kapsch

SPENGERGASSE
ausbildung mit zukunft

UNTERSUCHUNGSBERICHT

KTI – Kapsch Tablet Infrastructure

Sebastian Götze
Samuel Hammer
Michael Kaufmann
Konstanze Müller
Philip Steinhäuser

HTBLVA Spengergasse, Spengergasse 20, 1050 Wien

1 Inhaltsverzeichnis

2 Einleitung

Dieser Untersuchungsbericht dient dazu der Firma Kapsch BusinessCom AG eine Empfehlung für ein bei deren Kunden einzusetzendes Managementsystem für Tablets auf Basis Android auszusprechen. Diese Plattform muss gewissen Vorgaben des Unternehmens entsprechen, welche in der Anfangsphase des Projekts definiert wurden. Nach anfänglichen Untersuchungen konnte des Projektteam vier Kandidaten für Betriebsplattformen in die engere Auswahl ziehen. Diese vier Systeme wurden bezüglich ihres Nutzens für die Absichten der Firma Kapsch BusinessCom AG untersucht, dokumentiert und in diesem Untersuchungsbericht zusammengefasst. Bei diesen potenziell einsetzbaren Systemen handelt es sich um:

- Linux Manipulation
- Mobile Device Management
- Mobile Device Management + Container Technologien
- Samsung Knox

Diese werden in diesem Bericht detailliert dargestellt und es wird auf deren spezifische Stärken und Schwächen eingegangen. Am Ende stellt eine Nutzwertanalyse einen Vergleich der Systeme dar, an Hand derer das abschließende Fazit und die damit einhergehende Empfehlung erfolgen. Damit kann die Kapsch BusinessCom AG dann entscheiden, ob und wenn wie sie das System für ihre zukünftigen Projekte einsetzen können.

3 Linux Manipulation

3.1 Allgemein

Dieser Teil befasst sich mit der Veränderung des Grundsystems eines jeden Android Geräts. Dieses Grundsystem basiert auf dem Open Source Betriebssystem Linux und existiert dabei in einer für Mobilgeräte angepassten Form. In seiner Standardimplementation bietet es zwar einige Funktion zur Erhöhung der Gerätesicherheit, jedoch nicht genügend, um es in einem betrieblichen Umfeld einzusetzen. Da Linux ein Open Source System ist, darf der Source Code von jedem angesehen und nach eigenen Wünschen verändert werden. Und genau hier setzt die Methode der Linuxmanipulation an. In dem man den Source Code so verändert, dass bestimmte Teile des Betriebssystems unzugänglich gemacht oder verschlüsselt werden, ist es möglich den späteren Benutzer vor unabsichtlichen Änderungen am System zu bewahren, welche den reibungslosen Betrieb stören könnten. Das bedeutet, dass dadurch ein vollkommen an die Bedürfnisse des Kunden angepasstes Betriebssystem möglich wäre. Um sich einen besseren Eindruck davon zu verschaffen, wie diese Manipulationen letztendlich aussehen, lohnt es sich auf die diversen frei am Markt erhältlichen Derivate zu werfen. Bekannte Beispiele dafür wären:

- CyanogenMod
- Android AOSP
- Paranoid Android
- Dirty Unicorns
- Etc.

Zwar sind diese nicht mit securitytechnischen Absichten entwickelt worden, aber sie zeigen trotzdem auf was mit einer Menge an Entwicklungsaufwand möglich ist. Da aber durch die tiefgreifenden Eingriffe in das System eines Android Gerätes auch die Garantieansprüche verloren gehen, ist das Projektteam zu einem schnellen Fazit zu kommen.

3.2 Schlussfolgerung

Die Methode der Linuxmanipulation ist für die Zwecke der Kapsch leider absolut nicht einsetzbar, da sich bei ihr gewisse Konflikte bezüglich Garantieanspruch und Kosten ergeben. Zwar wären über diese Methode sämtliche Anforderungen an das Endprodukt erfüllbar, jedoch bedarf es dazu eines so großen Entwicklungsaufwands, dass dieser sich in einem dermaßen hohen Endkundenpreis niederschlagen würde, welcher von kaum einem Unternehmen zu bezahlen wäre. Denn nicht nur die Beschäftigung einer Vielzahl von Entwicklern über einen langen Zeitraum hinweg, sondern auch der anfallende Support für das Produkt würde sich selbst für ein großes Unternehmen wie Kapsch nicht rentieren. Ein weiteres großes Manko dieser Methode ist die verfallende Garantie für die Hardware. Egal mit welchen Android Tablet diese Software ausgeliefert werden würde, sobald eine Veränderung der darauf vorinstallierten Software stattfindet, gehen sämtliche Garantieansprüche an den Hersteller verloren. Bei der geplanten Menge an ausgelieferten Geräten durch die Kapsch, wäre dies nicht vertretbar. Für einen industriellen Einsatzzweck ist die Variante daher absolut nicht geeignet und der damit einhergehende Aufwand würde sich nur durch einen extrem hohen Verkaufspreis ausgleichen lassen. Somit bleibt dem Projektteam nichts anderes zu sagen, als, dass diese Variante nicht passend für die Absichten der Kapsch ist.

4 Mobile Device Management (MDM)

4.1 Allgemein

Die folgenden Zeilen beschäftigen sich mit dem Einsatz von Mobile Device Management Systemen als Betriebsplattform für potentielle Kunden der Firma Kapsch. Durchgeführt wurden alle Untersuchungen am bereits am Markt etablierten MDM-System MobileIron. Es wird beleuchtet, was der MDM-Standard ist, welche Funktionen für den alltäglichen Gebrauch unumgänglich sind und wie diese im System realisiert sind. Ein besonders wichtiger Punkt hierbei ist auch das Aufzeigen von nicht vorhandenen Funktionen, die jedoch für das Unternehmen Kapsch von fundamentaler Wichtigkeit sind. Des Weiteren wird auf die Bedienbarkeit und die Komplexität der Installation eingegangen und inwiefern dies für den Projektauftraggeber und dessen Kunden relevant ist. Abschließend wird ein Statement abgegeben, ob bzw. wie es möglich ist diese Form von System für die von Kapsch gedachten Zwecke einzusetzen.

Abbildung 1 Logo MobileIron

4.2 Mobile Device Management Standard

MDM bezeichnet einen von der Open Mobile Alliance (OMA) festgelegten industriellen Standard zur Verwaltung mobiler Endgeräte wie zum Beispiel Smartphones, Tablets oder Laptops. Es dient dazu, die allgemeine Verwaltung einer Vielzahl von Geräten zu erleichtern und somit Zeit und Kosten zu sparen. Die mobile Hardware kann dabei vom Unternehmen zur Verfügung gestellt werden oder, sofern mit dem Mitarbeiter abgesprochen, von diesem selbst mitgebracht werden. „Bring Your Own Device“ (BYOD) nennt sich dieser Ansatz. Dieser Standard wird in der Software verschiedenster Hersteller implementiert, welche dann dieses Komplettsystem verschiedenen Unternehmen zur Verwaltung ihrer Geräte anbieten. Beispiele dafür sind.

- MobileIron
- Samsung EMM
- Cisco Meraki
- MaaS360
- AirWatch
- etc.

Bestandteile dieser Softwarelösung sind eine Serverkomponente und die verschiedenen mobilen Clients. Der Server dient dabei dazu, die Konfigurationen und Statistiken für die Geräte zu halten und zu verwalten. Er sendet auch, auf dem MDM-Standard basierende, Management Kommandos an die Clients aus, wenn sich ein Parameter in deren Konfiguration verändert hat. War es am Anfang der MDM-Systeme noch notwendig das Gerät dazu physisch mit dem Server zu verbinden, geschieht dies heute vollautomatisch über Netzwerkverbindungen. Die implementierten Funktionen können zum Beispiel eine over-the-air (OTA) Verteilung von Applikationen, Daten oder Konfigurationen sein. So braucht ein Administrator nicht auf 100 Geräten das Wifi-Netzwerk einrichten, sondern kann per Knopfdruck diese Konfiguration auf alle im System registrierten Geräte verteilen. Auch in Punkto Sicherheit bieten MDM-Systeme einige Möglichkeiten und deshalb sind sie so interessant für die Zukunftspläne der Firma Kapsch. So bieten diese Systeme die Möglichkeit Passwortrichtlinien zu setzen oder sogar ganze Teile des Betriebssystems zu sperren, damit diese für den Benutzer nicht zugänglich sind. Dadurch soll die Anfälligkeit für Fehler im Berufsumfeld gesenkt und ein ordentlicher Arbeitsablauf genehmigt werden.

