

Nulägesbeskrivning

Fiktivmyndighetens IT-miljö version 1.02

Fiktivmyndigheten

Innehållsförteckning

- 1 Om detta dokument 2
- 2 Om Fiktivmyndigheten 2
- 3 Allmänt om IT-miljön 3
- 4 Datacenter 4
- 5 Hårdvara 4
- 6 Kommunikation 5
- 7 Systemprogramvaror 7
- 8 Systemunderhåll 7
- 9 Kontorsstöd 8
- 10 Verksamhetssystem 9
- 11 Volymer 10

1 Om detta dokument

Detta dokument avser att ge en översiktlig bild av hur Fiktivmyndighetens IT-miljö ser ut vid aktuellt dokumentdatum och ska vara ett underlag för dialog och hjälp vid upphandling och avrop av IT-system till Fiktivmyndigheten.

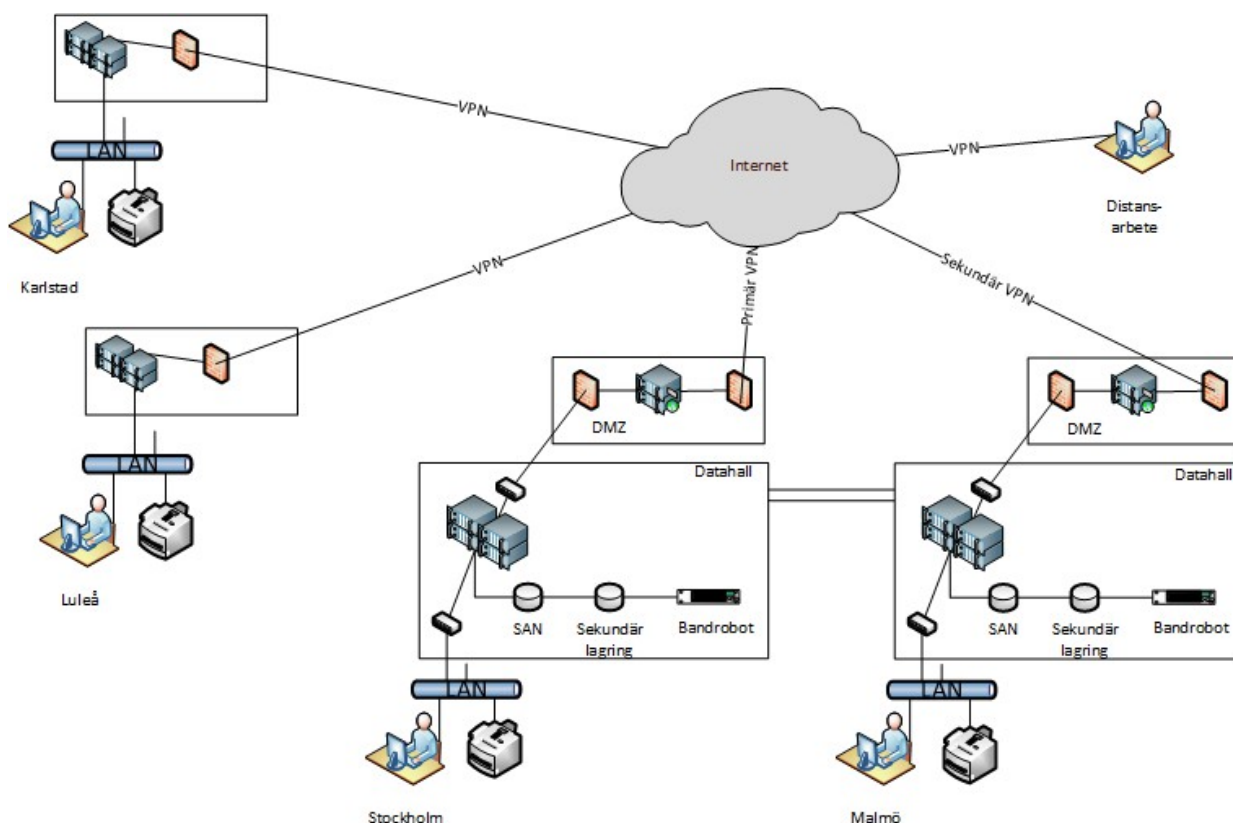
2 Om Fiktivmyndigheten

Fiktivmyndigheten har kontor i Stockholm, Luleå, Karlstad och Malmö. Det är totalt ca 700 anställda fördelat på 350 i Stockholm, 20 i Luleå, 80 i Karlstad samt 250 i Malmö. IT-avdelningen har ca 25 anställda. Fiktivmyndigheten behandlar i dagsläget personuppgifter och sekretessbelagd information men ingen information som är säkerhetsklassificerad. Risk- och sårbarhetsanalyser för verksamheten genomförs regelbundet. Även en katastrofplan som uppdateras regelbundet finns.

