Mobila informationssystem

Säkerheten i mobila informationssystem

ES2022-12

Oktober 2022

Innehåll

1. Inledning

Promemorians syfte är att beskriva utmaningar med mobila informationssystem och redogöra för några av de lösningar som myndigheter har gjort. Promemorian gör inte anspråk på att vara heltäckande. Lösningar och rekommendationer kan behöva förändras över tid när omvärldens förutsättningar förändras.

Vidare har varje myndighet ansvaret, att göra egna bedömningar av hur man ska hantera utmaningarna på det här området. Lämpligen bör verksamheten, it- och rättsavdelning vara delaktiga i det här arbetet.

Promemorians huvudsakliga målgrupper är arkitekter, strateger, utvecklare, tekniker och personer inom säkerhetsområdet. Den kan också ge beslutsfattare en övergripande inblick i komplexiteten.

De exempel som presenteras i kapitel 7 Bilagan, beskriver hur några svenska myndigheter hanterar en del av de utmaningar som presenteras i promemorian. Exemplen ska inte uppfattas som exakta svar eller rekommendationer på hur myndigheter ska lösa utmaningarna, utan betraktas som en ögonblicksbild inom ett område som kräver kontinuerligt arbete och ständiga förbättringar.

2. Utmaning – säkerhet och laglighet samt funktionalitet och enkelhet

En arbetsgivare har ett långtgående ansvar att förebygga, upptäcka och förhindra informationsincidenter som till exempel personuppgiftsincidenter. Integritetsskyddsmyndigheten (IMY) har, vad gäller mobila lösningar, konstaterat att det är otillräckligt med organisatoriska åtgärder som rutiner och riktlinjer. Man måste ha tekniska åtgärder på plats för att förhindra informationsincidenter[1]. Många av dagens mobila informationstjänster levereras i form av publika molntjänster vars leverantörer kan ha koppling till länder utanför EU/EES-området eller att informationen behandlas eller på olika sätt görs tillgänglig där. Många av tjänsterna som kan användas i en mobiltelefon erbjuder synkronisering av information, exempelvis bilder och kontakter, till molntjänster som till exempel Apple iCloud, Dropbox, Google Photo, Google Mail och Microsoft OneDrive för att nämna några. Detta är praktiskt, enkelt och lättanvänt

[1] https://www.imy.se/tillsyner/tullverket/

för en användare men synkronisering måste i vissa fall undvikas av svenska myndigheter, för att överföring av personuppgifter eller känslig information inte ska ske.

Om myndigheten tillåter privat användning av tjänstetelefonen kan det uppstå situationer där man ställs inför säkerhetsfrågor av olika slag och komplexitet. Att separera den privata från den tjänsterelaterade informationen, ställer höga krav på tekniska lösningar och tydliga kommunicerade riktlinjer för att uppnå önskad separation. Att kunna säkerställa att någon inte tar ett tjänsterelaterat foto på en whiteboard med känslig information med den privata kamera-appen i stället för med den foto-app som myndigheten tillhandahåller, är ett måste för att undvika risken att informationen av misstag hamnar i en molntjänst.

Myndigheten behöver göra en riskanalys för den mobila enheten och den information som ska hanteras och överväg hur man begränsar eller eliminerar identifierade risker. Frågan är om man kan hantera risker på ett tekniskt acceptabelt sätt. Bara att identifiera samtliga informationsmängder på en tjänstemobil kan vara en utmaning. Utmaningen blir desto större om mobilen tillåts för privat bruk.

För att identifiera vilken information som kan komma att behandlas i mobila enheter, är det bra att förstå hur affärsmodellerna ser ut i den mobila informationsvärlden. I flera av dagens publika appar sker en omfattande informationsinhämtning vilket bland annat har beskrivits av Apple som nyligen har infört möjligheter att begränsa vilken information som lämnar mobiltelefonen. Innan man tar en app (mobil informationstjänst) i bruk, bör man genomföra en appanalys för att bland annat se vilken information som lämnar telefonen och hur informationen hanteras i nästa steg. Denna analys måste göras regelbundet eftersom apparna ständigt uppdateras. Det är av betydande intresse om informationen säljs vidare till ett annonsnätverk, annan organisation eller endast används för att förbättra tjänsten.

När man identifierar informationsmängderna kan de grupperas enligt följande:

1) **Metadata (”data om data”)**. Metadata måste hållas isär från nyttoinformationen som sådan, dvs. den data som är avsedd att hanteras på enheten. Metadata används ibland synonymt med telemetridata (se nedan). Metadata kan visa vem som kommunicerar med vem, när, hur länge och var och lagras ofta i världsomspännande datacentra. Metadata kan vara av mer eller mindre känslig karaktär. Myndigheter bör ta i beaktande att tillskapande och lagring av metadata kan ske på flera ställen och av flera olika leverantörer.

Uppkomst och hantering av metadata kan ske i appar av app-tillverkare, i operativsystemet av tillverkaren och av MDM/EMM-system.

2) **Telemetridata**. IMY definierar telemetridata[2] som *Data som genereras genom användning av tjänsten, även för säkerhetsändamål.* Telemetridata består normalt av säkerhetsrelaterade data och loggar (hur enheten används, vad den stöter på för problem, dess prestanda, etc.), inklusive klientinställningar och olika mätdata som hämtas och hanteras av leverantören. Ofta sker denna informationsinsamling utan att den enskilde användaren märker det. Även denna typ av data är vanligt förekommande i mobila informationssystem.

3) **Verksamhetsdata** är den information som bearbetas för att utföra en arbetsuppgift. Informationen behandlas i själva enheten och kan bestå av ritningar, journaler, e-post-kontakter m.m**.** Här bör man identifiera vilken verksamhetsdata som behandlas på enheten samt vilka risker informationen utsätts för.

4) **De juridiska avtalen (normalt användarvillkoren)**. När en medarbetare laddar ner och registrerar sig för en tjänst ingår hen, genom sitt samtycke, ett avtal med leverantören. En fråga som normalt uppkommer är vad leverantören får göra med information som hanteras i appen, vilket regleras genom villkoren och tillhörande dokument, ofta s.k. integritetspolicy eller liknande. En annan fråga är huruvida man över huvud taget får använda appen som myndighet eller företag utan kompensation av något slag.

~~5)~~ **Privat data**. Användning av privata enheter och tjänster i tjänstesyfte kan förekomma bland företags- och myndighetsanställda eftersom de är lättillgängliga och enkla att använda. Att det är enkelt innebär inte att det är säkert eller tillåtet. En anledning till att det både kan ta lite tid och vara lite krångligare att få igång en bra tjänst på en myndighet eller ett företag är den så kallade certifieringsprocessen vars syfte är att säkerställa en tjänsts funktion, informationshantering och avtal.

6) **Loggdata, krav på loggning.** Myndigheter har ofta krav på sig att logga vem som tar del av information, vilka åtgärder som utförs samt när i tid det sker. Att realisera loggkrav för appar som Facetime, Signal, och Whatsapp ligger bortom myndighetens kontroll. Som stöd i detta arbete kan man använda matrisen som redovisas i **avsnitt 4**.

