Exchange-baserad e-postlösning och kalender i Microsoft Outlook Live med 10 GB lagringsutrymme, och Windows Live Mobile för e-posthantering i mobiltelefonen
- Ett utökat chattverktyg med Windows Live Messenger
- 25 GB online-lagring genom Windows Live SkyDrive
- Samarbete genom Microsoft Office Live Workspace och Windows Live Spaces

Microsoft Live@edu är helt kostnadsfritt för skolans alla elever. Arbetsbördan för IT-avdelningen minskar, inköp av lagringsmedia begränsas och samarbetsmöjligheterna mellan elever och lärare når en helt ny nivå.

Läs mer om Microsoft Live@edu här.

Konfigurering, inställningar och funktionalitet hittar du här.

8.11.4 Single Sign On/Federation

Live@edu erbjuder idag en single sign on-koppling.

För BPOS planeras en kommande uppdatering att erbjuda single sign on med ADFS 2.0. Det innebär då att ett lokalt AD används för all autentisering.

8.11.5 Lagring utomlands

BPOS tillhandahålls idag från flera olika datacentraler världen över. I Europa finns det idag datacentraler i Dublin, Irland och i Amsterdam, Nederländerna. Enligt jurister på området finns inga hinder att lagra data utanför Sveriges gränser. Ett flertal kunder inom offentlig förvaltning i Sverige använder sig idag av en eller flera av ovanstående tjänster.

8.12 Verksamhetslösningar

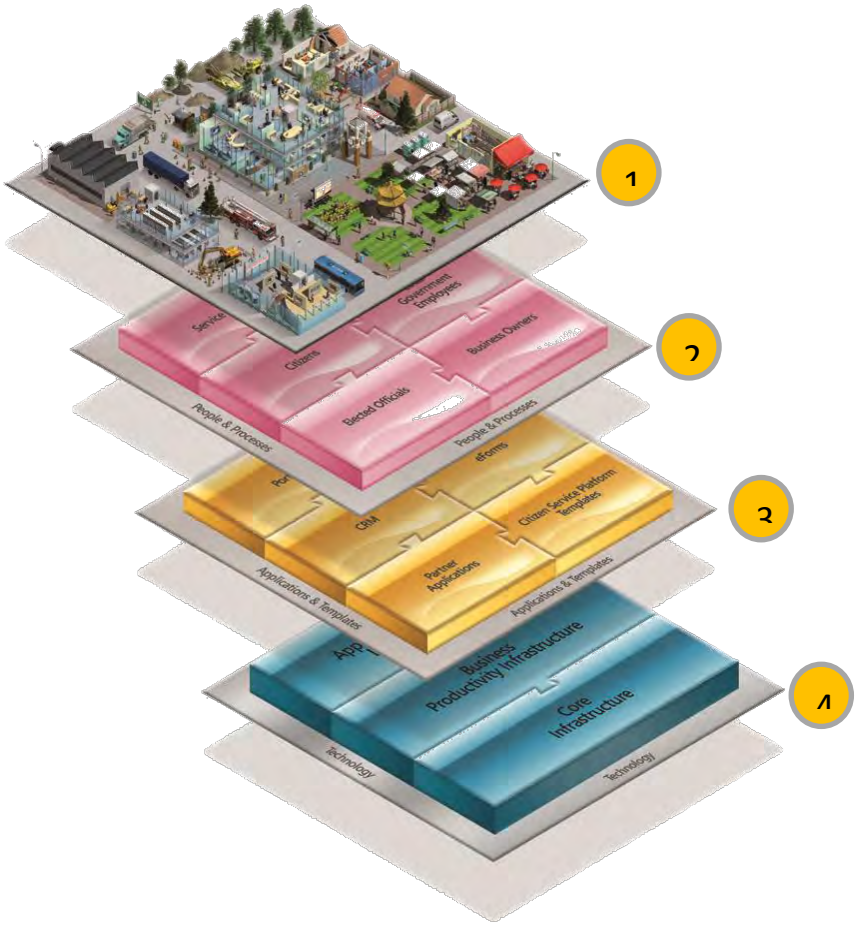
8.12.1 Microsoft Citizen Service Platform

Microsofts ramverk för kommunlösningar är baserat på den erfarenhet och de utvecklings-möjligheter vi erbjuder i Microsoft Citizen Service Platform (CSP). Den visar också på vår bredd av lösningar på ett sätt som vi tror är meningsfullt för våra kunder. CSP lanserades i april 2008.

Citizen Service Platform modellen visar de klara sambanden mellan

- De utmaningar staden/verksamheten står inför för att uppnå visionen
- De verksamhetsprocesser som behöver transformeras för att svara mot dessa utmaningar
- De IT applikationer som behövs för att stödja de processer staden transformerat
- Den underliggande IT infrastrukturen ni behöver för att stödja applikationerna på ett säkert integrerat och skalbart sätt som minimerar kostnader och komplexitet.

Microsoft har investerat i forskning i syfte att förstå kommunernas utmaningar, hur de interagerar och vilka effekter det får för kommunernas behov av ICT. Kommuner och partner över hela Europa har tillsammans med Microsofts Public Industry team medverkat och utvecklat det ramverk som CSP utgör.



Ramverket är indelat i fyra lager.

Översta lagret beskriver utmaningar och förutsättningar.

Andra lagret roller och processer. All verksamhet kretsar runt de människor och processer som är nödvändiga för att leverera den bredd av service som staden erbjuder sina medborgare.

Tredje lagret samlar de applikationer och mallar som finns tillgängliga. Microsoft- och partnerlösningar som den kommunala organisationen behöver för att agera effektivt. Från verksamhetsapplikationer till applikationer som möjliggör kvalitativa medborgar och näringslivskontakter.

Det fjärde lagret motsvarar Microsoft kommundesign och är den basinfrastruktur som kommunens tjänster baseras på

Fördelarna med att använda CSP som bas och modell i sitt förändringsarbete är att man då kan utnyttja redan utvecklade lösningar som andra städer har tagit fram tillsammans med Microsoft partners. Ledtiden för de egna projekten kan då bli avsevärt kortare och därmed också mer kostnadseffektiva. CSP är det strategiska ramverk som Microsoft och våra partner kontinuerligt kommer att fortsätta att utveckla och investera i som ett stöd för kommunala organisationer.

Läs mer om Microsoft Citizen Service Plattform här. Information om CSP referenser finns här. På följande plats finns kodexempel mm att ladda ner och testa.

8.12.2 Arkitekturer som stöds av infrastrukturen i MSKD 4.0

8.12.2.1 Cloud Computing

Med tidigare MSKD-versioner har vi konsoliderat till *ett* Active Directory (AD) per kommun. Nästa steg i konsolideringen av identitetshantering är federation. Med Active Directory Federations Services 2.0 (ADFS 2.0) på plats som en del av MSKD infrastruktur får kommunen möjlighet att köpa lösningar och tjänster i molnet utan att behöva utsätta användarna för den belastning som hanterandet av multipla identiteter innebär. Single Sign-On blir med denna teknik och lösning en självklar rättighet och ett berättigat krav som alla kan ställa på så väl programvara som tjänster (software + services).

ADFS 2.0 kommer att lanseras som en nedladdningsbar produkt för de kunder som äger Windows Server 2008 R2 licenser utan kostnad.

Läs mer om ADFS 2.0 och Cloud Computing här.

8.12.2.2 Windows Identity Foundation

Windows Identity Foundation har under utvecklingen kallats för ”Geneva Framework”. Windows Identity Foundation beskriver ramverket för att skapa applikationer som kan hantera identitets-information. Ramverket ger en abstraktion av WS-* protokollen som utvecklarna kan använda i form av API:er för att enkelt skapa integration med identiteter och säkerhetsmekanismer. WIF ramverket är främst för utvecklare som ska bygga tjänster i molnet som sedan kan konsumeras i kommunerna genom användandet av Geneva Server/ADFS 2.0 komponenterna.

För information om utveckling med ramverket WIF se följande länk på MSDN.

8.12.2.3 SOA

Tjänsteorienterad arkitektur (Service Oriented Architechture, SOA) innebär att ett distribuerat IT-system organiseras som en struktur av kommunicerande tjänster. En tjänst är här en betjänande funktion som är väldefinierad, självständig och oberoende av sin omgivning. Kommunikationen kan innebära ett enkelt godkännande av data eller involvera två eller flera tjänster som samordnar en aktivitet. I ett system uppbyggt enligt SOA är resurser tillgängliga för andra system inom ett nätverk som oberoende tjänster, och kan anropas och adresseras på ett standardiserat sätt. Syftet med SOA är att uppfylla de affärsmässiga kraven på ett IT-system. En av styrkorna med SOA är att den mer än andra tekniker uppmuntrar till att återanvända redan befintliga tjänster/system.

Med Microsofts lösningsplattform bestående av .Net framework, BizTalk, Visual studio m.fl. kan kommunen skapa en omfattande portfölj med lösningar för SOA och affärslogik som snabbt kan skapa värde för organisationen.

Läs mer om SOA-lösningar här.

8.12.2.4 Web Services

Webbtjänster (engelska Web Services) betecknar webbaserade datorprogram som kommunicerar och samarbetar dynamiskt med andra webbtjänster på samma vis som en människa kan surfa till olika webbsidor. En webbtjänst är ett datorprogram som identifieras med en URL och vars gränssnitt och bindningar kan definieras, beskrivas och upptäckas som XML-föremål. En webbtjänst stödjer direktinteraktion med andra programagenter med hjälp av XML-baserade meddelanden som utbyts via Internetbaserade protokoll.

Webbtjänster kan samarbeta med varandra automatiskt och utan avbrott. Det är möjligt eftersom webbtjänster per definition är utvecklade i enlighet med samma standarder för självbeskrivning, publicering, lokalisering, anrop, kommunikation och datautbyte.

I Microsoft plattformen används .Net ramverket för att bygga webbtjänster. Läs mer om .Net Framework här.

8.13 Migrering

Migrering av i huvudsak två funktioner kan komma att bli aktuellt för att anpassa sin IT-infrastruktur efter MSKD 4.0: e-postsystemet och katalogtjänsten.

Detta avsnitt handlar om hur man kan hantera migreringar från de vanligaste katalogtjänsterna och e-postsystemen till MSKD 4.0 (ADDS på Windows Server 2008 R2 och Exchange 2010).

8.13.1 Vad är migrering?

Definitionen av begreppet ”migrering” är inte självklart för all IT-personal.

Enligt vissa har man genomfört en e-postmigrering om man installerat ett nytt e-postsystem, skapat användarnas brevlådor manuellt, och låtit användarna ansluta till det nya systemet utan någon som helst historik i e-post, kalender eller kontakter.

Ett sådant scenario skall snarare beskrivas som en nyinstallation, eller ett systembyte, än en migrering.

En migrering är ett byte av ett system, som med minimal inverkan på användaren, ger samtliga användare full historik (t ex tidigare e-post och hemkatalog), bibehållna rättigheter på alla typer av resurser (t ex skrivare och gemensamma filer), bibehållen identitet (användarnamn och lösenord), bibehållen användarupplevelse (t ex Windows-profil eller Outlook-regler), bibehållna gruppmedlemskap (t ex distributionsgrupper och rättighetsgrupper) etc. i det nya systemet (målmiljön).

För att genomföra en migrering krävs i regel någon form av verktyg. Det kan antingen vara Microsofts egna verktyg, t ex Exchange Migration Wizard (EMW) eller Active Directory Migration Tool (ADMT), eller så kan man använda ett tredjepartsverktyg.

8.13.1.1 Om tredjepartsverktyg

Att använda tredjepartsverktyg för migrering av e-postsystem och/eller katalogtjänst är inget krav. Beslutet om vilka verktyg man skall använda avgörs av rådande omständigheter.

Komplexitet i rättighetsstrukturer, antal resurser som behöver behålla sina rättigheter, krav på samexistens och tolerans för användarpåverkan är exempel på faktorer som är avgörande i frågan.

Exempel på fördelar med att använda tredjepartsverktyg är:

- Automatisk överföring av brevlådehistorik (ingen hantering av exempelvis pst-filer, oavsett källmiljö).
- Enkel resursuppdatering (migrering av rättigheter av exempelvis DACL, SQL-rättigheter, skrivarrättigheter och brevlåderättigheter).
- Ger möjlighet till samexistens mellan system (båda för e-post och katalogtjänst).
- Ger möjlighet till snabb tillbakarullning vid oförutsedda fel.
- Spårning, loggning och överblick i migreringsprojektet vilket är avgörande om man är flertalet administratörer som utför migreringen.

8.13.2 Migrering från befintlig Active Directory-domän

Den gällande domäntopologin för MSKD 4.0 är ”en skog, en domän”. Befinner man sig inte i en domäntopologi med den utformningen så står man inför en AD-migrering för att anpassa sin infrastruktur efter MSKD 4.0.

Det går alltså inte att anpassa ett AD med felaktig topologi efter MSKD, utan ett nytt AD måste installeras, enligt beskriven praxis, till vilket man migrerar användare, grupper och resurser etc.

När det nya AD:t finns på plats börjar planeringen inför migreringen. Under planeringen gäller det att först hitta alla risker med AD-migreringen.

8.13.2.1 Exempel på risker som måste hanteras vid en AD-migrering

- Hur kommer kommunens applikationer att reagera på migreringen?

- Är resursernas rättigheter anpassade efter att skola och administration befinner sig i samma domän (delat gruppmedlemskap för ”Domain Users”)?
- Hur hanterar vi driftstopp vid migrering av servrar?
- Kan namnkollisioner uppstå i de fall man migrerar fler, separata, AD:n till ett nytt (t ex för användarkonton eller säkerhetsgrupper)?
- Hur hanterar vi bärbara datorer som är domänanslutna och behöver migreras?
- Hur kommer befintliga applikationer att reagera på de DNS-förändringar en AD-migrering innebär?

När man rett ut riskerna och hanterat dem kan man gå vidare och planera migreringen mer i detalj utifrån den specifika källmiljön.

8.13.2.2 Exempel på faktorer som uppmärksammas i en AD-migrering

- Vill man migrera samtliga resurser, datorer och användare över en natt/helg, eller önskas samexistens mellan mål- och källmiljö under migreringen?
- Hur viktig är användarupplevelsen? Är det exempelvis ett krav att användaren behåller sin Windows-profil, användarnamn och lösenord i målmiljön?
- Hur hanterar man resursuppdatering och migrering av klientdatorer? Skall exempelvis skolans datorer installeras om vid migreringen, hur hanteras i sådant fall detta?
- Vill vi förändra skrivarhanteringen i samband med migreringen?
- Skall befintliga Group Policy Objects och inloggnings-script migreras? Kommer de då i så fall vara kompatibla med målmiljön?
- Hur hanterar vi AD-rättigheter på respektive resurser, exempelvis SQL-databaser, skrivare, filsystem (DACL), Windowstjänster, COM+, schemalagda aktiviteter, IIS etc?
- Vad kommer hända med AD-integrerade system, exempelvis VPN-lösningar som är integrerade med IAS?
- Vilka användare bör delta i en pilotmigrering (vid samexistens) så att alla tänkbara fenomen kan förutses?
- Hur ska vi informera användarna om förändringen och deras påverkan?

