Säker åtkomst till företagsnätverk via mobila enheter

Björn Bergström

Examensarbete

Informationsteknik

2014

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Informations- och medieteknik
Identifikationsnummer:	4836
Författare:	Björn Bergström
Arbetets namn:	Säker åtkomst till företagsnätverk via mobila enheter
Handledare (Arcada):	Jonny Karlsson
Uppdragsgivare:	Nordiska Investeringsbanken NIB

Sammandrag:

Detta examensarbete är ett beställningsarbete åt Nordiska Investeringsbanken NIB. Uppdragsgivaren vill att användare skall med sina mobila enheter komma åt sina filer inom det säkra interna nätverket och erbjuda åtkomst för personliga enheter om det är möjligt. Detta skall lösas genom att ta i bruk en tjänst som erbjuder detta. Uppdragsgivaren vill också veta hur de största operativsystem för mobila enheter som finns på marknaden gör för att säkra information som finns på enheter.
Arbetet är uppbyggt i tre delar. Första delen innehåller kort teori om olika sätt att göra en distansanslutning med mobila enheter. Det förklaras även hur mobila enheter administreras i företag. Andra delen förklarar de tre största mobila operativsystemen och vad dessa gör för att skydda information som finns på mobila enheter. I den tredje och sista delen presenteras tre alternativa tjänster som uppfyller uppdragsgivarens önskemål.

Nyckelord:	Nordiska Investeringsbanken, Mobile Device Management, iOS, Windows Phone 8.1, Android, Airwatch, XenMobile, Good Technololgy
Sidantal:	60
Språk:	Svenska
Datum för godkännande:	10.2.2015

DEGREE THESIS	
Arcada	
Degree Programme:	Information Technology
Identification number:	4836
Author:	Björn Bergström
Title:	Secure ways of connecting to an internal network using mobile devices
Supervisor (Arcada):	Jonny Karlsson
Commissioned by:	Nordic Investment Bank NIB

Abstract:

This thesis is commissioned by Nordic Investment Bank NIB. The commissioner wants users to be able to use their corporate and possibly also their personal devices to connect to an internal network and access their files. This will be solved by implementing a suitable service software. The commissioner also wants to know how the largest mobile operating systems secure all the information that is saved on devices.
The thesis is divided into three parts. The first part consists of theory about different types of remote connections with mobile devices to internal networks. In this part it is also explained how mobile devices are managed in companies. The second part describes the three largest mobile operating systems and what these do to protect the information stored on mobile devices. In the third and last part three alternative services fulfilling the requirements of the employer are presented.

Keywords:	Nordic Investment Bank, Mobile Device Management, iOS, Windows Phone 8.1, Android, Airwatch, XenMobile, Good Technology
Number of pages:	60
Language:	Swedish
Date of acceptance:	10.2.2015

INNEHÅLL

Figurer

Tabeller

Lista över förkortningar

NIB	Nordiska Investeringsbanken
IFI	Internationell finansinstitution
BYOD	Bring Your Own Device
VPN	Virtual Private Network
PPTP	Point-to-Point Tunneling Protocol
L2TP	Layer 2 Tunneling Protocol
EAS	Exchange ActiveSync
MDM	Mobile Device Management
MAM	Mobile Application Management
CA	Certificate Authority
LLB	Low-Level Bootloader
UID	Unique Identification Number
AES	Advanced Encryption Standard
DMA	Direct Memory Access
API	Application Programming Interface
SSL	Secure Socket Layer

TLS	Transport Layer Security
WPA, WPA2	Wi-Fi Protected Access
SSO	Single Sign-on
UEFI	Unified Extensible Firmware Interface
BIOS	Basic Input-Output System
TPM	Trusted Platform Module
IRM	Information Rights Management
S/MIME	Secure/Multipurpose Internet Mail Extension
LOB	Line-of-Business
ASLR	Adress Space Layout Randomization
DEP	Data Execution Prevention
WEP	Wired Equivalent Privacy
EAP-TLS	Extensible Authentication Protocol - TLS
EAP-TTLS	EAP – Tunneled Transport Layer Security
IPC	Inter Process Communication
TOU	Terms of Use

SDK	Software Development Kit
AD	Active Directory
HTTP	Hypertext Transfer Protocol
SAML	Security Assertion Markup Language
XML	Extensible Markup Language
KCD	Kerberos Constrained Delegation

1 INLEDNING

Detta examensarbete är beställt av Nordiska Investeringsbanken, NIB. NIB är en internationell finansinstitution (IFI) som ägs av Finland, Sverige, Danmark, Norge, Lettland, Litauen, Estland och Island. Huvudkontoret finns i Helsingfors och NIB har ungefär 200 anställda. Teorin i arbetet är baserad på empirisk forskning.

Uppdragsgivaren vill att alla deras anställda skall enkelt ha möjlighet på ett säkert sätt ansluta till det interna nätverket och komma åt sina filer var än de befinner sig med sina mobila enheter. Detta skall ske på ett säkert sätt så att inte konfidentiell information läcker ut åt utomstående parter. För tillfället kommer alla användare åt sin e-post, men idén är att man även skall komma åt Microsoft Sharepoint omgivningen och sina personliga filer som finns inom det interna nätverket. Examensarbetet kommer att gå ut på att kort granska säkerhetsarkitekturen i de tre största mobila operativsystemen och sedan utreda vilka olika tjänster som passar företagets infrastruktur. Olika tekniker som används för att åstadkomma detta kommer även att presenteras.

1.1 Målsättningar

Målet med examensarbetet är att undersöka olika lösningar som erbjuds som tjänster, d.v.s. inte att skapa ett system själv. Denna tjänst skall erbjuda möjligheten att en användare säkert kommer åt sina filer inom det interna nätverket. En betydande fördel skulle vara om tjänsten även skulle erbjuda en så kallad ”Bring Your Own Device” (BYOD) modell. Uppdragsgivaren erbjuder sina anställda smarttelefoner men skulle även vilja att användare skulle ha möjlighet att använda sina egna telefoner och pekplattor för sitt arbete. Detta kräver att det skulle finnas en miljö inom den personliga enheten som inte kan kommunicera med andra personliga program som finns just i den enheten. Det finns företag som erbjuder dessa tjänster och ur dessa företag kommer några att väljas och presenteras, sådana som skulle vara passliga för uppdragsgivaren.

1.2 Avgränsningar

Jag kommer inte att presentera hur själva nätverket är uppbyggt inom NIB och därför kommer inte arbetet att innehålla vilken tjänst som möjligen blir vald. Arbetet omfattar snarare en utförlig beskrivning på olika tjänster som uppfyller uppdragsgivarens behov.

På grund av licensavtal och praktiska arrangemang ingår ingen information om implementering eller testning av den valda tjänsten hos uppdragsgivaren i examensarbetet.

2 EN ÖVERSIKT ÖVER TEKNIKER SOM ANVÄNDS FÖR DISTANSANSLUTNINGAR SAMT ADMINISTRATION AV MOBILA ENHETER

Detta kapitel förklarar kort centrala begrepp som behandlas senare i arbetet. Främst sådana begrepp som har betydelse för hur distansanslutningen till interna nätverket skapas samt lite olika termer som är bra för läsaren att veta.

2.1 VPN

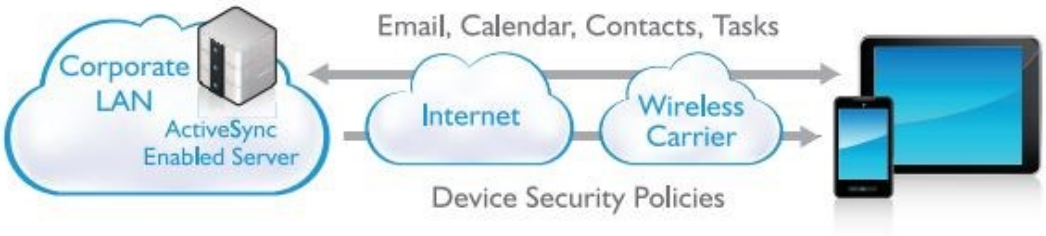
”Virtual Private Network” (VPN) är en teknik för att ansluta datorer till nätverk på distans (Technical Information about VPN: How data is protected, 2010). All information som skickas över Internet är i klartext och vem som helst kan tyda den om kommunikationen avlyssnas. Därför är det viktigt, speciellt för företag, att enbart säkra distansanslutningar till företagets nätverk tillåts. Med hjälp av VPN kan man kryptera det data som skickas över Internet och skapa en så kallad ”tunnel”, se Figur 1, mellan plats A (mobila enheten) och plats B (VPN servern).

Figur 1. Bild över VPN tunnel som skapas (Technical Information for VPN: How data is protected, 2010)

De paket som skickas krypteras först på enheten, sedan skickas de genom tunneln m.h.a. ett säkert protokoll t.ex. ”Point-To-Point Tunneling Protocol” (PPTP) eller ”Layer 2 Tunneling Protocol” (L2TP). När paketen kommer fram till servern dekrypteras dessa till läsabart innehåll igen (How VPN Works, 2003).

2.2 Exchange ActiveSync

”Exchange ActiveSync” (EAS) är ett system som är skapats av Microsoft (Understanding the role of Exchange ActiveSync in Mobile Device Management, 2014). Med EAS kan man synkronisera sin kalender, e-post samt sina kontaktuppgifter. För att använda EAS måste man ha en Exchange- server som kan skicka ut och synkronisera alla dessa med klienter som har ActiveSync aktiverat, se Figur 2. Genom EAS kan man även skicka ut olika säkerhetspolicyn till mobila enheter, och dessa tas sedan i bruk via klienten. I början gick det bara att använda EAS på Microsofts egna operativsystem, men i dagens läge stöder de största mobila operativsystemen EAS så som iOS och Android.



Figur 2. EAS anslutning över Internet (Understanding the role of Exchange ActiveSync in Mobile Device Management, 2014)

Ett problem med EAS är att om man tar i bruk det på en Exchange- server och låter användare kontakta sin e-post med mobila enheter, kan användaren ansluta med flera olika enheter och det finns inget sätt för en administratör att veta vilka alla enheter som har anslutit till en viss e-post låda. Om en enhet blir stulen med uppsatt EAS anslutning är det en säkerhetsrisk om inte administratörerna vet om detta. På grund av dessa och andra behov blir ”Mobile Device Management” (MDM) system implementerade i företag för att stöda EAS.

2.3 Mobile Device Management

MDM är ett system för att administrera mobila enheter i ett företag (Madden, 2014). Detta är inte ett speciellt varumärke utan ett gemensamt namn för sådana system, och det finns många olika företag som erbjuder dessa tjänster. För att använda sig av ett MDM-system behövs tre olika delar:

- Mobila enheter som är möjliga att administreras.
- Ett protokoll som används för administreringen på distans.
- En server eller tjänst var man kan konfigurera olika policyn och skicka dessa ut till alla maskiner.

Med ett MDM-system är det enklare för IT- avdelningen på ett företag att konfigurera och administrera alla mobila enheter. Man kan t.ex. kryptera data, ställa in Wi-Fi- och VPN-profiler eller ställa in företags e-post. Man kan även få reda på mobila enheters serienummer, vilka program som är installerade och hur mycket utrymme som finns kvar. Det är viktigt att man med ett MDM-system kan administrera mobila enheter på distans eftersom de sällan är på kontoret. Det kan hända att det är tillräckligt att ställa in alla säkerhetskonfigurationer när man tar i bruk appararaten, men det finns situationer när man inte manuellt har möjlighet att göra ändringar. Ett exempel är att en enhet blivit stulen och man måste som IT-administrator få den tömd, detta är bara möjligt att göra på distans.

2.3.1 Mobile Application Management

”Mobile Application Management” (MAM) kan tolkas som nästa steg från ett MDM-system (Madden, 2014). Med ett MAM-system kan man administrera ungefär samma saker (kryptering, lösenord, hur en anslutning görs) men detta gör man på programnivå. Som administrator kan man ställa in manuellt på enheten företagets policyn för program, eller så kan man göra detta på distans. Med hjälp av MAM kan man på ett enkelt sätt kontrollera vilka program som kan kontakta varandra och på så sätt begränsa att viktig information hamnar in i fel program.

De som erbjuder MAM-tjänster åt företag har ofta byggt upp egna program för webbläsning, e-post och fildelning. Dessa är säkra och synkroniserade så att de fungerar bra med varandra.

2.4 BYOD

BYOD är termen som används för mobila enheter som används i företag som ägs av användaren (Madden, 2014). I NIB får alla som är permanent anställda en smarttelefon, men det finns många som vill använda sig av sina egna pekplattor. Tekniskt sett fungerar alla dessa MDM- och MAM-system för mobila enheter, och skillnaden mellan personliga och företagsägda enheter är från den synvinkeln den samma. Problem som uppstår med BYOD inom företag är att användaren kan tro att företaget har tillgång till den privata delen av enheten. Detta kan till viss mån vara sant, beroende på hur företaget ställt upp sin BYOD-policy i MDM systemet. Ett annat problem som uppstår från användarens sida är att företag ofta vill ha i bruk komplexa låskoder och andra säkerhetsåtgärder, vilka tas i bruk på den personliga enheten om man tar i bruk företagets programvara och policyn.

En positiv aspekt med ett BYOD-program i företaget, om användaren kan använda egna enheter för arbete, är att användaren bryr sig mera om enheten. Om man erbjuder enheter åt användarna kan de tänka på det sättet att de enkelt får en ny om den gamla skulle förvinna eller bli stulen.

