STATENS IT

Bilag 11
Statens It's standarddriftsplatform

Version 2017-1

Indhold

1 Indledning

Den 1. januar 2010 fik Statens It ansvar for alle opgaver vedrørende administrativ it, it-infrastruktur samt en række opgaver vedrørende drift, vedligehold og brugeradministration af fag-it for en række ministerområder. Statens It er herigennem med til at skabe fundamentet for den videre digitalisering af staten.

Statens It har ansvaret for at drive en effektiv it-understøttelse og sikre en høj og ensartet it-service på tværs af staten. Hovedopgaverne omfatter drift, support, udvikling og harmonisering af it i staten.

I 2011 blev Statens It's datacenter implementeret og udgør i dag fundamentet for den standarddriftsplatform, som skal gøre det muligt for Statens It at levere sikker og stabil it-drift, der understøtter kundens forretning samt bidrager til at optimere it-ressourceforbruget i staten som helhed.

1.1 Formål

Formålet med dette dokument er at beskrive den standarddriftsplatform, som gør Statens It i stand til at levere den bedste og billigst mulige it-understøttelse til kundernes forretning. Standarddriftsplatformen er den platform hvor Statens It sikrer sammenhængen mellem kompetencer, leverandørsupport og supporting services som eksempelvis patch management og overvågning. Standardriftsplatformen er også den platform, der sikrer en robusthed overfor ressortændringer, samt udgør grundlaget for tvær-statslige it-løsninger.

Dokumentet skal understøtte udviklingsprojekter for kundens fagapplikationer, som er beskrevet i aftalekompleksets bilag 6 "Snitflader mellem Kunden og Statens It", og derved give en hurtigere og mere smidig implementering i standarddriftsplatformen[1]. Dette forudsætter dog, at der fra leverandørens side leves op til de beskrevne anbefalinger, der er formuleret på baggrund af arkitektur og sikkerhed på standarddriftsplatformen. Såfremt sikkerhedsanbefalingerne ikke følges, er det kundens fulde ansvar jf. ansvarsfordeling beskrevet i aftalekompleksets bilag 4 "Informationssikkerhed".

Statens It's kunder er ikke forpligtet til at efterleve Bilag 11, men dokumentet er en beskrivelse af den platform, som sikrer at Statens It kan opnå økonomiske fordele ved stordrift. Hvis anbefalingerne ikke følges, kan omkostningerne til etablering og drift stige og Statens It kan ikke garantere SLA på tilgængelighed og løsningstid. Der henvises til bilag 6, afsnit 8.1. Fraviges anvisninger i en sådan grad, at det udgør en sikkerhedsrisiko, så isoleres it-løsningen fra den øvrige it-infrastruktur og kan dermed ikke gøre brug af de etablerede fællesservices såsom det fælles Active Directory.

1. Bilag 11 udgør ikke den samlede dokumentation i forbindelse med projekter – her må henvises til http://statens-it.dk/leverandoerer/projektpakken.html hvor den komplette oversigt over projektdokumentationen ligger.

Såfremt det ikke er muligt at leve op til anvisningerne i dokumentet, skal der rettes henvendelse til Statens It med henblik på indgåelse af en særlig aftale.

1.2 Læsevejledning

Målgruppen for dette dokument er Statens It's kunder, herunder systemejere, samt tredjepartsleverandører.

Det forudsættes, at læseren er bekendt med de mest generelle begreber inden for it.

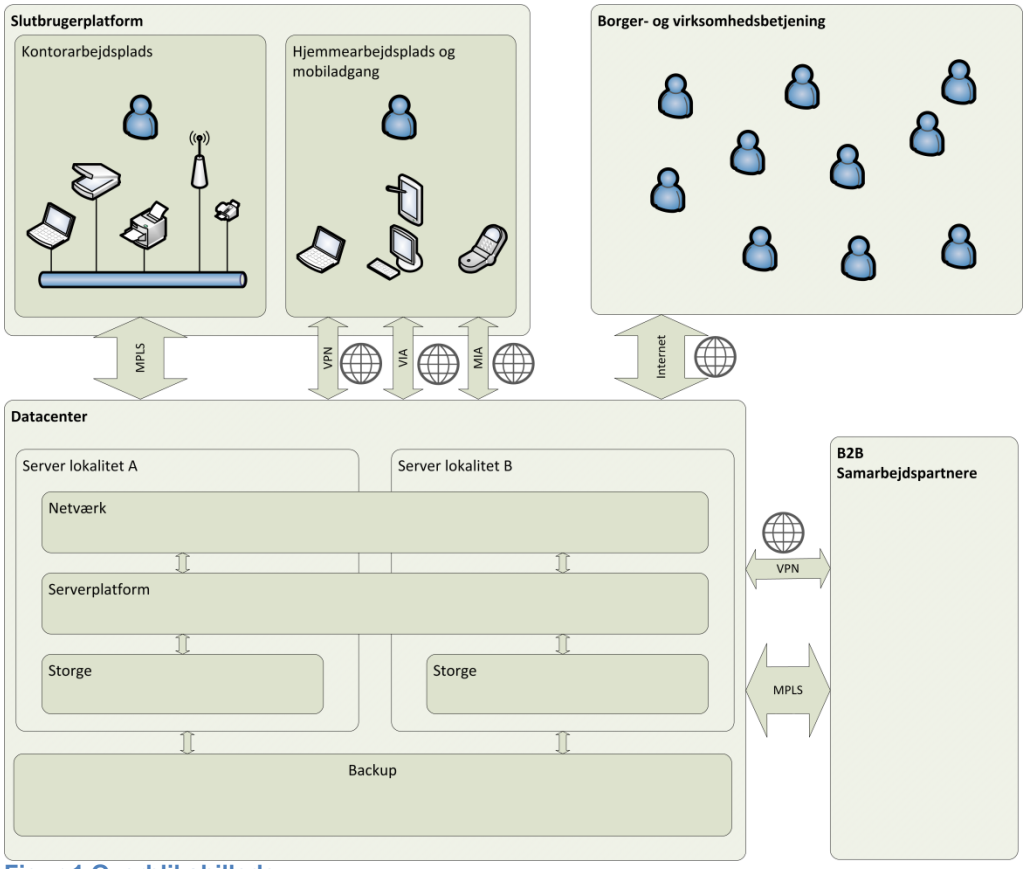
1.2.1 Underbilag til bilag 11

Der er oprettet to underbilag, som uddyber følgende emner:

A) Standardserverkonfiguration i Statens It's standarddriftsplatform – 2017-1
B) Backuppolitik i Statens It's standarddriftsplatform 2017-2

2 Overblik

For at sikre et fælles udgangspunkt, inden der i de følgende afsnit dykkes ned i detaljen om Statens It's standarddriftsplatform, gives der hermed et indblik i den samlede it platform.



