UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

TADEJ PREŠEREN

# CELOVITI PRISTOP OBVLADOVANJA MOBILNIH NAPRAV V FARMACEVTSKEM PODJETJU

**MAGISTRSKO DELO**

Ljubljana, 2008

UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

TADEJ PREŠEREN

# CELOVITI PRISTOP OBVLADOVANJA MOBILNIH NAPRAV V FARMACEVTSKEM PODJETJU

**MAGISTRSKO DELO**

Mentor: doc. dr. Marko Bajec

Ljubljana, 2008

# Zahvala

Zahvaljujem se doc. dr. Marku Bajcu za strokovne nasvete in priporočila pri izdelavi magistrske naloge ter podjetju Krka,d. d., Novo mesto, ki mi je omogočilo dostop do različnih virov za raziskovalno delo.

Za strokovne nasvete in priporočila pri izdelavi magistrske naloge se zahvaljujem tudi kolegu mag. Boštjanu Žvanutu.

Posebna zahvala gre moji zaročenki Katji Može, ki je kljub številnim večernim uram, ki sem jih zaradi raziskovalnega dela preživel za računalnikom in literaturo, spodbujala moje želje po nadaljnjem strokovnem izpopolnjevanju. Zahvala gre tudi staršema Janezu in Sonji, bratu Alešu in sestri Petri ter vsem, ki so mi stali ob strani v celotnem obdobju študija.

# Kazalo vsebine

# Kazalo slik



# Kazalo tabel

## Slovar tujk

| | |
|---|---|
| **AI** | Acquire and implement |
| **AS** | Aplikacijski strežnik |
| **ATM** | Asynchronous Transfer Mode |
| **BSI** | British Standard institute |
| **CCTA** | Central Computer and Telecommunications Agency |
| **CDMA** | Code division multiple access |
| **CFP** | Capability Provision Functionality |
| **CIM** | Commo Information Model |
| **COBIT** | Control Objectives for Information and related Technology |
| **CRC** | Capability Retreive Component |
| **CRM** | Customer relationship management |
| **DMEU** | Device Management Execution Unit |
| **DMTF** | Distributed Management Task Force |
| **DMZ** | Demilitarized zone |
| **DS** | Deliver and Support |
| **ERP** | Enterprice resource planning |
| **FMC** | Fixed Mobile Convergence |
| **FTP** | File transfer protocol |
| **GPRS** | General Packet Radio Service |
| **GSM** | Global System for Mobile communications |
| **HSDPA** | High Speed Downlink Packet Acces |
| **HTTP** | HyperText Transfer Protocol |
| **IDC** | International Data Corporation |
| **IMS** | IP Multimedia Subsystem |
| **IP** | numerična identifikacija naprave na omrežju |
| **IPM** | Personal Information Management |
| **ISA** | Microsoft Internet Security and Acceleration Server |
| **ISO/IEC** | International Organization for Standardization/International Electrotechnical Commission |
| **IT** | Informacijska tehnologija |
| **ITGI** | Information technology Governance Institute |
| **ITIL** | Information technology infrastructure library |
| **LDAP** | Lightweight Directory Access Protocol |
| **MDM** | Mobile Device Management |
| **MDMS** | Master Device Management Server |
| **ME** | Monitor and evaluate |
| **MMS** | Multimedia Messaging Service |
| **NCC** | National Computing Centre |
| **OBEX** | OBject Exchange |
| **OGC** | Office of Government Commerce |
| **OMA-DM** | OMA Device Management |
| **ORC** | Opinion Research Corporation |
| **PC** | Personal Computer |

| | |
|---|---|
| **P-CSCF** | Prox-Call Session Control Function |
| **PDA** | Personal Digital Assistant |
| **PDCA** | Plan-Do-Check-Act model |
| **PIN** | Personal Identification Number |
| **PO** | Plan and organize |
| **SDP** | Session Description Protocol |
| **SIP** | Session Initiation Protocol |
| **SKMS** | Service Knowledge Management System |
| **SLA** | Service Level Agreement |
| **SLP** | Service Location Protocol |
| **SMB** | Smart Box Manager |
| **SMS** | Short message service |
| **SNMP** | Simple network management protocol |
| **SOAP** | Simple Object Access Protocol |
| **SUZS** | Sistem za upravljanje z znanjem storitev |
| **TAC** | Transport Adaptation Component |
| **TCO** | Total Cost of Ownership |
| **UMTS** | Universal Mobile Telecommunications System |
| **URL** | Uniform Resource Locator |
| **WAP** | Wireless Application Protocol |
| **WBEM** | Web-Based Enterprise Management |
| **WDSL** | Web Design Solution Limited |
| **WIFI** | Ime brezžične tehnologije |
| **WIMAX** | Worldwide Interoperability for Microwave Access |
| **WLAN** | Wireless local area network |
| **WSP** | Wireless Session Protocol |
| **XCAP** | XML Configuration Access Protocol |
| **XDSL** | Digital subscriber line |
| **XML** | Extensible Markup Language |

## Povzetek

Magistrsko delo z naslovom Celoviti pristop obvladovanja mobilnih naprav v farmacevtskem podjetju predstavlja smernice, ki jih je smiselno upoštevati pri vzpostavljanju sistema obvladovanja mobilnih naprav. V magistrskem delu sem skušal predstaviti, kako se lotiti upravljanja mobilnih, kajti le to področje se v zadnjem času izredno hitro razvija. Magistrsko delo zajema vse ključne korake, ki jih je potrebno upoštevati. Izdelan je bil pregled standardov ter priporočil na področju varnosti na mobilnih napravah. Podane so smernice, ki jih je smiselno upoštevati pri izdelavi varnostne politike, izdelana pa je tudi analiza tveganj za farmacevtsko podjetje. Podrobno je predstavljen model za upravljanje mobilnih naprav ter nato analiza orodij, ki so trenutno najpogosteje prisotna na trgu. V nalogi so podane tudi smernice nadaljnjega razvoja mobilnih naprav.



**Ključne besede:**

Informacijska varnost, mobilne naprave, ITIL, COBIT, ISO/IEC 27001, upravljanje mobilnih naprav, ocena tveganj, informacijska tehnologija.

## Summary

The areas of the mobile device management is developing very fast. Hence, the thesis "An approach for management of mobile devices in pharmaceutical company" introduces all key directives that should be considered when implementing mobile device management. A survey of standards and recommendations on the mobile device security has been elaborated. Relevant guidelines for security policy definition are presented with the risk analysis for mobile device usage. Furthermore, the model for managing mobile devices and tool analysis are given in detail. The thesis concludes with the introduction of further development of mobile devices.

**Key words:**

Information security, mobile devices, ITIL, COBIT, ISO/IEC 27001, mobile device management, risk assessment, information technology.

# 1 Uvod

## 1.1 Opredelitev problema

Vloga sodobne informacijske tehnologije (IT) se je od omejene uporabe osnovne IT razvila do razširjene in za poslovanje podjetja pomembne infrastrukture. Investicije v tako infrastrukturo so pomembne, še posebej glede vpliva te infrastrukture na poslovanje in stroške ter tveganja napačnih odločitev, da bi jih prepustili svojemu toku [33]. Do tega pojava je prišlo zaradi dejstva, da so sredstva IT za današnje uspešno poslovanje tako pomembna in draga, da jih je potrebno upravljati, vzdrževati ter nadzorovati. Podjetja, ki se zavedajo pomembnosti kakovostnega upravljanja sredstev IT, vedo, da ta sredstev predstavljajo temelj za realizacijo poslovne strategije organizacije. Prav tako se zavedajo, da brez učinkovite infrastrukture z visoko razpoložljivostjo ter stalnim zagotavljanjem ustreznega nivoja storitev danes ni moč uspešno poslovati.

Običajno je obvladovanje osebnih računalnikov farmacevtskih podjetjih zelo dobro podprto. Podjetja imajo za obvladovanje osebnih računalnikov določeno standardno platformo, procese, varnostno politiko ter tudi orodja, s katerim si pomagajo pri uresničevanju zastavljenih politik, procesov ter poslovnih potreb.

Dandanes je v uporabi vse več mobilnih komunikacijskih naprav. Naprave so vse manjše ter vse bolj zmogljive. Po funkcionalnostih se lahko že primerjajo z osebnimi računalniki.

Pogosto pa zasledimo, da je področje mobilnih naprav v podjetjih neurejeno. V podjetju, ki ga v magistrski nalogi obravnavamo, je v uporabi preko tisoč pametnih mobilnih naprav (npr. pametni mobilni telefoni, dlančniki, zmogljivejši mobilni telefoni...), število pa strmo narašča.

Mobilne naprave delujejo na različnih platformah in zagotavljajo različne funkcionalnosti. V obravnavanem farmacevtskem podjetju se na mobilnih napravah trenutno zagotavlja zgolj storitev elektronske pošte, vendar je lahko kljub temu na mobilnih napravah velika količina zaupnih ali strogo zaupnih podatkov.

Področje obvladovanja mobilnih naprav ter proces upravljanje konfiguracij na mobilnih napravah trenutno ni mogoče izvajati, pojavljajo se težave predvsem pri uvajanju novih storitev, ker je potrebno vpoklicati v storitveni center (ang. Service Desk) vse mobilne

naprave, na katerih bi želeli uporabljati novo storitev. To zahteva velike stroške, nered, nezadovoljstvo uporabnikov, slaba fleksibilnost, nizka odzivnost, ni poročil ter statistik o uporabi ter težavah na mobilnih napravah. V podjetju tudi ni celovitega sistema za varovanje in zaščito informacij v primeru izgube ali kraje mobilne naprave, ki bi ga potrebovali.

Ocenjujem, da ima uporaba mobilnih aplikacij v informacijskemu sistemu podjetja še veliko rezerve. Tako mobilne naprave, kot tudi njihovo obvladovanje, je novo področje v znanosti, ki se intenzivno razvija v zadnjih dveh desetletjih. Problem obvladovanja večjega števila mobilnih naprav je zanimiv ne samo v farmacevtskem podjetju, ampak v vseh združbah, kjer jih uporabljajo. Še večji poudarek pa je pri organizacijah, ki na mobilnih napravah zagotavlja storitve povezane z dejavnostjo podjetja (npr. elektronska pošta, mobilne aplikacije npr. aplikacije za upravljanje s strankami…) in imajo informacije na mobilnih napravah še večjo vrednost.

## 1.2 Raziskovalno področje

Živimo v informacijski dobi. To je čas, v katerem informacijska tehnologija nima več statusne vrednosti, temveč predstavlja tako posamezniku kot podjetjem osnovo, brez katere je praktično nemogoče uspešno funkcionirati. Mnoga podjetja so z informacijsko tehnologijo neločljivo povezana in si ne morejo predstavljati svojega obstoja in delovanja brez nje. Nihče se več ne sprašuje, ali so vlaganja v informatizacijo smiselna. Namesto tega se postavlja vprašanje, kako jo čim bolje izkoristiti, približati poslovanju in jo narediti učinkovitejšo, zanesljivejšo in bolj razpoložljivo[1].

Managerji se vedno bolj zavedajo vpliva informatike na uspešnost združbe. V današnjih časih je uporaba informacijske tehnologije pri poslovanju postala imperativ. Največjo prednost združba pridobi, ko se nauči uporabljati IT kot sredstvo ali mehanizem za dosego poslovnih ciljev [2].

Pomembno je spoznanje, da IT lahko obravnavamo kot enega ključnih virov združbe, pri čemer preostalih pet virov predstavljajo zaposlenci, finančni viri, fizični viri, intelektualna lastnina ter razmerja. Posledica te ugotovitve je, da je IT – tako kot ostale vire – potrebno upravljati, kar pa ni lahko, saj je od vseh virov najmanj razumljiv. Izkaže se, da je najpomembnejši prediktor dodane vrednosti, ki jo podjetju prinaša informatika, ravno učinkovito upravljanje [3].

Obvladovane mobilne naprave pripomorejo k lažjemu in učinkovitejšemu zagotavljanju storitev ter k boljši uporabniški izkušnji na mobilnih napravah[4]. Boljšo uporabniško izkušnjo pa zagotavlja tudi avtomatska konfiguracija mobilnih naprav [5]. Da je možno učinkovito obvladovati mobilne naprave je potrebno zagotoviti integracijo mobilnih naprav v IT infrastrukturo podjetja [6].

Pri vzpostavitvi sistema varovanja in zaščite informacij se je smiselno in koristno opreti na uveljavljene standarde in priporočila. Za potrebe določitve varnostne politike, za podjetja na področju mobilnih naprav, je potrebno izhajati iz krovne varnostne politike podjetja ter ostalih standardov in priporočil s področja varovanja informacij. Priporočila in standardi, iz katerih se priporoča izhajati, so [7]:

- Information Technology Infrastructure Library (ITIL) predstavlja zbirko najboljših praks za upravljanje informacijskih storitev [8].
- Control Objectives for Information and Related Technology (COBIT) je zbirka nadzornih ciljev, ki predstavljajo najboljšo prakso za upravljanje informacijske tehnologije [9].
- Standard BS 7799 je mednarodno uveljavljen standard za varovanje informacij. Predstavlja enega najbolj celovitih dokumentov na tem področju. Najnovejšo različico sestavljajo trije deli: prvi del BS ISO/IEC 17799:2005, drugi del BS ISO/IEC 27001:2005 ter tretji del BS 7799-3:2006 [10].

Z večanjem zmogljivosti mobilnih naprav se povečuje pomen zagotavljanja ustrezne avtentikacije uporabnikov na mobilnih napravah [11]. Potrebno bi bilo tudi raziskati možne ter smiselne načine uporabniške avtentikacije na mobilnih napravah in najprimernejšo integrirati v infrastrukturo podjetja in jo uskladiti z varnostno politiko.

Ker sta si zbirka nadzornih ciljev COBIT ter zbirka najboljših praks ITIL komplementarni [12], ju je smiselno uporabiti kot priporočila in izhodišča pri integraciji obvladovanja mobilnih naprav v obvladovanje celotne informacijske tehnologije v podjetju.

## 1.3 Namen in cilji magistrskega dela

Osnovni cilj magistrskega dela je vzpostavitev pristopa obvladovanja mobilnih naprav v podjetju. Vzpostavljen pristop obvladovanja mobilnih naprav v podjetju pa bo imel za

posledico nižje stroške upravljanja z mobilnimi napravami, zmanjšale se bodo varnostne grožnje, zaradi distribucije novih storitev »preko zraka« se bo povečala produktivnost uporabnikov. Zelo pomemben cilj je tudi zagotoviti obvladovanje mobilnih naprav in povečanje nivoja varnosti na njih, ne da bi se zmanjšala uporabnost oz. da se ne bi oviralo dela na mobilnih napravah.

Magistrska naloga bo koristila farmacevtskemu podjetju, v pomoč pa bo tudi vsaki organizaciji, ki se srečuje s podobnimi problemi. Naloga bo predstavila predvsem probleme ter nakazala možne rešitve, na koncu pa podrobneje prikazala najboljšo rešitev. Ker se tehnologije na področju mobilnih naprav izredno hitro razvijajo, je smiselno evidentirati tudi nove storitve, ki jih bo v prihodnosti mogoče ponuditi uporabnikom.

Magistrska naloga bo definirala celovit pristop k obvladovanju mobilnih naprav. Prispevala bo k razjasnitvi in definiranju procesa upravljanja s konfiguracijami mobilnih naprav in njegovo umestitev v obvladovanje celotne informacijske tehnologije v podjetju.

## 1.4 Metode dela

Pri magistrskem delu sem uporabil znanja, pridobljena na podiplomskem študiju na Fakulteti za računalništvo in informatiko v Ljubljani in izkušnje, pridobljene z delom na področjih informatike, informacijske varnosti ter informacijske infrastrukture.

Pri določanju varnostne politike podjetja za področje mobilnih naprav sem uporabil deskriptivno metodo na osnovi domače in tuje literature. Pri pisanju naloge pa so bila uporabljena tudi interna gradiva podjetja.

Z metodo primerjalne analize sem medsebojno primerjal glavna sodobna orodja za obvladovanje mobilnih naprav ter predlagano najprimernejše orodje za implementacijo v farmacevtskem podjetju. Z metodo analize so bila identificirane tudi potencialne storitve, ki bi jih bilo smiselno ponuditi uporabnikom.

Za preverjanje rezultatov magistrskega dela sem uporabil metodi opazovanja ter intervjuvanja.

# 2 Informacijska varnost na mobilnih napravah

Informacijska varnost je področje, ki se ukvarja z varovanjem podatkov pred nepooblaščenim dostopom, uporabo, razkritjem, uničenjem, spremembo ali razpoložljivostjo. Termini informacijska varnost, računalniška varnost ter varnost informacijskih sistemov (ang. Information assurance) se pogosto uporabljajo izmenično. Čeprav vsa tri področja delijo mnoge skupne lastnosti oz. imajo vsa skupen cilj v varovanju zaupnosti, celovitosti ter razpoložljivosti informacij, obstajajo med njimi razlike glede vidika, s katerega pristopajo k tem ciljem in načinov zagotavljanja le teh.

Definicija varnosti po ISO 17799:2005 se glasi [13]:

Informacijska varnost zagotavlja ohranitev zaupnosti, celovitosti in razpoložljivosti informacij; dodatno so lahko vpletene tudi druge lastnosti, kot so istovetnost, odgovornost, preprečevanja nepriznavanja in zanesljivost.

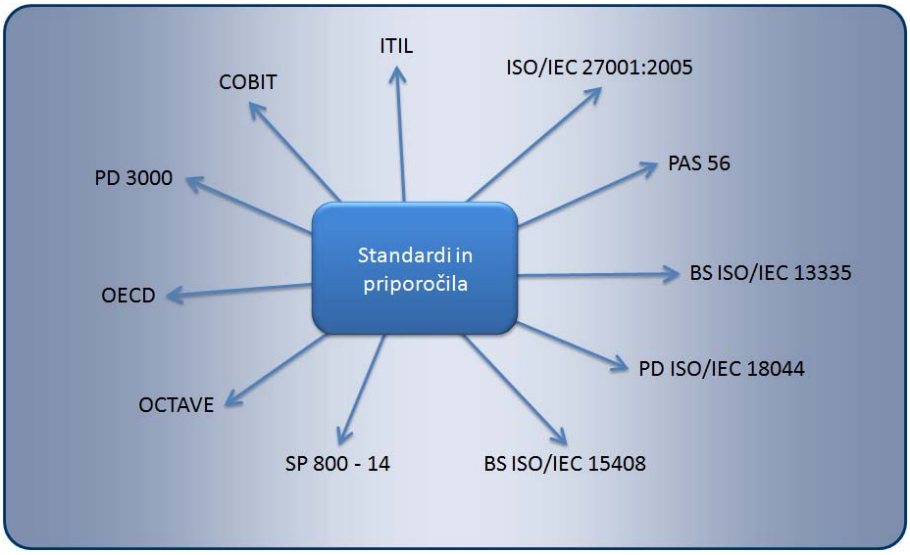

**Slika 1: Trije glavni cilji informacijske varnosti [14]**

Varnost informacijskih sistemov pristopa nekoliko drugače, tako da upošteva predvsem varovanje sistemov, ki omogočajo hrambo, procesiranje, predstavitev ali prenos informacij. Dodatno daje poudarek na vprašanje glede zasebnosti, upoštevanja zakonskih in drugih določil, neprekinjeno poslovanje ter okrevanje po katastrofi. Računalniška varnost se osredotoča na zagotavljanje varne uporabe računalnikov. Osnovni pristop je izdelava računalniških platform, jezikov in programov z vgrajenimi omejitvami, tako da agenti lahko izvedejo le določene akcije. Danes pa vse bolj uveljavlja varnost mobilnih naprav.

## 2.1 Standardi in priporočila na področju informacijske varnosti v praksi

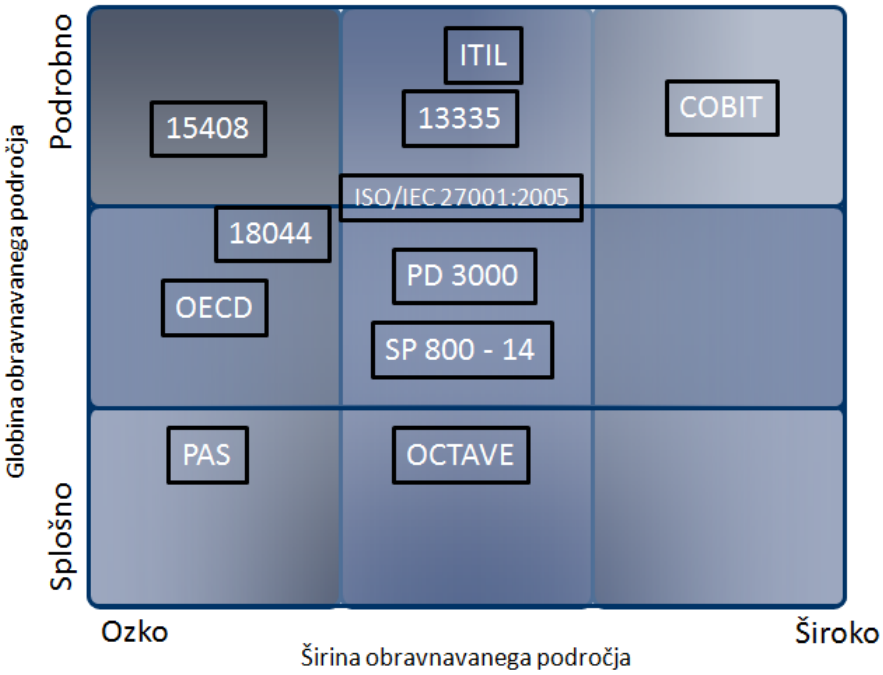
Na voljo je vse večje število standardov, ki se ukvarjajo s področjem varovanja informacij. Nekateri so splošnejši in namenjeni vsem organizacijam, drugi so bolj specializirani. Na spodnji sliki (Slika 2) so navedeni tisti dokumenti, ki so se v praksi najbolj uveljavili in se tudi najpogosteje uporabljajo.

Dokumenti navedeni na spodnji sliki (Slika 2), lahko organizacijam služijo kot pripomoček pri oblikovanju sistema za upravljanje informacijske varnosti. Med seboj se razlikujejo glede na širino in globino področja, ki ga posamezen dokument obravnava.




**Slika 2: Standardi in priporočila na področju informacijske varnosti, ki se v praksi najpogosteje uporabljajo [16]**

Nekateri od naštetih dokumentov so bolj splošne narave in pokrivajo širše področje zagotavljanja varnosti. Razvrstitev dokumentov glede na širino in globino obravnavanega področja je sistematično prikazano na sliki 2.




**Slika 3: Razvrstitev dokumentov na področju informacijske varnosti glede na status dokumenta ter glede na širino in globino obravnavanega področja**

Med vsemi referenčnimi sistemi za to področje je verjetno najbolj celovit, zagotovo pa najbolj priznan ISO 17799. Zelo veliko vlogo pa ima tudi zbirka najboljših praks za upravljanje IT – ITIL ter delovni okvir COBIT. Vsi trije prispevki k informacijski varnosti pa so v nadaljevanju podrobneje predstavljeni predvsem z vidika mobilnih naprav.

## 2.2 COBIT

Zaradi potrebe po poenotenju standardov vodenja in nadzora informatike v združbi ter povezovanja strokovnjakov s področja upravljanja informacijskih virov je leta 1998 nastal Information Technology Governance Institute (ITGI). COBIT je eden najpomembnejših izdelkov ITGI. Gre za delovni okvir s pripadajočimi orodji, ki omogočajo vodstvu, da zapolni vrzel med zahtevami po nadzoru informatike, problemi tehnične narave in poslovnimi tveganji. COBIT predstavlja splošen procesni model, ki sestoji iz 34 procesov, ki se lahko pojavljajo v službah za informatiko [9]. Model je zasnovan tako, da je razumljiv tako informatikom kot vodstvom združb.

Podjetja potrebujejo objektivne ocene o tem, kakšno je trenutno stanje in kje so potrebne izboljšave. Razviti morajo skupek orodij za ravnatelje za spremljanje izboljšav. Slika 4 prikazuje standardna vprašanja in orodja za zagotavljanje informacij

ravnateljstvu za iskanje odgovorov, vendar pa pri nadzorni plošči potrebujemo indikatorje, pri kazalniki potrebujemo ocene ter pri primerjavi potrebujemo lestvice za primerjavo.


**Slika 4: Upravljalske informacije [9]**

Kot odgovor, na zgornje zahteve za definiranje in spremljanje primerne IT kontrole ter nivoja zmogljivosti, ima COBIT naslednje definicije:

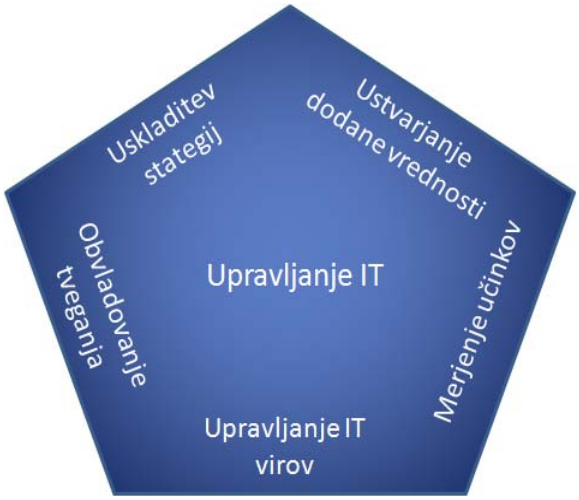
- **Primerjava** – zmogljivosti in sposobnosti IT procesov, izražena v zrelostnem modelu, ki je izpeljan iz Software Engineering Institute's Capability Maturity Model.
- **Cilji in ocene** – IT procesov za definiranje in merjenje izhodov in zmogljivosti
- **Cilji aktivnosti** – da so vsi procesi pod kontrolo.

Področja upravljanja IT:

- **Strateška usklajenost (ang. Strategic alignment) se osredotoča na:**
  - povezavo med poslovnim planom in planom IT,
  - opredeljuje, vzdrževanje in uveljavljanje predlagane vrednosti IT,
  - skladnost delovanja IT z delovanjem združbe.
- **Dodajanje vrednosti (ang. Value delivery) se osredotoča na:**
  - predlagano vrednost koristi skozi celoten cikel,
  - izpolnjevanje obljubljene prednosti IT v skladu s strategijo,

- optimizacijo stroškov in dokazovanje resnične vrednosti IT.

- **Upravljanje tveganj (ang. Risk management) se osredotoča na:**
  - zavedanje zaposlenih na vodilnih položajih o možnih tveganjih,
  - raven tveganja, ki ga je združba pripravljena sprejeti,
  - razumevanje zahtev glede skladnosti,
  - transparentnost pomembnih tveganj združbe,
  - vključevanje obveznega upravljanja s tveganji v združbo.
- **Upravljanje sredstev (ang. Resource management) se osredotoča na:**
  - optimalne investicije,
  - pravilno upravljanje kritičnih sredstev IT; ključni problemi zahtevajo optimizacijo znanja in infrastrukture.
- **Merjenje rezultatov (ang. Performance measurement) se osredotoča na:**
  - sprejemanje in nadziranje vpeljevanja strategije,
  - zaključevanje projektov,
  - uporabo sredstev,
  - izvrševanje procesov in storitev.




