

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA
KATEDRA INFORMAČNÍCH TECHNOLOGIÍ



OS Windows Mobile – Správa mobilních zařízení

Diplomová práce

Praha 2010 ©

Vedoucí práce: Ing. Jiří Vaněk, Ph.D.

Autor práce: Jiří Šilhán

Prohlášení

Prohlašuji, že jsem diplomovou práci na téma „*OS Windows Mobile – správa mobilních zařízení*“ vypracoval samostatně, pouze za odborného vedení vedoucího diplomové práce.

Dále prohlašuji, že veškeré podklady, ze kterých jsem čerpal, jsou uvedeny v seznamu použité literatury.

V Praze, dne 18.3.2010

Podpis:

Poděkování

Rád bych tímto vyjádřil poděkování Ing. Jiřímu Vaňkovi, Ph.D. za jeho cenné připomínky, odborné vedení a ochotu při vedení mé diplomové práce.

Název

OS Windows Mobile – správa mobilních zařízení

Souhrn

Diplomová práce se zabývá praktickým testováním aplikací pro správu mobilních zařízení Afaria a Microsoft Mobile Device Manager, jejich vzájemným porovnáním a zhodnocením možností jejich použití pro správu mobilních zařízení v síti. V rámci diplomové práce byl zpracován konkrétní návrh implementace aplikace Afaria v projektu mobilní výukové sítě, která byla navržena pro Střední průmyslovou školu na Proseku. V diplomové práci byla také uvedena charakteristika operačního systému Windows Mobile.

Klíčová slova

Windows Mobile, Afaria, Mobile Device Manager, Správa mobilních zařízení, Mobilní výuková síť

Title

OS Windows Mobile – mobile device management

Summary

The diploma work deals with practical testing of applications for management of mobile devices Afaria and Microsoft Mobile Device Manager, their comparison and evaluation of their possibilities for management of mobile devices in network. In scope of the diploma work was processed concrete project of implementation Afaria application in project of Mobile education network, that was designed for Střední průmyslová škola na Proseku. In the diploma work was also bring in characteristics of operation system Windows Mobile.

Key Words

Windows Mobile, Afaria, Mobile Device Manager, Mobile device management, Mobile education network

Obsah

1	Úvod.....	8
2	Cíl práce a metodika.....	9
2.1	Cíl práce	9
2.2	Metodika.....	9
3	OS Windows Mobile.....	10
3.1	Verze operačního systému WM	10
3.1.1	Windows CE 1.0	11
3.1.2	Windows CE 2	11
3.1.3	Windows CE 3	12
3.1.4	Windows CE 4	13
3.1.5	Windows CE 5	13
3.1.6	Windows CE 6	13
3.1.7	Windows CE 6.5	14
3.2	Architektura Windows Mobile.....	15
3.2.1	Základní přehled jednotlivých komponent OS	16
3.2.2	Ovladače zařízení	16
3.2.3	Kernel - Jádro	16
3.2.4	Systém správy souborů	16
3.2.5	GDI - Graphic Device Interface (rozhraní grafického zařízení)	17
3.2.6	Komunikační rozhraní a lokalizace.....	17
3.3	Základní vlastnosti OS	17
3.3.1	Synchronizace s PC.....	19
3.3.2	Zálohování dat.....	19
3.3.3	Zabezpečení.....	20
3.3.4	Síťové aplikace na platformě WM.....	21
3.3.5	Správa mobilních zařízení v podniku.....	21
3.3.6	Synchronizace	21
3.3.7	Zabezpečení.....	22
3.3.8	Správa zařízení	22
3.3.9	Využití WM při obchodní činnosti	23
3.3.10	Produkty pro WM	24
4	Microsoft System Center Mobile Device Manager	25
4.1	Architektura aplikace.....	26
4.1.1	Gateway Server	27
4.1.2	Device Management (DM) Server	28
4.1.3	Enrollment (zapisovací) Server.....	28
4.1.4	Databáze	28
4.1.5	Active Directory	28
4.1.6	OTA (Over-The-Air) řízení a zavádění.....	28
4.1.7	OTA SW distribuce založená na WSUS 3.0.....	29
4.1.8	Informace o klientských zařízeních	30

4.1.9	Role-based administrace	30
4.1.10	Self-Service Portal (SSP)	30
4.1.11	Škálovatelná architektura	31
4.1.12	Mobilní VPN	32
4.2	Zabezpečení	33
4.3	Možnosti použití	35
5	Afaria – management mobilních zařízení	40
5.1	Architektura aplikace	41
5.1.1	Afaria server	43
5.1.2	Afaria administrator	46
5.1.3	Afaria serverové pole	46
5.1.4	Typy klientů	46
5.1.5	Relay server	48
5.2	Zabezpečení	49
5.3	Možnosti použití	53
6	Správa mobilních zařízení – možnosti implementace a hodnocení	57
6.1	Návrh mobilní sítě pro výukové účely na SŠ	58
6.1.1	Hadwarové zabezpečení mobilní sítě	60
6.1.2	Softwarové zabezpečení mobilní sítě	66
6.2	Implementace	67
6.3	Ekonomická analýza	71
7	Závěr	72
8	Seznam literatury	73
9	Seznam zkratk	74
10	Seznam obrázků	76

1 Úvod

Mobilní technologie a mobilní zařízení jsou dnes rozšířeny v mnoha oborech lidské činnosti. Jsou nenahraditelnými pomocníky, kteří usnadňují práci. PDA a MDA zařízení slouží pro sběr dat při průzkumech veřejného mínění, pro zpracování objednávek od obchodních zástupců až po jejich nasazení v oblasti válečné chirurgie.

Jedním z velmi rozšířených operačních systémů v mobilních zařízeních je Windows Mobile. Výhodou tohoto operačního systému je dostupnost velkého množství programů založených na platformě Windows Mobile. S nasazením mobilních zařízení s operačním systémem Windows Mobile v podniku vyvstává také potřeba jejich centrální správy a údržby, a to včetně údržby aplikací, které jsou v mobilních sítích používány.

Nejpoužívanějšími aplikacemi pro správu mobilních zařízení jsou Microsoft System Center Mobile Device Manager a Afaria. Správci mobilní sítě umožňují tyto aplikace provádět veškerou vzdálenou údržbu mobilních zařízení jak po hardwarové tak i softwarové stránce.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je praktické otestování aplikací pro správu mobilních zařízení Afaria a Microsoft Mobile Device Manager, jejich vzájemné porovnání a zhodnocení možností jejich implementace. Dalším cílem pak je implementace zvolené aplikace pro správu mobilních zařízení v rámci projektu mobilní výukové sítě a charakteristika operačního systému Windows Mobile.

2.2 Metodika

Nejprve bude uvedena charakteristika operačního systému Windows Mobile (WM) a síťových aplikací pro platformu WM. V následující kapitole budou prakticky testovány možnosti použití aplikace pro správu mobilních zařízení v síti Microsoft System Center Mobile Device manager. V další kapitole budou prakticky testovány možnosti použití aplikace pro správu mobilních zařízení v síti Afaria. Poslední kapitola se bude zabývat porovnáním obou aplikací a návrhem mobilní výukové sítě pro střední školu, možnostmi její implementace a ekonomickou analýzou.

3 OS Windows Mobile

Počátky vývoje Windows Mobile (též označovaný jako Windows CE) se datují do roku 1992. Hlavním cílem bylo vyvinout mobilní zařízení s operačním systémem Windows. Myšlenkou bylo upravit zdrojový kód platformy Windows 16 do nové x86 platformy. Projekt WinPad však předběhl ve vývoji svou dobu. Počítalo se s podporou moderních technologií jako např. rozpoznávání písma. Standardní hardware té doby nebyl dostatečně výkonný. Takto náročné technologie vyžadují 32 - bitové procesory, které nebyly ještě standardem pro komerční použití. Stejným problémem bylo i malé množství paměti u vyvíjených kapesních počítačů. Po diskusi s partnery, kteří se podíleli na vývoji projektu WinPad, se Microsoft rozhodl od něho odstoupit. Definitivně byl projekt WinPad uzavřen roku 1994.

Souběžně existoval projekt Pulsar, jehož myšlenkou bylo vytvoření multifunkčního zařízení, které by bylo dostatečně levné pro sériovou výrobu s jednoduchou obsluhou a ovládáním pouze několika tlačítky pro využití různých praktických funkcí. Zmíněná vize se zdála společnosti Microsoft jako pravděpodobně správný směr budoucího vývoje. Od myšlenky praktické realizaci byla však ještě dlouhá cesta. Předpokládalo se, že o takové zařízení by mohl být na trhu zájem a že vize podoby budoucího zařízení je ta správná. Předpoklady pro sériovou výrobu byly podpořeny úspěchy firem Apple a Psion s jejich nabídkou mobilních zařízení. Na počátku 90. let však ještě trh a zákazníci nebyli připraveni na příchod nového typu zařízení. Bylo nezbytné počkat s uvedením moderních technologií na trh. Týmy vědců z projektu WinPad a Pulsar byly sloučeny do jednoho a tím vznikl projekt Pegasus.

3.1 Verze operačního systému WM

Po sloučení projektů WinPad a Pulsar začal nový vývojový tým práci na zcela novém systému založeném na 32 bitové technologii. Roku 1995 započaly testy na operačním systému Windows Pegasus, který byl použit na zcela nové řadě mobilních zařízení. Pro mobilní zařízení, která měla být určena pro nový operační systém, byly stanoveny poměrně přísné specifikace pro použitý hardware. Několika výrobcům

hardware byly poslány parametry, jak má nové mobilní zařízení vypadat. Rozměry 18x10x2,5 cm , napájení na dvě AA baterie, váha menší než 500g, QWERTY klávesnice, dotykový LCD display se 480x240 pixely, stylus pro použití místo myši na dotykové obrazovce, minimálně 4 MB paměti ROM a 2 MB paměti RAM, infračervený port, slot pro PCMCIA karty, RS-232 sériový port, výstup pro audio a architekturu procesoru založenou na MIPS 3000 nebo MIPS 4000. Zařízení pro Win. Pegasus mělo být víceúčelové , pracující na 32-bit procesorové technologii a OS (operační systém) měl obsahovat kódování Unicode (kvůli použitelnosti v různých jazykových variantách). Několik měsíců po založení projektu Pegasus začaly konzultace s výrobcí hardware a OS byl nazván Windows CE 1.0

3.1.1 Windows CE 1.0

Vývoj se soustředil na to, aby se mobilní zařízení pro tento OS stalo skutečně kapesním. S ohledem na nově se rozvíjející trh vývoj směřoval k tomu, aby se PDA stalo doplňkem Notebooku. Mobilní zařízení v této době stále obsahovala kompletní klávesnici. Firma HP upravila jedno z těchto zařízení a nabídla rozlišení displeje 640x240, též lze použít označení "HVGA". Zařízení se stalo více populární než jeho předchůdci s rozlišením 480x240. Toto rozlišení se stalo standardním pro mobilní zařízení s Windows CE. Další verzí tohoto OS je Win. CE 1.01, které obsahovalo japonštinu. Windows CE 1 postrádal širší podporu pro produkty od jiných výrobců než je Microsoft.

3.1.2 Windows CE 2

S příchodem Windows CE 2 přestává být Windows CE operačním systémem pouze pro Handheld PC (tj. kapesní počítač obsahující hardwarovou QWERTY klávesnici). CE 2.0 je první vestavěný OS. Výrobci hardware nyní mohli využít jakoukoliv část platformy Windows CE pro svá zařízení a měli volné ruce pro vytvoření libovolných zařízení založených na této platformě. Windows CE bylo možné použít tedy jak v Handheld PC zařízeních, tak v autech, herních konzolích, automatech atd. CE 2 mohl běžet na zařízeních s HVGA i plném VGA rozlišení. Existovaly a existují dvě

skupiny koncových zákazníků: Jedna skupina standardních uživatelů PDA zařízení a druhá skupina uživatelů, která hledá zařízení schopné nahradit Notebook, aby poskytlo více uživatelské volnosti. Prodejnost CE 2 napomáhala podobnost uživatelského rozhraní s Windows 98. Ke standardnímu vybavení CE 2 patřil nejen Internet Explorer, ale také i MS Word, Excel, Outlook a Powerpoint. Ve verzi Windows CE 2.11 pro Handheld PC byl obsažen i MS access. CE 2 byl navržen pro velké množství různých procesorů s nízkou spotřebou energie jako Intel x89(468DX / Pentium), NEC VR4300 (MIPS) nebo DEC SA1100 (StrongArm). Windows CE 2.10 obsahoval některé upgrady jako podporu FAT 32, USB, podporu pro 256 různých systémů souborů a další upgrady. Původním synchronizačním softwarem byl Windows CE Services 2x, později byl překonán softwarem nazývaným ActiveSync 3.0. Vývoj Windows CE 2 byl zastaven po rozhodnutí vyvinout nový univerzální operační systém, který umožní širší hardwarovou podporu a tím podpoří další rozvoj mobilních technologií a využije pokrok ve vývoji nových procesorů a výkonnějších baterií. S příchodem Windows CE 3 vznikl první reálný kapesní počítač.