När man gått igenom alla förutsättningar kan man genomföra en migrering.
Det är i detta skede man har tillräckligt med underlag för att kunna avgöra huruvida man kommer att kunna genomföra migreringen med eller utan tredjepartsprodukter.

8.13.3 Novell NDS-migrering

En övergång från en befintlig Novell NDS-baserad struktur till en Windows 2008 R2-baserad Active Directory-struktur kan innebära en omstrukturering alternativt ett bibehållande av en fungerande katalogtjänst (OU-design) i en ny skepnad. I båda fallen kräver detta en *migrering* (översättning och mappning) av en existerande Novell NDS-struktur då dessa inte bygger på samma rättighets- och katalogtjänstprinciper som Microsoft Active Directory.

8.13.3.1 Viktiga punkter vid en övergång från NDS till MSKD 4.0 Active Directory

- ***Val av Objekt och Migrering***
  Vilka existerande NDS-objekt (OU, Användare, Grupper) ska finnas i den nya Active Directory-strukturen?

- ***Val av Data och Migrering***
  Vilket gemensamt och personligt data ska flyttas? Vilka behörigheter ska översättas från existerande Novell-datavolymer till nya Microsoft NTFS-volymer?
- ***Ingen påverkan för användare och supportpersonal***
  Hur möjliggörs en förflyttning av alla existerande kopplingar (profiler, mappningar, genvägar, OLE-länkar) som en användare har innan en migrering?
  Hur avinstalleras Novells inloggningsklient från samtliga system?
  Hur minimera den tidsperiod som dubbla inloggningsmiljöer existerar?

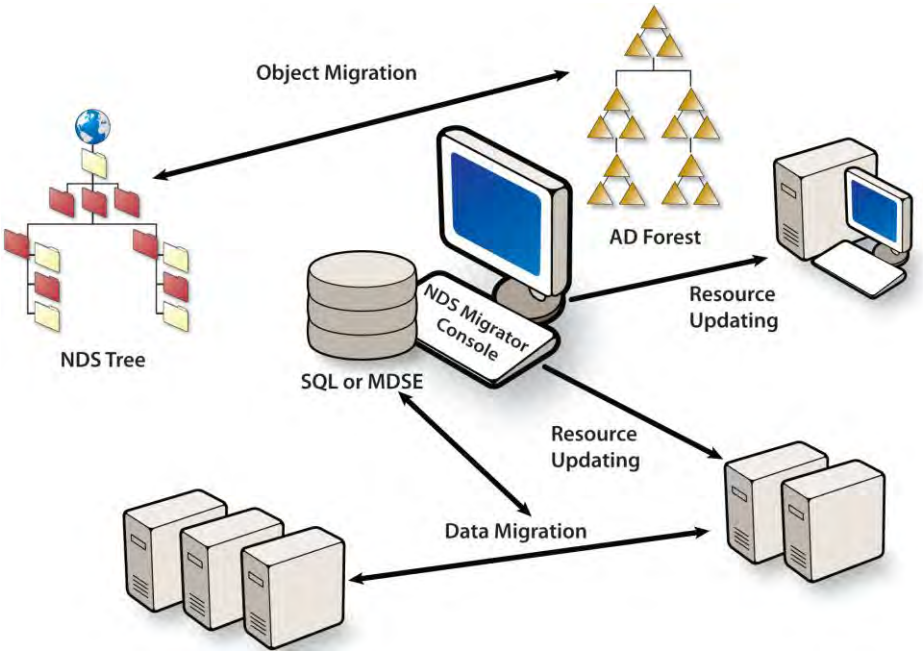
8.13.3.2 Migrering från NDS till Active Directory med Quest NDS Migrator

NDS Migrator från Quest Software är ett verktyg anpassat för att överbygga alla de olikheter som existerar mellan Novell NDS katalogtjänst och Microsoft Active Directory i samband med en migrering.

NDS Migrator ger en kontrollerad övergång med bibehållen funktionalitet mellan de båda katalogtjänsterna under den tid migreringen pågår.

Nedan sammanfattas de olika funktionerna som NDS Migrator tillhandahåller vid migreringen mellan Novell NDS och Microsoft MSKD 4.0 Active Directory:

- *Mappning och planering inför Migrering*
  Skapa kopplingar mellan OU-strukturer och objekt för kontrollerat genomförande av migrering.
- *Underlätta migrering av OU-struktur till Active Directory*
  Automatiserat återskapande av existerande OU-struktur med inkluderade objekt enligt önskemål.
- *Automatiserad migrering av användare och grupper till Active Directory*
  Välja mål OU, byta namnstandarder, inkludera gruppmedlemskap samt synkronisera förändringar av gruppmedlemskap under övergångsperioden.
- *Automatisk resursuppdatering*
  Uppdatering av användarprofiler, gruppmedlemskap, NTFS-rättigheter, enhetsmappningar, skrivbordsgenvägar och serverbaserade OLE-länkar för Word, Excel samt Powerpoint.
- *Säker datamigrering till Windows*
  Översättning av fil- och katalogrättigheter från Novellstandard (inklusive IRF) till Microsoft NTFS-standard med synkronisering under pågående migrering.



8.13.4 Migrering från Exchange

Om man befinner sig i en äldre version av Exchange kan man ställas inför två migreringsscenarion.

1. **Uppgradering.** Om Exchange finns installerat i en domäntopologi som redan är anpassad efter MSKD 4.0 handlar det om en uppgradering till Exchange 2010. Detta är en relativt smärtfri process som kräver olika mycket förberedelser och risker beroende på vilken version man ligger på. Steget från Exchange 2007 till Exchange 2010 är långt ifrån lika utmanande som en uppgradering från exempelvis Exchange 2000.
2. **Migrering.** Om Exchange finns installerat i en Active Directory-domän man planerar att migrera ifrån är utmaningen desto större. I det läget är det starkt rekommenderat att använda tredjepartsprodukter för att genomföra migreringen.

I båda fallen finns det risker och faktorer som måste hanteras under planeringsfasen för att genomföra en lyckad migrering.

8.13.4.1 Exempel på risker som måste hanteras vid en Exchangemigrering

- Hur minimerar vi risken att användare fortsätter att arbeta mot fel Exchangemiljö efter migreringen, och på så sätt går miste om inkommande e-post?
- Hur kan vi hantera en eventuell tillbakarullning, utan att gå miste om inkommande e-post, ifall migreringen skulle misslyckas?
- Vad händer om migreringen orsakar stopp på inkommande e-post för kommunens verksamhetssystem?

Migrering av e-postsystem innebär alltid risker, men de flesta är specifika för respektive källmiljö. Det är viktigt identifiera dessa inför migreringen.

8.13.4.2 Exempel på faktorer som uppmärksammas i en Exchangemigrering

- Vill man migrera alla användare över en natt/helg, eller önskar man samexistens mellan käll- och målmiljön?

- Hur skall Outlook-klienter konfigureras mot målmiljön vid migrering?
- Vad händer med klienter som använder källmiljön som SMTP-relä efter genomförd migrering?
- Skall distributionslistor migreras?
- Skall bokningsbara resurser migreras?
- Hur formulerar och distribuerar vi informationen till användarna inför migreringen?
- Vad händer med e-postintegrerade applikationer under och efter migreringen?

Beroende på hur viktigt man anser att e-postsystemet, och användarpåverkan kring det är, tar man beslut om man vill använda tredjepartsverktyg för Exchange-migreringen eller inte.

8.13.5 Migrering från Lotus Notes/Domino

Att migrera e-post från Domino till Exchange är inte komplicerat även om det finns ett antal punkter att tänka på. Man kan genomföra migreringen på olika sätt beroende på vilken nivå av samexistens man vill uppnå medan migreringen fortgår. Efter migrering kommer användarna att få med E-post, kalender, kontakter, uppgifter och rättigheter till sin brevlåda i Exchange. Man kan även föra över distributionslistor och gemensamma bokningsbara resurser.

8.13.5.1 Några saker att ha i åtanke inför en migrering från Domino till Exchange:

- Kontakter lagras lokalt på klientdator i Domino. Detta hanterar man genom att synkronisera kontakter till den centrala servern.
- Domino/Lotus Notes är ett system som ofta anpassas till kommunens behov. Ifall anpassningar är gjorda bör dessa utredas eftersom de kan störa migreringsprocessen. Ett exempel är hanteringen av bokningsbara resurser som ofta anpassas.
- Finns det andra applikationer i Domino än e-post? Applikationer som eventuellt kommer att vara kvar i Domino-miljön kan hanteras genom att man utnyttjar en terminalserver-lösning eller genom migrering till SharePoint.
- Man kan migrera brevlådedata i förtid, innan migrering, vilket ger möjlighet att utföra erforderliga tester och kontroller.
- Man strävar alltid att hålla samexistensperioden så kort som möjligt.
- Utbildning av användare krävs generellt eftersom klientprogramvaran har nytt utseende och nya funktioner. Hur kommer kommunens anställda reagera på en ny e-postprogramvara?
- Datamigreringen sker helt utan att användarna störs. Dom kan arbeta vidare som vanligt under hela processen.
- Migrering av brevlådedata sker parallellt vilket ger hög överföringshastighet.
- Ny klientprogramvara måste rullas ut.

8.13.6 Migrering från Groupwise

Groupwise är ett renodlat e-postsystem med snarlika funktioner som Exchange. Detta gör att de olika delarna (e-post, kalender, kontakter) mappar väl mot Exchange vilket gör migreringen smidig. Även distributionslistor, bokningsbara resurser och rättigheter går att föra över. Man kan även starta dataöverföringen i förtid vilket gör att man kan få en smidig övergång under en helg.

8.13.6.1 Några saker att ha i åtanke inför en migrering från Groupwise till Exchange:

- Lösenordshanteringen för migreringsverktyget fungerar på olika sätt beroende på vilken serverversion Groupwise har.
- Vidarekoppling av e-post under samexistens har sina begränsningar i Groupwise. I vissa lägen blir vidarebefordrade e-post en bilaga vilket gör det komplicerat för användarna.
- Man strävar alltid att hålla samexistensperioden så kort som möjligt.
- Utbildning av användare krävs generellt eftersom klientprogramvaran har nytt utseende och nya funktioner. Hur kommer kommunens anställda reagera på en ny e-postprogramvara?
- Datamigreringen sker helt utan att användarna störs. Dom kan arbeta vidare som vanligt under hela processen.
- Migrering av brevlådedata sker parallellt vilket ger hög överföringshastighet.
- Ny klientprogramvara måste rullas ut.

8.13.7 FirstClass

En utförlig guide för migrering från FirstClass till Exchange Server återfinns i Appendix 4: FirstClass-migrering.

9 Licensiering

Detta kapitel beskriver olika licensformer och typer av produktlicenser men inte aktuella priser. Priser kan erhållas från någon av Microsofts återförsäljare.

9.1 Nivåer

MSKD 4.0 finns i tre nivåer som i huvudsak bygger på de licenspaketeringar som finns. Följande tabell är densamma som den som finns i avsnitt 5.5.

Nivå	Infrastruktur	Klient
Basic	Windows 2008 R2 Ett AD SDI TMG 2010	Hanterad standardklient Windows 7 MDT 2010 Lite Touch
Core	Exchange 2010 SharePoint 2007 SCCM 2007 SP2	MDT 2010 Zero Touch SCCM client Office 2007 Professional Plus
Enterprise	OCS Forefront Client Security Forefront Server Security UAG	Forefront Client Security

9.2 Licenser

Mer specifikt är det följande licenser som är rekommenderade för respektive MSKD-nivå.

	Serverlicenser	**Klientlicenser**
Basic	Windows Server Threat Management Gateway	Windows Server User CAL Windows Upgrade with MDOP
Core	Windows Server Threat Management Gateway Exchange Server SharePoint Server SCCM w SQL	Professional Desktop with MDOP
Enterprise	Windows Server Threat Management Gateway Exchange Server SharePoint Server SCCM w SQL Office Communications Server Forefront Client Security Management Console w SQL	Enterprise Desktop with MDOP

9.3 Volymlicensiering

En svensk kommun med över 100 användare på administrationssidan bör köpa sina licenser genom en erkänd återförsäljare, en s.k. Large Account Reseller (LAR). LAR'arna är Microsofts partner med rättigheter att sälja Select- (Academic och Goverment) och Enterpriseavtal som redan är upphandlade via Kommentus till en specifik prisnivå. För kommuner med färre anställda än 100 på administrationssidan finns möjligheten att köpa via Open Value Government alternativt Open Value Subscription Government från den partner som de föredrar. School Agreement köps från alla partner som är certifierad Authorised Education Reseller (AER).

9.3.1 Enterprise Agreement

Varaktig licensrätt - Microsoft Enterprise Agreement löper på 3 år med årliga betalningar. EA är ett direktavtal mellan Microsoft och kunden. Samtliga datorer som ingår i avtalet skall licensieras med grundprodukter dvs en standardisering. Övriga produkter som erbjuds under ett EA-avtal kan beställas som tilläggsprodukter. Software Assurance ingår som standard i EA.

Läs mer om Microsoft Enterprise Agreements här.

9.3.1.1 True-Up

För den kund som har ett volymlicensavtal så hanteras förändringar av antalet licenser genom att en True-Up görs. Det innebär att om antalet datorer eller användare har ökat sedan den senaste rapporteringen måste en True-Up göras. Det innebär att man köper extra licenser till nya användare och/eller datorer. Det går också att göra reduceringar i avtalen vid denna avstämning.

9.3.2 Software Assurance

Sofware Assurance (SA) är Microsofts tilläggspaket för licenser som ger en rad förmåner som ger utökad funktionalitet hos vissa produkter samt stödjer varje del i en programvaras livscykel; planering, implementation, användning, underhåll och övergång.

Nedan följer exempel på SA- förmåner:

9.3.2.1 Planering

Med Software Assurance har organisationen alltid rätt till den senaste versionen av Microsofts programvara vilket gör att man i god tid kan planera för bytet till senaste programvara.

- Nya versionsrättigheter
- Fördelade kostnader

9.3.2.2 Implementation

Få hjälp av er partner med workshops eller den praktiska utrullningen av Windows/Office, SharePoint eller Exchange med hjälp av följande tjänster.

- Desktop Deployment Planning Services DDPS
- SharePoint Deployment Planning Services SDPS
- Exchange Deployment Planning Services EDPS
- Business Value Planning Services BVPS

9.3.2.3 Användning

Använd och utbilda er kring de senaste produkterna från Microsoft och bygg bättre tekniska förutsättningar för deployment och migrering.