**Slika 5: Upravljanje IT**

Zgoraj našteta področja morajo izvršni vodje obravnavati pri upravljanju IT znotraj združbe. COBIT ponuja generični procesni model, ki je lahko razumljiv tako operativnim vodjem IT kot poslovnim vodjem. V njem so predstavljeni vsi procesi, ki se običajno izvajajo v organizacijskih enotah IT. COBIT-ov procesni model je preslikan na vsa področja upravljanja IT in ponuja most med tem, kar morajo operativni vodje izvesti, in tem, kako želi izvršilno vodstvo upravljati.

Najpomembnejši dokumenti delovnega okvirja COBIT so [9]:

- COBIT okvir (ang Framework), kjer je razložena organizacija ciljev upravljanja informacijskih virov in najboljših praks za posamezne IT procese ter njihova povezava s poslovnimi zahtevami.
- Kontrolni cilji (ang. Control Objectives), kjer so predstavljeni kontrolni cilji IT procesov.
- Prakse na področju nadzora IT procesov (ang. Control Practices), kjer so razloženi razlogi za vpeljavo določenega nadzora in način, kako to narediti.
- Kotrolni cilji v skladu z odredbo Sarbanes-Oxley (ang. IT Control Obejctives for Sarbanes-Oxley), kjer so predstavljeni kontrolni cilji v skladu z odredbo Sarbanes-Oxley, ki velja na področju Združenih držav Amerike. Odredba določa nova pravila upravljanja, nadzorovanja in standardov na področju IT procesov za javne združbe.

- Vodnik za vpeljavo upravljanja informacijskih virov (ang. IT Governance Implementation Guide), ki podaja napotke, kako vpeljati v združbo upravljanje informacijskih virov s pomočjo COBIT-a in njegovih podpornih orodij.
- Vodnik za hitro vpeljavo COBIT-a (ang. COBIT Quickstart), ki vsebuje osnove nadzora IT za manjše združbe in prvi možen korak pri vpeljavi COBITa v večja podjetja.
- Temelji varnosti po COBIT-u (ang. COBIT Security Baseline), ki se osredotoča na temeljne korake pri implementaciji varnostne politike v združbi.

Vpeljava delovnega okvirja COBIT, ogrodja za upravljanje IT, prinaša naslednje koristi:

- večjo skladnost s poslovnimi procesi,
- vodstvo bolj razume delo IT oddelka,
- jasno opredeljene zadolžitve in odgovornosti,
- splošna sprejemljivost ogrodja COBIT,
- porazdeljeno razumevanje med vlagatelji, ki temelji na skupnem jeziku,
- zadostitev potrebi po kontroli IT, na podlagi ogrodja COSO.

### 2.2.1 Splošno o COBITu

Kot odgovor na potrebe po upravljanju IT, opisane v zgornjem poglavju je ogrodje COBIT, ki je izdelano tako, da je [9]:

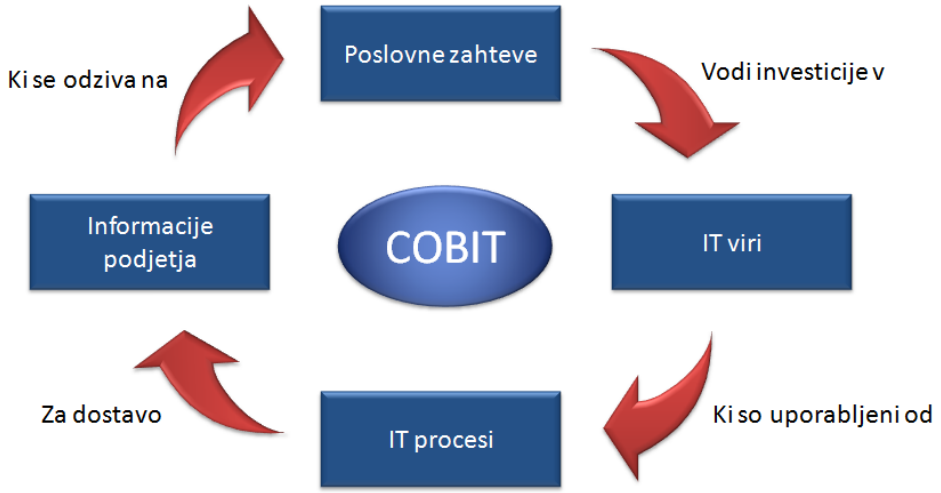
- poslovno osredotočeno (ang. Business Focused),
- procesno orientirano (ang. Process Oriented),
- temelječe na kontrolah (ang. Controls Based),
- vodeno z meritvami (amg. Measurement Driven).

Glavna pomanjkljivost COBIT-a je osredotočenost na nadzor nad procesi in manj na njihovo izvajanje [9].

#### *2.2.1.1 Poslovno osredotočeno*

Poslovna usmerjenost je glavna tema COBITa. Načrtovan je tako, da ga ne uporabljajo le informatiki (tu mislimo predvsem na tehnične kadre), temveč gre za vodenje in razumevanje delovanja informatike uporablja tudi vodstvo združbe in lastniki poslovnih procesov.

Spodnja slika prikazuje osnovni princip ogrodja COBIT. Za zagotovitev informacij, ki jih združba potrebuje za dosego svojih ciljev, mora le-ta voditi in kontrolirati sredstva IT ter z uporabo strukturiranih procesov dostaviti želeno informacijo, ki se odziva na poslovne potrebe.




**Slika 6: Osnovni princip modela COBIT [9]**

##### 2.2.1.1.1 Informacijski kriteriji

Informacije dostavljene v jedro poslovnih procesov morajo izpolnjevati določene kriterije, katere lahko razdelimo v tri osnovne skupine po zahtevah iz katerih izhajajo [9].

**Zahteve po kakovosti**

- Učinkovitost – informacije morajo biti ustrezne in primerne za poslovni proces. Dostavljene morajo biti pravočasno, biti morajo pravilne, dosledne ter uporabne.
- Uspešnost – informacije se morajo pridobiti z optimalno (najbolj produktivno in ekonomično) rabo virov.

**Varnostne zahteve**

- Zaupnost – občutljive informacije je potrebno zaščititi pred nepooblaščenim dostopom.
- Celovitost – informacije morajo biti natančne in popolne.
- Razpoložljivost – informacije morajo biti razpoložljive poslovnemu procesu v sedanjosti in prihodnosti, kar pomeni tudi rezervacijo potrebnih virov in s tem povezanih kapacitet.

**Zahteve po zanesljivosti**

- Skladnost – poslovni proces mora biti v skladu z zakoni, predpisi in pogodbenimi dogovori.
- Zanesljivost – zagotavljanje pravnih informacij ravnateljstvu za upravljanje in vodenje.

#### 2.2.1.1.2 Viri IT

Po definiciji metodologije COBIT se informacijska tehnologija napaja iz petih virov [9]:

1. **Podatki** – podatkovni objekti v najširšem pomenu (notranji in zunanji), strukturirani ali nestrukturirani, grafični, zvočni ipd.
2. **Aplikacijski sistemi** – razume se kot skupek ročnih in programiranih postopkov.
3. **Tehnologija** – tehnološki viri predstavljajo strojno opremo, operacijske sisteme, sistemi upravljanja baz podatkov, mrežna programska in strojna oprema, multimedijski pripomočki ipd.
4. **Pripomočki** – vsi ostali viri za upravljanje in podporo delovanju informacijskih sistemov.
5. **Ljudje** – sposobnosti, pomanjkljivosti in produktivnost zaposlenih pri planiranju, organiziranju, dostavi, podpori nadzoru in ocenjevanju informacijskih sistemov.

#### *2.2.1.2 Procesno orientirano*

COBIT definira IT aktivnosti v splošnem procesnem modelu s štirimi domenami, ki so prikazane tudi na spodnji sliki. Te domene so [9]:

- Planiranje in organiziranje (*ang. plan and organize* ali krajše *PO*)

  Domena zajema strategijo, taktiko in skrbi za identifikacijo načinov, kako lahko IT najbolj pripomore k uresničevanju poslovnih ciljev.

- Pridobitev in uvedba (*ang. acquire and implement* ali krajše *AI*)

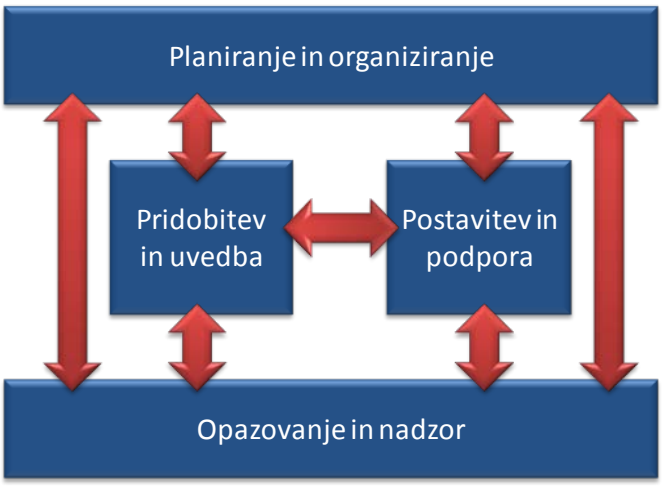
  Za uresničitev strateških ciljev IT je potrebno identificirati rešitve, jih razviti ali nabaviti ter vpeljati in integrirati v poslovne procese. Poleg tega ta domena pokriva tudi spremembe in vzdrževanje obstoječih sistemov.

- Postavitev in podpora (*ang. deliver and support* ali krajše *DS*)

  Domena pokriva izvajanje podpornih procesov IT. Vključuje izvedbo, varnostno politiko, podporo uporabnikom in upravljanje s podatki.

- Opazovanje in nadzor (*ang. monitor and evaluate* ali krajše *ME*)

  Vhod v to domeno predstavljajo izhodi iz vseh drugih domen. Domena omogoča učenje, odpravljanje napak in izboljševanje procesov.




**Slika 7: Štiri medsebojno povezana področja COBIT-a [9]**

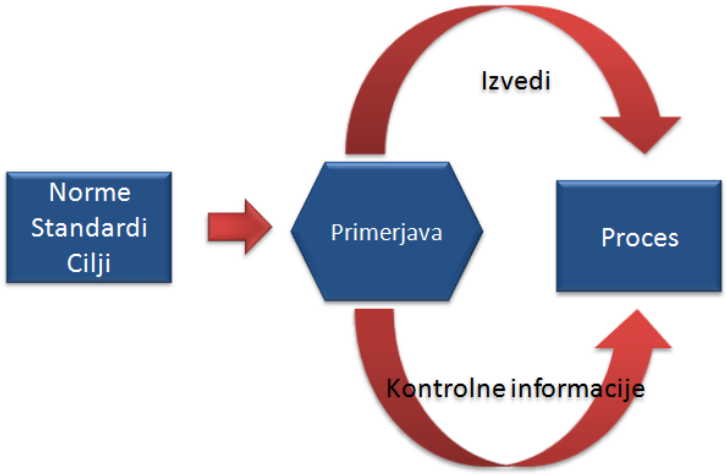
Vsako od področij je dalje razdeljeno na procese, ti pa naprej na aktivnosti. COBIT sestoji iz 34 procesov, ki so skladni z najboljšimi praksami, in kot taki dajejo podlago

oziroma referenčni okvir za učinkovito organizacijo informatike v združbi. V seminarju je pozornost posvečena predvsem procesoma DS8 ter DS10 ter delnim procesom, ki sodijo poleg. Tu so mišljeni predvsem delni proces nadzora ter analize smernic pri obeh procesih.

Vsakemu izmed 34 procesov odgovarja kontrolni cilj na najvišjem nivoju. Lastnikom poslovnih procesov zagotavljajo, da je uveden primeren kontrolni sistem za okolje informacijske tehnologije, v kolikor so doseženi kontrolni cilji in na najvišjem nivoju. Pri doseganju teh ciljev upoštevamo poslovne zahteve za učinkovitost, uspešnost, zaupnost, celovitost, razpoložljivost, skladnost in zanesljivost. Glavni cilj projekta COBIT je zagotoviti jasno politiko in dobro prakso za vpeljavo kontrol informacijske tehnologije v vseh vejah industrije [15].

#### *2.2.1.3 Temelječe na kontrolah*

Kontrole so opredeljene kot politike, postopki, prakse in organizacijske strukture, ki dajejo razumno zagotovilo za doseganje poslovnih ciljev s preprečevanjem ali vsaj z odkrivanjem in odpravljanjem neželenih dogodkov. Standardni model kontrole deluje po spodaj prikazanem modelu (slika 5).




**Slika 8: Model kontrole [9]**

Delujoče kontrole zmanjšujejo tveganje in povečujejo učinkovitost, ker pripomorejo k zmanjšanju števila napak in celovitejšemu pristopu k vodenju.

#### *2.2.1.4 Vodeno z meritvami*

Osnovna potreba vsake združbe je, da razume status svojih IT sistemov in da določi nivo upravljanja in nadzora, ki ga lahko združba zagotovi.

Zrelostni modeli upravljanja in nadzora IT procesov izhajajo iz metode ocenjevanja združbe. Model je sestavljen iz šeststopenjske lestvice, katera označuje zrelost ocenjevalnega procesa od zrelostne stopnje "non-existent" – ne obstaja (0), do zrelostne stopnje "optimized" – optimiziran (5).

Opis splošnega zrelostnega modela [9]:

**0 Ne obstaja** – Popolno pomanjkanje katerih koli prepoznavnih procesov, združba sploh ni spoznala, da obstaja problem, s katerim se je potrebno soočiti …

**1 Začetni** – Združba je sicer spoznala, da obstajajo problemi, ki jih je potrebno obravnavati, nima pa standardiziranih postopkov, problemov se loteva na individualni ravni, odvisno od posameznega primera, celoten pristop do upravljanja je neorganiziran.

**2 Ponavljajoči** – Procesi so razvidni do take mere, da se ne glede na izvajalca, rešujejo podobno, vendar ni formalnega usposabljanja in posredovanja standardnih postopkov, naloge so prepuščene posameznikom; obstaja visoka stopnja zaupanja v znanje posameznika in zato so napake verjetne.

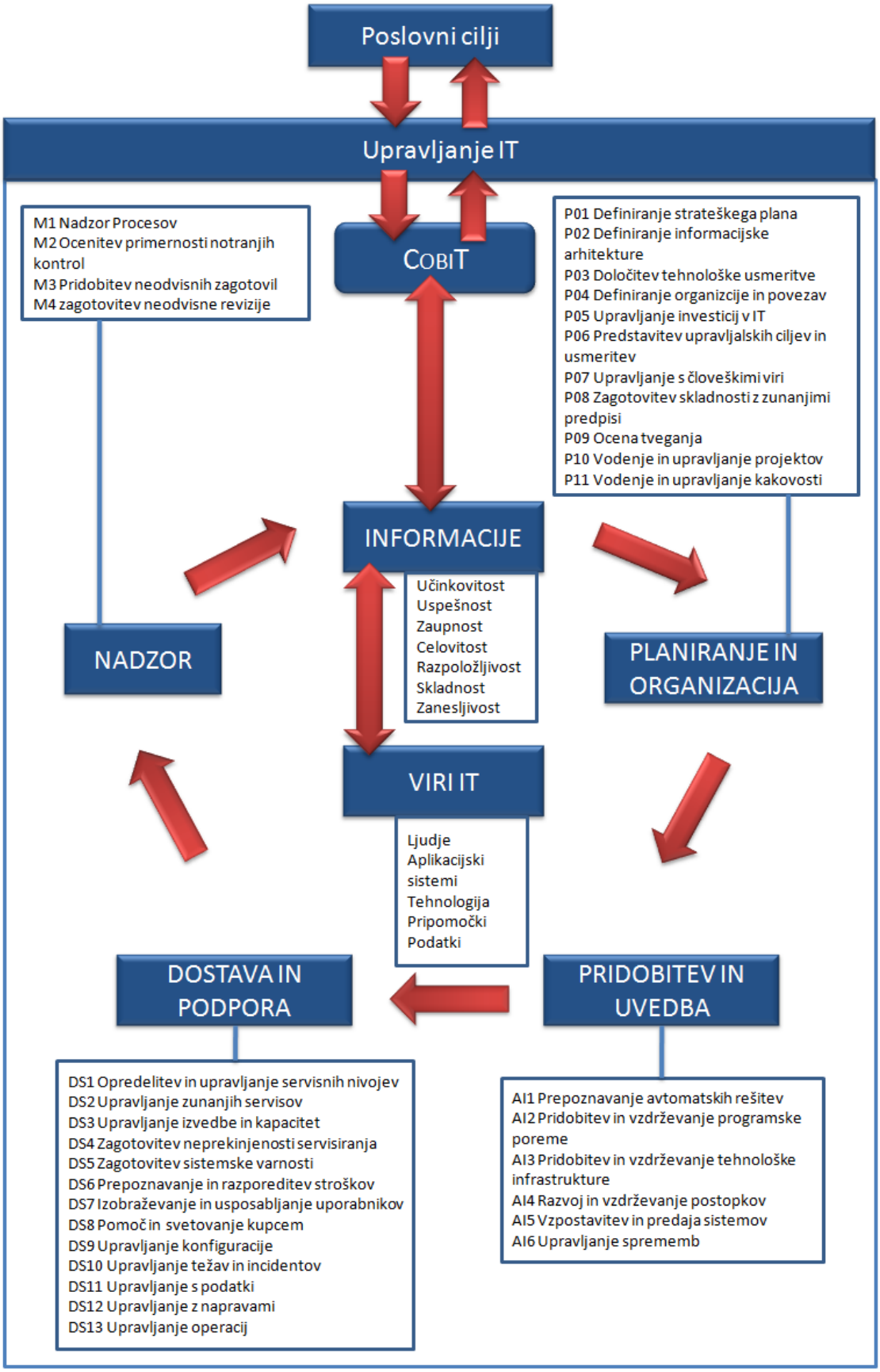
**3 Definirani procesi** – Procesi so že standardizirani in dokumentirani; zaposleni se udeležujejo usposabljanj, vendar je izvajanje prepuščeno odnosu posameznika do dela, zato so odmiki od dogovorjenih postopkov težko ugotovljivi; postopki sami niso posebej napredni in so bolj formaliziranje praktičnih postopkov dela.

**4 Upravljani in merjeni** – Kjer se procesi ne izvajajo pričakovano, se opravijo podrobne meritve in nadzor. Procesi so neprestano pod nadzorom in optimizacija se izvaja le na posameznih delih procesov. V primeru neučinkovitosti procesa se takoj reagira.

**5 Optimizirani** – Procesi so bili izboljšani do nivoja najboljše prakse ter se neprestano izboljšujejo in prilagajajo, IT nudi orodja za avtomatično povezavo delovnih postopkov in zagotavlja njihovo kvaliteto, učinkovitost in hitro prilagodljivost.

### 2.2.2 Struktura delovnega okvirja COBIT

Spodnja slika prikazuje celoten pregled delovni okvir COBIT s pripadajočimi domenami; medsebojne povezave in odvisnosti, si je moč ogledati na naslednji sliki. Spodnja slika prikazuje tudi porazdelitev posameznih procesov po domenah (Slika 6).




**Slika 9: Struktura modela COBIT [9]**

### 2.2.3 COBIT ter varnost mobilnih naprav

V delovnem okvirju COBIT področje mobilnih naprav ni eksplicitno obravnavano. Podani so splošni kontrolni cilji. Ker se v nalogi v prvi vrsti osredotočam na varnost mobilnih naprav, bom v nadaljevanju podrobneje predstavil proces DS5, ki se ukvarja s kontrolnimi cilji, povezanimi z informacijsko varnostjo.

Sama informacijska varnost je preko kontrolnih ciljev zajeta v posameznih procesih, proces DS5 – zagotavljanje varnosti sistemov (ang. Ensure Systems Security), pa varnost obravnava v celoti.

Proces DS5 je sestavljen iz naslednjih področij, ki so opisana v nadaljevanju. Pri vsakem področju je še podan predlog, kaj storiti v primeru mobilnih naprav. Pri vseh predlogih se izhaja iz predpostavke, da je v organizaciji že vzpostavljen sistem varovanja informacij, da so izdelane varnostne politike …

**DS5.1 – Management of IT Security (Upravljanje informacijske varnosti)**

Upravljanje informacijske varnosti na najvišjem organizacijskem nivoju, da so varnostne aktivnosti povezane s poslovnimi potrebami.

> V upravljanje informacijske varnosti je potrebno vključiti tudi mobilne naprave. V večini primerov se na mobilne naprave pozabi ter se jih ne obravnava glede na njihove funkcionalnosti in podatke, ki jih lahko vsebujejo.

**DS5.2 – IT Security Plan (Plan informacijske varnosti)**

Prenos poslovnih groženj ter compliance v krovni IT varnostni plan, ki upošteva infrastrukturo ter varnostno kulturo. Zagotoviti je potrebno implementacijo plana v varnostnih politikah in procedurah skupaj, s primernimi investicijami, storitvami, ljudmi, programsko in strojno opremo. Potrebno je tudi skomunicirati politike ter postopke odgovornim in uporabnikom.

> V krovnem varnostnem planu je potrebno pokriti tudi področje mobilnih naprav ter ga podrobneje definirati z varnostno politiko.

**DS5.3 – Identity Management (Upravljanje z identitetami)**

Potrebno je zagotoviti, da se vse uporabnike (notranje, zunanje in začasne) ter njihove aktivnosti na IT sistemih (poslovne aplikacije, IT okolje, sistemske operacije, razvoj,

vzdrževanje), enolično identificira. Omogočiti je potrebno uporabniške identitete preko avtentikacijskih mehanizmov. Potrebno je zagotoviti, da pravice uporabnikov za dostop ali upravljanje sistemov izhajajo iz poslovnih potreb. Zahteve za dodelitev pravic uporabnikom morajo priti s strani nadrejenih uporabnikov, ki pa morajo biti potrjene s strani lastnikov sistemov, implementirane pa morajo biti s strani odgovorne osebe za varnost. Vzdrževanje uporabniške identitete ter dostopne pravice v centralnem repozitoriju.

> Potrebno je zagotoviti identifikacijo uporabnikov na mobilnih napravah na enak način kot se uporablja pri ostalih IT sistemih, s pomočjo centralnega repozitorija. Postopki dodeljevanja pravic morajo biti enaki kot za vse ostale sisteme.

**DS5.4 User Account Management (Upravljanje z uporabniškimi računi)**

Potrebno je definirati procese za zahtevanje, vzpostavljanje, izdajanje, suspendiranje, spreminjanje in zapiranje uporabniških računov ter uporabniških pravic.

> Procesov za področje mobilnih naprav ni potrebno spreminjati, v kolikor so v organizaciji definirani. Če v organizaciji procesi niso definirani, jih je priporočljivo definirati in nato dosledno izvajati ter neprestano izboljševati.

**DS5.5 Security Testing, Surveilliance and Monitoring (Varnostno testiranje, Opazovanje, Nadzor)**

Implementacijo IT varnosti je potrebno testirati na proaktiven način. Informacijska varnost mora biti pregledana v časovnih periodah, da se zagotovi stalno izboljševanje varnosti.

> Na mobilnih napravah je potrebno zagotoviti mehanizme, ki bodo omogočali takšno vrsto nadzora. To so tako imenovana management orodja, ki jih je danes na trgu že veliko.

**DS5.6 Security Incident Definition (Definicije varnostnih incidentov)**

Potrebno je jasno definirati in sporočiti karakteristike možnih varnostnih incidentov, da so lahko primerno klasificirani in posredovani procesu za upravljanje z incidenti in problemi.

> Tudi za področje mobilnih naprav je potrebno definirati varnostne incidente.

### DS5.7 Protection of Security Technology (Varovanje varnostnih tehnologij)

Potrebno je zagotoviti ustrezno varovanje varnostnih tehnologij, ni priporočljivo razkazovati varnostno dokumentacijo po nepotrebnem.

### DS5.8 Cryptographic Key Management (kriptografsko upravljanje z gesli)

Potrebno je definirati, da so politike in procedure zmožne generirati, spreminjati, ponovno dodeljevati, uničevati, distribuirati, certificirati, hraniti, vnašati, uporabljati ter arhivirati kriptografske ključe, za zagotavljanje zaščite ključev proti spremembi in nepooblaščenim razkritjem.

### DS5.9 Malicious Software Prevention, Detection and Correction

Potrebno je zagotoviti ažurne varnostne popravke, definicije virusov v celotni organizaciji za zaščito informacijskih sistemov in tehnologije pred zlonamerno kodo (npr. virusi, spamom, spywearom).

> Potrebno je zagotoviti pravočasno ter ažurno posodabljanje mobilnih naprav z zaščito pred zlonamerno kodo.

### DS5.10 Network Security (Varnost omrežja)

Uporaba varnostnih tehnik ter z njimi povezano upravljanje (npr. požarni zid) za omejevanje dostopa in kontrole toka informacij iz ter na internet.

### DS5.11 Exchange of Sensitive Data

Izmenjava občutljivih transakcijskih podatkov samo preko zaupnih kanalov in z zagotavljanjem avtentikacije ter dokazljivosti submission, dokazljivosti prejema in nespremenljivosti.

> Zagotoviti varnostne mehanizme na mobilni napravi, ki bodo omogočali tako varen način prenosa in dostopa do zaupnih informacij.

## 2.3 ITIL v3

### 2.3.1 Splošno o ITIL

Trenutno je v svetu na področju upravljanja informacijskih sistemov eden najbolj priznanih standard ITIL, saj ga uporabljajo in priporočajo vsa večja svetovna računalniška podjetja kot so Microsoft, HP, IBM in drugi.

ITIL je zbirka dokumentov z opisi in napotki za uvajanje in kakovostno upravljanje s storitvami, ki temeljijo na uporabi informacijske tehnologije (IT). V ITIL-u je dokumentirana t.i. najboljša praksa (best practice) pri upravljanju s storitvami ob sodelovanju mednarodnih strokovnjakov, tako iz javnega kot privatnega sektorja v gospodarstvu. Lastnik in razvijalec ITIL-a je britanski Office of Government Commerce (OGC) oz. Urad za trgovino britanske vlade (prej poznan kot Central Computer and Telecommunications Agency CCTA). ITIL skupaj z Britanskim inštitutom za standarde (British Standards Institution's Standars for IT Service Management) podpira britanski standard za upravljanje s storitvijo IT BS15000 [16].

ITIL uporabljajo strokovnjaki za informacijsko tehnologijo, ki se ukvarjajo s storitvami IT in potrebujejo podroben vpogled v procese in postopke upravljanja storitev.

### 2.3.2 Zgodovina

ITIL je bil zasnovan konec 80-ih let in je prvotno služil potrebam britanske vlade. Zaradi njegove univerzalne uporabnosti se je kmalu razširil na vse panoge gospodarstva v Veliki Britaniji in v tujini. Kmalu pa je ITIL postalo najbolj uveljavljeno, na procesih zasnovano ogrodje za uveljavljanje 'najboljše prakse' pri upravljanju s storitvijo IT v svetu [16].

Prvotna usmeritev ITIL-a je bilo upravljanje informacijske infrastrukture v angleških vladnih ustanovah, danes pa se uporablja po vsem svetu kot eden od standardov v gospodarstvu in negospodarstvu.

Tako danes ITIL predstavlja več kot samo standard. Okrog nje je nastala cela panoga, ki vključuje [16]:

- izobraževanje,
- potrjevanje znanja posameznikov s certifikati,

- svetovanje,
- programska orodja,
- itSMF (IT Service Management Forum), mednarodna neprofitna organizacija v službi promocije upravljanja s storitvijo in ITIL-a,
- certificiranje celotnih podjetij.

