



## Koncessionskontrakt vedr. ekspeditionen af pas, kørekort og øvrige borgerserviceopgaver.

Københavns Kommune  
Kultur- og Fritidsforvaltningen

Bilag 3

Beskrivelse af Kundens IT-hardware, software og netværksmiljø



## INDHOLD

---

1	Indledning.....	3
2	Arbejdspladser .....	4
3	Sagsbehandling, udvikling og arkivering .....	11
4	Centralt miljø.....	12
5	Netværksmiljø.....	14
6	Logpoint SIEM .....	20
7	Integrationsplatforme .....	20
8	Store eksterne platforme .....	21
9	IT organisering.....	21
10	Kommende ændringer til KS it-miljø .....	27
11	Koncern IT organisation.....	28
12	Københavns Kommune politiske organisation .....	29



# 1 INDLEDNING

---

## Metadata

Denne udgave af IT-miljøbeskrivelse er sidst opdateret den 22.12.2016.

Dato	Aktivitet	Ansvarlig enhed
	Generel revision	Arkitektur i IT Udviklingscentret (KIT)
22.12.2016	Generel revision	Arkitektur i IT Udviklingscentret (KIT)
20.10.2016	Revision af Integrationsplatforme. Tilføjet SIEM.	Arkitektur i IT Udviklingscentret (KIT)
13.09.2016	Revision af MDM, Servere, Storage, Kvantum	Arkitektur i IT Udviklingscentret (KIT)
06.05.2016	Informationer om Windows10, IE11 og MS Edge	Arkitektur i It Udviklingscentret (KIT).
11.2.2016.	Informationer om smartphones, tablets og printløsninger samt eDoc er blevet opdateret.	Arkitektur i It Udviklingscentret.
12.1.2016.	Informationer om browsere blev opdateret.	Arkitektur i It Udviklingscentret (Koncern IT).

## Københavns Kommunes IT-miljø

Dette bilag indeholder Københavns Kommunes beskrivelse af relevante dele af sit nuværende it-miljø. Københavns Kommune (inkl. selvejende institutioner) benævnes "Københavns Kommune" eller "Kunden" i dokumentet.

Dokumentet er på ingen måde et udtømmende dokument med alle informationer omkring Københavns Kommunes IT, men er ment som en hjælp til leverandøren for at kunne angive eventuelle krav til ændringer i kundens it-miljø som forudsætning for at opfylde kravene i kontrakten.

Beskrivelsen af det administrative IT område i Københavns Kommune kan overordnet opdeles i:

- Arbejdspladser
- Centralt miljø
- Netværksmiljø
- IT-organisation



## 2 ARBEJDSPLADSER

---

### PC-arbejdspladser

Der findes i dag et stort antal forskellige IT arbejdspladser i Københavns Kommune. Disse IT arbejdspladser er primært baseret på PC'er med operativsystemet Microsoft Windows 7. Enkelte PC'er har som test fået installeret Microsoft Windows 10.

Der er registreret ca. 22.000 PC'er, hvoraf 9.000 er bærbare PC'er. Dertil findes et mindre antal PC'er til brug for borgerne. PC'erne fordeler sig aldersmæssigt jævnt. Levetiden for de eksisterende PC'er er gennemsnitlig 40 måneder. Stationære PC'er skiftes også automatisk, når de er 54 måneder gamle. Der forventes en mindre årlig vækst i antal klient-PC'er (ca. 2 %).

Nedenstående skema beskriver fordelingen af PC'er:

Forvaltning	BIF	BUF	KFF	KS	SOF	SUF	TMF	ØKF	Total
Antal PC'er (tal fra Q3 2015)	3.229	3.504	2.053	1.316	5.182	4.181	1.831	836	22.161

Der er et stigende antal bærbare PC'ere og tablets med mobildata 4G-opkobling som ad hoc-opkobling til netværket.

Mobilt bredbånd, 4G/LTE: der er pt. ca. 4.000 mobile bredbåndsopkoblinger og tallet er stigende.

Det er primært til brug for alternativ opkobling uden for kontorarbejdspladsen. Abonnementet er bagud kompatibelt, hvormed 3G netværk også understøttes.

Bruger kan som udgangspunkt fordeles som 20 % tunge brugere og 80 % lette brugere.

Tunge brugere er i denne sammenhæng brugere, som til dagligt benytter tung grafik, tegneprogrammer, mv. og som i dag typisk vil arbejde på en high-end laptop eller workstation med udvidet grafikkort.

Lette brugere er i denne sammenhæng brugere, som primært benytter almindelige kontorpakker, og som i dag typisk vil arbejde på en standard laptop eller standard-PC.

Kunden har ikke noget egentligt estimat over den endelige fordeling og fordelingen kan justeres.

### Citrix-arbejdspladser

Kunden anvender i dag flere systemer, som tilgås via remote desktops som leveres via Citrix XenApp 4.5 og 6.5. Citrix serverfarmen er virtualiseret i VMware servermiljøet.



Der er pt. ca. 2.200 samtidige Citrix brugere på tværs af forvaltningerne. Licensmæssigt er der til 3.000 samtidige brugere.

Totalt set er der ca. 10.000 brugere med mulighed for Citrix adgang fordelt over hele døgnet, ligeledes på tværs af forvaltningerne.

### Mobile arbejdspladser

Der er i dag et stort antal mobile enheder i brug i Københavns Kommune. Mobile enheder forstås som alle enheder, der enten anvender iOS eller Android som styresystem. Windows 10 tablets hører således til i pc-kategorien. KK's koncernfælles telefoniaftale indeholder de mobiltelefoner, der på ethvert gældende tidspunkt er tilladte enheder i KK. For så vidt angår tablets, anvendes der alt overvejende iPads, men også Samsung tablets. Andre typer tablets accepteres ikke. Tablets bestilles via KIT.

Overblikket over fordelingen af mobile enheder i KK primo marts 2017 ser således ud:

Forvaltning	Antal aktive enheder	iOS andel	Android andel
BIF	962	594	368
BUF	2.981	2.254	427
KFF	925	686	249
SOF	3.381	2.119	1.262
SUF	1.194	741	453
ØKF inkl. BR	1.596	1.209	387
TMF	1.986	1.209	777

Som nævnt kan smartphones og telefoner anskaffes via central indkøbsaftale med et begrænset udvalg af modeller og der kan pt. købes smartphones baseret på iOS og Android.

Tablets indkøbes via central indkøbsfunktion og er primært baseret på iOS og Android. Der er en stigende anvendelse af tablets, både som egentlig erstatning af tidligere pc-arbejdsplads og ved digitalisering af nye forretningsområder.

### Profilhåndtering

I dag bruges Windows standard profilhåndtering, hvor der gemmes en profil lokalt på computeren. Som hjælpeværktøjer benyttes UPHC og DELPROF fra Microsoft til at fastholde profilens integritet og sikre, at der ikke ligger gamle versioner af profiler og skaber problemer. Der benyttes GPO til profilhåndtering.

### Printløsning

Der findes ikke én standardiseret printerløsning i Københavns Kommune.



Printerløsningen dækker i dag mange forskellige behov i kommunen, hvilket gælder integration til Citrix-plattformen, og steder i Københavns Kommune, hvor internetforbindelsen er langsom. Ydermere understøtter printerløsningen store såvel som små institutioner.

På en række små lokationer, såsom børneinstitutioner og lignende, forefindes der typisk installationer som er sat op med lokalprint. Det er installationer med print via usb-port.