- Enterprise-version av Windows 7 – ger tillgång till funktioner som BitLocker, DirectAccess mm.
- Training Vouchers – Utbildning hos våra utbildningspartners.
- E-Learning – Obegränsade online-kurser på klientprodukter för era medarbetare.
- Home Use Program – Möjlighet för anställda att få tillgång till Microsoft Office för hemanvändning
- Employee Purchase Program - Ger alla anställda rabatt i Microsofts online-butik.

9.3.2.4 Underhåll

- 24x7 Problem resolution support – få tillgång till Microsofts Supportservice genom SA-incidenter.
- Cold Backup for Disaster Recovery – För varje server med SA får en exakt likadan vilande (kall) finnas konfigurerad för att snabbt göra återställning av servern.
- TechNet – Ger möjlighet att utvärdera Microsofts programvara samt tillgång till nyhetsgrupper mm.

9.3.2.5 Övergång

- Windows Fundamentals for Legacy PCs – Specialversion av Windows XP som kan installeras på äldre datorer som inte stöder fulla Windows XP-kraven.
- Extended HotFix Support- Om organisationen fortfarande har gammal programvara.

9.3.3 Enrollment for Enterprise Agreement

För kunder som tecknar ett Enterprise-avtal kan man även teckna avtal för att få en effektiv prisbild för Microsofts applikationsplattform resp infrastrukturprodukter. Dessa avtalsformer ger en ökad flexibilitet för att hantera antalet licenser och ger dessutom ett effektivare utnyttjande av de produkter som ingår i avtalen.

9.3.3.1 Enrollment for Application Platform (EAP)

Med ett EAP avtal får man tillgång till site-licenser för följande produkter och kan använda dessa obegränsat inom organisationen. Därefter gör man sedan en avstämning varje eller vart tredje år av antalet produkter som man använder och tillför dem i form av True-Up.

För mer information om detta licensavtal se följande länk.

9.3.3.2 Enrollment for Core Infrastructure (ECI)

Denna avtalsform gör det möjligt att licensiera produkterna nedan per processor. En uppskattning görs vid tecknandet för antalet licenser och därefter gör man sedan en avstämning varje år av antalet produkter som man använder och genomför ev justeringar i form av True-Up.

För mer information om denna licenstyp se följande länk.

9.4 Licensing Management Suites

Microsoft har skapat licenspaket för de kunder som använder flera av komponenterna i System Center. Dessa paket ger en enkel och fördelaktig paketering av licenser för SCOM, SCCM, DPM och VMM. De två licenspaketen kallas Server Management Suites *Enterprise* SMSE och Server Management Suites *Datacenter* SMSD och de innehåller följande:

- Enterprise Server Management Licenses (SML) för
    - System Center Operations Manager 2007 R2
    - System Center Configuration Manager 2007 R2
    - System Center Data Protection Manager 2007
    - System Center Virtual Machine Manager 2008 R2
- System Center Virtual Machine Manager 2008 Management Server

Licenspaketen är speciellt förmånliga när man har en hög grad av virtualisering och de kan nyttjas så här:

- Server Management Suites Enterprise ger dig rätten att hantera upp till 4 virtuella instanser av OSE (Operating System Environments) på 1 fysisk server.
- Server Management Suites Datacenter ger dig rätten att hantera ett obegränsat antal OSE (Operating System Environments) på 1 fysisk server. SMSD licensieras per CPU (minimum 2 processorer).

Dessa licenssviter kräver inte volymlicensavtal och de innehåller alltid Software Assurance. Läs mer om licenssviterna här.

9.1 Professional Desktop

Professional Desktop är den paketering av licenser som kunder har möjlighet att köpa via Enterprise Agreement eller Enterprise Agreement Subscription. I Professional Desktop-paketeringen ingår Office Professional Plus, Windows License och en Client Access Licens-paktering kallad Core CAL. Core CAL-pakteringen innebär en rabattering av licenserna som var för sig skulle betinga ett högre pris, och består av:

- Windows CAL
- Exchange Standard CAL
- SharePoint Standard CAL
- System Center Configuration Manager CAL

9.2 Enterprise Desktop

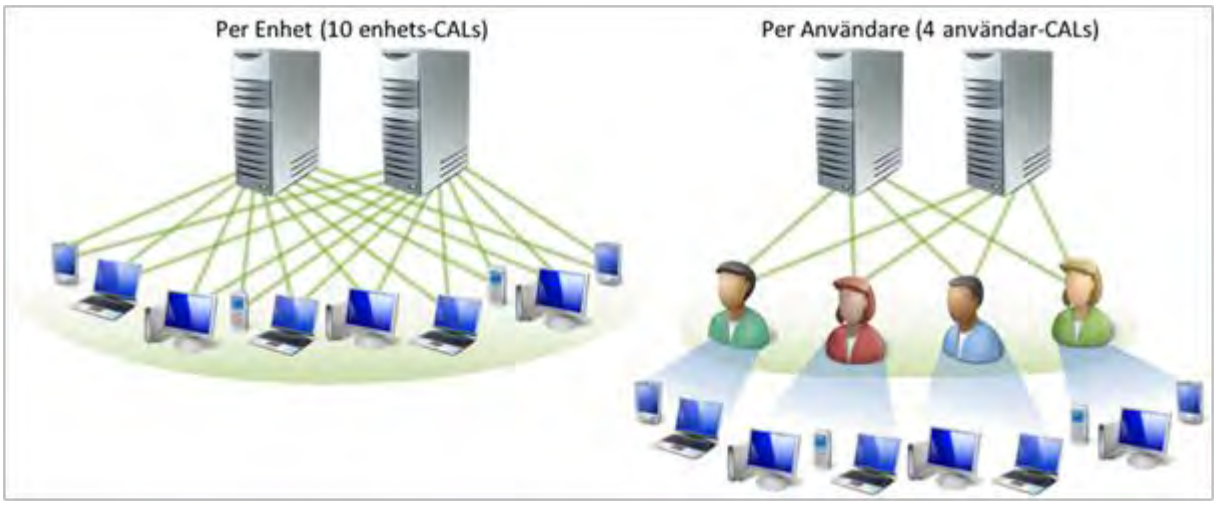
Enterprise Desktop utgörs av Microsofts mest kompletta paketering av licenser. Förutom licenserna som ingår i Professional Desktop tillkommer Office Enterprise (som i Office 2010 kommer heta Professional Plus), System Center Operations Manager Client, Windows Rights Management, Forefront Security Suite och ytterligare följande CALs:

- Exchange Enterprise Cal
- SharePoint Enterprise Cal
- OCS standard Cal
- OCS Enterprise Cal

9.3 Per User/Per Device

Traditionellt sett inom kommunerna så har man i normalfallet använt sig av enhets-licensiering (en licens för Dator, en för Laptop, en för mobiltelefon osv). Detta har sitt ursprung i att det historiskt har funnits många fler anställda än vad det funnits enheter, och av detta skäl har det varit mer ekonomiskt att licensiera per enhet istället för per användare. Nu pekar dock trenden mot att kommunerna blir mer datorintensiva och det är inte helt ovanligt att anställda har en stationär dator, en laptop, en mobiltelefon med mail-synk och en hemmadator med Outlook Web Access. I ett enhetslicensscenario innebär detta att den anställde behöver 5 licenser för att uppfylla kraven. I ett användarlicensscenario så behövs endast en licens för användaren, oavsett antal enheter.

Nedanstående bild illustrerar dessa två olika modeller, och beroende på situation och förutsättningar så är det en bedömning som får leda fram till det mest fördelaktiga sättet att licensiera. En enkel tumregel är att ju fler enheter per användare, och ju högre man önskar gå i MSKD 4.0-hierarkin för bästa värde, desto mer fördelaktigt blir det med en användarlicens.



9.4 Windows Server

Windows server 2008 R2 är grundkomponenten för MSKD och den levererar följande funktionalitet:

- ADDS
- ADCS
- ADFS
- Server and Domain Isolation
- Microsoft Deployment Toolkit (MDT)
- DirectAccess
- Virtualisering med Hyper-V
- Terminal Services

9.4.1 Virtualisering

Windows Server finns i flera versioner. De olika versionerna innehåller olika funktioner. De olika serverversionerna medger även installation av flera virtuella instanser på en licensierad fysisk server:

Windows Server Standard	1 virtuell instans
Windows Server Enterprise	4 virtuella instanser
Windows Server Datacenter*	obegränsat antal virtuella instanser

*Windows server Datacenter är licensierad per processor till skillnad från Standard och Enterprise som licensieras per fysisk server. Utnyttjar man alla virtuella instanser, medger licensieringen bara att den fysiska instansen utnyttjas för virtualisering och management av virtualiseringen. Behöver man fler virtuella instanser kan man naturligtvis köpa fler serverlicenser.

9.4.2 VDI

När man använder virtualisering för att installera och tillhandhålla Windows-klienter (även kallat Virtual Desktop Infrastructure, VDI) behöver man en extra Windows-licens som kallas VECD. Denna licens ersätter OEM-licensen som Windows Client Upgrade normalt utgår ifrån.

9.5 Threat Management Gateway 2010

Threat Management Gateway 2010 är den mjukvarubaserade brandvägg som upprätthåller säkerheten i MSKD. Den är licensierad per processor och kräver inga CALs.

9.6 Exchange Server 2010

Exchange Server 2010-licensen finns som Standard- eller Enterprise-version och kräver en CAL för varje användare.

9.7 Office

Office finns i olika paketeringar. För att stödja infrastrukturlösningarna i Exchange, Sharepoint och OCS krävs minst Office Professional Plus, som alltså är den rekommenderade versionen.

9.8 Windows Client

Windows 7 med Microsoft Desktop Optimization Pack (MDOP) licensieras per dator och rekommenderas i MSKD 4.0. I MDOP ingår bland annat App-V och MED-V som verktyg för att lösa och hantera kompatibilitetsproblem med de applikationer och verksamhetssystem som en kommun har och använder.

9.9 Skola

Grundregeln säger att alla servrar som står och utnyttjas av administration ska köpas av administration. Alla servrar som är dedikerade för skolan och inte utnyttjas eller administreras av den administrativa personalen är per definition en skollicens. En elev som ansluter till eller autentiserar sig mot en server i den administrativa eller skolmiljön ska ha CAL under något av skolavtalen.

En elev anses inte som en anställd av kommunen så man kan använda sig av enhetslicensiering för datorerna i skolmiljön och kan istället köpa Windows och Exchange External Connectors för eleverna.

10 Appendix 1: Samarbete mellan kommuner

En tydlig trend nu är att närliggande kommuner inleder samarbete inom IT-verksamheten. Drivkrafterna för denna trend är naturligtvis önskan om att uppnå en kritisk massa som gör att man kan samla tillräcklig kompetens för att bygga de lösningar som verksamheten efterfrågar och dagens teknik möjliggör. Det finns naturligtvis stordriftsfördelar, och framför allt kan man med en större volym i IT-verksamheten bemanna fler av de funktioner man har behov av. I vissa fall är samarbetet begränsat till projektsamverkan, men ofta konsoliderar man infrastrukturen till en gemensam datahall. I de fördjupade samarbetsformerna bildar man kommunförbund så att man även legalt har en gemensam organisation.

10.1 Infrastrukturdesign i ett kommunsamarbete

Frågan som ställs när man bestämt sig för att konsolidera två eller flera kommuners infrastruktur till en gemensam datahall blir då hur man skall designa den konsoliderade infrastrukturen. Skall vi bara ställa in servrarna i samma hall eller skall vi migrera ihop användarna så att vi använder samma system?

10.1.1 Active Directory-design

I MSKD utgår infrastrukturen från AD och det är där vi måste ta vårt första beslut. Skall vi ha ett gemensamt AD eller varsitt? Enligt AD Design Guide och traditionellt MSKD-tänkande skall vi (om vi har en gemensam IT-organisation som hela verksamheten kan ha ett förtroende för) ha **ett gemensamt AD**. Denna design medför då att vi måste migrera från de existerande AD och infrastrukturerna till ett gemensamt AD. Denna migrering berör alla användare och alla klienter (som inte från början är i rätt AD) och är på så vis ett omfattande IT-projekt.

Vi bör därför fundera på hur stabilt eller dynamiskt det aktuella kommunsamarbetet är. Kan det vara så att flera av grannkommunerna kommer att vilja gå med, när de ser hur bra det fungerar? Kan det bli aktuellt med andra konstellationer efter ett kommunval? Om det är så att vi kan förvänta oss förändringar i samarbetsparter och konstellationer, kanske vi inte skall bygga en statisk infrastruktur som kräver migrering vid strukturförändringar. Kommunbegreppet som sådant är fortfarande statiskt, men omfattningen av IT-samarbetet får vi nog i den närmsta framtiden räkna med vara dynamiskt och föränderligt. Den bästa strukturen blir i detta fall att **varje kommun har sitt eget AD**.

10.1.2 Federation

Eftersom kommunerna har inlett sitt IT-samarbete för att kunna fördjupa samarbetet och konsolidera gemensamma resurser i den mån samarbetet gör dem överflödiga behöver vi ändå se hur tekniken kan möjliggöra detta. Med ett gemensamt AD och därmed gemensam infrastruktur är detta inget problem, men om vi förutsätter att varje kommun har sitt eget AD får vi en utmaning. Den allmänna termen för ett lösare samarbete än ett rent samgående är *federation*. Tekniken som möjliggör federation håller på att mogna. Vi kan förvänta oss att produkter och teknologier som ADFS 2.0, Exchange 2010, OCS 2010, SharePoint 2010, BPOS, Windows Azure m fl kommer att stödja scenarion som gör att vi mellan kommuner som samarbetar, kan slå upp varandras kontaktuppgifter, se varandras kalendrar och närvaro, skicka snabbmeddelanden och ge varandra åtkomst till varandras verksamhetssystem i den mån vi önskar för att kunna verka som vikarier och göra gemensam semesterplanering mm.

11 Appendix 2 - Namnstandard

För att standardisera men också göra det möjligt att maskinellt genomföra olika saker i sin miljö (t.ex. MDT, ILM, scripts, logganalys, sortering i verktyg, uppföljning etc.) är det viktigt att införa enhetliga namnstandarder överallt där det är möjligt. Nedan följer exempel på hur det skulle kunna se ut i MSKD.

Se dessa exempel som en utgångspunkt vid design då de kan behöva anpassas för den specifika miljön. Det finns naturligtvis fler namn att standardisera på i en lösning för att få överblickbarhet och enkelhet bl.a. inför administration och övervakning, men framförallt för att på ett enklare sätt kunna bygga ut och bygga om miljön vart efter tiden går.

Försök samla denna namnstandard i centralt underhållna dokument. Det är viktigare att man har central kontroll än att namnstandarden är helt perfekt.