Nedavno se je ITIL spremenil od procesno usmerjenega pristopa do pristopa življenjskega kontinuiranega cikla storitev IT. Način vpeljave ITILa v poslovno strategijo in cilje organizacije je opredeljeno v petih ključnih kategorijah:

- Strategija storitev (ang. Service Strategy), ki povzema skupne poslovne namene in pričakovanja ter zagotavlja planiranje IT strategije v skladu z njimi.
- Načrtovanje storitev (ang. Service Design), ki se začne z nizom novih ali spremenjenih poslovnih zahtev in konca z razvojem rešitve, ki ustreza zapisanim potrebam poslovanja.
- Tranzicija storitev (ang. Service Transition), ki zadeva upravljanje sprememb, zavarovanje tveganj in zagotavljanje kakovosti.
- Izvajanje storitev (ang. Service Operation), ki se osredotoča na izvajanje storitev v produkcijskem okolju organizacije.
- Nenehno izboljševanje storitev (Continual Service Improvement), ki ima celosten pregled vseh ostalih elementov in išče možnosti, ki zagotavljajo izboljšave skupnih procesov in storitev.

ITIL V3 Foundations zagotavlja splošen pregled nad življenjskim ciklom upravljanja storitev IT (ang. IT Service Management Lifecycle) in podpornimi procesi, funkcijami in vlogami.

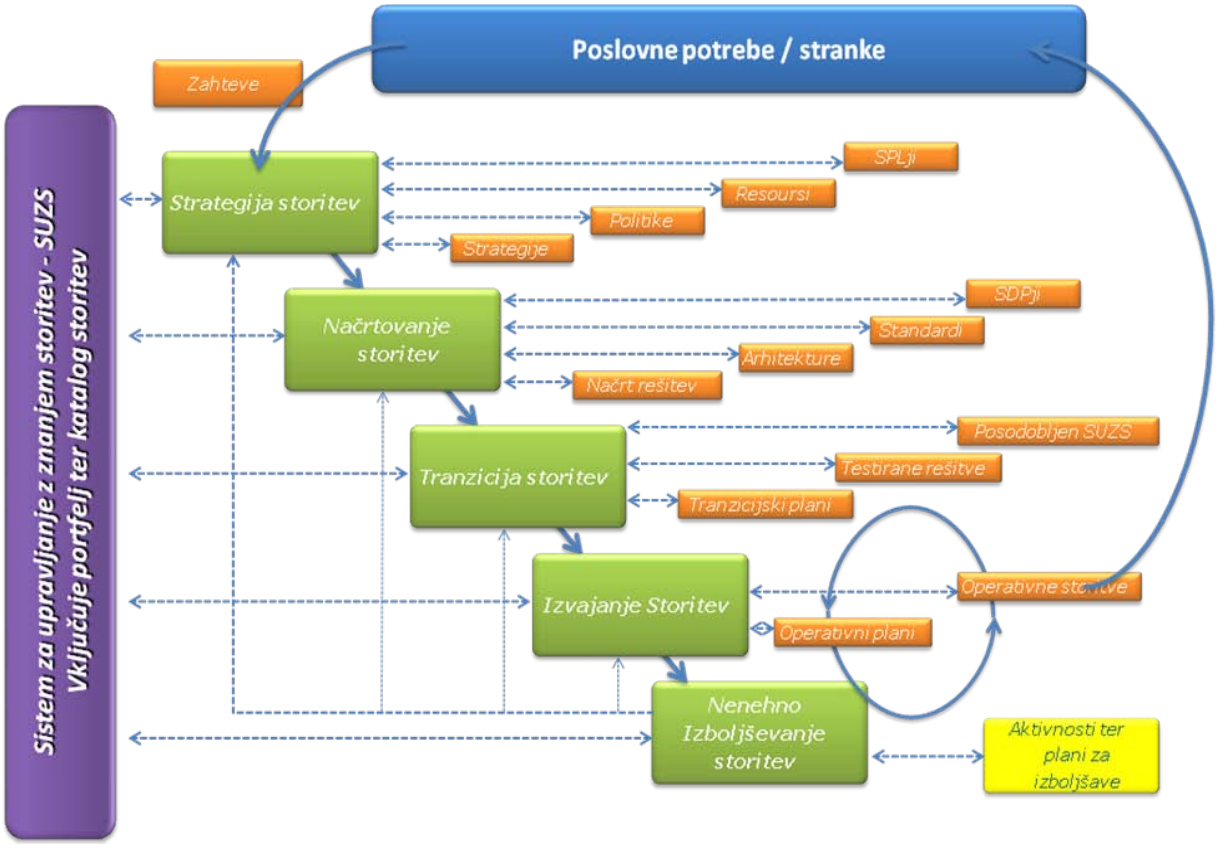
Vse rešitve storitev ter aktivnosti bi morale izhajati iz poslovnih potreb ter zahtev. Spodnji diagram (Slika 10) prikazuje, kako se življenjski cikel storitve sproži oz. prične s spremembo oz. zahtevo iz poslovnih potreb.

Zahteve so identificirane ter dogovorjene z nivojem Strategija storitev z nivojem paketa storitev (ang. Service Level Package - SLP) ter definiranim naborom poslovnih izhodov.

Ta prehaja v fazo načrtovanja storitev, kjer se izdela rešitev storitve skupaj s paketom načrtov storitev (ang. Service Design Package – SDP), ki vsebuje vse potrebno za to, da lahko storitve potujejo skozi vse faze življenjskega cikla [17].

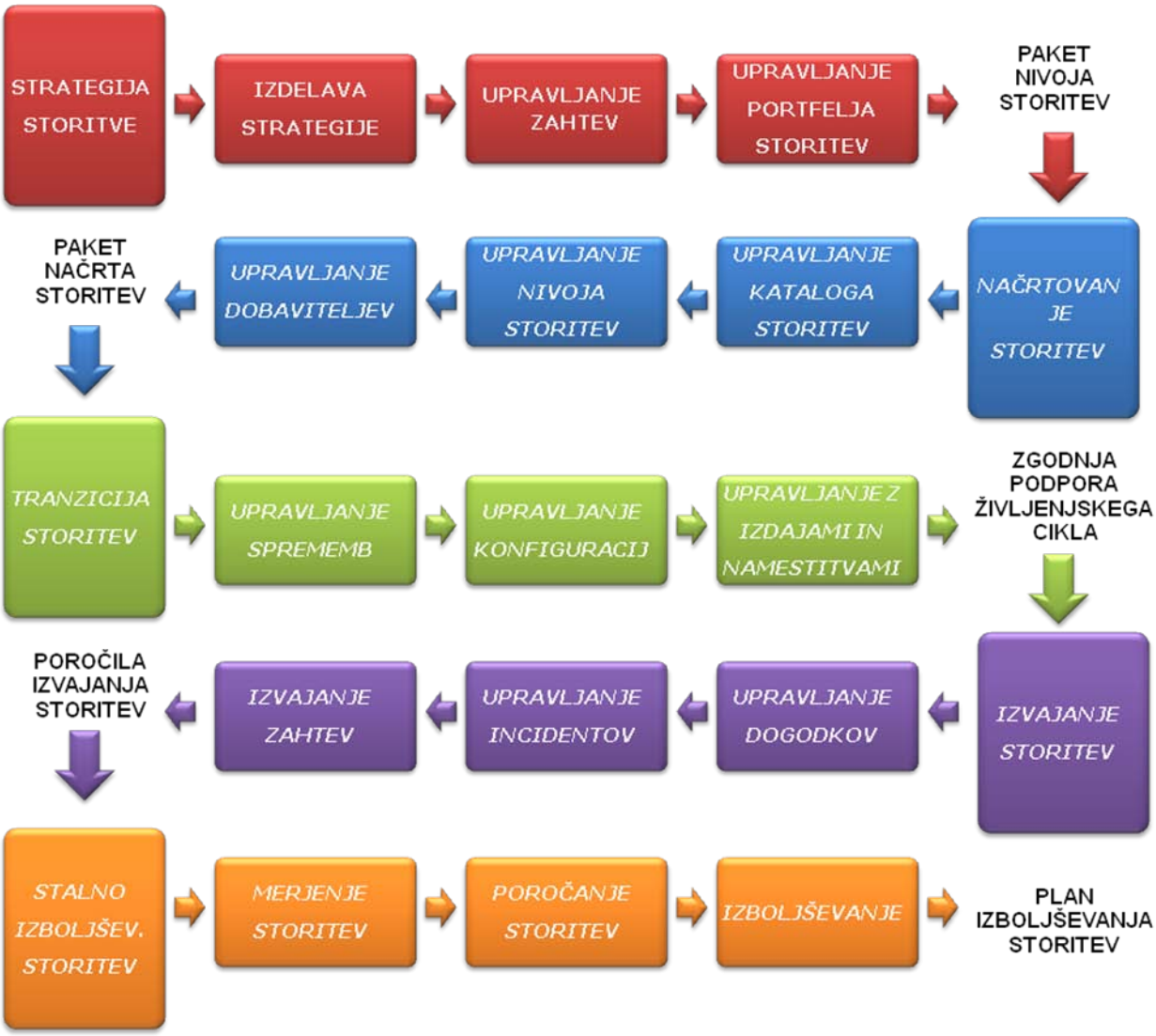
SDP prehaja v fazo tranzicije storitev, kjer je storitev ocenjena, testirana ter validirana. Sistem za upravljanje z znanjem storitev (krajše SUZS) (ang. Service Knowledge Management System - SKMS) je posodobljen in storitev je postavljena v živo okolje, kjer preide v fazo izvajanja storitev.

Kjerkoli je mogoče stalno izboljševanje storitev, identificira priložnosti za izboljšavo slabosti ali napak v kateri koli fazi življenjskega cikla [17].




**Slika 10: Povezave, vhodi in izhodi posameznih faz življenjskega cikla storitev [17]**

Spodnja slika prikazuje, kako so posamezna področja ter procesi ITIL v3 med seboj povezani ter skupaj zagotavljajo »end-to-end«, povezano upravljanje storitev (ang. Service Management).




**Slika 11: Prikaz modela storitev na najvišjem nivoju [17]**

### 2.3.3 ITIL in varnost mobilnih naprav

ITIL se neposredno ne navezuje na mobilne naprave. Je zelo pomembno orodje pri definiranju procesov v katere so vključene tako mobilne naprave kot tudi ostale naprave. ITIL ima splošna priporočila varnosti, ki jih je nujno potrebno upoštevati tudi pri področju mobilnih naprav.

## 2.4 Standard ISO 27001:2005

### 2.4.1 Zgodovina BS 7799

Standard je primeren za vse vrste organizacij. Ker se vedno bolj uveljavlja po celotnem svetu, bi ga v tem članku vzel za primer, ki bo v bližnji prihodnosti še zelo prisoten pri sistemih vodenja varovanja informacij. Z njim pa bomo verjetno dobili točna navodila, ki bodo v veliki meri pripomogla k povečanju varnosti v informacijskih sistemih in večjem zaupanju med organizacijami. Obvladovanje informacijske varnosti bo na tak način poenoteno, to pa pomeni, da se bodo vzpostavila pravila, po katerih se bodo ravnali vsi uporabniki informacijskih tehnolog. S tem bodo zmanjšana tveganja, metodologija upravljanja z informacijsko varnostjo pa bo enaka povsod po svetu.

Za razumevanje, kam nas vodijo trenutni trendi razvoja, je potrebno najprej pogledati v zgodovino. Samo tako v celoti vidimo, kako se razvijajo potrebe po informacijski varnosti. Sami zametki tega standarda segajo že v zgodnja devetdeseta leta, ko je bil izdan Royal Dutch/Shell Group Information Security Policy Manual. To je bil pravilnik, po katerem so se ravnali v omenjeni organizaciji in iz katerega so kasneje to povzeli v National Computing Centre (NCC) iz Velike Britanije. Počasi se je pravilnik začel spreminjati in 1993 ga je oddelek za trgovanje in industrijo (United Kingdom Department of Trade and Industry) izdal v obliki dokumenta BSI-DISC PD003. British Standards Institute (BSI) ga je nato leta 1995 izdal kot BS7799, prvi priznani standard za infrmacijsko varnost. Kasneje se je le-ta razdelil na BS7799-1 in nato v BS7799-2. Tako se iz BS7799-1 leta 2005 razvil ISO/IEC 17799 (27002), iz BS7799-2 pa ISO/IEC 27001. Standard je s tem pridobil mednarodno veljavo in se postavil ob bok vsem pomembnejšim standardom, ki jih izdaja Mednarodna organizacija za standardizacijo [60].


**Slika 12: PDCA krog nenehnega izboljševanja [60]**

Standard deluje po principu Demingovega ali PDCA kroga nenehnega izboljševanja, temelji pa na treh predpostavkah informacijske varnosti: zaupnost, celovitost in razpoložljivost. Sestavljen je iz 8 poglavij in 133 kontrol, ki določajo, kakšne so zahteve za organizacijo, ki hoče vzpostaviti sistem vodenja varovanja informacij. Treba se je zavedati, da je standard orodje, ki daje okvir, v katerem gradimo varnost. Ta pa mora obsegati tako varovanje informacijske opreme (varnost programske in strojne opreme), kot tudi samo organiziranost in varovanje vseh oblik informacij, tudi tistih, ki so v fizični obliki (papirni dokumenti). Upoštevati moramo vse vrste tveganj, ki lahko ogrozijo organizacijo in vzpostaviti primerne načine za obvladovanje teh tveganj na način, ki je primeren za posamezno organizacijo. Le na ta način zagotovimo celovito varnost in zmožnost odgovora na grožnje, ki pretijo. Standard je skladen s standardom vodenja kakovosti in drugimi sistemi vodenja v organizacijah, zato je tudi bolj primeren za vpeljavo, saj ga v podjetjih, kjer je vpeljan že sistem vodenja kakovosti, (ISO 9001:2000) lažje implementirajo. Ravno iz te primerljivosti pa lahko predvidevamo trende rasti v prihodnje. Na Mednarodni organizaciji za standardizacijo je bila 23. novembra 2007 izdana raziskava o certificiranju, ki kaže na 16% povečanje certifikacije sistemov vodenja v letu 2006 glede na leto 2005. Do konca leta 2006 je bilo po svetu izdanih 897.866 certifikatov za sisteme vodenja kakovosti in to v samo 20. letih od kar obstaja ta standard. Trendi razvoja za ISO/IEC 27001 so podobni, saj se je v slabih dveh letih po podatkih Mednarodne organizacije za standardizacijo certificiralo že več kot 5.797 organizacij [60].

### 2.4.2 Družina standardov ISO 27000

ISO/IEC JTC 1/SC27 odbor si je za naložil razvoj družine standardov za sisteme upravljanja z varnostjo podatkov. Ta nova družina je družina standardov 27000:

- ISO/IEC 27000: Temeljni principi in pojmovnik (ang. Vocabulary and definitions). Ta standard usklajuje strokovno izrazoslovje za vso družino standardov ISO/IEC 27000.
- ISO/IEC 27001: Specifikacije sistema za upravljanje varovanja informacij (ang. Specification for an Information Security Management System).
- ISO/IEC 27002: Primeri dobre prakse implementacije sistema za upravljanje z varnostjo informacij (ang. Code of Practice for Information Security Management). Namenjen je tistim, ki skrbijo za implementacijo, izvajanje ali za vzdrževanje SUVI.
- ISO/IEC 27003: Napotki za vzpostavitev sistema za upravljanje informacijske varnosti (ang. Implementation Guidance).
- ISO/IEC 27004: Merila sistema za upravljanje informacijske varnosti (ang. Information security Management Metrics and Measurement).
- ISO/IEC 27005: Upravljanje informacijskih tveganj (ang. Guidelines for information security risk management).
- ISO/IEC 27006: Smernice za ponovno vzpostavitev informacijskega sistema po katastrofi (ang. Guidelines for information and communications technology disaster recovery services).

### 2.4.3 Zagotovila pri upravljanju varnosti informacij

Uporaba standarda prinaša poslovne koristi. Pri vpeljavi standarda organizacije dobro poznajo tveganja, s katerimi se srečujejo in jih zmanjšajo na želeno raven. V stikih s partnerji organizacije v skupno zadovoljstvo varujejo lastne in partnerjeve informacije, kar prispeva k dobrim odnosom in zmanjševanju nesporazumov ali zamer. Pri elektronskem poslovanju in njegovem ritmu dela je opora na standard skoraj nujna, da se organizacije izognejo nepreglednemu poslovanju in ravnanju z informacijam. Ko organizacije upravljajo z varnostjo informacij, šele takrat postanejo njeni dobri gospodarji [21].

Koristi opiranja na standard ISO 27001:2005 v organizacijo so [22]:

- standard omogoča osnovo za vpeljavo najboljših praks,
- je upravljavsko, tehnološko in organizacijsko neodvisno orodje ter dovolj splošen, da je primeren za vse vrste organizacij,
- s standardom zagotovimo celovito pokrivanje področja informacijske varnosti (zmanjšamo možnost, da bi spregledali pomembna področja),
- standard BS 7799 omogoča sistematičen in konsistenten pristop, ne samo pri vpeljavi, temveč tudi pri vzdrževanju sistema za upravljanje informacijske varnosti,
- uporaba standarda za varovanje informacij omogoča osnovo za ugotavljanje odstopanj in predvideva tudi vire za varovanje,
- opiranje zgolj na izkušnje posameznikov ni več potrebno, saj se pri zapisovanju politike in nadzorstev, ki zagotavljajo ustrezen nivo varnosti, lahko naslonim na standard.

Koristi uvedbe standarda ISO 27001:2005 v organizacijo so [22]:

- povečanje produktivnosti,
- revizije omogočajo nepristranski zunanji pogled na poslovanje, odkrivanje možnosti za izboljšanje,
- standard vpeljuje discipline, kot so ocenjevanje tveganj in hranjenje zapisov,
- povečanje zanesljivosti delovanja celotnega informacijskega sistema,
- omogoča hitro in učinkovito uvajanje novih sodelavcev,
- poveča zaupanja poslovnih partnerjev in drugih interesnih skupin,
- povečanje ugleda,
- povečanje prednosti pred tekmeci,
- izboljšanje osnov za marketing in trženje storitev,
- izpolnjevanje zakonskih zahtev,
- izpolnjevanje zahtev poslovnih partnerjev in odjemalcev.

### 2.4.4 ISO/IEC 27001:2005 ter mobilne naprave

Standard ISO/IEC 27001:2005 pokriva tudi področje mobilnih naprav ter dela na daljavo, priporočila pa so predstavljena v nadaljevanju.

Glavni cilj področja je zagotavljati informacijsko varnost pri uporabi mobilnih naprav ter pri delu na daljavo. Podrobnosti ter priporočila za implementacijo se nahajajo v nadaljevanju.

#### *2.4.4.1 Mobilne naprave ter komunikacije*

Potrebno je definirati ustrezno varnostno politiko ter primerne varnostne indikatorje za zaščito pred grožnjami pri uporabi mobilnih naprav ter komunikacij.

**Priporočila za implementacijo:**

Pri uporabi mobilnih naprav se je potrebno zavedati groženj pri delu v nenadzorovanih okoljih ter temu primerno definirati varnostne politike.

Varnostna politika za mobilne naprave mora vsebovati priporočila za fizično zaščito, dostopno kontrolo, kriptografske tehnike, varnostne kopije, protivirusno zaščito. Politika naj tudi vsebuje pravila in nasvete pri povezavi mobilnih pripomočkov v omrežje ter priporočila uporabe teh pripomočkov na javnih krajih.

Posebno skrb je potrebno imeti pri uporabi mobilnih naprav na javnih krajih, sejnih sobah ali drugih prostorih izven organizacije. Implementirana mora biti zaščita, da ne pride do nepooblaščenega dostopa ali razkritja informacij shranjenih in obdelanih na mobilnih napravah (kriptografske tehnike …).

Uporabniki mobilnih naprav na javnih krajih morajo tudi paziti na nepooblaščen prevzem nadzora. Potrebno je zagotoviti zaščito pred zlonamerno kodo in mora biti vedno posodobljena.

Varnostno kopiranje kritičnih poslovnih informacij mora biti narejeno pogosto. Oprema mora zagotavljati hitro in varno izvajanje varnostnih kopij. Varnostne kopije morajo biti ustrezno varovane.

Vzpostavljeni morajo biti primerni mehanizmi varovanja mobilnih naprav pri povezavi na internet. Za oddaljen dostop do poslovnih informacij preko javnih omrežij je potrebno zagotoviti pravilno identifikacijo, avtentikacijo ter primerne mehanizme za nadzor dostopa.

Mobilne naprave je potrebno tudi ustrezno fizično zaščititi pred krajo, še posebej v avtomobilu, hotelskih sobah, konferenčnih centrih ….V organizaciji je potrebno

vzpostaviti procese za primere kraje mobilnih naprav. Oprema, ki vsebuje pomembne poslovne informacije, mora biti ustrezno varovana in je ni dovoljeno nenadzorovano puščati na javnih krajih.

Priporočljivo je izvesti usposabljanje za uporabnike mobilnih naprav. Predvsem jih je potrebno seznaniti z nevarnostmi ter možnimi posledicami, da se bodo tudi sami zavedali pomena vgrajenih varnostnih mehanizmov pri uporabi mobilnih naprav.

# 3 Varnostna politika

Varnostna politika definira odgovore na dejavnike, ki ogrožajo informacijski sistem od zunaj, kot tudi na dejavnike, ki ogrožajo sistem od znotraj. Varnostna politika je program varnosti in je v pristojnosti vodstva. V tem programu so definirani cilji, pravila in odgovornosti v zvezi z varnostjo informacijskih virov podjetja, razni postopki in pravila. Program obsega pravila o fizičnem in tehničnem varovanju ter pravila, s katerimi je določeno, kakšni bodo načini varovanja. Dobra varnostna politika ima dovolj informacij, virov ter ljudi v podjetju. Sestavljena je iz skupka varnostnih pravil, s katerimi morajo biti seznanjeni vsi zaposleni. Ta pravila opredeljujejo način obnašanja, odgovornosti, naloge in splošna pravila za delo zaposlenih [18].

## 3.1 Naložbe v varnost

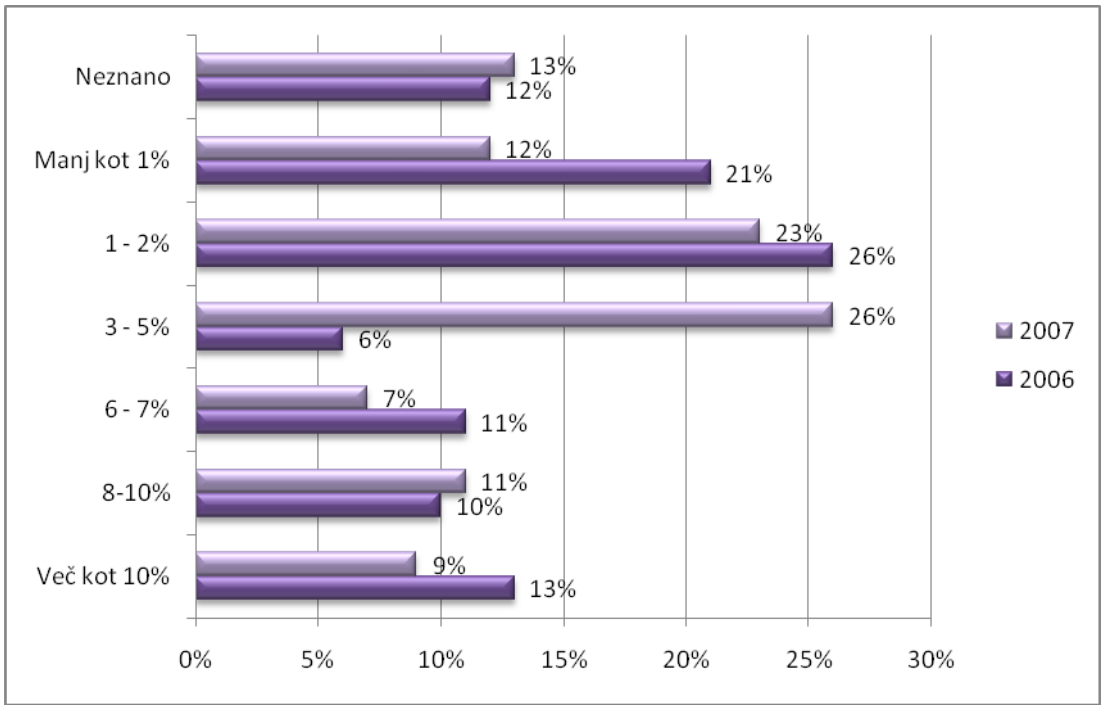
V nadaljevanju so prikazani rezultati raziskave, ki prikazujejo stanje vlaganj v informacijsko varnost v najrazličnejših organizacijah.

Raziskavo je leta 2007 opravil Computer Security Institute. 61 odstotkov udeležencev se je opredelilo, da so njihove organizacije za informacijsko varnost namenile 5 odstotkov ali manj njihovega letnega proračuna za informatiko. To je primerljivo tudi z rezultati iz leta 2006, kjer je bil rezultat 53 odstoten.

Največji viden napredek je v razponu od 3 do 5 odstotkov sredstev za IT namenjenih za informacijsko varnost, in sicer iz 6 na 26 odstotkov. Leta 2006 je tudi več kot 47 odstotkov organizacij podalo podatek, da porabijo manj kot 3 odstotke proračuna za informatiko, letos je takih organizacij zgolj 35 odstotkov.

Razmerje sredstev namenjenih za informacijsko varnost se povečuje, kar pa lahko ne odraža dejansko povečane količine denarja namenjene za informacijsko varnost. To je odvisno predvsem od tega, ali se količina denarja, namenjena za IT povečuje, ostaja enaka ali pa se celo zmanjšuje.

Slika 13 prikazuje dejanske rezultate raziskave.




**Slika 13: Raziskava o vlaganjih sredstev informatike v informacijsko varnost [25]**

V raziskavi leta 2008 so vključili tudi vprašanje, koliko denarja organizacije namenijo za osveščanje uporabnikov.

Raziskava je tudi pokazala, katere so bile najpogostejše grožnje, povezane z mobilnimi napravami, ki so doletele organizacije. Zaznati je bilo povečanje nevarnosti kraje mobilnih naprav iz leta 2006, ko je take vrste napadov zabeležilo 47 odstotkov organizacij, na 50 odstotkov. Med anketiranimi organizacijami je bilo zaznati tudi veliko nepooblaščenih dostopov do informacij, in sicer pri kar 25 odstotkih.

Zaznali so tudi veliko drugih pogostejših groženj, ki pa neposredno z mobilnimi napravami niso povezane.

## 3.2 Analiza tveganj

### 3.2.1 Osnovni pojmi

Varnostna analiza tveganj je osnovna zahteva standarda ISO 27000, ki je mednarodno priznan kot generičen standard za varnost informacijskih sistemov. Analiza tveganj je izdelana na osnovi glavnih aspektov informacijske varnosti zaupnost, celovitost ter dostopnost. Kriterij sprejetosti grožnje je definiran z varnostno politiko organizacije [20].

Obstaja veliko metod ter priporočil za pripravo analiz tveganj, vendar vse vključujejo glavna tri področja:

- identifikacija groženj ali možnih neželenih incidentov,
- analiziranje vpliva ter verjetnosti groženj,
- ovrednotenje grožnje z ozirom na kriterije odobritve.

Postopek izdelave analize tveganja vključuje naslednje korake:

- Identifikacija vsebine analize: opis sistema, ki ga bomo v analizi obravnavali.
- Identifikacija groženj: identifikacija možnih scenarijev, ki se lahko zgodijo.
- Analiza vpliva ter verjetnosti pojavitve posamezne grožnje.
- Ocena tveganja: v povezavi z ocenjenim tveganjem ter kriterijem sprejemljivosti[1].
- Grožnje tveganj: identifikacija in ugotavljanje možnosti groženj.

