




# EKLIENT STANDARD


## MOBILA ENHETER O APPLIKATIONER

### 1.2

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		1 av 23


## Historik

Datum	Version	Av	Förändring
<b>2014-01-27</b>	0.1	Olof Mårtensson	Skapat dokumentstruktur
<b>2014-02-12</b>	0.3	Andreas Lönnmo	Revidering av struktur
<b>2014-05-30</b>	0.5	Andreas Lönnmo	Revidering av innehåll, addering av innehåll
<b>2015-03-01</b>	0.9	Olof Mårtensson	Nytt material, samt borttag av MDM leverantörer
<b>2015-04-13</b>	0.92	Olof Mårtensson	Revidering av titel
<b>2015-09-29</b>	1.0	Olof Mårtensson	Lyft dokumentstatus, viss text revidering
<b>2017-02-13</b>	1.1	Emil Åbrink	Revidering av text, addering av innehåll
<b>2017-09-22</b>	1.2	Peter Abrahamsson	Revidering av text, addering av innehåll

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		2 av 23

## Innehåll

Historik .....	1
Dokumentinformation .....	3
Syfte.....	3
Målgrupper.....	3
Revision .....	3
Styrande principer .....	3
Referenser .....	3
Summering .....	3
Termer och begrepp.....	4
Avgränsningar.....	4
Beskrivning .....	5
Definition av mobila enheter .....	5
EMM – Enterprise Mobility Management .....	5
Livscykelhantering.....	6
MDM – Mobile Device Management.....	12
MAM – Mobile Application Management .....	15
MCM – Mobile Content Management.....	15
Mobil säkerhet .....	16
Certifikatshantering.....	16
Autentisering .....	16
Antivirus .....	17
Rooting /Jailbreak .....	18
Micro VPN .....	18
Appar och applikationer.....	18
Styrande principer .....	18
Klasser och kategorier .....	18
MEAP – Mobile Enterprise Application Platform .....	20
App-säkerhet .....	21
App-förvaltning .....	22
Rekommendationer .....	23

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		3 av 23

## Dokumentinformation

### Syfte

Detta dokument agerar referensdokument och tillhör dokumenttypen standards inom eKlient. En standard definierar ett gemensamt språk mellan aktörer och underlättar det dagliga livet för intressenter.

Dokumentet definierar egenskaper, krav och instruktioner som behövs i dialog mellan landsting/regioner, med driftspartners/driftsorganisation och med applikationsleverantörer. Man är ofta övertygad om att man i en samling pratar om samma sak - men så behöver det inte uppfattas av alla! En standard visar på vad man kan förvänta sig, båda styrkor o svagheter och accepteras av inblandade.

Syftet med en standard för Mobilitet är både att etablera en gemensam guide till begrepp i den mobila världen och att ge underlag till en mobil strategi.

### Målgrupper

Intressenter och medlemsorganisationer i eKlient

Aktörer på marknaden med intresse att följa eKlient

Partners till medlemsorganisationer i eKlient

Applikationsleverantörer och produktägare till medlemsorganisationer i eKlient

### Revision

Detta dokument revideras årligen.

Senaste revidering 2017-08-31.

## Styrande principer

- Användarvänlighet avseende enkelhet för användaren
- Säkerhet anpassade till legala krav och interna policys
- Kostnadseffektivitet

## Referenser


- Andra standards eKlient
  - Klassificering av klienter

## Summering

Mobilitet och mobila enheter ger ofta stora möjligheter till ökad effektivitet i verksamheten.

Vinsterna ligger i förenklade processer, minskat dubbelarbete och tillgänglighet. För att åtnjuta alla fördelar med mobilitet så är det viktigt att definiera en mobil strategi och att investera i verktyg- och processer som ger en god översyn och förenklad administration.

Denna standard (Mobila enheter o applikationer) beskriver övergripande vilka komponenter som är nödvändiga för en framgångsrik förvaltning beroende på ambitionsnivå i den mobila strategin.


<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		4 av 23

## Termer och begrepp

	<i>Begrepp/term</i>	<i>Beskrivning</i>
<b>T1</b>	<i>EMM</i>	<i>Enterprise Mobility Management – Begrepp som omfattar alla delar av mobil hantering</i>
<b>T2</b>	<i>MDM</i>	<i>Mobile Device Management – verktyg för att centralt hantera enheter på distans</i>
<b>T3</b>	<i>MAM</i>	<i>Mobile Application Management – Verktyg för distribution och hantering av appar</i>
<b>T4</b>	<i>MCM</i>	<i>Mobile Content Management – Verktyg för distribution och hantering av filer och lagringsytor</i>
<b>T5</b>	<i>BYOD</i>	<i>Bring Your Own Device – Innebär att medarbetaren använder privat inköpt utrustning i sin yrkesroll</i>
<b>T6</b>	<i>Enterprise Appstore</i>	<i>Ett stöd i vissa MDM – system som förenklar tillgången till företagets egna appar och rekommenderade appar i respektive operativs app-butik</i>
<b>T7</b>	<i>Micro VPN</i>	<i>En teknik för att lägga säkerhetsskydd på en unik app för att skydda vid integration eller synkronisering med verksamhetens infrastruktur</i>
<b>T8</b>	<i>Rooting/ Jailbreak</i>	<i>En metod för att kringgå inbyggda restriktioner i Android eller iOS för att kunna ladda ner appar som inte är auktoriserade och komma åt mobiloperativsystemets filsystem</i>

## Avgränsningar

- Telefonväxel
- Mobil trafik
- Trafikrelaterade kostnader
- Medicintekniska tillämpningar
- Fjärråtkomst till internt nät

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer	5 av 23	

## Beskrivning

### Definition av mobila enheter

Definitionen av en mobil enhet är en handhållen surfplatta, mobiltelefon eller annan design som är gjord för bärbarhet, och är därför både kompakt och lätt. Ny datalagring, bearbetning och skärmt teknik har gjort att dessa små enheter kan erbjuda funktion och tillgänglighet som tidigare har varit förbehållet större persondatorer. För de mobila enheter som idag förekommer på svenska marknaden så är följande operativsystem mest förekommande:

- Apple iOS
- Google Android
- Windows Phone

Det finns utöver dessa även operativsystem i historiskt inköpta enheter som fortfarande är i drift eller enheter med operativsystem som har svagt fäste i Sverige. Exempel på dessa är:

- Symbian (Främst äldre modeller från Nokia och SonyEricsson)
- Windows Mobile/CE (Främst inom lager och distribution)
- Blackberry OS (Främst inom bank, finans och försäkring samt vissa ledningsgrupper)

För att få en grundläggande förvaltning av enheter med mobila operativsystem effektivt krävs ett EMM/MDM-system.