På stort set alle lokationer er print opsat til Windows-print via Koncern ITs printservere. Der er på nuværende tidspunkt 16 printservere, opsat med fortrinsvis Windows Server 2008. Antallet af servere udvides efter behov. Hele denne installation er baseret på virtuelle servere.

Derudover kører hele Sundheds- og Omsorgsforvaltningen, dele af Børne- og Ungdomsforvaltningen samt få brugere i øvrige forvaltninger. Her tilbydes Universal Print Driver via Citrix, og der kan således printes på stort set alle tilgængelige netværksprintere og lokale printere via denne løsning

Decentralt print er en del af Københavns Kommunes printopsætning. En meget stor del af kommunens fagsystemer printer via decentralt print. Der er indkøbt en del printeridenter hos KMD. Disse tildeles af Printservergruppen i KS som videreformidler identen til brugerne, som selv indsætter i deres fagsystem.

På enkelte lokationer er der indført SKY-Print også kaldet Follow-Me print. Systemet hedder PaperCut og kan udvides med mulighed for Mobil Print – print fra mobile enheder. Funktionaliteten i Mobil Print er, at man via mail fra sin mobile enhed kan sende print til SKYen.

Print frigøres fra SKYen ved hjælp af en Mifare chip, som den enkelte bruger skal være i besiddelse af – ellers frigøres det via en webside, som bruger logger på.

### **Periferiudstyr<sup>1</sup>**

Den enkelte IT-arbejdsplads benytter udover selve PC'en op til flere tilknyttede periferikomponenter. De mest generelle er skærm, tastatur og mus. Derudover benyttes som tidligere nævnt ofte lokalt tilsluttede printere.

Af andre komponenter som kan forekomme er fx:

- USB-devices generelt
- USB disks/sticks
- Trådløse mus/keyboards (Bluetooth, wireless m.m.)
- Ergonomisk rullemus (en rullestang placeret nederst på keyboard)
- USB drev (CD/DVD)
- skærms løsning (flere skærme end 2 forekommer, men sjældent)
- Mobiltelefon synkronisering

---

<sup>1</sup> Listen er på ingen måde en udtømmende. Den viser de mest anvendte typer



- Tablets (drawboards)
- IP telefoni
- Headset
- Kortlæser

### **Software**

Software installeres dels igennem images (præinstallerede), dels efterfølgende gennem Microsoft Configuration Manager 2012 (SCCM).

Software kan også hentes via Shoppen, der anvender SCCM. Shoppen indeholder over 500 forskellige applikationer.

Der findes endvidere ca. 450 fagsystemer med tilhørende software hos Københavns Kommune, hvoraf ca. 20 % er indeholdt i de ovenfor nævnte pakker.

### **Adgangsgivende systemer**

Følgende systemer opfattes som helt centrale i forhold til brugeradministration:

- ZI-sikkerhedssystem - CICS1 (KK-mainframe)
- CICS 87 (KMD mainframe) og CICS 1 (KK mainframe). CICS 1 er under udfasning
- Microsoft Active Directory
- KKorg
- Digital signatur
- KØR / KVANTUM
- Navision
- KOS2
- SAP
- KMD Opus Løn
- CSC social
- Airwatch

Der findes flere små systemer, der administreres via andre sikkerhedssystemer, som vil opfattes som centrale af forvaltningsforretningen.



#### KSP CICS

KSP CICS er KMD's sikkerhedssystem. De KMD applikationer, som Københavns Kommune anvender, er i ét eller anden omfang baseret på KSP/CICS.

IBM NVAS er blevet implementeret som broker mellem bruger og KMD systemerne. Der er implementeret 1 NVAS til KK systemer og 1 til KMD systemer.

Brugeradministrationen anvender KSP/CICS til at administrere brugerautorisationer, hvilket indebærer:

- oprettelse og ajourføring af brugerprofiler
- oprettelse og ajourføring af brugere og deres autorisationer
- tildeling af unik brugerident

Alle brugere får tildelt brugeridenter via ZI-sikkerhedssystemet i CICS1 (KK-mainframe).

Københavns Kommune anslår, at under 50 % af de 20.000 brugere anvender SAP-baserede systemer, herunder lønsystemet. KK kan pt. ikke med sikkerhed sige, om tallet mere præcist er 10 % eller 45 %.

Københavns Kommune stiller SPML version 1.0 interface til rådighed til integration til KSP/CICS.

#### Microsoft Active Directory

AD anvendes i dag til styring af brugere og roller i forhold til fil- og printressourcer.

I BIF og SOF oprettes brugerne via en natkørsel baseret på udtræk i KSP/CICS

I SUF anvendes Hyena, i øvrige områder arbejdes direkte i AD. Der anvendes desuden Group Policies i det omfang det er muligt. Der anvendes Hyena fra SystemTools Software Inc. som værktøj til administration af brugere, grupper mm.

#### KVANTUM

Kvantum, der er Københavns Kommunes nye ERP-system, forventes at afløse KØR og en række Microsoft Navision installationer i løbet af 2018 med indkøring i TMF allerede i januar 2017. Kvantum er bygget på en SAP-plattform.

Kvantum understøtter alle processer indenfor budget, budgetopfølgning, regnskab, økonomisk ledelsesinformation, projektøkonomi, målstyring, indkøb, lager og likviditet.

Kvantum vil p.t. erstatte 37 eksisterende systemer og have relationer til ca. 50 andre.

#### KØR

Økonomisystemet består af brugerfunktionalitet til håndtering af regnskabsopgaver såsom finansbogføringer, interne fakturaer, elektronisk indkøb, godkendelse og betaling af leverandørfakturaer (elektroniske og manuelle fakturaer), cash management, registrering og afsendelse af debitorfakturaer





(manuelt og elektronisk), automatisk registrering af indbetalinger, registrering og afskrivning af anlægsaktiver, projektregnskaber samt vedligehold af kommunens kontoplan.

Systemet afleverer dagligt udbetalinger til bankerne og Nemkonto, ligesom det dagligt modtager indbetalinger fra bankerne. Systemet håndterer endvidere opkrævninger via PBS.

Økonomisystemet modtager og afsender e-fakturaer via Nemhandelssystemet i Danmark

#### KKorg (APOS2)

KK-org (som også kendes under navnet APOS2) er Københavns Kommunes autoritative kilde til informationer om organisatoriske forhold samt diverse klassifikationer i forhold hermed. KK-org indeholder bl.a. oplysninger om:

- De enkelte enheder i den administrative organisation
- De hierarkiske strukturer som den enkelte enhed indgår i (fx ledelseshierarkiet)
- Lederne af enhederne og disses evt. stedfortrædere
- Særlige rolle mv.

Herudover udstiller KK-org data fra andre autoritative systemer. Dette drejer sig pt. om data om medarbejdere i Københavns Kommune (ansættelsesforhold eller engagementer) og it-brugere (medarbejdere samt f.eks. eksterne konsulenter). Disse data hentes primært fra hhv. lønsystemet OPUS og kommunens administrative AD, men KK-org er selv autoritativt for udvalgte kontaktoplysninger mv.