Analiza tveganj predstavlja formalni pristop za oceno izpostavljenosti. Ugotoviti je potrebno, katere grožnje pretijo ter kako lahko te grožnje vplivajo na poslovanje. V nadaljevanju je prikazana analiza tveganja za mobilne naprave. Analiza tveganj je osnova za izdelavo varnostne politike.

Grožnja je dogodek ali okoliščina, ki bi lahko šla v sistemu narobe (požar, poplava, vdor napadalca, okvara opreme itd.) in bi posledično povzročila izpad informacijskih virov ter škodo pri poslovanju. Grožnje so prisotne v vsakem informacijskem sistemu [26].

Obstajajo štirje različni pristopi, kako se spopasti z grožnjami [19].

- **Sprejem grožnje** skladno z varnostno politiko organizacije. Dovolj majhne grožnje, ki so lahko sprejemljive. Sprejem grožnje ne pomeni sprejem neželenega incidenta identificiranega z grožnjo.

- **Zmanjšanje grožnje** na sprejemljiv nivo. Odkar je grožnja posledica verjetnosti ter posledic, to pomeni zmanjšanje verjetnosti ali posledice, lahko pa tudi obeh.

[1] Kriterij sprejemljivosti pomeni stopnja grožnje katere se zavedamo, vendar jo sprejmemo in stojimo za njo.

Običajno je težko zmanjšati posledice. Bolj smiselno in lažje se je v prvi vrsti usmeriti na zmanjšanje verjetnosti dogodka.

- **Izognitev grožnji** – ne počnite stvari, ki lahko povzročijo uresničitev grožnje.
- **Prenos grožnje na tretjo stranko** (npr. zunanjega izvajalca).

Z analizo tveganj sistematično opredelimo informacijske vire in grožnje, ki jim pretijo ter na ta način podrobno spoznamo naravo in strukturo tveganj. Izvedba analize tveganj in poznavanje metodologije ocenjevanja prispevata k razumevanju izpostavljenosti in bistveno pripomoreta h kakovostnim odločitvam poslovodstva glede načina in obsega obvladovanja tveganj. Ocenjevanje in analiza tveganj je eden od osnovnih in prvih korakov, ko ugotavljamo skladnost varovanja podatkov in informacij s skupino standardov ISO 27000. Že ISO/IEC 27001 v poglavju o postavitvi in upravljanju ISMS sistema govori o zahtevi po določitvi metode ocenjevanja in analiziranja tveganj. Ocenjevanje in analiziranje tveganj je rdeča nit cele družine standardov ISO 27000, zato je ključnega pomena, da izberemo in uvedemo metodo, ki je jasna, učinkovita in ekonomična. Redkokdaj analiziramo vsa tveganja. Največkrat se odločimo podrobneje analizirati le zelo velika, manjša tveganja pa sprejmemo[27].

### 3.2.2 Metoda izdelave analize tveganj

Za analiziranje varnostnih izzivov za mobilne naprave v farmacevtskem podjetju sem pripravil splošno kvalitativno analizo tveganj informacijske varnosti na mobilnih napravah. Glavni cilj je identifikacija varnostnih groženj pri uporabi mobilnih naprav ter v prvi fazi funkcionalnost elektronske pošte na njih, ter poiskati sprejemljive rešitve za posamezne grožnje.

Pri izdelavi analize sem šel skozi pet glavnih korakov izdelave analize tveganj, predstavljenih v predhodnem poglavju.

1. Identifikacija vsebine analize

Vsebina analize se nanaša na službene mobilne naprave kot samostojne naprave ter uporaba službene elektronske pošte na njih. Elektronsko pošto na mobilnih napravah se zagotavlja s pomočjo ActiveSync tehnologije. Uporablja pa se tudi strežniški in klient certifikat za avtentikacijo. Avtentikacija je integrirana z aktivnim imenikom podjetja.

Storitev ActiveSync pa deluje na osnovi "push"[2] tehnologije. Ostalih storitev zaenkrat na mobilnih napravah v farmacevtskem podjetju ne podpiramo.

2. Identifikacija groženj

Identifikacija groženj je bila izdelana s pomočjo »ustvarjalnega pretresa« (ang. brainstorming) varnostnega inženirja podjetja ter strokovnjaka, ki pokriva mobilne naprave v podjetju. Rezultat identifikacije groženj pa je prikazan v tabeli s polji:

- unikatna številka grožnje,
- opis grožnje oz. neželenega dogodka,
- opis posledic,
- verjetnost pojavitve,
- vrednost grožnje,
- komentar.

Pri strukturiranem brainstormingu je bil narejen pregled arhitekture z upoštevanjem predefiniranih smernic ter atributov. Smernice so se nanašale predvsem na vidike varnosti, kot je zaupnost, integriteta ter dostopnost. Atributi pa so bili interne in zunanje grožnje ter premišljene in naključne aktivnosti, ki se lahko zgodijo.

Tabela z grožnjami ni statična in je uporabljena kot orodje skozi celoten proces. V tabelo so bile zapisane vse možne grožnje. Na koncu je bilo izdelano »čiščenje« tabele. Ta metoda se imenuje HazOp metoda (HazOp – hazard and operability study) za identifikacijo groženj, ki lahko pripeljejo do hazarda. HazOp je razvil metodo za analiziranje varnosti sistemov v industriji. Kasneje je bil apliciran na ostala področja.

3. Analiza vpliva in verjetnosti

Identificirane grožnje ter neželjeni incidenti so analizirani. Za vsako goržnjo pa je bil izdelan vpliv oz. posledice v primeru, da se izvrši. Vsaka grožnja je pridobila kvantitativno vrednost za posledice in verjetnost pojavitve (npr. zelo malo, malo, srednje, veliko, zelo veliko). Definicije za kvalitativne vrednosti posledic ter verjetnosti so predstavljene v spodnji tabeli.

[2] **Push tehnologija** ali **server push** je komunikacija, ki poteka preko interneta, sejo pa iniciira strežnik.

| Posledice | Opis |
|---|---|
| **Zelo majhne** | Ne vpliva na zaupnost, integriteto ter dostopnost informacij. V nekaterih primerih lahko vpliva na zanesljivost nekaterih uporabnikov. |
| **Majhne** | Kratke motnje dostopnosti za nekatere uporabnike ali skupine uporabnikov. Ni vpliva na zaupnost ali integriteto. |
| **Srednje** | Prekinitve dostopnosti za vse uporabnike ali skupino uporabnikov za daljšo časovno periodo. Ni vpliva na zaupnost ali integriteto. |
| **Velike** | Vpliv na informacijsko zaupnost, integriteto in dostopnost, ki vpliva na vsakega posameznega uporabnika, ne pa na storitev kot celoto. |
| **Zelo velike** | Vpliva na infomacijsko zaupnost, integriteto ter dostopnost, ki vpliva na vse uporabnike ter na storitev kot celoto. |
| **Verjetnost pojavitve** | |
| **Zelo malo** | Zelo redko. Pojavi se manj kot v 0,1% primerih |
| **Malo** | Redko. Pojavi se v primerih med 0,1% ter 1%. |
| **Srednje** | Se lahko zgodi. Pojavi se v primerih med 1% in 5%. |
| **Veliko** | Precej pogosto. Pojavi se v primerih med 5 in 20%. |
| **Zelo veliko** | Zelo pogosto. Pojavi se v več kot 20% primerih. |
| **Nivo tveganja** | |
| **Brezpredmeten** | Sprejemljivo. |
| **Majhen** | Sprejemljiva grožnja. Storitev se lahko uporablja z identificirano grožnjo, vendar pa je potrebno grožnje opazovati, da se ne bi zaradi kakšnih sprememb povečala grožnja. |
| **Zmeren** | Za storitev lahko obstaja sprejemljiva grožnja, vendar pa je potrebno za vsak primer ugotoviti, ali so bile implementirane ustrezne mere. |
| **Visok** | Ni sprejemljiva grožnja. Storitev se ne sme pričeti uporabljati, dokler se ne zmanjša stopnje tveganja. |

**Tabela 1: Definicije posledic, verjetnosti ter tveganj, ki se uporabljajo pri analizi tveganja**

4. Ocena tveganja

Tveganje za vsako grožnjo je bilo izračunano kot produkt posledice ter verjetnosti, predstavljeni v dvodimenzionalni matriki. V celice matrike so vpisane številke posameznih groženj. Glede na kriterij sprejemljivosti so definirani štiri nivoji tveganj: brezpredmeten, majhen, zmeren, visok. Nivo tveganja visoko je določen kot

nesprejemljiv. Vsaki grošnji s tem nivojem tveganja je potrebno določiti ukrepe ,s katerimi se bo nivo tveganja zmanjšal na sprejemljivega.

5. Ukrepi

Za vse grožnje z nesprejemljivim nivojem tveganja so bili predlagani ukrepi. Ukrepi so opisani v poglavjih 3.2.4 Grožnje povezane z uporabo mobilnih naprav 3.2.5 Grožnje povezane s škodljivo programsko opremo ter 3.2.6 Grožnje povezane z arhitekturo sistema.

### 3.2.3 Rezultati analize tveganja

Spodnja tabela prikazuje grožnje, ki so bile identificirane tekom izdelovanja analize tveganja. Tabela za vsako grožnjo prikazuje ocenjeno verjetnost uresničitve grožnje ter posledice.

Veliko identificiranih groženj je splošnih, predvsem so povezane z mobilnimi napravami ter zaupnimi podatki, seveda pa so v tabeli navedene tudi grožnje, ki so vezane tudi na specifičnost obravnane storitve na mobilni napravi.

V izdelani analizi tveganj sem našel tri grožnje, ki imajo nesprejemljiv nivo tveganja, kot je lahko tudi razvidno iz matrike tveganj (Tabela 2). Dve izmed teh groženj (8 ter 17) se nanašata na verjetnost pojavitve tveganja, ko je mobilna naprava istočasno povezana iz ene možne povezave v varno, nadzorovano omrežje, z drugo možno povezavo pa istočasno na javni internet in je tako izpostavljena tveganjem z interneta. Ta grožnja predstavlja zelo veliko tveganje, kajti na ta način je potencialnemu napadalcu odprta prosta pot do internega omrežja podjetja.

| Posledice / Verjetnost | Zelo majhne | Majhne | Srednje | Velike | Zelo velike |
|---|---|---|---|---|---|
| Zelo majhna | | | | 7 | |
| Majhna | 16 | | 18, 19 | 9 | 4 |
| Srednja | 11 | | 14 | 1, 3, 12, 15 | |
| Velika | 13 | | 2, 6 | 5, 8 | |
| Zelo velika | | | | 17 | |

**Tabela 2: Matrika tveganj za storitev elektronske pošte, kjer so prikazani tudi različni nivoji tveganj (brezpredmeten, majhen, zmeren, visok).**

Pri identifikaciji možnih groženj je potrebno upoštevati predvsem to, da so mobilne naprave vse bolj zmogljive ter da na njih narašča količina poslovno kritičnih informacij. Potrebno se je zavedati groženj ter pričeti izvajati aktivnosti. Sprememb ni mogoče narediti v trenutku, temveč je za to potreben čas [23].

| Zap. Št. | Grožnja |
|---|---|
| 1 | Mobilna naprava z aktivnim klientom se lahko izgubi ali pa je ukradena s strani tretje osebe, ki lahko v imenu uporabnika pridobi določene informacije ter pošilja/prejema elektronsko pošto v imenu uporabnika. |
| 2 | Ugasnjeno mobilno napravo lahko nepooblaščena oseba najde ali ukrade – uporabnik ostane brez mobilne naprave. |
| 3 | Ugasnjeno mobilno napravo lahko nepooblaščena oseba najde ali ukrade. Nepooblaščena oseba lahko poskuša resetirati PIN kodo ali kako drugače priti do podatkov shranjenih na mobilni napravi. |
| 4 | Ugasnjeno mobilno napravo lahko nepooblaščena oseba najde ali ukrade. Nepooblaščena oseba lahko poskuša priti do gesla samega klienta. Pri tej grožnji se predpostavlja, da je nepooblaščeni osebi že uspelo ugotoviti PIN kodo. |
| 5 | Izguba zunanje spominske kartice, na kateri so shranjeni zaupni podatki. Podatki so lahko razkriti nepooblaščenim osebam – kršenje zaupnosti podatkov. |
| 6 | Izguba zunanje spominske kartice, na kateri so shranjeni zaupni podatki. |

| Zap. Št. | Grožnja |
|---|---|
| | Podatki so izgubljeni in nedostopni. |
| **7** | Prejem virusa na mobilno napravo pri sinhronizaciji podatkov s PC. |
| **8** | Povezave preko bluetootha ali ostale storitve oz. omrežja, ki dostavljajo podatke od zunaj (SMS, MMS, infrared). Lahko dajo poln dostop do storitev na mobilni napravi. Metode napada so lahko prepis podatkov, zloraba slabosti protokolov itd. Storitve, ki lahko spremenijo konfiguracijo naprave (SMS). |
| **9** | Nepooblaščeni uporabniki lahko mobilno napravo najdejo oz. jo za kratek čas ukradejo ter spremenijo konfiguracijo naprave, npr. vklopijo Bluetooth. To lahko nepooblaščenim osebam omogoči dostop do storitev ali izrabo pomanjkljivosti protokolov (glej grožnjo 8). |
| **10** | Kršenje interne varnostne politike ter nenamerno povezovanje internega omrežja (npr. preko WiFi) ter zunanjega omrežja (npr. preko GSM/GPRS). S tem se celotno interno omrežje odpre za zunanje napadalce in omogoči nekontroliran prenos podatkov iz internega omrežja v zunanje omrežje. |
| **11** | Mobilna naprava je ves čas povezana na internet (npr. preko GPRS) ter tako izpostavljena vsem mogočim grožnjam z interneta.<br>Npr. prenehanje delovanje storitve |
| **12** | Mobilna naprava je ves čas povezana na internet (npr. preko GPRS) ter tako izpostavljena vsem mogočim grožnjam z interneta.<br>Npr. nepooblaščene osebe lahko pošiljajo elektronsko pošto v imenu uporabnika, jo berejo, odgovarjajo. To predstavlja kršitev zaupnosti, integritete ter dostopnosti. |
| **13** | ISA strežnik, preko katere je objavljena storitev elektronske pošte, je lahko zlorabljena s strani nepooblaščenih oseb, ker se nahaja v DMZ. Storitev ni dostopna oz. ne deluje. |
| **14** | ISA strežnik, preko katere je objavljena storitev elektronske pošte, je lahko zlorabljena s strani nepooblaščenih oseb, ker se nahaja v DMZ. Sporočila niso poslana naprej oz. niso poslana ob pravem času. |
| **15** | Obstajajo občutljivi podatki, shranjeni na sami mobilni napravi. Podatki so zlorabljeni, s tem je povzročena kršitev zaupnosti, če mobilno napravo uporabi nepooblaščena oseba. |
| **16** | Zloraba LDAP strežnika |

| Zap. Št. | Grožnja |
|---|---|
| | Nepooblaščena oseba lahko spremeni uporabniško ime in geslo, storitev uporabniku ne deluje več. |
| **17** | Mobilni uporabnik se lahko premika iz nadzorovane cone v nenadzorovano (uporaba brezžičnega omrežja). Mobilna uporaba je lahko uporabljena kot mehanizem za komunikacijo oz. prenos podatkov med nadzorovano in nenadzorovano cono. Poleg prenosa podatkov se v nadzorovano okolje lahko prenese tudi neželena programska oprema ali virus, ki lahko okuži nadzorovano okolje oz. okolje podjetja. |
| **18** | Storitve niso dostopne, ker se uporabnik giblje izven dosega GSM/GPRS omrežja. |
| **19** | Storitve niso dostopne, ker se uporabnik giblje na območjih, kjer je uporaba mobilnih naprav prepovedana ( bolnišnice, letala ...). |
| **Grožnja 10 ni bila upoštevana v analizi tveganj, kajti ni bilo mogoče objektivno oceniti verjetnosti pojavitve.** | |

**Slika 14: Grožnje na mobilnih napravah**

### 3.2.4 Grožnje povezane z uporabo mobilnih naprav

Večina najbolj resnih groženj, ki sem jih identificiral, se nanašajo na možno razkritje zaupnih informacij. Razkritje zaupnih informacij se lahko zgodi na različne načine:

- Ena izmed splošnih groženj pri uporabi mobilnih naprav je možnost, da uporabniki izgubijo mobilno napravo (grožnje od 1 do 5 ter grožnja 9). Z velikim številom uporabnikov mobilnih naprav obstaja tudi zelo velika verjetnost, da jo bo nekdo izmed uporabnikov izgubil. Če je izgubljena mobilna naprava najdena, ima najditelj možnost, da poskusi dostopiti do storitev na mobilni napravi ter se predstavljati v imenu uporabnika. Če so zaupne informacije shranjene ter nekriptirane na sami mobilni napravi, so lahko prebrane s strani nepooblaščene osebe (grožnja 18). Obstaja tudi majhna verjetnost, da bo nepooblaščena oseba poskusila ugotoviti ali zamenjati geslo mobilne naprave, da bo lahko uporabljala storitev elektronske pošte na mobilni napravi (grožnja 4). Ko je mobilna naprava izgubljena, je velika razlika med tem, ali je naprava vklopljena ali je izklopljena:

  - Če je mobilna naprava izključena, je določena stopnja zaščite zagotovljena z obvezno uporabo PIN kode pri vklopu naprave (grožnja 2), še vedno pa obstaja možnost, da bo najditelj poskusil zlomiti PIN (grožnja 3). Brez številke PIN najditelj lahko zamenja SIM (subscriber identity module) kartico, z njegovo SIM kartico, katere PIN pozna ter ima tako prost dostop do vseh informacij shranjenih na mobilni napravi, ki niso kriptirane (grožnja 15).
  - Če je mobilna naprava izgubljena, ko je vključena ( grožnja 1 in 9), je možno grožnjo omejiti z mehanizmom, ki po določenem času neaktivnosti zahteva ponoven vpis PIN kode. Časovno okno je potrebno določiti z upoštevanjem razmerja med varnostjo ter uporabnostjo. Prepogosto vnašanje kode PIN bi namreč pri uporabnikih vzbudilo fustracije.

- Zunanja spominska kartica lahko ravno tako vsebuje zaupne informacije, ker informacije niso zaščitene s PIN številko, jih je enostavno ukrasti, ne da bi bila ukradena celotna naprava (grožnja 5).

Najbolj enostaven način za zmanjšanje groženj je, da se izognemo shranjevanju zaupnih informacij na mobilno napravo. Priporočeno je, da se sporočila, ki vsebujejo zaupne informacije zbriše ali pa kriptira, ter na tak način onemogoči neposreden dostop do zaupnih informacij. Možno je tudi omejiti, koliko elektronske pošte za nazaj se shranjuje na mobilni napravi (za 14 dni, 1 teden).

Če uporabnik izgubi njegovo mobilno napravo, bodo storitve nedosegljive (grožnja 2 in 6). Da uporabniki ne bi bili preveč dolgo časa brez storitev na mobilnih napravah, je potrebno v primeru izgube, kraje ali okvare naprave definirati postopke zamenjave mobilne naprave.

Storitve na mobilni napravi postanejo nedosegljive tudi, če mobilna naprava izgubi povezavo do omrežja (grožnja 18 ter 19). To se lahko zgodi, če se v omrežju pojavijo napake, če je naprava zunaj dosega omrežja ali če se naprava nahaja v območjih, kjer je uporaba mobilnih naprav prepovedana. Zgoraj naštete težave so neizogibne.

Veliko bolj resna grožnja je  povezana z možno izgubo informacij iz poškodovanega spomina, kot posledica prekinitve v napajanju, napake v programu, napake na napravi.

Grožnja je lahko veliko bolj pomembna, če so bila sporočila shranjena, vendar še neprebrana, vendar pa imajo uporabniki vsa sporočila shranjena tudi še na sporočilnem sistemu.

### 3.2.5 Grožnje povezane s škodljivo programsko opremo

Naslednja skupina resnih groženj je povezana z direktno povezavo mobilne naprave in varnega omrežja podjetja ter s tem možnost okužbe s škodljivo programsko opremo:

- Ena mobilna naprava je lahko istočasno povezana na zunanje nezaščiteno omrežje preko GPRS ter interno nadzorovano omrežje, preko wireless omrežja (WLAN) (grožnja 17). V takem primeru je mobilna naprava mehanizem za prenos podatkov med varnim in nevarnim območjem omrežja. Na tak način se lahko prenese tudi škodljiva programska oprema. To je lahko tudi »malware« za osebne računalnike, priključene v omrežje, brez povzročitve škode na mobilni napravi, ki je uporabljena zgolj kot prenosni medij. Danes obstaja že kar nekaj virusov, ki lahko okužijo tudi mobilne naprave, vendar pa število teh virusov strmo narašča [56].

- Sinhronizacija mobilne naprave z uporabnikovim osebnim računalnikom je naslednji način za prenos škodljive programske opreme. Če mobilna naprava uporablja GPRS istočasno, ko je povezana na PC v lokalnem omrežju, lahko naprava ponesreči povzroči povezavo med tema dvema omrežjema. Potencialnemu napadalcu se s tem popolnoma odprejo vrata iz zunanjega omrežja v notranje omrežje in s tem nenadzorovan pretok podatkov.

- Napadalec se lahko na mobilno napravo poveže preko Bluetootha ali katere druge omrežne storitve (infrardeča povezava, SMS/MMS) (grožnja 8). V najslabšem primeru lahko napadalec pridobi popoln nadzor nad mobilno napravo. Napad je lahko izvršen s prekoračitvijo spomina, izkoriščanje slabosti protokola ali izvajanje ukazov, ki lahko spremenijo konfiguracijo mobilne naprave.

Za zmanjšanje grožnje okužbe je priporočljivo definirati omejitve pri uporabi mobilne naprave, predvsem pri povezovanju mobilne naprave na razna omrežja. Istočasna uporaba Bluetootha ali IR-a ter ostalih omrežnih povezav je prepovedana. K zmanjšanju grožnje bo pripomogla tudi namestitev antivirusnega programa na mobilno napravo in

na osebni računalnik. Mobilna naprava bi morala biti skonfigurirana na način, da ne bi mogla biti istočasno povezana na notranje in zunanje omrežje.

### 3.2.6 Grožnje povezane z arhitekturo sistema

Napadi na mobilni napravi so lahko usmerjeni na osebne računalnike, na samo storitev, ki se izvaja na mobilni napravi ali pa celo na lokalno omrežje. To lahko povzroči različne vrste problemov. Storitev lahko postane nedosegljiva, sporočila niso dostavljena ali so dostavljena ob napačnem času. Napadalec lahko v imenu uporabnika pošilja sporočila in celo pride do zelo občutljivih podatkov podjetja.

Napadalci lahko tudi napadejo in prevzamejo nadzor nad proxy strežnikom, vendar je to manj verjetno, ker se ta strežnik ponavadi nahaja v bolj varovanih območjih.

Veliko število groženj sistemu je povezanih z načinom uporabe mobilnih naprav, ne pa s tehnologijo. Tehnične rešitve za izboljšanje varnosti bodo imele majhne učinke brez ustreznega zavedanja uporabnikov [56]. Za zmanjšanje tveganja se je potrebno torej osredotočiti tudi na netehnične ukrepe. Najbolj pomemben ukrep je izobraževanje uporabnikov, jih obveščati in seznaniti z grožnjami ter jim razložiti razloge za tehnične omejitve in postopke pri uporabi.

## 3.3 Varnostna politika farmacevtskega podjetja

Obravnavano farmacevtsko podjetje ima izdelano krovno varnostno politiko za varovanje informacijskega sistema in podatkov podjetja. Varnostna politika se uporablja za zaščito vseh delov informacijskega sistema tako, da predpisuje pravila in postopke za zagotavljanje varnosti. Politika obravnava področje uporabe strojne in programske opreme, varovanja dostopov do opreme in prostorov, pravila za nadgrajevanje in menjavo opreme, postopke za zagotavljanje, preverjanje in hranjenje varnostnih kopij podatkov, metode za zagotavljanje varnosti prenosa podatkov itd.

V zadnjih letih je farmacevtsko podjetje dograjevalo varnostno politiko in prakso z novimi pravili in postopki za dnevni nadzor informacijskega sistema, za poročanje o dogodkih operativnega tveganja, za evidentiranje incidentov. Poleg navedenega podjetje izvaja redno letno izobraževanje zaposlenih, kjer jih informira in opozarja v zvezi z uporabo informacijske tehnologije in varnostjo poslovanja. Varnostna politika in postopki za zaščito informacijskega sistema so del rednih pregledov notranje in zunanje revizije. Leta 2007 je farmacevtsko podjetje pridobilo standard ISO/IEC 27001.

Pri vzdrževanju varnostne politike in zagotavljanju zaščite informacijskega sistema podjetje poskuša upoštevati mednarodna standarda ISO/IEC 17799:2005 ter ISO/IEC 27001:2006. Poleg navedenega farmacevtsko podjetje upošteva tudi zbirke najboljših praks v informatiki.

## 3.4 Varnostna politika za mobilne naprave

Ob upoštevanju smernic, ki jih navajajo varnostni standard BS 7799, delovni okvir COBIT, zbirka najboljših praks ITIL ter predhodno izvedena analiza tveganj je nastala varnostna politika za mobilne naprave, ki je predstavljena v nadaljevanju. Konkretna varnostna politika ni predstavljena, temveč so predstavljena predvsem področja, ki jim je potrebno v varnostni politiki posvetiti največ pozornosti.

Varnostne politike za mobilne naprave definirajo pravila, kako uporabniki uporabljajo naprave ter se povezujejo z njimi v podjetje. Če je naprava mobilna in vsebuje podatke podjetja, moramo biti prepričani, da so podatki varni tudi če naprava pride v napačne roke.

Varnostna politika bo zahtevala kriptiranje podatkov na napravi, kot tudi povezovanje v podjetje. Varnostne politike podjetja tudi zahtevajo, da so naprave zaščitene z gesli ter da geslo in naprava ne moreta biti zlorabljena s strani nepooblaščenih uporabnikov.

Politika tudi določa pravila pri geslih npr. kako dolgo mora biti geslo, iz kakšnih znakov je lahko sestavljeno, na koliko časa ga je potrebno zamenjati, kaj se zgodi, ko je vneseno napačno geslo ….

Politika od administratorjev zahteva, da izdelajo enostavne varnostne rešitve, ki jih je lahko upravljati, ponavljati ter temeljijo na varnostnih zahtevah podatkov podjetja.

### 3.4.1 Kje začeti

Potrebno je začeti z vzrokom, zakaj se uporabljajo naprave v podjetju. S to informacijo je potrebno zapisati omejitve, ki se jih želi narediti nad podatki podjetja. Nato je potrebno želene omejitve pretvoriti v tehnične rešitve.

Varnostna politika so prava tehnična vodila oz. priporočila in morajo biti tudi zahteva, ki jo mora srečati vsaka naprava. Priporočila morajo izhajati iz krovne IT varnostne politike podjetja, ki jih je potrebno upoštevati. Ker so te varnostne politike na višjem nivoju, ni potrebno, da vsebujejo vse podrobne informacije o vsaki napravi. Za

podrobnosti pri vsakem področju se priporoča narediti poseben dokument, ki opisuje vse specifike in detajle področja, ki ga pokriva.