3 SÄKERHETSARKITEKTURER

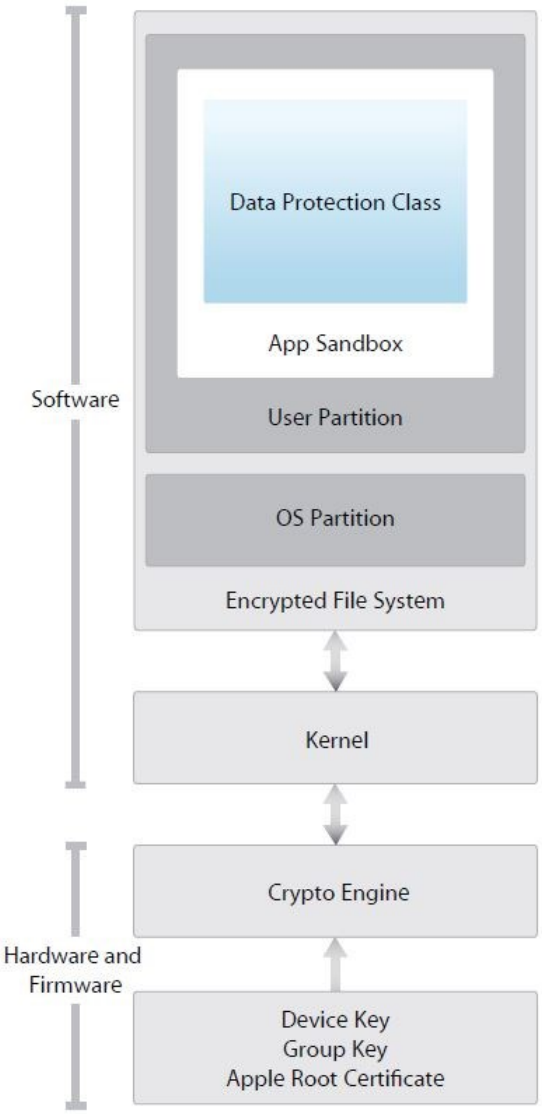
I det här kapitlet kommer säkerhetsarkitekturen av tre olika mobila operativsystem att presenteras, dvs. Apple iOS, Windows Phone 8.1 och Android. Syftet är att ge en överblick för företag över hur konfidentiell information skyddas i olika mobila operativsystem samt vilka möjligheter som finns för dessa ändamål.

3.1 Apple iOS

Apple har utvecklat sitt mobila operativsystem med säkerheten som en viktig del. Redan från hårdvarunivån är enheterna skyddade och detta fortsätter ända till mjukvarunivån. Apple använder sig av assymetrisk kryptering, säkerhetsnycklar (privata och publika) samt extra säkerhetshårdvara såsom fingeravtrycksläsare. I detta avsnitt behandlas data-säkerhet i iOS fr.o.m. version 7 och framåt.

3.1.1 Hårdvarusäkerhet

Apples olika mobila enheter (iPhone, iPad, iPod) är alla uppbyggda så att säkerheten tas redan i beaktande när man startar upp maskinen, se Figur 3 för säkerhetsarkitekturen i operativsystemet. Figuren visar vilket som sköts på hårdvaru- och vilket som sköts på mjukvarunivå. Mjukvarunivån är krypterad och här finns en del för operativsystemet och för användarinformationen. All användarinformation för olika program sätts innanför ett ramverk (”App Sandbox”) och skyddas även vidare med dataskyddsklasser. När man startar en Apple-enhet körs det kod från maskinens BootROM, vilket är endast ett läsbart minne som finns inbyggt i alla enheter. Inne i denna kod finns publika nyckeln för Apples rotcertifikatutfärdare (”Certificate Authority”, CA) med vilken det verifieras att ”Low-Level Bootloader” (LLB) är signerad av Apple och får köras. Detta minne läggs till i varje maskin när de skapas i fabriken och är mycket pålitligt. Om något går fel, eller inte kan verifieras vid uppstart, måste maskinen kopplas upp till en maskin med iTunes för att kunna ställa in fabriksinställningar.



Figur 3. Säkerhetsarkitektur i iOS (iOS security, 2014)

Nyare Apple-enheter har en A7 processor som har inbyggt i sig en skild processor som sköter om säkerhet (”Crypto Engine” i Figur 3), så att inte applikationsprocessorn behöver göra detta. Alla dessa har ett unikt ”Unique Identification Number” (UID) som de får redan från fabriken. Denna processor använder bara minne som den själv krypterat tillsammans med sitt UID, och all data som den sparar är också krypterat. I de nyare enheterna som Apple har använder de sig av fingeravtrycksautentisering, kallad Touch ID, för att göra användarautentiseringen säkrare. När en användare använder sig av Touch ID skickas datat om fingeravtrycket direkt till A7 processorn. Denna skickar sedan iväg informationen om fingeravtrycket till säkerhetsprocessorn för autentisering. Data som skickas är krypterat och kan bara öppnas genom att använda en gemensam nyckel som

bara säkerhetsprocessorn och Touch ID sensorn har. Med Touch ID kan företag göra det enklare för användare att logga in eftersom de inte behöver ange en lång och komplicerad låskod varje gång som de öppnar telefonen. Men för att Touch ID skall kunna användas i en iOS-enhet krävs det att man även har en låskod. Det finns situationer när man måste sätta in sin låskod, här följer några exempel:

- Om enheten har blivit omstartad.
- Om telefonen inte låsts upp under 48 timmar.
- Efter att man misslyckats låsa upp med fingeravtryck 5 gånger.
- När man ändrar vilket finger som låser upp.
- Om man på distans har skickat ett låskommando.

3.1.2 Dataskydd

Med dagens mobila enheter är det viktigt att de fungerar så snabbt som möjligt och att de använder sitt batteri så effektivt som möjligt. För att lösa detta har varje Apple maskin en ”Advanced Encryption Standard” (AES) kryptomotor, som är inbyggd i ”Direct Memory Access” (DMA) rutten mellan flashminnet och systemminnet. Dessa kryptomotorer använder sig av 256- bitars nycklar för att kryptera data.

Apple använder sig också av extra dataskydd för filerna som finns sparade på maskinen. Efter iOS 7 uppdateringen använder så gott som all mjukvara på telefonen sig av detta dataskydd. Varje gång som en fil skapas på flashminnet skapas det en ny 256- bitars nyckel som sedan ges åt AES motorn, vilken krypterar filen med den nyckeln som är given. Om man tar i bruk en låskod på maskinen aktiveras detta dataskydd automatiskt. Låskoden kan man konfigurera så att om det matas in fel kod ett visst antal gånger töms hela telefonen, hur många gånger det krävs kan man ställa in i sin EAS eller MDM policy.

Alla filer som skapas indelas även i olika dataskyddsklasser och beroende på klassen får filen en nyckel med vilken systemet vet när denna fil kan användas. Dessa klassnycklar sparas i maskinens metadata. Metadata i Apples maskiner skyddas genom att det vid

installation skapas ett slumpmässigt tal som sedan används för att kryptera det metadata som sparas. De olika klasserna som en fil kan höra till är:

- ”NSFileProtectionComplete”.
- ”NSFileProtectionCompleteUnlessOpen”.
- ”NSFileProtectionCompleteUntilFirstUserAuthentication”.
- ”NSFileProtectionNone”.

Om filen får klassnyckeln ”NSFileProtectionComplete” betyder det att nyckeln förstörs varje gång som den mobila enheten låser sig, vilket sedan betyder att filen är oläsbar ända tills maskinen låses upp och en ny nyckel skapas. Den andra klassen, ”NSFileProtectionCompleteUnlessOpen” används på sådana filer som kan behöva användas fastän maskinen är i lås, som exempel kan vara att om någonting skall laddas ner i bakgrunden. ”NSFileProtectionCompleteUntilFirstUserAuthentication” har samma funktionalitet som den första klassen, förutom att nyckeln som skapas förstörs inte när maskinen låser sig. ”NSFileProtectionNone” betyder att filer som ligger inom denna klass bara är skyddade med säkerhetsprocessorns UID. All information på en iOS-enhet är krypterad, även om någon fil inte hör till en speciell dataskyddsklass. Filer får sin dataskyddsklass när de skapas och det är programmet som skapar dem som lägger in de i klassen.

3.1.3 Programsäkerhet

Programsäkerheten är mycket viktig för Apple. Företaget vill se till att inget skadligt laddas upp i deras programbutik och att allting är verifierat. Alla program jobbar inom sitt eget ramverk på enheten och kan inte direkt kontakta eller få information av ett annat program, förutom via speciella ”Application Programming Interface”(API) som erbjuds och är verifierade av Apple.

All programvara som skapas för iOS måste verifieras och signeras av ett Apple certifikat. Detta certifikat finns för att man säkert vet att det är en officiell produkt och att den inte är skadlig för enheten eller operativsystemet. Om man vill börja skriva program för Apple maskiner måste man, eller företaget, registrera sig som en Apple utvecklare. På detta sätt ser Apple till att all programvara på marknaden kan länkas till någon viss per-

son och att all programvara uppnår till Apples standarder. Företag kan även ansöka om lov att skapa programvara som bara används inom företaget och sedan distribuera det åt sina användare. För att höja säkerheten bland programvara tillåter inte Apple att användare kan fritt ladda ner vad som helst.

Som tidigare nämnt stängs alla program på en Apple-enhet i sitt eget ramverk och för att kunna kontakta, eller hämta information, från ett annat program krävs att man använder APIn gjorda för dessa ändamål. Detta gäller speciellt tredje parts programvara som skapas och laddas ner på enheter. Apple erbjuder en stor del olika tjänster och APIn för att göra det enklare för utvecklare att skapa speciella program. Det viktiga är bara att man måste använda sig av en API som är verifierad av Apple. Dessa ser även till att inte programvara själv försöker höja sina rättigheter för att möjligtvis skada enheten.

Apple har också ett licensprogram för olika tillbehör. Detta betyder att om man vill skapa och sälja tillbehör borde man kontakta Apple och komma med i detta program. Det finns tillbehör som inte är med i detta program, men varje gång man kopplar ett sådant tillbehör till enheten meddelar den att den inte är verifierad av Apple.

Liksom alla andra aktuella operativsystem kommer Apple ut med uppdateringar för att fixa säkerhetshål. Dessa uppdateringar kan en användare installera genom att koppla enheten till en dator med iTunes eller till ett trådlöst lokalnät. Det rekommenderas i båda fallen att enheten är ansluten till elnätet eftersom att uppdateringarna kan vara stora.

3.1.4 Nätverkssäkerhet

Apple använder sig av standardiserade nätverksprotokoll för att hålla förbindelser autentiserade och krypterade när man kontaktar olika nätverk. På iOS behövs inte heller någon skild brandmur eftersom operativsystemet begränsar redan från början de portar som används för avlyssning och Apple har även tagit bort onödiga nätverkstillämpningar som exempelvis Telnet. Apple använder sig av ”Secure Socket Layer” (SSL) och ”Transport Layer Security” (TLS) för att skapa säkra och krypterade anslutningar till

olika nätverkstjänster. För utvecklare finns det olika APIn som kan användas för att implementera säker kommunikation i programvara.

Apple iOS stöder de vanligaste Wi-Fi protokoll så som ”Wi-Fi Protected Access” (WPA, WPA2-Enterprise) kryptering för att erbjuda autentiserad anslutning till trådlösa företagsnätverk. För krypteringen av WPA2-Enterprise används 128-bitars AES, vilket försäkrar att informationen är säker när den skickas eller blir mottagen över W-Fi lokalnät.

iOS-enheter stöder även de vanligaste protokoll och autentiserings metoder för VPN, och att konfigurera dessa går enkelt. Operativsystemet stöder också nätverk som använder certifikatautentisering. Med hjälp av olika policyn kan man konfigurera vilka domän som kräver en VPN-anslutning. Efter iOS 7 versionsuppdateringen kan man även via företagets MDM ställa in program som använder sig av en fördefinierad VPN-konfiguration för att kontakta interna nätverk.

”Single Sign-On”(SSO) kan användas med Apple-enheter. Detta går att använda som autentiserings metod till flera olika tjänster och användaren behöver bara logga in en gång till flere olika tjänster, t.ex. Safari (Apples webbläsare) stöder SSO. Med olika APIn kan man även bygga in SSO i tredje parts programvara. I företag kan SSO inställningar skickas till alla maskiner via MDM(iOS Security, 2014).

3.2 Windows Phone 8.1

Windows Phone 8.1 är det nyaste mobila operativsystemet som Microsoft kommit ut med. I denna uppdatering har operativsystemet blivit mera flexibelt och mera säkert än tidigare. Microsoft eftersträvar att alla deras operativsystem (för mobildatorer, bordsdatorer, pekplattor) skall påminna om varandra så att användare enklare kan byta mellan enheter och att utvecklare skall kunna skapa programvara som kan användas i samtliga operativsystem.