KK-orgs indhold af data om de organisatoriske enheder er bestemt af hvilke oplysninger, et givet system eller en given service efterspørger om enhederne. Pt. kan der om en enhed registreres op mod 40 forskellige oplysninger, idet disse datamodelmæssigt er knyttet til enten selve enheden eller til den/de geografiske placering(er), som enheden har (denne kobling kaldes for en lokation). Eksempler på disse data er:

- Navnet på enheden.
- Et eventuelt forkortet navn (benyttes af lønsystemet OPUS som maksimalt kan håndtere 39 tegn).
- CVR-nummer.
- SE-nummer.
- EAN.
- Enhedstype (f.eks. skole, beskæftigelsescenter, plejehjem med aktivitetstilbud).
- Ejerskabsforhold (kommunal, selvejende, privat).
- Organisationstype (en klassifikation målrettet borgervendte løsninger).
- Organisationsplacering
- Distriktsmæssig placering (benyttes ikke i alle forvaltninger og er forskellig fra forvaltning til forvaltning).
- To referencefelter til brug for mapningen imod kommunens økonomisystem, KØR



- Det såkaldte administrative enhedsid ("SAP-nøglen"), som er den nøgle, som anvendes i OPUS

I forbindelse med oprettelse af en it-bruger kobles ansættelsesforholdet i KK-Org med it-brugeren. Hertil har KS et KK-org staging område (MySQL database), som data om personale og organisationen læses fra.

KS Integration til KK Staging foregår hovedsageligt over KS Integration som er bygget op om en Microsoft IIS platform, hvor programmeringssproget PHP anvendes til udvikling af integrationer. REST er den primære protokol der anvendes på KS Integration og KK Staging.

#### SAP

Integration til SAP kan ske via standard SAP BAPI.

#### Airwatch

Airwatch er KK's Enterprise Mobile Management (EMM)-system til mobile enheder. Alle brugere, der skal anvende Airwatch på deres enheder, skal registreres og tildeles rettigheder i Airwatch. Dette sker i samarbejde med Brugeradministrationen.

Airwatch styrer den grundlæggende sikkerhed på alle mobile enheder samt application management i forhold til adgang til mail, kontakter og kalender samt de fagsystemer, der skal tilgås fra de mobile enheder enten via Airwatch's Secure Browser eller via en app. Når apps styres fra Airwatch opnås Single Sign On på enhederne og dermed samme sikkerhed, som fra en administrativ pc.

#### **Systems Management på arbejdspladser**

PC'er og applikationer installeres via images (operativsystem) og pakker fra centralt hold. Symantecs Altiris er centralt system management værktøj til denne håndtering af PC'erne. Bl.a. installeres antivirus m.m. gennem dette værktøj.

Alle applikationer publiceret via Citrix installeres i Citrix som msi-pakker via Citrix applikation Manager, dvs. at alle Citrix distribuerede applikationer forefindes som msi-pakker. I forhold til de systemer og pakker, der leveres som msi anvendes Wise Package Studio som værktøj til generering af installationspakker

Københavns Kommune anslår at have licens til 10.000 brugere af Symantec Endpoint Virtualisation.

Atrium (BMC/Remedy): CMDB'en er implementeret og der er tilført følgende dataklasser:

- PC'er
- Org.nr.
- Lokationer
- Datalinier
- Token
- ADSL

KØR-org.nr. opdateres via daglig import fra KØR/RUBIN.

Lokationer opdateres via daglig import fra KK-org.



Data om PC'er opdateres via automatiserede processer i Remedy og Altiris. Dette sikrer opdatering af Status samt relation til Lokation og KØR-org.nr. for hver enkelt PC. Derudover opdateres CMDB med skanningsdata fra Altiris og fra selvudviklet skanningsværktøj.

Data om Datalinier, Token og ADSL opdateres manuelt.

Data i CMDB'en udgør faktureringsgrundlag mod forvaltningerne. Data er tilgængelige for kunder og interne brugere via frontenden <http://cmdbviewer>. Internt er data desuden tilgængelige via Remedys Incident modul.

I pipeline er data om følgende:

- Mobilsync (kobling til AD som kilde)
- Server (kobling til FISKK + Symantec Server Manager + evt. Altiris Asset som kilder)
- Print, kopi, skan
- Tablets (med enhedens serienummer som nøgle)

Altiris er implementeret som Licensstyringsværktøj. Der er pt. ingen integration ml. Software Asset Management i Altiris og BMC Atrium CMDB eller Remedy.

### **Browsere**

Københavns Kommune anvender en dualstrategi for browsere på pc'er rettet imod intern administrativ anvendelse, hvilket inkluderer de følgende browsere:

1. Microsoft Internet Explorer 11.
2. Microsoft Edge
3. Google Chrome for Business.

I forbindelse med opgradering til Windows 10, vil også browseren Microsoft Edge være tilgængelig. Tests på diverse systemer i Københavns Kommune viser dog, at disse systemer ikke er kompatible med Microsoft Edge, hvorfor IE 11 bliver installeret på Windows 10 PC'er.

## **3 SAGSBEHANDLING, UDVIKLING OG ARKIVERING**

---

### **Fujitsu eDoc 4.1**

I Københavns Kommune anvendes Fujitsu eDoc 4.1.9 som det primære Elektroniske Sags- og Dokumenthåndteringssystem (ESDH). Notater, indstillinger, referater og kommunikation med borgere samt virksomheder bliver arkiveret i eDoc.

Der findes i øjeblikket flere integrationer fra fagsystemer til Fujitsu eDoc med henblik på at lette sagsgangen og journaliseringspligten for medarbejderne i Københavns Kommune. Der kan udvikles nye integrationer til



Fujitsu eDoc, men dette har licensmæssige konsekvenser for Københavns Kommune og skal koordineres med systemejeren for eDoc.

#### **JIRA**

I forhold til udvikling og fejlhåndtering anvendes Atlassian JIRA v.6.3.4 med Atlassian Greenhopper v. 6.2. De to løsninger bruges af IT Rådgivning og Udvikling, Koncern IT Infrastruktur (servere) og Københavns Borgerservice (multisite platformen m.m.). JIRA anvendes også af eksterne udviklingsleverandører til håndtering af udviklingsprojekter for Københavns Kommune. Der er planlagt opgradering til version 7.2.4 i starten af 2017.

## **4 CENTRALT MILJØ**

---

### **Servere**

Københavns Kommunes servere er primært placeret i to datacentre sikret med elektronisk overvågning og adgangskontrol. Datacentrene er strømforsynet fra et "no break" anlæg med redundant kølemiljø. De to datacentre er placeret geografisk på hver sin lokation.

I datacentrene er der ca. 1450 virtuelle servere, og et mindre antal fysiske servere, fortrinsvis baseret på operativsystemet Windows server. Servere er virtualiseret på en VMware ESX 5.5i infrastruktur.

Windows-servere er primært Windows Server 2008 R2. Nye servere deployes med Windows Server 2012 R2.

De fysiske virtualiseringsservere (ca. 50 host servere) er implementeret fra marts 2013 og fremefter. Host serverne vurderes at have en levetid på 4 år.

### **Storage**

#### NAS/Netværksdrev:

Datalagring af vores netværksdrev ligger i dag på EMC Isilon, hvor der kører en Active/Passive asynkron løsning i mellem DC1 og DC2. Vi har ca. 519 TB kapacitet, og vi bruger omkring 70 % af kapaciteten.

#### Primær storage:

Vores primære storage består af EMC VNX5700 (Tiering med: SSD-SAS-NL-SAS). Virtualisering af storage miljøet via VPLEX, som sørger for Active/Active og Synkron lun replikering. Vi har ca. 300 TB, og vi bruger 90% af kapaciteten.