3.1.3 Windows CE 3

Tento OS změnil směr vývoje OS Windows Mobile. Záměrem firmy Microsoft bylo vytvořit vestavěný OS a mobilní zařízení schopné konkurovat PDA založeným na konkurenčním OS Palm. Prakticky se mělo změnit uživatelské rozhraní a přiblížit se zařízením s OS Palm. Jednalo se již o dnešní kapesní počítače. Kapesní počítač, na rozdíl od Handheld PC, neobsahuje hardwarovou klávesnici, má pouze několik funkčních tlačítek, přičemž klávesnice je na dotykové obrazovce zařízení a ovládá se stylusem (pero používané pro ovládání dotykové obrazovky). Nové grafické rozhraní CE 3 doznalo určitých změn a bylo celé od základu zjednodušeno. Microsoft přidal podporu pro nové komunikační a aplikační rozhraní, aby se rozšířilo jádro Windows CE Cedar. Windows CE 3.0 s pozdějším názvem Pocket PC 2000 byl uveden na trh v květnu 2000. Tímto OS získala navrch nová PDA nad starými modely Handheld PC. K rozšíření PDA přispělo také snižování cen těchto zařízení.

3.1.4 Windows CE 4

Je více známý pod názvem Windows Mobile 2003, byl doplněn o mnohá další vylepšení, hlavně podporu ARM procesorů od firmy Intel. Jádro CE 4 je oproti CE 3 kompletně přeprogramované. Během 12 měsíců od vydání původního Windows CE 4 přišly na trh ještě další dvě verze: Windows CE Net 4.1 a 4.2 označovaná jako Windows Mobile 2003 Second Edition, která doznala dalších vylepšení jako možnost rotace obrazovky. Samozřejmě je, že systém obsahuje kapesní Internet Explorer, Windows Media Player a Pocket Office.

3.1.5 Windows CE 5

Windows Mobile 2005 byl vyvíjen pro plnou podporu Windows Vista, které však měly oproti WM 2005 ve vydání velké zpoždění. Pokrokem u CE 5 je navýšení možností mobilních zařízení. WM 2005 nese kódové označení Macallan, podporuje také Smart Display Remote Protocol, který umožňuje CE 5 jednat jako prodloužení pracovní plochy stolního PC. Poprvé v historii Microsoft také u tohoto OS zpřístupnil část zdrojového kódu pro vývojáře pracující na této platformě. Pokrok představuje zejména skutečnost, že OS je uložen ve flash paměti a do paměti RAM je následně načítán. Pro hráče her je zajímavé také to, že CE 5 obsahuje plnou verzi DirectX 8 Direct3D. Toto vylepšení dovoluje vývoj lepších a graficky propracovanějších her pro mobilní zařízení.

3.1.6 Windows CE 6

Windows CE 6 pokračuje ve stopách předchozích Windows CE a je určen jako doplněk pro Windows Vista. CE 6 má jádro nové generace. Jádro umožňuje běh až 32000 virtuálních procesů a dovoluje přidělit procesu až 2 GB virtuální paměti. Windows Mobile existuje v několika verzích pro různá zařízení: Handheld PC (dnes již tato platforma není tak rozšířená), kapesní počítače (nejrozšířenější platforma) a pro takzvané MDA (Mobile Digital Assistant), což je zařízení obsahující GSM modul. MDA kombinuje funkce kapesního počítače a mobilního telefonu. Microsoft přináší s CE 6 nový, relativně velmi stabilní mobilní OS. Novinkou u CE 6 je integrovaný VOIP klient (rozumí se klient pro IP telefonii). Další novou podporovanou službou je

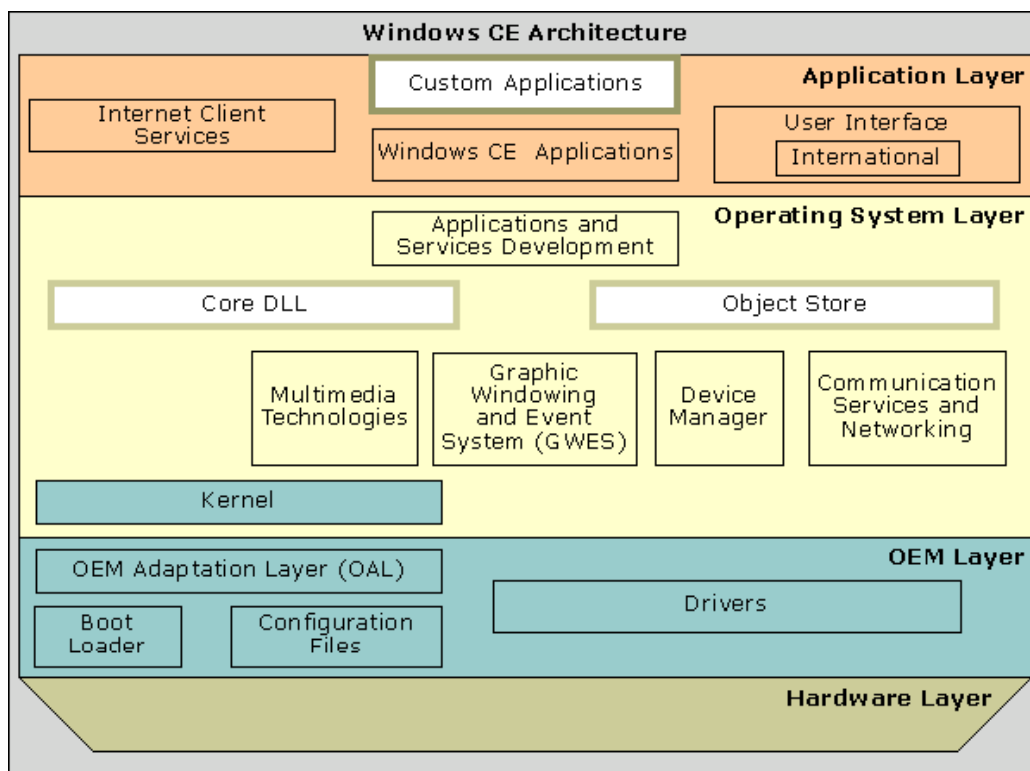
Windows Live. Služba má pomoci s hledáním informací online (k tomuto účelu slouží aplikace Windows Live Home a Windows Live Search), kontaktováním dalších osob prostřednictvím programů Windows Live Messenger a Windows Live Spaces. Windows Live je dostupná rovněž ve stolních Windows Vista. Jejich přidání do nejnovější verze Windows Mobile značí snahu o přiblížování stolní a mobilní verze Windows k sobě. Microsoft vytváří komplexní balík produktů pro uživatele zřejmě ve snaze upevnit své postavení jedničky na trhu. Propojování a návaznost jednotlivých produktů z dílny spol. Microsoft je pravděpodobně novým (staronovým) trendem. Microsoft tlačí uživatele k maximálnímu využívání software ze své produkce. Na druhou stranu je to pro uživatele výhodou. Je zaručena kompatibilita jednotlivých produktů a uživatelská podpora.

3.1.7 Windows CE 6.5

Je v současné době nejnovější verzí operačního systému Windows Mobile. Výrazné zlepšení doznal operační systém v oblasti ovládání prsty bez stylusu a komfortnějšího ovládání webového prohlížeče (ovládání mobilního Internet Exploreru se přibližuje mobilní verzi webového prohlížeče Opera). Jsou podporovány dvě nové služby. Služba MyPhone pro bezdrátovou synchronizaci fotek, zpráv, kontaktů, videí a služba Windows Market Place pro jednoduchý nákup resp. stažení dalších aplikací přímo do mobilního zařízení. Obchodní název pro mobilní operační systémy společnost Microsoft změnila na Windows Phone. Operační systémy Windows CE jsou však i nadále označovány Windows Mobile.

3.2 Architektura Windows Mobile

Windows CE je otevřený 32 - bitový operační systém s multitaskingem a multithreadingem pro různá mobilní zařízení jako kapesní počítače, smartphony, MDA, prodejní terminály a celou škálu dalších různých zařízení. Windows CE byl navrhován tak, aby se grafické uživatelské rozhraní podobalo co nejvíce stolním verzím Windows. Dále obsahuje klasickou podporu internetových komunikačních protokolů pro práci s internetem. Rozhraní Win32 API (application programming interface), což znamená rozhraní pro programování aplikací, dovoluje vývojářům software vyvíjet a upravovat software na platformě Windows CE. OS se skládá z jednotlivých modulů, které mohou být nezávislými vývojáři sestavovány pro potřeby implementace OS na určitá hardwarová zařízení. Podporuje velké množství hardwarových periférií, USB zařízení, tisk a přídatná paměťová média. Podporuje širokou škálu procesorů: Procesory NEC, Samsung, Hitachi SH3, SH4, ARM, Intel X-Scale a mnoho dalších.



obrázek č. 1 – Architektura Windows CE [1]

3.2.1 Základní přehled jednotlivých komponent OS

Operační systém Windows Mobile tvoří několik základních systémových vrstev (anglicky „layer“). Každá vrstva zabezpečuje určitou část služeb OS. Vrstvy se skládají z několika dalších komponent viz. obrázek č. 1. **Application Layer** (Aplikační vrstva) – komunikuje s aplikacemi. Jsou v ní definovány základní služby jako elektronická pošta, WWW apod. **Operating System Layer** (Vrstva operačního systému) – se skládá z jádra, DLL knihoven, objektového skladiště (Object store), komunikačních a síťových protokolů a Grafického „okenního“ událostního subsystému (Graphic Windowing and Events Subsystem - GWES). GWES zabezpečuje interface mezi aplikacemi, uživatelem a OS. **OAL - OEM** (Original Equipment Manufacturer) **Adapation Layer** - OAL odděluje jádro a hardwarovou vrstvu. Ta je součástí OS, protože Windows CE není navržen pro žádný konkrétní hardware. Specifikuje pro jádro OS konkrétní hardware. Řídí hardwarová přerušení, implementuje periferie, systémový čas a napájení. **Hardware Layer** (vrstva hardware) – je fyzický hardware, na kterém je OS spuštěn.

3.2.2 Ovladače zařízení

Windows CE obsahuje ovladače pro podporu správného fungování displeje, napájení, připojených USB zařízení, tisku v síti a dalších funkcí.

3.2.3 Kernel - Jádro

Jádro obsahuje vícevláknový, preemptivní multitasking. Jádro je založeno na platformě Win32. Pracuje se systémem několika úrovní priorit vláken procesů. Stránkování paměti je podporováno pamětí RAM a ROM. Čekací doba jednotlivých vláken je velmi nízká. Díky OAL je jádro schopné pracovat s více typy procesorů.

3.2.4 Systém správy souborů

Funguje jako objektové skladiště (Object store). Skládá se ze systému souborů, databáze a systémových registrů. Tyto služby poskytuje stálé skladiště aplikacím a datům, které souvisejí s danými aplikacemi. Objektové skladiště může být až 256 MB

komprimované, nevolatilní (stálé) RAM paměti. Systém souborů může být v paměti typu RAM (Random Access Memory) a ROM (Read only Memory) nebo pouze ROM. U kombinace paměti RAM a ROM je objektové skladiště v RAM paměti a poskytuje přístup do ROM paměti. Pokud je pouze paměť ROM systém souborů, nedovolí umístění souborů do objektového skladiště. Data uložená v paměti ROM jsou nepřístupná přes Windows adresář. Databáze umožňuje ukládání, třídění a přístup k datům. Systémové registry naproti tomu ukládají data o aplikacích, řadiče a konfiguraci nastavení. Object store podporuje různé typy souborových systémů.

3.2.5 GDI - Graphic Device Interface (rozhraní grafického zařízení)

Slouží k podpoře grafiky, která není závislá na použitém hardware. Umožňuje definování grafického výstupu pomocí funkcí vykreslování. U Windows CE pracuje na principu rastru.