Fiktivmyndigheten

3 Allmänt om IT-miljön

3.1 Schematisk bild över IT-miljön



3.2 Övergripande beskrivning

Fiktivmyndighetens verksamhet är informationsintensiv och hanterar stora mängder data. För att säkerställa hög tillgänglighet på IT-systemen har man två datacenter för verksamhetssystemen samt två mindre datorrum för utskriftsservrar och filservrar.

Kontoren är utrustade med såväl trådbundet som trådlöst lokalt nätverk. Kontoren är sammankopplade via VPN (Virtual Private Network) över Internet. Datacentren är sammankopplade med separata förbindelser.

Fiktivmyndigheten har en standardiserad klientplattform som används av merparten av alla anställda. Utöver detta finns ytterligare ett antal klienter i verksamheten som inte använder den myndighetsgemensamma klientplattformen.

För utskrifter använder Fiktivmyndigheten multifunktionsskrivare och en utskriftstjänst som innebär att utskrifterna köas i en myndighetsgemensam utskriftskö.

Myndighetens IT-miljö innefattar även smartphones och surfplattor.

Fiktivmyndigheten

All IT-utrustning livscykelhanteras över fyra år vilket innebär att utrustningen byts ut mot ny motsvarande utrustning efter ca fyra år.

4 Datacenter

Fiktivmyndigheten har två datacenter placerade i Malmö respektive Stockholm.

Datacentren är prefabricerade datacenter enligt säkerhetsklass SS/EN 1047-2 och är utrustade med klimatanläggning och har dubbla redundanta strömförsörjningar samt UPS (Uninterruptible Power Supply) och reservkraft i form av dieselaggregat.

Datacentren är speglade och är samtidigt aktiva vilket innebär att lasten fördelas mellan bägge datacentren.

I vardera datacenter finns servrar för verksamhetssystem, test och utveckling. Test och utvecklingsservrar är på båda orterna placerade i separata rack i en avgränsad zon av vardera datacenter.

Utöver dessa stora datacenter finns även mindre datorrum i Luleå och Karlstad. I dessa finns servrar för delning av filer och utskriftstjänster.

Central lagringsutrustning, SAN (Storage Area Network), utrustning för säkerhetskopiering samt kommunikationsutrustning för servrar och lagringsutrustning är placerade i datacentren i Stockholm och Malmö.

5 Hårdvara

5.1 Servrar

Servrar i datacentren i Stockholm och Malmö är rackservrar. Samtliga rackservrar har hög redundans i form av dubbla kraftaggregat, speglade systemdiskar samt dubbla nätverks- och SAN-anslutningar och använder SAN för lagring.

Servrar i Luleå och Karlstad är rackservrar med hårddiskar monterade i separata diskabinett.

Installation, konfiguration, uppdatering, uppgradering, licenshantering, övervakning m.m. av serverna sköts av Fiktivmyndighetens IT-avdelning.

Operativsystem m.m. som används på serverna redovisas under avsnittet Programvara.

5.2 Lagring och säkerhetskopiering

Lagring av verksamhetsdata för samtliga servrar i datacentren i Stockholm och Malmö sker centralt i ett SAN där all prioriterad data synkroniseras mellan datacentren.

Utrustning för sekundärlagring som främst används för säkerhetskopiering finns placerad i båda datacentren.

Utrustning för säkerhetskopiering som finns i båda datacentren består av produkter från blandade leverantörer. All säkerhetskopiering görs i datacenter i Stockholm med utrustningen i Malmö som

Fiktivmyndigheten

reserv.

För att minimera den tid som verksamhetssystemen påverkas av säkerhetskopieringen sker den i två steg. Först en snabb kopiering mellan SAN och sekundärlagring. Därefter kopieras allt från sekundärlagring till band med hjälp av en bandrobot.