3.2.1 Hårdvarusäkerhet

Före uppstart av operativsystemet startas ”Unified Extensible Firmware Interface”(UEFI) hårdvaran vilken är en modernare och säkrare version av ”Basic Input-Output System” (BIOS). Med UEFI granskas hårdvarans digitala signatur varje gång som en mobil enhet startas upp. På detta sätt kommer det fram om något på denna nivå har skadats eller om någon försöker ändra på hårdvarans funktionalitet. Denna granskning fungerar samtidigt som ett stopp för olika skadliga program som kanske kan försöka köras på en enhet för att starta enheten i ett mindre säkert läge. Detta kallas Secure Boot (Säker Uppstart) och går inte att stänga av på Windows Phone 8.1 operativsystemet.

Windows Phone 8.1 använder sig på samma sätt som iOS 7 av en säkerhetsprocessor som kallas ”Trusted Platform Module” (TPM). TPM- modulen är en kryptoprocessor som huvudsakligen sköter om att skapa och skydda olika kryptografiska nycklar och hash-koder, men används även för att signera data med en privat nyckel som inte all programvara kommer åt. De nycklar som skyddas av TPM- modulen är t.ex. nycklar för kryptering med BitLocker och olika certifikat. Bitlocker sköter om full enhetskryptering i Microsoft Windows och finns till förfogande i nyare Windows operativsystem.

En viktig säkehetsförbättring i Windows Phone 8.1 är stödet för virtuella smartkort. Ett virtuellt smartkort fungerar på samma sätt som ett fysiskt inloggningskort, men kräver ingen fysisk kortläsare utan använder sig av TPM- modulen istället. Användning av virtuella smartkort leder till att man kan tillämpa 2-stegsautentisering. Samma virtuella smartkort kan användas på flera olika Windows-enheter.

3.2.2 Dataskydd

Information som lagras på en enhet är mycket viktigt att skydda för att undvika att företagshemligheter läcker ut om en enhet blir stulen. I Windows Phone 8.1 används flera olika tekniker för att skydda den information som sparas på maskinen.

Krypteringen av hårdskivan på mobila enheter använder sig av BitLocker teknologin, som även används i andra Windows operativsystem. För krypteringen används 128-

bitars AES. Krypteringsnyckeln sparas sedan i TPM- modulen så att det inte skall vara möjligt att flytta hårddisken till en annan maskin och via den öppna innehållet. Man kan med olika policyn påverka på hur krypteringen tas i bruk och implementeras. Det är på detta sätt möjligt att göra det omöjligt för en användare att ta ur bruk krypteringen vilket gör företagsdata på enheten säkrare. Dessutom kan man ställa in att hela enheten töms om en användare exempelvis anger en låskod för många gånger fel. På så vis minskar man risken att någon försöker med våld och automatiserade system låsa upp enheten och komma åt information som finns på den.

Nytt i Windows Phone 8.1 är att man nu även kan spara och installera programvara på extra minneskort. Om man installerar ett program på detta vis, finns det färdigt en krypterad del på kortet var programmet installeras. Detta görs helt och hållet automatiskt och kräver inte från användaren några åtgärder. Som systemadministrator kan man ta i bruk en policy för att blockera användningen av extra minneskort, om man ser detta som en säkerhetsrisk.

Windows Phone 8.1 är ett av de få mobila operativsystem som erbjuder stöd för ”Information Rights Management” (IRM) som standard, vilket betyder att användare kan delta i IRM-skyddade e-post diskussioner och öppna dokument på sina enheter vilka är skyddade med IRM. Om man använder sig av IRM, kan man skydda sina dokument och e-post meddelanden genom att skilt kryptera dessa och exempelvis ställa in vilka rättigheter andra användare har över dokumentet eller meddelandet. Man kan ställa in att dokumentet inte kan ändras eller printas, blockera e-post meddelanden från att bli skickade vidare eller ställa in att andra bara kan läsa dokumentet. Administratörer kan ta detta i bruk med policyinställningar i sin MDM. Detta operativsystem stöder även kryptering och signering av e-post meddelanden med ”Secure/Multipurpose Internet Mail Extensions” (S/MIME), inställningar för detta går också att ställa in på MDM-servern.

Microsoft har byggt in i sitt operativsystem olika möjligheter att skydda den information som finns på en mobil enhet om den tappas eller blir stulen. Tidigare i texten nämns det att man kan ställa in att tömma enheten om låskoden matas in fel för många gånger, men det erbjuds flera andra möjligheter att styra enheten på distans. Exempel på dessa är:

- Administratörer kan välja att på distans tömma enheten, oberoende om låskoden matas in fel eller inte.
- Om telefonen är administrerad av ett MDM-system kan man på distans ”pensionera” enheten. Detta betyder att all programvara som är konfigurerad av företaget tömms från minnet. Till dessa hör exempelvis e-post konton, VPN- och Wi-Fi inställningar.
- Man kan låsa telefonen om man vet var den finns men inte kommer åt den direkt och det finns en chans att någon utomstående kan läsa viktig information.
- Om det behövs kan man på distans nollställa låskoden.
- Man kan göra att enheten börjar ringa om en användare inte kan hitta sin enhet.

3.2.3 Programsäkerhet

När man startar upp en Windows Phone 8.1-enhet laddas alla systemfiler och all den programvara som startas automatiskt. Alla dessa granskas att de är signerade och om någon ändring märks startas inte den filen eller programvaran överhuvudtaget. Program som körs med detta operativsystem måste alla vara signerade. På så vis kan Microsoft se till att ingen skadlig kod körs och har hög klass på programvaran i sin programbutik. Speciellt företag kan till stor del minska riskerna för att användare skulle ladda ner skadlig kod till sina enheter om de bara använder sig av Microsofts officiella programvarubutik. Om företag vill skapa egna program som bara används inom företaget kan de skapa ”Line-Of-Business”(LOB) program som måste internt granskas, men för att kunna signera sina program måste företaget registrera sig med Microsoft.

Alla program som finns på en Windows Phone 8.1-enhet är instängda inom sitt eget lilla ramverk och har begränsat med rättigheter ut från detta ramverk. Olika säkerhetspolicyn kan användas för att ta i bruk och implementera ramverk. Det finns standardinställningar för varje ramverk och dessa innehåller t.ex. rättigheter till sin egen del av lagringsutrymmet. För att ändra dessa rättigheter måste det göras ändringar i programmets programkod, vilket betyder att rättigheterna inte kan ändras medan programmet körs. Olika orsaker varför detta system används är:

- Svårare att göra en skadlig attack mot programmet när det är begränsat.
- All information om vilka delar programvaran har rättigheter till finns listade i programbutiken före man laddar ner programvaran, och man måste som användare godkänna dessa.
- Alla program är isolerade och kan bara kommunicera med varandra via fördefinierade kanaler.

Fastän ett operativsystem är så säkert som möjligt, kommer det alltid att komma fram nya sätt att skada systemet. Personer som vill skada system hittar svaga punkter och använder sedan dessa för att skriva skadlig programkod. Windows Phone 8.1 använder sig av olika sätt att minska risken för skadlig programkod med ”Adress Space Layout Randomization” (ASLR) och ”Data Execution Prevention” (DEP). Med ASLR menas att systemminnet som används för programvara väljs ut slumpmässigt, vilket gör det svårare att placera in skadlig programkod på en viss plats i systemminnet för att skada programvara. Med DEP ser systemet till att det finns delar av systemminnet som det helt enkelt inte är möjligt att köra programkod på. Detta är sådant minne som bara används för att spara information på och genom att blockera kod från att köra minskas risken att någonting skadas.

För Internet finns webbläsaren Internet Explorer 11 installerad på alla Windows Phone 8.1-enheter. Webbläsaren är speciellt byggd för mobila Windows-enheter och stöder de flesta webbsidor. Utvecklarna har också sett till att de flesta extra komponenter som kan behövas finns inbyggt i webbläsaren att användarna inte behöver ladda ner och installera dessa, eftersom detta kan vara en stor risk när det finns många skadliga tilläggskomponenter. Det används också filter som säger åt användaren om någon sida är klassificerad som skadlig. Denna version av Internet Explorer stöder även kryptering med SSL.

I företag kan det vara bra att ha kontroll över vilka program som användare kan ladda ner till sina mobila enheter. I Windows Phone 8.1 stöds möjligheten att ta i bruk en policy med vilken man kan bestämma vilka program som går att ladda och vilka som inte går.

3.2.4 Nätverkssäkerhet

Allt mera information måste skickas över Internet, och företag kräver mer och mer att all kommunikation är säker. I Windows Phone 8.1 finns det stöd för många olika VPN tekniker, men om man vill använda sig av SSL VPN måste behövlig programvara laddas ner.

Fastän mobila nätverk blir allt snabbare kommer användare att i framtiden använda sig mera av trådlösa lokalnät (Wi-Fi), eftersom mängden data som skickas ständigt ökar och Wi-Fi erbjuder ständigt bättre överföringshastigheter än de mobila nätverken. För kryptering av Wi-Fi kommunikation används WPA, WPA2-Enterprise och ”Wired Equivalent Privacy” (WEP). Efter uppdateringen till Windows Phone 8.1 stöder operativsystemet även ”Extensible Authentication Protocol-TLS” (EAP-TLS) och ”EAP-Tunneled Transport Layer Security” (EAP-TTLS) tillsammans med WPA2-Enterprise. För användning av EAP-TLS måste det finnas ett certifikat installerat på enheten. Detta certifikat används för att försäkra sig över att det är en pålitlig enhet och är oftast utgiven av företagets CA, och på detta sätt kan man även försäkra sig över att det är en av företagets enheter. Om man använder sig av EAP-TTLS autentiserar sig användaren för en autentiseringsserver med användarnamn och lösenord, medan servern autentiserar sig för enheten med t.ex. ett certifikat. Om företaget använder sig av ett MDM-system kan man med hjälp av systemet distribuera certifikatet till de enheter som administreras. Förutom detta kan man:

- Distribuera Wi-Fi konfigureringsprofiler, innehållande namn och lösenord.
- Man kan stoppa enheter från att dela med sig sin anslutning till Internet.
- Göra det omöjligt för användare att ansluta enheten till opålitliga Wi-Fi nätverk och spara nya profiler(Windows Phone 8.1 Security Overview, 2014).

3.3 Android

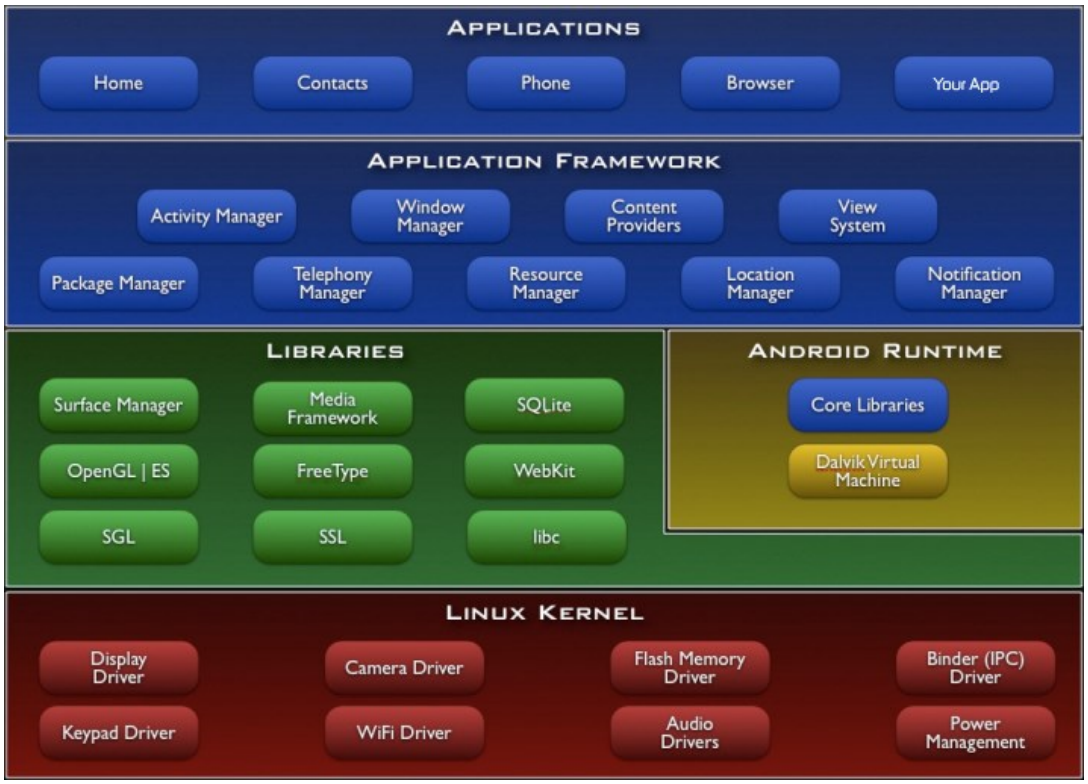
Android är ett mobilt operativsystem som är utvecklat av Google. Till skillnad från iOS och Windows Phone 8.1 är meningen med Android att det skall vara öppet för utvecklare och användare. Detta betyder att säkerheten är utvecklad på flera olika nivåer för att

upprätthålla säkerheten . Eftersom användare har hög kontroll över programvara förväntas det att skadliga program skall infinna sig på Android-enheter men operativsystemet är planerat på ett sådant sätt att möjligast lite skada kan uppstå i fall dett händer.