Genom att konsekvent gå igenom alla risker som kan uppkomma kan man därefter vidta rimliga tekniska åtgärder, kanske i form av en s.k. EMM/UEM-produkt[3], samt

[2] Enligt definition i IMY's frågeformulär om molntjänster.
[3] Enterprise Mobility Management (EMM) och Unified Endpoint Management (UEM) är tekniska hjälpmedel för styrning och kontroll av framförallt myndighetens mobila enheter.

kompletterande organisatoriska åtgärder såsom utbildning och riktlinjer för användandet av mobila enheter.

3. Juridiska förutsättningar

De vanligaste mobila informationstjänsterna tillhandahålls direkt eller indirekt av leverantörer med koppling till tredje land. Detta ställer särskilda krav utifrån dataskydds- och sekretessregelverket[4].

Mot bakgrund av domen i EU-domstolen i det så kallade Schrems II-målet [5](C-311/18), riskerar användning av mobila tjänster att leda till otillåtna informationsöverföringar av personuppgifter till USA. I den nämnda domen slog EU-domstolen fast att det avtal, Privacy Shield[6], som då gällde mellan EU och USA inte gav ett tillräckligt skydd för personuppgifter som överförs till USA eftersom avtalet inte skyddade personuppgifter från att bli utlämnade till amerikanska myndigheter. Eftersom USA:s underrättelselagstiftning är extraterritoriell kan även personuppgifter som inte förts över till USA (alltså lagras i ett EU-land), men som behandlas av leverantörer som är bundna av amerikansk lagstiftning, bli föremål för utlämnande till amerikanska myndigheter.

Myndigheter behöver beakta ett flertal sekretessfrågor och eSams juridiska expertgrupp har i ett rättsligt uttalande[7] slagit fast att sekretessreglerade uppgifter får anses vara röjda om de görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt.

Givet detta kan man fundera på hur det går att påverka leverantörer så att de kan tillhandahålla tjänster anpassade till offentlig sektor i Sverige.

[4] Offentlighets- och sekretesslag (2009:400) Svensk författningssamling 2009:2009:400 t.o.m. SFS 2022:1314 - Riksdagen och Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning Svensk författningssamling 2018:2018:218 t.o.m. SFS 2022:444 - Riksdagen
[5] https://www.imy.se/lagar--regler/dataskyddsforordningen/tredjelandsoverforing/sa-har-paverkar-schrems-ii-domen-overforingar-till-tredje-land/

[6] https://www.privacyshield.gov/Program-Overview

[7] https://www.esamverka.se/download/18.1d126bc174ad1e6c39cac3/1542007824143/eSam%20-%20Ra%CC%88ttsligt%20uttalande%20om%20ro%CC%88jande%20och%20molntj%C3%A4nster.pdf

4. Risker och konsekvenser vid användning av mobila tjänster

Resultatet av ”säkra och legala mobila lösningar” kan innebära begränsningar eller medföra konsekvenser i hur myndigheter och organisationer jobbar med mobilitet och digitalisering idag. Ett sådan konsekvens kan t.ex. vara att tjänstemobilen inte längre bedöms som ”värd” att ta hem kvällstid eftersom man inte får installera appar som är intressanta för privat bruk. Appar som används i myndighetsutövandet med inbyggda funktioner som kan användas för att spåra, avlyssna eller lagra information (t.ex. bilder) om medarbetaren på okända lagringsplatser utan användarens vetskap, kan trots nytta för myndigheten behöva blockeras av säkerhetsrisk. Detta gäller också appar av mer privat natur som kan behöva begränsas på grund av att apparna kan medföra informationsläckage eller andra risker. En negativ effekt av att inte tillåta privat användning av tjänstemobilen är att medarbetare använder sin privata mobil även för vissa tjänsterelaterade aktiviteter, vilket i sig kan medföra läckage av myndigheters information.

Man bör både identifiera, värdera och analysera risker som kan uppkomma och göra konsekvensbedömningar. Risker kan minimeras med olika slags åtgärder, exempelvis på följande sätt:

Risk	Konsekvens	Åtgärd	Konsekvens av åtgärd
Medarbetares GPS-information registreras av appar och företag som säljer informationen vidare	Tjänstemän kan spåras och känsliga platser kan röjas	Inför vitlista för tillåtna appar eller förhindra möjligheten att installera appar	Begränsning av vad användare kan installera kan medföra ökat användande av tjänsterelaterade tjänster i privata mobiler
Kontakter i mobilen fångas upp av andra appar	Kontakter kan publiceras eller säljas vidare	Gör ”kontakter” till en managerad isolerad app	Kontakter ej tillgängliga i icke-managerade appar såsom meddelande- och telefon-appar
Bilder/filmer i bildgalleriet fångas upp av andra appar	Bilder/filmer kan publiceras eller säljas vidare. Metadata i bilderna som plats, tid, info om telefon m.m. röjs	Hantera bilder/filmer i app i säker yta som myndigheten har möjlighet att fullt ut kontrollera och där bilderna/filmerna lagras internt direkt	Man måste lösa hur bilder/filmer transporteras från mobiltelefonen till en betrodd lagringsplats
Appar synkroniserar information till olika molntjänster.	Myndighetens information läcker till obehöriga	”Boxa in” myndighetens information, installera endast tillförlitliga appar, utveckla egna appar, koppla appar endast mot interna system eller betrodda molntjänster, säkerställ DLP-skydd i appar	Publika appar (t.ex. parkerings- och biljettappar) som behövs i arbetet kan inte användas eller utgör fortfarande en risk. Att använda dem med privat användare riskerar ändå att läcka myndighetsrelaterad information

Mötesappar som ”lånar” mikrofon eller kamera	Risk för oönskad avlyssning	Se raden ovan för förslag på åtgärd. Bedöm risken för att andra appar än den av myndigheten utpekade appen ”lånar” detta. Ta sedan beslut hur andra appar än myndighetens ska hanteras	Användaren blir begränsad i vilka mötesappar som får användas
Operativsystem och appar är inte uppdaterade	Myndighetens enheter och appar kan innehålla säkerhetsproblem som en antagonist kan utnyttja	Säkerställ att rutiner finns för kontinuerligt arbete med att hålla enheter och appar uppdaterade	Kräver resurser att hålla allt uppdaterat beroende på hur många operativsystem och appar som måste säkerställas

Utifrån ovanstående exempel på risker bör ett ordinarie informationssäkerhetsarbete utföras.

5. Scenarier

Det finns myndigheter som till största del utför sitt uppdrag i kontorsmiljö och myndigheter som delvis eller helt bedriver sina uppdrag ute i fält. Behovet och nyttjandet av en mobiltelefon skiljer sig åt beroende på var myndigheten bedriver sin verksamhet. Två scenarier beskriver de speciella förutsättningar som finns för de två typerna av myndigheter.

5.1 Kontorsbaserade myndigheter

Medarbetare vid de kontorsbaserade myndigheterna tillbringar största delen av arbetsdagen framför ett digitalt verktyg, företrädesvis en PC. Mobiltelefonen blir i många fall ett komplement i arbetsvardagen. Syftet med mobiltelefonen blir att, förutom att ringa samtal, ta del av information och lösa enklare och snabbare arbetsgifter samtidigt som användaren är mobil. Det kan handla om att läsa och svara på e-post, hantera beställningar av olika slag, ta del av allmän och riktad information, hantera fakturor, söka support och hantera tidsregistrering. Nämnda arbetsuppgifter går också, liksom de flesta arbetsuppgifter, att utföra via myndighetens PC.