I tillägg till mobila enheter kan den mobila arbetsplatsen även omfatta enheter med professionella operativsystem såsom Windows 7, Windows 8, Windows 10, MacOS etc. Dessa enheter kan normalt hanteras via etablerade förvaltningssystem (Microsoft SCCM, Jamf m.fl.) och omfattas inte i detta dokument. Över tid ser vi att EMM-systemet kommer spela en större roll och även förvalta professionella operativsystem.


### EMM – Enterprise Mobility Management

Enterprise Mobility Management är ett samlingsnamn som omfattar alla de olika komponenter och funktioner som behövs för att driftsätta, spåra, underhålla, säkra och stödja mobila användare, enheter, applikationer, data och användarupplevelser. Övriga definierade termer är undergrupper till begreppet EMM.

Bilden nedan ger en övergripande beskrivning av EMM med tillhörande undergrupper:

<b>Livscykelhantering</b> <ul style="list-style-type: none"> <li>- Hårdvaruplattform</li> <li>- Certifiering</li> <li>- Teknisksäkring</li> <li>- Leverans/konfigurering</li> <li>- Inventering</li> <li>- Support</li> <li>- Service/reparation</li> <li>- Återvinning</li> </ul>	<b>MDM – Mobile Device Management</b> <ul style="list-style-type: none"> <li>- Provisionering</li> <li>- Spårning av enheter</li> <li>- Identifiera enheter</li> <li>- Distribuering av nativa inställningar och appar</li> <li>- Tvingande policies</li> <li>- Lösenordshantering</li> <li>- Fjärrradering</li> <li>- Identitetshantering</li> </ul>	<b>MAM – Mobile Application Management</b> <ul style="list-style-type: none"> <li>- Appdistribution</li> <li>- Versionshantering</li> <li>- Separera privat- och företagsdata</li> <li>- SDK/Wrapping-möjligheter</li> </ul>	<b>MCM – Mobile Content Management</b> <ul style="list-style-type: none"> <li>- Tvingande policies hur innehåll får delas.</li> <li>- Versionshantering av filer</li> <li>- Integrering mot befintliga lagringsytor</li> <li>- SDK-möjligheter</li> </ul>
--	---	--	---

Enterprise Mobility Management

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		6 av 23

## Livscykelhantering

### Grundprincip

I så stor utsträckning som möjligt harmoniera processerna mellan klienter och mobila enheter när det gäller certifieringar, beställningsprocess, support och service, policys och återvinning.

### Hårdvaruplattform

Valet av hårdvaruplattform präglas av ett antal ställningstaganden där respektive ställningstagande kan skapa möjligheter och utmaningar. Mobilitet är starkt konsumentdrivet vilket har skapat svårigheter avseende standardiseringar och policys. Företeelsen BYOD, vilket avser företagsmiljöer i vilka medarbetarna har möjlighet att använda sina privat inköpta enheter, skapar ytterligare en dimension i arbetet med att erbjuda en attraktiv, säker och fungerande mobil arbetsmiljö.

Då valet av hårdvaruplattform även har kraftig påverkan på eventuell intern app-utveckling, supportorganisation, integrationer med infrastrukturen m.m. är det viktigt att en konsekvensanalys utförs innan policyn drivs igenom.


Vissa organisationer kan gynnas av att ha differentierade policys för olika delar av verksamheten. Exempelvis där olika delar av verksamheten har särpräglade arbetsuppgifter såsom fältservice, städning, linjeuppdrag m.m. och andra har mer allmänna uppgifter såsom arbetsledning, administration m.m.

Se riktlinjer nedan:

Plattform	+	-	Passar för
Multi-OS	Brett produkturval Hög användaradaption	Underhållsdrivande Supportdrivande Komplicerar och fördyrar app-utveckling	Verksamheter eller medarbetare som i normalfallet inte använder verksamhetskritiska appar.
Singel-OS	Förenklar app-utveckling Minskad supportbelastning Enklare utrustning	Utmaningar vid bristsituationer Minskad användaradaption Risker vid förändringar av OS (Blackberry, Symbian etc)	Verksamheter eller medarbetare i en linjeorganisation som använder verksamhetskritiska appar för ökad effektivitet i arbetet.

### Val av operativsystem

Val av hårdvaruplattform bör alltid föregås av ett strategiskt val av operativsystem då detta i stor utsträckning påverkar den tekniska förvaltningen, app-plattformen och livscykeln. Det finns idag tre dominerande operativsystem för Smartphones: Android, iOS och Windows Phone. Av dessa är Android den vanligast förekommande före iOS, medan Windows Phone har en marknadsandel på under 0,6% (Se graf nedan). När det gäller Läsplattor är idag iOS det mest förekommande operativsystemet i Sverige och i världen. Android ligger på en andraplats och Microsoft med deras Windows RT är ej representerad längre. Microsoft hoppas att deras Surface-hårdvara (hybridversion av Laptop och Läsplatta) med Windows 10 skall ta marknadsandelar från Apple och Google.

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		7 av 23

Worldwide Smartphone Shipments by OS, Market Share, and 5-year CAGR, 2015-2020 (shipments in millions)							
Platform	2016 Shipment Volume*	2016 Market Share*	2016 Year-over-Year Growth*	2020 Shipment Volume*	2020 Market Share*	2020 Year-over-Year Growth*	2015-2020 CAGR*
Android	1,240.5	83.7%	6.2%	1,565.3	85.1%	5.3%	6.0%
iOS	226.8	15.3%	-2.0%	267.1	14.5%	3.5%	2.9%
Windows Phone	11.2	0.8%	-61.6%	6.8	0.4%	-9.5%	-25.3%
Others	4.0	0.3%	-55.7%	0.5	0.0%	-9.7%	-43.1%
<b>Total</b>	<b>1,482.5</b>	<b>100.0%</b>	<b>3.1%</b>	<b>1,839.7</b>	<b>100.0%</b>	<b>5.0%</b>	<b>5.0%</b>

Source: IDC Worldwide Quarterly Mobile Phone Tracker, June 1, 2016

För att undvika standardiseringar som är kostnadsdrivande rekommenderas följande process:

1. Genomlysning av befintlig plattform dvs. nulägesfördelning mellan de olika operativsystemen i nuvarande hårdvaruplattform i verksamheten.
2. Utifrån de säkerhetskrav som finns i verksamheten, eventuellt existerande MDM-system samt befintliga appar, besluta om vilka operativsystem som ska stödjas idag och vilka operativsystem som ska stödjas under de närmsta 24 månaderna.
3. Utifrån beslut i punkt 2 ovan gå vidare med val av hårdvara som stödjer valt/valda operativsystem.