3.3.1 Hårdvarusäkerhet

Operativsystemet Android är uppbyggt på en Linux-kärna. Linux-kärnan har använts en lång tid och används i många olika, säkra omgivningar runtom i världen. Kärnan har testats med olika attacker och blivit fixad många gånger och är 2014/2015 mycket stabil och pålitlig. Se Figur 4 för operativsystemets uppbyggnad i Android. Säkerhetsexperter i olika företag litar på grund av detta på kärnan och bygger upp sin omgivning runtom den. För Android erbjuder Linux-kärnan olika säkerhetsfaktorer:

- En användarmodell för rättigheter.
- Isolering av olika processer som körs.
- Mångfattande stöd för ”Inter-Process Communication” (IPC).
- Möjligheten att inte använda onödiga och potentiellt skadliga delar av kärnan.



Figur 4. Android operativsystemets uppbyggnad (Android Architecture – The Key Concepts of Android OS, 2012)

3.3.2 Dataskydd

Android stöder hela filsystemets kryptering. Detta betyder att all användarinformation som finns på mobila enheter krypteras på kärnan med en 128-bitars AES-nyckel. Denna nyckel skapas och skyddas av låskoden som sätts upp på enheten när man startar den. Nyckeln är den samma ända tills man nästa gång återställer enheten till fabriksinställningar då det skapas en ny krypteringsnyckel.

Som standardinställning på mobila Android-enheter körs bara kärnan och en del inbyggda program med roträttigheter. Detta betyder att dessa har rätt till all information som finns på enheten. Det är viktigt att det finns roträttigheter för utvecklare, för att operativsystemet skall vara öppet. Det är möjligt att installera ett helt nytt operativsystem på Android-enheter med fulla roträttigheter, men som säkerhetsåtgärd för hemlig användardata, krävs det att hela enhetens lagrade användardata blir raderat vid installation. Om någon kommer åt roträttigheter via säkerhetshål, exempelvis i kärnan, kommer man åt all krypterat data som finns på enheten. Att rotanvändare kommer åt all information på enheten, kan man blockera genom att ta i bruk en krypteringsnyckel som man sparar externt, exempelvis på en server. Eftersom nyckeln inte ligger på enheten kan man skydda hemlig information, men om ägaren av enheten behöver komma åt informationen behövs krypteringsnyckeln för att öppna informationen och då kommer rotanvändare åt det.

Android stöder Exchange ActiveSync för att administrera säkerheten på enheter. Med EAS kan man exempelvis skicka ut policyn för komplexiteten på låskoder för att bättre skydda sin information från utomstående. Via EAS kan administratörer även tömma innehållet från borttappade eller stulna enheter.

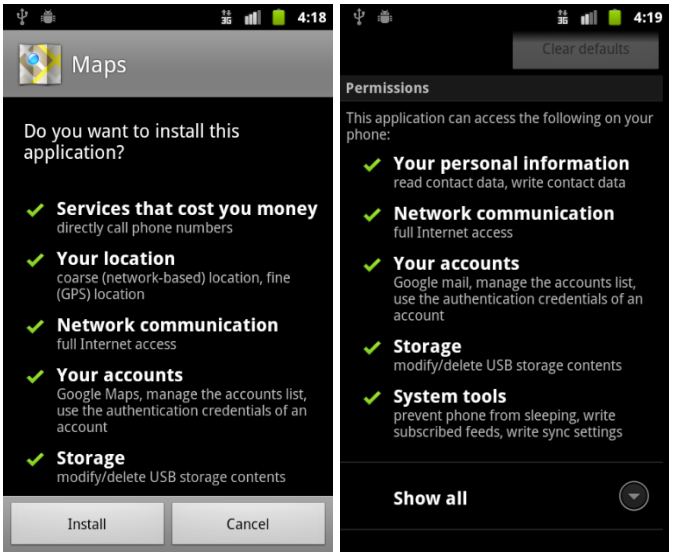
3.3.3 Programsäkerhet

Programsäkerheten i Android grundar sig på en Linux baserad säkerhetsarkitektur och isolerar sin programvara på lite annat sätt än andra operativsystem. I Android får all programvara en egen unik ID och alla program körs i en skild process med specifika rättigheter för detta ID. På detta sätt byggs det upp ett ramverk för varje program, som är skyddat på kärn-nivå. Som standardinställning har inte ett program rättigheter att

komma åt ett annat programs data och information. Eftersom allt detta sköts redan på kärn-nivå är även nativ programkod och operativsystemets inbyggda program skyddade. Med detta skydd kan man begränsa skada som kan uppstå med minneskorruption. Om en del av minnet blir korrupterat eller skadat, begränsas det bara till det program som det från första början träffat.

Utveckling av programvara i Android skall vara möjligast öppen. För att inte vad som helst skall komma in i Googles programbutik, krävs det att all programvara som laddas upp är signerade av registrerade utvecklare. Om ett program inte är signerat stoppas det från att installeras redan i programbutiken eller alternativt blockerar Android-enheten installationen. Med signering får även användaren reda på vem som skapat programmet och utvecklare kan enklare uppdatera fel i programvara som redan laddats upp i programbutiken. Med signerad programvara har Google en större chans att hitta den ansvariga om programmet gör något olagligt eller skadligt. Som tidigare nämnt får alla program ett unikt ID, och när ett program blir signerat av Google skrivs den unika IDn in i programmets certifikat. Från och med Android 4.2, kan en användare välja att använda sig av programverifiering vilket innebär att programmet verifieras före installation. På detta sätt kan användaren få veta om programvaran har identifierats som skadligt före programmet hinner skada den personliga enheten.

Om ett program behöver tillgång till något av de inbyggda system som finns i mobila Android-enheter (kamera, position, telefon) måste detta definieras i en konfigurationsfil, AndroidManifest.xml. När man installerar ett program på en Android enhet kommer det upp en förfrågan med en lista på vad som programmet måste komma åt, se Figur 5 för exempel på förfrågan. Användaren måste sedan godkänna dessa före man kan fortsätta att installera programmet. I detta skede måste man godkänna allt, och man kan inte definiera skillt sådant som man godkänner och sådant som man inte godkänner. Efter att man en gång godkänt vad programmet skall komma åt och programmet installerats visas inte förfrågan för användaren flere gånger. Om programmet avinstalleras försvinner även rättigheterna. Det finns inställningar som man kan stänga av globalt (position, Wi-Fi) och om något av dessa är globalt stängda kommer inga program åt dem. I Android har man valt att inte fråga användaren om dessa rättigheter varje gång ett program öppnas eftersom det lätt leder till att användaren sedan bara godkänner vad som helst.



Figur 5. Exempel på förfrågningar när man installerar program i Android (Android Security Overview, 2014)

Uppdateringar kommer ut till Android-enheter regelbundet. Det skickas ut både säkerhetsuppdateringar och ny programvara till alla mobila enheter. Dessa uppdateringar kan skickas ut genast till alla enheter eller så kan de komma upp någonstans packade, varifrån användare sedan själva kan gå och ladda ner dem. På Google finns det en skild grupp av anställda personer som jobbar med att fixa säkerhetshål. Dessa följer med på diskussionsforum och nyheter efter problem med Android och ser sedan till att de blir fixade så snabbt som möjligt. Vem som helst kan anmäla åt dem om brister i säkerheten genom att skicka ett e-post meddelande till adressen security@android.com (Android Security Overview, 2014).

3.3.4 Nätverkssäkerhet

Operativsystemet Android stöder de vanligaste Wi-Fi krypteringsmetoder så som WPA och WPA2-Enterprise. För användning av WPA2-Enterprise krävs certifikatautentisering för att verifiera användare som ansluter sig till säkra WPA2-Enterprise trådlösa lokalnät och detta kan vara ett problem att konfiguera på Android-enheter. Android gör det svårt för användare att komma åt vissa säkerhetsinställningar vilket menar att det kan uppstå problem vid installering och konfigurering av CA certifikat på enheter, det finns även risken att inte användare har tid eller orkar konfigurera dessa manuellt. För att göra detta enklare så finns det tjänster som erbjuder programvara för att göra installationer av certifikat automatiskt(WPA2 for Android, 2014).

Operativsystemet har inbyggt stöd för VPN, men operatörer väljer om de vill inkludera detta eller inte. Om det finns en VPN klient på den mobila enheten kan man via den sätta upp en säker anslutning till en VPN server som ligger exempelvis i företagets interna nätverk. I fall operatören som skapat enheten har valt att inte inkludera stödet för VPN, kan genom att ladda ner och skapa ”Secure Shell”(SSH)- tunnlar till SSH- servrar istället. Problemet med detta är att det kräver roträttigheter, vilket inte är passande från ett företags synvinkel(How to secure your Android Wi-Fi, 2012).

3.4 Sammanfattning

De tre största mobila operativsystemen som har presenterats i detta kapitel är delvist olika uppbyggda och tar säkerheten i beaktande på olika sätt. Apple iOS och Windows Phone 8.1 strävar efter att försäkra sig att all information är skyddad från början medan Android strävar efter att ha ett öppet mobilt operativsystem men samtidigt skydda den information som sparas på mobila enheter. Tabell 1 nedan sammanfattar och jämför diverse egenskaper i dessa mobila operativsystem.

Tabell 1. En jämförelse mellan de presenterade operativsystemen.

	Apple iOS	**Windows Phone 8.1**	**Android**
Kryptoprocessor	X (A7)	X (TPM)	
Fingeravtrycks sensor	X		
Stöd för EAS	X	X	X
AES kryptering	256-bitars	128-bitars	128-bitars
MDM- administrering	X	X	X
Dataskyddsklasser	X		
Programramverk	X	X	Med unika ID och programrättigheter
Fri nedladdning av programvara			X

SSL/TLS kryptering	X	X (med nya Internet Explorer 11)	X
WPA2 kryptering för Wi-Fi	X	X	X
VPN stöd	X	X (SSL-VPN behöver tilläggsprogram)	X
Certifikat autentisering	X	X	X
Stöd för SSO	X		
Stöd för virtuella smartkort		X	
Delvis tömning	Med MDM	X	Med MDM
Granskar signering av hårdvara vid uppstart	X	X	
Programbutik	X	X	X
ASLR	X	X	
DEP		X	
Rotmöjligheter	”Jailbreak”		X

4 TJÄNSTER FÖR DISTANSANSLUTNINGAR OCH ADMINISTRERING AV MOBILA ENHETER

Detta kapitel kommer att behandla tre stora företag som erbjuder tjänster som uppdragsgivaren söker. Dessa företag erbjuder allting från MDM- och MAM-tjänster till olika sorts fungerande BYOD-system som stöder de flesta mobila operativsystem som idag finns tillgängliga på marknaden. Avancerad filhantering och säkra sätt att ansluta till interna nätverk hör även till företagens tjänster. De företag och tjänster som kommer att behandlas i kapitlet är: VMware Airwatch (Airwatch Solutions, 2014), Citrix XenMobile (Citrix XenMobile Technology Overview, 2014) och Good Technology (Secure Mobility Solutions, 2014). Dessa tjänster är valda för att de hör till de ledande tjänsterna

inom MDM- system enligt Gartners Magic Quadrant. (Mobile Device Management Gartner Magic Quadrant 2014, 2014)

4.1 VMware Airwatch

Airwatch är en tjänst som erbjuds av företaget VMware. Denna tjänst erbjuder många olika komponenter för att kunna hantera de företags- och privatägda mobila enheter i företag. Till följande presenteras de olika delar som tjänsten har att erbjuda.

4.1.1 BYOD

Airwatch har fullt stöd för en BYOD omgivning (Airwatch Solutions, 2014). Man kan på ett simpelt sätt hantera alla mobila enheter som finns i ett företagsnätverk, både företags- och privatägda. Efter att man definierat olika grupper för enheter som skall hanteras kan man skapa och distribuera olika profiler, säkerhetspolicyn och programvara gruppvis. Som administrator kan man definiera vilka enheter och operativsystem som stöds i omgivningen. Efter att en användare har autentiserats blir profiler, programvara och innehåll automatiskt konfigurerade enligt vilken användare det är och vilken enhet som blir inskriven i systemet. Med hjälp av profiler kan man ställa in färdiga VPN anslutningar till interna företagsnätverk så att de blir säkra också med privatägda enheter. Användare har även möjlighet att själv registrera nya enheter i omgivningen via en konsol som tjänsten innehåller.

Airwatch uppdelar allt information som finns på enheten i två delar, företags- och privatinformation, och på detta sätt så begränsas åtkomst till företagets hemliga information som finns på enheten. Man kan hantera privata enheter på samma sätt som företagsägda enheter, men det går att konfigurera sin omgivning så att ett företag inte kommer åt personlig information och att man exempelvis inte kan tömma hela enheten på distans. Man kan även som administrator ta i bruk ”Terms Of Use” (TOU) för att informera användaren vad som företaget kommer åt ifall enheten registreras i ett företagsnätverk. Om någon slutar på företaget så kan man på distans tömma de mobila enheter som användaren haft i sitt bruk och på så sätt att bara företagsinformation försvinner, detta betyder att all den personliga informationen blir kvar på enheten.