Säkerhetskopiering av all verksamhetskritisk data sker automatiskt efter ett schema bestående av dels total säkerhetskopiering och dels säkerhetskopiering av förändringar sedan föregående kopiering.

Säkerhetskopiering för serverna på kontoren i Karlstad och Luleå sker till datacenter i Stockholm.

5.3 Klientdatorer

Fiktivmyndigheten har standardiserat ett antal klientpaket som de anställda använder.

Dels finns ett paket med stationär PC dels ett paket med bärbar PC. Båda paketen kompletteras vid behov med tillhörande kringutrustning såsom bildskärm, tangentbord och mus.

5.4 Smartphones

Fiktivmyndighetens anställda har mobiltelefoner fördelade 50/50 på IOS och Android.

Förutom telefonfunktionerna används de främst för e-post och kalendersynkronisering samt webb.

5.5 Surfplattor

Fiktivmyndighetens ledning, informationsavdelning och IT-avdelning har surfplattor fördelade 50/50 på IOS och Android.

5.6 Skrivare

Fiktivmyndigheten har en central utskriftsserver och användarna har tillgång till multifunktionsskrivare (MFP) som fungerar som nätverksskrivare, kopiator och skanner.

MFP nyttjar funktionerna Follow Me Print och Secure printing vilket innebär att utskriften ligger kvar i skrivarkön och tas ut på valfri MFP efter autentisering med kort. Drivrutin är installerad i samtliga klientdatorer. MFP ligger på eget VLAN.

6 Kommunikation

6.1 Datacenter

I datacentren finns nätverksväxlar som sköter kommunikation mellan servrar, SAN och LAN (Local Area Network) i datacentren samt mellan datacenter. Dessutom finns lastbalanserare vars uppgift är att fördela lasten mellan datacentren.

All kommunikation i SAN består av redundant Fibre Channel.

För att uppnå en snabb och säker kommunikation mellan datacentren i Stockholm och Malmö finns två redundanta svartfiberförbindelser vilka är fysiskt åtskilda genom hela landet.

Fiberförbindelsen mellan Stockholm och Malmö är dels 10Gbps Ethernet och dels 16Gbps Fibre Channel.

6.2 Internet

För verksamhetens behov av kommunikation mellan kontoren och för att nå verksamhetssystemen

Fiktivmyndigheten

används Internet med VPN. För att skapa redundans och för att Fiktivmyndigheten inte ska vara beroende av en ISP (Internet Service Provider) är kontoren i Stockholm, Karlstad och Luleå anslutna mot en ISP medan kontoret i Malmö har en annan ISP. Alla Internetanslutningar termineras hos Fiktivmyndigheten med routrar som ägs av ISP. Fiktivmyndigheten har fulla administrativa rättigheter till ISP:s routrar.

Anslutningen mot Internet är redundant med BGP (Border Gateway Protocol) mellan router i Stockholm och Malmö.

All trafik från Karlstad och Luleå, inklusive trafik till Internet, skickas i VPN-tunnel primärt till Stockholm och med Malmö som sekundär anslutning.

Användare i Malmö går primärt ut på Internet via anslutning i Malmö med Stockholm som sekundär anslutning.

Samtliga anslutningar mot Internet har stöd för IPv4 och IPv6, BGP samt skydd mot DDOS-attacker (Distributed Denial of Service).

6.3 LAN

På varje kontor finns både trådbundet och trådlöst LAN.

LAN består av redundant Ethernet med 10 Gbit/s och 1 Gbit/s anslutningar.

Alla kontorsarbetsplatser och konferensrum är utrustade med trådbundna nätverksuttag för RJ45-anslutna enheter. Dessutom är alla kontorsplan utrustade med minst två accesspunkter per plan för trådlöst LAN.

Fastighetsnätets kablage är av typ kategori 6. I korskopplingsrum på varje våningsplan ansluts de trådbundna nätverksuttagen mot korskopplingspaneler varifrån de patchas mot nätverksväxlar. Även accesspunkterna för trådlöst LAN ansluts mot nätverksväxlarna i närmaste korskopplingsrum. Dessa nätverksväxlar ansluts i sin tur via fiber mot en nätverksväxel för varje kontor som därefter ansluter mot Internet.

Fiktivmyndigheten har standardiserat nätverksväxlarna i korskopplingsrummen till 24-portars växlar. Nätverksväxlar är av olika fabrikat. Samtlig utrustning är fullt övervakningsbar och stöder alla normalt förekommande öppna standarder.