Syftet blir därmed till stor del att möjliggöra ökad effektivitet bland medarbetare genom ett mobilare arbetssätt, en förändring som förhoppningsvis också bidrar till nöjdare medarbetare. För kontorsbaserade myndigheter är det därför viktigt att fundera på hur mobiltelefonen får användas. En förutsättning för att det ska vara möjligt att använda telefonen även för visst privat bruk är att man kan garantera it-säkerheten genom att

myndighetens information på mobiltelefonen skyddas. Det är viktigt för att minska behovet av att användarna behöver både en myndighetsmobiltelefon och en privat mobiltelefon. Om användarna måste använda två mobiltelefoner finns det risk att myndighetsmobiltelefonen inte används så mycket. Den effektivitetshöjning som hade kunnat infinna sig om användarna hade möjlighet att utföra vissa arbetsuppgifter när det passar användaren utan att det utgör en risk, uteblir. Dessutom finns en ökad risk att medarbetare börjar utföra arbetsrelaterade uppgifter på sin privata mobil i stället.

5.2 Myndigheter som till stor del eller delvis arbetar i fält

Det finns myndigheter där medarbetare helt eller delvis arbetar ute i fält där mobiltelefonen inte är ett komplement till ett kontorsbaserat arbete utan ett arbetsverktyg. Denna typ av mobiltelefon kanske inte är lämplig att använda till annat än myndighetstjänster vilket kan motivera att den hanteras och styrs centralt samt att alla nödvändiga appar tillhandahålls av myndigheten.

När man arbetar med en mobiltelefon i fält krävs det att den tål väta, stötar och smuts. Man kan skydda en mobil enhet mot stötar genom att använda ett mobilskal. Det finns också speciella mobiltelefoner som klarar av väldigt tuffa miljöer som populärt kallas för ”ruggade enheter”. En ruggad enhet kan vara certifierad enligt IP-standarden vilket anges som t.ex. IP68. Ett EMM-system kan hantera ruggade enheter på samma sätt som vanliga enheter förutsatt att dess operativsystem har stöd för det.

6. Rekommendation

För att få bättre kontroll över vilken information enheter och appar samlar in utifrån de sex exemplen i **avsnitt 2** finns det några åtgärder att vidta utifrån att enheterna och apparna ska användas som mobil informationstjänst för myndighetens information.

6.1 Införa EMM/UEM-system

Den första och viktigaste rekommendationen är att införa ett EMM/UEM-verktyg för att lösa flera av utmaningarna med säker informationshantering på mobiltelefoner. Ett EMM/UEM-verktyg ger följande fördelar;

- Genom att via EMM/UEM-verktyg styra de inställningar som anses nödvändiga på mobiltelefonen för att säkerställa myndighetens information, kan myndigheten undvika risker med informationsincidenter.
- Möjlighet att konsumera interna tjänster i mobiltelefonen och undvika behovet att exponera interna tjänster mot Internet.
- Tillhandahåller inbyggd flerfaktorautentisering för appar och webbtjänster, endast en autentiseringsmetod behövs för all åtkomst.
- Möjlighet att erbjuda privat användande av mobiltelefonen om myndigheten anser det tillämpligt, genom att separera myndighetens information från övrig information på mobiltelefonen.
- Möjlighet att tillämpa BYOD/CYOD-konceptet.
- Möjlighet att sätta krav som enheter måste uppfylla innan de får åtkomst till myndighetens information för att säkerställa att endast säkra enheter får åtkomst.

Samtidigt kan ett EMM/UEM-verktyg ge andra verksamhetsnyttor enligt nedan:

- Tillåta fler typer av plattformar (öppna upp för en större flora av enheter).
- Förutsättningar för att konsolidera och modernt hantera även datorer med Windows och macOS från ett och samma verktyg.
- Kostnadseffektvisering genom inventering av enheter och dess nyttjande för att identifiera telefoner som ligger i en skrivbordslåda och inte används.

Exempel på olika EMM/UEM-verktyg som används i myndigheter och hur de används finns i **bilaga 7.2.**

6.2 Information till användare

En annan rekommendation är att se över myndighetens information och riktlinjer till användare, tillsammans med tekniska alternativ.. Det kan till exempel vara instruktioner om hur man använder vissa funktioner i mobiltelefonen bäst och lämpligast för att hantera myndighetens information. Se exempel i **bilaga 7.1**.

6.3 Använda webbgränssnitt för appar

En tredje rekommendation är att myndigheter använder ett webbgränssnitt i stället för en app. Ofta finns det ett mobilanpassat webbgränssnitt med liknande funktionalitet som appen i sig, kopplat till de flesta mobila tjänsterna. Fördelen med att använda det mobilanpassade webbgränssnittet istället för appen är att det inte samlar på sig information kring användandet på samma sätt. Flertalet interna webbtjänster finns ofta också tillgängliga genom ett mobilanpassat webbgränssnitt.

Des mobilanpassade webbgränssnitten kan tillgängliggöras för användaren genom en centralt hanterad app för webbläsare, vars inställningar kan styras centralt via UEM/EMM-system. Då räcker det att myndigheten säkerställer att appen har en tillräcklig säkerhetsnivå i stället för att säkerställa att varje enskild app uppfyller samma säkerhetsnivå vid införande och över tid.

6.4 Ställa krav på apputvecklare

Appar som flera myndigheter använder borde ge möjlighet att föra dialog med leverantörer i syfte att ställa krav på att apparna innehåller funktioner och säkerhetsåtgärder som passar svenska myndigheter. Det finns inget tekniskt hinder för en app-utvecklare att tillhandahålla en app för publika marknaden och en för svenska myndigheter.

Om leverantörer kan tillhandahålla en app-version som inte funktionsuppdateras så ofta och som har en begränsad mängd funktionalitet, till exempel att inte använda kontakter eller GPS-position som kan vara känsligt eller olämpligt att dela i en molntjänst, kan det öka möjligheterna för myndigheter att kunna använda den. . Konsekvensen kan bli att leverantören får en kostnad om inte appen kan användas i sitt grundutförande, men beroende på vilka risker och vilken nytta det finns med appen, kan det vara en investering värd att ta för en myndighet.

Alla appar som används av en myndighet bör genomgå en certifiering och det finns verktyg för att bl.a. granska vilken information en app samlar in när den används. Många av verktygen är molnbaserade men det finns även onpremise-verktyg. För de molnbaserade verktygen måste myndigheten själv bedöma vad som är möjligt och lämpligt att använda.

6.5 Utveckla egna/gemensamma appar

Ett alternativ att få kontroll på vad appar gör och hur de samlar in och delar med sig av information är att själva utveckla apparna som ska hantera myndighetens information. Detta skulle kunna göras genom myndighetssamverkan för appar som är vanligen förekommande.

En annan fördel med att bygga apparna själv är att det finns möjlighet att anpassa dem så att de direkt stödjer de arbetsprocesser som utförs på myndigheten. Apparna behöver inte alltid byggas helt och hållet från grunden. Ett alternativ kan vara att använda sig av open source-produkter i grunden och sedan utveckla kompletterande delar själv.