4.1.2 Airwatch Workspace Management

Airwatch Workspace Management är en tjänst för att separera företags- från privatinformation på mobila enheter (Airwatch Solutions, 2014). Detta hjälper även med privata enheter för att all företagsprogramvara stängs in i ett eget ramverk, vilket gör det möjligt att bara hantera den delen av enheten separat t.ex. tömma företagsinformationen på distans, se Figur 6. Allting som ligger inom detta ramverk så är krypterat och det är möjligt att begränsa användare från att kopiera filer ut ur ramverket. Detta ramverk kan en administrator konfigurera så att det väsentliga som behövs finns till förfogande. Företagsprogram som finns inom ramverket syns på enheten som helt vanlig programvara, för att göra användningen så enkel som möjligt för användaren. Airwatch Workspace Management stöder SSO-autentisering och en användare kan inte öppna programvara före han/hon har autentiserat sig i systemet. Inom detta ramverk ligger även all programvara som kommer med tjänsten så som e-post klient, säker filhantering och webbläsare. Dessa presenteras noggrannare senare i texten.

Figur 6. Airwatch Workspace fungerar inom ett eget ramverk på enheten(Airwatch Solutions, 2014)

4.1.3 Airwatch MDM

VMware Airwatch erbjuder även ett fullständigt MDM- system för att hantera alla de mobila enheter som kommer åt det interna nätverket i ett företag (Airwatch Solutions, 2014). Med detta MDM- system kan man hantera säkerheten för användare, enheter, program, information, e-post och nätverk. Man kan även kontinuerligt följa med informationen i alla enheter för att försäkra sig över att information som finns på de mo-

bila enheterna är säker. MDM- systemet stöder även BYOD möjligheten och det går att ställa in flera faktorers autentisering för att komma åt företagsinformation på enheter. Om en enhet blir borttappad eller stulen så kan man på distans låsa eller tömma den.

Man kan ställa in olika policyn för programvara som finns på den mobila enheten. Detta betyder att man kan exempelvis blockera nativprogramvara från att användas och dela på programvara i listor enligt vilka som man anser vara skadliga och vilka som är godkända av företaget. Det är även möjligt att ställa in att det automatiskt blir omöjligt att komma åt företagsinformation om en enhet blir skadad för att göra enheten säkrare. Om man vill skapa programvara internt inom företaget så kan man använda sig av Airwatch ”Software Development Kit”(SDK) och ”App Wrapping” för att integrera säkerheten inom tjänsten i sin egen programvara.
Administratörer kan även konfigurera certifikat-baserad anslutning till företagsVPN och Wi-Fi nätverk och på så sätt hindra utomstående enheter från att ansluta sig till nätverket.

Allt detta går att administrera centralt från en webbbaserad admin-konsol som tillhör tjänsten. Från denna konsol kan man på ett enkelt sätt administrera alla enheter som är inskrivna, oberoende av tillverkare eller operativsystem. Denna konsol går att integrera med företagets ”Active Directory” (AD) struktur för att göra det möjligt att exempelvis distribuera en viss programvara till en viss grupp med användare. Via denna konsol kan man rigistrera nya enheter i systemet, och som tidigare nämnts kan användare även göra detta. Om en användare registrerar en ny enhet blir den automatiskt konfigurerad enligt användarens inställningar i systemet. Konsolen gör det även möjligt att på distans göra ändringar i profiler (lösenord, e-post, VPN) utan att det stör användaren. Dessa ändringar kan även delas ut åt bara vissa grupper eller typer av enheter. Här kan administratörer också göra ändringar i TOU, och följa med vilka användare som godkänt dessa och vilka som inte gjort det. Det är möjligt för en administrator att skicka olika kommandon till enheter via denna konsol. Man kan t.ex skicka kommandon för att: ta bort låskod, låsa enhet, hitta enhet eller tömma enhet. Hur konsolen ser ut och vilka egenskaper som visas går att ställas in av användaren.

Här erbjuds även en hel del olika rapporter som går att användas för att följa upp vilka enheter som är registrerade och vad de har installerat i omgivningen. Det är även möjligt att skapa egna rapporter.

4.1.4 Airwatch MAM

Airwatch erbjuder ett mångsidigt MAM-systemet i sitt MDM- system för att administrera programvara som finns på mobila enheter i ett företags nätverk(Airwatch Solutions, 2014). Med detta kan man ställa in program som är godkända av företaget och erbjuda egna program som är utvecklade för något speciellt behov. Man kan hantera och distribuera köpt och gratis programvara från en konsol till alla enheter som finns inskrivna i omgivningen, fastän dessa skulle vara privatägda. Från denna konsol kan administratörer även följa upp hur en installation av en specifik programvara har gått och hur många som har lyckats få den installerad.

Airwatch använder sig av en App Catalog för att hantera program som skickas ut åt användare, se Figur 7. Denna katalog så integreras med stora företagsprogrambutiker (t.ex. Microsoft, Apple och Google) för att göra det möjligt att hantera publik programvara inom företagets system. Katalogen kan sättas innanför Airwatch ramverket på alla mobila enheter, eller som fristående programvara utanför. Användare kan sedan gå in i katalogen och se programvara som är godkända eller rekommenderade av företaget. Här kan både finnas publik och intern programvara, och det går att gruppera dessa på olika sätt enligt AD grupperna i företaget. Inom App Catalog programmet kan användare rösta och kommentera på olika program som finns i listan, här kan administratörer få viktig information som kan hjälpa med beslut om ett program skall finnas eller inte.

Figur 7. Airwatch App Catalog listar upp program som är godkända av administratörer(Airwatch Solutions, 2014)

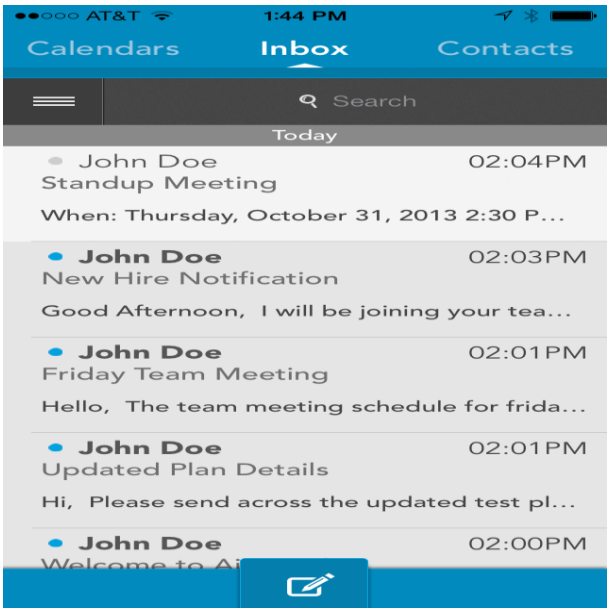
För att företag skall ha möjlighet att försäkra sig att program (speciellt från 3:e parter) är säkra att använda så erbjuder Airwatch ”App Reputation Scanning”. Med detta kan en administrator köra olika test på programvara och hitta säkerhetsrisker som osäkra nätverksanslutningar och skadlig kod. Efter att resultaten har kommit så kan man sedan göra beslut enligt dessa. Resultaten delas in enligt risknivå och riskområde. Testen går att köra direkt från administratorkonsolen och information skickas som e-post när testet är färdigt.

Som tidigare nämnt erbjuder Airwatch en SDK och ”App Wrapping”. Med den SDK som utvecklare har tillgång till i företag kan man enkelt integrera all den säkerhet som Airwatch erbjuder i den programvara som kommer med tjänsten, och dessa går enkelt att använda. Utvecklare kan lägga mera tid på programvarans funktionalitet när det enkelt går att integrera säkerheten. Dessa interna program kan man även administrera från samma konsol som man registrerar och administrerar enheter. Med ”App Wrapping” kan man lägga in existerande programvara i samma ramverk och höja på säkerheten. Detta ger också flera möjligheter att hantera programvara som redan ligger på enheten när man tar i bruk Airwatch.

4.1.5 Airwatch programvara

Airwatch stöder de nativa program som kommer med de största operativsystemen, men erbjuder även egna program som går att använda i företag.

Airwatch Inbox är en e-post klient som är säker och separerar privat- från företagsinformation. Information i Airwatch Inbox är skyddat med 256- bitars AES både när det skickas och när det ligger sparat. Programmet är enkelt att använda och man kommer åt företags e-post, kalender och sina kontaktuppgifter från ett och samma program, se Figur 8.



Figur 8. Airwatch Inbox, innehåller e-post, kalender och kontaktuppgifter (Airwatch Solutions, 2014)

Denna klient kan distribueras till enheter som ett skilt program eller inom ”Airwatch Workspace”. Användare kan autentisera sig med användarnamn och lösenord, det går även att använda sig av digitala certifikat. Airwatch Inbox erbjuder även mera säkerhet och administratörer kan ställa in vad som kommer att användas. Man kan bl.a.:

- Blockera möjligheten att kopiera information ut från Airwatch Inbox.
- Blockera användare från att skicka e-post till domäner som inte man litar på.
- Ställa in den maximala storleken på bifogade filer.

- Kräva att alla bifogade filer öppnas i Airwatch Secure Content Locker (se nästa delkapitel).
- Totalt förbjuda bifogade filer.
- Ställa in att alla länkar till externa webbsidor öppnas med den säkra webbläsaren som hör med i Airwatch paketet.

Med Airwatch Inbox kan användaren skapa möten och nya kontaktuppgifter, och dessa synkroniseras sedan med företagets e-postserver så att man kommer åt dem på alla enheter som användaren har i bruk. Man kan använda sig av SSO så att användaren kan hoppa mellan olika företagsprogram utan problem och autentisering varje gång.

Med tjänsten medföljer även en egen mobil webbläsare, Airwatch Browser. Denna webbläsare kan administratörer konfigurera enligt de behov som företaget har och allting går att ställa in via den gemensamma administratorkonsolen. En administrator kan göra listor över sidor som tolkas som skadliga och blockera användare från att besöka dessa. Via konsolen kan man distribuera olika policyn för olika inställningar. Man kan ta andra webbläsare ur bruk så att bara denna används på mobila enheter som är registrerade i systemet. Inom webbläsaren kan man ställa in interna sidor och nätverk som användaren kan komma åt. Airwatch Browser är som standard konfigurerad att använda ”Airwatch App Tunneling” genom ”Airwatch Mobile Access Gateway” för att skapa en säker anslutning till interna nätverk. ”Airwatch Mobile Access Gateway” är en gemensam väg in i säkra nätverk för alla de mobila enheter som är inskrivna i systemet. För kryptering av kommunikationen används TLS/SSL.

4.1.6 Säker fildelning med Airwatch

Till ett fullständigt Airwatch paket hör även Secure Content Locker. Detta kan användas som en central plats var användare kan spara, hitta, uppdatera och dela med sig viktiga företagsfiler från alla sina mobila enheter (Airwatch Solutions, 2014). När man använder detta i sitt företag så kan många olika avdelningar komma åt sina egna filer från vilken plats som helst och dela dessa med t.ex. potentiella kunder. Fildelning på detta vis drar även företag mot papperfria kontor vilket kan spara på kostnader. Anslutningar som blir uppsatta till Secure Content Locker använder inte traditionella VPN lösningar, utom

är uppbyggda med infrastrukturen som Airwatch erbjuder och använder sig av ”App Wrapping”, ”Airwatch App Tunnel” och går via ”Airwatch Mobile Access Gateway”. Systemet går att ta i bruk med Airwatch MDM, Airwatch Workspace eller utan dessa som ett helt fristående program.

Denna fildelning krypteras med 256-bitars AES och kräver att användaren autentiseras för att sätta upp en anslutning. För att autentisera användare kan man använda AD, Kerberos eller olika certifikatbaserade metoder. Rättigheter till filer och kataloger kan tilldelas enligt AD grupper. För att vidare skydda information som finns inom Secure Content Locker kan man ta i bruk olika policyn för att exempelvis blockera kopiering av innehåll eller möjligheten att printa ut dokument. Systemet går även att integrera med olika system som redan kanske är i bruk i företaget så som Sharepoint och nätverksenheter. VMware erbjuder även möjligheten att spara all information i molnet om inget system finns i företaget från tidigare.

Secure Content Locker kan användas som ett mobilt program. Med detta program på sina mobila enheter kan användare skapa och editera dokument för Microsoft Word, Microsoft Excel och Microsoft PowerPoint. Det går även att använda en webbbaserad portal som man kan komma åt från vilken enhet som helst bara man har en fungerande Internet-anslutning. För bords- och bärbara datorer kan man installera en skild klient, ”Airwatch Secure Content Locker Sync”, med vilken man kan synkronisera innehållet direkt till datorn. Användare kan även banda in ljud så att dessa inspelningar sparas direkt upp till Secure Content Locker, t.ex. utbildningstillfällen och möten med kunder. På samma sätt kan man göra när man tar bilder eller spelar in videofilmer, så att dessa inte sparas direkt på enheten och finns till förfogande om enheten skulle råka försvinna.

För själva fildelningen kan användare skapa länkar till sina dokument. Secure Content Locker kan skapa länkar som användaren kopierar och sedan exempelvis skickar vidare. Dessa dokument går att ytterligare skyddas av användaren genom att lägga till lösenord, giltighetstid för länken eller begränsa antalet gånger ett dokument kan laddas ner. För att dela hela kataloger kan användaren själv, om han är ägare, ge rättigheter åt andra så att de kommer åt att se eller editera dokument inom katalogen. För att göra systemet

mera socialt, kan användaren kommentera filer eller märka andra användare (en märkt användare får ett e-post meddelande om detta görs).