Ko se določa varnostna politika, se ne sme upoštevati, ali določena pravila trenutna tehnologija lahko omogoči ali ne. Ko so priporočila izdelana, je potrebno izdelati varnostne rešitve, da ustrezajo priporočilom, ter v kolikor je potrebno, se lahko izdela prilagoditev priporočil po opravljeni oceni. Če je prišlo do ocene, da je nemogoče zadostiti priporočilom določenih v varnostni politiki, se je potrebno odločiti, ali se mobilne naprave v podjetju prepove ali pa se priporočila spremenijo. Odločitev mora biti osnovana na tveganjih ter preučena na poslovnem nivoju in ne na tehničnem.

**Prijava na mobilno napravo**

Glavni del varnostne politike je prijava na napravo. Na standardni napravi je lahko uporabljen enostaven štirimestni pin ali bolj zahtevno geslo. Lahko se nastavi tudi tako, da je potrebno vnesti geslo vsakič, ko se naprava prižge. To je vsekakor bolje, kot da bi bila naprava brez varnosti. Če je naprav izgubljena ali ukradena, ima uporabnik neomejene možnosti za preizkušanje pravilnosti gesla ter tehnične možnosti, da pride do podatkov na napravi.

Uporabnik ima lahko tudi zelo enostavne pin številka, kot npr. 0000, vendar pa je enostavne pin številke enostavno uganiti.

Zagotoviti je potrebno orodja, s katerimi se upravlja z opcijami gesel. Orodja morajo zagotavljati različne aktivnosti v primeru napačnega vnosa gesel nekajkrat zaporedoma, npr. resetiranje naprave na tovarniške nastavitve, blokiranje prižiganja naprave, zahtevanje sprememb gesel na določeno časovno periodo.

**Oddaljeno uničevanje ter onemogočanje**

Nekatera orodja imajo funkcionalnost za oddaljeno uničenje naprave ter podatkov na njej, vendar pa se na funkcionalnost ne sme zanašati, ko so naprave ukradene ali izgubljene.

**Ukradena mobilna naprava**

Ukradena mobilna naprava predstavlja varnostno grožnjo iz vidikov naprave in omrežja. Ker naprava ne vsebuje zgolj informacije podjetja, kot so dokumenti, elektronska pošta,

temveč vsebujejo tudi omrežne informacije, predvsem avtentikacijske informacije za dostop do omrežja podjetja. V kolikor napadalec ukrade napravo, nima samo dostopa do podatkov podjetja, temveč ima dostop tudi do infrastrukture podjetja. Ko imajo napadalci te informacije, je napad na celotno podjetje trivialen. V izogib takšnim situacijam se lahko uporabi funkcionalnost, oddaljeno uničevaje, s čimer se uničijo vsi podatki na napravi, vključno s konfiguracijami.

Ni se varno zanašati na oddaljeno uničevanje podatkov. Saj lahko da naprava ni povezana v omrežje in je torej nedosegljiva za ukaze centralnega sistema za upravljanje z napravami. Storilec lahko odstrani SIM kartico ali pa jo zamenja z drugo, naprava je lahko zunaj dosega omrežja mobilnega operaterja, WiFi omrežja, lahko pa je tudi prazna baterija na mobilni napravi, naprava je lahko povezana na drugo podatkovno omrežje ali pa je povezana preko drugega uporabniškega imena in gesla. Zgoraj je naštetih preveč vzrokov, da bi se na omenjeno funkcionalnost lahko z gotovostjo zanesli.

**Izgubljena mobilna naprava**

Če je naprava izgubljena, se lahko nahaja v neznanih rokah. Z oddaljenim uničenjem podatkov na napravi je za uporabnika v primeru izgube naprave enostavno poklicati administratorja ter od njega zahtevati uničenje podatkov na napravi. Če je naprava »resetirana« (to se lahko zgodi zgolj, da so izpolnjeni vsi pogoji in je naprava povezana v pravo omrežje), se napravo lahko najde, potem je uporabnik brez nje vse dokler administrator ne nastavi vseh potrebnih parametrov za nemoteno nadaljnjo uporabo naprave. Če je uporabnik v drugi državi ali na oddaljeni lokaciji, pa je lahko zelo resna nevšečnost.

Lahko se uporabi tudi drug način upravljanja naprav, in sicer da se uporabi varnostne aplikacije, ki uničijo podatke na napravi, v kolikor se vnese napačen pin ali geslo. To zagotavlja, da se izbris podatkov zgodi v pravi situaciji, to je, ko želi nekdo nepooblaščeno priti do podatkov na napravi. To se ne bo zgodilo uporabniku, ki pozna geslo.

**Varnostno kopiranje in objavljanje**

V kolikor je naprava ukradena ali izgubljena, je možnost restavriranje informacij ukradene naprave na drugo novo napravo. Procedure za varnostno kopiranje in

obnavljanje morajo biti dobro definirane in sledljive. Večina mobilnih naprav ima v paketu tudi programe za varnostno kopiranje in restavriranje. Tudi enostavno kopiranje podatkov na osebni ali prenosni računalnik ter IPM sinhronizacija je bolje kot da ne obstajajo kopije potrebnih informacij za nadaljnje nemoteno delo uporabnika.

Politika bi morala definirati, kdaj se podatke kopira, frekvenco kopiranja ter zagotoviti, da se kopije podatkov hranijo in varujejo na enak način kot originalni podatki.

**Pomnilniške kartice**

Pomnilniške kartice so tako priročne kot možnost razširitve vgrajenega spomina na napravi, vendar so tudi prenosne in predstavljajo dodatno varnostno grožnjo. Potrebno je imeti v mislih zaklepanje dostopa do podatkov na spominski kartici, kriptiranje podatkov na spominski kartici. Tudi za to obstajajo orodja, ki omogočajo omejen dostop do vsebine na podatkovnih karticah ali kriptiranje vsebine na podatkovnih karticah.

**Aplikacije**

Če se določi politika, ki uporabniku omejuje dostop do določenih funkcionalnosti ter aplikacij, je potrebno določiti, kako naj se uporabnik ogne omejitvam pri nameščanju dodatne programske opreme. Obstajata dva pristopa. Prvi je onemogočanje dostopa do specifičnih aplikacij, kar je učinkovito za določene aplikacije, v kolikor si uporabnik namesti drugo aplikacijo, ki ima enake funkcionalnosti, potem zaščita ne velja več. Drugi pristop je, da se naredi seznam podprtih in dovoljenih aplikacij ter omejitev uporabnika na list aplikacij. Potrebno pa je pazljivo nastaviti omejitve, kajti v primeru, ko ima uporabnik pravico preimenovati datoteke ali na mobilni napravi ali preko ActiveSync aplikacije, bo lahko preprečil zaščito s preimenovanjem nedovoljene aplikacije v dovoljeno.

**Prenos informacij**

Potrebno je zagotoviti tudi varovanje pretoka informacij na in iz naprave. Večina novih naprav vsebuje enega ali več načinov prenosa podatkov, kot so npr. BlueTooth, WiFi, Cellular Data, Infrared, Storage cards, Active Sync, RAPI povezava. Varnostna politika podjetja mora določati, ali so te funkcionalnosti vklopljene ali izklopljene, ter tudi v primeru, ko se jim dovoli, da so vklopljene, npr. BlueTooth, ali so lahko naprave vidne drugim napravam ali ne.

Za lokalne povezave je potrebno zmanjšati tveganje nameščanje nepooblaščenih aplikacij, kot so razne igre, potrebno je tudi določiti pravila, kako upravljati s temi aplikacijami ter jih onemogočiti.

Omrežne povezave morajo pokriti tako oddaljen dostop do mobilne naprave kot tudi metode, ki se jih uporablja za povezavo do podatkov podjetja.

Če gre za povezavo preko omrežja, je potrebno zagotoviti tudi varnost na nivoju omrežja. Potrebno je predvsem določiti, kdaj je omrežna povezava zaupanja vredna in kdaj ne, npr. private access controlled network ali public available network. Če omrežje ni zaupanja vredno, potem je potrebno omejiti storitve, ki so dosegljive določenemu omrežju na tista omrežja, za katere ste prepričani, da so dovolj varni.

Požarni zidovi so zelo dobri za zaščito naprav zunanjih napadov na osebnih računalnikih, njihova uporabnost na mobilnih napravah pa je omejena, kajti v osnovi ni nabora storitev, ki so potencialne za napad. Ponavadi so na mobilnih napravah nameščene posebne aplikacije, ki imajo posebne zahteve, različne ena od druge, zato je potrebno premisliti, kdaj se splača namestiti orodja, ki imajo funkcionalnosti požarnega zidu.

**Komu zaupamo?**

Potrebno se je vprašati, koliko zaupamo svojim zaposlenim. Ali striktno določite standarde ter jih vsilite svojim zaposlenim preko varnostnih in programskih sistemov ali samo zahtevate enostavna gesla za dostop do naprave ter kriptiranje podatkov, izbiro katere aplikacije bo uporabnik uporabljal pa prepustite posameznemu uporabniku. Seveda je ta odločitev odvisna od vrste podatkov, s katerimi uporabniki operirajo na mobilnih napravah, kako bodo mobilne naprave uporabljene in kdo jih bo uporabljal.

**Ugotovitve**

Ko je varnostna politika definirana, se hitro izkaže, da dejansko ne obstaja niti ena aplikacija, ki bi ustrezala vsem vašim zahtevam ter potrebam. Npr. ugotovite, da varnost na napravi deluje z enim produktom odlično, vendar pa ne omeji dostopa aplikacij v zadostni meri. Potrebno je biti pripravljen na uporabo hibridne rešitve ter potrebno je testiranje hibridne rešitve kot celote. Vsaka organizacija je drugačna in ima drugačne varnostne potrebe.

# 4 Obvladovanje mobilnih naprav

Obvladovanje ter upravljanje mobilnih narav (ang. Mobile Device Management – MDM) je pojem, ki opisuje rešitve za oddaljeno upravljanje z mobilnimi napravami. V magistrski nalogi s pojmom mobilne naprave označujem osebne digitalne pomočnike (ang. Personal digital assistent–PDA), pametne telefone ter druge manjše prenosne naprave podobnih funkcionalnosti. Večina rešitev za upravljanje mobilnih naprav se osredotoča na PDA naprave ter na pametne telefone [24].

Naprave imajo tipično nameščen okrnjen operacijski sistem (ang. micro operating system), ki omogoča, da na napravah tečejo aplikacije. Trenutni vodilni proizvajalci operacijskih sistemov so Symbian, Palm in Microsoft.

V preteklosti so bile mobilne naprave zelo popularne za aplikacije, ki upravljajo osebne informacije, kot so kontakti, naslovi, koledar ter elektronska pošta. Ko so postale naprave zmogljivejše ter hkrati cenejše, so se začele na napravah uporabljati tudi funkcionalnosti brezžičnih internetnih dostopov (WiFi, GSM/GPRS, CDMA etc.), podjetja pa so jih začela uporabljati kot pomembno orodje. Danes je mogoče najti različne razpoložljive aplikacije za upravljanje mobilnih naprav (inventory/asset management), field force automation ter manjše aplikacije, ki imajo dostop do informacijskih sitemov za upravljanje s strankami (ang. Customer relatioship management–CRM) ter informacijskih sitemov za načrtovanje virov podjetja (ang. Enterprise resource planing – ERP) [24].

V splošnem so podjetja spoznala, da so mobilne naprave postale zadnje področje računalništva podjetij oz. prstne konice sistema podjetja (finger tips of an enterprise system).

**Stroški mobilnosti** [24]:

Industrijski analitiki se strinjajo, da so celotni stroški lastništva (ang. Total cost of ownership – TCO) za mobilne naprave okoli 2000€-3000€ letno, ter lahko celo več, če se naprave uporabljajo za industrijske namene. TCO mobilnih naprav je precej večji v primerjavi s prenosnimi ter osebnimi računalniki, predvsem zaradi tega, ker nimajo običajne internetne povezave, se jih lažje izgubi, ukrade ali poškoduje.

Vse večja mobilnost podjetij zahteva implementacijo rešitev za upravljanje z mobilnimi napravami.

**Oddaljeno upravljanje z mobilnimi napravami (ang. Remote Device Management)** [24]:

Večina rešitev za upravljanje z mobilnimi napravami ima naslednje funkcionalnosti:

**Asset management**–zmožnost pregleda, grupiranja naprav glede na lokacijo, tipa naprave ali drugih kategorij.

**Software management**–oddaljeno nameščanje programske opreme na naprave ter nameščanje varnostnih popravkov, nadgradenj.

**Configuration Management**–zagotavlja administratorju zmožnost za konfiguracijo nastavitev ter vnosov v registre mobilnih naprav.

**Performanse in diagnostika**–zagotavljanje informacij o stanju mobilnih naprav, vključno s spominom, baterijami, konfiguracijo omrežja z možnostmi proženja alarmov ter poročil.

**Varnostno kopiranje ter restavriranje mobilnih naprav** – to je ključno za zmanjšanje TCO mobilnih naprav.

**Upravljanje z varnostjo** – zmožnost potiskanja varnostnih nastavitev na napravo, kot je geslo pri vklopu naprave, oddaljeno zaklepanje naprave, če se izgubi ali je ukradena ali celo zmožnost brisanja vseh zaupnih podatkov podjetja.

## 4.1 Upravljanje s konfiguracijami mobilnih naprav

Tako kot ostali IT procesi, je tudi upravljanje konfiguracij najbolje definirano v uvodnem delu magistrske naloge, predstavljenem ogrodju COBIT ter zbirki najboljših praks ITIL. V nadaljevanju je predstavljen splošen proces upravljanja konfiguracij po priporočlih ITILa ter COBITa, na koncu poglavja pa je podana še povezava z mobilnimi napravami.

### 4.1.1 Osnovni pojmi

Proces upravljanja konfiguracij zadovoljuje poslovno potrebo za IT po optimizaciji IT infrastrukture, kapacitet, zmogljivosti ter zbiranju informacij o IT sredstvih.

Upravljanje konfiguracij je usmerjeno v vzpostavljanje in vzdrževanje primernega ter popolnega repozitorija konfiguracije IT sredstev, atributov ter osnovnih konfiguracij, s primerjanjem dejanskega stanja konfiguracije sredstev.

Upravljanje konfiguracij je mogoče izvajati predvsem z vzpostavljenim centralnim repozitorijem z vsemi elementi, ki se konfigurirajo, z identifikacijo elementov in vzdrževanjem ter pregledom integritete konfiguracijskih podatkov.

### 4.1.2 Kontrolni cilji procesa upravljanja konfiguracij

Potrebno je vzpostaviti orodje ter centralni repozitorij, ki bo vseboval vse relavantne informacije o mobilnih napravah, ki so vključene v konfiguracijo. Potrebno je beležiti nabor vseh sredstev ter sprememb v sredstvih. Potrebno je tudi voditi osnovno konfiguracijo o vsakem objektu posebej, da se v primeru napak oz. nepravilnosti pri nastavljanju novih konfiguracij lahko vrnemo na osnovno konfiguracijo, ki deluje.

Potrebno je vzpostaviti tudi postopke za poročanje vodstvu o izvajanju konfiguracij. Potrebno pa je te procedure integrirati s postopki upravljanja konfiguracij, incidentov in problemov.

Potrebno je periodično pregledati podatke o konfiguraciji za potrjevanje integritete trenutne in predhodne konfiguracije, ter tudi pregledati nameščene programe, ali so v skladu s politiko, ter odstraniti programe, ki so v nasprotju s politiko ali licenčnimi pogodbami.

### 4.1.3 Povezava z mobilnimi napravami

Podjetje ima vzpostavljen sistem za upravljanje konfiguracij delovnih postaj, strežnikov, ter ostale IT infrastrukture. Področje mobilnih naprav, kot sem že omenil v uvodnih poglavji, ni urejeno in se ne upravlja sistematično, zato je potrebno zagotoviti integracijo mobilnih naprav v obstoječe procese za upravljanje informacijske tehnologije, ki so se izkazali kot učinoviti.

## 4.2 Upravljanje informacijske tehnologije v podjetju

V podjetju se trenutno uvaja procese po priporočilih najboljših praks ITIL. Trenutno se že izvajajo procesi incident management, problem management ter service desk. Nastajajo pa že zametki procesa upravljanje konfiguracij, vsaj kar se tiče delovnih postaj in strežnikov.

Za upravljanje konfiguracij delovnih postaj, prenosnih računalnikov ter strežnikov v farmacevtskem podjetju uporabljamo Microsoftov produkt System Center Configuration Manager.

Definiran in podprt je tudi že proces upravljanja delovanja, kar izvajamo tudi s pomočjo Microsoftovega produkta System Center Operations Manager. S tem produktom so pokriti vsi strežniki v podjetju, vsi ključni procesi ter tudi kritične delovne postaje, od katerih je odvisno celotno delovanje proizvodnje ali pa informacijske infrastrukture (npr. naprave za nadzor klima naprav …).

Področje mobilnih naprav je potrebno smiselno vključiti v vsakega izmed procesov, ki se v podjetju že izvaja. To se vsekakor od podjetja do podjetja razlikuje. Nekatera podjetja še nimajo definiranega nobenega procesa za upravljanje informacijske infastrukture oz. virov, spet druga imajo že do potankosti definirane procese, jih izvajajo in tudi optimizirajo.

# 5 Modeli upravljanja mobilnih naprav

## 5.1 Uvod

Točno definiran koncept termina upravljanje z napravami -»device management«- pomaga oz. je ključen za razvoj mehanizmov za upravljanje. Upravljanje naprav lahko obravnavamo kot storitev, ki omogoča uporabniku, da upravlja z vsemi mobilnimi napravami kot celoto [28]. Zajema vse vrste komunikacijskih naprav kot en velik virtualni terminal, z mnogimi vhodnimi in izhodnimi zmogljivostmi in predstavlja, kako neprestano vzdrževati, opazovati in posodabljati konfiguracijo virtualnih terminalov, na kakšen način poteka distribucija podatkov, nastavitev ter konfiguracij na ciljne naprave.

Oddaljeno upravljanje mobilnih naprav je definirano [29] kot: imeti dostop do vseh označenih podatkov ter izvajati označene funkcije na ciljnih napravah na varen ter stroškovno učinkovit način. Nekatere raziskave so se osredotočale na funkcionalnosti orodij za upravljanje mobilnih naprav, kot študija na »Smart Box Manager (SBM)« [30]. SBM zagotavlja storitve, kot so oddaljena aktivacija, rekonfiguracija, posodobitve programske opreme, diagnostika SMB naprave.

Glede na arhitekturo Internet Protocol Multimedia Subsystem (IMS) je mogoče vzpostaviti komunikacijo vsak z vsakim (peer-to-peer oz. P2P) tipom klienta [31], operaterja, ponudniki storitev, ki se soočajo z zagotavljanjem čim boljše kvalitete storitev, ter uporabniške izkušnje ne glede na uporabljeno mobilno napravo.

V nadaljevanju je predstavljen pregled obstoječih tehnik in sistemov implementacije za upravljanje z napravami. Predstavljene so tudi zahteve za IMS, arhitektura upravljanja naprav v IMS ter kvaliteta upravljanja naprav.

## 5.2 Obstoječe tehnologije za upravljanje naprav

V tem poglavju je predstavljen pregled tehnologij za upravljanje mobilnih naprav.

### 5.2.1 Simple Network Management Protocol - SNMP

SNMP je protokol za upravljanje omrežij in omogoča upravljanje omrežja na daljavo: konfiguracije, zajem statistik, nadzor dostopa ipd. [32].

### 5.2.2 Spletno upravljanje naprav

V veliko primerih gre zgolj za enostaven spletni strežnik, ki skrbi za zagotavljanje ustreznih informacij uporabniku. Uporabnik lahko naravo konfigurira enostavno s

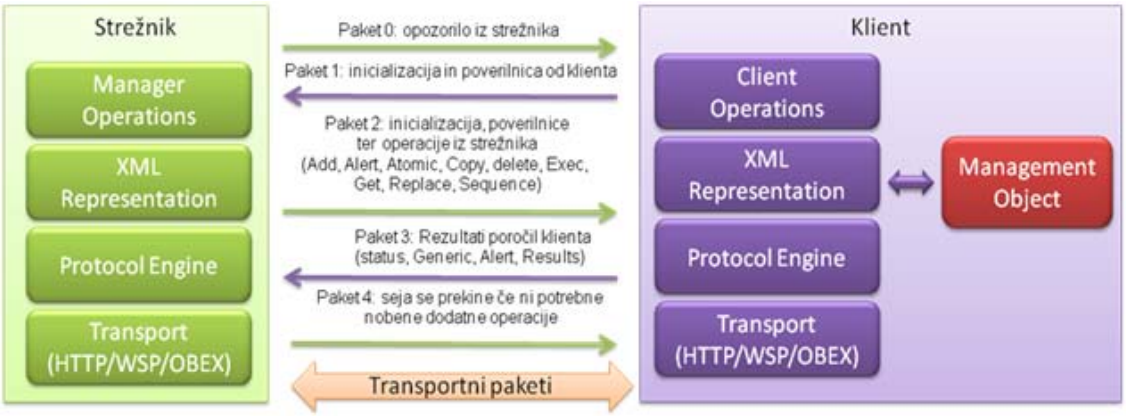
klikom na ustrezno URL povezavo ter definiranjem ustreznih informacij. Standard za spletno upravljanje v podjetjih (Web-Based Enterprise Management–WBEM) definira »Distributed Management Task Force –DMTF« [34]. Standard je nabor standardov za upravljanje ter internet tehnologij za poenotenje upravljanja porazdeljenih računalniških okolij.

WBEM definira skupen informacijski model (Commo Information Model – CIM) kot osnovni podatkovni model, specifikacije za kodiranje ter transportni mehanizem za Cim operacije preko HTTP. Specifikacije opisujejo splošen protokol na osnovi SOAP za upravljanje sistemov, kot so PC-ji, strežniki, mobilne naprave, spletne storitve ter druge entitete za upravljanje [35].

### 5.2.3 OMA Device Management – OMA DM

OMA DM je bila razvita s SyncML iniciativo in je oblikovana za prilagoditev zahtev mobilnega okolja in mobilnih storitev. OMA DM omogoča izvajanje upravljanja na objektih upravljanja (Management Objects – MO), organiziranih v drevesni strukturi predstavljeni z XML, kjer MO lahko predstavijo predvsem dve zadevi: konfiguracijo naprave ter trenutno stanje programske opreme na napravi. Aktivnosti, izvedene v povezavi s konfiguracijo mobilne naprave, vključujejo pridobivanje vrednosti nastavljenih parametrov ter ključev, medtem ko aktivnosti izvedene na področju konfiguracije mobilne naprave s programsko opremo lahko vključuje namestitev, nadgradnjo ali odstranjevanje programske opreme. OMA DM je standard za upravljanje mobilnih naprav. OMA DM pripravlja nekaj orodij iz infrastrukture upravljanja naprav, ki bodo pokrivala posodabljanje strojne programske opreme/programske opreme, zagotavljne parametrov za povezave, oddaljeno diagnosticiranje, določanje urnika ter zagotavljanje vmesnika spletnih storitev. OMA DM standard vsebuje nekaj osnovnih ukazov: Add, Alert, Atomic, Copy, Delete, Exec, Get, Replace, Results, Sequence and Status.

OMA DM uporablja protokol strežnik – odjemalec, ki se lahko prenaša s HTTP, WSP ali OBEX. Slika 15 predstavlja pregled arhitekture OMA DM standarda ter podrobnosti transakcijskega protokola [36].




**Slika 15: OMA DM arhitektura [37]**

### 5.2.4 Implementacije upravljanja mobilnih naprav

Metode za upravljanje mobilnih naprav ter same vsebine na njih, ki podpirajo več različnih tipov naprav v določenih scenarijih uporabe, so predstavljeni v [46], ki so skladni z »virtualnim terminalom« v nekaterih pogledih.

Oomen je predstavil ogrodje za upravljanje CDMA mobilnih naprav preko zraka z uporabo protokola Wireless Application Protocol (WAP) [51]. Predstavilo pa se je veliko število ponudnikov rešitev za upravljanje mobilnih naprav. Na spletnih straneh OMA DM je predstavljenih preko trideset produktov, ki uporabljajo njihov standard [52].

## 5.3 Zahteve za upravljanje naprav

Z gradnjo konvergenčnih omrežij in storitev IMS zagotavlja širok nabor podatkov, zvoka ter multimedijskih storitev preko veliko različnih naprav ter vseh vrst omrežij [38]. Upravljanje naprav bi moralo pospešiti učinkovito konvergenco ponudbe storitev preko heterogena omrežja v IMS. Zahteve za upravljanje so kategorizirane preko naslednjih poglavij: vzdrževanje konfiguracij povezav na napravah, oddaljeno diagnosticiranje naprav, oddaljeno posodabljanje naprav, upravljanje zmožnosti naprav, zagotavljanje storitev ter sledenje, opazovanje kvalitete omrežja in zahtev za protokol upravljanja.

### 5.3.1 Vzdrževanje konfiguracij povezav na napravah

IMS je odvisen od dostopa in teče preko heterogenih dostopov do omrežja, kot so GSM/GPRS, UMTS, HSDPA, WIFI, WIMAX, tudi xDSL itd. Vsaka naprava, ki ima podprtih več različnih načinov dostopa do interneta, potrebuje tudi konfiguracijo

posameznega dostopa do interneta, kar pa povečuje kompleksnost nastavitev naprav. IMS mora zagotavljati standardiziran način zagotavljanja nastavitev posameznih povezav, ki predstavlja in zagotavlja parametre povezave za vsako posamezno omrežje. Vzdrževanje konfiguracij povezav na napravah zajema tudi izbor omrežja, ko je na voljo več različnih načinov povezave. Vzdrževanje konfiguracij povezav bi moralo postati močno orodje pri FMC (Fixed Mobile Convergence).

### 5.3.2 Oddaljeno diagnosticiranje naprav

IMS ponuja uporabnikom zanimive multimedijske storitve, kar zahteva da je naprava dovolj zmogljiva, da lahko procesira multimedijsko vsebino. IMS mora zagotoviti standardiziran način za oddaljeno diagnosticiranje, ki generira informacijo o napaki na napravi, vrne poročilo o napakah ter če je mogoče, sproži procedure za odpravo napak.

### 5.3.3 Oddaljeno posodabljanje mobilnih naprav

Proizvajalci mobilnih naprav ponudijo nove sistemske komponente mobilne naprave kasneje, kot se je pojavila naprava na trgu, npr. posodobitve strojne programske opreme, operacijskega sistema … Posodobljena mobilna naprava pripomore k boljši uporabniški izkušnji ter je pripravljena za novejše storitve. Posamezni uporabniki lahko mobilno napravo posodobijo tako, da jo priključijo na osebni računalnik ter poženejo nekaj za to primernih oz. izdelanih programov. Potrebno je ponuditi oddaljeno posodabljanje mobilnih naprav na primeren način, kar izboljša uporabniško izkušnjo (uporabniku ni potrebno skrbeti, ali je na voljo kakšna posodobitev), zmanjša stroške ter možnosti napak pri posodabljanju naprav.

### 5.3.4 Upravljanje zmožnosti naprav

Z naraščanjem tako zmogljivosti mobilnih naprav kot tudi pasovne širine brezžičnih dostopov do interneta, ljudje mobilne naprave uporabljajo za veliko več namenov, kot le komuniciranje. Za zmožnost heterogenosti mobilnih naprav, morajo inovativne podatkovne storitve pripraviti storitev primerno za vsako napravo posebej. Pri zmožnostih naprav je pomembno tudi dinamično kreiranje omrežnih storitev [39]. Zmožnosti so kategorizirane kot: zaslon, strojna oprema, aplikacijska platforma, jezik brskalnika ter protokoli [40]. Potrebno je poročati zmožnosti naprav ponudniku storitev (npr. podjetje) na standarden način, ki omogoča pridobivanje, posodabljanje, shranjevanje ter ponuja zmožnosti naprav dinamično [41].