6.6 Inte erbjuda mobiltelefon

Att inte erbjuda mobiltelefoner överhuvudtaget kan också vara ett sätt att lösa de krav som finns på säker informationshantering, eller att erbjuda en mobiltelefon utan smarta funktioner som bara hanterar grundfunktioner (samtal och sms). Givet det mervärde ett mobilare arbetssätt och lättillgänglig information ger, är det här egentligen inget alternativ. Bättre är då att med stöd av denna PM, upprätta rutiner, verktyg och ett gediget informationssäkerhetsarbete för att uppnå säkra mobila informationssystem.

7. Bilaga

Märk väl att exemplen i promemorian är hämtade från några svenska myndigheter och deras hantering av utmaningarna som presenteras i promemorian. Exemplen ska inte ses som exakta svar eller rekommendationer på hur myndigheter kan lösa dessa utmaningar. Det är ögonblicksbilder från ett område som kräver kontinuerligt arbete och ständiga förbättringar.

7.1 Exempel på information till användare

För att förebygga informationsincidenter behöver man ge användaren av mobiltelefonen instruktioner och förutsättningar för att använda den på ett säkert och effektivt sätt. T.ex. kan följande punkter, taget från en myndighet som endast erbjuder iPhone, ingå i den information som användaren behöver:

- All information är krypterad, likaså är all datakommunikation till och från mobiltelefonen skyddad från avlyssning genom kryptering, det vill säga allt utom vanliga telefonsamtal och sms som kan avlyssnas genom olika tekniker.
- Det tas inte backup på information som sparas lokalt. Den raderas till exempel i samband med en fabriksåterställning.
- Mobiltelefonen är låst till dig som användare och är personlig. Du öppnar telefonen med en lösenkod och/eller fingeravläsning/ansiktsskanning.
- Om du har skapat ett Apple-id och aktiverat iCloud men inte slagit av synkronisering av bilder till iCloud (under Inställningar, Bilder, ICloud-bilder) och tar bilder med kamera-appen så lagras bilderna både i mobiltelefonen och i molnet. Alla bilder lämpar sig inte att lagras i externa molntjänster.
- I din mobiltelefon ingår ett antal tjänsterelaterade appar.
- Du kan ladda ner ytterligare appar från den interna Appkatalogen
- Privat användning är tillåtet så länge det inte strider mot interna regler eller handledningar.
- SIM-kortet tillhör myndigheten och får inte flyttas till annan enhet.
- Dolt nummer är en standardinställning på myndighetens mobiltelefoner vid externa samtal. Vill du visa ditt nummer ska nummervisning beställas via intranätet.
- Innan du laddar ner en app, tänk på följande:
  - Identifiera vilken information som ska hanteras (ex ditt namn, ladda upp bilder, sökningar).
  - Läs igenom Integritetspolicyn (Privacy policy) om vilken information som samlas in. Denna information finns i respektive Appstore.

- Säkerställ att det är tillåtet att dela informationen som kommer att hanteras i appen med extern part (apptillverkaren).
- Om appen behöver åtkomst till kamera, bildarkiv eller kontakter finns det risk för informationsläckage.

- Tänk på att många appar bara är ett skal runt en webbsida som ofta kan ge extra funktionalitet men även öka risken för informationsläckage, till exempel platsdata via GPS eller kontakter i den öppna delen av telefonen. Många tjänsteleverantörer erbjuder både appar och vanliga webbsidor vilket kan innebära att det går lika bra att använda webbsidan som appen. Man kan välja att lägga en genväg till webbsidan på mobiltelefonens skrivbordsyta för att underlätta åtkomst av tjänsten.
- Du bör alltid tänka på vilken information du hanterar i mobiltelefonen när du är utomlands. Tänk också på att vanliga samtal och SMS kan avlyssnas. Förmedla aldrig skyddsvärd information via dessa kanaler i utlandet. Om du är osäker rådgör med din chef eller cybersäkerhetsteamet om lämpligheten att ta med din mobiltelefon utomlands.

7.2 Exempel från myndigheter på lösningar för mobilhantering enligt problemområden i avsnitt 2

7.2.1 Citrix Endpoint Management (CEM)

Plattform/bakgrundsinformation

Citrix Endpoint Management (CEM) erbjuds både som en lösning för egen drift samt som en molntjänst. Molntjänsten ger även möjligheten (beroende på licensenivå) att använda on premise lagring för vår ”collaborations-lösning”.

Idag hanteras både myndighetsägda och privat/konsultägda enheter i plattformen. Man har valt att tillåta både iOS och Android enheter, men dock standardiserat på begränsat antal modeller med Android för att underlätta i support och förvaltning. Enheter registreras med hjälp utav Apple DEP och Samsung Knox.

Myndigheten driftar själv CEM, som inte supporteras och utvecklas i samma utsträckning som molntjänsterna gör och detta har bidragit till att plattformen har varit svår att arbeta med.

Arbetsrelaterat användande i tjänstemobil/Verksamhetsdata

Myndighetens egna enheter är hanterade fullt ut med både MDM och MAM. Arbetsrelaterade åtkomsten (e-post, kontakter, kalender och intranät) sker via MAM-

registrering i samma plattform och space som MDM-registreringen. Åtkomsten ges via Secure Hub-apparna som kräver nedhämtning via AppStore/Google Play Store med privat konto. Myndigheten tillåter inte registrering via myndighetens e-postadress.

Arbetsrelaterat användande i privat mobil/Verksamhetsdata

Hanteras via MAM-funktion (BYOD) där inte hårdvaran styrs utan enbart myndighetens appcontainer på enheten. Myndigheten tillhandahåller tillgång till e-post och intranät till myndighetens mobila enheter samt till privata och konsultägda enheter i samma plattform och i samma ”space” och flöde via Secure Hub apparna. Dessa kräver nedhämtning via AppStore/Google Play Store med privat konto. Myndigheten tillåter inte registrering via myndighetens e-postadress.

Privat användande/Privat data i tjänstemobil

Inom myndigheten har du rätt att inom begränsad omfattning använda din mobiltelefon för personligt bruk. Mobiltelefonerna kan inventeras regelbundet, och icke godkänt innehåll och otillåtna förändringar i mobilerna kan därmed identifieras.

All privat lagring av information på utrustningen sker på egen risk. Innehållet på telefonen kan vid stöld, misstanke om missbruk, borttappad utrustning m.m. raderas utan förvarning.

Myndigheten har beslutat att klassa alla appar som publiceras på Apples ”App Store” och Googles ”Play Store” som godkända applikationer. Alla nedladdningar av appar sköter du via ditt personliga Apple- eller Google-konto, vilket innebär att du har ett personligt ansvar för dessa inklusive betalningen.

Du får inte utföra några privata betalningar med myndighetens IT-utrustning, på ett sätt som gör att dessa kostnader kommer att belasta myndigheten.

Myndigheten använder samma internetriktlinjer för mobila enheter som för övriga enheter (ex PC).

Tekniska åtgärder utförda i EMM/UEM-plattformen

-

7.2.2 MobileIron

MobileIron UEM är en mobilcentrerad zero-trust säkerhetsplattform för åtkomst och skydd av data i organisationens digitala arbetsplats. MobileIrons zero-trustmetod validerar enheten för att se till att endast auktoriserade användare, enheter, appar och tjänster har åtkomst till företagsresurser.

MobileIron UEM sätter organisationens mobilsäkerhet i centrum och låter organisationen till exempel eliminera lösenord (zero sign-on), för att säkerställa användarautentisering, (multifaktorautentisering (MFA)) och för att upptäcka och mildra säkerhetshot mot enheterna (mobilt hotförsvar (MTD)).