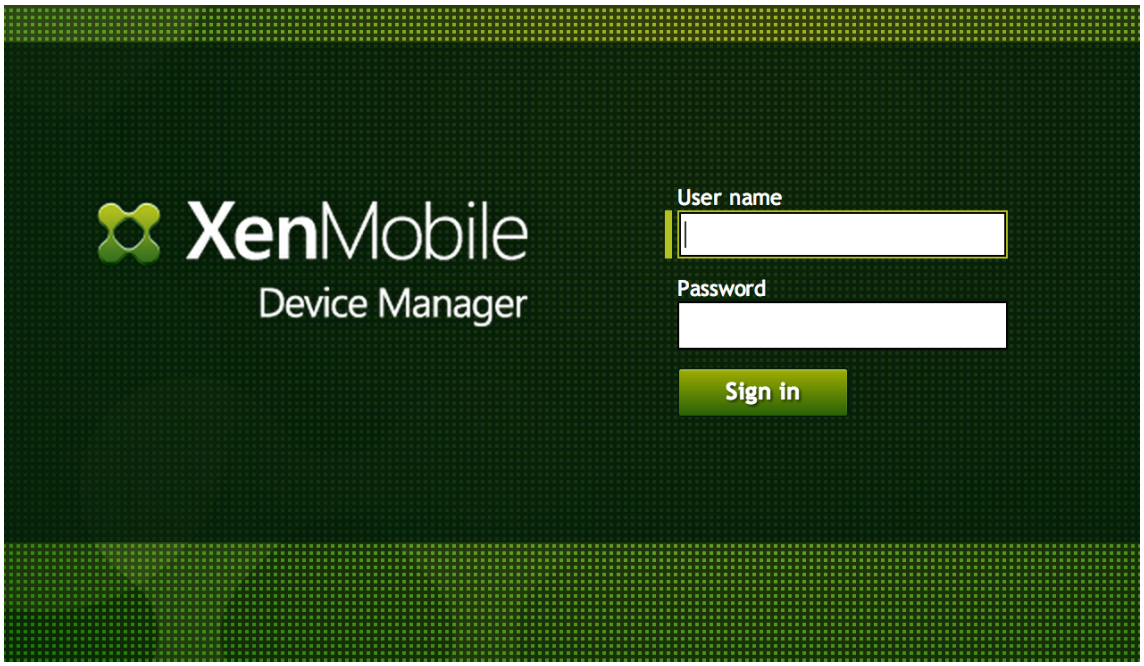
E-post trafik stöds av Secure Content Locker och systemet erbjuder hjälp för att dela filer via e-post. Om man i företaget använder Microsoft Outlook så kan man ta i bruk en tilläggsdel som installeras i programmet. Man kan använda sig av ”Hypertext Transfer Protocol”(HTTP)- länkar som läggs automatiskt till när man bifogar ett dokument för att spara på e-postserverns lagringsutrymme och underlätta skickandet av stora dokument. Dessa länkar kan man sedan skydda på samma sätt som dokumentlänkarna.

4.2 Citrix XenMobile

XenMobile är en tjänst som Citrix erbjuder för att hantera mobila enheter. Med XenMobile kan administratörer hantera stora mängder enheter från en och samma konsol, och skicka ut olika säkerhetspolicyn till alla dessa. Programvara går även att distribueras och hanteras via denna konsol. Citrix erbjuder också egen programvara som kan användas om företaget inte litar på nativa program som finns färdigt på de mobila enheterna. Tjänsten kommer att presenteras i detta kapitel.

4.2.1 XenMobile MDM och BYOD

Citrix XenMobile erbjuder ett fullständigt MDM- system åt företag (Citrix XenMobile Technology Overview, 2014). Detta system kan administratörer logga in till via en webbaserad konsol, se Figur 9. Här kan man registrera nya mobila enheter i systemet, godkänna och icke- godkänna program eller hitta enheter som inte är fullständigt säkra och blockera deras tillgång in i systemet. Användarna som finns i företaget läses in från företagets AD och integreras med MDM- systemet. Systemet blir i direkt kontakt med ADn, vilket betyder att varje gång som en ändring görs körs ett kommando mot AD katalogen. På detta sätt kan administratörer enkelt ställa in olika rättigheter och distribuera t.ex. programvara bara till en viss grupp.



Figur 9. Exempel på webbaserad inloggningsruta i XenMobile (Citrix XenMobile MDM, 2014)

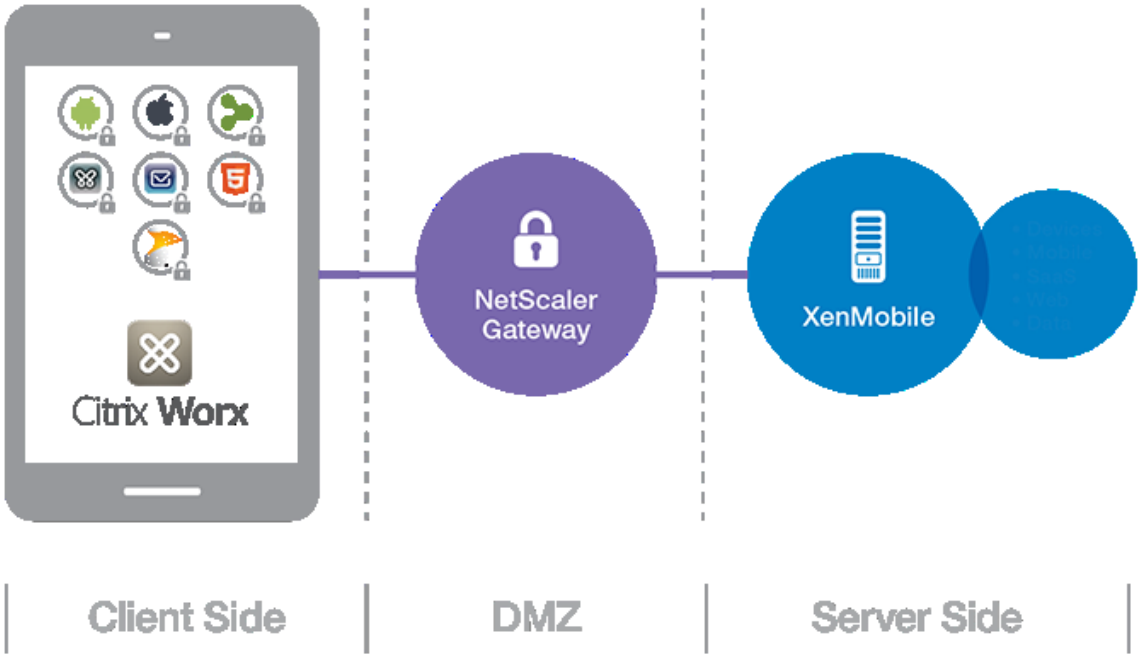
Med Citrix XenMobile kan man specificera vilka mobila enheter som kan registreras i systemet och få säkerhetspolicyn. Dessa delas upp med t.ex. vilket operativsystem som är i bruk på enheten och vilken version. Det kan finnas många policyn i bruk, och alla de olika definieras här. Man kan ställa in olika konfigurationer för olika operativsystem och ta i bruk exempelvis: Låskoder, enhetskryptering, EAS, Wi-Fi- och VPN- profiler. Här kan man även ange om den mobila enheten som registreras i systemet är företags- eller privatägda. Som administrator kan man också ge användare rättigheter att själv registrera nya enheter i systemet. Om detta görs så kan användare själva logga in i MDM-systemets konsol och göra simpla saker såsom: registrera, hitta, låsa eller tömma en enhet. Man kan även skicka åt användaren en inbjudan, via SMS eller e-post, att registrera en enhet om man inte vill att användaren skall ha tillgång att göra det flera gånger. Administratorn skickar en länk varifrån användaren kommer åt att göra detta, eller så får användaren en PIN-kod eller ett lösenord för att registrera enheter. Det går även att använda en kombination av alla dessa tre. Om en användare har en BYOD-enhet inskriven i systemet så kan en administrator göra en delvis tömning av enheten. Detta betyder att bara viktig företagsinformation och programvara tas bort, privatinformation blir kvar på den personliga enheten. När man tömmer en enhet helt och hållet så återställs enheten till fabriksinställningar och är färdig att tas i bruk på nytt om det behövs.

Med MDM- systemet kan man också följa upp enheter och kontrollera att de ännu är säkra. Det går att få fram rapporter om exempelvis vilken programvara som är installerad och om säkerheten är konfigurerad som företagspolicyn säger.

4.2.2 XenMobile Worx Home

XenMobile använder sig av ett centralt program som heter Worx Home. Detta kan laddas ner till alla mobila enheter och gör det möjligt för administratörer att hantera enheterna (Citrix XenMobile Technology Overview, 2014). Från användarens sida behövs bara att han/hon loggar in med sin e-post adress, användar- ID och lösenord. Efter detta konfigureras Worx Home automatiskt enligt användarens och företagets inställningar. Som administrator kan man konfigurera säkerhetspolicyn och inställningar som sedan distribueras till enheter som har Worx Home installerat på enheten. I detta program finns även en programbutik var företag kan lägga in vilka program som användare kan ladda ner. Program som visas här kan vara olika för användare, beroende på vilka roller de har och vilka AD-grupper de hör till. De program som användare väljer att ladda ner visas sedan i deras arbetsmiljö, som visas när man öppnar Worx Home, och man kan sedan enkelt komma åt dessa därifrån. Programmen sparas sedan i XenMobiles ”App Controller” databas, vilket betyder att om en användare tar i bruk en ny enhet kommer alla program automatiskt fram i den nya. Worx Home granskar i bakgrunden efter policyändringar och tar dessa i bruk utan att användaren lägger märke till det.

”NetScaler Gateway” fungerar mellan interna företagsnätverk och användare, se Figur 10. Denna kan administratörer enkelt hantera och här kan de begränsa åtkomsten till nätverket. ”Netscaler Gateway” fungerar m.a.o. på samma sätt som en brandmur (Citrix XenMobile Securing the mobile enterprise, 2014). Sessioner som försöker ansluta sig till nätverket kan granskas på användar- och enhetsnivå för att försäkra sig om vem och vad som försöker ansluta sig. På grund av detta så kan autentiserade användare ansluta sig varifrån som helst.



Figur 10. Hur Citrix Worx anluter till företagsdata (Citrix Xenmobile Technology Overview, 2014)

XenMobile ”App Controller” är den del av systemet som sköter om resurserna i ett företag. När ett program körs så autentiserar ”App Controller” i bakgrunden en användare genom att verifiera att användaren har rättigheter till programmet eller tjänsten. Denna stöder även SSO- autentisering vilket betyder att om användaren är autentiserad från tidigare så frågas det inte efter något lösenord eller PIN kod. För att ett program skall kunna använda sig av SSO mot ”App Controller” måste programmet konfigureras enligt en av många modeller som ”App Controller” stöder t.ex. ”Security Assertion Markup Language” (SAML), vilket använder sig av autentiseringsinformation i ”Extensible Markup Language” (XML)- format.

Som tidigare nämnt erbjuder Worx Home en programbutik. I denna visas sådan programvara som användaren kommer åt, men det kan även visas program som inte användaren har direkt rättigheter till. I sådana fall kan en användare be att få rättigheter till dessa program. När detta händer så skickas det en förfrågan till administratörerna som sedan skall ge rättigheter eller inte. Det kan krävas att flera administratörer måste godkänna före rättigheter ges åt användaren. Att konfigurera vilka vägar dessa förfrågningar går kan man med hjälp av AD och ”App Controller” göra.

Integrerat i Worx Home finns det även en portal, ”GoToAssist”, vilken fungerar som en direkt länk till servicepersonalen på företaget. Via denna kan man starta en direkt diskussion med någon som kan hjälpa, om operativsystemet stöder så kan administratörer även styra enheten på distans.

4.2.3 XenMobile MAM

Som tidigare nämnt så finns alla program och resurser sparade i ”App Controller” (Citrix XenMobile Technology Overview, 2014). Detta betyder från Citrix XenMobiles synvinkel att all information som en användare har sparat (SSO, program) följer med om man blir tvungen att byta enhet eller registrerar en ny enhet i systemet. På grund av detta kan en användare ladda ner Worx Home på sin nya enhet så att han/hon ser allt som har funnits där tidigare.

När program läggs in i Worx Home så blir de låsta till ett skilt ramverk. Med detta ramverk blir det möjligt för administratörer att hantera program och distribuera säkerhetspolicyn som berör program, även från tredje parter. För hanteringen av program och programdata använder sig ”App Controller” av teknologin ”Citrix MDX”. Med ”Citrix MDX” är all företagsinformation instängt i ett ramverk, vilket betyder att företagsprogram inte kan kommunicera med privata program och vice versa. Detta gör det möjligt att upprätthålla en BYOD miljö inne i företaget. ”Citrix MDX” teknologin gör det möjligt att på distans låsa, tömma och kryptera data med olika policyn. Man kan även ställa in att program använder sig av enskillda mikro VPN anslutningar för att göra upp en säker anslutning med interna företagsnätverk. Detta ingår automatiskt i programvara som Citrix erbjuder åt företag (mera om dessa senare). Från säkerhetssynvinkeln är detta bra eftersom man inte behöver öppna en VPN anslutning för hela enheten, utan det är programspecifikt.

Olika delar som kan användas i hantering av ett program inom Citrix XenMobile är:

- Autentisering via Worx Home om användaren är ansluten men inte har loggat in sig i systemet ännu.