4.3 Informationen der getesteten Software

Name:	MobileIron EMM
Hersteller:	MobileIron, 415 East Middlefield Road, Mountain View, CA 94043
Version:	7.5.0
Datum:	27.1.2015
Preis:	/
Website:	http://www.mobileiron.com/
Dokumentation:	https://support.mobileiron.com/eval/

4.4 Installation

Die Installation von MobileIron gestaltet sich relativ einfach, wobei doch einige wichtige Dinge zu beachten sind. Nach dem Download einer Datei aus dem Online-Zugangsportal von MobileIron kann über diese das Betriebssystem installiert werden. Diese gestaltet sich für erfahrene Nutzer sehr einfach, allerdings ist auf eigene Dinge Acht zu geben:

Folgende Daten müssen bereit stehen bzw. eingerichtet werden:

- Lizensierungsinformationen (Firma, Kontaktperson, E-Mail)
- IP-Adresse
- Externer Hostname (Sehr wichtig, weil die mobilen Geräte den Server von außerhalb erreichen müssen)
- Command Line Interface Passwort
- Administratorname und – passwort
- Mindestens 1 physisches Interface
- Subnetzmaske
- Default Gateway
- Mindestens 1 zu erreichender DNS-Server
- Wahlweise
    - SSH-Zugriff
    - Telnet-Zugriff
    - NTP

Ist die Einrichtung erfolgt, kann man das System nach einem Neustart bereits einsetzen. Während dem Evaluierungsprozess sind dem Projektteam allerdings einige wichtige Details aufgefallen. Ein funktionierender externer Hostname ist von höchster Wichtigkeit, weil ohne ihn zwar die Einrichtung der Software auf den mobilen Endgeräten funktioniert, leider jedoch die Verbreitung von Konfigurationen versagt. Da jedoch 99 Prozent aller modernen Unternehmen über solche Möglichkeiten verfügen sollten, dürfte dies im realen Betrieb weniger problematisch ausfallen. Hervorzuheben ist hierbei die hervorragende Dokumentation, die MobileIron für den Installationsprozess zur Verfügung stellt. Auf deren Website findet sich eine Sammlung an Dokumenten, welche den Administrator am Anfang zwar überwältigen könnten, aber sich als eine schnell zu durchforstende Sammlung an bebilderten Skripten zur Einrichtung sämtlicher Funktionen herausstellen. Generell lässt sich die Webplattform, welche MobileIron hier zur Verfügung stellt, gut bedienen und bietet Informationen zu den verschiedenen Implementierungsszenarien und Komponenten des Systems. So findet man sich nach kurzer Zeit bereits relativ gut zurecht und weiß, wo man suchen muss, um die benötigte Information zu finden.

4.5 Features

4.5.1 Key-Features

In diesem Teil werden die wichtigsten von MobileIron gebotenen Features beleuchtet und erklärt. Die folgende Liste stellt die wichtigsten Funktionen dar, welche während des Evaluierungsprozesses festgestellt werden konnten:

- MDM-System
- Management von verschieden vielen Geräten
  - Jeder Gerätetyp ist möglich, egal ob Smartphone, Tablet oder Laptop
  - Lokalisierung sämtlicher eingebundener Geräte
  - Leicht aufzusetzen und zu verwenden
    - Installation einer einzigen App ist notwendig, um das Gerät in die Plattform einzubinden
  - Verwendbar ab dem ersten Gerät
  - Mehrsprachig
  - Geringe Wartungskosten
- Konfiguration der eingebundenen Endgeräte
  - Vorkonfiguration von Email-Konten und sonstigem (Wifi, VPN, etc.)
    - Der Angestellte muss dies nicht selbst erledigen
    - Keine Chance einer Fehlkonfiguration
    - Verteilbar auf hunderte Geräte innerhalb von Sekunden
- Statistiken
  - Verfügbare Statistiken
    - Gerätestatus
    - Kompromitierungsstand
    - Betriebssystem
    - Betriebssystemversion
    - Zugehörigkeit (gehört dem Unternehmen oder dem Angestellten)
    - Netzbetreiber (3, A1, Telering, etc.)
    - Registrierungszustand
  - Logging von Events:

Device Actions	**App -**	**Policy -**	**Space -**	**Status -**
Register	Install	Activate	Add Space	Not started
Wipe	Uninstall	Modify	Remove Space	In progress
Lock	Set setting	Deactivate	Change Space Prioritization	Completed successfully
Retire	Unset setting		Assign Space Admin	Failed
			Delete Space Admin	

- Policies
  - Dienen zur Erhöhung der Sicherheit von registrierten Mobilgeräten
  - Blockieren von Systemteilen oder Einstellungen
    - Zum Beispiel: Der Benutzer kann das WLAN oder GPS nicht mehr ausschalten
    - Diese Funktion wird benötigt, wenn die Chance besteht, dass der Anwender durch gewollte oder ungewollte Aktionen das Gerät in einen unbenutzbaren Zustand bringt.
  - Passwortpflicht
    - Der User ist dazu gezwungen, ein Passwort nach Unternehmensrichtlinien zum Sperren und Entsperren seines Gerätes zu setzen
  - Globaler Proxy
    - Sämtlicher Netzwerkverkehr wird durch einen Proxy-Server des Unternehmens geleitet, welcher dazu dient, ungewollte Websiteinhalte zu filtern oder um Unternehmensdaten vor dem Verlassen des Firmennetzwerks zu schützen.
  - Kiosk-Modus
    - Das Gerät wird in einen Zustand versetzt, in dem nur mehr das Benutzen einer einzelnen Applikation möglich ist.
  - Applikationen
    - Erlauben von spezifischen Apps
    - Verbieten von spezifischen Apps
    - Erfordern von spezifischen Apps

4.5.2 Zusatzfeatures

MobileIron bietet die Möglichkeit seine Vielfalt an Features zu erweitern, indem man es an eine sogenannte „Standalone Sentry“ anbindet. Diese ermöglicht es dem Administrator des MDM-Systems die von MobileIron entwickelten Applikationen auf allen Geräten zu installieren. Diese Applikationen dienen dazu den E-Mail-Verkehr, das Webbrowsing, die Installation von Applikationen und den Zugang zu Unternehmensdokumenten zu sichern. Sie heißen:

- Apps@Work
- Docs@Work
- Web@Work

Nachdem sich das Projektteam in diese vertieft hatte, hat es erkannt, dass diese Applikationen eine sogenannte Containertechnologie einsetzen und somit nicht Bestandteil eines standardmäßigen MDM-Systems sind. Daher werden diese in einem anderen Teil des Evaluierungsprozesses behandelt, welcher „MDM+Container“ heißt. Eine weitere Zusatzfunktion, die MobileIron bietet, sind „ActiveSync Policies“. Diese stellen dabei einfach nur durchgehend upgedatete Policies dar, welche bei einer Verletzung sofort Alarm schlagen.

4.6 Testphase und -Ergebnisse

Während der Testphase wurde das System eingehend getestet und festgestellt, ob es den Anforderungen der Firma Kapsch genügt. Hierbei wurden vom Projektteam verschiedenste Szenarien durchgespielt und diverse Arten von Konfigurationen getestet. Im folgenden Abschnitt werden die Ergebnisse der Untersuchungen und deren Auswirkungen präsentiert.

4.6.1 Erfüllte Anforderungen

1. **Nutzung ohne öffentliche Cloud-Services**
   Das getestete Endgerät ist vollständig ohne öffentliche Cloud Services einsetzbar. Das bedeutet, dass kein Google-Konto oder ähnliches notwendig ist, um es zu verwenden. Natürlich entfallen dadurch auch bestimmte Features wie der Google Play Store zur Installation von Applikationen.

2. **Keine Zuweisung zu einer spezifischen Person notwendig**
   Es war dem Projektteam möglich, das Tablet einzusetzen ohne es einem konkreten Projektmitglied zuzuweisen. Jeder aus dem Team konnte es gleichermaßen ohne jegliche Einschränkungen verwenden. Dabei bleibt natürlich zu beachten, dass die Passwörter und Zugangsdaten allen Benutzern mitzuteilen sind. Dies kann über Wege wie eine Textdatei, Notizzettel oder Ähnlichem geschehen.

3. **Verhinderung der Installation von Applikationen**
   Über die verschiedenen Policies, welche das System bietet, ist es möglich die Installation einzelnen oder allen Applikationen zu blockieren. Dies verhindert, dass der spätere Anwender ungewollte Apps installiert, welche den Zustand des Systems verändern könnten und es somit für den Arbeitsgebrauch unbrauchbar machen.

4. **Keine Zugriff auf die Einstellungen**
   Durch eine Policy war es dem Projektteam möglich, sämtlichen Zugriffe auf die Einstellungen zu sperren, egal ob über die App oder über die Taskleiste am oberen Bildschirmrand. Diese Möglichkeit ist deshalb so wichtig, um den Anwendern davon unerwünschte Änderungen durchzuführen.

5. **Verstecken der Standard-Applikationen**
   Diese Anforderung konnte die MDM-Lösung nicht vollständig umsetzen. Dem Projektteam ist es zwar gelungen einige einzelne Standardapplikationen auszublenden (Google Play, YouTube, Browser), allerdings war es nicht für alle Systemapps möglich. Zu diesen nicht auszublendenden Softwarepacketen gehören die Galerie, Gmail, alle weiteren Google Play Apps (Music, Movies, etc.), die Kontakte, Maps und noch einige weitere. Dies muss nicht unbedingt zu Probleme im Betriebseinsatz führen, stellt aber trotzdem ein nicht zu unterschätzendes Risiko dar.