Plattform/bakgrundsinformation

Idag hanteras en del av myndighetens ägda enheter i plattformen och övriga ska flyttas över eftersom. Det har inte ännu tagits fram en färdig lösning för konsult och privata BYOD-enheter.

Myndigheten har valt att tillåta både iOS och Android enheter, dock standardiserat på ett begränsat antal modeller med Android för att underlätta i support och förvaltning. Enheter registreras med hjälp utav Apple DEP och Android Enterprise.

Det genomfördes en krav- och behovsanalys med lösningsalternativ av extern part 2019. Lösningen som pekades ut som bästa alternativ för myndigheten var MobileIron utifrån följande krav:

- Lösningen ska vara möjlig att drifta av myndigheten (med tydlig färdplan för det)
- Stödjer device management, livscykelhantering & säkerhet på myndighetens mobila enheter inkl. asset managememt, enhetshistorik, policies, konfiguration, compliance kontroll m.m. De vill säga full MDM-funktionalitet
- Stödjer Zero-Touch deployment (m.h.a. Apple DEP och Android Enterprise/Samsung KME)
- Tillåter användning av flera mobila OS, framförallt Android & iOS
- Tillåter användning av standardappar för t.ex. myndighetens e-post och intranät (lämnar container-tänket)
- Stödjer kombination av privat- och myndighetsanvändning, bl.a.
- Inget behov av privata Apple eller Google-konton för att utföra myndighetsarbetet
- Tillåta privat webbanvändning

- Tillåta nerladdning/användning av public store appar
- Tillhandahålla plattform för
- licensering/publicering av myndigheten utvalda public store-appar (t.ex. via Apple VPP)
- utveckling/publicering av tredjepartsutvecklade myndighetsappar
- utveckling/publicering av myndigheten egenutvecklade appar (native & PWA)
- Stödjer full nyttjande av myndighetens telefonilösningar t.ex. hänvisning, katalogsök, MEX, skypesamtal m.m.
- Stödjer användarens/verksamhetens mobila arbetssätt
- Stöd för fleranvändarenheter
- Stöd för avvikande hantering av resultatenheter
- Stöd för säker åtkomst till myndighetens interna resurser från konsulters mobiltelefoner

Arbetsrelaterat användande i tjänstemobil/Verksamhetsdata

Myndighetens egna enheter är hanterade fullt ut med både MDM och MAM. MDM- och MAM-registreringen sker tillsammans i registreringen/uppstarten av enheten. MobileIron ger möjligheten att använda native-apparna i mobilen för e-post, kontakter, kalender och intranät. Vilket tar bort kravet för AppleID/Google-konto för att få åtkomst till myndighetens information som tidigare behövts.

Arbetsrelaterat användande i privat mobil/Verksamhetsdata

Myndigheten tillåter även åtkomst till e-post, kontakter, kalender och intranät från privata enheter. Idag finns den lösningen i XenMobile via Secure Hub-apparna.

Man kan för tillfället också nå sin e-post på privata mobilenheter via ”Min sida - extern anslutning” på Myndigheten.se. Myndigheten jobbar på att ta fram en lösning för åtkomst för privat- och konsultägda enheter i MobileIron som ännu inte är färdig.

Privat användande/Privat data i tjänstemobil

Inom myndigheten har du rätt att inom begränsad omfattning använda din telefon för personligt bruk. Mobiltelefonerna kan inventeras regelbundet, och icke godkänt innehåll och otillåtna förändringar i telefonerna därmed identifieras.

All privat lagring av information på utrustningen sker på egen risk. Innehållet på telefonen kan vid stöld, misstanke om missbruk, borttappad utrustning m.m. raderas utan förvarning.

Myndigheten har beslutat att klassa alla appar som publiceras på Apples ”App Store” och Googles ”Play Store” som godkända applikationer. Alla nedladdningar av appar sköter man via sitt personliga Apple- eller Google-konto, vilket innebär att man har ett personligt ansvar för dessa inklusive betalningen.

Man får inte utföra några privata betalningar med myndighetens IT-utrustning, på ett sätt som gör att dessa kostnader kommer att belasta myndigheten. Myndigheten använder samma internetriktlinjer för mobila enheter som för övriga enheter (ex PC).

Tekniska åtgärder utförda i EMM/UEM-plattformen

- MobileIron har installerats on prem i myndighetens egen miljö och på egna servrar, och driftas internt på myndigheten utav egna drifttekniker.
- Registrering av mobiltelefonerna för effektiv förvaltning, bl.a. se vem telefonen tillhör.
- Funktion för att se bilagor i e-post men spärrat att kunna spara ner dessa på enheten och att kunna skicka dem vidare via privata mailen.
- Spärrat skärmklipp (tillåts för ett fåtal användare).
- Spärrat iCloud-backup.
- Spärrat åtkomst mellan Android-enhet och dator via sladd.
- Spärrat synkning av draft-mappen via PointSharp. I förlängningen ska det istället införas scanning med lcap där man initierar detta från PS.
- Använder arbetsprofil på Android-enheterna.
- Support i form av hjälp med bland annat upplåsning, låsning och spärrning av sin mobila enhet.
- Säkerhet genom att vi kan styra åtkomst till enheten så enbart den anställde som enheten tillhör har åtkomst,samt spärra funktioner som it-säkerhet beslutat inte är tillåtna.
- Möjliggör utveckling, licensering och publicering av myndighetsanpassade appar.
- Lägsta nivå på tillåtna version av respektive OS, uppdateras inte enheten kontinuerligt tappar enheten åtkomst till myndighetsinformationen tills den uppfyller kraven igen.
- Första enrollment kräver autentisering i tre steg.
- Myndighetens-konto + PIN-kod.

- Användaren ska vara uppkopplad via ett myndighetskontor.
- Koll på enhetens unika id.
- Enheterna i plattformen har krav på skärmlåskod, längdkrav samt att denna ska bytas ut regelbundet precis som lösenord på datorn.
- Myndigheten använder idag både Mideye OTP (intranät) samt PointSharp med biometri (e-post) med en synktid som först var satt till 72h men förlängdes till 7 dagar innan lansering. Om tiden för autentiseringen gått ut försvinner alla e-post och bokningar från enheten tills den förlängs. Kommer över tid enbart bli PointSharp för båda.

7.2.3 WMware Workspace ONE

Workspace ONE Unified Endpoint Management (UEM) är en lösning som hanterar alla enhetstyper på alla plattformar i alla användningsfall. Den innehåller modern enhetshantering, applikationshantering och säkerhet för att ge organisationen kontroll över en diversifierad enhetsflora som finns i många organisationer idag. Workspace ONE finns tillgänglig som publik molntjänst och som on prem-installation. Den publika molntjänsten går att få i en delad miljö eller som en dedikerad miljö hos VMware.

Plattform/bakgrundsinformation

Workspace ONE består av flera komponenter och praktisk användning finns av nedanstående. Där samtliga är tillgängliga on prem.