3.2.6 Komunikační rozhraní a lokalizace

OS podporuje protokoly TCP/IP, FTP, HTTP, připojení do místních sítí LAN, do světové sítě Internet, přímé připojení ke stolnímu PC a možnosti propojení s dalšími mobilními zařízeními. Obsahuje kódování Unicode, díky kterému je možná široká jazyková podpora.

3.3 Základní vlastnosti OS

GUI (graphic user interface - grafické rozhraní) je uživatelsky velmi přívětivé, podobné stolním Windows. OS se ovládá pomocí stylusu (pero sloužící k ovládání dotykového displeje) a několika hardwarových tlačítek. Tato tlačítka jsou programovatelná a lze jim navolit různé funkce, spouštění aplikací apod. Stylus nahrazuje u kapesního počítače myš. Při delším přidržení stylusu na obrazovce se zobrazí nabídka jako po kliknutí pravého tlačítka myši. Klávesnice je u Windows Mobile softwarová a ovládá se také pomocí stylusu. Základním procesem, který u Windows Mobile neustále běží, je Today Screen (obrazovka Dnes). Funguje jako pracovní plocha. Její pozadí se dá nastavit podle vlastního výběru. Na Today Screen se

zobrazují jednotlivé položky, které lze rovněž nastavovat podle vlastních potřeb. Těmito položkami jsou došla pošta, události z kalendáře, datum, svátky a spousta dalších položek. Na obrazovce je také horní lišta, na které se nachází tlačítko start. Po kliknutí na start se rozbalí menu. V první části jsou zástupci jednotlivých programů, je zde však pro ně omezený počet míst. Jednotlivé zástupce v menu si může uživatel sám nadefinovat. Další částí menu jsou naposledy spuštěné aplikace a poslední jsou napevno nadefinované zástupci položek: programy, nastavení a nápověda. Na horní liště se ještě nachází systémový čas, nastavení hlasitosti a indikátor připojení k síti nebo dalším zařízením. Na spodní liště je tlačítko "Nový", které umožňuje vytvoření nových dokumentů různých aplikací. Dále spodní lišta obsahuje ovládací prvky bezdrátových připojení a klávesnice.



obrázek č. 2 – Obrazovka Dnes [1]

3.3.1 Synchronizace s PC

Windows Mobile je možné synchronizovat se stolním PC. Nejčastěji používaným programem je ActiveSync. Tento software je standardně dodávaný k OS WM. Zařízení PDA s OS WM je možné připojit ke stolnímu PC pomocí USB přes synchronizační kolébku nebo synchronizační kabel. Další způsob je bezdrátové připojení přes Bluetooth, popřípadě infračervený port. Dříve byla možná synchronizace přes wi-fi, která v pozdějších verzích již není k dispozici. Synchronizační software převádí formáty souborů mezi stolními Windows a Windows Mobile. Jeho prostřednictvím jsou instalovány ze stolního počítače aplikace do mobilního zařízení a samozřejmě je i možnost jejich odinstalování. Lze synchronizovat a zálohovat elektronickou poštu, záznamy v kalendáři, jednotlivé kontakty a oblíbené položky z mobilního internet exploreru. ActiveSync obsahuje průzkumníka, pomocí něhož lze pracovat se soubory v kapesním počítači skrze stolní PC. Je možné přímo převádět databázové tabulky z MS Access, provádět synchronizaci PDA s PC přes internet pomocí Microsoft Exchange Server 2003. Díky MS Exchange Server není nutná fyzická přítomnost u stolního PC. Synchronizace je nastavitelná buď automaticky nebo ručně. Pomocí ActiveSync se zálohují data a systémové nastavení Windows Mobile do stolního PC. V případě poruchy hardware kapesního počítače nebo softwarové závady není problém zálohu načíst a obnovit tak ztracená data a nastavení.

3.3.2 Zálohování dat

Zálohování dat a nastavení OS je velmi podstatná záležitost. V případě ztráty dat a nastavení OS nebo HW restartu PDA mohou být všechna data na zařízení ztracena. Díky souboru se zálohou systému nemusí být tato ztráta nezbytně nevratná. Zálohování se provádí přímo v mobilním zařízení pomocí Backup manageru. Soubor se zálohovanými daty je možné uložit do paměti vlastního zařízení nebo na paměťovou kartu. Zálohovat se dá obsah dokumentů, elektronická pošta, osobní databáze a systémové údaje. Soubor s datovou zálohou se dá vytvořit také prostřednictvím aplikace ActiveSync. Záloha je pak uložena na disku stolního PC. Další možnost, jak

vytvořit zálohu, je přes Wi-Fi síť prostřednictvím synchronizačního SW. V případě poškození nebo ztráty dat je zálohový soubor načten.

3.3.3 Zabezpečení

Požadavky na úroveň zabezpečení dat na mobilních zařízeních jsou různé. Základním aspektem je definovat, jaká nebezpečí hrozí a jak důležitá data jsou v PDA. Jinou úroveň zabezpečení dat bude požadovat uživatel, který používá PDA k soukromým účelům a jinou firma, jejíž zaměstnanci využívají mobilní zařízení při výkonu práce. Základní bezpečnostní opatření je zaheslování přístupu do mobilního operačního systému a tím i k datům uloženým v paměti zařízení. Různá může být bezpečnostní úroveň hesla. Nízkou úroveň se rozumí například heslo, které má pouze 4-6 znaků a není vyžadována žádná kombinace písmen a číslic. Větší zabezpečení poskytuje heslo, které čítá více znaků a vyžaduje kombinaci číslic a písmen. Dalším opatřením, které minimalizuje možnost prolomení hesla do OS, je zadání maximálního možného počtu pokusů pro zadání hesla. Tato opatření brání cizí osobě manipulovat s daty v případě odcizení nebo ztráty kapesního počítače. PDA mají celou řadu bezdrátových komunikačních rozhraní, kterými se připojují do různých sítí. Neoprávněnému přístupu do mobilního zařízení skrze takovou síť může zabránit nainstalovaný firewall. V případě, že kapesní počítač disponuje slotem pro paměťové karty, jsou zneužitelná i data uložená na paměťové kartě. Nejlepším způsobem, jak je zabezpečit, je zašifrování těchto dat. Jejich rozšifrování je možné pouze na kapesním počítači a OS, který je zašifroval. Popřípadě je možné proces rozšifrování zabezpečit ještě heslem. Pokud je kapesní počítač využíván zaměstnancem nějaké firmy pro přístup do firemní sítě, hrozí nebezpečí úniku dat při zcizení kapesního počítače a to nejen dat uložených v paměti zařízení, ale z celé podnikové sítě. Firma musí počítat, že v případě nahlášeného zcizení mobilního zařízení by administrátor sítě měl mít možnost zakázat přístup do firemních síťových aplikací uživatelským profilům, které jsou ve zcizeném mobilním zařízení nastaveny, popřípadě zakázat přístup do celé podnikové sítě z tohoto mobilního zařízení. Další možností zabezpečení v situaci, kdy mobilní zařízení je po odcizení nebo ztrátě stále připojeno do sítě je dát příkaz na dálku smazat veškerá data na

mobilním zařízením. Důležité je, aby data byla zálohovaná. Pokud by bylo zařízení opětovně nalezeno, lze jeho systémové nastavení a veškerá data opět obnovit.

3.3.4 Síťové aplikace na platformě WM

Využití WM je možné jak v malé, tak i velké soukromé firmě, neziskovém sektoru a ve státních organizacích. Praktické nasazení WM je ovlivněno několika aspekty. Použitým typem PDA – tj. jaké technické možnosti nasazení umožňuje použitý hardware a jaký další konkrétní software daná firma pro své potřeby využívá. Obecné možnosti aplikace WM pro firmy jsou v několika oblastech: vztah firmy k zákazníkům, správa dokumentů a informací, sdílení dat a aplikace pro pracovní týmy, mobilní sběr dat, logistika a další. Zavádění mobilních technologií ve firmách podporují hlediska jako minimalizace nákladů na administrativu, zrychlení a zkvalitnění chodu firmy a díky zavedení těchto technologií může firma získat a posílit své „know how“ na trhu oproti konkurenci.

3.3.5 Správa mobilních zařízení v podniku

Hlavní potřeby jsou synchronizace dat pro všechny uživatele v podnikové mobilní síti s hlavní firemní sítí. Musí se synchronizovat složitější data, i jednoduché firemní informace a dále systém zpracování těchto dat. Klíčové je samozřejmě i zabezpečení firemní mobilní sítě, jak zabezpečení dat uložených v jednotlivých PDA uživatelů, tak zabezpečení komunikace mobilních zařízení s centrálním serverem. Posledním aspektem je správa zařízení a softwaru.

3.3.6 Synchronizace

Existují dvě možnosti, jak může uživatel synchronizovat data ve svém PDA: V místě pracoviště (tato možnost je finančně výhodnější) nebo synchronizovat data s firemním serverem online pomocí GSM sítě nebo Wi-Fi sítě (pokud je na místě dostupná). První možnost (synchronizace v místě pracoviště) je velmi jednoduchá. Pomocí ActiveSync se PDA synchronizuje se stolním PC. Data a soubory jsou synchronizovány s centrální podnikovou databází. Např. se může jednat o Microsoft SQL Server, webový obsah, došlá emailová pošta nebo jakákoliv další aplikace, kterou

firma používá. Druhou možností je vzdálená synchronizace. V tom případě je nutné zajistit připojení PDA k firemní síti, nejčastěji prostřednictvím sítě GSM, dále také pomocí modemu, Wi-Fi nebo jakéhokoliv jiného připojení. PDA s WM umožňuje k firemnímu serveru telefonické připojení s podporou RAS (Remote Access Service) nebo je možné využít připojení k internetu pomocí protokolu PPP (Point-to-Point Protocol). Zařízení PDA s WM také umožňují použití webových aplikací pro připojení k serverům pomocí sady protokolů TCP/IP, protokolů HTTP a FTP. Webový obsah z firemního serveru lze zpřístupnit např. pomocí klienta AvantGo. Obsah lze prohlížet, i když není PDA připojeno k serveru. Další možností je služba RDA (Remote Data Access), která umožňuje aplikacím vzdálený přístup k datům uloženým ve firemním SQL serveru. Ve výčtu možností pro vzdálenou synchronizaci následují Internetové aplikace na bázi práv. Aplikace na PDA naváže spojení pomocí protokolu HTTP s SQL serverem, který je za firewallem. Může použít služby jako ověřování, autorizace a šifrování. Programem s těmito možnostmi je např. SQL Server 2000 Windows CE Edition.

3.3.7 Zabezpečení

Zabezpečení mobilních zařízení firmy mají dvě hlediska. Přístup k datům a zabezpečení dat uložených v PDA. Druhým hlediskem je přenášení dat mezi PDA a podnikovou sítí. Možnosti zabezpečení PDA a firemní sítě byly již uvedeny v kapitole č. 3.3.3 s názvem Zabezpečení.

3.3.8 Správa zařízení

Na trhu existuje velké množství Software pro správu uživatelů, kteří využívají zařízení PDA v podnikové síti. O zařízeních v síti je dobré mít neustálé informace. Je třeba sledovat aktuální konfiguraci zařízení, data registru, instalované aplikace, dostupnou paměť, verze OS apod. Tyto informace pomáhají správci sítě předcházet možným síťovým selháním a rychlejšímu obnovení zálohy. Centrální správu podnikových mobilních zařízení umožňují aplikace Unicenter, Afaria a Mobile Device Manager. Zmíněné programy obsahují také možnosti centrální správy a aktualizace

software. Inovace a aktualizace software se tím velmi zjednodušuje. Zařízení v síti se dá rozdělit do několika skupin, třeba podle typu procesoru PDA. Do každé skupiny je následně možné nainstalovat správnou verzi aplikace pro daný typ procesoru. Podle stejné zásady lze rozdělit i skupiny uživatelů do různých profilů a pro každý profil instalovat centrálně potřebné aplikace. Co se týká zálohování, lze určit, jaká data a kdy mají být zálohována. V případě poruchy mohou být pak velmi rychle obnovena. V případě fyzického zničení PDA není problém vytvořit ze zálohy identickou kopii tohoto zařízení. Obnovení zálohy na dálku se provádí např. pomocí aplikace ScoutIT. ScoutIT se nainstaluje do paměti ROM, pokud je proveden úplný reset PDA. V tom případě se dají veškerá data obnovit automaticky na dálku.