11.1 OU

OU:s i AD bör namngivas som allt annat i AD på ett strukturerat sätt för att det ska bli enklare att få överblick, men också för att övervakning och analys av struktur kan ske på maskinell väg. OU-namnen kommer att användas av flera automatiserade funktioner som MDT, ILM. Därför bör namnen inte överskrida 10 tecken, inte innehålla mellanslag eller specialtecken om möjligt.

Position	Funktion	Exempel
(Position 1-10)	Tydlig namngivning av OU	Servrar

Exempel: Grupper, under Grupper finns ex Edu, Adm, Klienter, Servrar, Infra, App

11.2 GPO

GPO:er i AD bör namngivas som allt annat i AD på ett strukturerat sätt för att det ska bli enklare att få överblick, men också för att övervakning och analys av struktur kan ske på maskinell väg. OU-namnen kommer att användas av flera automatiserade funktioner som MDT, ILM. Därför bör namnen inte vara men än 20 tecken långa, inte innehålla mellanslag eller specialtecken om möjligt.

Notera att GPO:er som importeras direkt från Security Guide redan har en definierade namn.

Position	Funktion	Exempel
(Position 1-3)	Anger att det är en Botkyrka byggd/anpassad GPO	bot
(Position 5-20)	Tydlig namngivning av GPO för dess funktion	bpc-smart, bpc-mobil

Exempel: bot-bpc-smart, bot-bpc-mobil

11.3 Grupper

Säkerhetsgrupper används inom lösningen för att gruppera samtliga resurser eller användare som ska ha åtkomst till en specifik resurs. Notera att en enskild person eller dator aldrig får tilldelas behörighet direkt, utan att all behörighetstilldelning måste ske via grupper. Övervakning och analys av tilldelning av behörigheter inom och utom grupper kan komma att ske på maskinell väg.

Position	Funktion	Exempel
(Position 1-3)	Anger att det är ett servicekonto	grp
(Position 5-19)	Anger säkerhetsgruppens	Buf, soc,

	funktion (Max 15 tkn långt)	
(Position 21-25)	Anger om behörighet, ex omfattar gruppen alla anställda inom ex Buf anges alla. Anges ”r” menas läsbehörighet på specifik resurs, anges ”rw” anges läs- och skrivbehörighet på specifik resurs.	Alla, r, rw

Exempel: grp-buf-alla, grp-buf-r, grp-buf-rw

11.4 Användarkonton

Fast anställd personal ges unika personliga konton som ej återanvänds om personen slutar. Notera att en person som tillhör IT-administrationen kan ha ett motsvarande IT-administrativt konto, se avsnitt nedan. Kontot ska återanvändas om personen återkommer för spårbarhet.

Position	Funktion	Exempel
(Position 1-3)	Användarens första tre bokstäver i förnamnet	ann
(Position 4-6)	Användarens första tre bokstäver i förnamnet	and
(Position 7-9)	Löpnummer, nästa lediga nummer ges till användare	001..999

Exempel: magval001, booekk001

11.5 IT-Administrativa konton, interna

Fast anställd IT-personal ges unika IT-administrativa konton som ej återanvänds om personen slutar. Notera att detta konto måste ha ett motsvarande normalt användarkonto som tillhör samma person, se avsnitt ovan om användarkonto. Kontot ska återanvändas om personen återkommer för spårbarhet. Notera att dessa konton kommer att kunna övervakas för att se hur de används i lösningen, exempelvis via ACS/SCOM.

Position	Funktion	Exempel
(Position 1-3)	Anger att det är en IT-administratör	adm
(Position 5-7)	Användarens första tre bokstäver i förnamnet	ann
(Position 8-10)	Användarens första tre bokstäver i förnamnet	and
(Position 11-13)	Löpnummer, nästa lediga nummer ges till användare	001..999

Exempel: adm-magval001, adm-booekk001

11.6 IT-Administrativa konton, externa

Inhyrd, externt anställd eller kontrakterad IT-personal som utför IT-administration ges unika IT-administrativa konton som ej återanvänds om personen slutar. Notera att detta konto måste ha ett motsvarande normalt användarkonto som tillhör samma person, se avsnitt ovan om användarkonto. Kontot ska återanvändas om personen återkommer för spårbarhet. Notera att dessa konton kommer att kunna övervakas för att se hur de används i lösningen exempelvis via ACS/SCOM.

Position	Funktion	Exempel
(Position 1-3)	Anger att det är en IT-	adm

	administratör	
(Position 5-7)	Användarens första tre bokstäver i förnamnet	Ext
(Position 9-11)	Användarens första tre bokstäver i förnamnet	ann
(Position 12-14)	Användarens första tre bokstäver i förnamnet	and
(Position 15-17)	Löpnummer, nästa lediga nummer ges till användare	001..999

Exempel: adm-ext-magval001, adm-ext-booekk001

11.7 Elevkonton

För elever och andra externa användare skapas unikt konto enligt följande regler som motsvarar vanligt användarkonto ovan. Dessa konton återanvänds ej då personen slutar. Kontot ska återanvändas om personen återkommer för spårbarhet. Notera att dessa konton kommer att kunna övervakas för att se hur de används i lösningen exempelvis via ACS/SCOM.

Position	Funktion	Exempel
(Position 1-3)	Anger att detta är ett kontor för en pedagogisk användare	edu
(Position 5-7)	Användarens första tre bokstäver i förnamnet	ann
(Position 8-10)	Användarens första tre bokstäver i förnamnet	and
(Position 11-13)	Löpnummer, nästa lediga nummer ges till användare	001..999

Exempel: edu-annand001, edu-booekk001

11.8 Konsultkonton

För extern personal som tillfälligt ges access till internt system skapas unikt konto enligt följande regler som motsvarar vanligt användarkonto ovan. Dessa konton återanvänds ej då personen slutar. Kontot ska återanvändas om personen återkommer för spårbarhet. Notera att dessa konton kommer att kunna övervakas för att se hur de används i lösningen exempelvis via ACS/SCOM.

Position	Funktion	Exempel
(Position 1-3)	Anger att detta är ett kontor för en extern användare, ex konsult, tempanställd	ext
(Position 5-7)	Användarens första tre bokstäver i förnamnet	ann
(Position 8-10)	Användarens första tre bokstäver i förnamnet	and
(Position 11-13)	Löpnummer, nästa lediga nummer ges till användare	001..999

Exempel: ext-annand001, ext-booekk001

11.9 Servicekonton

Ska namnsättas så att de är förståeliga och anger att det handlar om ett servicekonto. Se exempel nedan. Notera att dessa konton kommer att kunna övervakas för att se hur de används i lösningen exempelvis via ACS/SCOM.

Position	Funktion	Exempel

(Position 1-3)	Anger att det är ett servicekonto	svc
(Position 5-19)	Anger servicekontots funtion (Max 15 tkn långt)	Backupagent
(Position 21-30)	Servernamn (max 10 tkn något enligt servernamnstandarden)	

Exempel: svc-funktion-servernamn, svc-backupagent-servernamn

11.10 AD-Sitenamn

Ska vara 3-10 tecken som korrekt urskiljer kommunens olika fysiska platser entydigt. Denna namnstandard kommer att återanvänds för DHCP-scopenamn samt Location nedan.

Position	Funktion	Exempel
(Position 1-10)	Anger unikt platsens namn	Cen, skola1

Exempel: cen, sbot, ishallen (namnen ska vara tillräckligt entydiga inom organisationen)

11.11 Location

Används bl a ihop med skrivare och skrivarkönamnsättning (Printer Location) av användare såväl som administratörer.

Ska vara 3-10 tecken som korrekt urskiljer kommunens olika fysiska platser. Denna namnstandard kommer att återanvänds för DHCP-scopenamn och AD-Sitenamn.

Position	Funktion	Exempel
(Position 1-n)	Se bilaga 1 för exempelmatris	Cen

Exempel: Sth/Skola123/ByggnadA/Plan1, Gbg/Kommunhuset/Hus1/Plan2a

11.12 Root CA

När PKI implementeras är det lämpligt att namnge den egna organisationsspecifika CA-infra-strukturen på ett strukturerat sätt då detta namn initialt kommer att synas internt men också kan komma att används externt. Detta för att kunna bättre övervaka certifikatsanvändning och administration.

Position	Funktion	Exempel
(Position 1-20)	Anger unikt organisationens namn samt att det är frågan om en Root CA	Kommunen

Exempel: PajalaRootCA

11.13 Utgivade CA

När PKI implementeras är det lämpligt att namnge den egna organisationsspecifika CA-infra-strukturen på ett strukturerat sätt då detta namn initialt kommer att internt men också kan komma att används externt. Detta för att bättre kunna övervaka certifikatanvändningen och administration.

Notera att organisationen kan ha en eller flera utgivande CA för olika ändamål och/eller redundans.

Position	Funktion	Exempel
(Position 1-4)	AD-siteplacering av resurs (max 4 tkn långt). Se även AD-sitennamnstrandard för detta fälts namngivning	cen

(Position 5-7)	Anger att det är en serverresurs men anger inte dess funktion av säkerhetsskäl (alltid = srv) (eventuellt = uca om det är en Utgivande CA som kan komma att finnas kvar länge)	srv eller uca
(Position 8-10)	Unikt Löpnummer på servern	001..999

Exempel: cenuca001, censrv100

11.14 Certifikatmallar/PKI

När PKI implementeras är det lämpligt att konstruera egna organisationsspecifika certifikatsmallar som utgår från en befintlig standardmall (om och när en standardmall uppdateras kan det få oönskad effekt, jämför med hur standard-GPOer används).

Denna kopiering görs också för att eventuellt kunna justera parametrar samt övervaka certifikats-användning/utdelning effektivt/maskinellt.

Position	Funktion	Exempel
(Position 1-3)	Anger unikt organisationens namn förkortat	sth
(Position 4-20)	Certifikatets ursprungsmall anges här så att det är tydligt vilken mall/användningsområde certifikatet avser	Computer, Dccert

Exempel: sth-computer, gbg-IPsec, lul-efs, udd-ssl

11.15 Skrivarnamn

Skrivarens fysiska namn namnges exakt som dns-namnet för att underlätta administration och maskinell övervakning.

Notera att klienter/servrar aldrig ansluter direkt till skrivaren utan går via logiskt namnsatta skrivarköer som dessutom har en ”Location”-text som fylls i på förhand och som kan sökas på i AD från alla klienter och servrar.

Position	Funktion	Exempel
(Position 1-10)	Sitenamn	Cen, skola1
(Position 11-13)	Ander att det är en skrivare	Prn
(Position 14-17)	Unikt ordningsnummer	0001-9999

Exempel: cenprn0001, skola1prn0010 med ett FQDN: skola1prn0010.kommun.se

11.16 Skrivarkönamn

Skrivare ska i första hand hittas och kommas åt via skrivarkönamnet i AD. Detta namn är en kombination av skrivarkönamnet med ”Printer Location”-namnsättningen vilket gör det lämpligt att namnge skrivarkön som användare kommer hitta via AD på ett förklarande sätt.

Skrivarkönamnet behöver bara vara unikt inom respektive AD-site. Om skrivaren finns på plan 1 på Skola 1, är en HP Color Laserjet 3800 och det är en AD-site kan skrivarkönamnet vara ”Plan 1 – HP Color LJ 3800” av informationen via ”Printer Location” vet man redan att skrivaren finns på ”GBG/Skola1/Plan1”, ”STH/Stadshuset/Plan2” eller ”STH/Kommunalhuset”´.

Position	Funktion	Exempel
(Position 1-40)	Beskrivande namn inklusive våningsplan där skrivare finns, eventuellt rumsnummer samt skrivarens märke och modell	Plan 1 - HP LJ 8500, Plan3 - Rum 358 - OKI C9600GA

Exempel: ”Plan 1 – HP Color LJ 3800”, ”Plan 1 – Rum 500 – OKI C9600GA”

11.17 DHCP-scopenamn

Anges motsvarande AD-Sitenamn ovan.

Position	Funktion	Exempel
(Position 1-10)	Anger unikt platsens namn	Cen, skola1

Exempel: cen, sbot, ishallen,

11.18 Klientnamn

Position	Funktion	Exempel
(Position 1-3)	Anger att det är en administrativ klient (apc) eller en pedagogisk klient (ppc)	apc eller ppc
(Position 5-14)	Unikt Löpnummer som skapas vid klientinstallation via MDT/RIS (Max 10 tkn långt).	0000000001..FFFFFFFFFF

Exempel: apc-0000000099, ppc-0000000032

11.19 Servernamn

Unikt servernamn skapas för både fysiskt och virtuell server enligt nedanstående. Notera att enda undantaget kan vara utgivande CAs

Position	Funktion	Exempel
(Position 1-4)	AD-siteplacering av resurs (max 4 tkn långt). Se även AD-sitennamnstrandard för detta fälts namngivning	cen, skola1
(Position 5-7)	Anger att det är en serverresurs men anger inte dess funktion av säkerhetsskäl (alltid = srv) (eventuellt = uca om det är en Utgivande CA som kan komma att finnas kvar länge)	srv (uca)
(Position 8-10)	Unikt Löpnummer på servern	001..999

Exempel: censrv001,skola1srv001, cenuca001

11.20 WLAN-accesspunkt

Unikt servernamn skapas för både fysiskt och virtuell server enligt nedanstående

Position	Funktion	Exempel
(Position 1-10)	AD-siteplacering av resurs (Se även AD-sitennamnstrandard för detta fälts namngivning	cen, skola1
(Position 11-13)	Anger att det är en WLAN-accesspunkt för nätverket	nap

(Position 14-16)	Unikt Löpnummer (3tkn långt).	001..999

Exempel: skola1nap001, cennap001

11.21 LAN-nätverksutrustning

Unikt servernamn skapas för både fysiskt och virtuell server enligt nedanstående

Position	Funktion	Exempel
(Position 1-10)	AD-siteplacering av resurs (Se även AD-sitennamnstrandard för detta fälts namngivning	cen, skola1
(Position 11-13)	Anger att det är en switch (nsw), router (nro) etc.	nsw,nro
(Position 14-16)	Unikt Löpnummer (3tkn långt).	001..999

Exempel: skola1nsw001, cennro001

12 Appendix 3: Offentlig sektor och säker e-post

12.1 Sammanfattning

Att införa, upprätthålla och bevisa regelefterlevnad för e-post är ett nyckelkrav för de flesta delarna i den offentliga sektorn.

I Microsoft Exchange Server 2007 finns nya, inbyggda funktioner som är utformade för att olika instanser ska få hjälp att kostnadseffektivt kunna följa gällande föreskrifter. Med början i den nya policymotorn har den här versionen funktioner för regelefterlevnad som till exempel förbättrad journalföring, sökning i flera postlådor, meddelandekategorisering, automatisk arkivering och radering av meddelanden samt redovisningsspårning. Organisationer kan skapa och upprätthålla de policys de behöver för sina specifika verksamhetskrav.

Microsoft Exchange Hosted Services kompletterar Exchange e-post-servrar genom att hantera specifika områden inom regelefterlevnad, till exempel kryptering och arkivering.