#### Val av hårdvara


För att välja hårdvara så bör följande kriterier utvärderas:

- Operativsystem utifrån val av vilka som ska stödjas i förvaltningen
- Organisationens avskrivningstid/utpekad livstid för en mobil enhet måste synka med leverantörens åtagande avseende uppdateringar och support
- Möjlighet till inbyggd kryptering av enheten och minneskortet
- Förutsättningar för hantering via MDM- eller annat förvaltningssystem (möjlighet att bl.a. använda API:er för fjärrstyrning)
- Hur länge modellen förväntas finnas tillgänglig på marknaden
- Garantitid
- Pris i förhållande till prestanda

En lämplig indelning kopplat till olika roller i verksamheten är:

- **Bas**  
Medarbetare som på en mobil enhet inte använder funktioner som kräver åtkomst till resurser i infrastrukturen, mobil epost eller liknade system.
- **Plus**  
Medarbetare som använder den mobila enheten för åtkomst till system med okänslig eller inte säkerhetsklassad information som till exempel e-post, vissa dokument m.m.



<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		8 av 23

- **Premium**

Medarbetare som använder den mobila enheten för mobil epost och/eller använder enheten för verksamhetskritiska applikationer som kräver access till säkerhetsklassade resurser i infrastrukturen. Ytterligare krav på informationssäkerhet kan vara nödvändiga för att uppfylla interna policys och legala krav. Till exempel inskränkningar i rätten att använda privata appar, krav på andra autentiseringsformer m.m.

För vissa roller kan ytterligare specifikationer adderas beroende på i vilken miljö enheten ska användas. Kraven bör då inte ställas på enheten utan istället på funktionen då vissa tillgängliga tillbehör kan lösa behoven. Detta gäller bland annat tålighet mot fukt och damm, stötskydd vid fall, möjlighet för att desinfektera etc. Om kraven ställs på själva enheten så minskar valmöjligheterna drastiskt.

### Val av leverantör

Val av leverantör skall givetvis föregås av en formell upphandling enligt LOU. Det finns många aspekter att beakta vid val av leverantör. Om upphandlingen endast avser hårdvaruförsörjning så kan det vara tillräckligt med en förnyad konkurrensutsättning på Kammarkollegiets avtal "Mobiltelefoner" Vad som dock blir alltmer vanligt och nödvändigt är att upphandla Mobilitet, som en helhet och som tjänst, separat då hårdvara, appar och förvaltningssystem blir alltmer integrerade och i och med detta skapar utmaningar i att hantera dessa delar i separata avtal. För övrigt så är det viktigt att beakta följande kriterier i upphandlingar:


- Leverantörens kapacitet – Resurser, logistisk förmåga etc.
- Leverantörens finansiella ställning
- Formell kompetens i form av certifieringar
- Leverantörens relation med tillverkare och mjukvaruutvecklare
- Leverantörens förmåga att strategiskt stödja den mobila utvecklingen idag och i framtiden.

### Certifiering av hårdvara

Certifiering av hårdvara bör omfatta följande steg där utfall i respektive steg avgör om test ska fortsätta i nästa nivå:

1. Generell certifiering
  - a. Allmänt omdöme
  - b. Test av hårdvaruspecifikationer (batteri, antenn, samtalskvalité m.m.)
  - c. Generell utvärdering av hårdvara
2. Teknisk certifiering
  - a. Test av funktion i kända EMM/MDM – system
  - b. Test av kritiska appar (Active sync, Skype m.m.)
3. Verksamhetsspecifik certifiering
  - a. Test mot verksamhetsspecifika EMM/MDM – system
  - b. Test mot verksamhetsspecifika appar
  - c. Test av andra funktioner såsom telefonväxelprefix, certifikat, trådlösa nät etc. i verksamhetsmiljö

Testerna kan utföras i egen regi eller i samverkan med leverantör.

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		9 av 23

### Tekniksäkring

Då mobila enheter i normalfallet har en kort eller mycket kort livstid på marknaden kan det i förekommande fall vara kritiskt med tillgång till produkter. Vid modellbyten är det vanligt med bristsituationer för både utgående och tillkommande modeller. Rekommendationen är därför att i samverkan med leverantören bygga upp ett tekniksäkringslager för att säkra tillgång. Tekniksäkring kan uppfyllas genom att en förutbestämd volym öronmärks för den specifika verksamheten. Antingen genom att leverantören alltid lagerhåller ett specifikt antal enheter motsvarande 2-4 veckors förbrukning eller att vid modellbyte lagerhålla en specifik volym.

### Förkonfigurering

Mobila operativsystem ger relativt små möjligheter till förkonfigurering då konfigurationsmöjligheterna är intimt förknippade med kunskap om användarnamn, lösenord, domän- och serveradress etc. Då konfigurationsmöjligheterna skiljer sig åt beroende på val av operativsystem så rekommenderas följande förkonfigurationer beroende på behov:

- Batteriladdning och funktionstest
- Aktivering (gäller endast iPhone och i de fallen DEP ej används)
- Påklstring av skärmskydd för förlängd livstid
- Stöldskyddsmärkning
- Bipack av verksamhetsspecifik manual (anpassas till förvaltningslösning)

Beroende på val av MDM lösning kan enheten föraktiveras i systemet alternativt utför användaren detta själv via självserviceportal.


Det finns även teknik från Apple och Samsung som (tillsammans med MDM) förenklar "kom-igång"/uppstarten av en mobil enhet. Användaren behöver endast logga in med sina företagsuppgifter vid uppstart av en fabriksny enhet. Enheten aktiveras då automatiskt mot MDM som då skickar ut de konfigurationer, policys och appar som gäller för medarbetarens roll.

### Inventering

Ett MDM-system erbjuder ofta en djupare inventering av de enheter som är anslutna och har en installerad klient. Detta bör kompletteras med ett fysiskt register som antingen upprätthålls av leverantören eller som hanteras i egen regi. Detta för att identifiera de olika inventarier som finns och för att separera privata- och företagsinköpta enheter. Övriga mervärden är bl.a. garantikontroll, fördelning mellan de olika modellerna och operativsystemen samt underlag för budget. Databasen bör innehålla följande uppgifter:

- Inköpsdatum
- Tillverkare
- Modell
- Garantitid
- Kostnad

Under vissa omständigheter kan det vara aktuellt att koppla utrustningen till specifika användare. Det skall dock pångteras att detta kan vara mycket kostnadsdrivande och därför är rekommendationen att använda uppgifter från MDM systemet för att göra denna koppling.