#### Extreme storage:

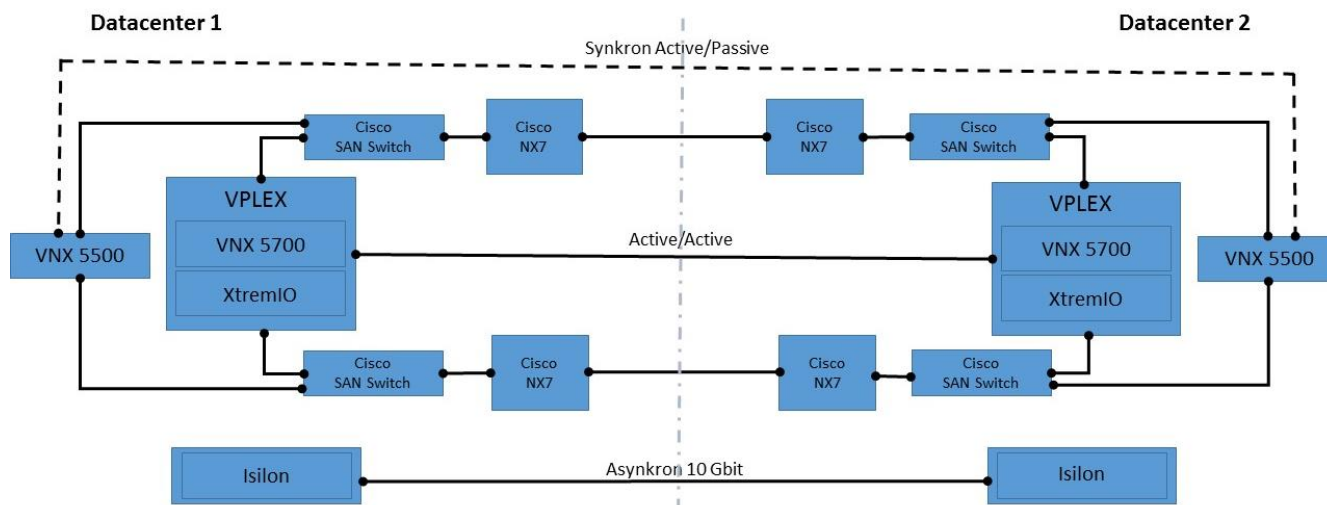
Vores storagemiljø til databaser eller applikationer, der har behov for god performance, er EMC XtremIO via VPLEX, som giver mulighed for Active/Active. Vi har ca. 15 TB, og vi bruger i dag omkring 56% af kapaciteten.

#### Archive/Backup storage:

Vores storagemiljø til Test, Preprod, Archive, Backup og udviklingsservere kører Active/Passive Synkron lun replikering. Vi har ca. 190 TM, og vi bruger ca. 90% af kapaciteten.



Storage miljøet er illustreret i nedenstående:



#### systems management på servere

Til management på servere benyttes SCCM / System Center Configuration Manager til installation af programmer og patchmanagement. Til overvågning og rapportering anvendes SCOM / System Center Operations Manager.

#### Mailsystem

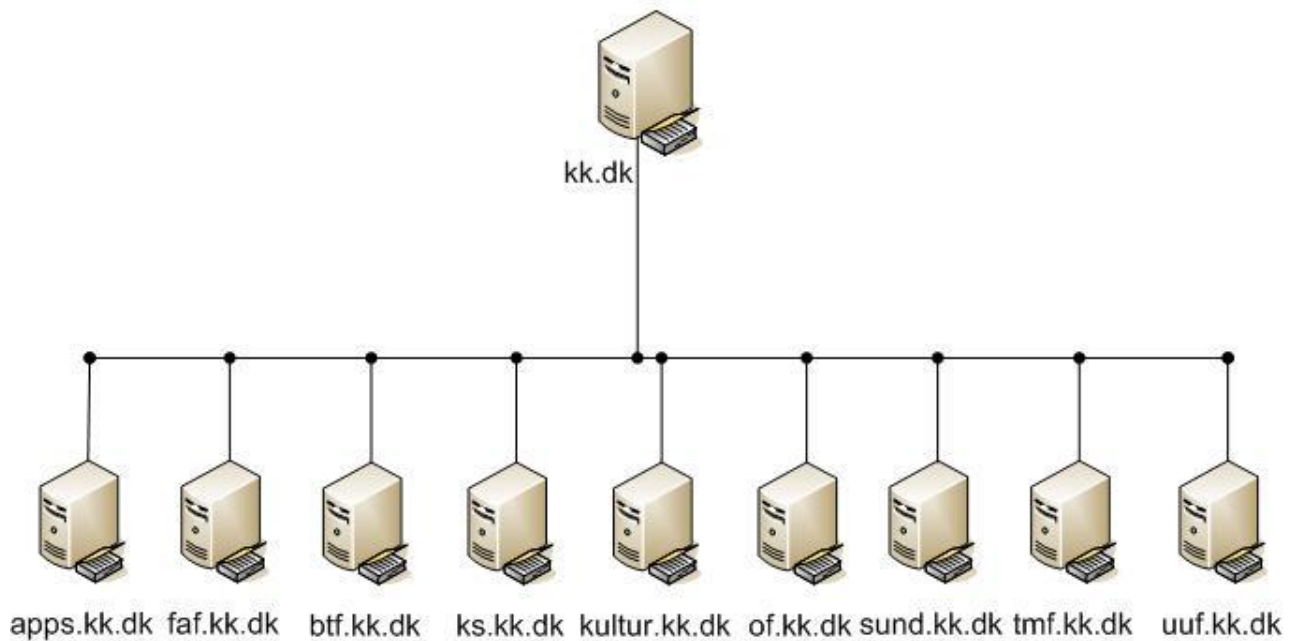
Kommunens fælles mailsystem afvikles på Microsoft Exchange 2013 SP1 CU8.

#### Certifikat-infrastruktur

Københavns Kommune anvender en 2-tier certifikat-infrastruktur fra Microsoft baseret på Windows Server 2003. Certifikatinfrastrukturen er under migrering til 2008. P.t. anvendes 2008-miljøet til udstedelse af certifikater til mobile enheder.

#### AD

Kommunens fælles AD er opbygget som Single Forest multiple domains, jf. nedenstående tegning. Domain controllers er baseret på minimum Windows Server 2008 R2. Forest level niveau er 2008 R2. Niveaulet vil i løbet af 2016 blive løftet til Microsoft Windows Server 2012 R2.



I DMZ ønskes anvendt Secure LDAP og/eller Global Catalog for sikring af AD-kommunikationen.

### **Intranet**

Kommunens intranet er baseret på Drupal. Visning på forskellige enheder er understøttet med responsive design.

Adgang til intranettet kontrolleres via standard LDAP-opslag i AD. Der anvendes en autentifikationsmekanisme, hvor løsninger der autentificerer mod intranettet på C-name skal kunne understøtte fallback til auth mod A-name.

### **Test-/udviklingsmiljø**

I dag findes ikke deciderede/dedikerede test-, udviklings- eller præproduktionsmiljøer. Det vælges fra system til system om der etableres et test-, udviklings- eller præproduktionsmiljø.

## **5 NETVÆRKMILJØ**

---

Serverne er forbundet via et switchet netværk, baseret på Ethernet, som også forbinder Københavns Kommunes institutioner til it-miljøet i datacentrene. Mellem de decentrale institutioner og de centrale serverrum er dette netværk baseret på optisk fiberkabling.