- Workspace ONE UEM
  - Device Services (DS)
  - Email Notification Service 2 (ENS2)
  - Unified Access Gateway (UAG)
  - AirWatch Cloud Messaging (AWCM)
  - AirWatch Cloud Connector (ACC)
  - Secure Email Gateway (SEG)
  - Self Service Portal (SSP)
  - Console Server (CS)
- Workspace ONE Access
  - Access Appliance
  - Access Connector

VMware upplevs dedikerade till att fortsätta med ett on prem-alternativ. Det de fortsätter påpeka skiljer på moln och on prem är att uppdateringar till on prem kan släpa lite i relation till molnleveransen. Detta är så klart något som både kan ses som en fördel och nackdel. En fördel är att uppdateringarna är mer testade i verkligheten innan man uppdaterar. Men vill man snabbt ha de senaste och nya funktioner kan det vara till nackdel. De viktigaste komponenterna för managering av mobiltelefoner finns on prem. Då ingår funktioner som e-post, kalender och kontakter i mobiltelefonen. Samt funktion för att tillgängliggöra interna funktioner/tjänster i mobiltelefonen m.h.a. autentisering- och enhetskontrollsfunktioner. Ett tydligt ställningstagande för deras åtagande på on prem-installation är att den nya komponenten Freestyle Orchestrator även kommer on prem. En komponent som konstaterats att den bara finns tillgänglig i molnet är Workspace ONE Intelligence.

VMware har flera olika licenspaketering, men en som täcker behovet för managering av iOS, Android, Mac och Windows är Advanced Edition. VMware håller i skrivande stund på att se över hur de ska paketera licenserna och kommer komma med mer differentierade paketeringar som ska vara mer uppdelade efter vilka plattformar man vill hantera, t.ex. en paketering för mobiltelefoner och en annan för datorer (VMware Workspace ONE Editions Comparison Table).

För att få till en bra och säker hantering kan det finnas anledning att titta på och ta ställning till, till viss del av VMwares och Apples molninfrastruktur. För att, där det behövs, nå den funktion som anses behövas. Ett exempel är VMwares Cloud Notification Service (CNS). Den behövs för att e-post- och kalenderappen Boxer ska kunna ta emot notiser för nya e-postmeddelanden. För att hantera att inte information om e-postmeddelandet ska skickas till VMware och Apple via APNS så kan man i Email Notification Service 2 (ENS2) konfigurera att endast en notis att det kommit ett e-postmeddelande skickas. Då tas inte ämne eller avsändare med i notisen. Det finns även några fler kopplingar till VMware för att infrastrukturen ska fungera korrekt. Innan man använder dessa bör man noga analysera t.ex. vad som skickas till VMware, till vilken grad man litar på dem och att inga användaruppgifter skickas till VMware.

För att nyttja Apples DEP-registrering och central införskaffning av appar behövs Apple Business Manager. Även där måste varje myndighet analysera molntjänsten och göra egna bedömningar om man anser den lämplig och i vilken utsträckning den går att använda.

Arbetsrelaterat användande i tjänstemobil/Verksamhetsdata

Med Workspace ONE finns möjligheten att ansluta mobiltelefoner till lösningen utan att behöva använda ett AppleID. Det finns olika scenarion för att ansluta en enhet. Dels ett där det första användaren behöver göra är att ladda ner en app, och då behövs ett AppleID. Men det finns också ett scenario där man istället använder en webbläsare för att surfa till en adress och då får appen distribuerad från Workspace ONE. I det scenariot behövs således inget AppleID. Använder man sig av DEP-registrering finns heller inget krav på AppleID. När väl mobiltelefonen är ansluten har Workspace ONE möjlighet att både distribuera och tillgängliggöra de appar som behövs för arbetet utan några krav på att användaren behöver ett AppleID.

I Workspace ONE finns tillgång till deras produktivitetsappar som t.ex. hanterar e-post, kalender, kontakter, uppgifter och anteckningar mot Exchange. Det finns även en webbläsar-app samt en app för att dela ut och spara filer mot interna lagringsytor. En stor fördel med dessa appar är att de kommer med VMwares SDK för Digital Workspace (SDKs: vSphere SDK, vCenter SDK, vCloud SDK - VMware {code}) inbyggt. Genom dessa SDKs så finns möjligheten att på detaljerad nivå styra inställningar i appen och skapa ett säkert DLP-skydd. T.ex. kan man styra om back up ska tas mot iCloud eller inte. Dessa SDKs finns dokumenterade och förklarade så att om myndigheten själv utvecklar appar kan dessa byggas in. Men det är även fritt fram för andra apputvecklare att bygga in dessa. I och med att den medföljande webbläsarappen har alla SDK inbyggt blir det, utifrån information på mobiltelefonen, relativt enkelt att tillgängliggöra interna responsiva webbtjänster i den myndighetskontrollerade ytan. Sedan måste autentisering och liknande också hanteras.

Produktivitetsappar som det finns faktisk aktiv användning av bland myndigheter är:

- Boxer, e-post, kalender och kontakter
- Web, webbläsare
- Intelligent Hub, app för managering och applikationsportal (för applikationsportal krävs Access)

Och några som utvärderas är:

- Content, hanterar koppling mot interna lagringsplatser
- Notebook, synkronisering av uppgifter och anteckningar till/från Exchange

Samtliga av dessa innehåller VMwares SDK och är således möjliga att hantera i den säkra ytan.

En utmaning i myndighetsmiljöer kan vara användning av EFOS (eller liknande) och smarta kort där man som användare inte känner till sitt lösenord. Med Workspace ONE är det möjligt att använda sig av certifikat som omvandlas till kerberos för autentisering mot Exchange. Det är med andra ord möjligt att få till en lösning där det inte krävs några lösenord för att få igång en synkronisering från Exchange till mobiltelefonen. Förutom PIN-kod till mobiltelefonen och den säkra ytan om man vill.

I Workspace ONE finns även komponenten Access som ger möjligheten att utöka verksamhetsnyttan i mobiltelefonerna. Komponenten har många funktioner, men det primära användningsfallet är att använda den till att ge säker åtkomst till mer verksamhetsinformation inom den säkra ytan. Access kan användas tillsammans med inloggning med t.ex. Mobilt EFOS för att ge åtkomst till t.ex. intranät, tidrapportering, fakturahantering, support. Efter inloggning med Mobilt EFOS är det sedan möjligt med SSO in till de funktioner som tillgängliggörs. Access har flertalet integrationsmöjligheter som t.ex. SAML, OpenID Connect och Mobile SSO. Access har också möjligheten att integrera med Workspace ONE UEM för att kontrollera enhetens status innan den släpps in.

Med hjälp av certifikat från Workspace ONE och egna utställda certifikat kan man helt eliminera behovet av lösenord. Det är däremot rekommenderat att ställa krav på är PIN-kod på mobiltelefonen och in till den säkra ytan. Båda dessa går att använda tillsammans med FaceID och TouchID på iOS.

Arbetsrelaterat användande i privat mobil/Verksamhetsdata

-

Privat användande/Privat data i tjänstemobil

Med hjälp av appar med SDK inbyggt finns möjligheten att skapa en säker yta på mobiltelefonen där myndighetens information kan hanteras säkert och inte riskera ofrivilligt läckage. Medan resterande del av mobiltelefonen har möjlighet att fungera så som plattformen är tänkt att fungera från tillverkaren.

Ett steg om man funderar på att tillåta privat användning är att man bör göra ett avvägande om man vill och kan tillåta användarna att skapa AppleID och använda på sin mobiltelefon. Där måste man ta i beaktande hur man vill att användarna ska kunna

använda mobiltelefonen och hur man ser på AppleID i sin organisation. Det är tekniskt möjligt att blockera användandet av AppleID eller AppStore via Workspace ONE.