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		10 av 23

## Support

Support har blivit en allt viktigare aspekt när det gäller den mobila användaren. En professionell användarsupport kan innebära stora tidsbesparingar för medarbetarna. Undersökningar visar att synkproblematik kan omfattas så mycket som 80% av det totala antalet anmälda incidenter. Verksamheten bör noga utvärdera om det är möjligt att erbjuda supporten i egen regi eller om detta ska vara en del av ett eventuellt förfrågningsunderlag.

Supporten bör delas upp på följande nivåer:


- First line (generell IT-support)
  - o Felanmälan
  - o Felsökning
  - o Handhavandefrågor
  - o EMM/MDM-relaterade frågor
  - o Stöld- och förlustanmälan
  - o Beställning av tjänster såsom retur och återvinning m.m.
- Second line (Djupare mobil kompetens)
  - o Hantering av eskalerade ärenden från first line
  - o Handläggning av serviceärenden
  - o Abonnemangsrelaterade ärenden
- Third line
  - o Eskalerade ärenden av djupare teknisk karaktär
  - o Incidenter där felet kan kopplas till andra resurser i infrastrukturen

Beroende på verksamhetens uppgift och medarbetarnas arbetstid så bör det finnas möjlighet till anpassad tillgänglighet för att på så sätt undvika onödigt kostnadsdrivande krav. Det är därför lämpligt att tillgänglighet kan levereras i följande intervall:

- Vardagar 8-17
- Vardagar 7-22
- måndag till fredag 00-24

Åtgärdstid är också en viktig komponent då det inte sällan är kritiskt för medarbetaren att få en incident åtgärdad. Det är därför nödvändigt att ha spårbarhet på åtgärdstid och ärendekategori för att på så sätt kunna arbeta proaktivt. Antal supportärenden påverkas i hög omfattning av hur stabil förvaltningsmiljön är samt hur det proaktiva förbättringsarbetet utförs. Incidentrapporten bör levereras och utvärderas månadsvis och ska då mins omfatta följande uppgifter:

- Antal ärenden per kategori
- Antal ärenden lösta i first line
- Tillgänglighet (antal ärenden inom och utanför SLA)
- Detaljerad ärendeförteckning med:
  - o Tid för mottagande av ärendet
  - o Tid för ärende slutfört
  - o Incidentbeskrivning
  - o Lösning


<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		11 av 23

### Service och reparation

Incidenthantering när det gäller hårdvara bör även den vara anpassad till hur kritiskt utrustningen är för användaren i det dagliga arbetet. Det bör därför prioriteras ha en anpassad SLA för olika delar av verksamheten beroende på användningsuppgift. Följande tre SLA: er rekommenderas beroende på utförandeförmåga och organisationens behov.

1. Inskicksservice  
Innebär att användaren efter felanmälan erhåller ett emballage i vilket enheten skickas till verkstad. Enheten repareras och returneras till användaren. Rimligt krav att ställa på denna tjänst är 10 arbetsdagar inklusive postgång. Denna nivå förutsätter lokal tillgång till reservenheter
2. Inskicksservice med lånetelefon  
Innebär att användaren erhåller en centralt administrerad lånetelefon under tiden för reparation. Tjänsten är normalt mycket kostnadsdrivande då processen innehåller många steg och att den driver fraktkostnader i de fall tjänsten inte kan tillhandahållas lokalt.
3. Utbytes- eller stafettsservice  
Innebär att användaren efter felanmälan erhåller ersättningsenhet av samma typ och modell samt ett emballage i vilket enheten skickas till verkstad. Enheten repareras och returneras till en centralt administrerad pool. Rimligt krav att ställa på denna tjänst är att ersättningsenheten skickas ut samma dag som felanmälan och användaren har därmed en fungerande utrustning 1-2 dagar efter felanmälan. Detta är en mycket kostnadseffektiv modell med hög användarnytta. Tjänsten kan med fördel kombineras med de krav som ställs på ny leverans av enhet inklusive förkonfigurering och registrering på ev. MDM-system.

Samtliga SLA: er ovan kan etableras som antingen en lokalt- eller en centralt hanterad tjänst. Fördelen med en lokalt hanterad tjänst är att medarbetaren har en mycket hög tillgänglighet och snabbt kan få incidenten åtgärdad. Utmaningen är dock tidsåtgång, skalbarhet i poolen av enheter som används för utbyte och kan endast rekommenderas för arbetsplatser med >200 medarbetare. Om inte verksamhetskraven är extremt höga rekommenderas central förvaltning antingen med egen drift eller hantering via leverantören.

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		12 av 23

## Retur och återvinning

### MDM – Mobile Device Management


MDM är beteckningen på en mjukvara som tillsammans med en klient i den mobila enheten ger möjligheter till att styra och kontrollera enheten på distans. Med ett MDM-system så kan man typiskt hantera:

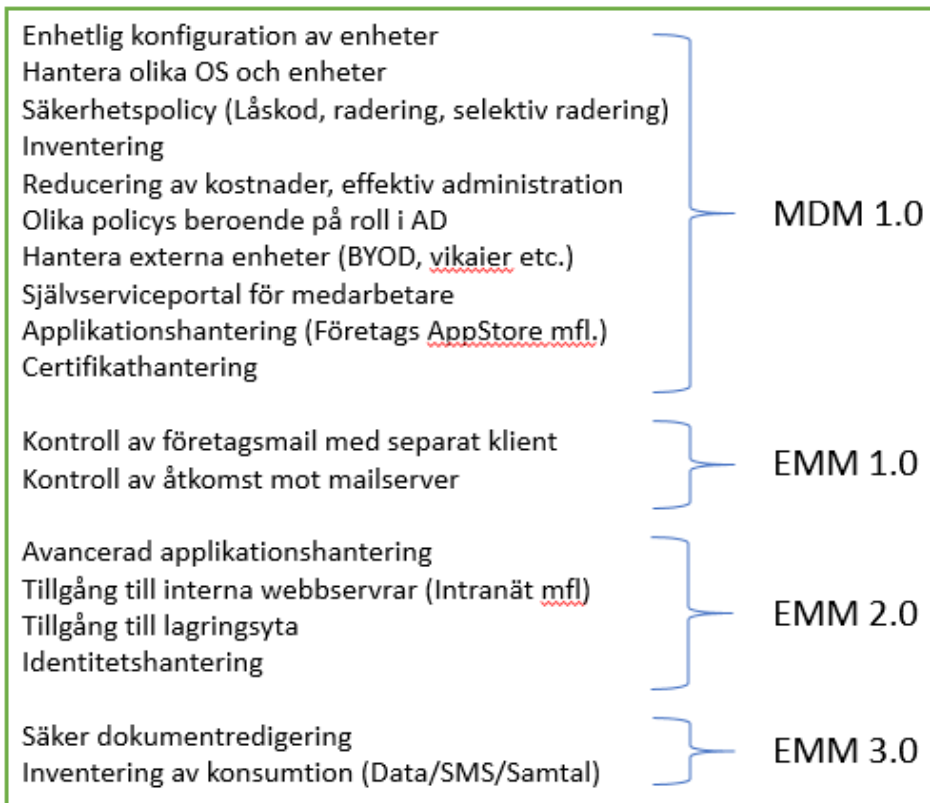
- Låskodspolicys
- VPN-inställningar
- Inställningar för Wifi
- Policys för tex. mailsynk
- På- och avstängning av vissa funktioner
- Utrullning av konfigurationsprofiler
- Utrullning av certifikat
- Enterprise Appstore (En egen "butik" på enheten där användaren kan ladda ner internt rekommenderade egenutvecklade- och generiska appar)
- Möjlighet att "trycka ut appar" till användarens enhet
- Grå och svartlistning av godkända och icke godkända appar
- Stöd för åtkomst till filserver och sharepoint
- Stöd och åtkomst till respektive leverantörers andra portföljprodukter som samverkansprogram, konferensmöjligheter etc.
- Epostfiltrering
- Etc.