Københavns Kommunes netværk består primært af en Cisco infrastruktur. Netværket består af en central layer-3 collapsed core (routed), hvortil der er tilsluttet en vifte af accessteknologier.

Designmodellen er 2-lags, med et collapsed core og et accesslag.

Collapsed core er en sammensmeltning af core-lag og distributions-lag til en fysisk enhed.

#### **Remote access**

Der findes fjernadgange med adgang via VPN.

Nogle af disse er rene mailklienter, dvs. løsning baseret på web-mail.

Alle remote access løsninger benytter en form for token løsning.

Den ene løsning er en Citrix Access Gateway Advanced, via en Citrix Netscaler løsning.

Derudover haves en Cisco AnyConnect løsning som også benytter en 2 faktor validering via SMS token.

#### **Token løsning**

Der benyttes p.t. Vasco SMS token til remote adgang. Løsningen er en sms-baseret token med rullende kode sendt til mobilt device.

Løsningen understøtter umiddelbart SSO.

#### **Datacenter (collapsed core)**

I datacentrene er der layer-2 og layer-3 teknologi, hvor det er muligt at oprette virtuelle netværk.

#### **Accesslag**

##### Access på xDSL

Der er meget få forbindelser som er baseret på DSL.

Accessteknologierne er en kombination af layer-2 og layer-3 teknologier, og er en kombination af xDSL og ethernet (med forskellige båndbredder).

Hvor der anvendes xDSL, leveres det som en routed løsning.

##### Access på ethernet

Hvor der anvendes ethernet som accessteknologi leveres også i flere varianter typisk via en 100Mbit fiber m/MPLS:

Opkoblingen til Københavns Kommunes centrale ressourcer og eksterne forbindelser leveres på gigabit ethernet.



### Separering

I et antal tilfælde er enkeltforvaltninger (BUF) separeret fra eller i proces med at blive separeret fra den øvrige kommunale layer-3 løsning.

Samlet oversigt over accesstyper til Københavns Kommunes institutioner:

- Gigabit ethernet.
- 100 Mb ethernet.

Forbindelsen mellem datacentrene er 10 Gbit (fiber) med fuld redundans.

På ethernet access leveres i ISP'ens switch typisk en 100 Mbit MPLS forbindelse.

### Trådløst netværk

Københavns Kommunes trådløse netværk er baseret på en Aruba platform. Netværket består af redundante centrale kontrollere, der terminerer wifi-trafikken via krypterede tunneler fra hvert enkelt AP/SSID, ind i centrale komplekse vlan og dmz-miljøer. Løsningen har decentrale firewall-, båndbredde-, sitedscanning og quality of service funktioner.

Løsningen er integreret ind i AirWave overvågning, ClearPass adgangskontrol samt Radius- og Certifikatvalidering..

### 3/4G-netværk/APN

Københavns Kommune har både usikrede 3/4G-netværker og sikrede netværker (APN). De primære sikrede leveres af TDC og er opsplittet i separate adskilte netværker tildelt de enkelte løsninger. Det hele afleveres i redundante MPLS/fiber opkoblinger til dmz-zoner i kommunens 2 datacentre. Der er ligeledes en tilsvarende løsning med Telenor, men hvor den sikrede trafik afleveres via APN over internet.

Adgang styres af mobiloperatørerne og sker primært via manuel tildeling af simkort, PIN-kode og specielle APN-navne. Adgang er under omlægning til Radiusvalidering baseret på MDM base.

### Enterprise Mobile Management (EMM)

Airwatch by VMware anvendes som Københavns Kommunes EMM-system. Airwatch er obligatorisk på alle mobile enheder (smartphones og tablets), der enten skal foretage mailsynkronisering eller give medarbejderen adgang til fagsystemer, som indeholder person- eller værdiopllysninger. Det er kun mobile enheder med styresystemerne Android og iOS, der kan anvende Airwatch.

Fagsystemer kan tilgås enten som "Native app's" eller via Airwatch's Secure Browser. Secure Browser gør det muligt for medarbejderne med smartphones og tablets at kunne tilgå webbaserede applikationer der er tilgængelige på Københavns Kommunes administrative netværk (sikker zone).





Airwatch agenten, der er installeret på den mobile enhed, er omfattet af SSO, så denne slår op igennem Airwatch i Active Directory om brugeren har brugerrettighederne til de specifikke apps. I tilfælde af enheden er offline, så slår AirWatch agenten op i en lokal kopi af seneste brugernavn og password.

Agenten på den mobile enhed slår også op i Airwatch med henblik på at verificere om enheden lever op til de krav, som stilles af Airwatch til om, klienten kan afvikle applikationer. Airwatch installationen har ikke kendskab til brugernes kodeord eller brugernavne, disse håndteres af henholdsvis Active Directory og agenten på Airwatch. Særligt gælder det at kodeordet på Airwatch er krypteret på enhederne, hvor agenten er installeret.

Alle tablets med Airwatch er indkøbt og udleveret af Koncern IT. En stor del af de anvendte smartphones er ~~også~~ indkøbt og udleveret gennem Koncern IT telefoniaftale. Da både Airwatch-server og –klient opdateres jævnligt, stiller det ligeledes krav til telefonernes hardware, ligesom de jævnlige opgraderinger af styresystem og fagsystem påvirker telefonens eller tablettens funktionsevne. Der er ikke fastsat en levetid for hverken mobiltelefoner eller tablets. Levetiden for enheder bestemmes således af det forretningsmæssige formål og den tekniske kompatibilitet med de afviklende forretningsapplikationer.

Politikken er at alle mobile enheder, som udgangspunkt er på seneste version af styresystemet og max to hovedversioner bagud. Det medfører i praksis, at iOS enheder har en maksimal levetid på ca. 4 år, hvor Android enheder ikke kan forventes at have en levetid højere end 1½-2 år, hvorefter de ikke længere er kompatible med de gældende versioner af styresystemet.

Vi henviser til vores positivliste over telefoner og tablets for gældende, anerkendte modeller. I forhold til supporterede versioner af styresystemer kan altid tages udgangspunkt i den seneste version og 2 hovedversioner bagud.



### Understøttede iOS styresystemer

iOS 10.0	
iOS 9.x	

### Understøttede iPhones

iPhone SE	
iPhone 6s plus	
iPhone 6 plus	
iPhone 6s	
iPhone 6	
iPhone 5s	
iPhone 5c	
iPhone 5	
iPhone 4s	Kan kun opdateres til iOS 9.3.x og ikke 10.x.