Tekniska åtgärder utförda i EMM/UEM-plattformen

I och med det skapas en säker yta på mobiltelefonen där ingen information får flyttas in eller ur den ytan så innebär det att Telefon-appen inte når kontakterna som finns lagrad i Boxer. Det innebär att det inte syns vilken kontakt det är som ringer eller vilken kontakt SMS-trådar hör till, endast telefonnumren syns. För inkommande telefonsamtal så finns det en inbyggd funktion i iOS under Inställningar -> Telefon -> Samtals-ID och blockering där användare kan aktivera Samtals-ID från Boxer. Det framgår då vid inkommande samtal vilken kontakt i Boxer som ringer. Detta gäller endast de kontakter man sparat som personliga kontakter och inte från globala adresslistan i Exchange. Vidare så är detta ingen inställning som går att styra centralt utan något som varje användare själv måste aktivera. För SMS finns inte vetskap om någon work around. Det kan verka som en banal funktion, men är något som man måste vara beredd på kommer generera diskussioner med användare.

En till sak som är bra att ha vetskap om är konsekvenserna om man inte tillåter att bifoga filmer och bilder till e-post i Boxer. Det innebär att användare inte kan fota eller filma med Kamera-appen i iOS och bifoga dem till e-post. Det är något man bör vara medveten om att det används ganska flitigt av användare. Det innebär att medarbetare använder iOS inbyggda funktioner och de eventuella problem som kan finnas med att filmer och bilder synkas till molntjänster. Om man helt vill undvika detta är ett tips att kika på Content-appen som VMware tillhandahåller. Där finns möjlighet att tillgängliggöra interna lagringsytor som en del av den säkra ytan på mobiltelefonen. Men det finns några om och men med den som man behöver anpassa sig efter.

7.2.4 BlackBerry UEM

BlackBerry UEM är ett UEM/EMM/MDM-verktyg från det kanadensiska företaget BlackBerry. BlackBerry hade från början en produkt som enbart hanterade det egna mobiloperativsystemet BlackBerry OS, men 2015 förvärvades det amerikanska företaget Good Technology och verktyget Good. Idag har man slagit ihop de två verktygen till ett, och det finns ett flertal paketlösningar för att tillgodose kundernas olika behov. BlackBerry UEM finns både som molntjänst och on prem.

I on prem-lösningar installeras servermjukvaran på kundens Windows-servrar och därefter ansluts tjänster såsom AD, e-postinfrastruktur, intranättjänster, Skype for

Business, Apple Push Notification Service och Googles Firebase Cloud Messaging. På användarnas enheter installeras och aktiveras ett antal BlackBerry-appar (klientprogramvara) som tillsammans bildar en krypterad sandbox/container som håller kundens information åtskild från övrig okontrollerad information på enheten. Klientprogramvaran finns för Android, iOS, iPadOS, macOS och Windows. För att aktivera BlackBerry hos myndigheten på en Android eller iPhone/iPad krävs att användaren är inloggad på en tjänstedator med ett smartcard. Användaren tar fram en engångs QR-kod på datorn som sedan skannas av mobilen. På så sätt kan tillitsnivån som datorn har även överföras till mobilen, eller med andra ord, man vet vem som håller i mobilen.

All datatrafik går krypterad från den krypterade sandboxen direkt till myndighetens on prem-miljö, med undantag när användaren aktiverar BlackBerry på sin enhet. Då överförs användarens företags-mejladress, i syfte att räkna licenser, till företaget BlackBerrys datacenter placerat i EU.

Beroende på vilket behov en myndighet har kan sandboxen innehålla olika BlackBerry-appar, till exempel standardfunktionalitet som e-post, kalender, kontakter, uppgifter, intranät, chat och närvarostatus. Men det går även att ansluta anpassade tredjepartsprodukter till sandboxen. Ett sådant exempel är CAPTOR for BlackBerry som kan skanna ett pappersdokument med mobilen och sedan transportera det till destinationen utan att informationen lämnar kundens krypterade infrastruktur. Ett annat exempel är ServiceNow for BlackBerry.

Plattform/bakgrundsinformation

Myndigheten initierade 2011 en förstudie för att ta fram en säker e-post-i-mobilen-lösning för Android-mobiler och iPhones. Verktyg som utvärderades var MobileIron, Good, AirWatch (numera VMware Workspace One), DME (dansk sandbox-lösning), Capricode, PointSharp samt Touchdown (en mejl-sandbox för Android). Förstudien visade att det inte gick att säkra upp myndighetens information på mobilerna med traditionella MDM-verktyg utan pekade på att dataläckage inte bara var en risk utan rent av ett faktum. Valet blev därför ett verktyg som byggde på sandbox-teknologi och det enda verktyg som då uppfyllde alla krav var Good. Myndigheten införde Good 2012 och har sedan dess haft samma lösning i drift men med olika leverantörer gällande licenser och support.

Våren 2021 avropade vi ett nytt avtal på Kammarkollegiets ramavtal Programvaror och tjänster. Två leverantörer med varsin produkt inkom med svar, Atea med VMware

Workspace One samt Crayon med BlackBerry. Crayon, som hade det lägsta priset, tilldelades licens- och konsultavtal under 2+1+1 år. Den avropade licensnivån (paketlösningen) är BlackBerry Spark UEM Express Suite. Antalet avropade licenser är för 6500 användare men kan justeras i steg om 500. Varje användare kan ha upp till 5 enheter.

Myndigheten hanterar drift, underhåll och support av lösningen med egen personal förutom fjärdelinjens support som utförs av BlackBerrys supportorganisation. I avtalet ingår även timmar för avrop av konsulthjälp om behov finns. Underleverantör till Crayon för konsulthjälp är det norskägda TechStep.

Myndigheten har cirka 11 000 medarbetare (anställda och konsulter). Att aktivera BlackBerry på sin mobiltelefon är frivilligt och under åren har mellan 40 och 50 procent av medarbetarna använt sig av BlackBerry. Under pandemin har andelen varit lägre men nu när återgång till arbetsplatsen har påbörjats, börjar siffran att klättra igen. Myndigheten har även infört OneDrive under hösten 2021 vilket innebär att användarna har flyttat sina dokument från filservrar till en plats som kan nås av BlackBerrys webbläsare på mobilerna. Samtidigt har intranätet bytt hemsida och blivit responsiv, vilket troligen också ökar intresset för att läsa information i mobilen.

Arbetsrelaterat användande i tjänstemobil/Verksamhetsdata

Vi har medvetet satsat på att göra interna responsiva webbtjänster för interna behov i stället för Android- eller iOS-appar av tre skäl. Det första är att användarna inte kan sina AD-lösenord och då blir det svårt/omöjligt att logga in med en app som är utanför BlackBerry-sandboxen. Det andra är att man slipper ha kompetens för utveckling och underhåll av Android- och iOS-apparna, och det tredje är att om/när man byter UEM-verktyg är det lätt att kliva ur och man behöver inte göra om alla appar igen.