De mest utvecklade systemen på marknaden har numera också stöd för mer avancerade funktioner såsom:

- Android For Work (Möjlighet att separera privat data med företagsdata direkt i operativsystemet och dra nytta av licensiering osv)
- Övervaka mängden trafik som konsumeras (Data/samtal/SMS)
- Apple Device Enrollment Program (Underlätta aktiveringen mot MDM)
- Apple Volume Purchase Program (Underlätta hanteringen av applikationslicenser)
- Samsung Knox Mobile Enrollment (Underlätta aktiveringen mot MDM)
- Djupgående rapporter
- Etc.


Vilken lösning som bör väljas beror i huvudsak vilken ambitionsnivå verksamheten har för den mobila arbetsplatsen i kombination med i vilket nuläge man befinner sig. Rimlig tidshorisont för investeringen är 36-48 månader beroende på val av lösning.

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		13 av 23



Nedanstående bild visar exempel på de olika licensmöjligheterna som finns beroende på mognadsgrad i bilden ovan där "Green" är kopplat till behov i MDM 1.0, "Orange" till EMM 1.0, "Blue" till EMM 2.0 och "Yellow" till EMM 3.0

	GREEN Suite	ORANGE Suite	BLUE Suite	YELLOW Suite
Mobile Device Management	✓	✓	✓	✓
Container	✓	✓	✓	✓
Catalog	✓	✓	✓	✓
Boxer		✓	✓	✓
App Wrapping			✓	✓
Browser			✓	✓
Content Locker Standard			✓	✓
VMware Identity Manager			✓	✓
Telecom				✓
Content Locker Advanced				✓

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer	14 av 23	

#### Val av EMM/MDM-system

Då det finns ett utbud av över 100 olika mjukvaror med MDM funktionalitet så kan det vara svårt att välja det verktyg som passar bäst för en specifik verksamhet. Gartner gör varje år en gallring och efter denna så lyfter de fram de 14 stycken mjukvaror som bäst motsvarar de krav som ställs inom EMM. EMM-systemen placeras sedan in i en kvadrant med viktning som styrs av bedömd möjlighet att exekvera på x-axeln och vision på y-axeln (känd som *Gartner Magic Quadrant*). Det topprankade verktygen (*LEADERS*) 2016 är:

- Airwatch by VMware
- Citrix Xenmobile
- Blackberry
- Mobile Iron
- IBM Maas360

Gartner placerar Microsoft i 2016 år Magic Quadrant for Enterprise Mobility Suites under *VISIONARIES* och säger (fritt översatt) att *"Gartner ser att Intune ofta används i det läget som Microsoft kallar "MAM-Only mode" tillsammans med en mer utvecklad EMM-tillverkare vilket gör att kunderna måste köpa licenser för flera produkter. Intune används i större utsträckning av kunder som redan har ett Microsoft Enterprise Agreement(EAs) då man använder andra produkter inom EMS. Intune rekommenderas för organisationer av alla storlekar där man har ett enklare behov och där man använder sig av Office 365 eller Azure AD"* [Från Gartner Magic Quadrant for Enterprise Mobility Suites 2016]

För att sortera mellan ovanstående och andra verktyg så kan nedanstående indelning vara lämpligt att tillämpa vid utvärdering av verktyg:

- Funktionella krav
- Etablering i Sverige/ Norden (egen regi eller via partners)
- Finansiell stabilitet (utvecklingskraft)
- Tillgänglighet i supportfrågor
- Tillgänglig dokumentation
- Pris och prissättningsmodeller


#### EMM/MDM-förvaltning

Moderna EMM-system kan ofta med fördel köpas som tjänst då det sällan lagras data lokalt. Undantaget är vid användande av inbyggda "Dropbox" – liknande applikationer där dokument lagras i leverantörens miljö.

Rekommendationen är därför att Säkerhet är en del av utvärderingsgruppen så att legala krav samt interna policys uppfylls av slutlig lösning.

Genom att köpa MDM som tjänst så säkerställer verksamheten att den alltid har tillgång till senaste versionen av programvara.

Vissa system och/eller verksamhetskrav tillåter inte att serverna står utanför kundens miljö. I dessa fall är det viktigt att redan i budgetarbetet ta höjd för backup och redundans. Verksamheten bör också investera i en fristående testmiljö för säkert testa systemuppdateringar, policyuppdateringar etc. innan utrullning i skarpt system.

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		15 av 23

### MAM – Mobile Application Management

Mobile Application Management avser mjukvara som hanterar tillgång, styrning och installation, av egenutvecklade och kommersiellt tillgängliga mobil-appar som används i affärssammanhang på både företagsägda- och BYOD enheter.

MAM skiljer sig från MDM-system då denna MAM fokuserar på applikationsförvaltning, det ger en lägre grad av kontroll över enheten, men en högre grad av kontroll över applikationer. MDM -system är utvecklade för att hantera hela enheten.

Vid egenutveckling av appar eller vid frekvent användning av flertalet appar i verksamheten så är MAM en nödvändighet för effektiv administration. Då MAM – funktionalitet i många fall är inbyggd i MDM – system så är rekommendationen att MAM är en del av kravställningen på MDM – systemet.

MAM – system kan bland annat innehålla dessa funktioner:

- Enterprise App Store
- App uppdatering
- App monitorering (hur appen beter sig)
- Autentiseringskontroller
- Krasch- och loggrapportering
- AD-gruppskontroller
- Versionshantering
- Konfigurationshantering
- Push-tjänster
- Användningsanalyser
- Licensieringsmetoder
- Rapporter

### MCM – Mobile Content Management

Mobile Content Management är en teknologi som adresserar distribution av innehåll till en mobil enhet. Det finns många lösningar som specialiserar sig på enbart denna hantering men i ett EMM-system erbjuds även denna funktionalitet.