Figur 1 Overbliksbillede

Standarddriftsplatformen, som er skitseret ovenfor, er delt op i forskellige platforme:

- Slutbrugerplatformen, der er den brugernære platform.
- Borger- og virksomhedsbetjeningsplatformen, der er borgernes og virksomheders adgang til de internet vendte it-services.
- Datacenteret, som i hovedtræk er facilitering af:
  - Serverplatformen, der er grundpillen i alle systemer.
  - Storage, der er lager for system- og bruger-data.
  - Netværksinfrastruktur, der sikrer forbindelse mellem brugere og systemer.
- Business-to-Business (B2B) platformen, er der hvor Statens It og kundernes samarbejdspartnere etablerer forretningssystem integrationer.

På serverplatformen stilles en række fællesservices til rådighed på standarddriftsplatformen. Et fælles Active Directory og en fælles Exchange løsning kan nævnes som nogle af de vigtigste. Serverplatformen stiller også

en lang række understøttende services til rådighed såsom NTP og DNS. Serverplatformen leverer også grundlaget for standardiseret fagapplikationsdrift.

Slutbrugerplatformen er den it-platform, som brugere er i direkte kontakt med. Kontorarbejdspladsen består af en pc med mulighed for scanning og udskrivning af dokumenter. I daglig tale refereret til som SIA (Statens It's it-arbejdsplads). Der er mulighed for etablering af et trådløst netværk, som gør fleksibiliteten med den bærbare pc optimal, samt et eller flere servicenet til opkobling af enheder, som dankortterminaler og andre specialenheder, der anvendes i forbindelse med kundens systemer.
Derudover består slutbrugerplatformen også af den mobile del af arbejdspladsen, med mulighed for at koble op via VPN til arbejdspladsen, når arbejds-pc'en tages med hjem eller på farten. En virtuel platform med mulighed for at arbejde på en virtuel arbejdsplads fra en vilkårlig pc eller fra en tablet, som i daglig tale refereres til som VIA (Virtuel it-arbejdsplads). Endeligt den mobile platform, der tilbyder arbejdsrelaterede applikationer direkte på telefon eller tablet, som i dagligtale omtales som MIA (Mobil it-arbejdsplads).

Datacenteret er hjertet i it-understøttelsen af ministerier og styrelser, hvor al teknikken og alle serverne, der understøtter den daglige sagsbehandling, er placeret. Datacenteret er udstyret med en redundant infrastruktur for at sikre høj tilgængelighed på kundernes systemer.

3 Slutbrugerplatform

3.1 Brugere

3.1.1 Brugerkonto

Som bruger hos en kunde i Statens It får man en brugerkonto i det fælles Active Directory (AD). Denne brugerkonto er udgangspunkt for styring af rettigheder til alle de fælles services, som Statens It udbyder til sine kunder. Den kan være adgangs- og rettighedsstyrede for kundens systemer, som er placeret hos Statens It.

Der er forskellige brugerkonti i Statens It's AD. En almindelig brugerkonto kan ikke have udvidede rettigheder i forhold til servere og AD. Hvis man som bruger har sådanne behov, får man tildelt en anden type brugerkonto. Dette uddybes i afsnittet vedr. autentificering og rettighedsstyring.

3.1.2 Mail og Kalender

Brugerkontoen har som udgangspunkt adgang til en mailkonto og en tilhørende kalender, opgaveliste og kontaktpersonregister.
Der er mulighed for at dele kalenderoplysninger på tværs af alle Statens It's brugere.

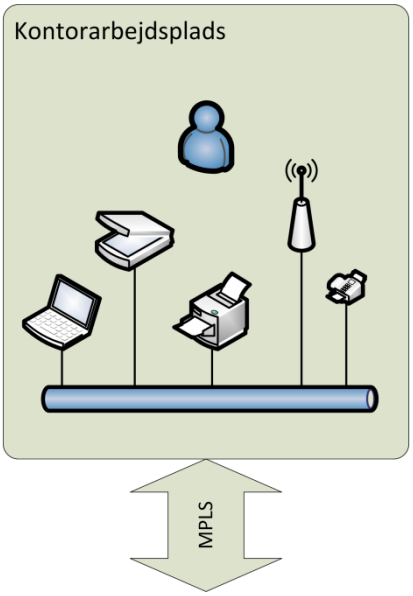
Mail og kalender er tilgængelig via mailklienter på standard pc'en (se afsnit 3.2.1), den virtuelle arbejdsplads (se afsnit 3.3) og arbejdspladsen til mobile enheder (se afsnit 3.3.3). Der er adgang via webmail fra andre klienter på øvrige enheder.
Mailløsningen understøtter også ressourcekalendere (møderum, biler etc.), distributionslister og fællespostkasser.

3.1.3 Fil service

Brugerkontoen har også adgang til at gemme fil-data på et personligt fillagringsområde. Dette sker på det centrale lager til person-genererede data. På dette centrale fillager er der også mulighed for at oprette organisatoriske og/eller opgavespecifikke fil-områder.
Fildrev er tilgængelige på standard pc'en, den virtuelle arbejdsplads og arbejdspladsen til mobile enheder.

3.2 Kontorarbejdspladsen

Kundens lokale arbejdssted består it-mæssigt af en standard pc, mulighed for print og scan, trådet og trådløst netværk og eventuelt et servicenet til andre specialenheder.
Kundens arbejdssted er netværksmæssigt forbundet til Statens It's datacenter via en kraftig MPLS netværksforbindelse.



Figur 2 Kontorarbejdspladsen

3.2.1 Standard pc (SIA)

Kundens brugere får udleveret en standard pc som i daglig tale omtales som SIA.
Standard pc'en udgøres af den ultrabærbar[2], der er tilgængelig på den overordnede indkøbsaftale i staten og som udstyres med et standard-image (operativsystem og grundlæggende applikationer) udviklet af Statens It. Det er en kontrolleret pc, som er under Statens It's kontrol, hvorfor den bliver opdateret og får applikationer installeret via Statens It.
Brugeren kan derfor som udgangspunkt ikke have lokal administrative rettigheder, men skal ved behov bestille software installeret via Statens It's Servicedesk.
For operativsystem og grundlæggende applikationer se afsnit 6.1

SIA er baseret på:

- Windows 7

Windows 10 bliver et supplement til Windows 7 og vil være tilgængelig som valg af operativsystem på SIA i 2017.