### 5.3.5 Oskrba s storitvami ter opazovanje storitev

IMS omogoča veliko storitev ter aplikacij na zgornjih heterogenih dostopnih omrežjih. Iz zornega kota naprave, je za uspešno zagotavljanje storitve potrebno zagotoviti nastavitve dodatnih parametrov ter namestitev dodatne programske opreme. Pri uporabi storitve pa je lahko storitev opazovana ter se pri morebitnih napakah delovanja storitve le-ta avtomatično zabeleži in sporoči v centralni sistem [37].

### 5.3.6 Opazovanje kvalitete omrežja

Kvaliteta omrežja vpliva neposredno na ponudbo storitve. Administrator omrežja, še posebej brezžičnega, (ang. Wireless) zagotavlja status omrežja na kateri koli možni poti [37].

### 5.3.7 Splošne zahteve protokola za upravljanje

Glede na različnost mobilnih naprav ter omejitev virov naprav, mora biti protokol upravljanja lahki protokol ter stroškovno učinkovit. IMS se lahko izvaja preko številnih dostopnih omrežij. Protokol upravljanja se mora znati prilagajati glede na razpoložljiv način prenosa podatkov, bodisi SMS, WAP PUSH ali običajni IP paketi. Protokol upravljanja mora zagotoviti tudi varnostne mehanizme, vključno z avtentikacijo ter integriteto za preprečitev varnostnih groženj [37].

## 5.4 Arhitektura sistema za upravljanje mobilnih naprav

Za zadostitev vseh zahtev, predstavljenih v predhodnem poglavju, je v tem poglavju predstavljen koncept arhitekture sistema za upravljanje z mobilnimi napravami. V predstavitvi so ločene upravljavske ter izvajalske funkcionalnosti. Arhitektura zajema tudi funkcionalnosti za aplikacijski strežnik za upravljanje nekaterih IMS zmožnosti.

### 5.4.1 Pregled arhitekture

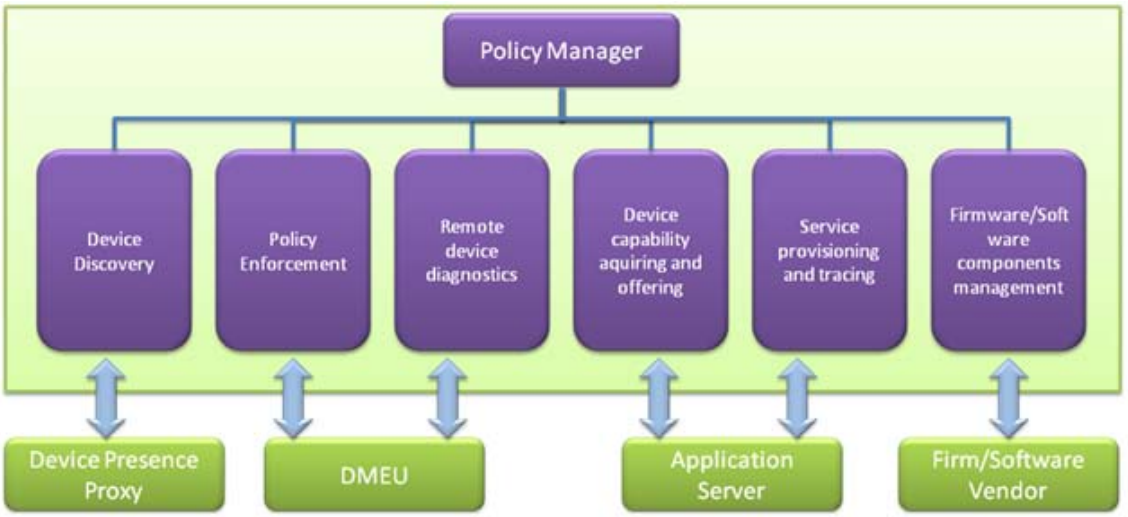
Kot prikazuje spodnja slika, je sistem sestavljen iz Master Device Management Serverja (MDMS), Device Management Execution Unit (DMEU), aplikacijskega strežnika (AS) ter pripadajočo IMS infrastrukturo. MDMS je glavna komponenta arhitekture, ki je glavna za definiranje globalnih upravljavskih politik v obravnavanem okolju. MDMS tudi sodeluje z aplikacijskim strežnikom ter z drugimi zunanjimi entitetami.


**Slika 16: Arhitektura sistema za upravljanje z mobilnimi napravami [37]**

### 5.4.2 Master Device Managemen Server - MDMS

Sistem je mogoče definirati tako, da operaterji definirajo domene upravljanja. Lahko se upravlja več domen (grupirane različne mobilne naprave, različni tipi uporabnikov ...), vendar pa je potrebno za vsako domeno zagotoviti po en MDMS sistem.

Na spodnji sliki so predstavljene funkcionalnosti MDMS sistema.




**Slika 17: MDMS funkcionalnosti**

MDMS sistem vsebuje naslednje funkcionalnosti:

1. **Odkrivanje naprav**

   Ta funkcionalnost vpliva na zmožnosti, pridobljene s funkcionalnostjo Prox-Call Session Control Function (P-CSCF). P-CSCF je prva kontaktna točka uporabnikov z IMS. Vso SIP signaliziranje na ali iz naprave gre preko P-CSCF [31]. Operater omrežja lahko nastavi Device Presence Proxy delegiranje P-CSCF za zagotavljanje informacije o prisotnosti naprave. Ko se P-CSCF zave, da je mobilna naprava »online«, je MDMS obveščen ter izvede ustrezne upravljalske operacije (npr. preverjanje konfiguracije, preverjanje, ali je za napravo namenjen kakšen posodobitveni paket, sprememba konfiguracije ...). Odkrivanje naprav tudi omogoča izogibanje nepotrebnim upravljalskim operacijam za mobilne naprave, ki niso povezane ali pa so ugasnjene.

2. **Upravljanje s politikami**

   Politika vsebuje naslednje komponente: obseg naprav za obvladovanje (kaj upravljati), tip operacij – kot npr. zagotavljanje parametrov, določanje urnika upravljanja – npr. čas začetka operacije. Vse upravljavske operacije so definirane kot politike, vključno s konfiguracijo, poizvedovanjem, zagotavljanjem, oddaljeno diagnosticiranje naprav, posodobitve programske ter strojne programske opreme itd. Sistem MDMS generira upravljavske politike in jih posreduje DMEU za izvedbo, opazovanje pravilnosti izvedbe, pridobitve

statusa izvedbe (uspešno neuspešno...). Funkcionalnost upravljanja s politikami je sestavljena iz dveh komponent: upravitelj politik ter uveljavljanje politik. Upravitelj politik skrbi za koordinacijo vseh funkcionalnosti MDMS ter generira politike. Komponenta za uveljavljanje politik pa je v interakciji z DMEU za dostavo politik ter poročil o izvedbi politik na napravah.

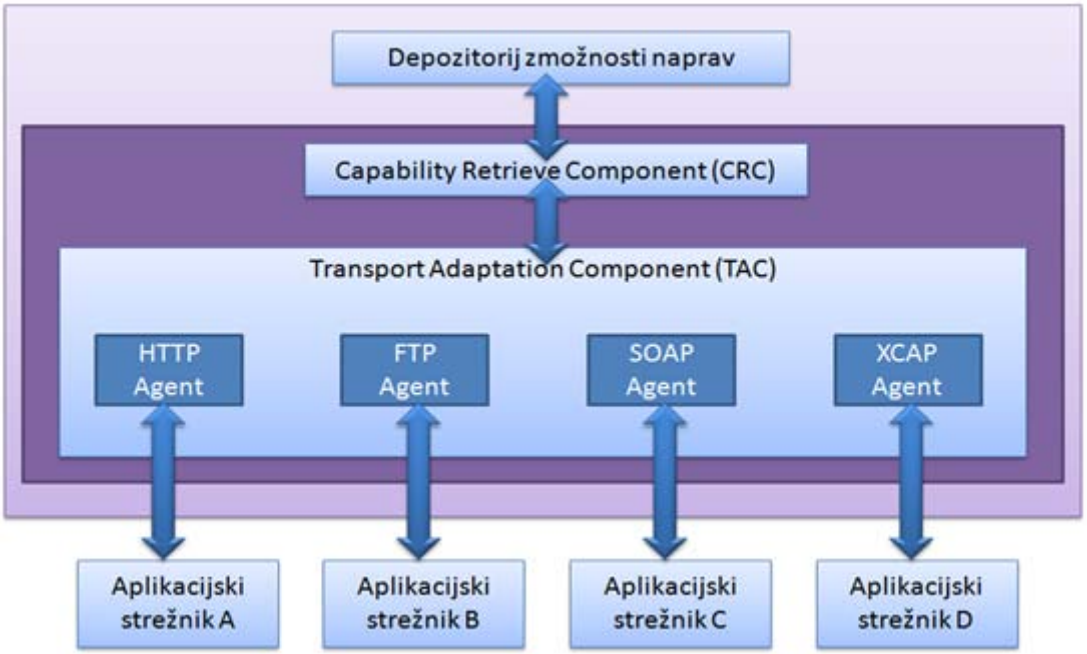
**3. Diagnosticiranje oddaljenih naprav**

Ko naprava odkrije napako ali drugo pomembno informacijo, ki bi jo bilo potrebno sporočiti centralnemu sistemu (kot npr. signal omrežja je zelo šibak), le ta pošlje podrobne informacije v DMEU. Če DMEU lahko reši problem, je poročilo poslano v MDMS, v nasprotnem primeru je napaka oz. informacija predana sistemu MDMS za reševanje.

**4. Pridobivanje zmožnosti mobilnih naprav**

Narejenih je bilo veliko raziskav, kako pridobiti zmožnosti terminalov pri posamezni storitvi [44] [45], vendar je malo poročil, kako pridobiti zmožnosti terminalov z enotno arhitekturo za različne storitve. MDMS lahko zagotavlja različne informacije o mobilni napravi, kot so: proizvajalec, model, verzija, konfiguracija ter detaljne zmožnosti z izvajanjem upravljavskih operacij preko politik. V prispevku [41] avtorji predstavljajo upravljalsko ogrodje za pridobivanje in poročanje zmožnosti naprav. MDMS koristno uporablja tudi druge podobne mehanizme za zagotavljanje zmožnosti naprav zunanjemu AS, kot je prikazano na spodnji sliki. Pridobljena zmožnost naprave olajša AS dostavljanje vsebine napravam v ustreznem formatu ter podpiranje dostopa vsem različnim tipom mobilnih naprav [46]. MSDMS shranjuje vse pridobljene podatke ter jih na zahtevo posreduje zunanjim aplikacijskim strežnikom preko enotnega vmesnika, ki je implementiran s pomočjo Capability Provision Functionality (CFP). CFP je sestavljen iz komponente Capability retreive Component (CRC) ter Transport Adaptation Component (TAC). CRC pridobi ustrezne podatke iz depozitorija zmožnosti naprav, ki vsebuje pridobljene podatke o zmožnostih posameznih naprav, ter jih dostavi v TAC. TAC mora znati upravljati z različnimi komunikacijskimi agenti za ravnanje z različnini transportnimi protokoli, ki so http agent, FTP agent, SOAP agent ter XCAP

agent. Agentje komunicirajo z različnimi aplikacijskimi strežniki preko ustreznih protokolov.




**Slika 18: Zagotavljanje zmožnosti naprav**

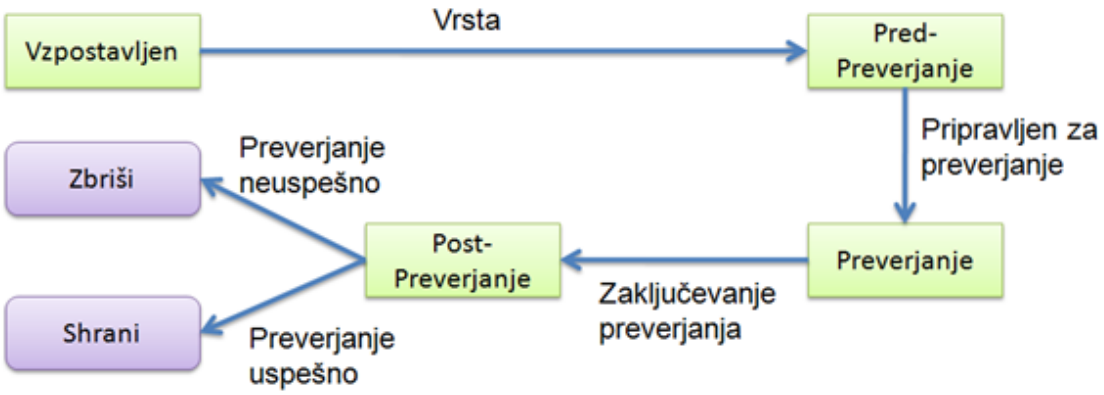
### 5. Zagotavljanje storitev ter opazovanje pravilnosti delovanja storitev

S pridobljeno konfiguracijo naprav lahko aplikacijski strežnik zagotavlja potrebne konfiguracijske parametre, programske komponente ali posodobitve v MDMS. MDMS generira upravljalske politike s parametri, ki jih dostavi DMEU za izvajanje. MDMS lahko definira politiko, ki vodi napravo za spremljanje izvajanja storitve ter poročanje informacij v primeru napak. Poročilo izvajanja in spremljanja je poslano iz MEMS na aplikacijski strežnik na podlagi rezultata izvedbe v DMEU. Na podlagi poročila lahko aplikativni strežnik ugotovi, ali je bil Service Level Agreement (SLA)[42] zagotovljen ves čas ter ali je bila izboljšana kvaliteta storitve z upravljanjem mobilnih naprav.

### 6. Upravljanje strojnih programskih/programskih komponent

Ko je potrebno posodobiti strojno programsko opremo na mobilni napravi ali programsko opremo, je potrebno izbrati pravi paket. Glede na raznolikost mobilnih naprav, je potrebno zagotoviti verifikacijo potrebnega paketa za posodobitev. Za te potrebe se je vpeljal koncept življenjskega cikla upravljanja [43]. Oblikovanih je veliko stanj za delegiranje stanj paketa za posodobitev. Ta

stanja so: Vzpostavljen, Pred-Verifikacija, Verifikacija, Post-Verifikacija, Briši in Shrani. Stanje Vzpostavljen je začetno stanje, medtem ko sta stanji Briši ter Shrani končni stanji. Celoten postopek prehajanja med stanji je prikazan na naslednji sliki.

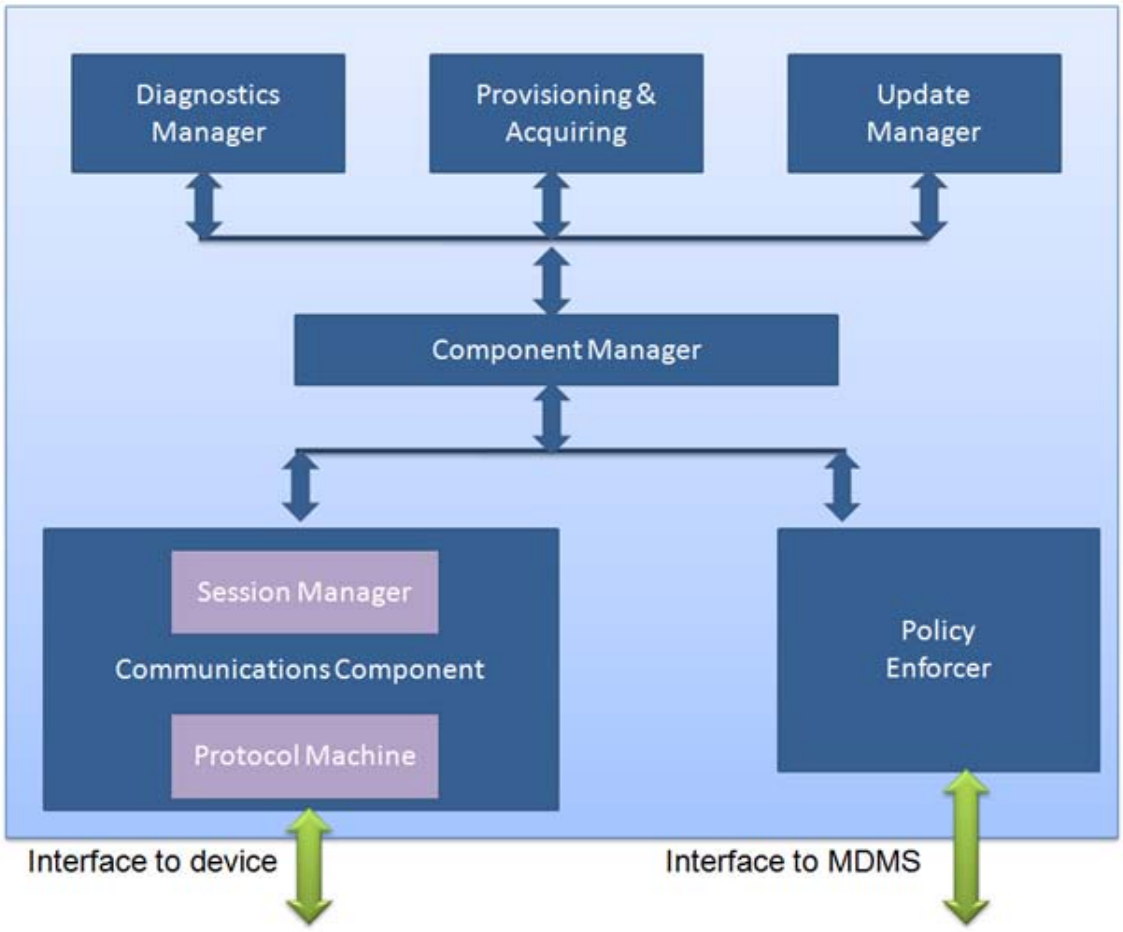



**Slika 19: Upravljavski življenjski cikel za posodobitveni paket [37]**

### 5.4.3 Device Management Execution Unit - DMEU

DMEU je vmesni med celotno arhitekturo za upravljanje in mobilno napravo. Zaradi heterogenosti mobilnih naprav ter podprtih upravljalskih protokolov, mora DMEU podpirati veliko vmesnikov. SNMP je široko podprt pri stacionarnih napravah, kot so PC … OMA DM pa se osredotoča na mobilne naprave. Podprti so tudi nekateri ostali upravljavski protokoli, kot je WBEM. DMEU je lahko postavljen tako, da skrbi zgolj za individualno vrsto naprave. Vsak DMEU lahko uporablja protokol, ki kar najbolje ustreza tipu naprav, ki jih podpira (npr. ena dMEU enota je namenjena za obvladovanje mobilnih naprav, druga pa za prenosne računalnike). Ena DMEU enota lahko podpira tudi več protokolov, kjer se to zahteva.

Poenostavljena arhitektura DMEU ogrodja je predstavljena na spodnji sliki. Ogrodje vpliva na OMA DM protokol in je sestavljeno iz komponent tipa upravljalskih operacij. Diagnostic manager je skladen s funkcionalnostjo oddaljeno diagnosticiranje. Update management ustreza posodabljanju strojne programske ter programske opreme. Provisioning & Acquiring funkcionalnost je skladna s funkcionalnostjo upravljanja konfiguracij. Policy Enforcer izvaja politike, ki jih prejme od sistema MDMS ter poda rezultat nazaj v MDMS sistem. Communications komponenta je sestavljena iz dveh elementov. Component Manager je glavni del DMEU enote, ki preusmerja sporočila iz ter do individualnih komponent.




**Slika 20: Poenostavljeno DMEU ogrodje [37]**

### 5.4.4 Aplikacijski strežnik - AS

AS ni neposredno povezan z operacijami upravljanja naprav. AS predstavlja upravljalske zahteve ter jih sporoča MDMS sistemu, vse upravljavske operacije so izvršene s pomočjo MDMS ter DMEU. AS ne potrebuje znanja o posameznih protokolih upravljanja, vendar zgolj skrbi za zagotavljanja storitve (posredovanje zahtev).

### 5.4.5 IMS Infrastruktura

Z vidika upravljanja mobilnih naprav je IMS osnova za zagotavljanje določenih zmogljivosti (SIP kontrola), kot so polnjenje, avtentikacija, kompresija, preusmerjanje. IMS zagotavlja komunikacijo med upravljalskim strežnikom ter napravo in zagotavlja funkcionalnost odkrivanje naprav ter drugih podprtih kompetenc.

### 5.4.6 Vmesniki

Kot je prikazano na sliki 15, IF1, vmesnik med MDMS in AS ter vmesnik IF2, vmesnik med MDMS in DMEU, sta lahko implementirana kot spletna storitev [47] ter opisana z Web Service Description Language (WSDL) [48].

Operacije vmesnika IF1 so namenjene zagotavljanju boljših storitev. AS potrebuje informacije o napravi, vključno s konfiguracijo naprave ter zmogljivostmi naprave (verzija programske opreme, podprtih storitev …) preko IF1. AS konfigurira naprave, povezane z informacijami o napravi, vključno z nastavitvami parametrov ter nameščanjem potrebnih posodobitev. AS sledi tudi statusu storitev in vrača poročila ko se uporablja storitev. Operacije IF2 se servisirajo iz namena sodelovanja med MDMD ter DMEU, ki vključuje poizvedovanje po politikah, poročila izvajanja ter asinhrono obveščanje. Poizvedovanje po politikah omogoča dostavo upravljavske politike iz MDMS v DMEU. Poročilo izvedbe politike je posredovano nazaj v MDMS sistem. Asinhrone notifikacije prenašajo asinhrone dogodke, npr. pomembna informacija iz naprave je posredovana v sistem MDMS.

Vmesniki med IMS infrastrukturo ter ostalimi elementi, IF3 ter IF4, se prilagajajo specifikacijam IMS odvisno od scenarijev implementacije.

### 5.4.7 Možnosti integracije več IMS funkcionalnosti v Upravljanje naprav

Prednost IMS je integracija SIP funkcionalnosti skupaj v celoto ter servisiranje multimedijske storitve. Nobeden od SNMP, WBEM ali OMA DM ne vpliva na SIP neposredno ter tudi ne morajo uporabljati IMS funkcionalnosti direktno. Možen pristop je, da se razvije nov protokol za upravljanje, ki je osnovan na SIP protokolu z razširjanjem nekaj metod ter glav [49]. Vendar ni eksplicitnih tehničnih razlogov za razvijanje novega protokola. Naslednji možen pristop je dodajanje SIP mehanizmov v obstoječe rešitve za izboljšanje performans.

Možne izboljšave se lahko upošteva kot sledi:

Lahko se razvije SIP povezava za OMA DM. OMA DM se lahko transportira z OBEX, http ter WSP. Povezava SIP transporta naredi implementacijo OMA DM bolj fleksibilno. Upravljavska seja med napravo ter strežnikom pa se lahko streže preko SIP protokola.

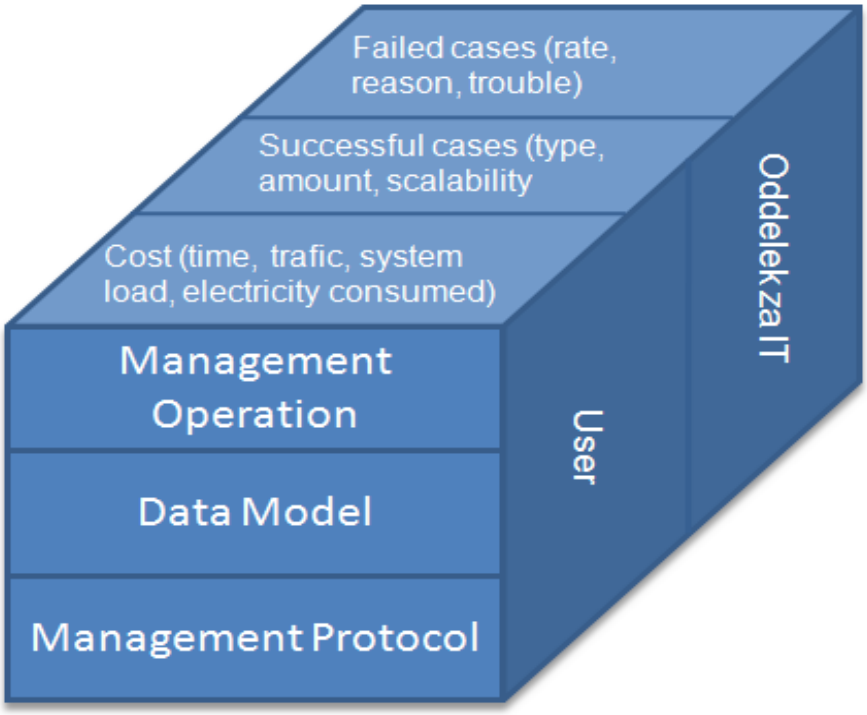
SIP mehanizmi za podpisovanje ter objave [50] so lahko implementirani v vlogi vmesnikov med različnimi strežniki. SIP podpisovanje ter objavljanje je uporabljeno kot sprejemanje sprememb statusov na ciljnih napravah. AS lahko te mehanizme uporabi za obveščanje MDMS-ja, da so na razpolago novi parametri.

Z vključevanjem novih SIP funkcionalnosti je lahko koristno uporabljenih več mehanizmov IMS infrastrukture, vključno s polnim naborom koristi avtentikacije. Na primer, ko se naprava registrira v P-CSCF, je lahko informacija o avtentikaciji deljena z upravljalskim strežnikom.

## 5.5 Kvaliteta upravljanja mobilnih naprav

Z naraščanjem števila vrst mobilnih naprav ter sistemov za upravljanje mobilnih naprav je vse bolj pomembno vrednotenje kvalitete upravljanja mobilnih naprav.

Vrednotenje kvalitete uporabljanja mobilnih naprav pomaga IT oddelkom pridobiti rezultate upravljanja ter pokaže področja, kjer je potreben dodaten napor v prihodnosti za izboljšave. Potrebno bi bilo narediti študijo o kvaliteti upravljanja mobilnih naprav. Nekaj študij je že bilo narejenih, ki vsebujejo zgolj kriterije za ocenjevanje kvalitete upravljanja omrežja ali sistema [53], [54], niso pa vključeni vsi kriteriji, s katerimi bi lahko objektivno ocenili kvaliteto upravljanja mobilnih naprav. Na spodnji sliki je prikazan splošen model za ocenjevanje, prikazanih pa je tudi nekaj primerov kriterijev iz različnih nivojev in perspektiv.




**Slika 21: Ocenjevalni model kvalitete upravljanja mobilnih naprav [37]**

Model za ocenjevanje kvalitete upravljanja se lahko razdeli v tri stopnje, ki so izvajanje upravljanja, podatkovni model in protokol upravljanja. Kriteriji kvalitete so definirani iz perspektive podprtih funkcij upravljanja, kot je na primer količina tipov operacij.