6. **Filtern von Browserinhalten**
   Diese Funktionalität ist über die Nutzung eines globalen Proxy-Servers gewährleistet. Dieser ist gesondert vom Unternehmen einzurichten und bietet alle Möglichkeiten wie Sie ein herkömmlicher Proxy bietet.

7. **Remote-Zugriff**

8. **Verwalten von Applikation per Remote**
   MobileIron bietet die Möglichkeit zu überprüfen, welche Apps auf einem Gerät installiert sind und es ist bei Bedarf möglich bestimmte Applikationen zu sperren bzw. sie als erforderlich einzustufen.

9. **Festlegen von Hintergrund und Lockscreen per Remote**
   Diese Funktionalität ist auch nur teilweise gegeben. Folgendes ist dabei aus den Tests des Projektteams hervorgegangen: Es ist möglich einen Lockscreen und ein entsprechendes Passwort vom User zu verlangen. Auch das Sperren von Widgets am Lockscreen ist ohne weiteres möglich. Das Festlegen und Ändern des Hintergrundbilds ist mit MobileIron jedoch nicht möglich.

10. **Logs der UP-/Downtime**
    Über die Weboberfläche des MDM-Systems ist es möglich zu überprüfen, wie lange ein Gerät mit dem System verbunden war oder auch nicht.

11. **Logs sortierbar nach Gerät und Ort**
    Für jedes im System registrierte Mobilgerät werden separate Logs generiert, über die die letzten Vorgänge verfolgt werden können. Diese sind sehr leicht abzurufen und werden auch übersichtlich dargestellt.

12. **Zurücksetzen des Geräts auf einen spezifischen Zustand durch den Benutzer**
    Diese Funktion ist in MobileIron nur begrenzt implementiert, weil es zwar die Möglichkeit gibt das Gerät auf den Werkszustand zurückzusetzen, aber nicht auf einen vom Unternehmen definierten Zustand. Gerade dies wäre für größere Kunden von der Kapsch sehr wünschenswert, weil so die Mitarbeiter bei einer Fehlfunktion des Geräts, dieses einfach wieder auf einen funktionstüchtigen Zustand zurücksetzen können. Somit ist die Funktionalität leider nur teilweise gegeben.

13. **Management mehrerer Gerätestandorte**
    Das Management mehrerer Standorte ist ohne weiteres möglich, weil im MDM-System Funktionen eingebettet sind Geräte nach Standort zu sortieren oder ihnen spezielle „Tags“ zu verleihen, über die sie bzw. ihr Standort identifiziert werden können.

14. **Ortung (inkl. Status) der Geräte über ein Dashboard**
    Auch die Ortung einzelner Endgeräte stellt mit MobileIron kein Problem dar. Zu jedem eingetragenen Tablet, Smartphone oder Tablet gibt es per Rechtsklick einen Eintrag „Locate“, über welchen das Gerät ausfindig gemacht werden kann. Dies funktioniert natürlich nur, wenn das Gerät mit dem Internet oder GPS verbunden und dabei eingeschalten ist.

15. **Fehlerberichte pro Endgerät und Standort**
    Für sämtliche Geräte ist es möglich einen Fehlerbericht zu erhalten, sollte z.B. bei der Einrichtung etwas fehlschlagen oder das Mobilgerät nicht den Unternehmensrichtlinien entsprechen. So lässt sich genau erkennen, warum es zu dem jeweiligen Fehler gekommen ist.

16. **Zurücksetzen des Geräts auf einen spezifischen Zustand per Remote-Zugriff**
    Wie bereits in Punkt 12 beschrieben lassen sich in das System eingebundene Geräte leider nur auf den Werkszustand zurücksetzen. Dies trifft ebenfalls auf das Management per Remote zu. Dem Administrator ist es somit über die Weboberfläche nur möglich das Endgerät auf den Auslieferungszustand zu setzen.

17. **Zugriff auf die Statistiken über Remote**
    Da sämtliche Statistiken im Onlineportal gesammelt werden und nicht auf den Geräten selbst, ist es selbstverständlich, dass diese auch dort abgerufen werden können. Die Informationen können somit von jedem Rechner, mit Zugriff auf Management-Backend von MobileIron, aufgerufen werden.

18. **Nutzbar ohne Kiosk-Modus**
    Um die Geräte im System nutzen zu können ist es nicht erforderlich sie in einem Modus schalten zu müssen, in dem nur eine einzige Applikation verwendbar ist. Die Haptik entspricht exakt der eines normalen Devices.

19. **Nicht zugeschnitten auf eine spezifische Hardware**
    Das gesamte System ist speziell im Hinblick auf Android mit jedem Gerät ab Version 2.3 verwendbar. Jedoch ist dabei zu beachten, dass nicht sämtliche Funktionen auf allen Geräten zur Verfügung stehen. So ist dem Projektteam bei seinen Untersuchung aufgefallen, dass ein LG Tablet weniger Konfigurationsmöglichkeiten bietet, als ein Samsung Gerät. Dies ist darauf zurück zu führen, dass das Samsung Tablet einen speziellen Chip eingebaut hatte, welcher es erlaubte einen tieferen Eingriff in das System durchzuführen. Somit sollte beim Einsatz dieses Systems darauf geachtet werden mit welchen Endgeräten es betrieben wird.

20. **Geringe Wartungskosten**
    Ein wahrer Vorteil dieses MDMs sind die nahezu nicht vorhandenen Wartungskosten. Ist das System einmal installiert und eingerichtet so läuft es praktisch ohne jegliche weitere Wartung. Lediglich die Lizenzkosten an das Unternehmen sind jährlich abzutreten. Dies stellt natürlich eine große Kostenersparnis dar.

21. **Filtern von expliziten Inhalte**
    Wie bereits in Punkt 6 beschrieben ist dies über den Einsatz eines globalen Proxy möglich. Somit können die Endgeräte frei von Gewalt, Extremismus, Pornographie, etc. gehalten werden.

22. **Mehrsprachig**
    MobileIron bietet sein MDM in verschiedensten Sprachen an, jedoch ist es trotzdem zu empfehlen das System in Englisch zu verwenden, da auch die Dokumentation in dieser Sprache geschrieben ist und somit die Installation und Einrichtung dadurch deutlich vereinfacht wird.

4.6.2 Nicht erfüllte Anforderungen

1. **Benutzer können Apps nicht deinstallieren**
   Aus den Untersuchungen des Projektteams ist hervorgegangen, dass das Deinstallieren von Applikationen nicht ausreichend verhindert werden kann. Es ist zwar möglich die Installation von Unternehmensapplikationen zu blockieren, jedoch werden diese automatisch wieder installiert, sobald sie deinstalliert wurden. Dies könnte jedoch zum Verlust von Daten führen. Für Applikationen, welche nicht vom Unternehmen bereitgestellt werden, ist es nicht möglich deren Deinstallation zu verhindern. Für einen Einsatz in einem professionellen Arbeitsumfeld ist das leider nicht ausreichend, weil dadurch eine große Anzahl von Problemen auftreten kann. Dies ist ein kritischer Punkt in der Systemauswahl und deshalb wurde diese Funktion vom Projektteam als nicht erfüllt bewertet.

2. **Websites/Links können per Remote verwaltet werden**
   MobileIron bietet ohne Einsatz von Containertechnologien leider nicht die Möglichkeit die Webseiten, welche auf dem Gerät geöffnet sind, über Remote zu verwalten. Auch das Öffnen eines speziellen Links lässt sich nicht realisieren. Unter gewissen Umständen könnte das zu gröberen Komplikationen in einem Unternehmensumfeld führen. In einem Lokal könnte somit nicht gewährleistet werden, dass immer die Website des Lokalbetreibers geöffnet ist.

3. **Inhalte können per Remote verwaltet werden**
   Die Möglichkeit Medien und andere Daten auf dem Gerät von außerhalb zu verwalten, ist leider nicht gegeben. Dies ist jedoch ein Punkt von äußerster Wichtigkeit, weil diese Funktion für die Einsatzzwecke eines Tablets im Businessalltag von Nöten ist. Ob es nun dazu gedacht ist um einen Manager die Umsätze des letzten Monats zu liefern oder einem Baumeister die Baupläne zur Verfügung zu stellen, diese Funktionalität muss gewährleistet sein, um das Gerät professionell einsetzen zu können.

4. **Logs von Benutzersessions, Nutzungszeit, App-Aufrufen und Webseiten**
   Das Mitschreiben der Dauer von Benutzersessions oder der Nutzungsdauer von Apps, etc. wird von MobileIron leider nicht unterstützt. Zwar ist dieser Punkt nicht so kritisch wie die vorherigen, aber zu Analysezwecken wäre es für Unternehmen doch sehr interessant zu wissen, wie sich ihre User verhalten, um Rückschlüsse auf Probleme oder Unklarheiten zu ziehen.