3.3.9 Využití WM při obchodní činnosti

Obecně lze říci, že mobilní technologie mají potenciální uplatnění ve velkém množství firem. Potenciál mobilních technologií mohou využít jak malé, tak i velké a střední firmy. Pro malé firmy, které nemají žádné IT oddělení a zaměstnávají pouze malý počet zaměstnanců, spočívá hlavní těžiště využití mobilních technologií v oblasti mobilní kanceláře. Zaměstnanci budou využívat PDA pro kontakt se svou kanceláří. Získají stálý přehled o svých schůzkách, pracovních povinnostech apod. Aplikovat mobilní řešení v malé firmě není nijak obtížné technicky ani časově.

Aplikace mobilního řešení pro velké a střední firmy je ovšem již technicky náročnější. Zde se již jedná o správu systému, ve kterém mohou být desítky až stovky mobilních zařízení. Firma musí mít pro správu systému vlastní IT oddělení. Důležité je funkční zaměření mobilního systému podle předmětu činnosti dané firmy a způsob realizace a vývoje celého systému. Je rozlišováno několik základních směrů aplikace mobilních řešení pro firmy podle jejich obchodní činnosti: Aplikace pro mobilní sběr dat, CRM systémy pro podporu obchodních zástupců, aplikace Go&Sell, dále např. objednávkové systémy apod. Při realizaci mobilního řešení záleží na tom, jestli je na trhu již dostupná vhodná aplikace pro daný typ obchodní činnosti firmy. V opačném případě je nutný vývoj dané aplikace, což vede ke zvýšeným nákladům.

3.3.10 Produkty pro WM

Velmi používanou aplikací pro vzdálený přístup k datům na serveru je Microsoft Exchange Server. Součástí Exchange Serveru je Exchange ActiveSync. Exchange ActiveSync je určen pro přenos informací mezi Exchange Serverem a PDA. Pracuje na základech protokolu HTTP a jazyka XML. Exchange ActiveSync slouží k synchronizaci e-mailových zpráv, kontaktů, úkolů, přístup ke sdíleným složkám atd.

Vývojem software pro PDA zařízení se na českém trhu zabývá zejména společnost Sunnysoft. Nabízí celou řadu aplikací, které mohou uplatnit firmy při své podnikatelské činnosti. Aplikace Sunnysoft mAgent slouží pro mobilní sběr dat a řízení pracovníků v terénu. Z hlediska hardware je nejefektivnější, pokud je PDA vybaveno GSM modulem. Veškerá data jsou tak přenášena mezi PDA a celou podnikovou sítí v reálném čase. Tento software v podstatě urychluje logistiku a případnou expedici zboží zákazníkům. Informace o cenách a produktech lze centrálně upravovat a použít i možnosti mobilního tisku na místě přímo u zákazníka, např. pomocí bezdrátové tiskárny vytisknout fakturu. Produkt mAgent se skládá ze dvou částí: Sunnysoft mServer a Sunnysoft mAgent „Go&Sell“. Sunnysoft mServer je aplikace, která zajišťuje výměnu dat mezi databází podniku a PDA. Sunnysoft mAgent „Go&Sell“ je aplikace pro PDA, která může být používána i offline. Získaná data jsou předávána mServeru. Pro spojení s mServerem může využít mAgent jak síť GSM (GPRS přenos dat), Wi-Fi nebo jiné internetové spojení.

Pro průzkumy veřejného mínění je kvalitní aplikací Sunnysoft mResearch, což je aplikace určená pro agentury zabývající se sociologickým výzkumem a průzkumy veřejného mínění. Umožňuje vytváření dotazníků, ty se pak mohou automaticky nahrát do PDA jednotlivým tazatelům. Získaná data lze okamžitě předávat dál ke zpracování a vyhodnocení celého průzkumu. Data je možné exportovat v XML (eXtensible Markup Language – XML dokument je vlastně normální textový editor doplněný o tagy) nebo CSV (Comma-separated values – je formát určený pro přenos tabulkových dat).

Na trhu je celá řada dalších software pro PDA zařízení určená pro nejrůznější účely. Sunnysoft mService je aplikace pro kontrolu servisních techniků. Vedení firmy může díky ní získat přehled o výkonech svých pracovníků, předávat pokyny zaměstnancům, sledovat, jaký materiál a v jakém množství byl při práci použit. Sunnysoft mStock je zase aplikace pro vedení skladové evidence. Usnadňuje inventury, příjem a výdej zboží. Tyto informace je možné následně synchronizovat s evidencí vedenou na stolním PC. Na PDA s WM je možné nainstalovat takřka libovolnou aplikaci. Pokud firma vybaví své pracovníky mobilními zařízeními, obsahujícími tyto aplikace, může se řadě firem urychlit celý organizační proces řízení pracovníků a zároveň logistické procesy související s nákupem a prodejem zboží. Vybavení zaměstnanců PDA je zároveň levnější než pokud by podnik pro správu všech svých činností používal např. Nootbooky.

Nejčastější je komerční využití WM v soukromém sektoru. Velký potenciál mají mobilní technologie také ve státním a neziskovém sektoru. Praktické je nasazení u bezpečnostních složek. V různých modifikacích se používají už i v lékařství. [1]

Kapitola byla zpracována podle bakalářské práce autora, ve které je toto téma více rozvedeno.

4 Microsoft System Center Mobile Device Manager

Microsoft System Center Mobile Device Manager umožňuje centrální správu mobilních zařízení s operačním systémem Windows Mobile 6.1 a vyšší verze od společnosti Microsoft. Jedná se o úplné řešení pro správu mobilních zařízení v podniku, umožňuje vzdálenou instalaci softwaru a přehled o jednotlivých zařízeních.

Mobile Device Manager 2008 SP1 umožňuje v podniku umístit více instancí Mobile Device Manageru uvnitř stejné stromové struktury Active Directory. Poskytuje možnost správy a zapsání (resp. zaregistrování nového) zařízení pomocí OTA (Over-The-Air) v podnikové síti.

Mobile Device Manager také zlepšuje viditelnost mobilních zařízení v podnikové síti pomocí rich inventory a nástroje zpráv založeném na Microsoft SQL Server 2005, správa mobilních zařízení je založena na role-based administraci, MMC snap-in a MS Windows PowerShell příkazech. Nový software lze mobilním zařízením jednoduše distribuovat pomocí OTA software distribuce (bezdrátově) založené na Windows Software Update Services (WSUS) 3.0 SP1. Mobile Device Manager 2008 SP1 je kompatibilní s Open Mobile Device Management (OMA DM).

V rámci zabezpečení nabízí Mobile Device Manager robustní bezpečnostní platformu kompatibilní s Active Directory. Je zde předdefinováno více než 125 pravidel zabezpečení, včetně funkcí pro vypnutí periférií mobilních zařízení, přerušení komunikace apod. Je možné konkrétní nastavení zabezpečení dle firemních pravidel.

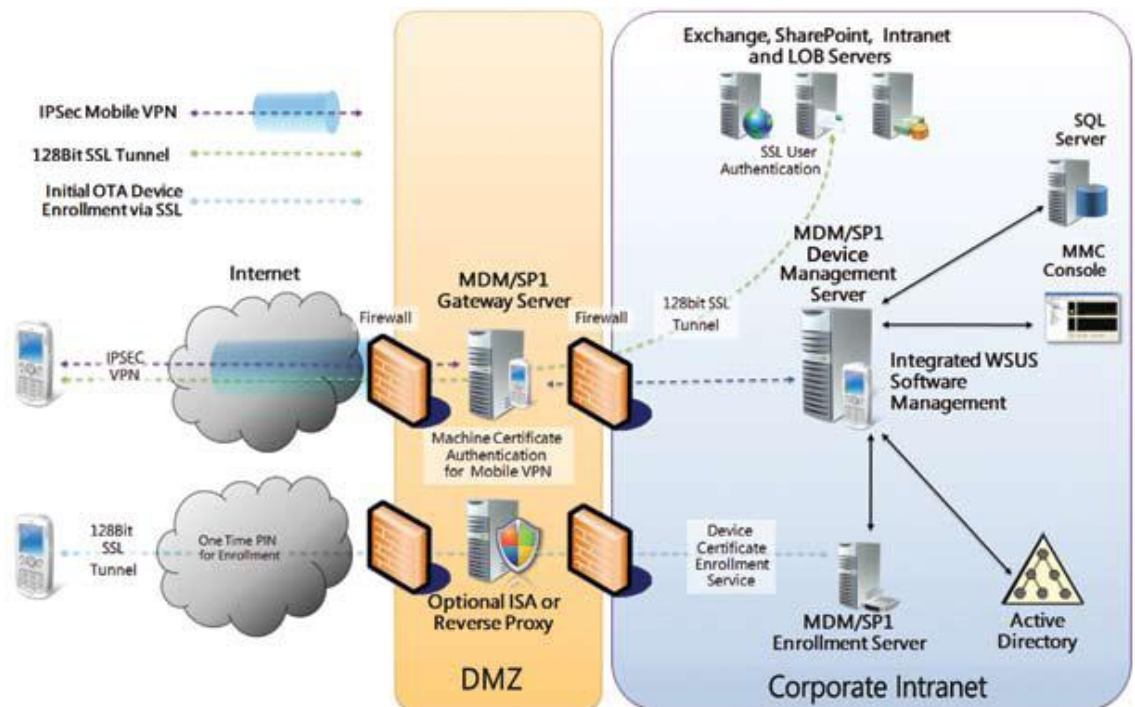
Mobilní VPN (Virtual Private Network) umožňuje zaměstnanci firmy pracovat s mobilním zařízením za podnikovým firewallem s firemními daty. Mobilní VPN je Mobile Device Managerem podporováno, včetně funkcí, jako je autentizace připojeného zařízení apod.

4.1 Architektura aplikace

Mobile Device Manager se skládá z následujících komponent:

- Gateway server
- Device management server
- Enrollment server
- Microsoft SQL Server 2005 database

Následující obrázek reprezentuje doporučenou topologii Mobile Device Manageru s mobilními zařízeními s operačním systémem Windows Mobile v podniku.



obrázek č. 3 – architektura Mobile Device Manageru 2008 SP1 [8]

4.1.1 Gateway Server

Je zpravidla umístěn na okraji sítě nebo v DMZ (tzv. demilitarizované zóně), a umožňuje přístup mobilním zařízením z vnějšku do vnitřní podnikové sítě a naopak komunikaci z vnitřní podnikové sítě s mobilním zařízením umístěným mimo vnitřní podnikovou síť. Gateway Server poskytuje end point (koncové) spojení pro:

- Ověření přichozího spojení od autorizovaného zařízení.
- Přidělení stabilní IP adresy mobilnímu zařízení (to umožňuje použití technologie Direct Push pro update softwaru zařízení a podporuje trvalost aplikací).
- Dovoluje rychlé pokračování nebo znovu připojení pro aplikace a zařízení.
- Zprostředkovává klíče pro zakódování spojení přes internet.

4.1.2 Device Management (DM) Server

Je primárním serverem pro správu a administraci mobilních zařízení zapsaných v systému Mobile Device Manager. Device Management Server je hub pro softwarové balíčky pro mobilní zařízení, skupinové nastavení mobilních zařízení a datových přenosů přes OMA DM. Tento server komunikuje s existujícími servery a další IT infrastrukturou v podniku a zprostředkovává příkazy mezi Mobile Device Managerem a mobilními zařízeními.

4.1.3 Enrollment (zapisovací) Server

Server řídí proces žádosti a vydání bezpečnostního certifikátu pro mobilní zařízení a vytvoření objektu Active Directory doménové služby, který reprezentuje zařízení v systému. Použití těchto objektů umožňuje spravovat mobilní zařízení jako člena domény. Tento proces využívá jednorázové heslo pro potvrzení zapsání mobilního zařízení do systému. Tato role dovoluje uživatelům zapsat jejich zařízení do systému bez nutnosti připojení zařízení k PC nebo fyzickému přístupu do podnikové sítě. Enrollment Server pomáhá vzájemnému ověření certifikátů a komunikace mezi mobilním zařízením a serverem, používá Active Directory k uchovávání identit.

4.1.4 Databáze

Služby na Device Management Serveru a Enrollment Serveru využívají databáze pro správu, konfiguraci, úkoly a informace o stavech mobilních zařízení. SQL server databáze jsou klíčové pro konfiguraci a update klientských zařízení.