Enkelhet vid regelefterlevnad är ett övertygande skäl att uppgradera till Exchange Server 2007.

I det här dokumentet behandlas de problem med att uppfylla de krav som till exempel kommuner, landsting och myndigheter står inför. Dokumentet är skrivet av teknisk personal från Microsoft AB efter intervjuer med ett flertal olika organisationer inom svensk offentlig sektor. Här visas hur offentlig sektor kan använda Microsoft Exchange Server 2007 för att snabbt införa omfattande åtgärder som uppfyller deras krav.

12.2 Inledning

Att följa föreskrifter finns hela tiden högt upp på dagordningen för chefer i alla branscher. Tack vare spridningen och de ständiga förändringarna av den nationella och internationella lagstiftningen, har det blivit en tung börda att tillse att alla dessa förordningar efterföljs inom hela organisationen. Inte minst gäller detta för de olika instanser som finns inom den offentliga sektorn.

Tyvärr finns det ett område av verksamheten där offentlig sektor ännu ofta inte har uppnått regelefterlevnad elektronisk kommunikation. Eftersom den största delen av organisationens kommunikation i dag sker elektroniskt, måste e-post och snabbmeddelanden hanteras och övervakas för att säkerställa att reglerna efterlevs. För att kunna följa alla aktuella förordningar måste de olika delarna inom offentlig sektor kunna följa upp, hantera, säkra och återfinna uppgifter från kommunikationen.

Ett exempel på att nya krav hela tiden tillkommer är Datainspektions krav från den 18:e December 2006 gällande att känsliga personuppgifter i e-post måste skyddas.

Delvis försvåras möjligheterna att uppfylla kraven av den ökande komplexiteten och kostnaden för att lägga till sådana möjligheter i befintliga e-post- och meddelandesystem. Detta förändras i och med att Microsoft Exchange Server 2007 finns tillgängligt. I Exchange Server 2007 finns nya och utökade funktioner för meddelandehantering inbyggda, och systemet är utformat för att organisationerna snabbt ska kunna införa och genomdriva omfattande åtgärder så att e-posthanteringen ska uppfylla kraven. I och med möjligheten att använda Microsoft Exchange Hosted Services kan till och med organisationer med begränsade IT-resurser följa föreskrifterna för sin e-post.

Vad behövs för att de olika instanserna inom den offentliga sektorn ska uppfylla kraven för e-postkommunikation? Den viktigaste komponenten är en organisationsövergripande e-postpolicy. De

ansvariga för regelefterlevnad eller riskhantering måste skapa övergripande meddelandepolicys, som utgår från gällande lagar för deras område, och som innehåller åtgärder för att uppfylla kraven.

De ansvariga för regelefterlevnad kommer att se att de flesta lagar och riktlinjer för organisationen kräver följande funktioner i e-posthanteringen för att denna ska följa e-postprinciperna:

1. **Meddelandearkivering –** De flesta instanser av den offentliga sektorn behöver möjlighet att automatiskt arkivera e-postmeddelanden under den tid som gällande lagstiftning kräver. Sökning och återställning av arkiverade e-postmeddelanden är en annan viktig egenskap. Utan såväl lämpliga policys och rutiner för arkivering och radering av e-post, som en sökfunktion, kan detta innebära stora kostnader. Bland annat från de resurser som krävs för att återställa och behandla e-post från säkerhetskopior.
2. **Kontrollerad tillgång –** En huvudkomponent i många lagar om sekretess eller integritet är skydd av privat information, liksom att hindra obehörig tillgång till vissa typer av uppgifter. Alla instanser måste kunna erbjuda säker e-postöverföring och hindra obehörigt avslöjande via e-post av vissa typer av uppgifter.
3. **Informations- och processintegritet –** Ofta krävs det att det finns åtgärder och kontroller för att säkerställa integriteten för vissa processer och typer av data. För att uppfylla kraven för e-post kan detta innebära att hanteringsanvisningar beträffande lämplig klassificering av e-post måste tillämpas eller att kopior av e-post automatiskt skickas till ansvariga för regelefterlevnad.

12.3 Uppfylla regelkrav – Microsoft Exchange Server 2007

Microsoft Exchange Server 2007 är en säker, tillförlitlig meddelandeserver för hela verksamheten, med inbyggda möjligheter för regelefterlevnad som ger en integrerad, kostnadseffektiv och hanterbar e-postlösning som uppfyller kraven. De inbyggda möjligheterna i Exchange Server 2007 tar hand om kraven på regelefterlevnad i organisationer inom finansiella tjänster, hälso- och sjukvård och andra reglerade branscher, och gör det enklare att följa principer och föreskrivna kontroller genom att filtrera, undersöka, ändra, journalföra och arkivera alla meddelanden i systemet.

Med Exchange Server 2007 får ansvariga för regelefterlevnad och e-postadministratörer till exempel möjlighet att hantera utmaningar inom meddelandearkivering, kontrollerad tillgång samt process- och dataintegritet genom att:

- Upprätta automatisk arkivering för att upprätthålla regler för arkivering, radering och spårbarhet
- Skapa e-postflödesregler för att upprätthålla krypterings- och förmedlingsprinciper
- Underlätta processen att granska meddelanden med kraftfulla nya verktyg och sökning igenom alla postlådor

Exchange Server 2007 som innehåller en uppsättning kraftfulla verktyg med vilka man kan skapa lösningar som följer e-postpolicys för sin specifika bransch och verksamhet, kan även integreras med Microsoft Exchange Hosted Services. Exchange Hosted Services hjälper till med filtrering (Anti-virus, Antispam), arkivering och kryptering på annan plats, samt tillgänglighet utanför organisationens nätverk.

12.4 Nya funktioner för regelefterlevnad inom Exchange Server 2007

I Exchange Server 2007 finns en uppsättning nya och förbättrade funktioner som är speciellt utformade för att ansvariga för regelefterlevnad och riskhantering samt e-postadministratörer ska kunna hantera och upprätthålla de policys som satts inom hela organisationen. Dessa funktioner,

tillsammans med topologiändringarna i Exchange Server 2007, gör att det går att kontrollera e-postflödet.

Administratörer kan till exempel skapa en regel som förhindrar att e-postmeddelanden som innehåller personuppgifter skickas externt alternativt att de automatiskt krypteras. Regler kan också skapas så att e-postmeddelanden som berör vissa ämnen, utifrån klassificering som tilldelas av e-postanvändarna eller administratörer, automatiskt arkiveras eller skickas till en regelansvarig för granskning.

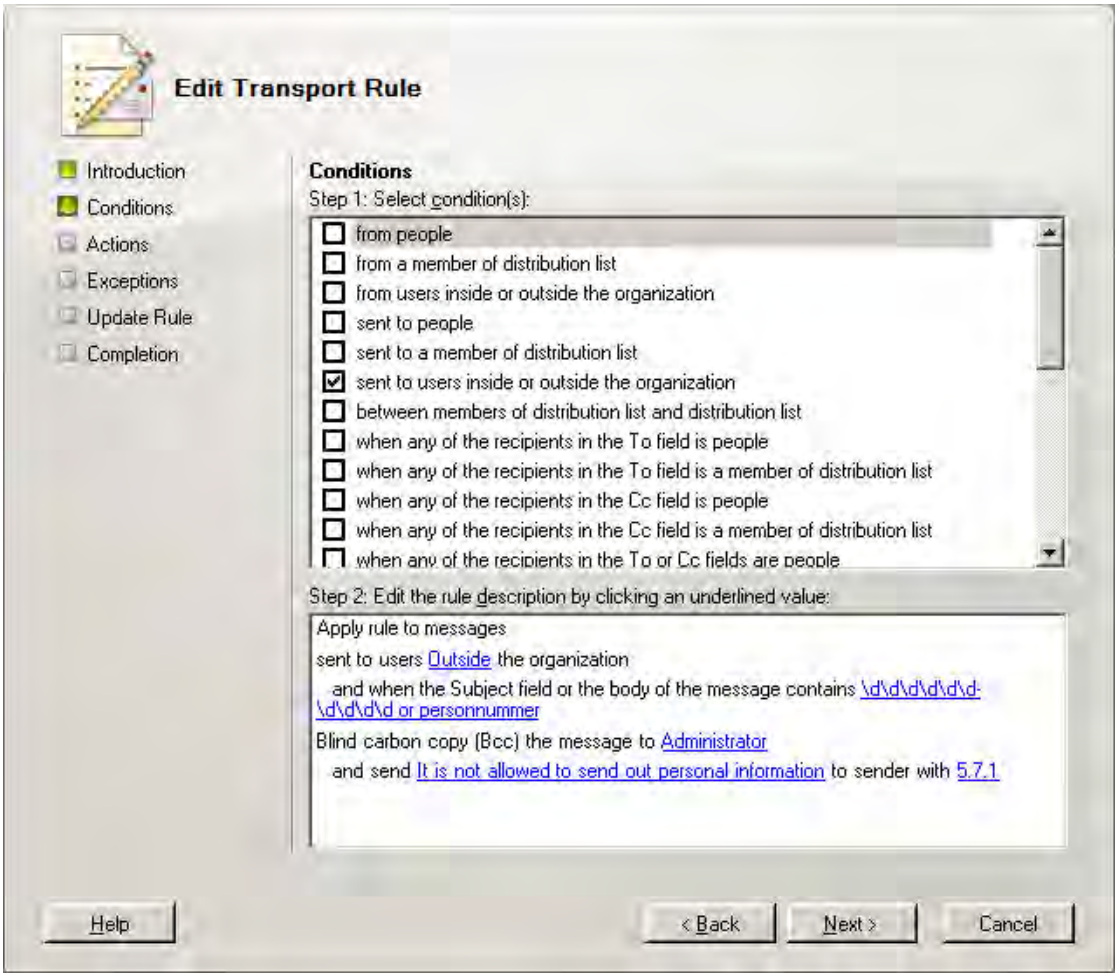
Policyhantering: Den nya policymotorn i Exchange Server 2007 hanteras genom att definiera transportregler, liknande Outlook-regler, och som enkelt skapas med Exchange Management Console. Med transportregler kan administratörer och ansvariga för regelefterlevnad upprätta och upprätthålla policys för intern eller utåtriktad e-post, röstmeddelanden och fax. Transportregler utgör en flexibel och omfattande uppsättning villkor, åtgärder och undantag som gör att administratörer och ansvariga för regelefterlevnad automatiskt kan säkerställa att reglerna efterföljs. Till exempel kan detta omfatta arkivering, kontrollerad tillgång till data, skydd av privat information och processkontroll, samt andra regler som berör regelefterlevnaden.

Med hjälp av en guide i Exchange Management Console eller kommandoraden i Exchange Management Shell kan man exempelvis skriva regler som hindrar kommunikation mellan medlemmar i olika distributionslistor, som kräver kryptering av alla meddelanden som innehåller konfidentiell information, identifierad genom matchning av text eller siffermönster, lägga till en ansvarsfriskrivning (disclaimer) i alla meddelanden som skickas externt eller skicka en hemlig kopia (BCC) till den ansvarige för regelefterlevnad när en specifik fras förekommer i meddelandets ämnesrad eller innehåll. Dessa regler kan automatiskt genomdrivas över hela organisationen.

För att åskådliggöra det här lite mer bifogas ett exempel i figur 1 nedan. I det här exemplet så har vi satt upp en regel som tittar på innehållet i alla mail som skickas till användare utanför organisationen. Ifall mailet innehåller siffror i formatet NNNNNN-NNNN eller innehåller ordet ”personnummer” så händer följande:

- Epostmeddelandet hindras från att skickas ut
- Ett meddelande skickas tillbaka till användaren och upplyser han/henne om att det inte är tillåtet att skicka ut information som innehåller personuppgifter.
- En kopia skickas samtidigt till den ansvarige för regelefterlevnad.

Figur 1. Exempel på transportregel i Microsoft Exchange Server 2007



Journalföring: Genom de avsevärt förbättrade möjligheterna till journalföring inom Exchange Server 2007 får man ytterligare flexibilitet att förenkla och effektivisera regelefterlevnad. Förutom att det nu går att införa journalföring per användare eller per distributionslista, kan administratörer automatiskt journalföra e-postmeddelanden baserat på policys med hjälp av journal- och/eller transportregler. Journalförda eller arkiverade meddelanden innehåller inte bara ursprungsmeddelandet utan också information om avsändaren, mottagarna, kopior och hemliga kopior. En annan ny funktion i Exchange Server 2007 är möjligheten att journalföra till en valfri SMTP-adress, vilket ger stöd för värdbaserade tjänster eller arkiv hos tredje part.

Meddelandearkivering: Den nya funktionen hanterade mappar gör att ansvariga för regelefterlevnad och administratörer kan skapa grupper för meddelandearkivering för att ordna och hantera e-postmeddelanden bättre. I hanterade e-postmappar finns automatisk arkivering av e-postobjekt i mappen. I en automatiserad process genomsöks inkorgen och dessa mappar för att behålla, avsluta eller journalföra kommunikation utifrån krav på regelefterlevnad. När administratörerna har skapat mapparna, kan användarna välja vilken arkiveringsgrupp, d.v.s. mapp, som gäller för ett visst objekt och Exchange Server ser till att de regler som är inställda för mapparna efterlevs.

Sökning och granskning: Tack vare Microsofts standardsökteknik är innehållet i postlådorna i Exchange Server 2007 fullständigt indexerat och sökbart med ett stort antal olika kriterier. Om informationssökning krävs för regelefterlevnad eller av lagkrav kan administratörer söka igenom flera postlådor inom en organisation med en enda fråga. Resultaten kan överföras till en postlåda som via Microsoft Outlook kan göras tillgänglig för ansvariga för juridik, personal, regelefterlevnad eller andra.

Meddelandesäkerhet: Exchange Server 2007 säkerställer ett tillförlitligt e-postflöde och skyddar känslig information under överföringen. Med kryptering, avsändarsignering och stöd för teknik att hantera rättigheter, förblir meddelanden konfidentiella både inom organisationen och på Internet.

Processintegritet: Tack vare konfigurationsloggning finns möjligheter till detaljerad redovisningsspårning, så att ansvariga för regelefterlevnad och administratörer kan uppvisa rutiner som uppfyller kraven. Alla åtgärder som en Exchange-administratör vidtar kan loggas, vilket ger dokumentation över efterlevnadsprinciper över tid. Dessutom finns statistikrapporter, där chefer och ansvariga för regelefterlevnad kan identifiera användare som inte följer reglerna. En annan ny funktion i Exchange Server 2007 är meddelandeklassificering, som gör att administratörer kan märka meddelanden för specialhantering med hjälp av förkonfigurerade eller anpassade klassificeringar, till exempel ”konfidentiellt inom organisationen” eller ”endast mellan ombud och klient”. Med en ny funktion i Outlook 2007 kan användare också klassificera meddelanden för specialhantering genom att välja bland egendefinierade kategorier. Ett inbyggt informationsfält anger de olika klassificeringarna.