Autentiseringen till det trådlösa nätet sker med 802.1X.

Distansarbete kan ske via VPN-uppkoppling och användarna har möjlighet att beställa mobilt bredband ifall arbetet kräver extra mobilitet. Utöver detta finns även ett separat trådlöst gästnätverk att erbjuda gäster som behöver tillgång till Internet.

6.4 DMZ

Fiktivmyndigheten har ett DMZ (Demilitarized Zone) i Stockholm och ett i Malmö i vilket servrar för VPN, DNS (Domain Name System), e-post och extern webb (www.fiktivmyndigheten.se) finns.

Brandväggar mot Internet och LAN är fysiskt separerade. Nätverksväxlarna i DMZ är fysiskt separerade från övriga LAN. IDS (Intrusion Detection System) finns.

Fiktivmyndigheten

Serverar för DNS och DNSSEC (The Domain Name System Security Extensions) är baserade på Linux och BIND 9 (Berkeley Internet Name Daemon).

Serverar för VPN är baserade på Linux och OpenVPN.

Allt på DMZ har dubbla IP-stackar, IPv4 och IPv6.

6.5 Telefoni

Telefoni-lösningen är en MEX-lösning (Mobile Extension) med hänvisningstjänst som synkroniserar med Exchange.

7 Systemprogramvaror

7.1 Operativsystem serverar

De fysiska serverarna i datacentren respektive datorrummen körs med följande operativsystem:

RedHat Enterprise Linux 6

Microsoft Windows Server 2008R2

Microsoft Windows Server 2012

Oracle Solaris 11.2

På de fysiska serverarna med Linux och Windows Server finns i vissa fall virtualiseringsprogramvara som innebär att verksamhetssystemen kan köras i virtuella serverar. Även på de virtuella serverarna används samma versioner av Linux och Windows Server.

7.2 Operativsystem klienter

På klienterna används följande operativsystem:

Microsoft Windows 7 (standardiserad klientplattform)

Ubuntu Linux 14.04

Apple OS X 10.9

7.3 Databaser

De databaser som används är:

Oracle 11g

Microsoft SQL Server 2012

PostgreSQL 9.3

MariaDB 5.5

MongoDB 2.6

Databasmiljön med Oracle är installerad på serverar med Oracle Solaris placerade i datacentren i Stockholm och Malmö. Miljön består av tre databaskluster.

En databasmiljö med Microsoft SQL Server placerad i datacentren i Stockholm och Malmö. Miljön består av ett databaskluster.

Det finns databaser som ingår som en del i system (även licensmässigt) och dessa är oftast installerade tillsammans med systemen på virtuella serverar.

8 Systemunderhåll

8.1 Övervakning

Fiktivmyndigheten har Icinga 2 som övervakningssystem som regelbundet kontrollerar status på

Fiktivmyndigheten

och tar emot larm från IT-miljöns hårdvaror och programvaror. Övervakningssystemet kan skicka kritiska larm vidare till systemadministratörerna via e-post och SMS.

8.2 Distributionsprogramvara

För klientdatorer med Microsoft Windows sker distribution av operativsystem, drivrutiner och applikationer via central policy med hjälp av Novell Zenworks.

För klientdatorer med OS X sker motsvarande distribution med DeployStudio Admin tillsammans med Apple Open Directory.

För klientdatorer med Ubuntu Linux administreras dessa lokalt av användarna.

8.3 SPAM-filter

All in- och utgående e-posttrafik till Exchange passerar ett molnbaserat filter som filtrerar bort skräppost och virusmittade försändelser.

8.4 Virussydd

Samtliga servrar och klienter har aktivt virussydd som styrs via central policyhantering.

8.5 Lagringshantering

IBM Tivoli Storage Manager används för SAN och säkerhetskopiering.

8.6 VPN

För kommunikation mellan kontor och för arbete på distans över Internet används VPN-tunnlar som administreras via OpenVPN.

9 Kontorsstöd

9.1 Katalogtjänst

För att användaren ska kunna komma åt sin arbetsmiljö krävs tillgång till en personlig användaridentitet. Beroende på vilken avdelning användaren tillhör får användaren med automatik åtkomst till standardapplikationer, övriga applikationer, lagringsarea såsom hemkatalog samt gemensam fillagringsyta. För hantering av rättigheter och styrning används Microsoft Active Directory. Samtliga klientdatorer autentiserar mot Active Directory.