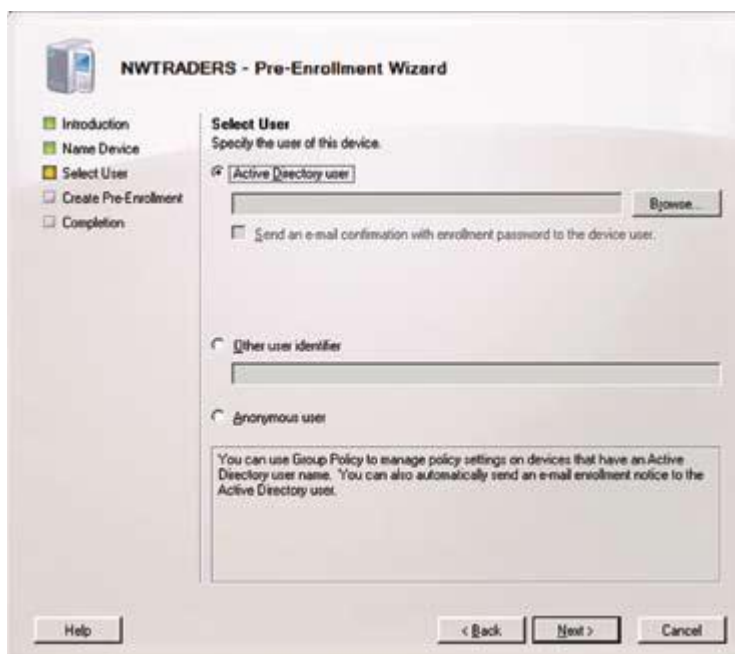
4.1.5 Active Directory

Je adresářová struktura používaná v systémech založených na MS Windows k uchovávání záznamů o sítích a doménách. Je založena na běžných internetových protokolech, jednoznačně definuje strukturu sítě a organizuje počítače a domény.

4.1.6 OTA (Over-The-Air) řízení a zavádění

Mobile Device Manager je uzpůsoben pro jednoduché zapsání zařízení v management serveru pomocí bezdrátového připojení. Uživatel poskytne e-mailovou

adresu, která je zadána do uživatelova mobilního zařízení. E-mailová adresa je použita pro nalezení Mobile Device Manager serveru pro připojení. Uživatel zadá PIN (ten musí být poskytnut uživateli zvlášť administrátorem systému nebo přes Self-Service Portal) k ověření zapsání. Po ověření a zapsání se zařízení může připojit ke Gateway Serveru pomocí IPSec – zašifrovaný kanál, se zapouzdřeným SSL k ochraně dat. Při prvním připojení Mobile Device Manager server může pomocí „push“ funkce aplikovat pro zařízení bezpečnostní nastavení a nainstalovat standardní software přímo do zařízení bez interakce s uživatelem zařízení.



obrázek č. 4 – Pre-Enrollment wizard [8]

4.1.7 OTA SW distribuce založená na WSUS 3.0

Mobile Device Manager používá WSUS (Windows Software Update Service) pro distribuci aplikací spravovaným mobilním zařízením. Mobile Device Manager spolu s WSUS kontroluje, zda nejsou vydány softwarové balíčky podle OMA DM synchronizačního plánu. Device Management Server určí, které balíčky mají být aplikovány na konkrétní zařízení a vytvoří OMA DM příkazy v databázi. Když bude mobilní zařízení synchronizováno, stáhne se a nainstaluje nabízený softwarový balíček.

4.1.8 Informace o klientských zařízeních

Mobile device Manager používá pro získávání informací o mobilních zařízeních systém založený na SQL Serveru 2005. Když je zařízení ověřeno Device Management Serverem, jsou posbírány důležité informace o zařízení. Jsou dostupné informace např. o:

- verzi operačního systému
- modelu mobilního zařízení a jazykovém nastavení
- informace o hardwaru zařízení a informace o uložených datech
- uživatelském nastavení

4.1.9 Role-based administrace

Poskytuje flexibilní správu mobilních zařízení v systému. Jako příklad lze uvést, že helpdesk administrátor může mít přidělený přístup k určitým skupinám funkcí v systému. IT administrátor může definovat rozdílné role pro specifické potřeby daných uživatelů. Tyto funkce vedou ke zjednodušení správy mobilních zařízení a určují bezpečnostní práva pro různé role.

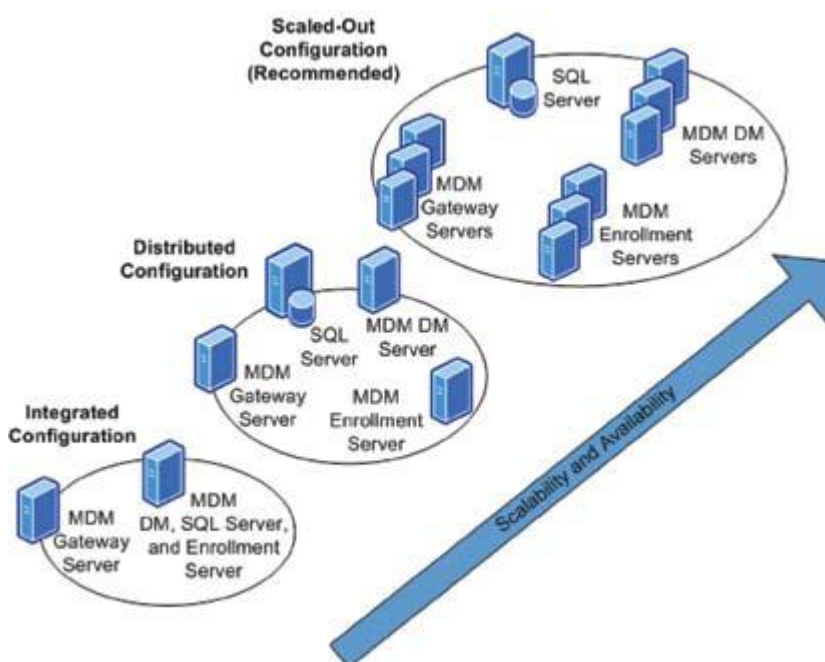
4.1.10 Self-Service Portal (SSP)

Je svým způsobem „helpdesk“ přímo v mobilním zařízení. Snižuje závislost uživatele na administrátorovi systému. SSP lze nastavit pro potřeby konkrétního podniku. SSP umožňuje uživateli následující:

- zobrazit seznam jeho mobilních zařízení pro lepší přehled a sledování
- vytvoření nového zapisovacího záznamu pro zapsání nového mobilního zařízení do systému
- reset uživatelova PIN kódu

4.1.11 Škálovatelná architektura

Mobile Device Manager má vysokou úroveň škálovatelnosti. Jeho architektura dovoluje flexibilní možnosti implementace na podnikových serverech. Konfigurace serverů záleží na dostupnosti zdrojů v organizaci (technického zabezpečení IT) a škálovatelnosti organizace.



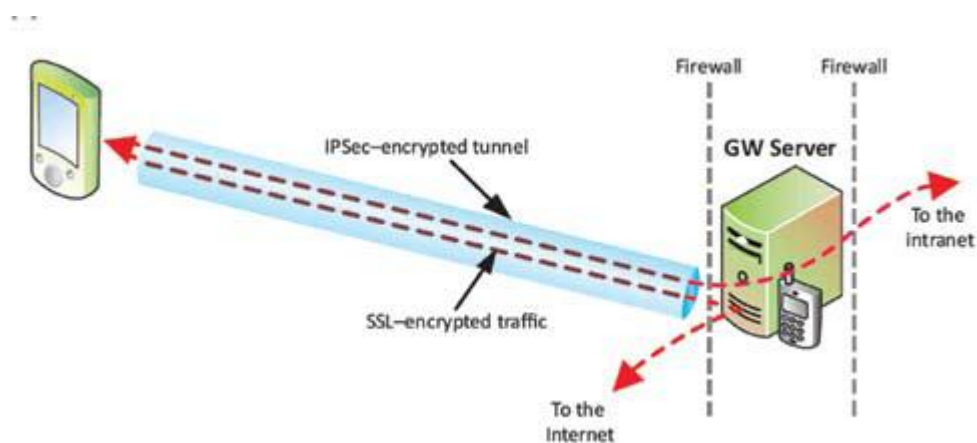
obrázek č. 5 – Konfigurace serverů [8]

- **Integrated Configuration** – komponenty systému jsou instalovány na dvou fyzických serverech s jedním doménovým serverem v intranetu a jedním serverem pro přístup do vnitřní sítě z venku. Tato varianta implementace neposkytuje nejlepší možnosti zabezpečení a nedovoluje spravovat větší množství mobilních zařízení.
- **Distributed Configuration** – každá komponenta Mobile Device Manageru je instalována na samostatném fyzickém serveru. Toto je doporučená možnost implementace. Poskytuje také oproti Integrated Configuration lepší zabezpečení a výkon systému.

- **Scaled – Out Configuration** – jedná se o konfiguraci Gateway Serveru a Management Serveru do více serverových polí. Tato konfigurace poskytne systému maximální výkon.

4.1.12 Mobilní VPN

Mobile Device Manager zvyšuje bezpečnost systému díky „single point“ připojení. Mimo podnikový firewall je pro přístup k podnikovým datům možné použít Mobilní VPN tunel. Mobilní VPN dovoluje uživateli bezpečný přístup k datům v intranetu. Mobilní VPN funguje v případě Mobile Device Manageru na principu IPSec tunelu mezi zařízením a Gateway Serverem. Data přenášená přes VPN připojení nemusí být šifrována pomocí SSL.



obrázek č. 6 – Autentizace mobilního zařízení [8]

4.2 Zabezpečení

Mobile Device Manager pracuje s Active Directory a skupinovým nastavováním práv. Active Directory dovoluje administrátorům nastavit bezpečnostní pravidla v jediném uživatelském prostředí. Mobile Device Manager zabezpečuje firemní data přímo v zařízeních díky šifrování. V případě nahlášení ztráty nebo zcizení klientského zařízení může administrátor v okamžiku, kdy se takové zařízení připojí k bezdrátové síti spustit vzdálené připojení k zařízení a zablokovat ho. V případě, že uživatel nemůže získat přístup do zařízení z důvodu zapomenutí či ztráty PIN čísla, lze ho vzdáleně resetovat.

Administrátoři mají možnost zablokování komunikace z bezpečnostních důvodů, včetně zablokování Bluetooth, SMS/MMS, infračerveného portu, POP/IMAP e-mailů a fotoaparátu. Různá bezpečnostní nastavení mohou být použita pro různé skupiny zařízení v Active Directory nebo pro různé statusy mobilních zařízení. Lze centrálně kontrolovat, jaký software je nainstalován v klientských zařízeních a povolovat či zakazovat jednotlivé funkce aplikací.

Microsoft Certification Authority (CA) dovoluje standardizovaným certifikačním šablonám automatické ověření a obsluhu klientských zařízení Mobile Device Managerem. Konfigurace Microsoft CA pro jediné použití zabrání neautorizovaným certifikátům nesprávně použít CA.

Mobile Device Manager dovoluje využívat pro správu mobilních zařízení s operačním systémem Windows Mobile **Active Directory**. Dříve než se může zařízení připojit pomocí Mobile Device Manageru do podnikové sítě, musí projít procesem ověření, že je skutečně součástí Active Directory domény.

Vynucení bezpečnostních pravidel je možné pomocí Active Directory. Active Directory je využíváno pro uložení certifikátů pro VPN a připojení založených na 802.1x a nastavení skupinových oprávnění pro mobilní zařízení. Mezi tato nastavení patří např. konfigurace nastavení ActiveSync nebo vyžadování zadání hesla při

přihlášení. Active Directory Management (ADM) šablony mohou být použity pro vytvoření dalších bezpečnostních pravidel a nastavení než jsou ta předdefinovaná.

Šifrování dat. Windows Mobile dovoluje šifrovat dokumenty uložené na externí paměťové kartě a Mobile Device Manager rozšiřuje tyto funkce o šifrování složek a souborů přímo v mobilním zařízení. Jedná se o šifrování PIM (personal information management) informací, složek s e-mail zprávami, cache složek Internet Exploreru, doménového hesla apod. Šifrování dat využívá stejný PIN kód jaký je pro přístup do celého zařízení při jeho startu a AES-128 šifrování. Šifrování dat v zařízení může administrátor celé zapnout nebo vypnout.

Mobile Device Manager dovoluje **blokovat aplikace** v mobilních zařízeních. Mobile Device Manager umožňuje nastavení seznamu aplikací, které mohou být nainstalovány nebo spouštěny na zařízeních v síti.

Remote wipe (automatické řízení) dovoluje okamžité získání dat z mobilního zařízení. Toto je možné díky tomu, že Mobile Device Manager pracuje na principu „always on“ připojení, tzn., že kdykoliv se zařízení bezdrátově připojí k internetu, je zařízení poslána zpráva skrze UDP, že má začít OMA DM synchronizace. Jakmile je zařízení synchronizováno, je proveden reset zařízení. Synchronizace zabezpečuje, že se zařízení nepřipojí k databázi se zastaralou konfigurací.