- Möjligt att göra en check som granskar att om användaren har rättigheter till det programmet, och man kan även tömma all information om användaren inte har rättigheter.
- Man kan ställa in tiden hur länge en användare kan använda program utan att vara ansluten.
- Köra uppdateringar av programvara, man kan även ställa in att användare har möjlighet att ändra tiden när den körs om han/hon är upptagen.
- Man kan definiera om en mobil enhet med roträttigheter har åtkomst till systemet.
- Man kan kontrollera vad en användare kan göra från ett program, t.ex. om det är möjligt att kopiera ut information ur programmet.

Citrix XenMobile erbjuder även användare deras egna program. Citrix WorxMail och WorxWeb är två nativa program som medföljer tjänsten. Med dessa har man en fullständig klient för e-post, kalender och kontaktuppgifter samt en säker webbläsare för att göra det möjligt att kontakta interna nätverk och surfa på Internet säkert via krypterad kommunikation. Om man har i bruk ett företagscertifikat kan man dela det med dessa program via ”App Controller”. Dessa program gör det enkelt för administratörer att på distans tömma all information om en enhet vore stulen, och de är instängda inom sina egna ramverk. Citrix erbjuder WorxMail som en skyddad e-post klient, men det går även att kryptera bifogade filer i de inbyggda e-post-klienterna som kommer med de största mobila operativsystemen om företaget vill använda sig av dem. Det är också möjligt att företaget själv väljer vilka typer av filer som skall vara krypterade om inte allt behöver vara.

4.2.4 ShareFile

ShareFile är en tjänst som Citrix erbjuder tilsammans med XenMobile och gör det möjligt för företag att ha all sin information synkroniserad i ett system (Citrix XenMobile Technology Overview, 2014). Detta är ett system som går att använda både innanför och utanför företags interna nätverk. Man kan som IT-administrator integrera systemet med företagets AD, och på detta sätt enkelt tilldela rättigheter till olika delar för olika

grupper och användare. ShareFile gör det möjligt för användare att komma åt all företagsinformation var de än är och från olika enheter.

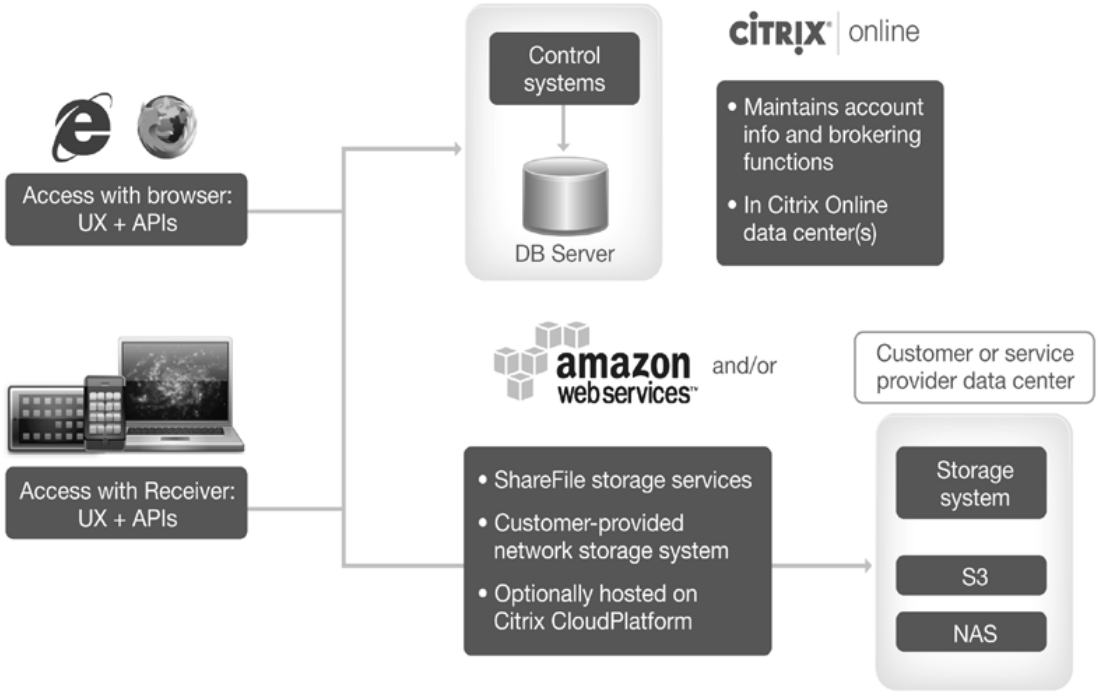
Olika delar som tjänsten ShareFile erbjuder är:

- Enkel SSO- autentisering tillsammans med Worx Home.
- Möjligheten att granska och editera dokument med olika program som finns på den mobila enheten.
- Man kan komma åt företagets Sharepoint-miljö eller nätverksenheter.
- Fullständig mobilitet med möjligheten att komma åt dokument fastän man inte har en Internet-anslutning till enheten.

Med ShareFile kan man på ett säkert sätt hantera och dela med sig information. Administratörer har möjlighet att följa med aktivitet bland användarna och på basis av detta kan man enkelt tilldela korrekta rättigheter för de användare som behöver dem. ShareFile går även att integrera med WorxMail (Citrix XenMobile Securing the mobile enterprise, 2014). Man kan som administrator ställa in en storlek på bifogade filer. Om den bifogade filen är större än vad administratorn ställt in så skickas det istället in länk till ShareFile. Det går även att ställa in att alla bifogade dokument måste vara en länk till ShareFile.

Hela tjänsten är uppdelad i två olika delar, ett kontrollsystem och ett system för lagring, se Figur 11. Kontrollsystemet används för att ha koll och hantera användarnas egna konton. All denna information är krypterad och skyddad samt ligger i ett av Citrix egna datacenter. Systemet för lagring används för att hantera och lagra all företagsinformation. ShareFile använder sig av ”StorageZones” för att dela upp informationen, och dessa kan man ha i företagets egna datacenter, i molnet eller använda sig av båda. All information är krypterat med SSL, både när den inte används eller skickas över Internet. En fördel med användning av eget datacenter är att informationshanteringshastigheten ökar när informationen ligger fysiskt nära. Eftersom man direkt kan integrera ShareFile med en färdig företagsmiljö för filer (Sharepoint, nätverksenheter) behöver man inte spendera tid på att migrera över all information till ett nytt system. Fastän ”StorageZones” kan

ligga inom företagsnätverket så ligger kontrollsystemet alltid i en av Citrix olika data-center.



Figur 11. Uppbyggnaden av en ShareFile- miljö (Citrix XenMobile Technology Overview, 2014)

ShareFile är en tjänst som företag kan skaffa skilt från XenMobile, men det är bara tillsammans med XenMobile som man kan få ett fungerande system för hantering av mobila enheter. Man kan med hjälp av XenMobile t.ex. på distans tömma all ShareFile information om en enhet blir borttappad. ShareFile går även att integrera med Worx Home så att en användare kan komma åt allting från en och samma plats.

4.3 Good Technology

I detta kapitel kommer tjänster som företaget Good Technolgy erbjuder att presenteras. Good Technology erbjuder sina kunder ett fullständigt system för att hantera mobila enheter, program och skydda information som företaget har. Företag får även tillgång till många olika program som är speciellt utvecklade av Good Technology.

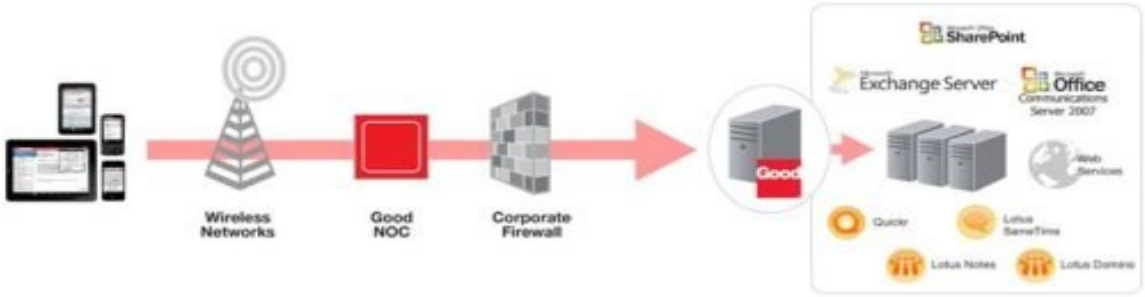
4.3.1 Good MDM

Good Technology ger företag ett fullständigt MDM- system för att hantera alla de mobila enheter som finns inom företaget (Secure Mobility Solutions, 2014). Systemet kan synkroniseras med företagets AD-uppbyggnad och man kan med detta sätta upp olika konfigurationer för olika användare. När systemet är uppbyggt och synkroniserat kan man ställa in alla konfigurationer, program och policyn som körs automatiskt på användarens enhet i systemet. Att registrera en enhet i systemet kan göras via en gemensam konsol, som administratörer och användare med speciella rättigheter kan använda. Administratörer kan ge användare speciella rättigheter att göra simpla uppgifter i omgivningen. Här kan man även tömma enheter som är försvunna, delvist bara företagsinformation eller fullständigt till fabriksinställningar. Användare med speciella rättigheter kan registrera enheter, tömma, låsa eller nollställa enheters lösenord utan hjälp från en administrator.

För administratörer erbjuder Good Technology många möjligheter att bygga upp policyn som passar just för det företaget. Man kan ställa in olika policyn för lösenordskrav, kryptering av enheter, kamera, VPN- och WiFi-konfigurationer. En administrator kan även skapa en lista över program som anses vara skadliga och förbjuda användare att ladda ner och installera dessa. Good Technology erbjuder även färdigt uppbyggda rapporter från vilka administratörer kan se i vilket skede en mobil enhet som är inskriven är. Man kan se vilka program som är installerade, lista vilka policyn som en enhet har haft och vilken version av policyn som nu är aktiv.

Good Technology erbjuder företag tjänsten med deras egen molntjänst Good Secure Cloud. Via detta kan man göra allting som behövs för att hantera mobila enheter inom företaget. Man kan integrera sin Microsoft Exchange, Microsoft Lync och många flera olika miljöer för att integrera företagsinformation i systemet. Hanteringen av allting fungerar via en webbbaserad konsol och företaget behöver inte inskaffa någon hårdvara, vilket betyder att man snabbt kan få igång ett fungerande system. Om företaget vill att allting skall fungera inom deras egen miljö är detta även möjligt. Man kan använda sig av Good Dynamics Direct Connect, som är en konfiguration vilken gör det möjligt för hanterade mobila enheter att direkt komma åt information inom företagets nätverk.

Detta fungerar genom att ställa in en server som förmedlar enheternas anslutning till rätta platser i nätverket. Good Technology erbjuder även en Good Proxy server, se Figur 12, som man får tillgång till med tjänsten. Genom att bygga upp systemet på plats kan man minska på väntetiden och få anslutningar att koppla upp snabbare.



Figur 12. Tillgång till interna nätverk från mobila enheter via en Good Proxy server (Good Technology, 2014)

4.3.2 Good MAM

I Good Technology's tjänst ingår även en programbutik vilken alla enheter som är inskrivna i systemt kommer åt (Secure Mobility Solutions, 2014). Här ser alla användare en lista på program som kan vara kommersiella eller utvecklade av företaget. Med denna butik kan administratörer enkelt ge användare tillgång till program som företaget vill att de skall använda sig av. Det går att ställa in att användare får påminnelser om viktiga uppdateringar som kommer åt program som finns i butiken. Med hjälp av denna programbutik kan företag också tilldela åtkomst åt utomstående parter (konsulter, BYOD- enheter) till program som företaget använder sig av, utan att registrera dessa enheter i systemet. Via denna programbutik kan man dela med sig alla olika program, skyddade av Good- ramverket (presenteras i nästa stycke) eller inte skyddade, och man kan även dela med sig filer som bilder, presentationer eller videon. Användare kan sedan kommentera på funktionalitet i program så att administratörer kan enkelt följa med om det hittas problem, speciellt i program som är utvecklade av företaget själv.

Alla program och all information är krypterade med 192-bitars AES, och är skyddade även om någon lyckas göra intrång på en enhet förbi låskoden. Med olika policyn kan företag skydda sin information som finns på enheter och administratörer kan blockera program som finns inom ramverk att kommunicera med varandra. Good Technology gör det möjligt att stänga in program inom ett Good-ramverk. Detta ramverk ser även till att information som temporärt sparas utanför ramverket på enheten är skyddad om

den har med det skyddade programmet att göra. Med Good-ramverket är det möjligt att omringa vilket program som helst, fastän man inte har tillgång till koden som finns inom programmet. Information som finns inom ramverket och som skickas ut är automatiskt krypterat. Rapportering av vilka program som användare laddat ner och vilka programpolicyn som är i användning kan administratörer enkelt få fram.