För att höja säkerheten nyttjar Fiktivmyndigheten Active Directory Certificate Services (ADCS) för dator- och användarautentisering.

9.2 Extern webbplats

Fiktivmyndigheten använder Linux, Apache HTTP server 2.4 och Wordpress 3 för den externa webbplatsen www.fiktivmyndigheten.se

9.3 Intranät

Fiktivmyndigheten har ett intranät som används som intern kommunikationskanal. För denna används Linux, nginx 1.7 och Drupal 7.

9.4 E-postserver

Som e-postserver använder Fiktivmyndigheten Microsoft Exchange 2010.

9.5 Kontorsprogram

Alla klientdatorer med Windows har Microsoft Office Professional Plus 2010, Adobe Acrobat Reader X, Google Chrome och Oracle Java 8 installerat.

Alla klientdatorer med OS X har Microsoft Office Standard 2011, Safari, Google Chrome, Oracle

Fiktivmyndigheten

Java 8 och Adobe Acrobat Reader X.

Alla klientdatorer med Linux har Libreoffice 4.4, Adobe Acrobat Reader 9, Google Chrome och Oracle Java 8.

9.6 Videokonferens

Fiktivmyndigheten har Google Hangouts för videokonferens. Både internt och för videokonferens med externa deltagare.

10 Verksamhetssystem

Fiktivmyndigheten har ett antal egenutvecklade myndighetsspecifika system som samtliga är utvecklade i Java. Det finns också ett antal större system från externa leverantörer.

10.1 Ärendehantering

Fiktivmyndigheten har en ärendehanteringsprogramvara som används för registrering och administration av myndighetens ärenden. Programvaran används också för diarieföring av handlingar.

10.2 Ekonomisystem

Fiktivmyndigheten har ett ekonomisystem för hantering av processerna för redovisning, kund- och leverantörsreskontra samt bokslut, analyser och rapportering. Fiktivmyndigheten använder en molnbaserad e-handelstjänst för elektronisk hantering av leverantörsfakturor och beställningar.

10.3 Personaladministrativt system

Fiktivmyndigheten har ett PA-system för hantering av rekrytering, personaladministration, kompetenshantering, tid och bemanning, resehantering, löner och förmåner.

10.4 Upphandlingsverktyg

Fiktivmyndigheten har ett elektroniskt upphandlingssystem i form av en molntjänst. Alla avrop och upphandlingar görs via upphandlingsverktyget.

10.5 Beslutsstöd

Som stöd till verksamhetsstyrningen, intern kontroll och uppföljning samt bättre planeringsprocesser har Fiktivmyndigheten ett beslutsstöd med tillhörande datalager som är integrerat med flera av myndighetens övriga IT-system.

Fiktivmyndigheten

11 Volymer

I denna tabell finns en sammanställning av volymer för Fiktivmyndigheten.

Objekt	Stockholm	Malmö	Karlstad	Luleå
Antal anställda (varav IT-enheten är 25)	350	250	80	20
Datacenter	1	1		
Datorrum			1	1
Rackserver	19	16	2	2
SAN	1	1		
Sekundär lagring	1	1		
Lokal lagring			1	1
Bandrobot	1	1		
Stationär PC, Windows 7	140	70	30	10
Bärbar PC, Windows 7	210	180	50	10
Bärbar PC, Linux	10	5		
MacBook, OS X	10			
Smartphone, IOS	175	125	40	10
Smartphone, Android	175	125	40	10
Surfplatta, IOS	10	5	1	1
Surfplatta, Android	10	5	1	1
Multifunktionsskrivare	24	17	7	2
Lastbalanserare	1	1		
Nätverksväxel	20	15	7	3
Accesspunkter trådlöst LAN	30	28	10	4
Brandvägg	2	2		
OS fysisk server, Windows Server 2008R2	5	4	2	2
OS fysisk server, Windows Server 2012	2	2		
OS fysisk server, Linux	12	10		
OS fysisk server, Solaris	3	3		
OS virtuell server, Windows Server	32	28		
OS virtuell server, Linux	44	37		
DB Oracle 11g	3	3		
DB Microsoft SQL Server 2012	24	12		

Fiktivmyndigheten

DB MariaDB 5.	8	8		
DB MongoDB 2.6	4	4		