Device Management Server využívá **OMA DM spojení** k předávání úkolů a akcí klientskému zařízení s Windows Mobile. Device Management Server převádí úkoly do OMA DM příkazů, které jsou následně posílány. OMA DM není využíváno jen pro posílání zpráv, ale také pro počáteční konfiguraci s Mobile Device Manager serverem.

4.3 Možnosti použití

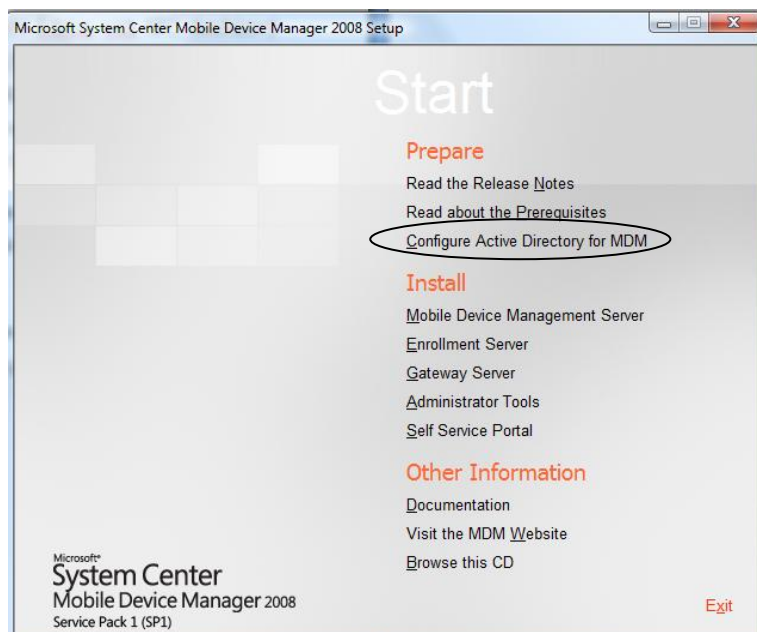
V rámci řešení diplomové práce byla testována aplikace Microsoft Device Mobile Manager 2008 SP1. Na webu společnosti Microsoft <http://www.windowsmobile.com/systemcenter/> lze stáhnout po zaregistrování testovací verzi software s licenci na 120 dní nebo lze aplikaci vyzkoušet pomocí interaktivní demoverze, která je dostupná taktéž na webu spol. Microsoft.

V instalačním CD se nacházejí následující komponenty systému: Mobile Device Management Server, Enrollment Server, Gateway Server, Administrator Tools, Self Service Portal. Hardwarové nároky systému jsou následující: x64 – bit procesor (nejlépe alespoň dvoujádrový), 4 GB paměti RAM, 100 GB volného prostoru na pevném disku a síťová karta nejlépe 100 Mb/s.

Po softwarové stránce vyžadují jednotlivé komponenty systému minimálně operační systém Windows Server 2003 Standard x64 Edition with SP2, databázový server Microsoft SQL Server 2005 Standard Edition Service Pack 2 nebo pozdější verze a .NET Framework 2.0 SP1 a pozdější verze. Jednotlivé komponenty systému musí být také součástí domény Active Directory. Některé administrační prvky systému dále potřebují Windows PowerShell 1.0 a WSUS 3.0 SP1 Console.

V případě použití instalačního CD je postup instalace následující:

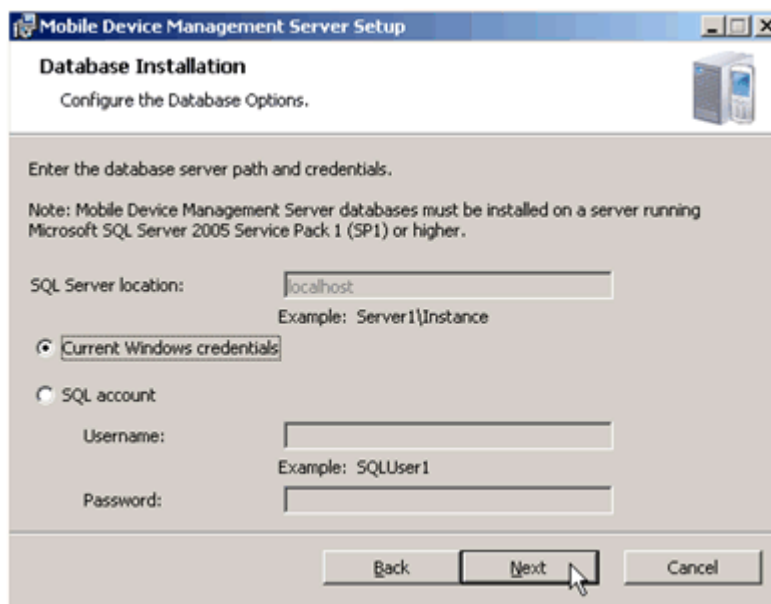
V prvním kroku instalace systému je nutné konfigurovat Active Directory pro Mobile Device Manager. Toto lze provést automaticky pomocí aplikace, která je přímo v instalačním CD systému.



obrázek č. 7 – Instalační CD MDM 2008 SP1 [printscreens autora]

Dalším krokem je instalace Enrollment Serveru, při které je nutné v krocích nastavit umístění Enrollment Serveru, port serveru, Device a Server Certification Authority.

Poté lze nainstalovat Management Server. Při jeho instalaci je nastaveno umístění MS SQL Serveru a přístupová práva k databázi.



obrázek č. 8 – Instalace databáze [printscreens autora]

Komponentou systému k administraci je Administrative Tool. Jeho součástí je také MDM Console a Software Distribution Console. Nezbytnou součástí systému je Gateway Server. Při jeho instalaci je nutné zadat IP adresu a port serveru, cestu ke konfiguračnímu souboru a certifikátům. Poslední komponentou systému je Self Service Portal.

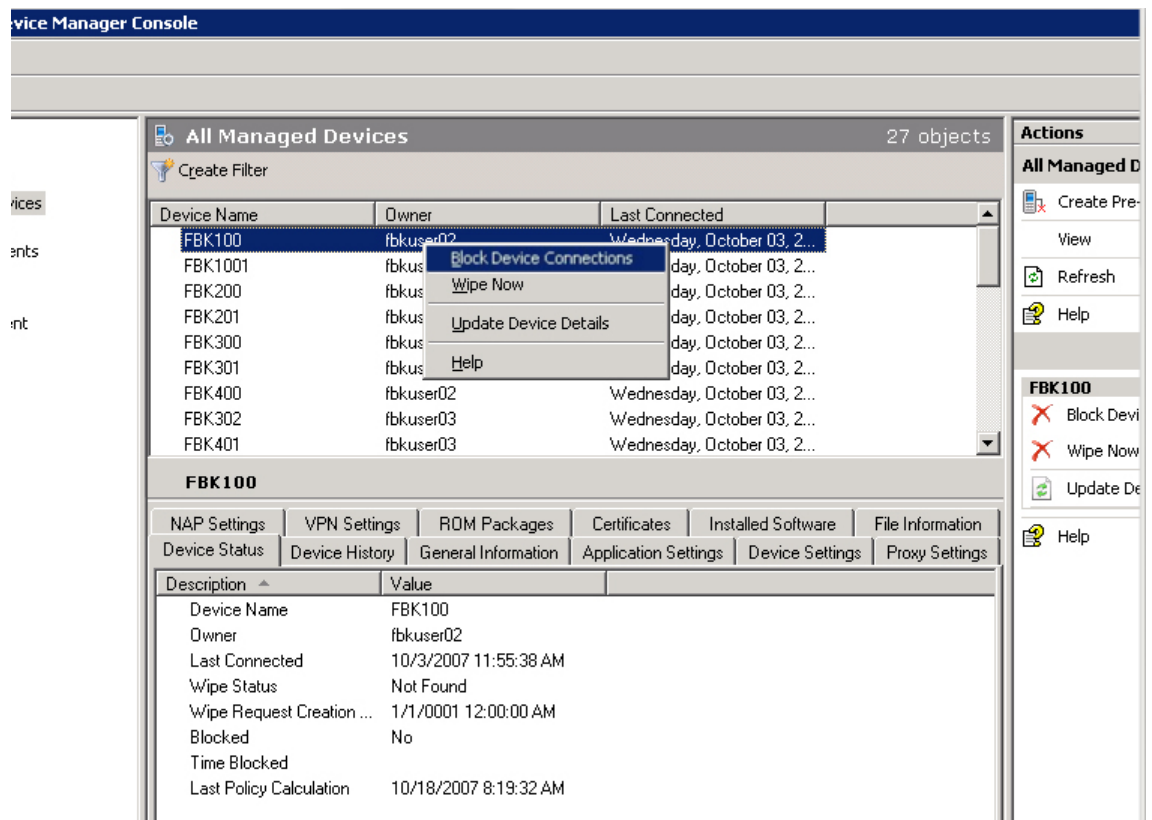
Z důvodu nedostatečných HW prostředků, které má autor k dispozici a zejména SW licencí nebyla aplikace testována za použití testovací verze, která je ke stažení na CD, ale pomocí interaktivní demoverze, která je založena na simulování jednotlivých funkcí aplikace. Demoverze je založena na principu interaktivní stránek v technologii Flash.

Testování pomocí interaktivní demoverze:

Ovládání jednotlivých funkcí probíhá přes Device Manager Consoly. Následující funkce pro správu zařízení byly autorem otestovány v interaktivní demoverzi aplikace. Blokování připojení jednotlivých mobilních zařízení, „Wipe“ zařízení, zapsání nového

zařízení pomocí Self Service portálu, vytvoření softwarového distribučního balíčku apod.

V oblasti zabezpečení byly vyzkoušeny funkce týkající se zablokování periférií zařízení, zablokování určitých aplikací, šifrování dat v zařízeních a bezpečnostní nastavení distribuce nových softwarových balíčků. Také byly otestovány funkce LOB (Line-Of-Business) aplikací přímo ve virtuálním mobilním zařízení.



obrázek č. 9 – Zablokování připojení zařízení [printscreens autora]

Interaktivní demoverze poskytuje základní možnosti pro vyzkoušení ovládání aplikace z hlediska administrace systému v Device Management Console a z hlediska uživatele pomocí simulátoru klientského mobilního zařízení.

V rámci zhodnocení systému lze říci, že Mobile Device Manager je systém, který poskytuje komplexní správu mobilních zařízení s operačním systémem Windows Mobile. Hlavní výhodou je možnost integrace systému do stávající firemní IT infrastruktury, pokud je založena na Microsoft technologiích. Nevýhodou jsou jeho HW nároky zejména pouze podpora 64bit architektury. Další nevýhodou je podpora jen určitých typů mobilních zařízení, které navíc musí obsahovat operační systém Windows Mobile.

5 Afaria – management mobilních zařízení

Afaria poskytuje možnosti pro management a správu notebooků, desktop PC a handheld zařízení. Afaria je nástroj pro automatizování business procesů, produktivitu firmy, bezpečnost zařízení a dat.