### Understøttede iPads

iPad Pro 12.9-inch	
iPad Pro 9.7-inch	
iPad Air 2	
iPad Air	
iPad 4th generation	
iPad 2	Kan kun opdateres til iOS 9.3.x og ikke 10.x.
iPad mini 4	
iPad mini 3	
iPad mini 2	



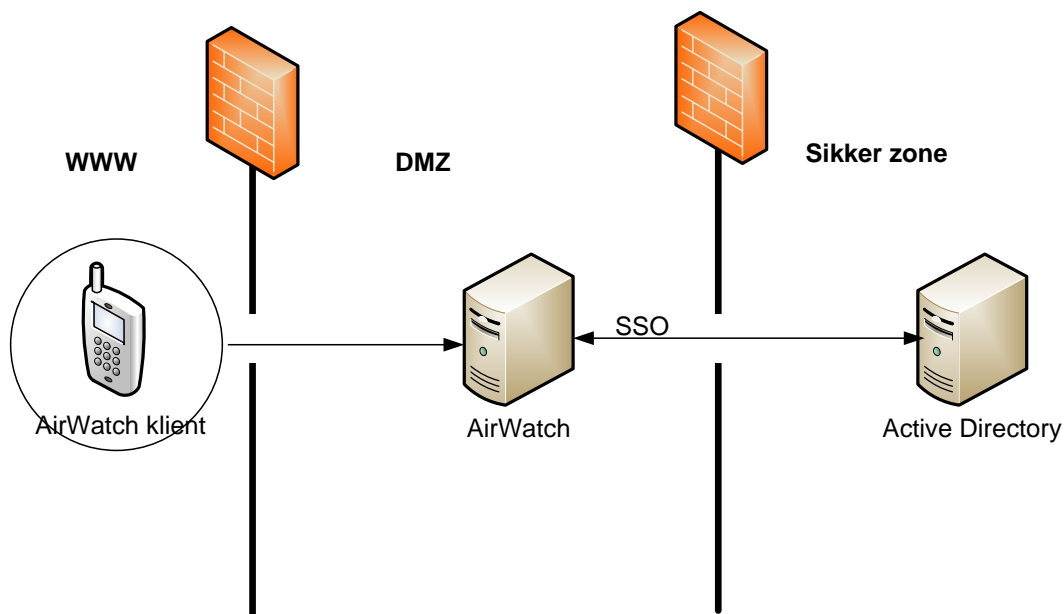
En mulighed for udvikling af applikationer til at fungere på den mobile platform under Airwatch, vil være at udvikle dem som webapplikationer og lade disse være driftet på Københavns Kommunes sikre zone, hvor smartphones og tablets vil kunne tilgå applikationerne, hvis webapplikationerne er bygget på responsivt design.

En anden mulighed vil være ved at anvende VMware SDK standard eller industristandarden AppConfig.org (tidligere ACE), hvor app'en får en Airwatch-skal om sig, der sikrer tunneltrafikken og brugerverifikation.

En tredje mulighed vil være ved at oprette en mini-VPN forbindelse mellem app'en og de bagvedliggende fagsystemer på Sikker Zone. Det skal noteres, at ved denne mulighed vil der ikke være Single Sign On. Dette kræver at app'en ligger indenfor Airwatch skallen, altså enten afvikles fra Airwatch Secure Browser eller som app udviklet med AppConfig.org standarden eller VMWare/Airwatch's SDK.

Ansvar for en sikker implementering af mobile fagsystemer på Airwatch ligger hos Mobility teamet i KIT. KIT's Mobility team har ansvaret for KK Airwatch installationen, og at systemet kan agere som forudsætningssystem for de forretningskritiske og livskritiske fagsystemer, der skal fungere på en mobil platform. Den enkelte systemejer har ansvaret for sit eget system, mens KIT's Mobility team har ansvaret for den sikre afvikling af løsningen.

AirWatch kan ikke anvendes til at sende eller modtage Digital Post (eBoks).





## 6 LOGPOINT SIEM

---

Logpoint SIEM (SIEM) er en Security Information and Event Management-løsning, som er implementeret i kommunens it-infrastruktur med det formål, at forbedre monitoreringen af kommunens it-systemer og give øget mulighed for logning og rapportering.

Konkret identificerer, overvåger, registrerer og analyserer SIEM hændelser i og omkring kommunens systemlandskab ved hjælp af logning. SIEM gør det muligt at sammenstille hændelser på tværs af mange logkilder og dermed sikrer kommunen mod misbrug og muliggør det at sætte ind mod trusler og angreb.

Følgende metoder kan anvendes for at overføre loggen til Logpoint SIEM:

- Syslog
- SNMP
- FTP
- Flows
- SCP
- SDEE
- OPsec
- WMI
- Agent

## 7 INTEGRATIONSPLATFORME

---

Københavns Kommune råder over følgende typer integrationsplatforme.

### RASP

REST API Service Proxy filtrerer funktionskald fra WWW og DMZ. Al indgående trafik skal gå igennem RASP, som validerer indholdet.

### KKI

Københavns Kommunes Integrationsplatform håndterer funktionskald til de fleste datakilder til brug på det netværk, som er kategoriseret som sikker zone.

KKI kaldes som udgangspunkt med REST API og svarer JSON. Der skal laves et dedikeret API per frontend-system. Alle datakilder skal som udgangspunkt tilgås igennem KKI. KKI er baseret på open source integrationsplatformen Wildfly med følgende komponenter installeret:

- Apache Camel
- Apache CXF
- Apache ActiveMQ



Hertil med understøttende teknologier:

- Java 2 SE (Standard Edition)
- Spring

KK anvender byggeserver-plattformen Jenkins til at compile integrationer.

## 8 STORE EKSTERNE PLATFORME

---

Københavns Kommune anvender komplekse IT-løsninger til forskellige fagspecifikke formål, og i den forbindelse er flere platforme outsourcete til eksterne leverandører. Nedenstående er eksempler på disse og ikke en udtømmende liste:

- CSC Social hos CSC
- CSC Sundhed hos CSC.

## 9 IT ORGANISERING

---

I de følgende afsnit beskrives Københavns Kommunes IT-organisering i Koncern IT.

### IT Sikkerhed

Borgerrepræsentationen vedtager kommunens IT-sikkerhedspolitik og IT-sikkerhedsregulativ. Overborgmesteren og de enkelte borgmestre har ansvaret for IT-sikkerhedsarbejdet inden for de enkelte forvaltningsområder.

Myndighedsopgaverne på IT-sikkerhedsområdet varetages i Koncern IT af henholdsvis af IT-sikkerhedsmyndigheden, IT-sikkerhedsfunktionen, IT-driftsorganisationen og Brugeradministrationen.

Arbejdsgrundlaget for myndighedsudøvelsen er Københavns Kommunes IT-sikkerhedshåndbog som er baseret på den internationale standard ISO 27001-2.

Koncern ITs IT-sikkerhedsmyndighed varetager ved tilsyn kommunens behov for at leve op til, og dokumenterer, overholdelsen af gældende love om beskyttelse af persondata.

IT-sikkerhedsmyndigheden sikrer at tilsynet med IT-sikkerhedsområdet i København s Kommune koordineres med intern og ekstern revisors udførelse af revision på området.

Tilsynet skal sikre at kommunens IT-sikkerhedsregler er i overensstemmelse med gældende lovgivning og evt. særlige politisk administrative ønsker.

Koncern IT IT-sikkerhedsmyndighed er forankret i enheden, IT Udviklingscenter.

IT-sikkerhedsfunktion fører det daglige tilsyn med overholdelsen af kommunens IT-sikkerhedsbestemmelser og koordinerer kommunens IT-sikkerhedsarbejde. IT-sikkerhedsfunktion er organisatorisk forankret i IT Driftscentret.



IT-sikkerhedsfunktionen løser en række myndighedsopgaver som fx:

- Rådgiver om IT-sikkerhedsmæssige forhold.
- Godkender sikkerhedsløsningen ved anskaffelse af i nye systemer
- Sikrer at forvaltningerne foretager kontrol af medarbejdernes adgangsrettigheder og autorisationer
- Ansvarlig for at der foreligger procedurer som sikrer tværgående styring af it-beredskabet.
- Håndterer IT-sikkerhedshændelser og IT-sikkerhedsbrud
- Ansvar for fælles informations og uddannelses materiale, herunder opbygning og opdatering af kommunens IT-sikkerhedshåndbog og supplerende vejledninger.