5. **Möglichkeit zur Löschung der Benutzerdaten durch den User**
   Auch eine Funktion zur Sicherheit der Anonymität eines Benutzers bringt MobileIron leider nicht mit. Zwar ist es dem User möglich seinen Browserverlauf durch das umständliche Suchen in Untermenüs zu löschen, allerdings wäre das für einen Laien nicht praktizierbar. Andere Nutzerdaten hingegen sind nicht durch den Benutzer löschbar und könnten nur durch ein Zurücksetzen auf den Ausgangszustand unauffindbar gemacht werden. Daher erachtet das Projektteam diese Funktionalität als nicht gegeben.

6. **Zurücksetzen auf einen definierten Zustand nach einem bestimmten Intervall an Inaktivität**
   Da bereits das Zurücksetzen auf einen anderen Zustand außer dem Werkszustand nicht vorhanden war, ist diese Möglichkeit leider auch nicht gegeben. Diese Funktion wäre besonders in öffentlichen Verkaufsräumen von Nutzen, wenn ein Gerät sich alle 2 Stunden wieder auf den Ausgangszustand zurücksetzen könnte und somit für Besucher in einem einheitlichen Zustand befindet.

7. **Einsetzbar ab einem Endgerät**
   Leider bedarf es bei MobileIron einer gewissen Anzahl an Geräten, damit man eine gültige Lizenz erhält. Eine Testversion gibt es zwar schon ab einem Client, diese kann jedoch leider nicht in einem produktiven Umfeld eingesetzt werden. Deshalb kann MobileIron diesen Punkt leider nicht erfüllen.

5 MDM + Container

5.1 MobileIron Containertechnologie

MobileIron Content Mangement (MCM) ist die Containertechnologie der gleichnamigen Firma MobileIron. Die Containertechnologie basiert auf dem MobileIron MDM-System, welches in diesem Projekt separat analysiert wird.

Der Hauptnutzen dieser bestimmten Containertechnolgie ist die Verwaltung von Benutzerressourcen. Ursprungsansatz der Entwicklung ist der fortschreitende Trend zur Arbeit auf mobilen Geräten wie Tablets. Das MCM-System ist auf folgende Module aufgeteilt: Docs@Work, Apps@Work, Web@Work.

5.2 Allgemeine Information der getesteten Software

Name:	MobileIron Mobile@Work
Manufacturer:	MobileIron 415 East Middlefield Road, Mountain View, CA 94043
Current Version:	
Date:	26.01.2015
Price:	-
Website:	https://www.mobileiron.com/en/products/product-overview
Documentation:	https://support.mobileiron.com/eval/

5.3 Installation

Die Konfiguration der Containertechnologie geschieht über ein Webinterface, welches man ebenso für das Standard MDM-System von MobileIron verwendet. Eine Dokumentation wie zum Beispiel ein Benutzerhandbuch über die Konfigurationsschritte von MobileIron direkt ist zwar vorhanden, wobei dieses erst größtenteils während unserer Projektzeit erschienen ist. Somit versuchte das Projektteam zunächst dies alleine zu bewältigen und scheiterte, da die gesamte Benutzeroberfläche nur gering selbsterklärend ist. Mittels des Benutzerhandbuches gelang es uns nach mehreren Versuchen die Containertechnologien Web@Work und Apps@Work funktionstüchtig zu bekommen. Für mehr Aufwand sorgten Zertifikate und Konfigurationsdateien, welche man für die Konfiguration benötigt und nur sehr oberflächlich in den bereitgestellten Dokumenten beschrieben worden sind. Weiters beschäftigte uns die nicht konstante und auffallend lange Synchronisationszeit zwischen dem Server und dem Client Device. Der Grund dafür war für uns nicht klar ersichtlich und hätte für eine genaue Analyse zu viel Zeit in Anspruch genommen. Jedoch deutet vieles darauf hin, dass die Ursache in unserem selbstaufgebauten Testnetzwerk entstanden ist, welches sehr klein und minimalistisch gehalten wurde.

5.4 End User Products

5.4.1 Docs@Work

Docs@Work stellt den Usern unternehmensinternen Content für deren tägliche Arbeit zur Verfügung. Dies basiert auf einem Cloud-Content-Management-System und wird am Gerät als eigene App dargestellt. In erster Linie gewährt die Containertechnologie einen sicheren Verbindungsaufbau zu „Content Repositories“. Unter „Content Repositories“ versteht man im Allgemeinen gewöhnliche unternehmensinterne Fileserver (SharePoint), welche als Netzwerkressourcen zur Verfügung stehen. Besonders dabei ist, dass auch empfangende Daten via Email in dem gleichen Ausmaß wie normale „Content Repositories“ den Sicherheitsrichtlinien unterworfen sind. Dem User steht die Möglichkeit des Downloads dieser Dokumente offen. Diese Funktion, welche offiziell unter dem Namen „Secure Email Attachment“ geläufig ist, basiert auf MobileIron AppContent. Diese Technologie stellt eine konsistente, sichere Umgebung auf dem Android Gerät zur Verfügung. D.h. Unternehmensdaten welche auf dem Mitarbeitergerät abrufbar sind, sind verschlüsselt.

Aus Administratorsicht gewährt Docs@Work neben der zentralen Verwaltung von Ressourcen für einzelne User ebenfalls die Möglichkeit bei nicht gewünschten Tätigkeiten eines Mitarbeiters seine Berechtigung einzuschränken. Administratoren können bestimmte Geräte von Mitarbeitern in Quarantäne verschieben bzw. diese ganz entfernen. Die betroffenen Geräte sind dann nicht mehr in der Lage sich mit dem Server zu verbinden.

Als gewissen Vorteil dieser Technologie kann man den Wegfall des üblichen zusätzlichen VPN auf den Geräten bezeichnen. Die Bedingung ist für den Anwender kompakter und schneller. Sofern der User Zugriff auf den „Content Repository“ hat, gilt die Regelung des Single-Sign-On. Dies gewährt eine einmaligen Anmeldung pro einem User Account und garantiert Zugriff auf alle verknüpften Anwendungen ohne weitere Log-in Sessions.

Die oben genannte Secure-Email-Attachment-Funktion ist nach Informationen von der offiziellen MobileIron Homepage bis zum heutigen Stand nur mittels Email-Applikationen namens Divide und Email+ funktionstüchtig.

Ebenso gibt es nur ausgewählte „Content Repositories“, welche Docs@Work unterstützen. Zu diesen zählen:

- Microsoft Sharepoint 2007/2010/2013
- CIFS Windows 2008 R2 SPI
- CIFS Samba CentOS 6.2
- Apache-based WebDAV content repositories
- IIS-based WebDAV content repositories

5.4.2 Web@Work

Web@Work garantiert Unternehmen einen sicheren, mitunter auch beschränkten Internetzugriff ihrer Mitarbeiter. Es basiert auf zwei Technologien namens AppTunnel und MobileIron Sentry, welche bei Nutzung von Web@Work auch konfiguriert werden müssen. Das Zusammenspiel dieser zwei Technologien gewährt eine Zugangsbeschränkung/Kontrolle sowie den verschlüsselten Datenaustausch. Die Administratoren sind in der Lage gewisse, in den Augen des Unternehmens wichtige Websiten für die Mitarbeiter frei zu schalten und somit den Besuch dieser zu erlauben. Unter diesen Websiten werden auch interne Unternehmens Websiten verstanden. Daten wie der Zwischenspeicher des Browsers, Cookies, die Web History als auch Daten von anderen Websiten werden alle verschlüsselt übertragen. Sofern ein Android-Gerät eines Mitarbeiters den Zugangsbestimmungen nicht mehr entspricht, werden all diese Daten aus Sicherheitszwecken gelöscht.

Laut der Dokumentation von MobileIron ist es möglich die User-/Geräte-Verwaltung dieses Systems mit dem Enterprise Directory des Unternehmens zu koppeln. Somit ist das Aktivieren und Zulassen von Websiten basierend auf bestimmten Gruppen von Usern möglich.

Die Gegenmaßnahme von MobileIron zur Prävention von DLP (Data Loss Prevention) ist die Deaktivierung vom Erstellen von Screenshots des Users.

Beim Einsatz dieser Technologie steht der Vorteil bezüglich des VPN im Vordergrund. Um Mitarbeitern einen sicheren, abgeschirmten Zugriff auf Webressourcen zu gewähren war bisher eine mögliche Variante, eine VPN Verbindung einzurichten. Web@Work ersetzt das VPN und gewährt weitere Möglichkeiten wie bereits oben beschrieben.

5.4.3 Apps@Work

Diese Technologie stellt dem Benutzer des Devices die benötigten Apps zur Verfügung. Dabei kann der User selbst nicht entscheiden, welche Apps er installiert, dies kann nur der IT Administrator. Somit wird das Verwenden des Devices für nicht unternehmensinterne Angelegenheiten verhindert. Der IT-Administrator deklariert alle Apps, die laut Unternehmensführung genehmigt sind. Alle anderen Apps, welche nicht angeführt sind, sind somit nicht für die Installation zulässig. Diese Technologie basiert auf AppConnect und AppTunnel.