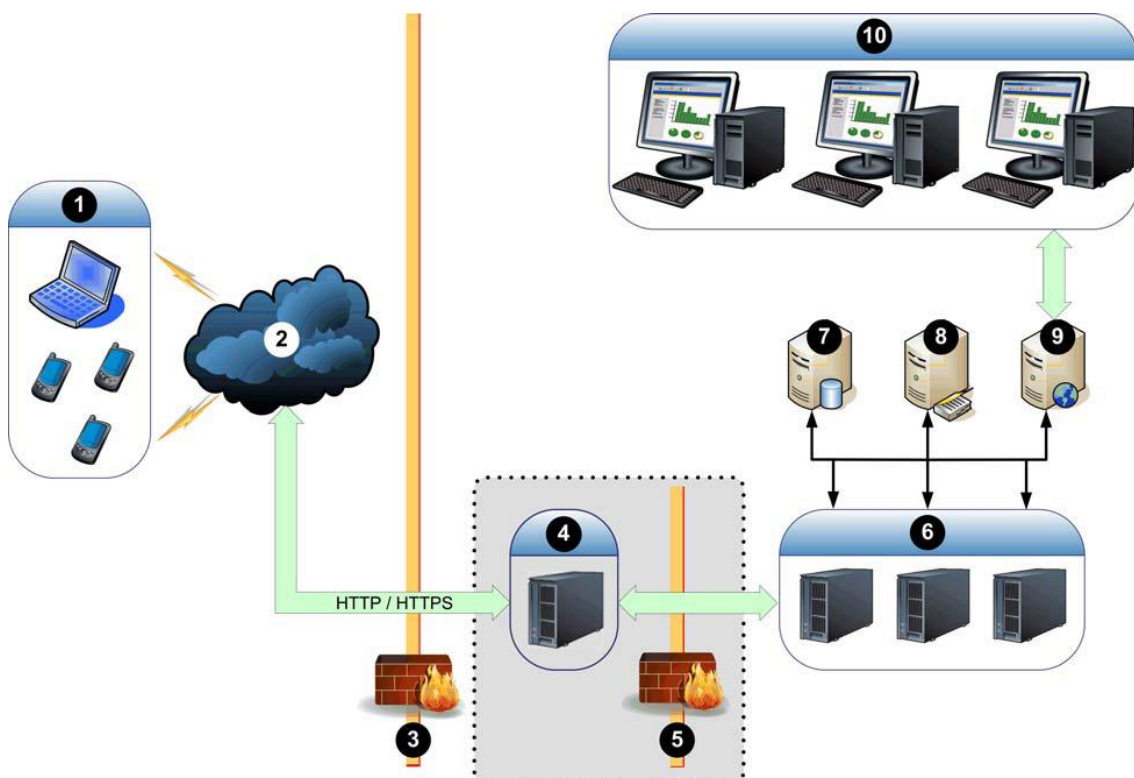
Afaria poskytuje efektivní bezdrátovou podporu pro:

- „Push“ schopnost – pro distribuci různého obsahu a úkolů do klientských zařízení a „Pull“ schopnost – pro vyžádání specifického obsahu ze serveru klientem.
- Dynamický přenosový rozsah – díky němuž je možnost využít efektivně celkovou přenosovou kapacitu jednotlivými klienty.
- „Byte-level differencing“ - detekování rozdílů mezi dvěma verzemi souborů nebo softwarových balíčků a poté rozesílání pouze „byte level“ změn (tj. pouze změněných částí souborů nebo balíčků) klientům, což zmenšuje požadavky na objem přenesených dat a přenosový rozsah.
- Segmentování souborů a doručování balíčků – je způsob členění souborů a balíčků do menších distribučních paketů, které dovoluje přenášení větších bloků dat přes několik připojení.
- „Check point restart“ – dovoluje při přerušení komunikace mezi klientem a serverem při příštím připojení klienta k serveru vyhnout se přenášení redundantních dat.
- Offline instalace – po přenesení dat, resp. programů jsou aplikace nainstalovány v offline režimu, zkracuje se tak doba nutná pro připojení k serveru.

- Komprese dat – umožňuje rychlejší přenosy dat a snižuje nároky na přenosový rozsah v síti.
- „Outbound notification“ (odchozí zprávy) umožňují informovat klienty nebo klientské skupiny o potřebě připojení k serveru a stažení aktualizací apod. V klientu je instalovaný tzv. „listener“, který vyhodnocuje příchozí zprávy a začíná komunikaci přes příslušný komunikační kanál se serverem.

Afaria umožňuje ochranu dat a zařízení. Umožňuje SSL komunikaci pro TCP/IP, HTTP a autorizaci uživatelů přes LDAP.

5.1 Architektura aplikace



obrázek č. 10 – architektura Afarie [13]

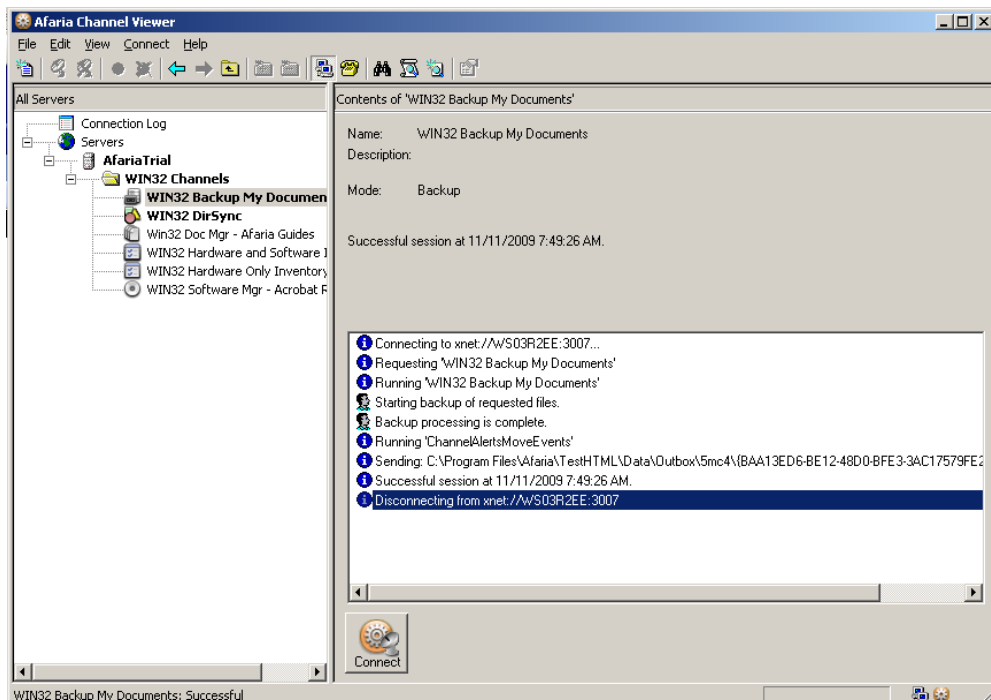
1. Klienti – klientské zařízení Afarie mohou být zařízení jako laptopy, telefony, handheld zařízení. Každé z těchto zařízení může mít nainstalovanou klientskou aplikaci Afarie. Klient inicializuje spojení se serverem. Server díky spojení může ovládat klientské zařízení, instalování updatů a přenos dat od klienta. Klient má různé možnosti dle zakoupené licence.
2. Síťové připojení – připojení klientů přes HTTP nebo HTTPS protokoly. Klienti se mohou připojovat také přes XNET a XNETS protokoly za podnikovým firewallem.
3. Externí firewall – chrání firemní síť před neautorizovaným přístupem z internetu. Povoluje příchozí komunikaci k Afaria serveru.
4. Relay (přenosový) server – funguje jako proxy server pro HTTP a HTTPS přenosy mezi Afaria serverem a Afaria klienty. Používání relay serveru podporuje větší bezpečnost sítě tím, že bod pro připojení klientů je před interním firewallem v tzv. DMZ (demilitarizované zóně).
5. Interní firewall – chrání firemní IT prostředky jako např. Afaria server před DMZ.
6. Afaria server – je server based řešení, které dokáže pracovat jako jediný server nebo více serverů – serverové pole. Server komunikuje s databázovým serverem, administrátorem a OTA (Over-The-Air) centrem a klienty.
 - a. jediný server – funguje na principu „one-to-one“ komunikace s databázovým serverem
 - b. serverové pole – funguje na principu „many-to-one“ komunikace s databázovým serverem

7. Databázový server – obsahuje databázi Afaria serveru.
8. Directory server – provádí ověření NT domény nebo LDAP služby, jako např. Active Directory, lze nastavit ověřovací metodu a doménu pro Afarii.
9. Afaria administrator – je webová aplikace, která působí jako interface pro Afaria server, přes který jsou vytvářeni klienti, uživatelé, je monitorována aktivita systému atd.
10. Individuální Afaria aministrátor, který je zodpovědný za ovládání aplikací.

5.1.1 Afaria server

Afaria server nemá žádné uživatelské rozhraní. Veškeré části programového vybavení jsou uloženy na počítači, kde je serverová aplikace nainstalována. Mezi programy, které jsou na serverovém počítači Afarie, také patří:

- Channel Viewer user interface – pokud je licencován klient Afarie pro Windows, je tento program automaticky nainstalován se serverovou instalací Afarie. Umožňuje běh klienta Afarie na tom samém počítači, kde je nainstalován Afaria server.



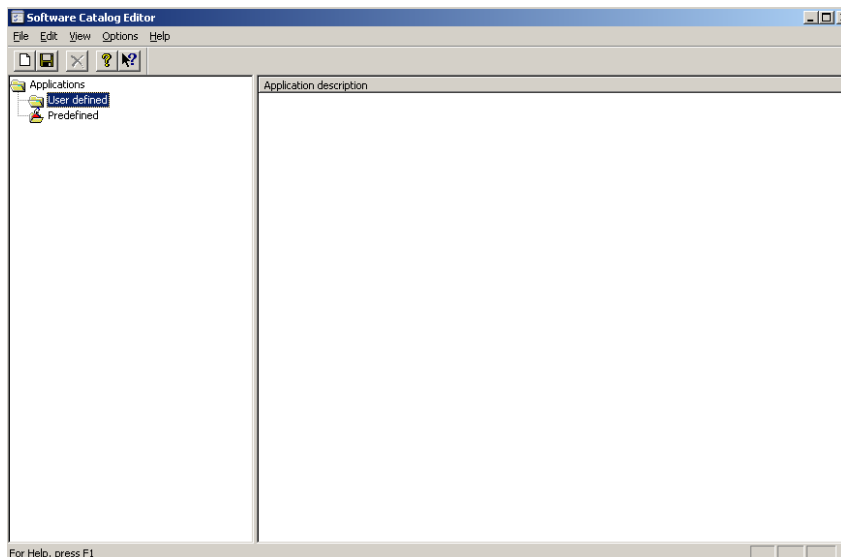
obrázek č. 11 – Channel Viewer user interface [printscreens autora]

- Create Client Installation – tento program umožňuje uživateli pomocí průvodce vytvářením klientských instalačních souborů vytvářet instalační balíčky klientských aplikací pro různé typy mobilních zařízení.



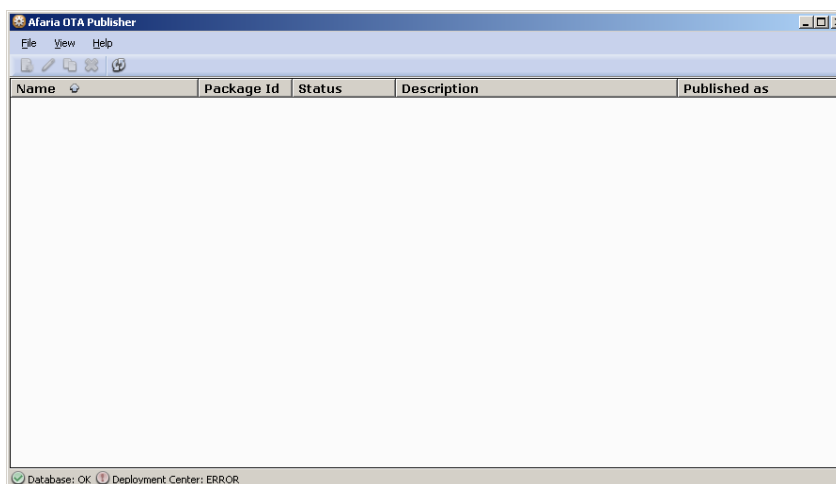
obrázek č. 12 – Create client Installation [printscreen autora]

- Software Catalog Editor – tato aplikace umožňuje sledovat instalovaný software na klientských zařízeních.



obrázek č. 13 – Software catalog editor [printscreen autora]

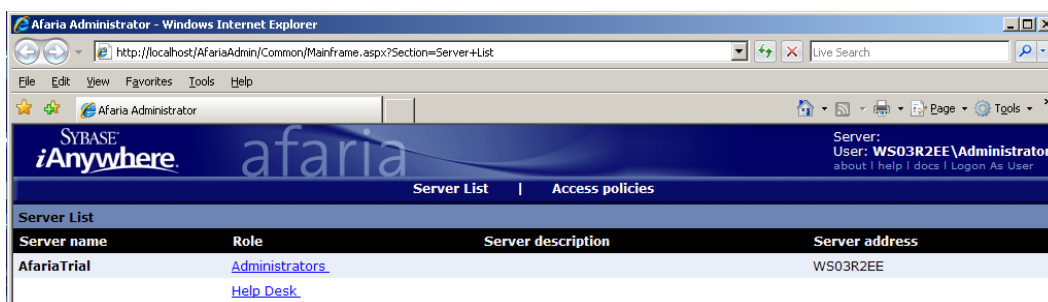
- Over-the-Air (OTA) Publisher – je používán pro posílání nových balíčků do OTA Deployment center a k řízení balíčků v centru.



obrázek č. 14 – Afaria OTA Publisher [printscreen autora]

5.1.2 Afaria administrator

Je interface pro přístup k Afaria serveru. Je spustitelný na počítači s operačním systémem Windows, Microsoft .NET runtime a webovým prohlížečem. Pomocí rozhraní Afaria Administrator lze zobrazit důležité informace o serveru, měnit konfigurační nastavení serveru, ovládat profily skupiny, jednotlivé komunikační kanály Afarie atd.



obrázek č. 15 – Afaria Administrator [printscreens autora]

5.1.3 Afaria serverové pole

Je skupina serverů, které jednají jako jediná entita. Podporují sdílené využití centralizované Afaria databáze, která obsahuje záznamy o loginech, výstrahách systému apod. Dynamicky volený počítač v serverovém poli funguje jako „master“ (pán) a obsluhuje výstrahy systému a detekuje změny u všech Afaria serverů. Na „master“ serveru jsou vytvářeny a spravovány všechny kanály, skupinové profily a pravidla. Klienti mohou navázat spojení s jakýmkoliv serverem, aby získali data z vyžádaných komunikačních kanálů. Z pohledu klientů je integrace serverů nepodstatná.