Krav til applikationer på standard PC'en

- Brugeren er som standard ikke lokaladministrator på pc'en, og applikationer må derfor ikke kræve dette for at afvikle.
- Applikationer skal kunne udrulles med Microsoft System Center Configuration Manager (SCCM).
- Det tilrådes at applikationer kan installeres uden opsættende check af softwareafhængigheder. Dette sikres under klargøringen af softwarepakken på SCCM platformen.
- Applikationer må ikke autoopdatere. Udrulning af opdateringer styres med SCCM efter test.
- Applikationer må ikke benytte "Click-Once Deployment", da applikationer i så fald ikke er under kontrol.

Afvigelser:
Kunden kan have behov for hardware, der afviger fra ultrabærbar. Så længe der installeres et standard image og pc'en er under Statens It's kontrol, er pc'en at betragte som en SIA pc.

Særlige pc'ere til helt specifikke formål såsom kiosk pc'ere er special-leverancer, der ikke behandles i dette dokument. Ved behov for sådanne skal kunden rette henvendelse til Statens It.

Visse programmer leveres kun som "Click-Once Deployment" og disse kan håndteres efter særlig aftale med Statens It.

---

2. Begrebet Ultrabærbar refererer til kravspecifikationen fra den statslige Indkøbsaftale for computere "Kontraktbilag 1B" og er i hovedtræk en let bærbar på max 1,7kg med en skærmstørrelse på 12,5 til 14 tommer og min. 8 GB RAM og min. 120 GB SSD.

3.2.2 Print og scanning
På kundens lokale arbejdssted oprettes et antal multifunktions maskiner og/eller printere efter behov. Dette giver brugere mulighed for at scanne og printe.
Brugere kan som udgangspunkt printe på alle printere i Statens It's AD. Brugere har derfor mulighed for at bruge en printer i nærheden, selvom om de er på besøg på en anden kundes lokalitet.

3.2.3 Trådet og trådløst netværk
Som kunde hos Statens IT etableres et kablet klientnetværk, som udelukkende må bruges til standard-pc'ere, scannere og printere.

Der kan etableres et trådløst netværk, som sikrer, at standard-pc'en har adgang til de fælles services, selvom den ikke er kablet. Overgangen mellem kablet net og trådløst net foregår automatisk.

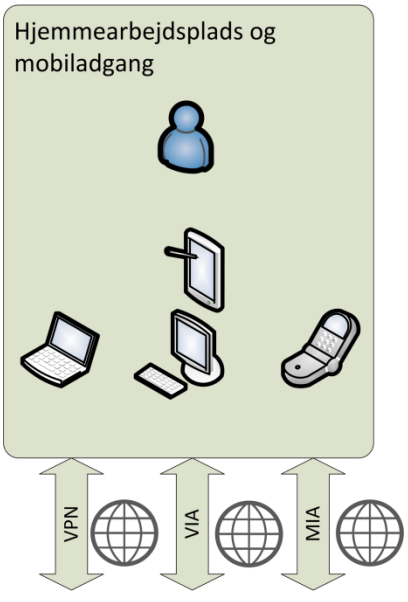
3.2.4 Servicenet
Derudover kan der stilles kablede servicenet til rådighed til særlige netværksenheder, såsom dankortterminaler o.a. Et servicenet er afgrænset så meget som muligt i forhold til de services der skal køre på nettet.

3.3 Hjemmearbejdsplads og mobil adgang
Brugere har mulighed for adgang til driftsplatformen, når de er derhjemme eller på farten. Der er forskellige tekniske løsninger, afhængig af hvilken enhed de ønsker adgangen fra.

3.3.1 Standard pc og VPN
Statens It understøtter VPN adgang til Statens It's standarddriftsplatform fra standard pc'en. For andre platforme skal det aftales specifikt med Statens it.

VPN er baseret på:
- Cisco AnyConnect Secure Mobility Client 4.2

Krav:
- Der anvendes to-faktor autentificering ved anvendelse af VPN, og det er derfor et krav, at brugeren er registreret korrekt med et gyldigt mobil-telefonnummer, som anvendes til fremsendelse af 2-faktor koden[3].



Figur 3 Hjemmearbejdspladsen

3. Alternativ løsning baseret på maskincertifikat er under implementering og vil erstatte ovenstående i løbet af 2017.

3.3.2 Virtual it-arbejdsplads (VIA)

Brugere har mulighed for at benytte sig af den virtuelle it-arbejdsplads, som i daglig tale kaldes VIA. Løsningen baserer sig på Citrix XenApp, hvor applikationer afvikles i datacenteret og leveres til enheder igennem en Citrix Receiver. Løsningen stiller streamede applikationer til rådighed for brugere og ikke en fuld desktop.

Der er adgang til VIA fra alle platforme der understøttes af Citrix Receiver.

De grundlæggende applikationer er de samme som på standard-pc'en – se afsnit 6.1

VIA er baseret på:

- Citrix XenApp 6.5 for Windows Server 2008 R2
- Microsoft App-V 5
- Windows Server 2008 R2

Krav til applikationer på virtuel it-arbejdsplads:

- Applikationerne på VIA skal kunne virtualiseres ved brug af Microsoft Application Virtualization – App-V.
- Brugeren er som standard ikke lokaladministrator på VIA, og applikationer må derfor ikke kræve dette, for at afvikle.
- Det tilrådes, at applikationer kan installeres uden opsættende check af softwareafhængigheder.
- Applikationer må ikke autoopdatere.
- Applikationer må ikke benytte "Click-Once Deployment", da denne type applikationer ikke understøttes på platformen.

3.3.3 Mobil It-arbejdsplads (MIA)

Kundernes brugere har mulighed for at benytte sig af den mobile it-arbejdsplads, som i daglig tale kaldes MIA. Løsningen baserer sig på Citrix XenMobile og er en MDM- og MAM-løsning, hvor apps afvikles i en sikret container på smartphones og tablets.

Den mobile it-arbejdsplads er baseret på

- Citrix XenMobile 10
- SecureHub 10 (iOS & Android)

Understøttede operativsystemer

- iOS 10.0 eller nyere
- Android 5.0[4] (Lollipop) eller nyere

Krav til apps på MIA:

- Apps skal kunne pakkes med Citrix MDX-toolkit for at fungere på den mobile platform.