Die erstangeführte Technologie AppConnect ist zuständig für die Implementierung eines Containers um die eigentliche App herum. Das Resultat daraus ist ein Schutz gegen „data-at-rest“-Daten des Devices bzw. Apps. Die vorhandenen Daten werden verschlüsselt und vor unberechtigten Zugriff geschützt. Auf dem jeweiligen Device sind alle App-Container der Apps verbunden und kommunizieren miteinander. Dabei werden Informationen, wie zum Beispiel Richtlinien und Single-sign-on-Daten, ausgetauscht.
AppTunnel ist für die Sicherheit und den Schutz der data-in-motion-Daten zuständig. Diese Technologie stellt sicher, dass die einzelnen Container um die Apps vom restlichen System abgeschirmt sind und keine Verbindung von außen über das Android-Basissystem auf die Container stattfinden kann. Die ‚certificate-based session authentication’ verhindert man-in-the-middle-Attacken.

Bei der Benutzung von Apps@Work unterscheidet man zwischen 3 verschiedenen Möglichkeiten Apps in das System einzubinden und dem User bereitzustellen.

Die wohl geläufigste Art Apps auf ein Android Device zu implementieren ist das Herunterladen mittels dem Google Play Store.

Der theoretische Ablauf ist folgender: Der IT-Administrator tätigt einen Vorschlag für eine ausgewählt App des Google Play Store und hat somit eine Freigabe für den Download dieser App. In unserem Anwendungsfall trifft diese Lösung nicht zu, da der Google Play Store einzig und allein bei Verwendung eines Google Accounts auf dem Device funktioniert. Die Verwendung eines Google Accounts ist in unserem Fall jedoch nicht zielführend, da weitere Sicherheitsprobleme auftreten würden. Daraus ergibt sich die zweite Variante zum Management der auf den Devices installierten Apps anzuwenden.
Die In-house Apps basieren hauptsächlich auf selbst entwickelten Applikationen, welche zum Bespiel das Unternehmen selbst in Auftrag gegeben hat. Für die Freischaltung zum Download dieser durch die User benötigt man die APK der App, welcher der IT Administrator zunächst selbst hochladen muss. Weiters kann man mittels Benutzung von In-house Apps ebenfalls zum Teil Apps installieren, welche im Google Play Store verfügbar sind. Voraussetzung dafür ist der rechtmäßige Besitz der APK Files der Apps.

5.5 Übereinstimmung mit den Anforderungen des Projektpartners

Die von unserem Projektpartner gestellten Anforderungen, welche bestmöglich erfüllt werden sollten, werden durch diese Containertechnologie zusammen mit dem gleichnamigen MDM System nur sehr geringfügig verbessert. Grund dafür ist in erster Linie, dass diese Containertechnologie - wie bereits oben erwähnt - sich auf die Verwaltung der Inhalte und Dokumente der User konzentriert. Unser Projektpartner stellt zwar ebenfalls 3 Anforderungen in diesem Bereich, diese kann man jedoch mittels dieser Technologie nicht wie gefordert umsetzen. Der Knackpunkt liegt in diesem Bereich bei der Verwaltung über Remote. Wir als Projektteam haben uns darauf geeinigt, dass wir unter diesem Punkt eine komplette Remotesteuerung verstehen. Ein entsprechendes Beispiel wäre das Auswählen eines Dokumentes zentral und ein sofortiges Öffnen dieses Dokumentes am Clientdevice. Für dieses Anliegen stellen die Produkte der Produktlinie Mobile@Work keine Funktion zur Verfügung und können somit nicht komplett als erfüllend angenommen werden.

Die meisten Anforderungen sind bereits durch das MDM System alleine abgedeckt worden. Wenige zusätzliche können einerseits durch Web@Work und andere durch Apps@Work realisiert werden.

5.5.1 Zusätzlich erfüllte Anforderungen

1) User Daten (zB. Browser History, Spielstände, Bookmarks) können gelöscht werden

Web@Work lässt dem Administrator die Möglichkeit offen, bisherige Daten, wie zum Beispiel die History und die Bookmarks, zu löschen. In der Regel passiert dies sobald die Zugangserfordernisse nicht erfüllt sind. Benutzer des Devices selbst können das Tablet jedoch nicht auf den ursprünglichen Standard zurücksetzen. Somit ist die Anforderung für den Gebrauch nicht ganz erfüllt.

2) Ressourcen (Dokumente, Videos, Bilder, etc) kann man per Remote verwalten/verändern

Docs@Work gewährt einen Verbindungsaufbau mit einem Content Repository eines Unternehmens. Mit Hilfe dieser Verknüpfung können Dokumente einzelnen Usern oder auch Gruppen zur Verfügung gestellt werden. Jedoch ist wie bereits oben genauer beschrieben ein kompletter Remote Zugriff nicht möglich.

3)Apps können per Remote verwaltet werden

Administratoren können Apps zur Installation freischalten und somit deren Installation erlauben.

6 Samsung Knox

Dieser Abschnitt beschäftigt sich mit dem Einsatz von Samsung Knox als System für potentielle Kunden von der Firma Kapsch. Hier befindet sich sowohl Informationen zu Samsung Knox im Allgemeinen, als auch jene, welche von der Firma Kapsch erwünschten Features mit Samsung Knox, die realisierbar sind und welche nicht. Außerdem wird noch auf die Bedienbarkeit und die Installation eingegangen.

6.1 Allgemeine Infos zu Samsung Knox

Name:	Samsung Knox
Manufacturer:	Samsung
Current Version:	2.1
Publishing Date:	08.07.2014
Price:	• Express (E): free but limited to 250 seats • Premium (P) : USD $1 MSRP per device/month • Workspace (W) : USD $3.60 MSRP per device/month
Website:	https://www.samsungknox.com/de
Documentation:	

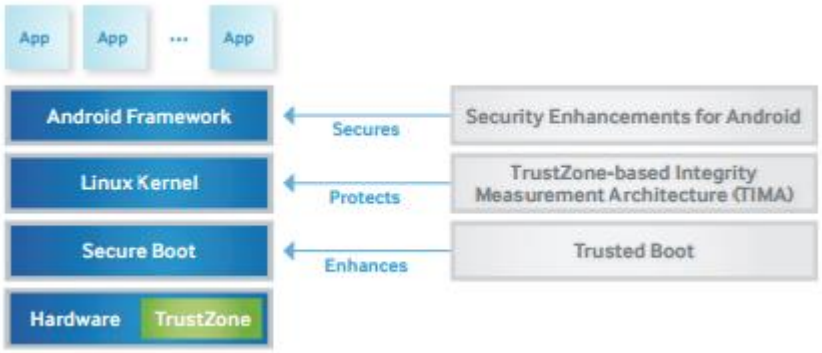
Samsung Knox ist eine Sammlung businessorientierter Sicherheitsfunktionen für Android-Geräte von Samsung. Das System, welches auf SE for Android basiert, ist speziell auf die Bedürfnisse von Unternehmen in Hinsicht auf die Sicherheit der Endgeräte ausgerichtet.

6.2 Samsung Knox Bestanteile

Um wirklich erklären zu können was Samsung Knox ist, muss man es zuerst einmal in seine 3 Hauptbestandteile unterteilen.

a. Plattform Security

In jedem Samsung Gerät ist ein physischer Hardware Chip eingebaut, welcher automatisch einen höheren Schutz für Samsung Geräte bieten soll. Mittels diesem Chip ist es Samsung möglich, bis in die tiefste Software-Schicht eines auf Android basierenden Geräts einzugreifen.



In der Grafik links sieht man den groben Aufbau eines Android Systems.In der Grafik rechts sieht man die Technologien, mit deren Hilfe es Samsung möglich ist in die Schichten einzugreifen.

a.1. Kerntechnologien der Plattform Security

a.1.1.SE for Android

a.1.1.1.So funktioniert es

SE for Android basiert auf SELinux-Technologie und definiert die Zugriffskontrolle auf Linux-Ebene. Mandatory Access Control (MAC) und Discretionary Access Control (DAC) überwachen und verwalten welche Dateien und Apps auf das System des Geräts zugreifen können.

a.1.1.2.Sicherheit

SE for Android erzwingt MAC, wobei Apps nur genau die Rechte zugewiesen erhalten, die sie für den Zugriff auf das System des Geräts benötigen. Sollte ein böswilliger Benutzer oder eine bösartige App also Zugriff auf das Gerät erhalten, dann betrifft der Schaden immer nur einen bestimmten Bereich, während die restlichen Bereiche des Geräts geschützt bleiben.