Kvaliteta kriterija podatkovnega modela je določena z vidika informacij, ki se jih lahko pridobi iz podatkov upravljanja, ki se zbirajo v centralni podatkovni bazi, kot je na primer moč izražanja. Kvaliteto kriterija protokol upravljanja se pridobi iz zmogljivosti komunikacije, kar vključuje fleksibilnost dostopa, robustnost, učinkovitost …

Kriteriji modela za ocenjevanje kakovosti upravljanja mobilnih naprav so lahko, iz vidika uporabnika in oddelka za IT, razdeljeni v tri kategorije, in sicer stroški, uspešni primeri ter neuspešni primeri. Uporabnika bolj zanimajo kriteriji posamezne izkušnje uporabe, kot je na primer strošek porabljenih sredstev (baterija, poraba električne energije …), medtem ko službo za IT zanimajo predvsem celotni faktorji, kot so skupna stopnja upravljavskih sej ter skalabilnost. Nekateri kriteriji so pomembni tako za uporabnika kot tudi službo za IT, kot so na primer poraba časa, stroški prenosa podatkov, potencialne težave pri neuspešnih posegih …

Glede na splošen model za ocenjevanje, lahko služba za IT ali ustrezna organizacija definira podrobne kriterije za ocenjevanje ter merila za definiranje zahtev upravljanja ter izboljša kvaliteto upravljanja mobilnih naprav.

# 6 Analiza orodij za upravljanje mobilnih naprav na trgu

V naslednjih poglavjih so predstavljena najbolj prepoznavna orodja trenutno na trgu, ki so namenjena upravljanju ter obvladovanju mobilnih naprav. Najprej je predstavljeno orodje prizvajalca Sybase iAnywhere Afaria 6.0, nato Nokijino orodje Intellisync Device Management ter na koncu še Microsoftovo orodje System Center Mobile Device Manager 2008.

Samih produktov v okviru naloge, zaradi časovne zahtevnosti ter s tem povezanimi visokimi stroški, nisem testiral. Primerjava je narejena zgolj na pregledu dokumentacije, ki jo podajajo proizvajalci.

## 6.1 Kriteriji primerjave

V naslednji tabeli so predstavljeni kriteriji, po katerih sem produkte primerjal med seboj.

| **Funkcionalnosti produktov** |
|---|
| **Podpora končnim uporabnikom**<br>**32-bit Windows kompatibilni** |
| Windows PPC 2000/2002/2003 |
| Windows Mobile 5/6/6.1 |
| Sony Ericsson M600i/P1i |
| Nokia E & N Series |
| Velikost klienta |
| **Funkcionalosti podprte na podprtih platformah Windows Mobile/Symbian** |
| Nameščanje agenta preko zraka |
| Zbiranje vseh podatkov o napravah |
| Distribucija programske opreme |
| Distribucija dokumentov |
| Konfiguriranje mobilnih naprav |
| Vsiljevanje varnostnih politik na mobilne naprave |
| Kriptiranje datoteke ali mape na napravi |
| Oddaljeno zaklepanje mobilne naprave |
| Oddaljeno resetiranje naprave na tovarniške nastavitve |
| Izdelovanje varnotnih kopij mobilne naprave |
| Izdelovanje skript za mobilne naprave |
| Podpora ob neuspešni sinhronizaciji |
| **Kompresija** |
| **Ponastavljanje točke povrnitve stanja na mobilni napravi** |
| **Sinhronizacija samo spremenjenih podatkov** |
| **Konfiguracija pasovne širine na posamezni mobilni napravi** |

| |
|---|
| **Granualna enkripcija podatkov pri sinhronizaciji: control channel/package/file** |
| **Dinamična podpora skupinam glede na hardware / software** |
| **Push distribucija** |
| **Podpora za upravljanje osebnih podatkov (personal information manager-PIM)** |
| **Podpora Enterprice directory** |
| **Generiranje poročil** |
| **Beleženje dogodkov, ki se izvajajo na napravah** |
| **Zunanje ter PDA sinhroniziranje podatkovne baze** |

**Tabela 3: Funkcionalnosti produktov**

Seznam kriterijev izhaja predvsem iz modela za upravljanje mobilnih naprav, ki je predstavljen v poglavju 5 Modeli upravljanja mobilnih naprav.

Za farmacevtsko podjetje imajo največjo težo predvsem platforme, ki jih orodje podpira, ter naslednje funkcionalnosti:

- nameščanje agenta preko zraka,
- zbiranje vseh podatkov o napravah,
- distribucija programske opreme,
- distribucija dokumentov,
- konfiguriranje mobilnih naprav,
- vsiljevanje varnostnih politik na mobilne naprave,
- kriptiranje datoteke ali mape na napravi,
- oddaljeno zaklepanje mobilne naprave,
- oddaljeno resetiranje naprave na tovarniške nastavitve,
- izdelovanje varnotnih kopij mobilne naprave,
- izdelovanje skript za mobilne naprave,
- podpora ob neuspešni sinhronizaciji.

Zelo pomemben kriterij je tudi zmožnost kriptiranja prometa ter zmožnost konfiguriranja pasovne širine, ki se lahko uporabi za upravljanje mobilne naprave.

## 6.2 Primerjava produktov

| Fukcionalnosti produktov za upravljanje mobilnih napra | Sybase iAnywhere Afaria 6.0 | Nokia Intellisync Device Management | System Center Mobile Device Management |
|---|---|---|---|
| **Podpora končnim uporabnikom 32-bit Windows kompatibilni** | D | D | D |
| **Windows PPC 2000/2002/2003** | D | D | D |
| **Windows Mobile 5/6/6.1** | D | D | D |
| **Sony Ericsson M600i/P1i** | D | D | N |
| **Nokia E & N Series** | D | D | N |
| **Integracija s SCCMjem** | D | N | D |
| **Funkcionalosti podprte na podprtih platformah Windows Mobile/Symbian** | | | |
| **Nameščanje agenta preko zraka** | D | D | D |
| **Zbiranje vseh podatkov o napravah** | D | D | D |
| **Distribucija programske opreme** | D | D | D |
| **Distribucija dokumentov** | D | D | N |
| **Konfiguriranje mobilnih naprav** | D | D | D |
| **Vsiljevanje varnostnih politik na mobilne naprave** | D | D | N |
| **Kriptiranje datoteke ali mape na napravi** | D | D | D |
| **Oddaljeno zaklepanje mobilne naprave** | D | D | D |
| **Oddaljeno resetiranje naprave na tovarniške nastavitve** | D | D | D |
| **Izdelovanje varnotnih kopij mobilne naprave** | D | D | D |
| **Izdelovanje skript za mobilne naprave** | D | D | D |
| **Podpora ob neuspešni sinhronizaciji** | D | D | D |
| **Kompresija** | D | D | D |
| **Ponastavljanje točke povrnitve stanja na mobilni napravi** | D | D | D |
| **Sinhronizacija samo spremenjenih podatkov** | D | D | N |
| **Konfiguracija pasovne širine na posamezni mobilni napravi** | D | D | N |
| **Granualna enkripcija podatkov pri sinhronizaciji: control channel/package/file** | D | D | D |
| **Dinamična podpora skupinam glede na hardware / software** | D | N | D |
| **Push distribucija** | SMS, IP | SMS, IP | SMS |
| **Podpora za upravljanje osebnih podatkov (personal information manager-PIM)** | N | D | N |
| **Podpora integraciji z aktivnim imenikom podjetja** | LDAP, AD | LDAP,AD | LDAP, AD |
| **Generiranje poročil** | D | D | D |
| **Beleženje dogodkov, ki se izvajajo na napravah** | D | N | D |
| **Zunanje ter PDA sinhroniziranje podatkovne baze** | D | D | N |

**Tabela 4: Ocena pregledanih produktov**

Kot je razvidno iz izvedene primerjave, so si produkti med sabo precej podobni. Vsi podpirajo večino zahtevanih funkcionalnosti, razlikujejo se zgolj po platformah mobilnih naprav, ki jih podpirajo.

Za farmacevtsko podjetje je zaradi trenutnega stanja, ko še ni jasno definiranih standardnih platform, zanimivo orodje, s čim širšim naborom mobilnih naprav, ki jih podpirajo. Za farmacevtsko podjetje je tako najbolj zanimivo orodje Sybase iAnywhere Afaria 6.0 ter Nokia Intellisync Device Management. Seveda pa je orodja potrebno preizkusiti in jih na tak način med sabo primerjati ter ugotoviti, katero je najbolj primerno za implementacijo v farmacevtskem podjetju.

V prilogi 1 so posamezni produkti nekoliko podrobneje predstavljeni.

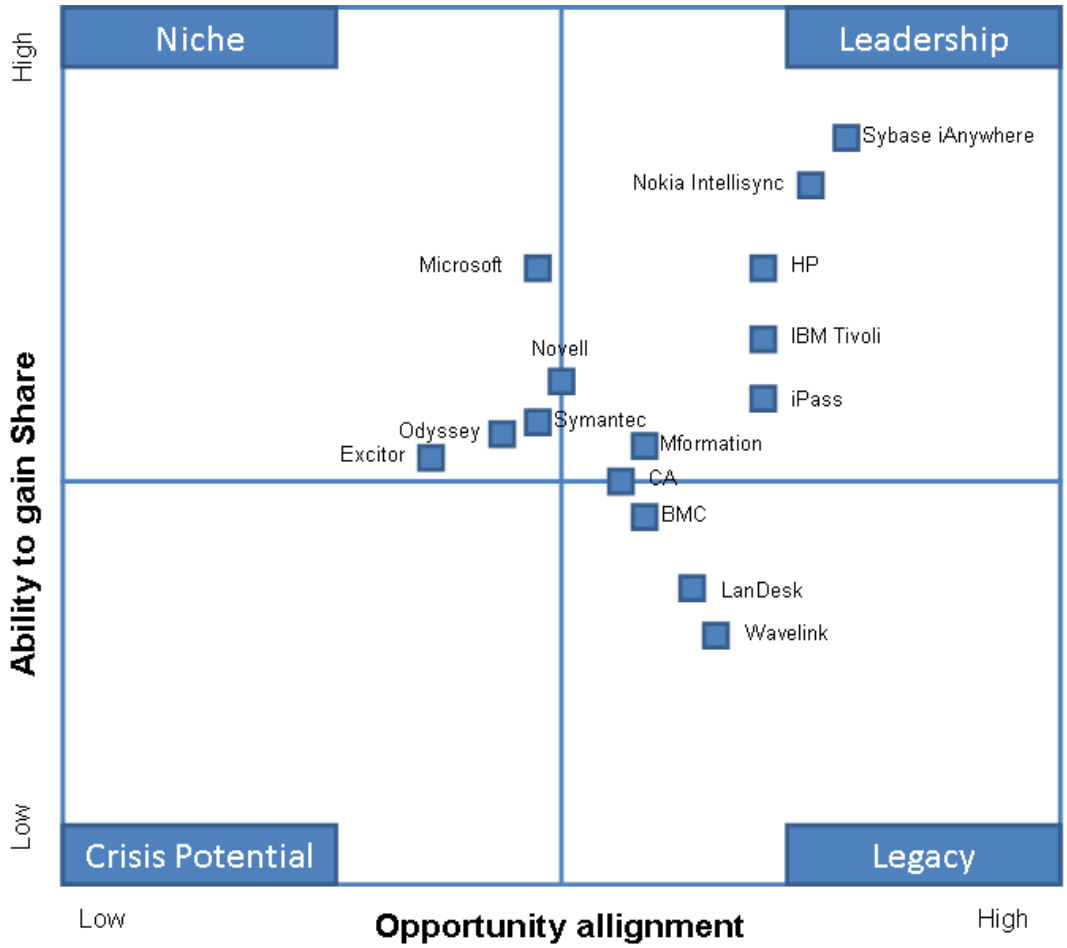
## 6.3 IDC kvadrant vodilnih proizvajalcev orodij za upravljanje z mobilnimi napravami

IDC kvadrant vodilnih proizvajalcev prikazuje kvalitativno primerjavo ponudnikov rešitev za upravljanje mobilnih naprav na trgu. Prikazana je slikovna predstavitev pozicije vsakega ponudnika na trgu glede na dva faktorja: ponudnikova zmožnost za dosego tržnega deleža ter njegove povezave s prihodnjimi tržnimi priložnostmi [67].

X os meri ponudnikov potencial pri izrabi priložnosti, ki se pojavljajo na trgu. X- os meri tudi potencialno ponudnikovo rast ter zmožnost postati najpomembnejši del trga. Y os meri zmožnost pridobiti delež na podlagi več faktorjev, in sicer kot so: finančne zmožnosti, percepcija strank ter partnerstvo [67].

Do neke mere IDC kvadrant vodilnih ponuja bolj splošno oceno položaja podjetja, nato pa samo tržni delež. IDC kvadrant vodilnih predstavlja analizo več faktorjev, ki so pomembni za uspeh [67].

Kot je razvidno iz kvadranta na spodnji sliki, je tudi IDC prišel do podobnih ugotovitev, kot jih je pokazal pregled treh produktov v nalogi.




**Slika 22: Prikaz IDC kvadranta vodilnih proizvajalcev programske opreme za upravljanje mobilnih naprav**

# 7 Celoviti pristop obvladovanja mobilnih naprav

Poglavje prikazuje vse aktivnosti, ki jih je potrebno upoštevati pri uvajanju sistema obvladovanja (upravljanja) mobilnih naprav. Slika 20 prikazuje tudi diagram poteka, kako naj si aktivnosti sledijo. Potek aktivnosti ni pravilo, ki se ga je nujno potrebno držati, so zgolj priporočila in usmeritve za ostala podjetja oz. organizacije, ki se bodo srečevala s podobnim problemom.

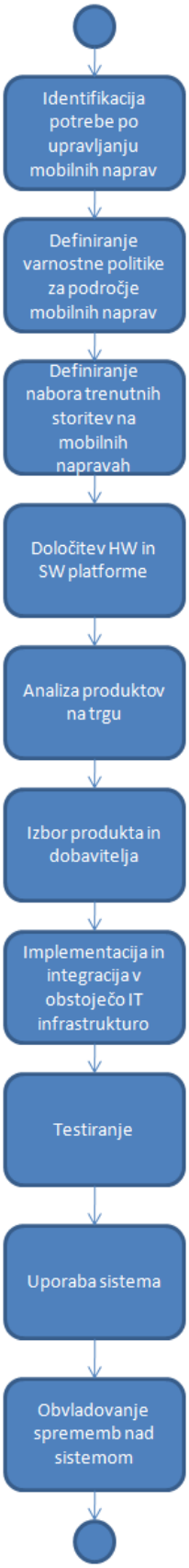
Proces se prične izvajati takrat, ko se pojavi dovolj velika potreba po upravljanju obilnih naprav. To se ne more zgoditi v kratkem časovnem intervalu, vendar je potreben določen čas, da te potrebe dozorijo.

Ko potrebe dozorijo, je potrebno definirati temelje uspešnega upravljanja mobilnih naprav, in sicer je to varnostna politika, nato trenutni podprti nabor storitev na mobilnih napravah ter trendi na področju storitev na mobilnih napravah. Definirati je potrebno tudi platformo strojne opreme in programske opreme (operacijski sistemi), ki se jih bo v podjetju uporabljalo. Platforma mora biti zastavljena tako, da mora predvideti zamenjavo modela mobilne naprave z novejšim modelom.

Ko so definirani temelji in okvirna pričakovanja (cilji) orodja za upravljanje mobilni naprav je priporočljivo izvesti analizo produktov na trgu ter izbrati najugodnejšega oz. tistega, ki najbolje pokriva vse zahteve.

Ko je produkt izbran, je potrebno zagotoviti uspešno implementacijo orodja v obstoječo infrastrukturo podjetja, te po možnosti zagotoviti integracijo orodja z drugimi orodji za upravljanje (npr. orodje za upravljanje delovnih postaj, strežnikov …).

Na koncu seveda sledi testiranje sistema ter uporaba v produkciji. Ko se sistem nekaj časa uporablja, se pojavijo tudi problemi oz. stvari, ki jih je potrebno popraviti ali izboljšati. Za to poskrbi aktivnost obvladovanja sprememb nad sistemom, s katero zagotovimo sledljivost vseh sprememb nad sistemom. Proces se ne sme nikoli končati, neprestano je potrebno spremljati delovanje sistema ter pri odstopanjih od pričakovanj ustrezno ukrepati.




**Slika 23: Prikaz diagrama poteka aktivnosti pri uvajanju sistema v organizacijo**

# 8 Razvoj področja mobilnih naprav v prihodnosti

V nadaljevanju je predstavljenih nekaj smernic, ki sem jih zasledil na področju mobilnih naprav in komunikacij.

## 8.1 Konvergenca

Z izrazom »konvergenca omrežij« v splošnem označujemo združevanje oz. približevanje obstoječih omrežij za prenos govora, omrežij za prenos podatkov in radio-difuzijskega omrežja; gre torej za približevanje telefonskega, radijsko-televizijskega in različnih vrst podatkovnih omrežij. Konvergenco omrežij spremlja tudi integracija ali zlivanje storitev, oboje pa predstavlja eno od najpomembnejših tendenc globalnega razvoja telekomunikacij [61].

Analitsko podjetje ABI Research ocenjuje, da je v obdobju dramatičnih sprememb telefonskih storitev eden najbolj vročih pojavov konvergenca fiksnih in mobilnih storitev (FMC) [64].

V letu 2011 bo približno 250 milijonov uporabnikov, ki bodo telefonske klice sprejemali in pošiljali prek združenih fiksno-mobilnih omrežij ter pristopnih točk, v katera bodo podjetja vložila več kot 450 milijonov dolarjev. Tovrstni uporabniki bodo dosegli 10-odstotni delež v poslovnem segmentu in 8-odstotnega v segmentu posameznih uporabnikov. Hitrejši razvoj trga zaenkrat ovirajo pomanjkanje nižjih tarif in preprostejše tarifne strukture ter slaba izbira naprav za tovrstne storitve [64].

Raziskava podjetja ORC International je pokazala, da so uporabniki pripravljeni zamenjati svojega ponudnika mobilnih telefonskih storitev ali dostopa do interneta in se preseliti k operaterju konvergenčne fiksne in mobilne storitve [63].

Storitev, pri kateri uporabniki lahko svoje klice opravljajo z mobilnega oziroma fiksnega IP-telefona, kadar so doma, zbuja precej zanimanja zaradi prihrankov, ki jih omogoča. Več kot 40 odstotkov od 500 vprašanih bi zamenjalo svojega ponudnika širokopasovnega interneta ali mobilnega operaterja in se preselilo k operaterju konvergenčnih storitev [63].

Konvergenca je predvsem zagotavljanje storitev, ki so se tradicionalno zagotavljale preko različnih infrastruktur, preko popolnoma ali deloma povezanih (združenih) novih infrastruktur.

Konvergenca poteka na različnih ravneh. Na splošno velja, da višje ravni integracije omogočajo doseganje večjih ekonomij obsega in povezanosti, kar ustvarja občutno učinkovitost pri zagotavljanju večih storitev.

### 8.1.1 Ravni konvergence

**Na napravi [65]**

Zagotavljanje večih storitev oz. posamezne storitve preko različnih dostopnih omrežij se izvaja na eni sami napravi.

Primeri:

- mobilna televizija in govor na isti mobilni napravi ali
- VoIP preko WIFi ali preko WiMAXa in govor preko 2G/3G na isti mobilni napravi.

**Na platformi [65]**

Ena sam platforma nudi eno oz. več storitev preko več jedrnih omrežij oz. eno samo jedrno omrežje, povezano z več dostopnimi omrežji.

Primeri:

- Platforma za mobilno in fiksno telefonijo, ki dopušča eno samo naročniško številko in končnega uporabnika doseže skozi mobilno omrežje oz. fiksno lokalno zanko.
- Platforma za mobilno televizijo, ki vsebino nudi skozi omrežja programskih vsebin, šifrirane podatke in z vsebino povezane interaktivne aplikacije pa na 2G/3G dostopnih omrežjih. Platforma za mobilno in fiksno telefonijo se lahko končnim uporabnikom zagotavlja preko mobilnega omrežja ali preko fiksne krajevne zanke.

**Na jedrnem omrežju [65]**

Prenos večih storitev se izvaja na eni sami jedrni omrežni infrastrukturi (ponavadi na Ethernetu oz. na ATM infrastrukturi). Platforme, ki zagotavljajo storitve, so povezane z konvergiranim jedrnim omrežjem.

**Na dostopovnem omrežju [65]**

Na eni dostopni zanki oz. na enem radijskem dostopnem omrežju je nudenih več storitev. Na ravni jedrnega omrežja je lahko za vsako storitev uporabljena ustrezna infrastruktura (npr. Ethernet za IPTV, ATM za Internet in SDH za govor).

Primeri:

- Bodisi z upravljanjem spektra, npr. PSTN in ADSL na kovinski parici ali televizija in internet/govor na kabelski televiziji.
- Bodisi z enim samim omrežnim protokolom: npr. z Internetom, VoIP in IP televizijo na DSL.

### 8.1.2 Konvergenčne ponudbe

Konvergenčne (združene) oziroma multiple-play (multi-play) ponudbe vključujejo vsaj dve različni vrsti storitev: fiksno telefonijo, mobilno telefonijo, prenos podatkov in televizijo.

Poznamo več oblik konvergnečnih ponudb storitev[65]:

- Dvojček (Double play): ponudba (zvezana ali nezvezana) vključuje dve od navedenih storitev: storitve fiksne govorna telefonije, storitve mobilne govorne telefonije, fiksne televizijske in radijske storitve, mobilne televizijske in radijske storitve, storitve fiksnega širokopasovnega dostopa in storitve mobilnega širokopasovnega dostopa.

- Trojček (Triple play): ponudba (zvezana ali nezvezana) vključuje tri vrste osnovnih storitev (govor, TV in radio, prenos podatkov), s tem da so storitve prenosa podatkov vezane na širokopasovni dostop.

- Četverček (Quadruple play): triple play ponudba (zvezana ali nezvezana), ki vključuje vsaj eno mobilno komponento. V tem primeru gre za fiksno-mobilno konvergenco.

## 8.2 Mobilni Customer Relationship Management - CRM

Vedno bolj pogosta je interakcija s strankami zunaj poslovnih prostorov. Dostopnost do vseh potrebnih informacij v pisarni in na terenu dobiva vedno večji pomen. Mobilni CRM omogoča ravno to, saj ima uporabnik na voljo točno tiste informacije, ki jih potrebuje za svoje vsakdanje delo. Uporabnik mobilnega CRM-ja postane bolj neodvisen, reakcijski čas je nižji, delo poteka hitreje, poveča se zadovoljstvo strank. Uporabnik mobilnega CRM-ja lahko vse želene informacije stranki posreduje takoj oziroma si zabeleži, da mora z njo stopiti v stik pristojna oseba. S tem se stranke izognejo iskanjem pomoči "od vrat do vrat", ko poskušajo dobiti informacijo, želijo oddati naročilo, podaljšati pogodbo, vložiti reklamacijo ipd. Ravno zaradi sodobnih potreb po informacijah postajajo mobilna CRM orodja odločilna za uspeh. Raziskovalna in svetovalna organizacija Gartner Research napoveduje, da bo do leta 2010 petnajst odstotkov vseh prodajnih informacij vnesenih preko mobilnih naprav [62].

Mobilne tehnologije pridejo zelo do izraza pri prodaji. Vsi zaposleni, ki opravljajo svoje delo tudi na terenu (npr. pospeševalci prodaje, vzdrževalci, serviserji, skrbniki strank, svetovalci ipd.), imajo s pomočjo mobilnega CRMja vedno pri sebi svoj razpored obiskov in sestankov, vse potrebne podatke o strankah, zgodovino stikov, naročil, reklamacij, statističnih podatkov ipd. Vse svoje ugotovitve lahko vnesejo v CRM že med obiskom ali takoj po njem. Mobilno CRM orodje ima konkurenčne prednosti, saj omogoča zajem informacij (npr. o prodajni priložnosti) v realnem času [62].

Podjetja, ki imajo v svoji prodaji veliko število terenskih prodajnih zastopnikov, skrbijo, da imajo čim bolj aktiven prodajni lijak (sales pipeline). Z drugimi besedami, skrbijo, da čim več potencialnih strank pretvorijo v realne priložnosti za prodajo, ki jih lahko na podlagi dobrih informacij o stranki hitro in uspešno uresničijo. Mobilno CRM orodje poleg tega omogoča terenskim delavcem, da s pomočjo vselej dostopnih informacij samostojno sprejemajo ustrezne odločitve [62].

Dobro mobilno CRM orodje mora omogočati tudi popolno integracijo z ERP sistemom podjetja, kajti šele takrat se lahko pričakuje, da bo CRM orodje prava konkurenčna prednost podjetja.

## 8.3 Trendi na področju mobilnih naprav

Garner je identificiral pet glavnih trendov, ki bodo vplivali na trg mobilnih naprav skozi leto 2009:

1. **Uveljavljeni proizvajalci se bodo utrdili, pridružili pa se jim bodo tudi novi:** Novi ponudniki mobilnih naprav, kot sta npr. Apple in Garmin, se želita razlikovati, medtem ko uveljavljeni ponudniki, kot je npr. Motorola se srečujejo z vse večjim izzivom pritiskov s trga, zato morajo biti vse bolj inovativni.
2. **Ponudniki mobilnih naprav gradijo ekosisteme:** Vse večji pritisk operaterjev na proizvajalce za zniževanje cen mobilnih naprav povzroča, da ponudniki mobilnih naprav poskušajo uporabnikom prodati tudi drugačne storitve, npr. Nokia z Ovi, SonyEricsson s PlayNow ter Apple z iTunes trgovino. To je v bistvu nov trg, ki prinaša spremembe med ponudnike, operaterje ter ponudnike vsebin.
3. **Izdelovalci mobilnih naprav zmanjšujejo kompleksnost uporabe:** Naraščajoče število funkcionalnosti ter potreba po drugačnosti zahteva tudi poenostavitev uporabniških vmesnikov ter izkušnjo storitev.
4. **Mobilne naprave postajajo del življenjskega stila:** Stil bo imel veliko vlogo pri vse večjem naboru mobilnih naprav. Ponudniki morajo definirati platforme, katerim je z majhnimi posegi in stroški mogoče zamenjati obliko ali barvo. Potrebne pa bodo tudi povezave z modnimi ali športnimi hišami za izboljšanje privlačnosti mobilnih naprav.
5. **Visoko zmogljive platforme je mogoče posodabljati:** Ponudniki morajo zagotavljati podporo, posodobitve ter nadgradnje naprav.

# 9 Zaključek

Problem se lahko reši šele takrat, ko se zavedamo, da obstaja. Pogledati je potrebno po organizaciji in prešteti, koliko različnih modelov mobilnih naprav se uporablja. Brez pravega pristopa pri upravljanju mobilnih naprav in brez pravega sistema upravljanja mobilnih naprav, bodo podjetja stežka preprečila odtekanje oz. krajo zaupnih informacij iz mobilnih naprav.

Podjetja se bodo morala soočiti z velikim naborom različnih platform mobilnih naprav. Za pričetek uspešnega obvladovanja mobilnih naprav pa bodo podjetja morala definirati standarde, kot je napisal Gold v enem od svojih zaključkov: "Standardizing on a platform will help, but will not totally isolate the company from device diversity. Companies will need to continually update their mobile strategy over the next few years to utilize the latest productivity-improving technologies." [66]

Obvladovanje mobilnih naprav v podjetju bo uspešno in bo imelo pozitivne učinke za podjetje zgolj, če se bo pri samem pristopu definiralo dobre temelje, na katerih se bo gradil celoten pristop. Dobri temelji pa so, kot je omenjeno v predhodnih odstavkih, dobro definiran in fleksibilen standard mobilnih naprav, ki se ga je potrebno dosledno držati.