Ovenstående krav om "Understøttede operativsystemer" betyder ikke, at MIA ikke virker på ældre enheder. Men Citrix tilbyder ikke support, hvilket betyder

4. I løbet af 2017 vil kravet til Android version ændre sig fra version 5.0 til version 6.0 som minimumskrav

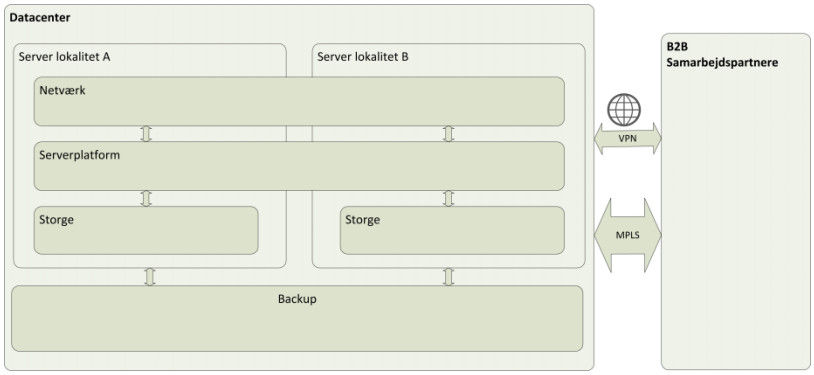
at Statens It heller ikke kan supportere ældre enheder. Statens It understøtter for nuværende ikke ”Windows Phone”-platformen.

Generelt

- Minimum 400 megabyte ledig plads på den mobile enhed til installation

4 Datacenter

Statens It's datacenter skal sikre kundernes tilgængelighed af services og skabe vedvarende sikker og stabil drift.



Figur 4 Datacenter

Datacentret består af flere fysiske adresser, med et eller flere serverrum på hver adresse. I dette dokument bliver der refereret der til adresserne som lokalitet A og B. Lokalitet A og B bruges til serverdrift og lagerkapacitet, og backup af data foregår på en tredje lokalitet.

Kapaciteten i datacenteret er tilstrækkelig til at dække kundernes behov. Kapacitet på serverrum, herunder strøm, køling og rack plads, vil løbende blive justeret i takt med kundernes behov, uden at kunderne skal forholde sig til dette.

4.1 Serverplatform

4.1.1 Virtualisering

Standardriftsplatformen stiller en fleksibel infrastruktur til rådighed for etablering af servere, men udfordrer også serverbegrebet som en fysisk enhed. En standard server hos Statens It er en virtuel enhed.

Virtualisering anvendes af flere årsager. Den primære er at gøre kundernes applikationer uafhængige af den underliggende hardware. Dette sikrer, at den nødvendige hardwarevedligeholdelse og udskiftning kan foretages uden, at det påvirker driften af serverne.
Samtidig opnås der høj fleksibilitet hvad angår ressourcetildeling til den enkelte server.

Virtualiseringen i datacenteret er baseret på:

- VMware vSphere 5.5/6.0.

4.1.2 Standardserverkonfiguration

Statens It har defineret en standardserver, som er konfigureret efter, hvad der erfaringsmæssigt har vist sig at være de bedste valg i datacenteret. Standardserverkonfigurationen opdateres løbende med udviklingen i

driftscenteret og er beskrevet nærmere i bilag A) Standardserverkonfiguration i Statens It's standarddriftsplatform.

Statens It's standardservere er konfigureret med et standardimage baseret på enten Microsoft Windows Server eller Redhat Enterprise Linux.

Gældende operativsystem versioner:
- Windows Server 2012 R2
- RedHat Enterprise Linux 7.4

I tilfælde af afvigelse fra standarden, skal der rettes henvendelse til Statens It.

4.1.3 Grundlæggende serverapplikationer
På Statens It's standarddriftsplatform tilbydes følgende applikationer, som danner grundlag for kundernes løsninger.

4.1.3.1 Databasesystemer
Statens It understøtter følgende databasesystemer på standarddriftsplatformen:
- Microsoft SQL Server 2014 SP2 (altid nyeste SP)
- Oracle Database 12c
- MySQL 5.7
- PostgreSQL Database System 9.4

4.1.3.2 Webserver
Statens it understøtter følgende webserverløsninger på standarddriftsplatformen:

- Microsoft Internet Informations Service (IIS) 8.5
- Apache HTTP Server version 2.4

4.1.3.3 Content management system (CMS)
Statens It understøtter følgende Content Management Systemer på standarddriftsplatformen:

- Microsoft Sharepoint Server 2013
- Sitecore XP 8.2
- Drupal 8.1

4.1.4 Supporting services
Supporting services er komponenter, som stilles til rådighed for løsninger på Statens It's standarddriftsplatform efter de gældende teknologivalg.

4.1.4.1 Mail og kalender
Statens It's fælles mailløsning er baseret på Microsoft Exchange og en central antispam-gateway med antivirus-check.

Mail og kalender er baseret på:

- Microsoft Exchange 2010[5]
  - Microsoft Exchange 2010 OWA
  - Microsoft Exchange 2010 EWS

Anvendelsesområder:
- Mail, kalender, kontaktpersoner og opgavestyring via Outlook, webmail og ActiveSync.
- Mail relay fra godkendte brugere og servere via den centrale anti-spam løsning.

Standarder:
- SMTP og Anonym SMTP.
- MAPI, IMAP4 og HTTPS.

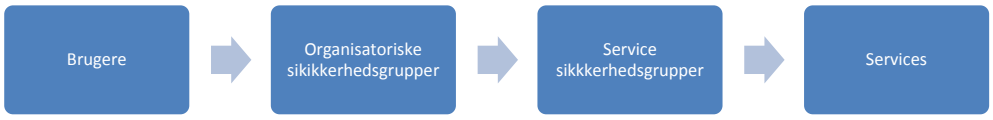
Klienter, der understøtter OutlookAnywhere og HTTPS, kan kommunikere fra internet til Exchange.
Klienter der kun understøtter protokollen IMAP 4 skal placeres i datacentret.

4.1.4.2 Autentificering og Active Directory

Domæne og brugerstyring, rettigheder og adgang
Statens It har etableret et Microsoft Active Directory (SIT AD) til styring af brugere, deres rettigheder og adgange.

Statens It's AD er opbygget omkring nogle principper og strukturer, som sikrer en ensartet administration på tværs af kunder og systemer. OU-strukturen anvendes til opdeling af Kunder og administrative enheder. Hver kunde er afgrænset i hver deres OU struktur.