Wenn SE for Android ausgelöst wird, sendet es eine Präventionsinformationsmeldung an den Benutzer des Geräts, die in der **Informationsleiste** erscheint. Die Präventionsinformationsmeldung gibt an, welche Anwendung versucht hat, auf Daten des Geräts zuzugreifen, und sie wird die Deinstallation der betreffenden Anwendung empfehlen. Beachten Sie dabei jedoch, dass SE for Android auch von autorisierten Anwendungen ausgelöst werden kann. Dies kann vorkommen, wenn die App einen von dem in der SE for Android-Richtlinie vorgegebenen Pfad verwendet. Wenn dies der Fall ist, sollten man die Datei der Sicherheitsrichtlinie entsprechend aktualisieren.

a.1.2.ARM TrustZone-basierte Integrity Measurement Architecture (TIMA)

a.1.2.1.So funktioniert es

TIMA schützt Ihr Gerät auf zwei verschiedene Weisen. Erstens prüft sie in regelmäßigen Abständen, ob der Kernel des Geräts geändert wurde, indem sie den gegenwärtigen Zustand mit dem Original-Kernel vergleicht. Zweitens authentifiziert TIMA Kernel-Module, wenn diese geladen werden, sodass Geräte nie ungeschützt sind.

a.1.2.2.Sicherheit

Die TIMA TrustZone ist ein manipulationssicherer Sektor des ARM-Prozessors in Ihrem Gerät. Sie authentifiziert und verifiziert den Linux-Kernel über regelmäßige Messungen. Wenn TIMA for Android ausgelöst wird, sendet es eine Ermittlungsinformationsmeldung an den Benutzer, die in der Informationsleiste erscheint. In der Meldung wird man normalerweise zum Neustart des Geräts aufgefordert.

a.1.3. *Secure Boot und Trusted Boot*

a.1.3.1. So funktioniert es

Secure Boot verhindert, dass unbefugte Bootloader und Kernels in das Gerät geladen werden. Dies bedeutet, dass das Gerät nicht manipuliert wurde und der KNOX-Container geladen werden kann.

Trusted Boot vergleicht den Bootloader und den Kernel des Betriebssystems mit den originalen Werksversionen. Dies wird dadurch erreicht, dass die Originaldaten des Geräts aufgezeichnet werden und das Gerät permanent beim Systemstart mit diesen gegengeprüft wird, um sicherzustellen, dass sich diese Daten nicht geändert haben.

a.1.3.2. Sicherheit

Es gibt 4 Bootloader auf dem Gerät. Jeder Bootloader prüft die Gültigkeit des vorhergehenden Bootloaders oder Kernels. Trusted Boot sichert diese Bootloader. Die Funktion ist in der ARM TrustZone, einem manipulationssicheren Sektor des ARM-Prozessors, eingebettet. Trusted Boot verwendet kryptografische Schlüssel, um sicherzustellen, dass die Messungen am Gerät dem Original entsprechen. Diese Schlüssel werden erst von Trusted Boot freigegeben, wenn SE for Android bestätigt, dass genehmigte Firmware auf dem Gerät ausgeführt wird.

b. Applikation Security

Der Bereich Application Security bietet folgende drei Sicherheitsfunktionen:

b.1. Application Containers

Container sind quasi ein Android im Android und bezeichnet einen gesicherten, separaten Bereich (Container) auf dem Gerät. Dieser Bereich hat einen eigenen Homescreen, eigene Anwendungen und eigene Daten. Diese Funktion ist somit vergleichbar mit einer Art Dual-Boot-Variante. Anwendungen außerhalb des Containers haben dabei keinerlei Zugriff auf die Daten oder Prozesse innerhalb des Containers. Anwendungen innerhalb des Containers haben grundsätzlich keinen Zugriff auf Daten außerhalb des Containers.

Mittels Richtlinienkonfiguration kann der IT-Verwalter des Gerätes einen read-only (nur lesen) Zugriff für bestimmte Anwendungen im Container auf Daten außerhalb des Containers einrichten. Umgekehrt besteht diese Möglichkeit allerdings nicht. Daten innerhalb des Containers werden dabei mit einem Verschlüsselungsalgorithmus und einem AES-256 Bit Schlüssel geschützt. Ein Zugriff ist erst nach Eingabe eines Passwortes möglich.

b.2. On-device Data Encryption (kurz ODE)

ODE ist ein im Knox enthaltenes Feature zur Verschlüsselung von Daten. Dabei kann sowohl der sichere Container als auch der normale Bereich, sowie interner als auch externer Speicher verschlüsselt werden. Verwendet wird ein AES Algorithmus mit einem 256 Bit starken Schlüssel. Die Verschlüsselungsfunktion kann vom User selbst unter den Einstellungen oder vom IT Administrator durch eine Richtlinie aktiviert werden.

b.3. Virtual Private Network Support

VPN-Verbindungen verwendet man um sicherzustellen, dass Daten bei der Übertragung geschützt sind und um den Netzwerkverkehr nicht mit den Daten von persönlichen Apps zu belasten.

b.3.1. So funktioniert es

KNOX Workspace bietet 3 VPN-Optionen für den Schutz der Daten bei der Übertragung. Ein geräteweites VPN kann von Benutzern konfiguriert werden, sofern sie den entsprechenden Servernamen und die dazugehörigen Informationen zur Hand haben. VPN pro App oder ein containerweites VPN kann von IT-Administratoren über die MDM-Konsole eingerichtet werden. Auf der MDM-Konsole kann man bis zu 5 verschiedene VPN-Profile einrichten und diese einzelnen Apps zuweisen, um VPN pro App zu implementieren.

b.3.2. Sicherheit

VPN-Verbindungen sind die sicherste Methode, um die Daten bei der Übertragung zu schützen. Der KNOX VPN-Client kann ein bestehendes VPN-Gateway für den Schutz von Daten verwenden. KNOX VPN ist über Ihre MDM-Konsole im FIPS-Modus konfigurierbar. Zu den Sicherheitsfunktionen gehören NSA-Suite-B-Algorithmen, Unterstützung für X.509 mit Zertifikatsprüfung auf OCSP-Basis und 256-Bit-AES-Verschlüsselung. Wenn Ihr Unternehmen SmartCards verwendet, können diese mit VPN-Anmeldedaten konfiguriert werden.

c. Management (MDM)

Mit MDM (Mobile Device Management) bietet Samsung Knox der IT-Abteilung des Unternehmens die Möglichkeit eine integrierte Lösung zur Verwaltung und Administration von Samsung-Geräten vorzunehmen, ohne dabei auf Drittanbieter zurückgreifen zu müssen. Der Nachteil dabei ist die ausschließliche Verwendung mit Samsung-Geräten, welche über Samsung Knox verfügen.

Samsung Knox gibt es in 2 Varianten, wobei beide Varianten ein MDM als Basis benötigen um zu funktionieren.

c.1. Knox Lösungen

c.1.1. Knox Express

Diese Lösung ist für kleine bis mittelständische Unternehmen gedacht. Sie ist gratis, jedoch limitiert auf 250 Geräte.

Falls die 250 Plätze nicht mehr reichen, kann man Knox Express problemlos auf Knox Premium updaten.

Das ist die Variante, die die Projektgruppe empfehlen würde, da sie gratis ist und da laut Angaben von der Firma Kapsch es eher unwahrscheinlich ist, dass ein Kunde mehr als 250 Geräte hat, und falls doch, ist es ja problemlos auf Premium erweiterbar.

c.1.2. Knox Premium

Diese Komplettlösung eignet sich ideal für Unternehmen, in denen Sicherheit oberste Priorität hat.

Knox Premium kostet pro Gerät pro Monat 1 $ und kann um zusätzliche Add-ons erweitert werden.

Weiters bietet Knox Premium einige zusätzliche Features für Android und eine bessere IOS Integration. In Hinblick auf die von Kapsch erwünschten Funktionalitäten bringen diese zusätzlichen Features jedoch keine Vorteile.

c.1.2.1. Add-ons

c.1.2.1.1. Knox Workspace

Knox Workspace ist eine Erweiterung im Bereich Container.

Dieses Add-on bietet eine einfachere Konfiguration, zwei Container pro Gerät, zusätzliche Apps und verbesserte Sicherheitsfunktionen.

Die Hauptfeatures, die Workspace mit sich bringt, sind:

- Erweiterte Containerverwaltung mit sicheren Richtlinien
- Datenverschlüsselung bei jedem Entsperren des Containers
- Pro-App-VPN für sichere und schnelle Verbindung
- Support für zwei separate Container für maximale Produktivität und für Trennung von arbeitsbezogenen und privaten Daten

All diese Einstellungen, die mit Knox Workspace dazu kommen, gelten nur innerhalb des Containers. Da es jedoch keine Einstellung gibt um zu verhindern, dass der Benutzer den Container verlässt und somit alle Workspace-Einstellungen umgeht, ist dieses Add-on in unserem Fall ungeeignet.

Jedoch soll in Zukunft eine Art Contaier-only-mode implementiert werden. Sobald dieser vorhanden ist, wäre Knox Worspace auf jeden Fall ein Add-on das in Betracht gezogen werden sollte

c.1.2.1.2. Knox IAM

Knox IAM ist eine SSO-Lösung (Single Sign-On-Lösung).