MCM ska klara av följande funktioner som minimum för det skall anses vara ett MCM:

#### Integrering

Det skall finnas möjlighet att integrera MCM med redan etablerade lagringsytor som man sedan tidigare använder som kund. Exempel på lagringsytor kan vara Sharepoint, CIFS, OneDrive, Google Drive etc. Det skall även gå att integrera mot system som tillhandahåller data loss protection (DLP).


#### Policyhantering

I MCM ska man kunna sätta policies på individuella filer för specifika ändamål. Exempel kan vara att sätta regler och inställningar hur filer från specifika lagringsytor skall hanteras. Andra exempel kan vara att åtkomsten och hanteringen skall regleras beroende på vad det är för typ av individ eller enhet som önskar åtkomst till organisationens resurser.

#### Distribution

I normala förhållanden är det alltid användaren som manuellt hämtar den informationen som är relevant för den specifika individen. Med MCM skall det finnas funktionalitet som gör detta automatiskt och pushar ut nödvändig information.



<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer	16 av 23	

Mer avancerade MCM-system har även funktionalitet som:

- Separera företagsdata med privat data
- Förkonfigurerade appar som är anpassade för att fungerar med EMM-lösningen.
- Möjlighet att göra anpassningar och integrera med egenutvecklade applikationer mot MCM.

## Mobil säkerhet

### Certifikatshantering

Digitala certifikat ger goda möjligheter att skapa en plattformsoberoende säkerhetslösning för flera olika delar av den mobila arbetsplatsen. Exempel på områden där certifikat kraftigt ökar säkerheten är:

- **Kryptering**  
Certifikat kan användas för att kryptera digital information oberoende av plattform. Till exempel utnyttjar S \ MIME-standarden certifikat för epostkryptering, medan HTTPS-protokollet (SSL) används för att kryptera webbsidor.
- **Signering**  
Verksamheter i behov av digitala signaturer kan utnyttja certifikat för att bevisa meddelandets integritet och visa att meddelandet kommer från en autentiserad avsändare och inte kommit i kontakt med en illasinnad tredje part. S/MIME kan också signera e-postmeddelande för att visa mottagaren att avsändaren är den de säger sig vara.
- **Autentisering**  
Eftersom digitala certifikat kan innehålla användarens- eller enhetens identitet och är certifierat av en betrodd källa så kan certifikatet ge säker autentisering i ett antal system såsom e-post, WiFi, och VPN.

Certifikatshantering kan ske via vissa MDM-system och vid införande av certifikat så bör detta vara ett skalkrav vid utvärdering av MDM-system.

### Autentisering


Båda legala krav och interna policys skapar ibland utmaningar i användandet av mobila enheter. Den största utmaningen är kanske användandet av s.k. Smarta kort. Utmaningen ligger i att den fysiska hårdvaran, den mobila enheten, i de flesta fall saknar läsare för denna.

Om kravet är två-faktorautentisering så finns det flera alternativa lösningar:

- Certifikatshantering i kombination med fingeravtryck eller lösenord
- Olika varianter av fysiska dockningsstationer med smartkortsläsare i vilken den mobila enheten placeras
- Inbyggd lösning i vissa MDM-system
- Separat dosa, dongel eller skal med smartkortsläsare

### SITHS-kort och mobila lösningar

SITHS är en tjänstelegitimation för både fysisk och elektronisk identifiering. Ett ordinarie SITHS-kort innehåller ett personligt Telia e-leg som visar vem du är, och ett SITHS-certifikat som visar identiteten

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		17 av 23

i din yrkesroll. För att kunna inneha ett SITHS-kort måste personen finnas med i en nationell databas som kallas HSA. SITHS-kortet uppfyller kraven på stark autentisering.

SITHS kort används bland annat till:

- Inloggning till datorer, olika system, e-tjänster framförallt inom vården, men också hos myndigheter
- Elektronisk signering av avtal, fakturor, journalhandlingar, recept, med mera

Då ett SITHS-kort är ett smart kort i grund och botten, så uppstår samma utmaning med ett SITHS-kort som med ett smart kort. För att kunna nyttja SITHS-kortet med mobila lösningar så krävs en dongel, dockningsstation eller ett skal och dessutom anpassning av Appar för att kunna få en likvärdig funktionalitet som vid inloggning med ett SITHS-kort på en klient.

Om möjligt bör separata donglar, skal och dockningsstationer undvikas då dessa riskerar att få kort livstid i samband med designförändringar av hårdvara och innebär en ökad kostnad. Det underlättar även för användaren att endast behöva ha kontroll på sin mobila klient och inte tillbehör som t ex kan gå sönder eller förloras. Dessutom så krävs normalt att den enskilda appen kodas för att kunna hanteras via autentiseringen.

Rekommendationen är att se över möjligheten för alternativ till autentisering/signering med SITHS-kort för mobila enheter. En alternativ autentisering/signering till ett SITHS-kort skulle kunna vara ett engångslösenord i kombination med en personlig PIN-kod för mobila enheter. Det finns flera aktörer som erbjuder likande lösningar för autentisering.

Ett annat alternativ kan vara en kombination av certifikat och en annan autentiseringsmetod som lösenord eller fingeravtrycksläsare.

Verksamheten bör sträva efter att ha Single Sign On i de fall flera olika applikationer används av samma medarbetare i linje med principerna för denna standard.


Den tekniska utvecklingen inom området går för tillfället mycket snabbt och olika tillverkare och OS leverantörer tillför hela tiden nya tekniska lösningar, men bransch-standarderna för stark autentisering med personligt certifikat på mobila enheter är fortfarande i vardande. Det är därför viktigt att löpande noggrant utvärdera tillgängliga lösningar. Undvik i möjligast mån att låsa in den tekniska lösningen mot en modell eller ett operativsystem och se noga över befintligt innehav så att strategiska val inte leder till oväntade kostnader i byte av mobilflotta.

### Antivirus

Antivirus-programvara har historiskt inte varit särskilt effektiv när det kommer till mobila enheter. En av anledningarna till detta är att operativsystemet i regel är uppbyggt så att respektive app ansvarar för sin egen säkerhet. Ett antivirusprogram skulle därmed i praktiken behöva vara en del av koden på respektive app.

De lösningar som finns på marknaden idag erbjuder funktionalitet som:

- Kontroll av kända skadliga appar
- Skydd mot nätfiskeförsök
- Brandvägg
- Jailbreak/rooting

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		18 av 23

Nackdelen med lösningarna som finns är att de ej är kompatibla med samtliga operativsystem.