12.5 Tänkbara scenarier

I följande exempel visas hur Exchange Server 2007 kan hjälpa de olika delarna inom offentlig sektor att fullständigt och kostnadseffektivt uppfylla lagkrav och organisationsprinciper som påverkar e-post och meddelandekommunikation.

12.5.1 E-postarkivering och sökning

Flera instanser inom den offentliga sektorn omfattas av stränga krav beträffande kontroll och bevarande av samt tillgång till inkommande kommunikation varav en del är e-post. Allt måste diarieföras och eftersom en stor del av kostnaderna är personalrelaterade är det ett viktigt mål att oavsett storlek minska komplexiteten och ansträngningarna för att uppfylla alla krav.

De nya inbyggda möjligheterna i Microsoft Exchange Server 2007 kan utnyttjas för att ta hand om denna utmaning. Genom att till exempel använda de nya, lättanvända transportreglerna i Exchange Server 2007 kan administratörer och ansvariga för regelefterlevnad upprätta automatisk journalföring eller arkivering av alla meddelanden som kommer in till eller lämnar organisationen. De uppgifter som kan sparas är meddelandets ursprung, mottagarna, vilka som fick kopior och vilka som fick hemliga kopior. Journalföringen kan också baseras på om avsändare eller mottagare är medlem i en viss grupp, om de är interna eller externa och andra villkor.

Administratörer kan också skapa hanterade mappar med arkiveringsregler. Användarna klassificerar sedan innehållet genom att dra objekten till hanterade mappar som till exempel ”remisser”, "Journaler” eller ”Personlig e-post”. Regler anges per mapp av e-postadministratören, vilket säkerställer att organisationens arkiveringspolicys upprätthålls och att e-posten raderas utan dröjsmål när den inte längre ska bevaras. Ansvariga för regelefterlevnad kan få kopior av e-postmeddelanden om så önskas. Administratörer och ansvariga för regelefterlevnad kan övervaka att bevarandeprinciperna följs tack vare sammanfattande rapporter om användningen.

Det finns flera olika alternativ när det gäller val av arkiv, allt från en arkivbrevlåda till en tredjepartslösning. Ett alternativ är att det går att arkivera till SharePoint 2007 som har inbyggda funktioner för att t ex diarieföra inkommande kommunikation.

För revisions- och sökningsändamål finns de utökade sökfunktionerna, som tillåter sökning genom flera postlådor. Sökresultaten kopieras sedan till en separat postlåda, till exempel hos en ansvarig för regelefterlevnad eller annan chef.

12.5.2 Säker leverans

Ett vanligt krav är att privat information måste skyddas. För att hindra avslöjande för obehöriga, måste de som hanterar till exempel patienters eller anställdas hälsouppgifter införa stränga policys för hantering av data, inklusive e-postmeddelanden.

Med Exchange Server 2007 blir det enklare för att uppfylla kraven tack vare de förbättrade möjligheterna att upprätthålla dataintegritet i e-postmeddelanden. Med allt från transportregler som tillämpar hanteringsanvisningar till kryptering av e-post och redovisningsspårning av konfigurationsändringar går det att upprätthålla e-postprinciper som förhindrar att obehöriga får tillgång till privata uppgifter.

Genom att använda guiden för transportregler kan en e-postadministratör till exempel skapa en regel som söker genom rubriken och innehållet i alla e-postmeddelanden efter ett mönster som liknar ett personnummer. Om avsändaren försöker skicka ett e-postmeddelande som innehåller ett personnummer till en mottagare utanför organisationen eller till någon som inte är definierad som behörig att ta emot konfidentiell information, skickas meddelandet tillbaka. Sedan får avsändaren ett förkonfigurerat felmeddelande.

Det går också att automatiskt kryptera e-postmeddelanden som innehåller konfidentiell information och skickas internt. Detta skyddar känslig information under överföringen utan att någon programvara behöver installeras eller användarna utbildas.

Det går också att komplettera funktionaliteten i Exchange 2007 och Exchange hosted services med Information Rights Management. Genom att göra det går det att skydda material även efter leverans genom att sätta regler på e-post eller dokument, till exempel att de inte ska kunna vidarebefodras eller att skrivas ut. För mer info se
http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx

12.5.3 Kontroll av policys

Förutom att uppfylla lagkrav bör organisationerna ha och upprätthålla policys för e-post som är baserade på erfarenheter och som går ut på att minska riskerna. Det finns ett antal inbyggda funktioner för detta bland annat:

- Tillägg av ansvarsfriskrivning i utgående meddelanden
- Skydd mot avslöjande av konfidentiell information
- Skydd mot att anstötligt språk eller innehåll skickas via e-post
- Sökning genom flera postlådor
- Automatiska policys för arkivering och radering

Med Exchange Server 2007 går det att införa och upprätthålla e-postregler som överensstämmer med de policys som är satta. Med transportregler kan administratörer välja villkor, åtgärder och undantag som kan hantera ett stort urval av möjligheter, allt från att lägga till ansvarsfriskrivningar till att filtrera bort anstötligt språk från innehållet.

En transportregel kan skapas som till exempel kontrollerar avsändare och/eller mottagare, automatiskt kategoriserar meddelandet som avsett endast för internt bruk och som därför hindras att skickas ut till en extern mottagare.

12.5.4 Microsoft Exchange Hosted Services

Exchange Hosted Services för meddelandesäkerhet och -hantering hjälper till genom att kunna uppfylla krav på regelefterlevnad och krav på extra hög tillgänglighet. Exchange Hosted Services är

idealiskt för de med begränsade resurser eller som saknar experter på regelefterlevnad. Det är lösningar som helt kan skötas utanför organisationen och arbetar ”ute på nätet” utan att någon programvara eller maskinvara behöver installeras på plats.

Bland annat innehåller Exchange Hosted Services lösningar som uppfyller krav på arkivering och kryptering. Eftersom arkiveringskrav tvingar fram att större registermängder måste bibehållas, kan tjänster som Exchange Hosted Archive göra terabyte av lagringsutrymme tillgängligt utan kostnaderna för att bygga upp och underhålla motsvarande infrastruktur på plats.

12.5.4.1 Hosted Archive-scenario

Om Exchange Hosted Archive används görs kopior av alla meddelanden när de passerar genom nätverket, och kopiorna sparas i ett datalager med förbättrad säkerhet. E-post som skickas inom organisationen fångas upp av journalföringsfunktionen i Exchange Server 2007 (och tidigare versioner av Exchange) och skickas till arkivet.

Förutom automatisk arkivering och radering av meddelanden har Exchange Hosted Archive andra nyckelfunktioner:

- Arkiv som inte kan manipuleras (meddelanden kan inte raderas före den schemalagda tiden)
- Automatisk arkivering av meddelanden, radering av utgångna meddelanden och insamling av meddelanden för granskning
- Klassificeringskategorier för granskade meddelanden med möjlighet till eskalering
- Bevisrapport: Bevis för att granskning utförs regelbundet, med uppgifter om vad som ska göras enligt schema och hur stor andel av dessa uppgifter som har utförts
- Tillfälligt avbryta radering av meddelanden
- Redovisningsspårning för rapportering av alla åtgärder som utförts inom programmet
- Sökning och återvinning vid behov för meddelanden från arkivet, med sökning efter nyckelord och fraser

12.5.4.2 Hälso- och sjukvård: Hosted Encryption-scenario

Möjligheten att dela patienters hälsoinformation mellan läkare, familjemedlemmar, husläkare, myndigheter och andra via e-post och meddelandebilagor är en viktig del i att förbättra snabbhet och effektivitet för hälso- och sjukvårdsorganisationer. Sådan kommunikation måste dock uppfylla krav på säker överföring av patientinformation. Dessa krav har visat sig vara besvärliga och dyra att uppfylla för många hälso- och sjukvårdsorganisationer, särskilt de mindre.

Med Exchange Hosted Encryption kan hälso- och sjukvårdsorganisationer garantera säker överföring tack vare kryptering av dessa e-postmeddelanden. Med en enkel process kan användarna kryptera och leverera all kommunikation utan att behöva köpa, konfigurera och underhålla komplex maskinvara eller programvara.

Genom att använda en vanlig identifierare, till exempel en e-postadress, som krypteringsnyckel ger denna lösning en enkel men mycket säker metod för kryptering av kommunikation. Användaren behöver inte vidta några ytterligare åtgärder eller några extra klickningar för att åstadkomma säker kommunikation eftersom användaren känns igen genom sin e-postadress eller inloggning.

Exchange Hosted Encryption är en kostnadseffektiv lösning och den kräver inte någon lokal hårdvara. I dagsläget finns inte tjänsten översatt till svenska.

12.6 Välja rätt lösning för regelefterlevnad

När en lösning ska väljas som uppfyller kraven för e-post, måste hänsyn tas till ett antal faktorer, inklusive de olika önskemålen och behoven hos alla potentiella inblandade: Slutanvändare, juridisk avdelning, personalavdelning, IT-drift och ansvariga för regelefterlevnad. När man har fått grepp om de interna och externa faktorerna kan man sedan utvärdera lösningar som följer reglerna för e-post och jämföra deras funktioner med kraven och organisationens filosofi.

De nyckelkriterier som ska tas hänsyn till vid utvärdering av lösningar för regelefterlevnad är bland annat:

- Möjligheter att uppfylla regelkraven på meddelandearkivering, kontrollerad tillgång samt informations- och processintegritet. Många lösningar hanterar en eller flera av dessa funktioner, men inte alla
- Minska komplexiteten vid regelefterlevnad för e-post med lättanvänd policyhantering inbyggd i lösningen
- Att endast införa de policys och regler som en bransch kräver
- Ha prestanda och tillförlitlighet som räcker till för hela organisationen
- Nära och problemfri integrering med organisationens meddelandehantering för att minska komplexiteten och ägarkostnaderna
- Ge valfrihet vid implementering mellan helt extern drift och intern lösning

Microsoft erbjuder våra kunder ett sortiment av lösningar för regelefterlevnad från Exchange Hosted Services till Exchange Server 2007 i egen regi.

Exchange Server 2007 har inbyggda funktioner och arkitekturändringarna som gör att organisationer kan hantera utmaningar i regelefterlevnad inom meddelandearkivering, kontrollerad datatillgång samt informations- och processintegritet på ett integrerat och flexibelt sätt över hela organisationen. Den har en stabil och lättanvänd verktygsuppsättning för anpassning av principer för att specifikt möta organisationens unika utmaningar inom regelefterlevnad.

Med de nya tjänsterna i Exchange 2007 behöver Exchange-kunder i de flesta fall inte leta efter tredjepartsprodukter för arkivering och e-posthantering."[1]

[1] "Microsoft Revamps Hosted-Messaging Services," Erica Rugullies, Forrester Research, 30 mars 2006, NewsFactor.com

13 Appendix 4: FirstClass-migrering

Samexistens och migrering från FirstClass till Microsofts samarbetsplattform

13.1 Sammanfattning

Idag har e-post och samarbetsfunktioner vuxit till att för de flesta företag och organisationer vara det mest affärskritiska IT-systemet i verksamheten. Att byta e-postsystem och samarbetsplattform och skapa strukturer för samarbete, datalagring och dokumenthantering, skolportal och liknande funktioner är ett och sannolikt flera omfattande projekt.

I det här dokumentet behandlas olika vägar till samexistens och migrering mellan FirstClass till Exchange Server 2007.

13.2 Strategier för att migrera

Idag har e-post och samarbetsfunktioner vuxit till att för de flesta företag och organisationer vara det mest affärskritiska IT-systemet i verksamheten. Att byta e-postsystem och samarbetsplattform och skapa strukturer för samarbete, datalagring och dokumenthantering, skolportal och liknande funktioner är ett och sannolikt flera omfattande projekt. Detta dokument ger en översiktlig bild av strategier som det går att välja mellan när man migrerar från FirstClass till Microsofts plattform för kommunikation.

Att genomföra en migrering till Windows Server System innebär ofta att man ställs inför många komplexa design- och planeringsbeslut. För det första måste en noggrann analys av befintlig miljö genomföras för att identifiera och analysera vilka befintliga funktioner och applikationer som används i dagens plattform. Även om möjligheten att migrera data via verktyg finns så kan det i vissa fall vara mer tilltalande att inte migrera några data alls eller bara delar från det gamla systemet. På så sätt går det att göra sig av med information och konton/brevlådor som inte längre används, man får ett system som är rent från gamla arv. Ett alternativ kan också vara att kombinera verktyg med att låta användarna själva avgöra vad de behöver migrera. Nedan framgår vad de olika alternativen innebär.

13.3 Mailbox-migrering med Exchange 2003 Migration Wizard

13.3.1 Inledning

Exchange 2007 har inte de inbyggda IMAP-migreringsverktygen som Exchange 2003 har, varför ett sätt att migrera data från FirstClass, eller annat Internet-Mail baserat e-postsystem, är att migrera via Exchange 2003 med hjälp av de verktygen som finns där.

För att migrera direkt från Internet-baserat e-postsystem till Exchange 2007 så finns det 3e parts IMAP komponenter, exempelvis *Mailbee.Net IMAP Component* (http://www.afterlogic.com/mailbee-net/net-imap-component.asp) som med fördel kan användas för att tillsammans med migreringsscript baserat på .Net och Monad migrera via IMAP4 protokollet.

Detta kapitel handlar primärt om migrering via Exchange 2003 till Exchange 2007, även om processerna är tämligen lika oberoende av målplattformen.