Das heißt mit dem IAM Add-on hat man nur mehr einen einzigen Account, mit den man sich in allen Apps anmelden kann.

c.2. MDMs

Knox bietet zur Verwaltung der Geräte ein eigenes MDM, das EMM, hat aber auch genügend Partner, deren MDMs Samsung Knox Funktionen implementiert haben.

Samsung Knox funktioniert also mit jedem MDM aus der nachfolgenden Liste.

c.2.1. Liste an kompatiblen MDMs

- Samsung EMM
- MobileIron
- Absolute Software
- AirWatch
- CA Technologies
- Centrify
- Citrix
- FancyFon
- MaaS360
- NQ Mobile
- Samsung SDS
- SAP
- SOTI

c.2.2. Samsung EMM

Samsung KNOX EMM ist eine cloudbasierte Verwaltungslösung für Unternehmen. IT-Administratoren können damit Benutzer, Apps und plattformübergreifende Geräte über eine cloudbasierte Konsole verwalten. Außerdem bietet KNOX EMM Single Sign-On (SSO) und eine starke Authentifizierung für eine benutzerfreundliche und sichere Arbeitsumgebung für Mitarbeiter.

Es ist einfach zu installieren und sehr übersichtlich gestaltet. Falls in der Firma noch keine andere MDM Lösung installiert sein sollte, ist EMM zu empfehlen.

6.3 Unterstützte Geräte

Ein riesiger Nachteil an Samsung Knox ist, dass ungefähr 90% aller Funktionen bei folgenden Geräten einstellbar sind:

- **ab KitKat 4.4.4**
  - Galaxy Note 4
- **ab KitKat 4.4.2**
  - Galaxy S5
  - Galaxy Avant
- **ab Jelly Bean 4.3**
  - Galaxy S4
  - Galaxy S3
  - Galaxy Note 3
  - Galaxy Note 2
  - Galaxy Express 2
  - Galaxy Grand
  - Galaxy NotePro 12.2
  - Galaxy Note 10.1
  - Galaxy Note 8.0
  - Galaxy Tab S
  - Galaxy TabPro
  - Galaxy Tab 4
  - Galaxy Tab 3
- **ab Jelly Bean 4.2.2**
  - Galaxy Mega
- **In jeder Version**
  - Galaxy Alpha
  - Galaxy Note Edge
  - Galaxy Ace
  - Galaxy Core

6.4 Erfüllte Funktionen

Dieser Abschnitt beschäftigt sich damit, welche für unser Projekt wichtigen Funktionen Samsung Knox mit sich bringt.

6.4.1 Kernfunktionen

Unter Kernfunktionen fallen die Funktionen die benötigt werden um den Anforderungen von der Firma Kapsch gerecht werden zu können.

6.4.1.1 Allgemeine Funktionen

- Nutzbar ohne Public Cloud Services
  - Samsung Knox ist so konfigurierbar, dass man keine Public Cloud Dienste verwenden muss.
- Keiner speziellen Person zugewiesen
  - Samsung Knox ist so konfigurierbar, dass das Gerät anonym bleibt, also keiner speziellen Person zugewiesen ist.
- Der Sperrbildschirm der Geräte kann fernverwaltet werden
  - Hintergrund des Sperrbildschirms kann geändert werden
  - Passwort für den Sperrbildschirm kann gesetzt werden

6.4.1.2 Inhaltseinstellungen (Apps,Webseiten, Marketing)

- Installieren von Apps kann verboten werden
- Dem Benutzer kann das Recht zur Verstellung der Systemeinstellungen genommen werden.
- Browserinhalt und bestimmte URLs können gefiltert werden
  - Für die Geräte ist es möglich einen Proxy-Server einzustellen. Durch das Konfigurieren dieses Servers kann man dann den Inhalt, den man filtern will, filtern.
- Remote Zugriff ist möglich
  - Das heißt man kann über das Internet mit Hilfe der Admin Konsole auf die Geräte zugreifen

6.4.1.3 Statistiken

- Es ist möglich, sogenannte Berichte generieren zu lassen
  - Das einzige Problem daran ist, dass man sie dafür erst selbst mittels SQL „programmieren“ muss.
  - Genauere Informationen über die Funktionsweise findet man unter https://emm3.samsungknox.com/vfslow/lib/docs/samsung/adminref/wwhelp/wwhimpl/js/html/wwhelp.htm#href=cloud-admin-reports.html
  - Informationen zum Syntax der SQL-Queries gibt es unter https://emm3.samsungknox.com/vfslow/lib/docs/samsung/adminref/wwhelp/wwhimpl/js/html/wwhelp.htm#href=cloud-admin-sql-func-exa.

6.4.1.4 Benutzer und Geräte

- Geräte können zum Auslieferungszustand zurückgesetzt werden

6.4.1.5 Managementseitige Anforderungen

- Geräteverwaltung ist von mehreren Standorten möglich
- Geräte inklusive Status können angezeigt werden
- Geräte können per remote auf den Auslieferungszustand zurückgesetzt werden
- VPN Einstellungen können mittels remote geändert werden
- Passwort Richtlinien können definiert werden
- Die Statistiken sind per remote auslesbar

6.4.1.6 *Zusätzliche Anforderungen*

- Das Gerät ist benutzbar ohne Kiosk-Modus
  - Im Kiosk-Modus kann man nur genau eine einzige App verwenden.
- Die Lösung ist nicht auf nur eine einzige Hardware beschränkt
  - Dies funktioniert jedoch nur mit den zuvor genannten unterstützten Geräten.
- Bestimmter Inhalt kann gefiltert werden
  - Es ist möglich für die Geräte einen Proxy-Server einzustellen. Durch das Konfigurieren dieses Servers kann man dann den gewünschten Inhalt filtern.
- Mehrsprachen Unterstützung
  - Samsung Knox unterstützt folgende Sprachen:
    - Englisch
    - Spanisch
    - Französisch
    - Deutsch
    - Italienisch
    - Portugiesisch
    - Brasilianisches Portugiesisch
    - Einfaches Chinesisch
    - Traditionelles Chinesisch
    - Koreanisch
    - Japanisch

6.4.2 Zusätzliche Funktionen

Darunter fallen Funktionen, die zwar nicht explizit von der Firma Kapsch erwünscht wurden, jedoch eventuell für die Firma Kapsch interessant sein könnten.

- Verschlüsselung
  - Geräte Verschlüsselung
  - Interne Speicher Verschlüsselung
  - SD Karten Verschlüsselung
- Management von Geräten
  - Mittels remote kann man
    - das Gerät zum Auslieferungszustand zurücksetzen
    - das Passwort des Geräts ändern
    - das Gerät lokalisieren
    - feststellen, ob die SIM-Karte im Gerät getauscht wurde
    - maximale Anzahl an falsch eingegebenen Passwörtern setzen
    - Firewall Einstellungen ändern
    - Whitelists und Blacklists einrichten für
      - Bluetooth
      - Wlan
    - Protokollierung von Anrufinformationen aktivieren
    - Protokollierung von Netzwerkstatistiken für Mobilfunkdaten aktivieren
    - Protokollierung von WLAN-Netzwerkstatistiken aktivieren
- Funktionen des Geräts für den Benutzer erlauben/verbieten
  - App Benachrichtigungen
  - Kamera
  - Mikrofone
  - USB- tethering
  - Bildschirm Übertragungen

- Screenshots
- USB-Debugging
- S-Voice
- Aufnahmen
  - Video
  - Audio
- Datum und Zeit Änderungen
- Roaming
- SMS
  - Senden
  - Empfangen
- Bluetooth-Einstellungen ändern
- Wlan-Einstellungen ändern

6.5 Fehlende Funktionen

Folgende von der Firma Kapsch erwünschte Funktionen sind mit Samsung Knox nicht realisierbar:

6.5.1 Inhaltseinstellungen(Apps, Webseiten, Marketing)

- Deinstallieren von Apps kann verboten werden
- Standard Apps können ausgeblendet werden
  - Bei Samsung Knox Premium wäre das möglich, da man dort einstellen kann, welche Apps vom Benutzer geöffnet werden können.
- App Content kann fernverwaltet werden
- Per remote können bestimmte Webseiten am Gerät geöffnet werden
- Der Inhalt der Geräte (Bilder, Videos, etc.) kann fernverwaltet werden.
- Der Sperrbildschirm der Geräte kann fernverwaltet werden
  - Hintergrund des Sperrbildschirms kann geändert werden
  - Passwort für den Sperrbildschirm kann gesetzt werden
- Der Hintergrund der Geräte kann fernverwaltet werden

6.5.2 Benutzer und Geräte

- Es ist möglich das Gerät auf einen beliebigen zuvor definierten Zustand zurückzusetzen.
- Es ist möglich gewisse Benutzerdaten(History, Highscores, Lesezeichen, etc.) zu löschen
- Das Gerät setzt sich nach einer gewissen Zeit automatisch auf einen bestimmten Zustand zurück.