Kundens organisation og rettighedstildeling styres gennem anvendelse af sikkerhedsgrupper. Kundens applikationer udbydes ligeledes ved brug af servicesikkerhedsgrupper og serviceressourcer. Kundens organisation er derfor ikke udstillet som et hierarki i en OU struktur. Organisationen kan afspejles som nestede organisatoriske sikkerhedsgrupper.



Figur 5 Rettighedstildeling via sikkerhedsgruppe-medlemskaber

De organisatoriske sikkerhedsgrupper kan blive medlem af servicesikkerhedsgrupper, som anvendes til tildeling eller rettighedsstyring af en service, og derved skabes relationen mellem kundens organisation og de udbudte services.

5. Statens It er i skrivende stund i gang med implementering af Exchange 2016, som indfases i 2017.

Bruger- og Servicekonti
Statens It har designet en standard for brugerkonti i AD, som sikrer, at der er en tydelig afspejling af princippet om funktionsadskillelse.

- En standard bruger kan ikke på nogen måde have privilegerede rettigheder i forhold til AD[6].
- En særlig brugerkonto etableres såfremt en bruger får behov for privilegerede rettigheder.
- Servicekonti er til systemer og kan ikke bruges som login.
- Ressourcekonti er til identificering af ressourcer og kan ikke bruges som login.
- Domain-administrative konti håndteres helt særligt og er underlagt en streng kontrol og er begrænset til så få som overhovedet muligt. Der vil aldrig blive tildelt en sådan konto til et system.

Applikationer skal designes med behov for færrest mulige rettigheder under princippet om ”least privilege”.

4.1.4.2.1 Active Directory
Statens It understøtter integreret Active Directory autentificering.

Active Directory er baseret på:

- Microsoft Active Directory
  - Functional Level Microsoft Server 2008 R2

Anvendelsesområder:

- Autentificering for interne og eksterne brugere.

Standarder:

- Kerberos
- NTLM v 2

Der kan ikke anvendes intern Active Directory-autentificering på løsninger, der er tilgængelige fra internettet. Hertil kan anvendes RADIUS eller to-faktor-autentificering.
Statens It tillader ikke skemaudvidelser af det interne Active Directory til brug for enkeltløsninger.
For eksternt rettede systemer, der ikke skal anvende intern autentificering, stiller Statens It et alternativt Active Directory til rådighed. Dette Active Directory er separeret fra det interne Active Directory.

4.1.4.2.2 ADFS
Statens It understøtter Active Directory Federation Services, baseret på Microsoft ADFS 2.0

ADFS er for nuværende kun tilgængeligt for interne systemer.

---

6. Applikationsspecifikke rettigheder er ikke at forstå som privilegerede rettigheder. En bruger kan derfor godt være administrator på en sharepointapplikation, uden at dette betragtes som priviligerede rettigheder.

4.1.4.2.3 RADIUS

RADIUS anvendes som autentificeringsmetode for løsninger, der ikke kan anvende Active Directory autentificering samt til to-faktor-autentificering.

Anvendelsesområder:

- For interne såvel som eksterne løsninger kan RADIUS anvendes til autentificering af interne brugerkonti.

Standarder:

- RADIUS

Der kan ydermere anvendes to-faktor-autentificering ved brug af RADIUS.

4.1.4.2.4 To-faktor autentificering

Statens It understøtter to-faktor autentificering i form af SMSPasscode.

Anvendelsesområder:

- Eksterne systemer, der kræver ekstra sikkerhed ved autentificering af interne brugere.

Standarder:

- Der anvendes RADIUS ved brug af to-faktor-autentificering.

Der understøttes to-faktor-autentificering via SMS-token eller hardware-token.

4.1.4.3 Sikkerhedskomponenter

Statens It anvender et bredt udsnit af sikkerhedskomponenter i datacenteret til beskyttelse af data og netværkstrafik.

Anvendelsesområder:

- Der anvendes antivirus/antimalware på alle servere.
- Der anvendes Intrusion Prevention System (IPS) for alle perimeteradgange til Statens It's datacenter.

Standarder:

- Se bemærkninger.

Bemærkninger:

- Af sikkerhedsmæssige årsager beskrives de løsninger, der anvendes, ikke.

4.1.4.4 Load balance / web-caching

For såvel internt som eksternt tilgængelige løsninger understøtter Statens It anvendelsen af load balancing samt web-caching.

Load balancing er en metode til at fordele trafik fra klienter mod to eller flere front end-servere og således optimere svartider, throughput og belastning på løsningen.
Web-caching er en metode til at optimere trafik fra klienter mod en eller flere webservere og således optimere svartider på løsningen.

Anvendelsesområder:

- Load balance og web-caching kan anvendes både til internt og eksternt tilgængelige løsninger.

- Der kan anvendes SSL offload, således at eksempelvis webservere ikke skal håndtere tung kryptering af trafik.

Standarder:

- Typisk anvendes HTTP og HTTPS som transportprotokoller. Andre protokol-standarder kan anvendes med forbehold.

Statens It understøtter kun Load Balance ved hjælp af hardwareappliance.

4.1.4.5 Domain Name System (DNS)

Statens It stiller DNS til rådighed for løsninger til brug for navneopslag.

4.1.4.6 Time Services

Statens It stiller Time Services (NTP) til rådighed for løsninger, interne såvel som eksterne, til brug for sikker og stabil tidssynkronisering. Statens It har to fysiske NTP-servere, der synkroniserer tid med den officielle danske NTP-pulje.

4.1.5 Overvågning

Statens It overvåger centrale it-services og komponenter og iværksætter en passende reaktion baseret på de enkelte events. Centralt for overvågningen er overvågningssystemkomplekset som pt. er baseret primært på HP's overvågnings-suite "Business Service Management" samt "SiteScope" som er udbygget med applikationsovervågningskomponenten "SiteRay".

Overvågningssystemkomplekset opsamler de enkelte events og præsenterer dem for bemandingen i Driftscenteret i form af advarsler og alarmer. Udvalgte alarmer rapporteres 24/7 til bagvagt.

Driftscenteret er bemandet hverdage 6:30-18:00, fredag dog 17:00

Driftsstatus

Statens It tilbyder kunder en Driftsstatus-App (Android og iOS), der frit kan hentes til såvel private som arbejdsenheder. I appen kan man abonnere på kritiske meldinger og information rettet mod hele styrelser eller ministerier.