Rekommendationen idag är därför att avvakta med investeringar i antivirus och istället använda säkerhetslösning i EMM/MDM-system för att ta bort säkerhetsrisker med infekterade appar i kombination med policys för Jailbreak och Rooting samt inaktivera möjligheten att installera appar från tredjepartsbutiker.

### Rooting /Jailbreak

Rooting (Android) eller Jailbreak (iOS) är namn på aktiviteter som avser att ta bort de begränsningar som finns på respektive operativsystem i syfte att primärt öppna upp för möjligheter att installera oauktoriserade appar och få tillgång till enhetens restriktiva filsystem. Detta kan leda till stor riskexponering för dataläckage och intrång i enheten och bör under inga omständigheter tillåtas i verksamheten.

För att identifiera rootade eller jailbreakade enheter används normalt ett MDM – system som i kombination med policys minimerar och oftast eliminerar risken. Exempel på automatiska policys som är lämpliga kan vara att enheten antingen fjärraderas alternativt inte längre har tillåtelse att synkronisera data med resurser i infrastrukturen.

### Micro VPN

Micro-VPN är en VPN-anslutning som öppnas på begäran och som ger säker åtkomst till företagets nätverk, webbplatser eller resurser. Vanligtvis öppnas anslutningen när medarbetaren öppnar en mobil app som t.ex. egenutvecklade app eller vissa tredjeparts-appar och som kräver access till företagets nätverk.

Syftet med MicroVPN är att inte behöva säkra hela den mobila enheten utan istället säkra den specifika applikationen. Detta är ett lämpligt tillvägagångssätt för BYOD enheter eller andra enheter som inte kontrolleras av verksamheten som t.ex. patienter och anhörigas egna mobila enheter där appar används för att komma åt informationen i verksamhetens infrastruktur.

För att etablera MicroVPN krävs en gateway och beroende på antalet appar och användare oftast en lastbalanserare som tex. Citrix Netscaler.

### Appar och applikationer


Appar och applikationer eller mobila lösningar kan rätt implementerade skapa stora förutsättningar för ökad produktivitet i och med effektivisering av arbetsuppgifter. Tillväxten är enorm och i stort sett varje företag och organisation använder appar i det dagliga arbetet oavsett om de är auktoriserade eller inte av intern IT.

### Styrande principer

- ROI – värde för verksamheten
- Agilitet dvs löpande anpassning till tillgänglig teknik och användningsområde
- Utvecklingskostnad
- Förvaltningskostnad
- Val av utvecklingsteknik beroende på behovet

### Klasser och kategorier


Appar kan delas in tre klasser beroende på målgrupp (inom parantes översatt till Landstingens situation):

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		19 av 23

- **B2C "Business to consumer"** (Landsting till medborgare)  
Främst avsedda att förenkla tillgången till information i olika situationer såsom anhöriginformation, sjukvårdsupplysning, olika enheters funktion och öppettider etc inom sjukvård, tidtabeller och trafikinformation inom kollektivtrafik m.m.
- **B2B "Business to business"** (Landsting till underleverantörer eller privata entreprenörer)  
Fältrapportering, information, arbetsordrar m.m.
- **B2E "Business to employee"** (Landsting – medarbetare)  
Inventering, tidrapportering, beställningar, support, journalsystem, m.m.

När det gäller att utveckla mobila lösningar går det generellt att dela in dessa utifrån fyra olika principer eller tekniker.

- **Nativ**  
När en app utvecklas så att koden ligger lokalt på enheten brukar appen benämnas som nativ.  
De tydligaste fördelarna med en nativ app är dels att det generellt är enklare att följa operativsystemets guidelines utifrån en användarupplevelse.  
Varje plattform såsom iOS, Android eller Windows 8/Windows phone har en tydlig profil i hur användaren navigerar och arbetar med gränssnittet. Om gällande guidelines följs brukar en nativ app brukar generellt upplevas mer som "iOS", "Android" eller "windows".  
Vidare så är det enklare att nå ett bra och effektivt offlinestöd med en nativ app. Med offline stöd menas att appen klarar att fungera utan internetuppkoppling.  
Den tydligaste nackdelen med nativ appar är att om den ska finnas på flera plattformar så krävs antingen parallell utveckling eller att en Enterprise Mobile Application Plattform används i utvecklingsarbetet.
- **Responsiv webb**  
En responsiv webb är egentligen inte en app utan snarare en webbsida som anpassar sig utseendemässigt till den storlek på skärm som den mobila enheten har.  
Genom att det går att skapa ikoner i enhetens operativsystem som direkt kopplar sig till en webbsida kan en websida upplevas som en app av användaren.  
Den absolut största fördelen med en responsiv webb är att utvecklingskostnaden i de flesta fall blir betydligt lägre än att utveckla en nativ app samtidigt som den mer eller mindre direkt blir tillgänglig på alla plattformar samt att den är billig att distribuera och underhålla då inga nya versioner behöver laddas ner till enheten.  
Ytterligare fördelar är att även integrationer mot bakomliggande system ofta blir billigare och enklare att bygga och underhålla.  
Genom att en webbsida behöver kompromissa utifrån själva användargränssnittet för att passa till alla plattformar så upplevs ofta en responsiv webb som mindre användarvänlig eller att känslan i appen inte är densamma som en nativ app.  
Det går att bygga offline stöd för webbsidor men dessa lösningar når i regel inte samma funktionalitet och enkelhet i underhåll som en nativ app.
- **Webb**  
Appen är helt webbaserad och ingen information lagras i enheten. Särskilt lämplig för B2B

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer	20 av 23	

och B2C då det enda kravet hos mottagaren är att enheten har en webbläsare. Åtkomst är dock beroende av uppkoppling mot mobilnätet eller wifi och appen kan därför upplevas som seg. Webbappar kan också ha vissa begränsningar när det gäller åtkomst till inbyggda funktioner i telefonen som t.ex. kamera och GPS samt samverkan med andra appar i den mobila enheten som t.ex. mailklient eller ordredigering.

#### - **Hybrid**

Den absolut vanligast förekommande app-formen idag. En hybrid app har vissa delar som är installerade på den mobila enheten som t.ex. kopplingar mot mail-appen, GPS eller kameran medan andra delar hämtas via en webbsida över via mobilnätet eller wifi. För användaren brukar dessa delar smälta samman så att han eller hon inte märker då respektive teknik används. En stor fördel med dessa appar är att de kan ha viss funktionalitet även när den mobila enheten helt saknar uppkoppling. Ett vanligt område för hybrid-appar är fältrapportering. Rapporterna "cashas" löpande och skickas när nästa uppkoppling sker.