Processerna, som närmare beskrivs nedan, är:

- Installera Exchange 2003 och Exchange 2007 servers

- Samexistens mailflöde
- Katalogsynkronisering
- Migrering av data

13.3.1.1 Installera Exchange 2003 och Exchange 2007 servers

Exchange 2007 servers kan installeras i samma Exchange organisation som Exchange 2003 servers, men inte tvärt om. En stor fördel är således att först installera Exchange 2003 på minst en server för att därefter installera Exchange 2007 serverroller på annan hårdvara som skall användas framgent. Själva datamigreringen måste dock ske från FirstClass via Exchange 2003 till Exchange 2007 om man använder Native verktygen i Exchange 2003

Om man redan installerat Exchange 2007 i produktion och inte har Exchange 2003 i samma Exchange organisation sedan tidigare, så installerar man Exchange 2003 i ett eget (tillfälligt) ”migrerings AD”. Nackdelen med denna lösning jämfört med att ha Exchange 2003 & 2007 i samma Exchange organisation är att man först får migrera data till Exchange 2003 och därefter göra en Cross-Organization migrering till Exchange 2007 (se http://TechNet.microsoft.com/en-us/library/aa996926.aspx)

Fortsättningsvis antas att vi har Exchange 2003 och Exchange 2007 i samma Exchange organisation

13.3.1.2 Samexistens mailflöde

Med fördel styrs inkommande och utgående e-post om från FirstClass till Exchange 2007 i ett tidigt skede så snart Hub transport och eventuella Edge server(s) är i produktionsstatus. Följande konfigurationsordning är att föredra

1) Verifiera att konnektivitet på port 25 finns mellan både FirstClass och Exchange Hub transport-servers samt mellan Exchange Edge-servers/extern mail gateway och Exchange hub & FirstClass. Se bild 1 nedan

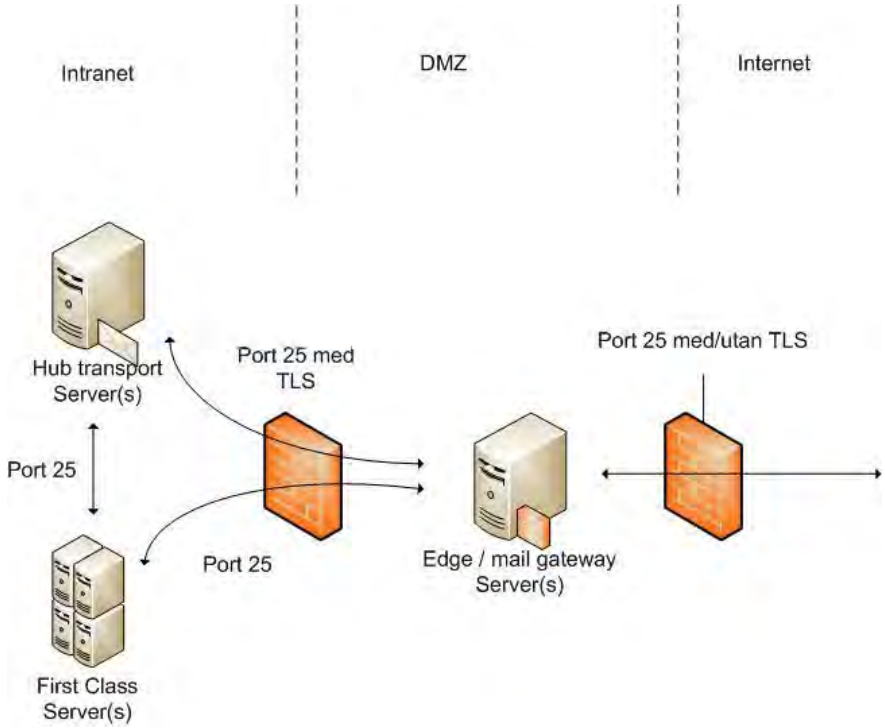


Bild 1: Verifiera konnektivitet på Port 25 mellan servrarna ovan

2) Verifiera om exempelvis TLS kryptering bör aktiveras för att öka säkerheten mellan Hub transport & mail gateway. Not: Mellan Hub Transport och Edge servers är alltid TLS aktiverat som standard
3) Aktivera/konfigurera utgående epost från Exchange 2007 mot Edge/mail gateway på DMZ
    a. Om man använder Edge servers sätts en Edge Subscription upp mellan Hub transport och Edge servers varvid Send connectors kommer skapas automatiskt.
    b. Konfigurera Internet Format för externa domainer, exempelvis character sets
4) Aktivera utgående epost från FirstClass via Exchange 2007. Genom att all inkommande och utgående SMTP trafik routas genom Exchange 2007 så blir eventuell felsökning med avseende på mailflöde enklare eftersom det är samma bärare in och ut. Dessutom minimerar det risken för mail-loopar
    a. Skapa en receive connector på Hub transport servern som accepterar SMTP från just FirstClass servrarna.
    b. Styr om utgående SMTP på FirstClass så att all mailtrafik routas via Exchange 2007
5) För att aktivera inkommande mailflöde via Exchange 2007 till FirstClass så är det mycket viktigt att veta huruvida FirstClass och Exchange 2007 delar samma SMTP domain; så är fallet i de flesta fall vid samexistens. I detta läge har vi inte några brevlådor i Exchange 2007 varför följande måste verifieras:
    a. Edge servern kan tack vare Edge subscriptions kontrollera om en mottagare finns internt i organisationen innan den processar mailet och skickar in det mot hub servern. Denna funktion måste vara avslagen, eftersom det ännu inte finns några brevlådor eller mailenablade objekt i organisationen. Inställningen ändras på Edge servern under i Recipient Filter agent.
    b. I Exchange Management Console under Accepted Domains, skall den delade SMTP domainen sättas som ”Inbound relay”. Detta möjliggör att mail som kommer till Exchange, men där det inte finns någon mottagare kommer skickas vidare i stegen nedan
    c. Skapa en Send connector på Hub transport rollen som pekar mot FirstClass servern och sätt ”Accepted domains” till den delade SMTP domainen. Genom detta och steg b) ovan kommer mail som inte har en adressat i Exchange att automatiskt vidarebefordras till FirstClass

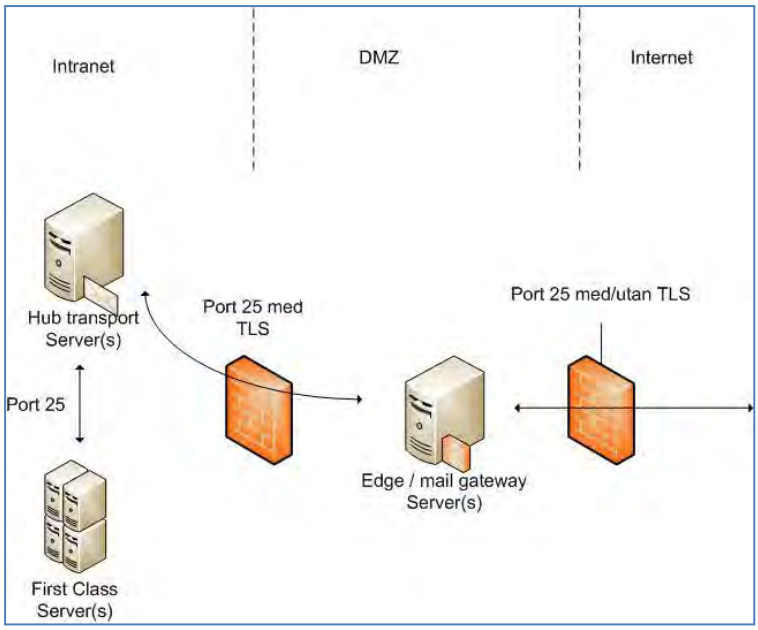


Bild 2: Mailflöde efter konfigurering enligt stegen ovan

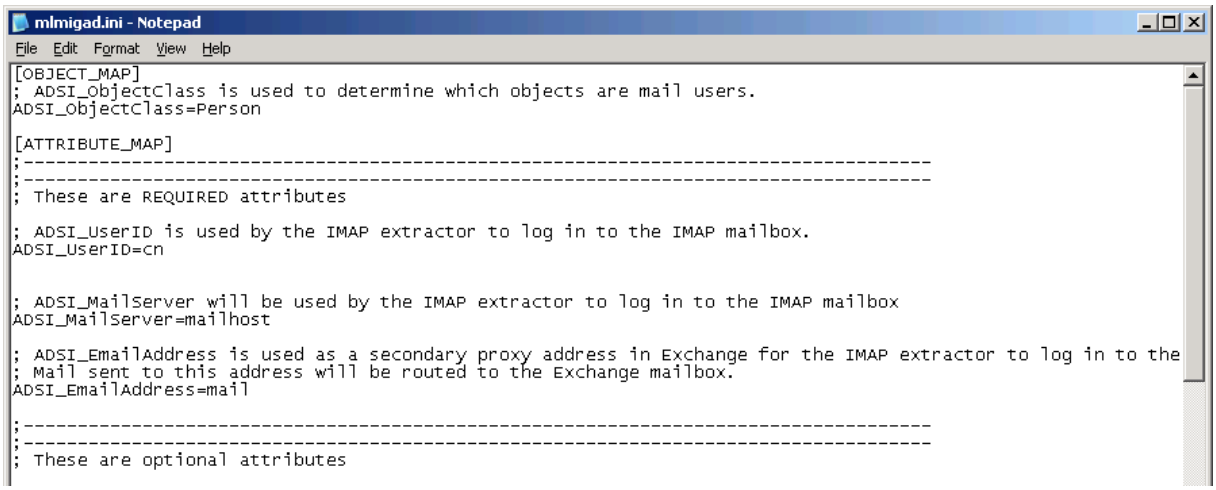
Not: För att mailflöde mellan FirstClass och Exchange skall fungera när brevlådor finns i båda systemen, så måste varje brevlåda i Exchange stämplas med en dummy-SMTP-adress, exempelvis <alias>@legacy.fabrikam.com. Denna adressen skall anges i Accepted Domains i Exchange 2007 som Authoratative domain, dvs en domain som Exchange 2007 tar ägarskapet över.

13.3.1.3 Katalogsynkronisering

FirstClass baseras på en LDAP katalog varför det finns ett flertal sätt att synkronisera AD/Exchange med FirstClass LDAP katalog. MIIS är ett alternativ om samexistens kommer ske under längre eller obestämd framtid. Andra alternativ är exempelvis att använda Active Directory verktyg såsom Ldifde.exe samt Csvde.exe för att skapa manuell synkronisering eller bulk import/export. Om man utöver ovanstående även scriptar i Vbscript så kan processen ges en mer automatiserad synkroniseringsprocess.

Ett i regel fullgott alternativ är att använda Exchange Migration Wizard i Exchange 2003. Med Migration Wizard kan man extrahera LDAP katalogen i FirstClass. Exchange Migration Wizard antar att användarkonton är av typen inetOrgPerson, men för FirstClass används Person. Editera mlmigad.ini (C:\Program Files\Exchsrvr\bin) och ange den objekt class som används i ADSI_ObjectClass

Nedan: Headern på mlmigad.ini



13.3.1.4 Tabell 1 Mlmigad.ini parametrar för LDAP directory export

Parameter	Standardvärden	Active Directorys motsvarighet
ADSI_ObjectClass	inetOrgPerson (FirstClass: Person)	organizationalPerson
ADSI_UserID	Uid (FirstClass: cn)	cn or sAMAccountName
ADSI_MailServer	mailhost	Mailhost
ADSI_EmailAddress	mail	Mail
ADSI_FullName	Inte angett	displayName
ADSI_FirstName	givenname	givenName
ADSI_LastName	sn	Sn
ADSI_Initials	initials	Initials
ADSI_NickName	uid	mailNickname
ADSI_Title	title	Title
ADSI_Company	Inte angett	company
ADSI_Department	ou	department

ADSI_Office	roomnumber	physicalDeliveryOfficeName
ADSI_PostalAddress	postaladdress	streetAddress
ADSI_City	l	L
ADSI_StateOrProvince	st	St
ADSI_PostalCode	postalcode	postalCode
ADSI_Country	Inte angett	Co
ADSI_TelephoneNumber	telephonenumber	telephoneNumber
ADSI_TelephoneNumber2	Inte angett	otherTelephone
ADSI_TelephoneHome	homephone	homePhone
ADSI_TelephoneHome2	Inte angett	otherHomePhone
ADSI_TelephoneMobile	mobile	mobile
ADSI_TelephonePager	pager	Pager
ADSI_TelephoneFax	facsimiletelephonenumber	facsimileTelephoneNumber
ADSI_AssistantName	secretary	assistant
ADSI_AssistantPhone	Inte angett	telephoneAssistant
ADSI_AlternateAddress	mailalternateaddress	proxyAddresses
ADSI_Comment	description	Info

När man kör LDAP exporten ”Migration from Internet Directory (LDAP via ADSI)” – ”Extract Migration Files Only” i Migration Wizard skapas en directory.pri som innehåller de användare man valt i exporteringsprocessen. Viktigt att man i detta läge dels har access till FirstClass servern på port 389, liksom att man har admin rättigheter i FirstClass (Standard är användarid Admin, med lösenord Admin). RUS i Exchange 2003 måste fungera för att de nyskapade objekten skall få en korrekt SMTP-standard.

Gör om filen till en LDF fil som kan användas av LDIFDE så att det skapas mailenablade AD-konton.

Nedan: Exempel på information i LDF-filen för import i AD

```
dn: CN=Hao Chen,OU=Remote SMTP Recipients,DC=fabrikam,DC=com
changetype: add
objectClass: contact
cn: Hao Chen
sn: Chen
givenName: Hao
displayName: Hao Chen
mailNickname: Hao
targetAddress: SMTP: Hao@legacy.fabrikam.com
mail: Hao@fabrikam.com
```

Kör LDIFDE enligt följande exempel: ” ldifde -i -f c:\importfile.ldf -s Server01.”

13.3.1.5 Migrering av data

Not: Migrering av data via IMAP fungerar mycket bra, men endast epost i FirstClass foldern ”Mailbox” migreras.

1) Öppna upp IMAPUSR.CSV som ligger i foldern som Migration Wizard skapat vid extrahering av FirstClass katalogen
2) Editera filen och ange
    a. Rätt lösenord till respektive brevlåda i FirstClass (attributet IMAP_Password)
    b. Rätt IP-adress till FirstClass servern (attributet IMAP_Server)
3) Starta Migration Wizard och välj Migrate from Internet Mail (IMAP4)
4) Välj i regel One Step Migration och peka ut sökvägen till migreringsfilerna
5) Ange en Exchange 2003 server och databas som data skall migreras till
6) Peka ut IMAPUSR.CSV filen
7) Välj att skapa brevlådor och om allt data eller bara viss tidsperiod skall migreras
8) I slutet av wizarden får man ange hur lösenorden skall skapas för nyskapade konton

9) När migrering av data har slutförts i denna batch, så är **skall en forward sättas i FirstClass** så att mail som skickas inom FirstClass automatiskt vidarebefordras till Exchange. Detta för att säkerställa att nya mail bara kommer till Exchange och inte till FirstClass brevlådan.
10) Migrera slutligen brevlådan från Exchange 2003 till Exchange 2007 genom att använda Exchange 2007 Management Console.

13.4 Mailbox migrering utan att använda sig av Mailbox migreringsverktyg

Även om möjligheten att migrera mail via Exchange 2003 verktyg finns så kan det i vissa fall vara mer tilltalande att inte migrera några data alls från det gamla systemet. Om användarna vill flytta över data från det gamla systemet så kan de göra det själva. Här följer några förslag på hur man kan låta användarna flytta över sitt egen data. Det är givetvis möjligt att kombinera de metoder man använder för migreringen.