Koncern ITs driftsorganisation og Brugeradministration varetager også myndighedsopgaver inden for IT-Sikkerhed (Enhedens øvrige ansvarsområder beskrives i selvstændige afsnit længere fremme).

Eksempler på driftsorganisationens myndighedsopgaver:

- Ansvar for sikkerheden på kommunens IT-platforme.
- Det IT-sikkerhedsmæssige ansvar for opbygning og anvendelse af it-driftsmiljø og kommunikationsforbindelser samt for de fysiske sikringsforanstaltninger i forhold til kommunens netværk, netværksudstyr og servere m.v.
- Udarbejder it-sikkerhedsforskrifter eller retningslinjer for it-installationer/driftsmiljø og de benyttede netværk.

Eksempler på Brugeradministrationens myndighedsopgaver:

- Ansvar for aftaler om og udførelse af brugeradministration af de systemer kommunens medarbejdere benytter.
- Sikre at der findes retningslinjer for adgangsstyringen af de enkelte systemer (dvs. hvilke medarbejdergrupper skal benytte systemet, hvilke rettigheder herunder dataadgang og funktioner må tildeles).
- Ansvar for den løbende opbygning og vedligeholdelse af medarbejdertyper.
- Sikre at der i forbindelse med brugeradministrationen altid er et gyldigt revisionsspor.

### **Support**

Supportfunktionen ligger i Serviceindgangen, som er Koncern ITs 1.level support og modtager derfor alle henvendelser.

Alle henvendelser kan ske via telefon eller selvbetjeningsløsningen.

Koncern IT visiterer sager efter de retningslinjer, der er aftalt med den enkelte forvaltning.



Kategorisering af sager sker altid efter prioritering:

- Ikke-kritisk
- Kritisk fejl
- Meget kritisk fejl
- Major incident

Major incidents er sager, hvor konsekvensen for Kundens forretning er meget omfattende.

I forbindelse med løsning af større opgaver udpeger forvaltningen og Koncern IT hver en løsningsansvarlig. I de tilfælde er det den løsningsansvarlige, som modtager henvendelser relateret til opgaven. En sag tilhører Serviceindgangens så længe den ikke er visiteret til en person som løsningsansvarlig.

### **Brugeradministration**

Københavns Kommune har en central brugeradministration i Koncern IT bestående af ca. 20 medarbejdere, der håndterer ca. 250 systemer. Brugeradministrationen er organisatorisk placeret i Serviceindgange. Der findes godt ca. 1.400 autorisationsberettigede personer. Der findes både elektroniske og manuelle metoder til håndtering af autorisations anmodninger.

Alle forvaltningsområder bestiller oprettelse og ændringer af it-brugere i en fælles IdM løsning, baseret på medarbejdertyper. Bestilling af sletninger af IT brugere genereres automatisk ifm. fratrædelsesprocessen. Bestillingerne indeholder information om rekvirent, It-bruger, medarbejdertype til autorisation og tillægsautorisationer. Løsningen sikrer et revisionsspør.

Autorisationsanmodninger kan kun bestilles af registrerede autorisationsberettigede, der er tildelt rettigheder i AD til at anmode om oprettelse, ændring, flytning og sletning af autorisationer til It-brugere, samt indmelding af autorisationsprojekter.

Autorisationsanmodninger sker efter enkeltsagsprincippet, med mindre der er tale om et projekt. Et projekt defineres som en anmodning omhandlende flere personer, der skal have samme handlinger foretaget ift. profiler.

### **IT Driftscentret**

Driftsorganisationen består af enhederne Netværk, Serverdrift, Viden, styring og proces (Systemejere, IT-Sikkerhed, overvågning, ITIL) og IT Support og Logistik.



### Systemejere

Systemejere er placeret i IT Driftscentret og arbejder med at:

- Sikre et stabilt, effektivt og sikkert system, der er tilgængeligt for relevante brugere, og som understøttes af effektive processer
- Sikre, at systemets funktionalitet og anvendelse løbende tilpasses og bedst muligt understøtter forretningens og brugernes behov
- Styre leverandørkontakt
- Er blandt andet ansvarlige for drift af store fællessystemer som AD, Exchange, CRM, AirWatch mv.

**IT Driftscentret** har som mål at sikre:

- At funktion og kvalitet er i overensstemmelse med specifikationer og aftaler herunder korrekt dimensionering i forhold til ønsket kapacitet.
- At sikkerhedsbestemmelser overholdes i forhold til opsætning og anvendelse af netværk og servere.
- Professionel fejlhåndtering og vedligeholdelse af netværkskomponenter, accessnet og tværgående datalinjer samt trådløse accesspunkter og servere herunder løbende udskiftning og opgradering af udstyr og datalinjer som anvendes på kommunes interne netværk, i datacentre og forbindelse til internettet.
- Korrekt konfiguration/opdatering af hardware, operativsystemer og applikationer.
- Vedligeholdelse køle-, UPS- og nødstrømsanlæg til datacentre og hovedkrydsfelter

IT Driftscentret har ansvaret for ydelserne:

- Datalinje
- Diskplads
- Rapporter
- Mobilsynkronisering
- Mobile netværksløsninger
- Serverdrift
- Trådløst netværk
- Virtuel fax
- Videokonference





Herudover yder IT infrastruktur rådgivning i forhold til netværksløsninger, systemanskaffelser og telefoniløsninger.

**IT Support og Logistics** (der er placeret i Driftscentret) ansvarsområder omfatter blandt andet lager og klargøring af PC, udskiftning af PC'er, flytninger mv.

IT Support og Logistik understøtter kommunens PC-brugere med alt omkring anskaffelse og support af PC'er, printere og tabletcomputere. Mere konkret er vores opgaver følgende:

- Ringer tilbage til brugerne hvis de har et PC-problem - eller kommer ud til dem på arbejdsstedet.
- Har et lager med PC'er, som vi gør klar til brugerne
- Flytter IT-udstyr
- Omlægger netværkslinjer på arbejdsstederne i kommunen
- Vedligeholder og opdaterer PC'er, som skal bruges til beredskab
- BR-medlemmer og direktørerne på Rådhuset får hjælp indenfor en time ved IT-problemer
- Sørger for at undervisnings-PC'er og publikums-PC'er virker
- Overvåger virus
- Udskifter ca. 6.000 PC'er om året
- Laver printsupport
- Bestiller tablets for brugerne.

IT-Sikkerhed (drift) er ansvarlige for:

- Awareness og kampagner.
- Beredskab.
- IT- sikkerhedshændelser (registrering og opfølgning).
- Lovgivning (Viden om relevant lovgivning).
- Risikostyring.
- Rådgivning af forretningen.
- Sikkerhedsprocedurer og -værktøjer.

Overvågning er ansvarlig for:

- Logning af hændelser – i centrale systemer (2015) og i forvaltningerne fra 2016.
- Proaktiv indgriben ved afvigelser fra normalbillede.
- Rådgivning af forretningen.
- Opbygning af funktion i 2015 og 2016.



### **IT Udviklingscentret**

Enheden **It Udviklingscentret** rådgiver forvaltningerne på alle niveauer fra forretningsløsninger over konkrete udviklingsopgaver til indkøb af særlig hardware eller software.

Enheden bistår med koordination ved større IT-sager samt løsningsmodner nye ydelser og løsninger i samarbejde med forvaltningerne og IT-driftsenhederne. Enheden er forvaltningernes IT-forretningspartner, når der skal udvikles nye leverancer, ydelseskatalog og serviceniveauer. Herudover er enheden ansvarlig for udvikling af kommunens web- og selvbetjeningsløsninger.