Magistrsko delo prikazuje pristop obvladovanja mobilnih naprav v podjetju, ki mu bo prinesel nižje stroške upravljanja z mobilnimi napravami, zmanjšale se bodo varnostne grožnje, povečala se bo produktivnost uporabnikov. Cilj pa je bil tudi zagotoviti povečanje nivoja varnosti, ne da bi se poslabšala uporabniška izkušnja. Delo prikazuje predvsem probleme ter nakazuje možne rešitve. Prikazane so tudi smernice razvoja mobilnih naprav v prihodnosti.

Delo definira celovit pristop k obvladovanju mobilnih naprav ter tako prispeva k razjasnitvi in definiranju procesa upravljanja s konfiguracijami mobilnih naprav ter njegovo umestitev v obvladovanje celotne informacijske tehnologije v podjetju.

Z varnostjo se je potrebno spoprijeti na vseh ravneh poslovanja in se ji posvetiti na dnevni ravni. Ključnega pomena so stalni pregledi sistema in njegovo izboljševanje, saj lahko le na ta način zagotavljamo varnost informacijskega sistema v vsakem trenutku, ne glede na spremembe, ki nastajajo v procesih in sredstvih. Ključni dejavnik vpeljave

sistema za upravljanje informacijske varnosti so zaposleni, vključno z upravo in vodstvom, ki morajo varnostno politiko sprejeti.

Ker se mobilne tehnologije izredno hitro spreminjajo, je potrebno biti pri definiranju celovitih pristopov previden. V nalogi predstavljen pristop bi bilo potrebno v praksi čim večkrat preizkusiti in ga dopolniti ter spremeniti glede na novo pridobljene izkušnje.

# Literatura


[1] Khosrow Pour Mehdi: Encyclopedia of Information Science and Technology. Hershey: Idea Group, 2005. 3121 str.

[2] T. Prešeren, B. Žvanut, M. Bajec: Izdelava celovitih IT procesov, Dnevi slovenske informatike, Portorož, 9.-11. April 2008. Zbornik posvetovanja. Ljubljana: Slovensko društvo Informatika, 2008, str. 120.

[3] Weill, Peter, and Jeanne Ross. *IT Governance: How Top Performers Manage IT Decision Rights for Supperior Results*. Boston: Harvard Business School Press, 2004.

[4] J. Ma, J. Liao, X. Zhu, "Device Management in the ISM," *Journal of Network and Systems Management*, vol. 16, št. 1, str. 46-62, 2008

[5] J. Strachey, "Automatic configuration for mobile users," *Card Technology Today*, str. 5, oktober 2003.

[6] T. Walter et al, "Secure Mobile Business Applications – Framework, Architecture and Implementation," *Information Security Technical Report*, vol. 9, št. 4, str. 6-21, 2004.

[7] A. Brezavšček, L. Zupan, "Standardi in priporočila na področju informacijske varnosti," *Uporabna informatika*, letnik XIV, Št. 2, str. 91-97, 2006.

[8] Office of Government Commmerce, *ITIL v3*, 2007.

[9] IT Governance Istitute, *COBIT 4.1*, 2007.

[10] BS ISO/IEC 17799:2005 *Information technology – Security techniques – Code of practice for information security management*, British Standards Institution, 2005

[11] N.L. Clarke, S.M. Furnell. "Advanced user authentication for mobile devices," *Computer&Security*, vol. 26, št. 2, marec 2007, str. 109-119.

[12] Krisper, M., Rožanec, A.. "Obvladovanje informatike v poslovnih sistemih – Pomen strategije in arhitektur," *Uporabna informatika*, Slovensko društvo Informatika, 2005, št. 4. Letnik XIII, str. 194.

[13] ISO 17799:2005 Information technology – Security techniques – Code of practice for information security management. Geneva: ISO/IEC, 2005, 115 str.

[14] ISO 27001:2005 Information technology – Security techniques – Information security management systems – Requirements. Geneva: ISO/IEC, 2005, 34 str.

[15] Potočnik, K., Tajnik, F. (2003). Uporaba modela COBIT za načrtovanje in poročanje o njej. 11 Mednarodna konferenca o revidiranju in kontroli informacijskih sistemov: Slovenski inštitut za revizijo, 105-123.

[16] Wikipedija angleška različica. Dostopno na: http://en.wikipedia.org/wiki/Main_Page. Maj 2008.

[17] Alison Cartlidge in soavtorji. *An Introductory Overview of ITIL v3*, itSMF Ltd, 2007.

[18] Petrović Damjan, "Analiza informacijske varnostne politike v Agenciji RS za kmetijske trge in razvoj podeželja", Diplomsko delo. Univerza v Ljubljani, Ekonomska fakulteta, 2007.

[19] E. Cavalli, A. Mattasoglio, F. Pinciroli, P. Spaggiari, "Information security concepts and practices: the case of a provincial multi-speciality hospital", *Int. J. Med. Inf.* 73 (2004) str. 297–303.

[20] Erlend Bønes et al., Risk analysis of information security in a mobile instant messaging and presence system for healthcare, International Journal of Medical Informatics (2006), doi:10.1016/j.ijmedinf.2006.06.002

[21] Ključevšek Rado, Vodopivec Tadej, Dolinar Peter: Obvladovanje varnosti informacij v skladu s standardom BS 7799. Ljubljana:SIQ, (Ključevšek Rado, 2001)2001, 45 str.

[22] Zupan Lucija: Zahteve za uspešno vpeljavo standarda BS7799-2 za področje informacijske varnosti. Ljubljana: Uporabna informatika, 13(2005), 1, str. 37-50.

[23] E. Eugene Schultz. "Mobile computing: The Next Pandora's Box", Computers & Security. Letnik 2007,volumen 26, št. 3, str. 187.

[24] Mobile Device Management, http://mobiledevicemanagement.com/ 20.5.2008

[25] Robert Richardson. " 2007 CSI Computer Crime and Security Survey", Computer Security Institute. 2007.

[26] Alan Calder, Steve Watkins. "International IT Governance: An Executive Guide to ISO 17799/ISO 27001", Kogan Page Limited, 2006.

[27] Potočnik Marko: Analiza tveganja za odločanje o ravni varovanja informacij. Varnostni forum. Ljubljana, 2006. str. 12.

[28] Van Thanh, D., Jonvik, T., Vanem, E., Van Tran, D., Audestad, J.A.: The device management service. In: Proceedings of IEEE Intelligent Network Workshop, Boston, US, 2001

[29] Mei, H., Lukkien, J.: A remote personal device management framework based on SyncML DM specifications. In: Proceedings of the 6th international conference on Mobile data management, Ayia Napa, Cyprus, 2005.

[30] Chakravorty, R., Ottevanger, H.: Arhitecture and implementation of a remote management tramework for dynamically reconfigurable devices. In: Proceedings of the 10th IEEE international conference on Networks (IEEE ICON 2002) Singapore, 2002.

[31] Poikselka, M., Mayer, G., Khartabil, H., Niemi, A.: The IMS: IP Multimedia Concepts and Services in the Mobile Domain. Wiley, West Sussex, 2004.

[32] Trček, Denis. Informatika: od tehnologije do poslovanja. Koper: Visoka šola za management. 2001

[33] Renkema Theo J. W.: The IT value quest: how to capture the business value of IT-based infrastructure. Chichester, England: John Wiley & Sons Ltd, 2000.

[34] Distributed Management Task Force, Web-Based Enterprise Management (WEBEM), http://www.dmtf.org/standards/wbem.

[35] Distributed Management Task Force, Web Services for Management, http://www.dmtf.org/standards/published_documents/DSP0226.pdf

[36] Open Mobile Alliance, OMA Device Management Protocol, http://openmobilealliance.org/release_program/dm_v1_2A.html

[37] Jun Ma, Jianxin Liao, Xiaomin Zhu. Device management in the IMS, Journal of Network and Systems Management, Springer Netherlands, Vol. 16, št. 1, str 46-62, marec 2008.

[38] Geer, D.: Building converged networks with IMS technology. Computer, št. 38 , vol. 11, str. 14-16., 2005.

[39] D' Arizeno, M., Pescape, A., Ventre, G.: Dynamic service management in heterogeneous networks. J. Netw. Sys. Manage. Št. 12, str. 349-370, 2004.

[40] Butler, M.H.: Current technologies for device independence, HP Laboratories Technical Report, št. 83, 2001.

[41] Ma, J., Liao, J., Zhu, X., Wang, C., Zhang, Y.:Mobile terminal capability management for services enabling. In: Proceedings of the International Conference on Wireless and Mobile Communications, Bucharest, Romania, July 2006.

[42] TeleManagement Forum, GB917-1 v2.0, SLA management handbook volume 1: executive overview (2004).

[43] Benatallah, B., Motahari, N.H.R., Fabio, C., Farouk, T., Julien, P.: Service mosaic: a model-driven framework for web services life-cycle management. IEEE Internet Comput. 10(4), 55-63, 2006.

[44] 3rd Generation Partnership Project, Transparent end-to-end Packet-switched Streaming Service (PSS); Protocols and codecs, 3GPP TS 26.234 v 6.2.0, http://www.3gpp.org.

[45] Open Mobile Alliance, SyncML Device Information Approved Version 1.1.2, http://www.open-mobilealliance.org/release_programs/ds_v112.html

[46] Akahoshi, Y., Kidawara, Y., Tanaka, K.: A content and device management method for multiple contents browsing with multiple devices. In: Proceedings of the 21st International Conference on Data Engineering (ICDE '05), Tokyo, Japan, April 2005.

[47] Karl, G., Stephen, G., Heather, K., James, S.:Introduction to Web services architecture. IBM Syst. J. 41 (2), 170-177, 2002.

[48] W3C, Web Services Description Language (WSDL), http://www.w3.org

[49] STATE, R., FRESTOR, O.: Management of wireless dynamic infrastructures. In: proceedings of the Eighth IEEE International Symposium on Computer and Communications, Kemer-Antalya, Turkey, 2003.

[50] IETF, Session Initiation Protocol (SIP) – Specific Event Notification (RFC 3265), http://www.ietf.org.

[51] Oomen, P.: A framework for integrated of mobile-stations over the air. In: Proceedings of 2001 IEEE/IFIP Internationa Symposium on Integrated Network Management, Seattle, USA, 2001.

[52] OMA Member Product information, http://product.openmobilealliance.org

[53] Meyer, K., Persinger, D., Phelps, R.: Network management stations performance metrics. In: Proceedings of the 1994 IEEE Network Operations and Management Symposium, Kissimmee, FL, USA, 1994.

[54] Pradeep, R.: Evaluation methodology for network management systems. In: proceedings of the 1998 IEEE Network Operations and MAnagement Symposium, Par 2 (of 3), USA, 1998.

[55] Systems Engineering Process Office, Configuration Management Precess, Space and Naval Warfare Systems Center San Diego, 2006.

[56] A. Shevchenko, An Overview of Mobile Device Security. Viruslist.co, Kaspersky Lab, 2005, http://www.viruslist.com/en/analysis?pubid=170773606

[57] Afaria – Sybase iAnywhere - Mobile Device Management and Security, http://www.sybase.com/products/mobileenterprise/afaria

[58] Microsoft System Center Mobile Device Manager 2008, http://www.microsoft.com/systemcenter/mobile/default.mspx

[59] Nokia Intellisync Device Management, http://www.nokiaforbusiness.com/nfb/find_a_product/

[60] M.Ozimek, "Obvladovanje informacijske varnosti s pomočjo standardov," Dnevi slovenske informatike, Portorož, 9.-11. April 2008. Zbornik posvetovanja. Ljubljana: Slovensko društvo Informatika, 2008, str. 125.

[61] Borut Klepec, " Konvergenca govornih podatkovnih komunikacij v poslovnih okoljih, ". Dostopno na: www.ltfe.org, 16.9.2008.

[62] INFO SRC.SI, Konvergenca omrežij, naprav in vsebin; Leto 2006, št. 48.

[63] Agencija NET, http://www.agencijanet.si/konvergenca-tehnologij-bo-povecala-menjave-operaterjev/, 16.9.2008.

[64] Agencija NET, http://www.agencijanet.si/konvergenca-fiksnih-in-mobilnih-storitev/, 16.9.2008.

[65] Tanja Muha, "Ključna vprašanja konvergence elektronskih komunikacij", APEK, 2008.

[66] R. Hickey, Mobile device trends: Security, consolidation and more, SearchMobileComputing.com, Maj 2006.

[67] IDC, Worldwide Mobile Device Management Enterprice 2007–2011 Forecast and 2006 Vendor Shares – Sybase iAnywhere Profile, 2007

# Priloga 1 – Pregled funkcionalnosti posameznih orodij

## 1 Microsoft System Center Mobile Device Manager 2008

Z izdajo operacijskega sistema Windows Mobile 6.1 so skrbnikom IT sistemov preko Microsoft System Center Mobile Device Managerja 2008 omogočene nove varnostne funkcionalnosti. Izboljšana je tudi kontrola nad Windows Mobile mobilnimi napravami.

Mobile device Manager ima predvsem naslednje lastnosti:

- pomaga zaščititi občutljive informacije v primeru izgube ali kraje mobilne naprave,
- omogoča neprestano čiščenje mobilnih naprav za zmanjšanje varnostnih groženj,
- pripomore k nižjim stroškom vzdrževanja ter odpravljanja težav,
- zagotavlja večjo skalabilnost,
- robustna razvojna platforma.

### 1.1.1 Komponente in glavne funkcionalnosti

V naslednjih poglavjih so predstavljene funkcionalnosti in komponente Microsoftovega produkta.

#### *1.1.1.1 Nastavitve politik gesel*

**Zahtevaj geslo**

Te nastavitve zahtevajo od uporabnika, da si nastavi geslo na mobilni napravi.

**Tip gesla**

Od uporabnikov se lahko zahteva, da vnesejo določen tip gesla (dolžina, znaki, terminsko spreminjanje ...).

**Potek gesla**

Določitev termina v katerem se mobilna naprava samodejno zaklene, za uporabo pa je potrebno ponovno vtipkanje nastavljenega gesla.

**Število pomnjenih gesel**

Sistem si lahko zapomni N gesel za nazaj, tako da mora uporabnik vsakič vnesti novo geslo, s tem se poveča nivo varnosti.

**Dolžina gesla**

Sistem lahko od uporabnika zahteva, da mora biti geslo daljše od neke določene dolžine.

**Določitev števila dovoljenih napačnih vnosov gesla**

Če se uporabnik zmoti pri vnosu večkrat kot je to dovoljeno v sistemu, se bo pri zadnjem dovoljenem vpisu gesla izpisalo opozorilo, da v kolikor se uporabnik zmoti še enkrat, se bo vsebina mobilne naprave izbrisala.

**Resetiranje gesla na mobilni napravi**

V kolikor je uporabnik pozabil geslo, se lahko naredi resetiranje gesla.

**Določitev termina veljavnosti gesla**

Administratorji lahko nastavijo, koliko časa gesla veljajo in čez koliko časa jih bo potrebno zamenjati.

#### *1.1.1.2 Onemogočanje/Omogočanje funkcionalnosti naprave*

Izklop POP in IMAP sporočil

Ta politika omogoča nastavljanje, kateri način dostopa do elektronske pošte bo omogočen na mobilni napravi. Lahko se uporabil IMAP4 ali POP3, lahko pa tudi kateri drugi način.

Izklop funkcionalnosti pošiljanja SMS in MMS sporočil

Ta opcija omogoča uporabnikom omogočanje ali onemogočanje pošiljanja ali prejemanja SMS oz. MMS sporočil.

Upravljanje s cetifikati

Orodje omogoča brisanje naslednjih tipov certifikatov iz naprav: SPC certifikati, Priviligirani certifikati, normalni certifikati, root certifikati …

Izklop kamere – vse funkcionalnosti povezane s kamerami.

Izklop brezžične povezave - onemogočitev te funkcionalnosti na mobilni napravi.

Izkop infrardeče povezave

Izklop Bluetooth povezave

Izklop podpore za zunanje pomnilniške kartice

Konfiguracija dovoljenih profilov za Bluetooth

Konfiguracija popravkov za operacijski sistem

Konfiguracija upravljanja mobilnih naprav pri gostovanjih

#### *1.1.1.3 Onemogočanje funkcionalnosti aplikacij*

Izpis opozorila, ko skuša uporabnik namestiti nedovoljeno aplikacijo na mobilni telefon.

Onemogočanje aplikacij na točno določeni vrsti mobilnih naprav.

#### *1.1.1.4 Varnostna politika*

Omogočanje, da se na napravi poganja nepodpisane aplikacije, dodeljevanje administratorskih pravic uporabnikom, dovoljevanje nameščanja nepodpisanih .cab datotek, vklop enkripcije podatkov, shranjenih na spominskih karticah, nastavljanje opozoril na napravi, ko je potreben ponovni zagon mobilne naprave. To pride v poštev predvsem pri spreminjaju konfiguracij, pri katerih je poseg večji in je za njihovo pravilno izvajanje potreben ponovni zagon mobilne naprave.

Omenjeno orodje ima na voljo še veliko drugih funkcionalnosti, ki pa jih v delu nisem posebej navajal.

### 1.1.2 Podprte naprave

Predstavljeni produkt podpira zgolj naprave z Windows Mobile operacijskim sistemom verzije 6.1. Kar je v glavnem tudi slabost, kajti trenutno v večini podjetjih nimajo definiranega standarda mobilnih naprav, ki bi temeljil izključno na Windows Mobile operacijskemu sistemu.

# 2 Afaria – Sybase iAnywhere - Mobile Device Management and Security

Afaria ima združene enostavne funkcionalnosti za varnost in upravljanje mobilnih naprav, s tem se zagotavlja, da so mobilne naprave posodobljene, zanesljive ter varne.

Afaria podpira vrsto različnih tipov mobilnih naprav, aplikacij, podatkov ter komunikacij, preko katerih se upravljanje izvaja, podprte pa so tudi različne pasovne širine.

Afaria zagotavlja upravljanje vseh vrst mobilnih naprav preko ene konzole.

### 2.1.1 Komponente

**Afaria Backup Manager**

Backup Manager zagotavlja centraliziran, avtomatiziran proces za arhiviranje kritičnih poslovnih podatkov končnih uporabnikov. S tem je zagotovljena dostopnost podatkov tudi če je mobilna naprava izgubljena, uničena ali ukradena.

**Afaria Configuration Manager**

Configuration Manager zagotavlja glavne funkcionalnosti za konfiguracijo mobilnih naprav, ne da bi uporabniki sploh vedeli oz. občutili, da se na mobilnih napravah konfiguracija spreminja.

**Afaria Document Manager**

Document Manager je enostavna rešitev za zagotavljanje vsebin končnim uporabnikom, ki jih potrebujejo. Skrbi za dostavo in posodabljanje podatkov, dokumentov ter vsebin mobilnim napravam brez vključevanja uporabnikov v sam proces

**Afaria Inventory Manager**

S povečevanjem števila mobilnih naprav v podjetju oz. organizaciji je zelo pomembno pridobiti informacije o strojni ter programski opremi na mobilnih napravah.

**Afaria License Manager**

Omogoča popoln pregled nad aplikacijami, ki se na mobilnih napravah uporabljajo. Spremlja nameščanje aplikacij, uporabo aplikacij, primerja dejansko uporabo z licenčnimi pogoji glede na število mobilnih naprav, na katerih so posamezne aplikacije nameščene, spremla lahko tudi datum poteka licence.

**Afaria OneTouch**

OneTouch poenostavi proces povezovanja naprav v omrežje, prijavljanje na napravo, dokončanje kritičnih aktivnosti, kot je npr. varnosti pregled naprave (antivirusni program), sinhonizacije, varnostne kopije.

**Afaria Patch Manager**

Patch Manager zagotavlja avtomatsko posodabljanje naprav, na katerih teče Microsoftov operacijski sistem.

**Afaria Remote Control**

Remote Control omogoča administratorjem popoln, varen oddaljen prevzem kontrole nad mobilno napravo, kar je predvsem koristno za Service Desk, ter za oddaljen dostop do naprav.

**Afaria Security Manager**

Security Manager ponuja varnost za mobilne naprave in prenosne računalnike. Omogoča centralno upravljanje varnosti, omogoča oddaljeno vsiljevanje varnostnih politik npr. vklop funkcionalnosti za vpis gesla pri vklopu naprave, vklop kriptiranja vsebine na nosilcih podatkov, upravljanje konfiguracije naprav, posodabljanje antivirusnih definicij …

**Afaria Session Manager**

Session Manager uporablja pristop, ki temelji na sejah (session-oriented), s tem pa omogoča avtomatsko izvajanje poslovnih procesov ter izboljša učinkovitost povezovanja naprav in sistemov.

**Afaria Software Manager**

Software Manager omogoča enostavno centralno nameščanje, distribuiranje, vzdrževanje ter podporo aplikacij, ne glede na to, kje se uporabniki nahajajo in kakšno vrsto naprave uporabljajo.

**Afaria SMS Integration Suite**

Omogoča integracijo z orodjem Systems Management Server 2003, ki je v osnovi namenjeno upravljanju konfiguracij delovnih postaj, prenosnikov ter strežnikov.

### 2.1.2 Glavne funkcionalnosti

**Varnost**

- Centralno vsiljevanje varnostnih politik podjetja
- Kriptiranje celotne vsebine trdega diska pri prenosnih računalnikih
- Kriptiranje elektronske pošte ter PIM na mobilnih napravah

- Kriptiranje preko zraka
- Začasno povračilo gesla
- Zaščita mobilne naprave s požarnim zidom ter antivirusnim programom

**Centralno upravljanje in kontrola**

- Upravljanje ter zagotavljanje varnosti iz ene konzole
- Posodabljanje aplikacij in podatkov po potrebi
- Upravljanja skupin in posameznikov
- Distribucija programske opreme preko zraka
- Minimalna uporabniška interakcija

**Interoperabilnost z tehnologijo Push emali**

- OneBridge push email, Microsoft push email (SP2)

**Podprti operacijski sistemi mobilnih naprav**

- Windows Mobile (Pocket PC, Windows Mobile 5.0, smartphone),Windows Notebooks, RIM BlackBerry, Palm OS, Symbian

**Podprte brezžične povezave**

- GPRS/EDGE/3G,W-LAN e.g. 802.11b/g, Infrared, Bluetooth

### 2.1.3 Podprte naprave

V spodnji tabeli so prikazane podprte mobilne naprave v orodju Afaria. Prvi stolpec prikazuje proizvajalca, drugi modele, v tretjem stolpcu pa je razvidno, kateri modeli so z orodjem dejansko podprti.

| Proizvajalec | Model | Podprt v orodju |
|---|---|---|
| **Nokia** | E50, E51, E60, E61, E61i, E62, E65, E66, E70, E71, E90 | Da |
| **SonyEricsson** | P1i, M608c, M600i, P990i | Ne |
| **HTC** | Vsi modeli | Da |

**Tabela 5: Podprte naprave z orodjem Sybase Afaria**

# 3 Nokia Intellisync Device Management

Orodje je zgrajeno na osnovi Open Mobile Alliance priporočil in je popolnoma kompatibilno z Nokia E serijo mobilnimi napravami ter z velikim nabodom mobilnih naprav različnih proizvajalcev, ki so tudi predstavljeni v nadaljevanju.

Orodje je tudi popolnoma kompatibilno z naslednjimi operacijskimi sistemi Symbian, Windows Mobile, Palm, BlackBerry ter Windows operacijskim sistemom za prenosne računalnike ter delovne postaje.

Vsebuje veliko orodij, ki omogočajo zaščito pred krajo, distribuiranje novih nastavitev po vseh mobilnih napravah istočasno in s tem zagotavljanje varnosti na mobilnih napravah.

Enostavni uporabniški vmesniki za administratorje.

### 3.1.1 Komponente in glavne funkcionalnosti

**Upravljanje z grožnjami podjetja**

Varne komunikacije

- Veliko možnosti kriptiranja (3DES, AES, SSL)
- Več opcij avtentikacije uporabnikov, vključno z avtentikacijo preko aktivnega imenika ter LDAP protokola
- Možnosti za javljanje poteka gesel …

Varnostne politike

- Politike gesel, gesla pri vklopu naprave
- Enkratna gesla za hitro obnavljanje
- Vsiljevanje varnostnih politik na mobilnih napravah

Zaščita pred krajo-izgubo mobilne naprave

- Zaklepanje mobilne naprave ob daljši neaktivnosti
- Brisanje določenih vsebin, datotek, map

**Enostavna administracija**

Upravljanje nastavitev mobilne naprave

- Uveljavljanje politik na mobilnih napravah preko zraka

- Vsiljevanje nastavitev

Upravljanje aplikacij

- Distribucija programske opreme ter popravkov
- Onemogočanje aplikacij ter vsiljevanje konfiguracij
- Targetirano posodabljanje mobilnih naprav, aplikacij ali uporabnikov
- Skriptni jeziki za razširitve in prilagoditve (Visual Basic)
- Zapoznela aktivacija programske opreme
- Tihe namestitve programske opreme

Upravljanje pridobljenih podatkov ter poročanje

- Inventar strojne in programske opreme
- Skladnost programskih licenc
- Planiranje prednameščanje programske opreme
- Administratorska opozorila osnovana na podatkih inventorija

**Fleksibilnost administracije**

Administrativna konzola

- Večvrstna administratorska konzola za upravljanje oddelkov ali strani, z ločenimi skupinami mobilnih naprav ali uporabnikom.
- Definirana administracija preko uporabniških skupin, strank, mest ali drugih organizacijskih meja.
- Akcije, ki se jih lahko konfigurira, ter določa termine izvajanja
- Spletni in Windows vmesniki

Inteligentnost preko zraka

- Določanje terminov ter dogodkov pri iniciiranju sej
- Optimizacija pri brezžičnih povezavah
    - Prenos samo sprememb namesto celotne datoteke
    - Distribucija objav, ki je odvisna od pasovne širine
    - Ponovno prenašanje podatkov od točke prekinitve

Odpravljanje težav pri mobilnih napravah ter podpora

- Opazovanje naprav v realnem času
- Beleženje aktivnosti klienta na strežniku
- Shranjevanje logov v podatkovni bazi, ki je ODBC podprta
- Spletna poročila za zaposlene v storitvenem centru

Obnavljanje mobilne naprave ter podpora

- Izdelovanje varnostnih kopij in nato obnavljanje konfiguracij, datotek, aplikacij
- Ohranjanje več vrst mobilnih naprav posodobljenih
- Uporabnik lahko v primeru kraje ali izgube mobilne naprave preko spleta izbriše vse občutljive vsebine na mobilni napravi

### 3.1.2 Podprte naprave

Podprte platforme:

- BlackBerry OS 3.7.1, 4.0.0
- Palm OS 3.5 up
- Symbian OS v7.0, v7.0s, v7.0sy, v8.0a, v8.1, v9.1, v9.2
- Windows Mobile 2003, 5.0, 6.0
- Windows 2000 and XP

Podprti standardi na področju upravljanja mobilnih naprav:

- Open Mobile Alliance (OMA)
- OMA CP 1.1
- OMA DM 1.1.2
- OMA DM 1.2

| Proizvajalec | Model | Podprt v orodju |
|---|---|---|
| **Nokia** | E50, E51, E60, E61, E61i, E62, E65, E66, E70, E71, E90 | Da |
| **SonyEricsson** | P1i, M608c, M600i, P990i | Da |
| **HTC** | Vsi modeli | Da |

**Tabela 6: Podprte naprave z orodjem Nokia Intellisync Mobile Device MAnagement**

## Izjava o samostojnosti dela

Izjavljam, da sem magistrsko delo izdelal samostojno pod mentorstvom doc. dr. Marka Bajca in dovoljujem javno objavo elektronske oblike magistrskega dela v zbirki 'Dela FRI'.

V Ljubljani, november 2008 Tadej Prešeren