Basisovervågning

Indeholdt er overvågningen af diske og ping af servere. Statens It har desuden teknisk overvågning på udvalgte komponenter i infrastrukturlaget samt overvågning af services, der ligeledes er fælles for kunderne – f.eks. print og e-mail.

Ud over basisovervågningen, som er standarden på standarddriftsplatformen, kan værktøjerne tilbyde forretningsprocesovervågning og udvidet komponent overvågning, men disse muligheder beskrives ikke yderligere i dette dokument.

For yderligere detaljering af overvågningsmuligheder kontakt Statens It.

4.1.6 System Management

Statens It anvender Microsoft Systemcenter Configuration Manager (SCCM) som værktøj til system management på Windows platformen og Red Hat Satellite på Linux platformen.

Sikkerhedsopdateringer til operativsystemer udrulles i førstkommende planlagte servicevindue efter udgivelsen.

4.2 Storage

Statens It har 3 typer storage på standarddriftsplatformen.

- **Tier 1** Meget hurtig:
  Flash storage med lav latency (ventetid på disken) og høj performance. Anvendes til applikationer der skal yde ud over det sædvanlige.
- **Tier 2** Hurtig:
  Traditionel San System med meget hurtig ydelse. San med meget hurtige diske. Anvendes til traditionelle applikationer.
- **Tier 3** Langsom:
  SAN med lav performance og høj latency (ventetid på disk). Anvendes til applikationer eller data der ikke anvendes særligt ofte.

Statens It's anbefaling er, at alle kunder starter på Tier 2 og efterfølgende flyttes til hurtigere eller langsommere Tiers om nødvendigt, i samråd med Statens It.
Der er ikke shared storage på SAN niveau mellem datacenterets lokaliteter. Hvis der er behov for shared storage, skal det løses på applikations niveau.

4.3 Backup

Statens It tilbyder, som en del af standarddriftsplatformen, at tage backup af løsninger.
Statens It's standard for backup af løsninger anvendes til Disaster Recovery, og backupprocedurerne er således ikke indrettet for at imødegå brugerfejl. På brugerfil niveau har Statens It dog mulighed for restore af enkelt-filer.
En uddybning af Backup og Restore findes i bilag B.

Statens It tager som standard følgende type backup på standardriftsplatformen:

- Daglig backup af servere
- For databaser tages der backup på denne måde
  - Microsoft SQL Server (snapshot)
    - Fuld backup 3 gange i dagtiden
  - Oracle Database
    - Fuld backup 1 gang om ugen
    - Incremental backup 1 gang i døgnet
    - Transaktionslog-backup foretages som standard 1 gang i døgnet. Det kan efter aftale foretages hver time i dagtiden.
  - MySQL
    - Håndteres efter aftale med Statens It
  - PostgreSQL
    - Håndteres efter aftale med Statens It
- Daglig backup af de centrale services, såsom fil og AD service.

I de tilfælde, hvor ovenstående standardbackup ikke er fyldestgørende, bedes der tages kontakt til Statens It.

4.4 Netværk

I dette afsnit er principperne for netværkssikkerhedszoner og principperne for opbygningen af kundernes og Statens It's netværk skitseret.

Specifikke detaljer om netværkets opbygning og komponenter er ikke beskrevet i dette dokument, da det betragtes som fortrolige oplysninger. Er det nødvendigt med mere detaljerede oplysninger, skal der rettes henvendelse til Statens It.

4.4.1 Netværkssikkerhedszoner

Netværkssikkerhedszoner er fundamentet i implementeringen af den netværkssikkerhed, der danner rammen for netværkskommunikation i Statens It's standarddriftsplatform.

En netværkssikkerhedszone er karakteriseret ved at være adskilt med en aktiv sikkerhedskomponent, og at det kun er tilladt for komponenter i en sikkerhedszone at tilgå komponenter i samme zone eller de umiddelbare nabozoner.

Nedenstående tabel viser, hvilke sikkerhedsmæssige principper, Statens It anbefaler i forhold til netværkssikkerhedszoner og udvikling af løsninger.

Princip	Beskrivelse
Defence in depth	En løsning bør separeres i flere niveauer af sikkerhed, således at kompromitteringen af en enkelt komponent ikke eksponerer hele løsningen.
Compartmentalization	Komponenter på samme sikkerhedsniveau bør adskilles logisk og isoleret ved brug af passende sikkerhedskomponenter. Dette sikrer, at løsninger på samme sikkerhedsniveau ikke kompromitterer hinanden.
Minimize attack surfaces	Antallet af tilgange til en løsning skal holdes til et minimum og adgangskontrolleres. Dette gælder på alle sikkerhedsniveauer.

Princippet om *defence in depth* er implementeret i Statens It ved etablering af flere lag af netværkssikkerhedszoner adskilt af sikkerhedskomponenter i form af firewalls.

Princippet om *compartmentalization* er implementeret i Statens It ved etablering af dels netværkssegmenteringer samt logisk ved stram styring af rettigheder.

Antallet af angrebsflader minimeres dels ved at placere et minimum af komponenter i de mindre sikre netværkssikkerhedszoner samt føre en stram kontrol med firewall åbninger i alle sikkerhedszoner. Ydermere stilles der krav om protokol minimering i forhold til de etablerede løsninger for opfyldelse af princippet om *minimize attack surfaces*.

4.4.2 Netværksmæssig opbygning

Statens It's kunder er netværksmæssigt etableret med et klientnet, som har direkte forbindelse til datacenteret. Fra klientnettet kan brugere tilgå servernettet og tilgå internettet via den centrale internetforbindelse i datacenteret.

Kunderne er som standard forbundet med en MPLS linie på 1Gbit.