6.5.3 Managementseitige Anforderungen

- Fehler Berichte sind per Gerät und per Standort auslesbar.
  - Per Gerät
  - Per Standort

7 Endergebnis und Empfehlung

Nach Abschluss des Evaluierungsprozesses ist das Projektteam an diesem Punkt in der Lage eine Empfehlung an das Unternehmen Kapsch auszusprechen. In diesem Teil wird nun erläutert, welches evaluierte Konzept mit den Anforderungen des Auftraggebers übereinstimmt und wodurch dies zu Stande gekommen ist. Nachdem die Linuxmanipulation aus Garantie technischen Gründen bereits als ausgeschieden gilt, befasst sich der folgende Abschnitt nur mehr mit den Konzepten MDM, MDM + Container und Samsung Knox.

7.1 Evaluierung

Um feststellen zu können welche der 3 Lösungen am besten die Anforderungen des Auftraggebers erfüllen kann, hat das Projektteam eine Nutzwertanalyse erstellt, mit derer Hilfe das Projektteam die Funktionen der Systeme direkt miteinander vergleichen konnten.

Nutzwertanalyse ERP Lösung		max. Punkte	Gewicht	MDM	Bewertung	MDM+ Container	Bewertung	Samsung Knox	Bewertung
Allgemein			**8**						
	Nutzbar ohne Public-Cloud-Services		3	10	30	10	30	10	30
	Keiner speziellen Person zugewiesen		5	10	50	10	50	10	50
Nutzwert Allgemein		***80***			**80**		**80**		**80**
Inhaltseinstellung			***44***						
	Installieren von Apps kann verboten werden		6	7	42	7	42	10	60
	Deinstallieren von Apps kann verboten werden		6	3	18	3	18	0	0
	Kein benutzerseitiger Zugang zu Systemeinstellungen		8	10	80	10	80	10	80
	Standard Apps können ausgeblendet werden		2	2	4	2	4	2	4
	Browser Inhalt kann gefiltert werden		4	10	40	10	40	10	40
	Remote-Zugriff ist möglich		8	10	80	10	80	10	80
	Apps können per remote verwaltet werden		5	6	30	8	40	10	50
	Websiten können per remote verwaltet werden		2	0	0	0	0	0	0
	Inhalt (Dokumente, Videos, Bilder) können per remote verwalten können		1	0	0	8	8	0	0
	Hintergrund und Speerbildschirm können per remote verwalten können		2	5	10	5	10	5	10
Nutzwert Inhaltseinstellungen		***440***			**304**		**322**		**324**
Statistik			***7***						
	Up/Down-Time einsehbar		3	10	30	10	30	10	30
	Statistiken sind pro Device und Standort auslesbar		3	10	30	10	30	10	30
	Statistiken über Aktivitätszeit, App aufrufe und Websiten		1	4	4	4	4	10	10
Nutzwert Statistik		***70***			**64**		**64**		**70**
Benutzer und Geräte			***10***						
	Geräte können zu einem spezifischen Status zurückgesetzt werden		5	3	15	3	15	3	15
	Benutzerdaten (History, Spielstände, Lesezeichen) können gelöscht werden		3	3	6	4	12	3	9
	Automatisches Zurücksetzen der Geräte nach einer Zeiteinheit		2	0	0	0	0	0	0
Nutzwert Benutzer und Geräte		***100***			**24**		**27**		**24**

Managementseitige Anforderungen			***20***						
	Geräteverwaltung von mehreren Standorten möglich		3	10	30	10	30	10	30
	Geräte (inkl. deren Status) können angezeigt werden		4	10	40	10	40	10	40
	Fehlerberichte sind pro Gerät und pro Standort verfügbar		4	7	28	7	28	9	36
	Geräte können zu einem spezifischen Status per Remote zurückgesetzt werden		5	3	15	3	15	3	15
	Statistiken können per remote ausgelesen werden		3	10	30	10	30	10	30
	Inhalt (Dokumente, Videos, Bilder) können per remote geändert werden		1	0	0	8	8	0	0
Nutzwert Mangementseitige Anforderungen		***200***			**143**		**151**		**151**
Zusätzliche Anforderungen			***11***						
	Gerät ohne Kiosk-Mode verwendbar		5	10	50	10	50	10	50
	Hardwareunabhängig		1	10	10	10	10	10	10
	Geringer Wartungsaufwand		2	10	20	10	20	10	20
	Mehrsprachen Unterstützung		2	10	20	10	20	10	20
	Einsetzbar ab dem ersten Gerät		1	0	0	0	0	10	10
Nutzwert Zusätzliche Anforderungen		***110***			**100**		**100**		**110**

Nutzwert Gesamt		*100*			715		744		759
Rang Nutzwert					**3**		**2**		**1**

Kosten		*10*			6		4		10
Rang Kosten					**2**		**3**		**1**

Kosten/Leistungsverhältnis - Kosten je Pkt.					118,67		186,00		75,90
Rang Kosten/Leistungsverhältnis					**2**		**3**		**1**

7.2 Auswertung der Evaluierung

Um ein aussagekräftiges Ergebnis zu erhalten, wurden die Anforderungen des Gesamtsystems in verschiedene Unterpunkte unterteilt, welche auf ihre Funktionstüchtigkeit hin untersucht wurden.

Die Lösungen wurden dann je nach Erfüllungsgrad der einzelnen Punkte bewertet, was eine objektive Vergleichbarkeit schaffen sollte.

7.2.1 Allgemein

Da alle 3 Systeme sowohl ohne pulic-cloud-service nutzbar waren als auch keiner speziellen Person zugewiesen werden müssen, haben alle 3 Lösungen die volle Punkteanzahl erreicht und sind somit, was diesen Punkt angeht, gleich auf.

7.2.2 Inhaltseinstellungen

In diesem Bereich, hat sich herausgestellt, ist Samsung Knox kapp aber doch noch vor der MDM+Container Lösung das am besten geeignete System. Denn auch wenn es mit MDM+Containern möglich ist, die Deinstallation von betriebsinternen Apps zu verbieten und man auch Inhalte der Geräte wie zum Beispiel Bilder, Dokumente, etc per remote verwalten kann, ist Samsung hier die bessere Alternative, da es eine bei weitem bessere Verwaltung von Apps per Remote bietet.

Eine Anforderung die jedoch keines der drei Systeme erfüllen konnte, war das Verwalten von Websiten per remote.

7.2.3 Statistik

Auch den Unterpunkt „Statistiken“ kann Samsung Knox wieder für sich entscheiden. Diesmal jedoch mit einem größeren Vorsprung. Zurückzuführen ist das darauf, dass Samsung Knox die Möglichkeit bietet, sich jede beliebige Statistik die man für sein Unternehmen haben will, einfach mittels SQL Code selbst zu erzeugen (siehe Punkt 6.4.1.3 Statistiken).

7.2.4 Benutzer und Geräte

In diesem Bereich kann die MDM+Container Lösung punkten. Denn im Gegensatz zu den anderen zwei Systemen, kann man mit dieser Lösung am Gerät gespeicherte Lesezeichen löschen.

Auch bei diesem Unterpunkt gibt es wieder eine Anforderung die mit keinem unserer getesteten Systeme umsetzbar war. Und zwar war es nicht möglich die Geräte so zu konfigurieren, dass sie sich nach einer gewissen Zeit von alleine auf einen definierten Stand zurücksetzen.

7.2.5 Managementseitige Anforderungen

Bei der Erfüllung der managementseitigen Anforderungen sind Samsung Knox und die MDM+Container-Lösung gleich auf. Denn den Vorsprung den Knox gewinnt durch besseres Handling der Fehlerberichte, kann die MDM+Container-Lösung dadurch wegmachen, das sie im Gegensatz zu Samsung Knox eine Möglichkeit bietet, Geräteinhalt per remote zu ändern.

7.2.6 Zusätzliche Anforderungen

Da Samsung Knox das einzige System ist, welches bereits ab dem ersten Gerät einsetzbar ist und sonst alle Punkte von allen Systemen erfüllt werden ist auch hier Knox der klare Sieger.

7.3 Empfehlung

Nach eingehender Analyse ist das Projektteam zu dem Schluss gekommen, dass für die geplanten Projekte der Firma Kapsch BusinessCom AG die Betriebsplattform Samsung Knox am ehesten geeignet ist. Es implementiert die meisten der benötigten Features, aber lässt dennoch einige fundamentale Punkte aus. Deshalb ist es hier für das Projektteam auch nicht möglich eine hundert prozentige Empfehlung zu geben. Den Informationen der Dokumentation von Samsung Knox zur Folge werden einige benötigte Features in kommenden Versionen eingebaut. Allerdings ist nicht absehbar ob und wann diese erscheinen. Für die beiden anderen Systeme kann deshalb keine Empfehlung ausgesprochen werden, weil sie weniger und besonders im Einsatz mit Nicht-Samsung-Geräten signifikant weniger Funktionen bieten.