#### MEAP – Mobile Enterprise Application Platform

Idag är det fortfarande vanligt att app-projekt är egna "silos" och det är inte helt ovanligt att projekten drivs direkt från verksamheten gentemot leverantören av den mobila lösningen. Detta kommer över tid att leda till stora utmaningar i förvaltningen vart eftersom fler appar kommer in i verksamheten. Under avsnittet "Mobile Application Management" så beskrivs bland annat möjligheten till en "Enterprise Appstore" som förenklar tillgängligheten till appar för användarna vilket är en del av lösningen. Men det är lika viktigt att även app-utvecklingen sker enligt en väl definerad struktur för att på så sätt minska kostnad för utveckling och integration av nya appar.

Mobile Enterprise Application Platform (MEAP) är ett ramverk för utveckling och spridning av appar och som tillhandahåller verktyg för klient, server och middleware för mobila lösningar. Den hanterar alla mobila applikationer på alla enheter, från en smartphone till en tablet; multikanal och offline kapacitet. Bäst lämpad för företag och organisationer som vill distribuera flera appar på en och samma infrastruktur, skalas till storleken på organisationernas nuvarande mobila erbjudande och finns i anpassningar för både online-och offline-läge.


Gartner rekommenderar införande av MEAP enligt sin "gyllende regel om tre":

- Tre appar eller fler
- Tre mobila operativsystem eller fler
- En investeringsplan på tre år eller mer

Om en eller flera av ovanstående påståenden stämmer in på er organisation så rekommenderas införande av MEAP.

MEAP-system

Nedan bild visar Gartners "Magic quadrant" för applikationsutveckling från augusti 2016:

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		21 av 23



Bilden visar att den oberoende lösningen som är ledare idag är IBM och då främst med sin mjukvara "Worklight" som erbjuder ett mycket kraftfullt verktyg för utveckling och förvaltning av applikationer. Adobe erbjuder verktyg för agil utveckling av enklare mobila applikationer.


### App-säkerhet

En app i en mobil enhet kan hantera data som för en verksamhet är säkerhetskänslig eller utgöra en risk i det fall den manipuleras eller sprids.

Utifrån att en mobil enhet just är mobil och används ute i "fält" där risken för stöld eller otillbörligt användande är större än i en låst kontorslokal är det viktigt att förhålla sig till hur säkerheten uppnås för den utvecklade appen och datakommunikationen mellan eventuella backend.

För att undvika att obehöriga får eller tar sig tillträde till känslig data behöver några viktiga aspekter beaktas.

En app som inte har några säkerhetskrav har kanske ingen autentisering av användaren, det vill säga den är öppen och kräver ingen inloggning. Normalt brukar en autentisering ske mot företagets katalogtjänst (active directory) där användaren loggar in i appen med samma inloggningsuppgifter som i det lokala nätverket.

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		22 av 23

För verksamheter med extra känslig information brukar kravet finnas på tvåfaktorsautentisering. Detta innebär att användaren validerar sin identitet i två steg, en sak användaren har med sig samt en sak användaren vet. Ett exempel på tvåfaktorsautentisering är nyttjande av SITHS-kort för autentisering. Användaren har ett unikt kort på sig som läses i en speciell kortläsare samtidigt som användaren anger ett lösenord.

Förutom att skapa rätt nivå av autentisering för en app är det även viktigt att de data som används och eventuellt lagras på enheten behandlas på ett korrekt sätt.

Ofta när behov finns av offline stöd finns även ett behov av att lagra data lokalt i den mobila enheten. Om data inte är krypterat på ett säkert sätt kan det enkelt läsas ut ur enheten.

Vidare behöver även den ström av data som flödar från och till den mobila enheten beaktas utifrån ett säkerhetsperspektiv. Om inte informationen som skickas krypteras är det relativt enkelt att läsa av dataströmmen och antingen återskapa känslig information eller "fånga" användaridentitet och lösenord.

### App-förvaltning

En bra mobil lösning skapar verksamhetsnytta och med det uppstår ett beroende från verksamheten att lösningen ska vara tillgänglig, supportas och utvecklas med verksamheten.

En bra förvaltning av appen/apparna säkerställer att rätt organisation svarar upp mot de olika behov som uppstår i en verksamhetskritisk lösning.

Exempelvis så bör en app med krav på hög tillgänglighet ha planerade releasefönster som säkerställer att appen testas mot nya versioner av operativsystem innan den rullar ut på klienterna. Vidare så behöver supportflödet tydliggöras så att ett problem eller förändringsbehov tydligt styrs till en mottagande funktion.

Följande områden bör beaktas inför en förvaltningssituation


- Support och servicedeskflöde
- Underhållsaktiviteter
- Felavhjälpning
- Funktionell kravfångst och releaseplanering

Vår rekommendation är att förvaltningsorganisationen tydliggörs mellan mottagande organisation och leverantörsorganisationen.

- Vilken förvaltningsorganisation ska motta systemet?
- Hur ser förvaltningsorganisationen ut?
- Vilka roller har leverantören i förvaltningsleveransen?
- Utbildningsbehov av SD+1st line?

Exempel på roller i en förvaltningsorganisation är

- Systemägare
- Förvaltningsledare
- Servicedesk

<b>eKlient i samverkan</b>	<b>Datum:</b> 2017-09-22	<b>Version:</b> 1.2	
<b>Dokumentstatus:</b> Godkänd	eKlient standard Mobila enheter och applikationer		23 av 23

- 1,2 och 3rd line support

#### Rekommendationer

1. Sträva i första hand efter att investera i redan färdiga applikationer eller applikationer som endast kräver förädling.
2. Vid utveckling av egna appar utvärdera i tur och ordning möjligheten till 1. Wapp-app, 2. Hybrid App, 3. Nativ-app.
3. Om ni har för avsikt att investera i appar och att ni bedömer att ni kommer uppfylla minst ett av kraven i Gartners "den gyllene regeln om tre" - Investera i ett MEAP – verktyg eller ställ krav på underleverantören att utveckling och förvaltning sker i ett anvisat MEAP-verktyg.
4. Säkerställ att ROI-kalkylen även omfattar den löpande förvaltningen av appen (distribution, uppdateringar, analys, support, incidenthantering m.m.)
5. Börja med något enkelt med en tydlig ROI som påverkar många medarbetare eller medborgare. Exempel på enkla lösningar kan vara tidrapportering, konferensrumsbokning, enklare inventeringsverktyg etc.
6. Ta ställning till om ni vill bygga egen kompetens om utveckling och förvaltning kring mobila appar eller om ni ska köpa det som tjänst och istället agerar som beställare