13.4.1 Mailbox Migrering

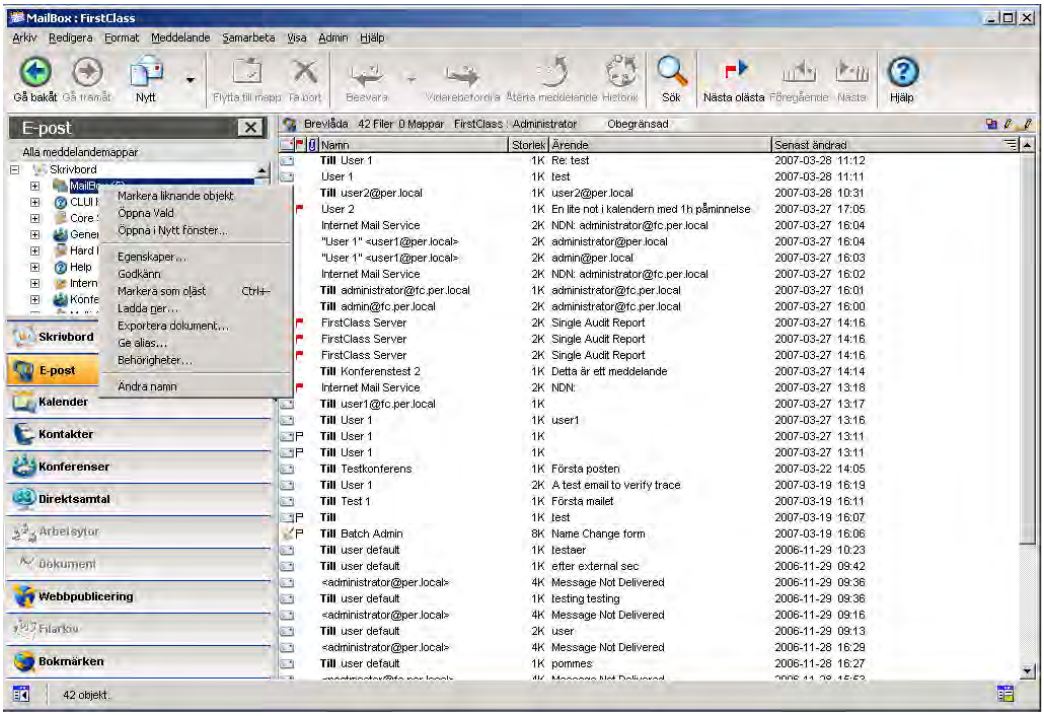
1. Ett sätt är att be användarna att skicka vidare information från FirstClass till det nya mail systemet. Detta innebär troligen att användarna bara skickar över den information som är mest värdefull för dem.
2. Instruera användarna i hur de kan konfigurera Outlook eller Outlook Express att använda sig av FirstClass servern som en IMAP server. Användarna kan sedan dra och släppa informationen som de tagit ned till lokala mappar på klienten. Den information man flyttat ut

kan sedan flyttas in i Exchange 2007 genom att koppla upp ett IMAP konto mot Exchange 2007 och dra över den information man flyttat dit.

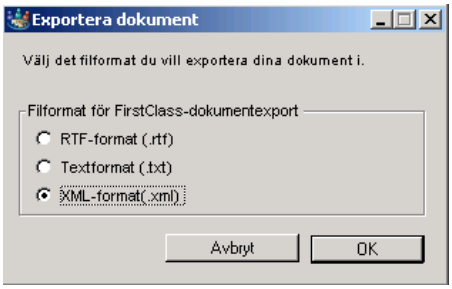
3. Instruera användarna om att spara ut alla sina mail som en text eller rtf fil. Detta innebär att användaren sparar ut all text i sina mail till dokument. Användaren får däremot inte med några kopplade dokument i detta scenario. Dessa filer kan sedan sparas i SharePoint eller på ett filshare.
4. Från FirstClass kan man även exportera mail till XML filer. Dessa skulle senare kunna behandlas av ett import program för att skapa dem i rätt format på Exchange 2007 servern. Det finns ett antal exempel script för import av XML data via Outlook. Det skulle även gå att bygga en egen import motor för att sköta detta.

13.4.1.1 Exempel på Migrering av Mailbox

1. Markera mappen med meddelanden som skall exporteras, höger klicka och välj Exportera dokument...



2. Välj vilket format du vill spara meddelandena i, RTF samt txt är läsbart för klienten xml skall användas om ni nyttjar ett separat script för import av informationen till Exchange.



3. Välj vilken mapp som de skall placeras i

13.4.2 Migrering av övrig Brevlådedata

13.4.2.1 Skickade Meddelanden

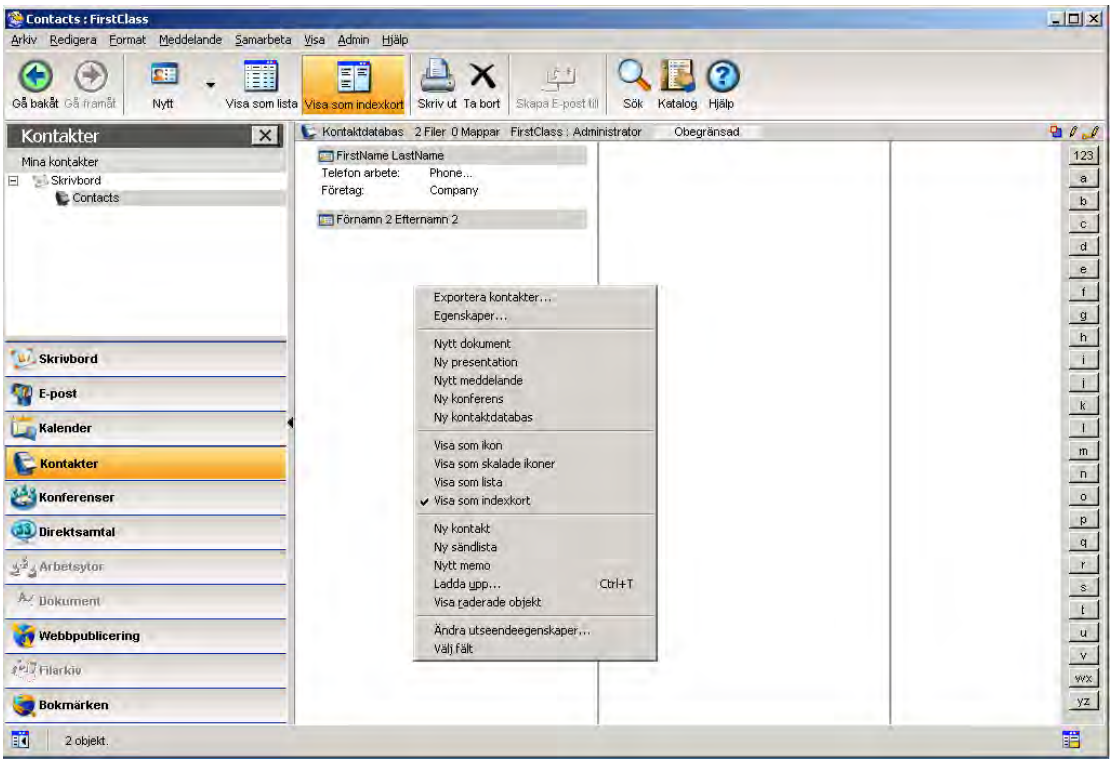
Skickade meddelanden kan inte nås från annan mjukvara än FirstClass klienten. De viktigaste meddelandena kan man skicka vidare till sin nya brevlåda medan man kan välja att spara det stora flertalet i text format och lägga upp det på SharePoint där man enkelt har det indexerat och lätt att komma åt. Se på ovanstående exempel för mailbox-migrering för mer detaljer.

13.4.2.2 Kontakter

Kontakter i FirstClass kan exporteras som vCard eller i CSV format vilket senare kan importeras i Outlook och de flesta andra mail klienter och därmed in i Exchange. Det enklaste är att dra och släppa vCards in i Kontakt mappen i Outlook. Däremot kan inte personliga adresslistor exporteras, de kan däremot sparas ned som textfiler och senare läggas in i Exchange. Det finns inga färdiga verktyg för att exportera kontakter från FirstClass till Exchange från serversidan.

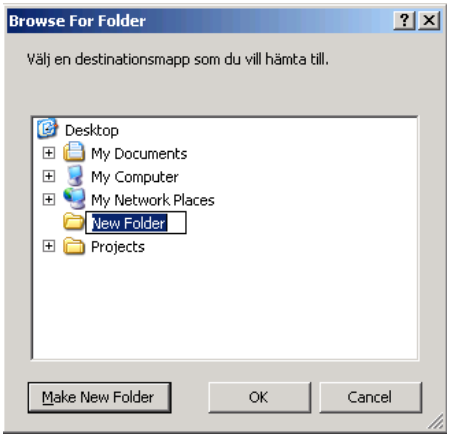
Här följer ett exempel på export av kontakter från FirstClass

1. Högerklicka i den vänstra ytan och välj Exportera kontakter...

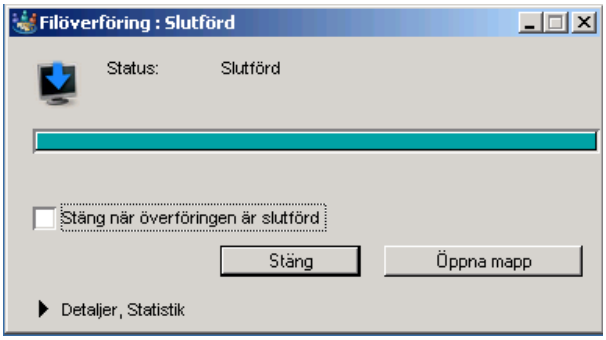


2. Välj Alla kontakter och formatet skall vara vCard

3. Välj en folder att placera kontakterna i



4. När exporten är färdig välj att Öppna mapp, dra och släpp kontakterna in i kontakt mappen i Outlook.

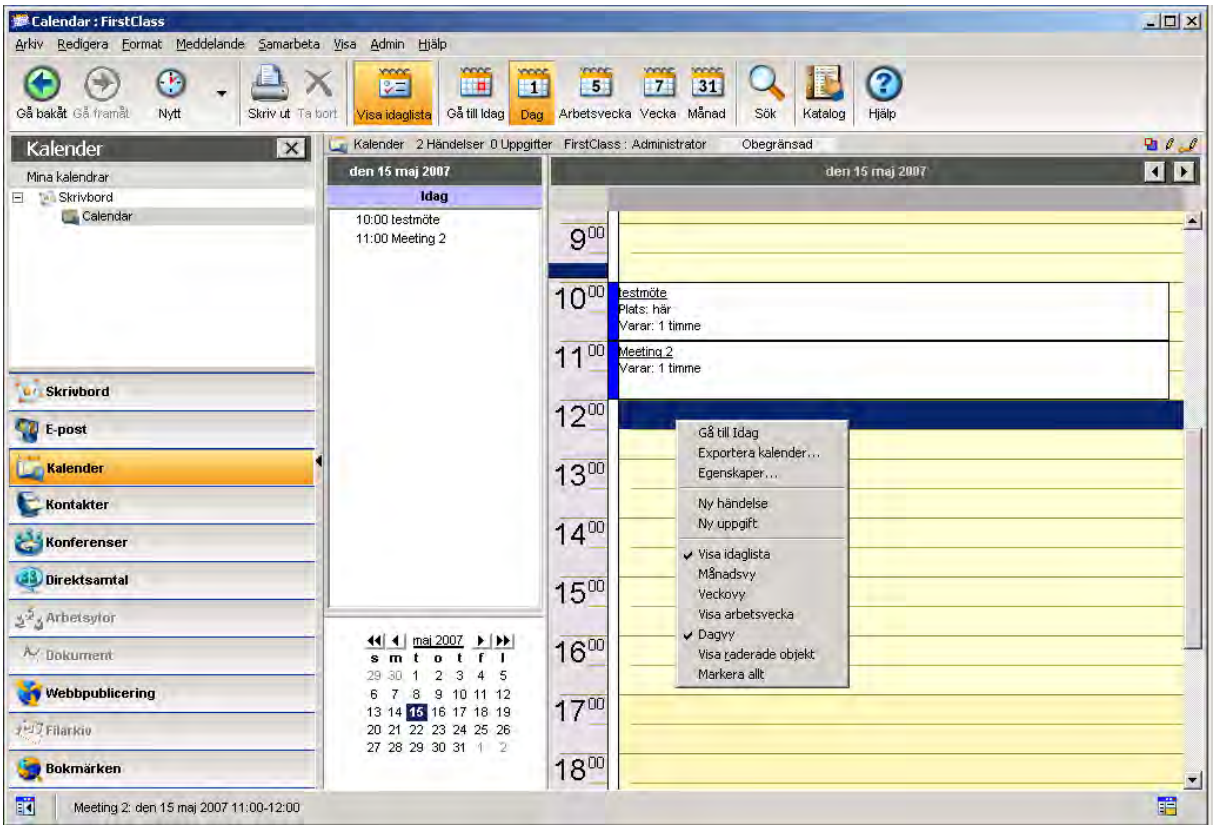


13.4.2.3 Kalenderdata

Kalenderdata kan sparas som vCalender från FirstClass klienten vilka senare kan importeras i Exchange via Outlook klienten. Man drar och släpper helt enkelt de vCalender objekt som man har exporterat rakt in i kalender mappen i Outlook. Observera att klienten i detta läge skall vara kopplad till Exchange servern för att nå bästa resultat.

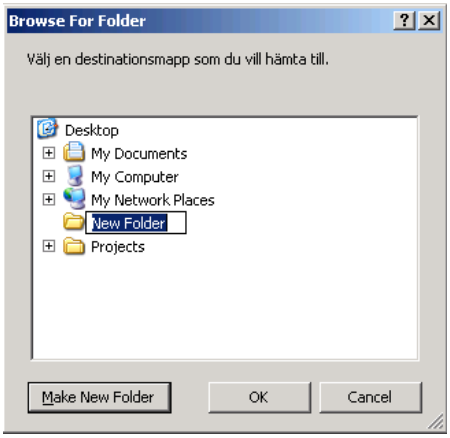
Här kommer ett exempel på export av Kalenderdata från FirstClass

1. Höger klicka i kalendern och välj Exportera kalender...



2. Välj Alla händelser och uppgifter, spara dem i vCalendar format

3. Välj vart du vill spara informationen



4. När exporten är färdig välj att öppna mappen, dra och släpp informationen in i kalendern i Outlook.

13.4.3 Migrering av Konferensdata

Det finns inga färdiga verktyg för migrering av konferensdata. Det är möjligt att exportera informationen precis som vi beskrivit tidigare i dokumentet till rtf,txt,xml filer och sedan importera det i SharePoint eller Exchange beroende på vilket system som är bäst anpassat för de syften man nyttjat konferensen till. Här skulle man kunna lägga ansvar på ägarna för konferensdatat att migrera informationen. Det stöd som finns att exportera information ifrån FirstClass till XML format ger en hel del möjligheter i form av anpassade importerings- verktyg. Ett verktyg som kan användas för import till SharePoint finns på följande webb länk.
http://apps.gotdotnet.com/workspaces/releases/viewuploads.aspx?id=6996fb17-2a54-4607-983b-35c7697baa53

Det finns ett antal verktyg som kan anpassas för import av XML data. Välj det som passar era syften bäst.