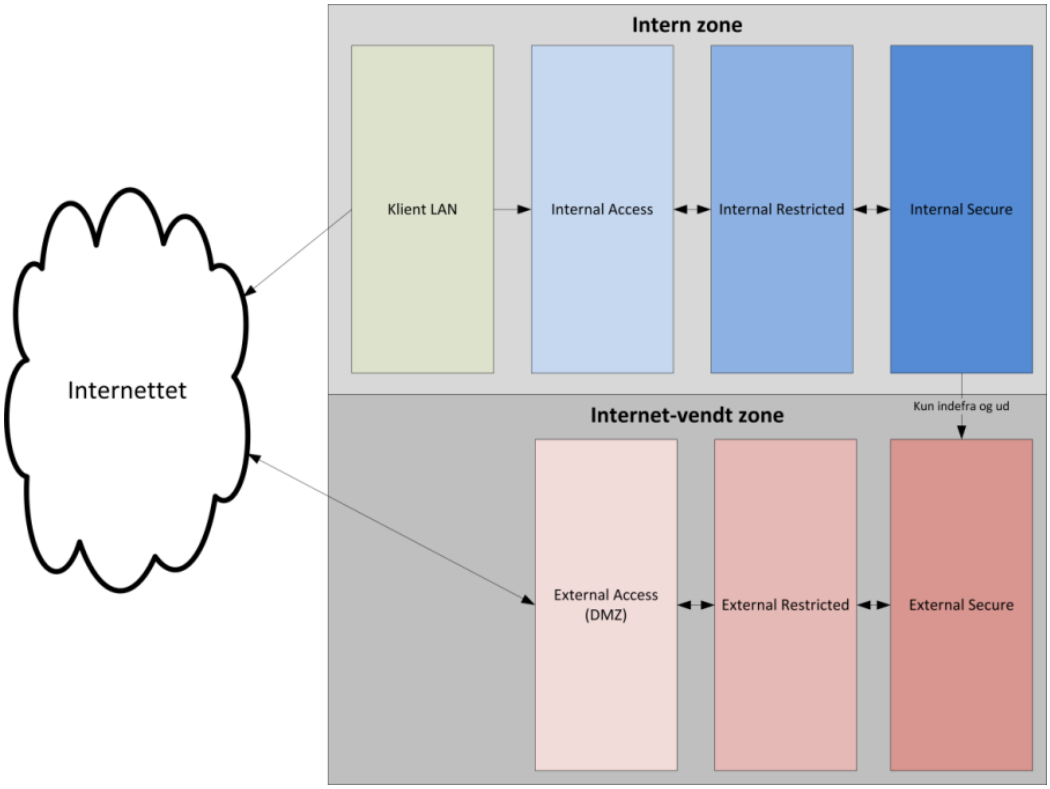
Servernettet er delt op og begrænset i forhold til, at det huser flere kunders it-miljøer. Der er en del af servernettet, hvor kundernes systemer er isoleret og kun kan tilgås af kundens egne brugere. Dette kaldes Hosted Services. Den anden del af servernettet indeholder de services, som deles af alle Statens It's kunder. Her ligger blandt andet AD, mail og fil løsningerne. Dette kaldes Shared Services.

For internetvendte systemer er der opbygget et antal sikkerhedszoner, som er med til at sikre de centrale systemer i servernettet. Sikkerhedszonen "DMZ", som er den yderste sikkerhedszone, er den eneste sikkerhedszone, hvor der er adgang ude fra internettet og ind i Statens It's datacenter. I denne zone er der ikke adgang til det centrale AD. Der er opbygget et alternativt AD i denne sikkerhedszone, som kan anvendes til servicekonti, brugere og sikkerhedsgrupper, såfremt løsningen kan løskobles fra den centrale brugerstyring.

Er der i kundens løsning behov for, at den yderste komponent er integreret med kundens brugerstyring i det centrale AD, skal der laves en specialløsning og Statens It kontaktes herom.

I datacenteret er der yderligere et antal interne sikkerhedszoner, således at ønsker om en høj grad af sikkerhed i form af lagdeling kan efterkommes baseret på princippet *defence in depth*. Statens It anbefaler, at løsninger implementeres med en 3-lags systemarkitektur jf. afsnit 5.

Principperne i opbygningen af "Hosted Services" er skitseret på følgende figur.



4.4.3 B2B forbindelser

Er der behov for en systemmæssig integration mellem kundernes systemer drevet af Statens It og systemer drevet af 3. part, kan der etableres en B2B-forbindelse mellem systemerne.

Fra det centrale servernet kan der etableres forbindelse til 3. parts leverandørens netværk, så der systemmæssigt bliver forbindelse ud til leverandørens løsning.

De forbindelsestyper der kan etableres er en dedikeret MPLS forbindelse eller en ”Site 2 Site” VPN forbindelse.

Ret henvendelse til Statens It i alle tilfælde.

5 Referencearkitektur

Referencearkitekturen er det målbillede, som applikationsleverandører skal sigte imod, når der designes applikationer til afvikling på Statens It's standarddriftsplatform.

5.1 Formål

Formålet med afsnittet er at beskrive Statens It's anbefalede systemarkitektur samt de netværkssikkerhedszoner, der anvendes i Statens It's datacenter. Statens It fokuserer på it-sikkerhed, samarbejder med GovCERT og følger deres anbefalinger samt markedets best practice.

5.1.1 Statens It's anbefaling til valg at arkitektur

Det er Statens It's anbefaling, at alle løsninger baserer sig på en arkitektur, der understøtter en lagdeling af applikationen i mindst 3 forskellige sikkerhedszoner, dvs. at de logiske lag i en løsning er separerede, både logisk og sikkerhedsmæssigt.

5.2 Systemarkitektur

For at imødekomme Statens It's arkitekturprincipper skal de løsninger, der implementeres, gøre brug af fler-lags-arkitektur.

Ved at opbygge en løsning i flere lag, vil der være øgede muligheder for udvikling og modificering af de enkelte lag, uden at hele løsningen skal omstruktureres. Ligeledes opnås mulighed for at placere de forskellige lag i forskellige sikkerhedszoner og dermed have fuld kontrol over hvilke komponenter, der udstilles, for hvilke systemer og brugere.

5.2.1 Logiske arkitekturlag

Flerlags-arkitektur er en klient-server-arkitektur, hvor løsningens komponenter er separeret i logiske arkitekturlag: præsentations-, forretnings- og datalogik.

Figur 6 - Logiske arkitekturlag

Præsentationslogiklag

Øverste lag af en løsning består typisk af en klientapplikation og en eller flere servere til distribuering af præsentationslogikken. Klientapplikationen kan enten være egenudviklet eller browserbaseret og afvikles på en klient enhed. I

dette dokument er præsentationslogikken udelukkende fokuseret på den serverbaserede del af præsentationslogikken.

Forretningslogiklag
Midterste lag af en løsning håndterer den forretningsmæssige behandling af input fra præsentationslaget og data fra datalogiklaget.

I forretningslogiklaget håndteres forretningsregler samt forretningspolitikker, såsom autentificering og autorisation.

Datalogiklag
Nederste lag af en løsning håndterer lagring af data.

Til hver af disse logiske lag har Statens It opbygget en sikkerhedszone, således at i den logiske applikationsstruktur, kan afspejles i en sikkerheds-zoneopbygning, afhængig af om systemet er internt eller internetvendt. Illustreret i nedenstående matrix.