I IT Udviklingscentret håndteres blandt andet følgende opgaver:

- IT-ydelseskatalog og serviceniveau
- IT-rådgivning
- Koordinering af leverancer der kommer fra Koncern IT (større sager der ikke følger standard)
- Indkøb af hardware og software
- Fakturering af IT-ydelser
- Udvikling af systemintegrationer og webløsninger
- Udvikling af selvbetjeningsløsninger
- Grunddata
- Udvikling af nye infrastrukturløsninger og opgradering af eksisterende infrastruktur
- 3rd level support.

### **Arkitektur (IT-arkitektur)**

Arkitektur er placeret i IT Udviklingscentret og har ansvaret for:

- IT-governance
- Platformsstrategi og teknologianbefalinger
- IT-anskaffelsesprocessen
- Effektivisering, standardisering, professionalisering og konsolidering af IT
- Sekretariatsfunktion for Arkitekturforum
- IT-Strategier, -politikker og -rammesætning
- Københavns Kommunes IT-strategi
- Interessevaretagelse i forhold til KOMBIT, KL og 6-by samarbejde
- Deltagelse i fælleskommunale IT-samarbejder (KOMBIT, KMD)



- Teknisk projektledelse
- Kravspecifikation
- Rådgivning og standardisering af test
- Udarbejdelse af businesscase
- Forretningsplaner for Koncern IT.

### Staben i IT Udviklingscentret

Staben er placeret i IT Udviklingscentret og referer til centerchefen. Nedenstående opgaver varetages af staben:

- Sekretariatsfunktion for digitaliseringschefkredsen
- Digitaliseringsstrategier.
- Deltagelse i fælleskommunale IT-samarbejder (KOMBIT, KMD, KL).

### Driftsstyring, KPI og Processer (DKP)

DKP varetager:

- Standardisering og udarbejdelse af tværgående ITIL-processer (Problem & Change).
- Analyse og udarbejdelse af KPI'er.
- CMDB.
- Fakturering af IT-ydelser.
- ESDH koordinering.
- Digitalpost koordinering.
- Projekt Management Office (PMO) og projektopfølgning.
- Sekretariatsfunktion for IT-strategi og Investeringsforum.
- Forretningspartnerskab.
- Vedligeholdelse, opfølgning og opdatering af Service Level Agreements.
- KPI og målstyring.
- ITIL har ansvar for udvikling og dokumentation af driftsprocesser og sikring af "best practice" governance på IT-driftsområdet.

## 10 KOMMENDE ÆNDRINGER TIL KS IT-MILJØ

---

Følgende er vedtagne ændringer, der vil slå igennem i løbet af 6-12 måneder, udover ændringer i øvrigt omtalt i dokumentet. Der er tale om foreløbige tidsplaner og specifikationer, så det skal ses som en indikator, men med forbehold for mulige ændringer undervejs.

### Implementering af Sagsoverblik – og Partskontakt (SAPA)

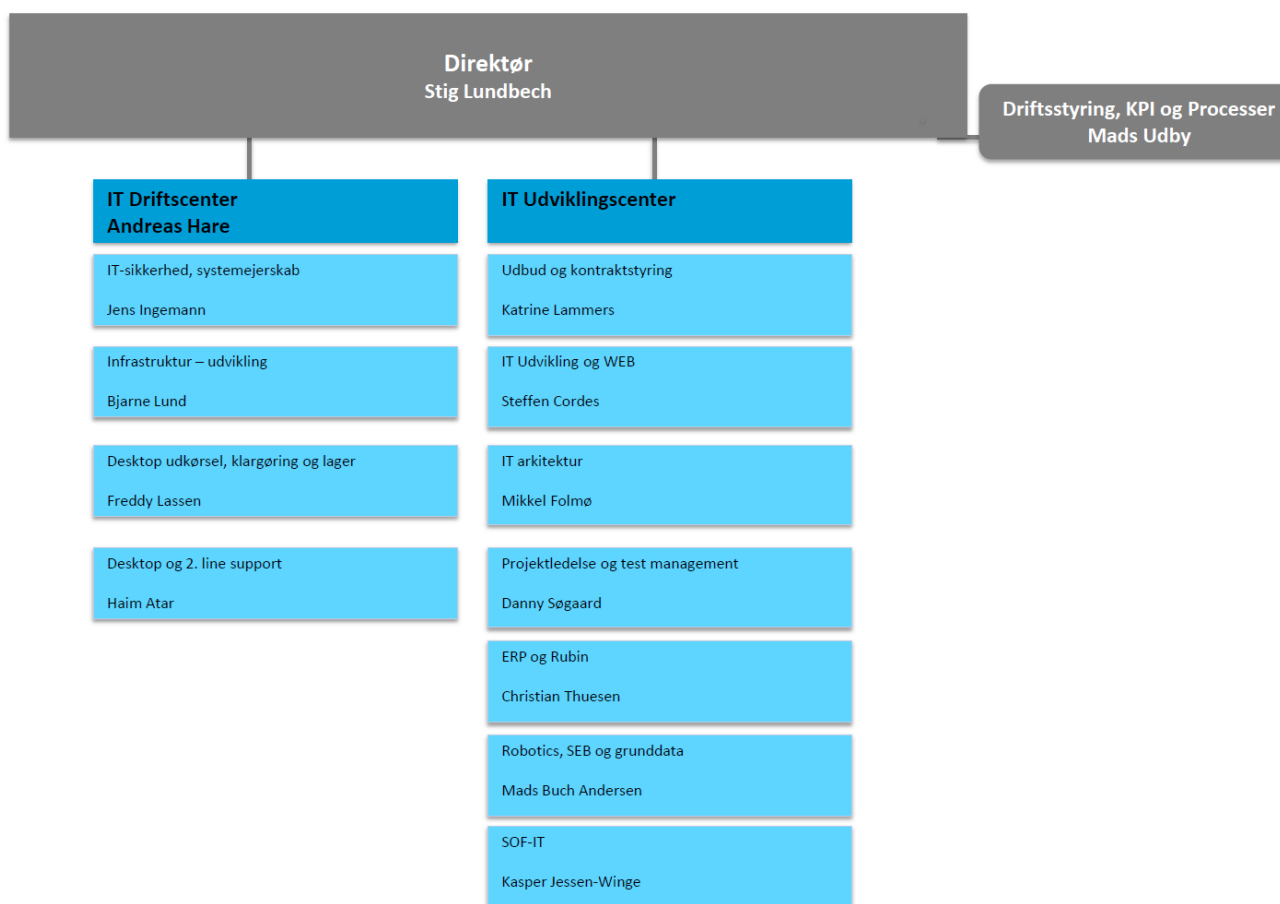
I fjerde kvartal 2016 og frem til slutningen af 2017 forventer KOMBIT at kommunerne implementerer SAPA. SAPA fungerer som en slags "glasplade", der henter data fra en række forskellige fagsystemer for at give



sagsbehandlere og andre interessenter i kommunerne et bedre overblik over de engagementer som borgere, organisationer og virksomheder har ved kommunen. Flere oplysninger om SAPA kan findes på KOMBITs hjemmeside.

## 11 KONCERN IT ORGANISATION

Pr. 01-09-2016.





## 12 KØBENHAVNS KOMMUNE POLITISKE ORGANISATION

---