Det finns endast en BlackBerry-profil för alla mobiler som skjuts ut när man aktiverar BlackBerry. Genom att ha en enda profil och samma rutiner för alla mobiler blir förvaltningen och supporten enklare. Vi gör alltså ingen skillnad på tjänstemobiler, privata mobiler eller konsulters mobiler, och ur BlackBerrys synvinkel är alla mobiler av typen BYOD (Bring Your Own Device). Detta är inget hinder för tjänstemobilerna eftersom vi inte har asset-hanteringen i BlackBerry utan i ett annat system. Vi ”enrollar” inte heller våra hyrda tjänstemobiler in i BlackBerry med hjälp av DEP/AZT/KME, men däremot använder vi molntjänsten KME för att låsa upp återlämnade Samsung-mobiler när användaren inte har tagit bort sina lösenord etc (när Factory Reset Protection har aktiverats). Genom att endast ha en ”BYOD-profil” blir det också lättare

kliva ur om/när man byter UEM-verktyg. Avtalet för hyra av tjänstemobiler, inkl enrollmenttjänsterna DEP, AZT och KME, är ett eget avtal och är inte synkroniserat med myndighetens nuvarande avtal för UEM-verktyg.

Arbetsrelaterat användande i privat mobil/Verksamhetsdata

-

Privat användande/Privat data i tjänstemobil

-

Tekniska åtgärder utförda i EMM/UEM plattformen

Utvärdering av CAPTOR for BlackBerry, en skanningsapp kopplad till BlackBerry-sandboxen för att skanna pappersdokument på (tillfälliga) kontor där det inte finns en skanner eller nätverk till skanner. CAPTOR finns även för andra UEM-verktyg. Man kan alltså fortsätta använda CAPTOR även om man byter UEM-verktyg.

Pilot att använda Wi-Fi-samtal på tjänstemobilerna när mobiltäckningen på kontor inte är tillräcklig genom att skjuta ut Wi-Fi-profil till mobilerna med hjälp av BlackBerry. När användaren kliver in på ett kontor så ansluts mobilen automatiskt till Wi-Fi-nätverket utan användarens medverkan. Mobilen växlar sedan automatiskt mellan Wi-Fi-samtal och samtal över mobilnätet.

7.2.5 Andra verktyg på marknaden

Arbetsgruppen har valt att beskriva de EMM/UEM-verktyg det finns praktisk erfarenhet av på myndigheterna. Förutom de verktygen det i arbetsgruppen finns praktisk erfarenhet av så finns det många alternativ på marknaden. Ett urval av dessa framgår i efterföljande avsnitt. Tänk också på att ta i beaktande vilka möjligheter det finns till egen drift av dessa verktyg och vilka som finns som molntjänst. Det är sedan upp till myndigheten att bedöma vilket verktyg som är lämpligt.

7.2.5.1 Microsoft Intune

Microsoft Intune är en molnbaserad tjänst som fokuserar på hantering av mobilenheter (MDM) och hantering av mobilprogram (MAM). Med Intune kan du välja att vara 100 % i molnet med Intune, eller vara samhanterade med Configuration Manager och Intune.

7.2.5.2 JAMF

Jamf-programsvit innehåller en mängd olika verktyg för att hantera Apple-enheter inklusive iOS, iPadOS, macOS och tvOS.

7.2.5.3 IBM MaaS360

IBM Security MaaS360 med Watson erbjuder en Software-as-a-Service (SaaS)-baserad UEM-lösning (Unified Endpoint Management) som kan hantera och säkra ett brett utbud av enheter, applikationer, innehåll och data. Tjänsten inkluderar mobile threat defence och Identity-as-a-Service (IDaaS) med multifaktorautentisering (MFA). Artificiell intelligens (AI) och analyser lyfter frågor och ger administratörer insikt i vad som påverkas och hur man kan åtgärda det.

8. Definitionslista

Begrepp	Definition
MDM	Mobile Device Management har kontroll över hela den mobila enheten och upprätthåller säkerhetspolicyer och möjliggör enhetsövervakning i realtid.
MAM	Mobile Application Management används för att hantera applikationer på en mobil enhet och för att separera jobbapplikationer från personliga applikationer.
MCM	MCM (Mobile Content Management) styr över innehållet på mobila enheter. T.ex. om och hur användarna får ta del av och skapa information på intranät, portaler och andra lagringsytor i mobila enheter.
EMM	Enterprise Mobility Management är en sammansättning av funktionerna MDM, MAM och MCM.
UEM	Unified Endpoint Management är en sammansättning av EMM-verktygsuppsättningarna. Förutom att hantera smartphones, surfplattor och bärbara datorer kan UEM-programvara hantera TV-apparater, Internet of Things (IoT)-enheter, wearables som smartwatches och mer.
BYOD	Bring Your Own Device (BYOD) tillåter anställda eller konsulter att använda sina personliga enheter

	i arbetssyfte. Arbetsgivaren kan komma att ge en ersättning för detta till den anställde.
CYOD	Choose Your Own Device (CYOD) ger anställda ett urval av godkända mobila enheter. Detta är ett alternativ till BYOD. Beroende på policy kan den anställde betala för enheten och äga den, eller så kommer företaget att betala anställda en ersättning för att täcka kostnaderna men behåller ägandet.
COPE	Corporate Owned, Personally Enabled (företagsägt personligt aktiverat) är en affärsmodell där en organisation förser sina anställda med mobila datorenheter och tillåter anställda att använda dem som om de vore personligt ägda bärbara datorer, surfplattor eller smartphones.
COBO	Corporate Owned, Business Only Företagsägt, endast företagsanvändande.
Mobilanpassade webbgränssnitt	Webbsidor som anpassar sitt utseende efter storleken på enhetens skärm för att skapa en bra användarupplevelse oavsett enhet.
Mobila informationssystem	Mobila informationssystem är informationssystem speciellt utvecklade för att användas eller nås via mobila enheter. De mobila informationssystemen, även kända som "appar", är kompakta informationssystem som utför specifika uppgifter för de mobila enheternas användare när som helst, var som helst, platsoberoende. Dessa appar kan antingen laddas ner och installeras eller nås via webbläsare beroende på bakomliggande system.
IP68	Ingress Protection 68, och det anger hur bra mobilen är att förhindra saker från att tränga in i den. Den första siffran anger hur bra den är på att skydda mot små fasta partiklar (damm/sand etc), med en maximal rating på 6. Den andra siffran är vätske- eller vattentäthetsklassificeringen, med ett maxvärde på 9. Detta var en enkel sammanfattning om IP-certifiering och du hittar mer info detta på https://en.wikipedia.org/wiki/IP_code.

eSam är ett medlemsdrivet program för samverkan mellan 34 myndigheter för att underlätta och påskynda digitaliseringen inom det offentliga Sverige. eSam bildades 2015 som en frivillig fortsättning på E-delegationen. En viktig uppgift för eSam är att ta fram stöd och vägledningar som ger förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Alla stöddokument finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, eHälso-myndigheten, Ekonomistyrningsverket, Folkhälsomyndigheten, Försäkringskassan, Havs- och vattenmyndigheten, Inspektionen för vård och omsorg, Jordbruksverket, Kriminalvården, Kronofogdemyndigheten, Lantmäteriet, Länsstyrelserna, Migrationsverket, Naturvårdsverket, Patent- och Registreringsverket, Pensionsmyndigheten, Riksarkivet, Rättsmedicinalverket, Sida, Skatteverket, Skolverket, Statens institutionsstyrelse, Statens servicecenter, Statens tjänstepensionsverk, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket och Universitets- och högskolerådet (december 2021)