LOGISKE LAG	INTERNE ZONER	INTERNETVENDTE ZONER
Præsentationslogik	Internal Access	External Access (DMZ)
Forretningslogik	Internal Restricted	External Restricted
Datalogik	Internal Secure	External Secure

6 Teknologivalg og roadmap

Statens It's kerneforretning er baseret på sikker og stabil drift, hvorfor der i videst muligt omfang vælges modne teknologier og løsninger.

Det anbefales tredjepartsleverandører at imødegå dette krav om modenhed og ikke basere løsninger på "bleeding edge"-teknologier, men derimod teknologier der allerede er på standarddriftsplatformen.

6.1 Klientplatformen

Klientplatformen er baseret på følgende komponenter:

6.1.1 Operativsystem og sikkerhed

- Windows 7 Professional SP1
- Symantec Endpoint Protection Version 12.1

Roadmap for Klient operativ system

Der er planlagt følgende større ændringer på klientplatformen:

- Windows 10
  Klientoperativsystemet Windows 10 vil blive indfaset i løbet 2017 og 2018.

6.1.2 Grundlæggende applikationer

Grundlæggende applikationer til klientplatformen opdateres versionsmæssigt mere hyppigt, hvorfor nedenstående er et øjebliksbillede.

- Microsoft Office 2010 Professional 32-bit Version 14.0
- LibreOffice (tidligere OpenOffice) Version 5.2
- Internet Explorer 11.0
- Mozilla Firefox. Version 48.0
- Google Chrome. Version 52.0
- 7 Zip 16.00
- Adobe Reader XI Version 11.0
- Adobe Flash Player 22.0
- Adobe Shockwave Player 12.2
- Cisco AnyConnect 4.2
- Citrix Receiver Version 4.2
- Java 8
- PDFcreator 2.3
- VLC Player 2.2
- Notepad ++ 6.8
- Microsoft .NET 4.6

Roadmap for Grundlæggende applikationer

Der er planlagt følgende større ændringer på klientplatformen:

- Microsoft Office 2016
  Office-pakken Microsoft Office 2016 vil blive indfaset i løbet 2017 og 2018.
- Flere af ovenstående applikationer vil blive udfaset som grundlæggende applikationer og overgå til tilvalgssoftware.
  Dette gøres for at minimere vedligeholdelsen af grundimage og for at sikre mindre pladsforbrug til fordel for brugerne.

6.2 Virtuel it-arbejdsplads

Virtualiseringsplatformen er baseret på følgende komponenter:

- Citrix XenApp 6.5 for Windows Server 2008 R2
- Microsoft Windows Server 2008 R2
- Microsoft App-V 5.0 SP2

De grundlæggende applikationer er de samme som på klientplatformen – se afsnit 6.1.2

Roadmap for virtualiseringsplatformen.

- Citrix XenApp 7.9 for Windows Server 2012 R2
  Indfases i løbet af 2017.

6.3 Den mobile platform

Den mobile platform er baseret på følgende komponenter:

- Citrix XenMobile 10.3
- SecureHub 10.4.0

Understøttede operativsystemer

- iOS 10.0 eller nyere
- Android 5.0[7] (Lollipop) eller nyere

Ovenstående krav om "Understøttede operativsystemer" betyder ikke at MIA ikke virker på ældre enheder. Det betyder at Citrix yder ikke support på disse, hvilket igen betyder, at Statens It heller ikke kan supportere ældre enheder.

Statens It understøtter for nuværende ikke Windows Phone platformen.

Roadmap for den mobile platform.
Der er ikke planlagt større ændringer på den mobile platform før efter 2017.

6.4 Serverplatformen

Serverplatformen er baseret på følgende komponenter:

6.4.1 Virtualiseringslag

- VMware vSphere 5.5

6.4.2 Operativsystem og sikkerhed

- Windows Server 2012 (Standard Edition)
- Red Hat Enterprise Linux v 7.3
- Symantec Endpoint Protection Version 12.1 (Windows)

Sikkerhedsopdateringer til operativsystemer udrulles i førstkommende planlagte servicevindue efter udgivelsen.

Roadmap for serverplatformen.
Der er planlagt følgende større ændringer på serverplatformen:

---

7. I løbet af 2017 vil kravet til Android version ændre sig fra version 5.0 til version 6.0 som minimumskrav

- Windows Server 2016
  Server operativsystemet Windows Server 2016 vil blive indfaset i løbet 2017 og 2018.
- Red Hat Enterprise Linux
  Red Hat Enterprise Linux platformen følger Red Hats support lifecycle og frigives når versionerne frigives til fasen "Production 1".

6.4.3 Grundlæggende serverapplikationer

Databasesystemer
- Microsoft SQL Server 2014 SP2 (altid nyeste SP)
- Oracle Database 12c
- MySQL 5.7
- PostgreSQL Database System 9.4

Webserver
- Microsoft Internet Informations Service (IIS) 8.5
- Apache HTTP Server version 2.4

ContentManagementSystem (CMS) Applikationer
- Microsoft Sharepoint Server 2013
- Sitecore XP 8.2
- Drupal 8.1.9

Roadmap for grundlæggende serverapplikationer:
- Microsoft Sharepoint Server 2016
  Microsoft Sharepoint Server 2016 vil blive indfaset i løbet af 2017.

- MySQL og PostgreSQL
  Statens It anvender den version der til enhver tid er tilgængelig på RedHat Sattelite distributionsserver. Denne version anses som vurderet for moden og drifts-stabil.

6.5 Supporting Services

6.5.1 Exchange
- Microsoft Exchange 2010
  - Microsoft Exchange 2010 OWA
  - Microsoft Exchange 2010 EWS

Roadmap for Exchange
- Microsoft Exchange 2016
  Microsoft Exchange 2016 implementeres I løbet af 2016 og 2017.

6.5.2 System management
- Microsoft System Center Configuration Manager 2010
- Red Hat Sattelite

6.5.3 Autentifikation
- Microsoft AD på Microsoft Server 2008 R2 functional Level
- RADIUS Server
- SMS Passcode 6.2

6.5.4 Loadbalancing

- F5 Viprion loadbalancing appliance

6.5.5 Backup

- Veritas NetBackup version 7.7

Roadmap for backup.

- Veritas NetBackup
  Veritas NetBackup opdateres løbende med leverandørens udgivelser, når versionen vurderes moden.

6.5.6 VPN

- Cisco AnyConnect Secure Mobility Client 4.2