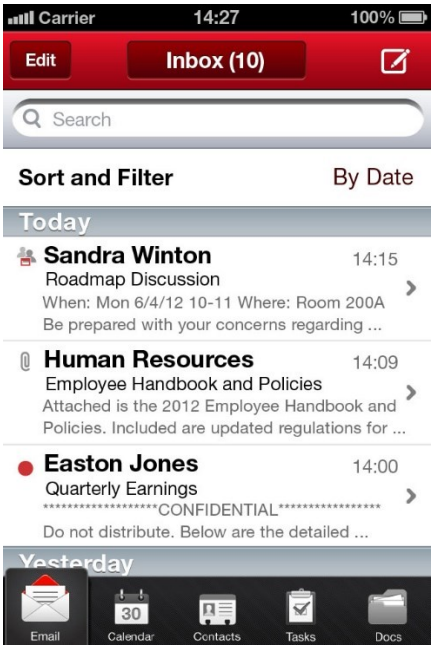
Good Technology stöder SSO-autentisering, vilket betyder att en användare behöver bara autentiseras en gång och kan öppna alla Good-specifierade program efter det. För detta så används ”Kerberos Constrained Delegation” (KCD) vilket betyder att en användare inte behöver överhuvudtaget använda sig av de inloggnings uppgifter på mobila enheter som de använder vanligtvis för att logga in i företagets nätverk. På detta vis behöver inte företaget oroa sig över att konfidentiell inloggningsinformation sparas på enheter, eftersom dessa aldrig lämnar företagets interna nätverk. Denna autentisering fungerar mellan alla program inom Good Collaboration Suite och 3:e parters program som är skyddade inom Good-ramverket.

4.3.3 Good Collaboration Suite

Good Collaboration Suite är ett paket med olika program som Good Technology erbjuder med sin tjänst (Good Collaboration Applications, 2014). Program som företag får i sin användning är en e-post klient med kalender och kontaktuppgifter, en säker webbläsare med vilken användare kan enkelt surfa på Internet utan att vara rädd att någon viktig information läcker ut, program för att hålla kontakt med andra användare och för att dela med sig dokument. Alla dessa program är skyddade inom Good- ramverket och kräver bara en SSO-autentisering för att användas. I denna del av texten kommer de olika program som kommer med tjänsten att presenteras.

Good Work är det program som kombinerar användningen av alla andra Good-program(kan jämföras med Worx Home i Citrix tjänst). Med detta centrala program kan användare snabbt och enkelt använda sig av de andra program som finns på den mobila enheten inom Good-ramverket. Man kan via en meny komma åt sin e-post, granska sin kalender eller kolla sina kontaktuppgifter, se Figur 13. Här kan man även se vilka kollegor som är aktiva, inaktiva eller upptagna. Här finns även en meny för att enkelt skriva

ett nytt e-post meddelande eller skicka ett direkt meddelande till en kollega som är aktiv exempelvis om man inte hinner i tid till ett möte.



Figur 13. E-post klienten med Good Technology ('Bring your own device' gets smarter with update from Good Technology, 2014)

Good Share är ett program av Good Technology som används för att komma åt och dela med sig filer. Med detta program kan användaren enkelt komma åt och editera dokument som ligger direkt inom företagets nätverk. Good Share går att synkronisera direkt med företagets SharePoint-miljö och användare kan editera dokument direkt på sin mobila enhet utan att spara dokumentet på enheten, Se Figur 14. Med dataskyddet som Good Technology erbjuder är all information krypterad när det editeras och när det skickas mellan olika program inom Good-ramverket. Med detta kan man på distans tömma all företagsinformation från en mobil enhet utan att tömma någon privat information.

Figur 14. Med Good Share kommer man åt dokument inom det interna nätverket (Good Share, 2014)

Good Connect är ett program för att användare snabbt och enkelt skall ha möjlighet att kommunicera med varandra med hjälp av direkta meddelanden. Man kan se från företagets globala adresslista alla kontaktuppgifter och enkelt se om andra användare är aktiva, upptagna eller inaktiva. Det går även att ringa och skicka e-post meddelanden om man vill. Alla meddelanden och all information som skickas vi Good Connect är krypterade och skyddade. Detta program går att integrera med system som redan är i användning i företaget, t.ex. Microsoft Lync, och inga extra servrar eller VPN anslutningar behövs.

Good Access är en säker webbläsare som ingår i Good Collaboration Suite. Med denna kan man öppna en säker anslutning till interna företagssidor och tjänster. Användare kan även säkert surfa på Internet. All information som går via Good Access är krypterad och skyddad i alla skeden. Administratörer kan med hjälp av olika policyn ställa in användningen av Good Access från användarens synvinkel. Man kan exempelvis blockera sidor som företaget inte vill att användare besöker med mobila enheter. Det är även möjligt att tömma all sparad information inom webbläsaren på distans.

4.4 Sammanfattning

I detta kapitel har tre stora företag presenterats som erbjuder tjänster för att administrera och göra distansanslutningar till företagsnätverk med mobila enheter. Airwatch, XenMobile och Good Technology erbjuder alla fullständiga MDM- och MAM system för

sina kunder och gör det möjligt att även hantera BYOD- enheter inom företaget. Alla dessa tjänster erbjuder även möjligheter att på ett enkelt sätt komma åt företagsinformation, editera och dela dokument mellan olika parter. Användning av Secure Content Locker, ShareFile och Good Share är alla tjänster som kan integreras med företagets SharePoint miljö, vilket betyder att användarna i företaget skulle komma åt och dela sina filer på ett säkert sätt. För att använda interna Internet-baserade tjänster kan de olika webbläsare som kommer med tjänsterna användas för att göra en säker distansanslutning till interna nätverk. Se Tabell 2 på nästa sida för en fullständig jämförelse mellan de olika tjänsterna.

Från uppdragsgivarens synvinkel erbjuder alla dessa företag på ett eller annat sätt vad de söker efter, en säker distansanslutning till företagets interna nätverk och åtkomst till filer som ligger inom nätverket. Alla tjänster kunde alltså vara potentiella att ta i bruk hos uppdragsgivaren. Personligen rekommenderar jag dock tjänsten som Good Technology erbjuder. Good Technology gör det enkelt att sätta upp ett fungerande system, administrera och hantera enheter i detta system. Användningen av de program som kommer med Good Collaboration Suite är enkla att använda, vilket är mycket viktigt i ett företag var det finns användare med bristfälliga tekniska kunskaper och som har svårt med användning av nya program. En betydande fördel som ingen annan tjänst erbjuder är den direkta kommunikationen som Good Connect erbjuder. Ingen möjlighet för direkta meddelanden finns nu hos uppdragsgivaren och all interna kommunikation sker med e-post eller telefonsamtal.

Tabell 2. En jämförelse mellan de presenterade tjänsterna.

	WMware Airwatch	**Citrix XenMobile**	**Good Technology**
BYOD	X	X (Citrix MDX)	X
Profiler för anslutningar	X	X	X
Policyn	X	X	X
Definiera operativsystem som är	X	X	

stödda			
MDM- system	X	X	X
MAM- system	X	X	X
Web konsol	X	X	X
Företags- eller privatägda enheter	X	X	X
Dela på företags- och privatinformation	X	X	X
Företagsprogram ramverk	Airwatch Workspace	Citrix MDX	Good Work
Flera faktorers autentisering	X	X	X
Stöd för SSO	X	X	X
App Wrapping	X		X
Active Directory synkronisering	X	X	X
Rapportering av enheter och program	X	X	X
Programlista/butik	AppCatalog	Worx Home	Good Work
Test av nya program	App Reputation Scanning		
Intern kommunikation			Good Connect med Microsoft Lync synkronisering
Direkt länk till stödpersonal		GoToAssist	
Egna program	- Airwatch Inbox - Airwatch Browser - Secure Content	- Worx Mail - Worx Web - ShareFile	- Good Work - Good Share - Good Connect - Good Access

	Locker		
Säker anslutning till interna nätverk	Med Airwatch Browser som använder Airwatch App Tunneling via Mobile Access Gateway.	Med Worx Web som gör en säker mikro-VPN anslutning till NetScaler Gateway inom nätverket	Krypterat med Good Access som kontaktar Good Proxy server
Filhantering/delning	Med Secure Content Locker som använder App Tunneling via Mobile Access Gateway. SharePoint integrering och editering av dokument möjlig. Delning med länkar.	Med ShareFile. Integrering med SharePoint möjlig. Användare kan editera dokument på enheten. All kommunikation krypterad med SSL. Delning med länkar.	Med Good Share som går att integrera med företagets SharePoint miljö. All information krypterat med 192- bitars AES.
Bara filhantering utan MDM- administrering	X	X	X

5 SLUTSATSER

Examensarbetet har utrett hur det tre största mobila operativsystemen är uppbyggda och vad de gör för att skydda information som finns i och skickas ut från mobila enheter. Windows Phone 8.1 och iOS är två mobila operativsystem som vill att all information skall vara så säker som möjligt och implementerar olika säkerhetsaspekter på såväl operativsystem- som hårdvarunivå. Android gör även mycket för säkerheten i operativsystemet, men vill samtidigt att utvecklare skall ha ett öppet operativsystem att jobba med och göra operativsystemet mångsidigare.

Uppdragsgivaren har i bruk ett MDM-system och EAS för att användarna skall komma åt sin e-post, men vill att användarna även skall komma åt annat som de kan behöva. En begränsning för detta är att bara företagsägda enheter kan registreras i uppdragsgivarens system. WMware Airwatch, Citrix XenMobile och Good Technology är alla olika tjänster som gör det möjligt att administrera och hantera mobila enheter i ett företag. Dessa tjänster erbjuder hela MDM- och MAM-system som företag kan använda sig av, och olika möjligheter för att göra en distansanslutning till företagsnätverk. Ett av uppdragsgivarens önskelmål var att tjänsten även skulle möjliggöra en BYOD- lösning, och de tjänster som studerats i examensarbetet erbjuder detta i någon form. Alla de studerade tjänsterna erbjuder olika program för e-post, fildelning och webbläsning.

Detta examensarbete skall fungera åt uppdragsgivaren som en informativ källa vilken fungerar som stöd för val av tjänst i framtiden. Inget direkt val av tjänst har gjorts i examensarbetet men författarens personliga rekommendation är Good Technology eftersom tjänsten erbjuder allting som uppdragsgivaren vill att skall ingå och är enkelt att använda, samt innehåller ny programvara(Good Connect) som hjälper användare att kommunicera.

KÄLLOR

Airwatch Solutions, VMware Airwatch. Tillgänglig: http://www.air-watch.com/solutions Hämtad: 19.11.2014

Android Architecture - The key concepts of Android OS, Android-App-Market.com. Tillgänglig: http://www.android-app-market.com/android-architecture.html Hämtad: 9.11.2014

Android Security Overview, Google Android. Tillgänglig: https://source.android.com/devices/tech/security/ Hämtad: 2.10.2014

'Bring your own device' gets smarter with update from Good Technology, thefone-cast.com. Tillgänglig: http://thefonecast.com/News/TabId/62/ArtMID/541/ArticleID/6143/Bring-your-own-device-gets-smarter-with-update-from-Good-Technology.aspx Hämtad: 14.12.2014

Citrix XenMobile MDM, Thomas Poppelgaard. Tillgänglig: http://www.poppelgaard.com/wp-content/uploads/2013/02/xenmobile-device-manager.png Hämtad: 26.11.2014

Citrix XenMobile Securing the Mobile Enterprise, Citrix XenMobile. Tillgänglig: http://www.citrix.com/content/dam/citrix/en_us/documents/oth/securing-the-mobile-enterprise.pdf Hämtad: 19.11.2014

Citrix XenMobile Technology Overview, Citrix XenMobile. Tillgänglig: http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-xenmobile-technology-overview.pdf?accessmode=direct Hämtad: 23.11.2014

Good Collaboration Applications, Good Technology. Tillgänglig: http://www1.good.com/applications/collaboration-suite/ Hämtad: 13.12.2014

Good Share, Reed Exhibitions. Tillgänglig: http://www.infosecurityeurope.com/en/Exhibitors/230821/Good-Technology/Products/630039/Good-Share Hämtad: 14.12.201

Good Technology, Bytes Technology Group. Tillgänglig: http://www.bytes.co.uk/vendors/solutions/good-technology/ Hämtad 13.12.2014

How to secure your Androids Wi-Fi, Geier, Eric. Tillgänglig: http://www.wi-fiplanet.com/reviews/ST/how-to-secure-your-androids-wi-fi.html Hämtad: 10.11.2014

How VPN works, Microsoft. Tillgänglig: http://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx Hämtad: 10.11.2014

iOS Security October 2014, Apple Inc. Tillgänglig: https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf Hämtad: 17.11.2014

Madden, Jack. 2014, *Enterprise Mobility Management: Everything you need to know about MDM, MAM, & BYOD*, 2. Uppl. San Francisco, California: Jack Madden. 176 s.

Mobile Device Management Gartner Magic Quadrant 2014, Mobility in SA. Tillgänglig: http://mobileinsa.blogspot.fi/2014/04/mobile-device-management-gartner-magic.html Hämtad: 2.1.2015

Secure Mobility Solutions, Good Technology. Tillgänglig: http://www1.good.com/good-dynamics-platform/ Hämtad: 23.11.2014

Technical Information about VPN: How data is protected, University of Texas. Tillgänglig: http://www.utexas.edu/its/help/vpn/1354 Hämtad: 30.10.2014

Understanding the role of Exchange ActiveSync in Mobile Device Management, Maas360. Tillgänglig: http://content.maas360.com/www/content/wp/wp_maas360_mdm_roleOfEAS.pdf Hämtad: 31.10.2014

Windows Phone 8.1 Security Overview, Microsoft. Tillgänglig: http://www.microsoft.com/en-us/download/details.aspx?id=42509 Hämtad: 9.10.2014

WPA2 for Android, Secure W2. Tillgänglig: http://www.securew2.com/wpa2-android Hämtad: 4.1.2015