5.1.4 Typy klientů

Afaria podporuje správu různých typů zařízení. Pro hostující zařízení jsou různé typy klientského software, zařízení jsou roztříděna podle typů klientů. Pro zařízení, která nemají klientský software Afarie, ale jedná-li se o zařízení podporující OMA (open-mobile-alliance), jsou zařízení roztříděna podle OMA typu klientu.

Klienti pro Windows

- Channel Viewer UI – uživatel může pomocí aplikace z desktopu PC provádět různé úkoly včetně zobrazování obsahu různých serverů, přihlásit se k odběru dat u různých kanálů a plánování automatických updatů kanálů.
- Browser UI – obsah kanálů je publikován na webové stránky a klient se připojuje ke kanálům za použití internetového prohlížeče.
- Scheduled mode – klient spouští kanály podle vytvořeného plánu bez interakce uživatele

Java klienti

Afaria podporuje spojení s Java klienty, kteří řídí zařízení s operačními systémy Sun Solaris, HP-UX a Linux.

Klienti pro Windows Mobile Professional

Windows Mobile Professional klienti podporují spojení přes kanály se serverem jak při synchronizaci zařízení se stolním počítačem nebo pomocí přímé komunikace klienta se serverem přes bezdrátové spojení. Obdobně fungují klienti pro Windows Mobile Standard.

Palm klienti

Spojení se serverem se může uskutečnit v momentě, kdy probíhá HotSync spojení se stolním počítačem nebo pomocí přímé komunikace klienta se serverem.

BlackBerry Clients

Afaria podporuje klientský software pro zjišťování informací např. o počtu uložených mailů, seznam instalovaného software nebo použití příkazů zamčení v případě krádeže klientského zařízení.

Symbian klienti

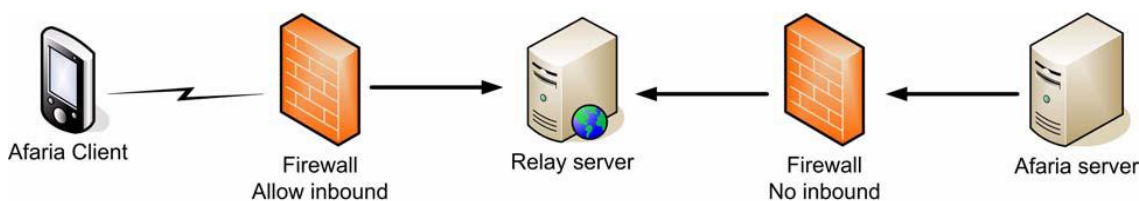
Podporují obvyklý způsob správy multimediálních zařízení podobně jako klienti pro Windows Mobile.

OMA DM typ klienta

Afaria podporuje také Open Mobile Alliance (OMA) Device Management (DM) zasilání OMA DM zpráv zařízením, které tyto standardy podporují. Pomocí editoru lze vytvářet OMA DM úkoly, které jsou transformovány na OMA DM zprávy.

5.1.5 Relay server

Afaria podporuje využití relay (přenosového) serveru jako proxy pro HTTP a HTTPS spojení mezi Afaria serverem a Afaria klienty. Použití tohoto serveru zvyšuje bezpečnost celé podnikové sítě přenesením příchozích spojení před interní firewall do tzv. „DMZ“ demilitarizované zóny.



obrázek č. 16 – schéma spojení Relay serveru [13]

Pokud je používán relay server Afaria klienti nikdy nevytvářejí přímé spojení s Afaria serverem, klienti navazují spojení nejdříve s relay serverem, který data předává Afaria serveru a naopak, spojení je ukončeno, teprve až jsou všechna data přenesena. Relay server může být jeden nebo serverové pole podobně jako Afaria server.

5.2 Zabezpečení

Data Security Manager pro handheld zařízení umožňuje definování bezpečnostních pravidel pro Afaria klienty. Bezpečnostní pravidla zahrnují ochranu pomocí hesla, několik způsobů zamčení klienta a šifrování dat. Podporované typy operačních systémů jsou: Windows Mobile Professional a Standard, Symbian a Palm.

Zabezpečení pomocí hesla chrání zařízení, data a aplikace před neoprávněným přístupem. Heslo může být také použito pro autorizaci, např. při vkládání paměťové karty nebo při spuštění synchronizace. Data Security Manager má různé možnosti správy hesel.

Power-on password – umožňuje vnutit používání hesla klientovi. Lze nastavit tzv. sílu hesla. Což je minimální počet znaků nebo číslic, které musí heslo mít dle firemních bezpečnostních zásad.

Administrator password – umožňuje kdykoliv přístup do klientského zařízení i v případě, že je zařízení uzamčeno a je vypnuté uživatelské heslo.

Remote-based recovery – tato funkce slouží pro obnovení uživatelského hesla v klientském zařízení v případě, že uživatel zapomene heslo. Pro tuto funkci je nutná spolupráce uživatele s administrátorem systému.

Device-based recovery – poskytuje možnost obnovení hesla bez asistence administrátora systému. Uživatel klientského zařízení si definuje bezpečnostní otázku pro případ ztráty hesla a odpověď na ni. Použití této metody obnovení hesla lze v systému povolit či zakázat.

Manual lock – dovoluje uživateli zamknout či odemknout zařízení bez nutnosti čekání na příkaz automatického zamčení zařízení. Uživatel musí pro zamknutí či odemknutí zařízení zadat platné uživatelské, administrátorské nebo dočasné heslo. Tato funkce zabraňuje neautorizovanému přístupu k zařízení či datům. Obdobou této funkce

je automatické uzamčení zařízení, kdy je klientské zařízení uzamčeno po určité době nečinnosti.

Data encryption – tato funkce dovoluje zašifrovat citlivá data v zařízení nebo na paměťové kartě. Pomocí kanálového editoru lze vybrat konkrétní data k zašifrování. Lze také povolit šifrování dat v zařízeních přímo uživatelům. Afaria podporuje různé šifrovací algoritmy včetně FIPS (Federal Information Processing Standards) a AES (Advanced Encryption Standard).

Password lock down a connection lock down metodika organizace – umožňuje stanovit zásady pro zablokování hesla v případě většího počtu neúspěšných pokusů o jeho zadání nebo v případě ztráty spojení se zařízením. Kromě zablokování hesla lze nastavit další pojistky jako smazání dat nebo „tvrdý“ reset zařízení do továrního nastavení.

Custom user interface – dovoluje uživatelům osobní nastavení některých částí klientského zařízení včetně grafického rozhraní pro zadávání hesla.

Data Security Manager uninstall – dovoluje administrátorovi odinstalaci Data Security Manageru z klienta Afarie. Odinstalační proces dešifruje všechna data v zařízení a na paměťové kartě.

Server-side descryption utility – dovoluje dešifrovat data na externí paměťové kartě, která byla zašifrována Afaria Data Security Managerem. Tato funkce je dobrá v případě, že původní zařízení, které obsahovalo kartu se zašifrovanými daty, bylo resetováno nebo byl odinstalován Afaria klient či se stala jiná událost, která zapříčinila nemožnost dešifrování dat původním klientem.

Data Security Manager reports – obsahuje předdefinované sestavy hlášení v oblasti změn hesel uživatelů, administrátorů nebo naopak v případě nezměnění hesla apod.

Data Security Manager pro Windows klienty dovoluje definování bezpečnostních pravidel pro počítače a notebooky s operačním systémem MS Windows. V manageru existují dvě vrstvy zabezpečení: boot-time autentifikace uživatelů a šifrování dat na pevných discích a přídatných médiích.

Šifrování pevných disků a přídatných médií je prováděno pomocí AES 128 bitového šifrovacího algoritmu. Šifrovací klíč pro každý pevný disk nebo přídatné zařízení je vždy unikátní. Data jsou dostupná pro každého uživatele bez narušení plynulosti spuštěných aplikací. „Tvrdý“ restart dovoluje kanálu Afarie spustit mód údržby pro Data Security Manager klienta. Tento mód dovoluje restart klienta bez interakce uživatele. Po restartu v tomto módu je operační systém nastartován ve stavu, kdy se další uživatelé nemohou nalogovat do systému. Mód údržby je vhodný pro úkony, jako je instalování aplikací, patchů apod.

Single sign on – je volba pro synchronizaci uživatele Data Security Manageru s heslem v systému Windows. Volba může být nastavená buď jako automatická akce nebo na základě volby uživatele.

Challenge-response recovery – je bezpečnostní mechanismus, který dovoluje autorizovanému uživateli získat kontrolu nad počítačem ze stavu, kdy bylo mnohokrát zadáno nesprávné heslo.

MediaViewer – je řešení, které umožňuje prohlížení obsahu pevných disků a dalších médií na počítači, na kterém není nainstalován Data Security Manager klient.

Sdílení přídatných zařízení, která jsou zašifrována, je možné několika způsoby:

Computer work groups – šifrovací klíč je sdílen skupinou klientských počítačů, pro sdílení médií všemi jejich uživateli. Single computer – šifrovací klíč je rezervován pro všechny uživatele jediného počítače. User work groups – šifrovací klíč je sdílen skupinou uživatelů na jednom nebo více počítačích. Single user – uživatel má šifrovací klíč pouze pro sebe.

Multiple Client users – jeden Data Security Manager podporuje více uživatelů, každý uživatel má svoje vlastní uživatelské jméno a zodpovídá za správu svých hesel a šifrovacích klíčů.

Client administrators – klient může podporovat více Data Security Manager administrátorů. Administrátoři mají právo spravovat uživatele, měnit bezpečnostní nastavení spravovat šifrovací klíče a vyřazovat klienty. Každý klient má alespoň jeden administrátorský účet, který je vytvořen při instalaci. Klient administrátor musí být současně Windows administrátorem.

Client management tool – klienti obsahují také uživatelské rozhraní pro administrátory a uživatele.

Afaria Administrator Client views – web console obsahuje definované uživatelské pohledy pro Data Security Manager klienty. Lze zahrnout také nová data při definování nového uživatelského pohledu.

5.3 Možnosti použití

Autorem práce byla testována aplikace Afaria ver. 6.0. Na stránkách společnosti Sybase <http://www.sybase.com/> lze stáhnout po zaregistrování pro účely testování trial verzi této aplikace na 30 dní.

Afaria 6.0 v trial verzi je dodávána jako virtuální obraz operačního systému MS Windows Server 2003 R2 Enterprise Edition SP2 s již nainstalovaným serverem Afarie, kde jsou licencovány tyto komponenty systému: Afaria Backup Manager, Afaria Configuration Manager, Afaria document manager, Afaria Inventory Manager, Afaria Licence Manager, Afaria Security Manager, Afaria Session Manager, Afaria Software Manager. Trial verze aplikace neobsahuje funkce a aplikace: Patch Manager, OneTouch, vzdálený přístup, SMS Integration Suite, OTA device provisioning, podporu pro bezdrátový e-mail. Na virtuální instalaci Windows Serveru 2003 jsou již také nainstalovány všechny další aplikace, které jsou potřeba ke spuštění Afarie (Microsoft .NET Framework a SQL Anywhere 11). Součástí dodávky je také aplikace Microsoft Virtual PC, na které byl autorem práce spuštěn a testován virtuální obraz Afaria serveru.

Afaria server byl testován na lokální síti s třemi klientskými zařízeními. Prvním klientským zařízením byl samotný virtuální server (OS Windows Server 2003 R2), na kterém je rovněž nainstalován Afaria Channel Viewer, který dovoluje používat samotný server zároveň jako klientské zařízení, dále notebook s OS MS Windows Vista Home Premium, na který byl nainstalován a předtím vytvořen pomocí aplikace Create Client Installation Afaria klient pro MS Windows a posledním zařízením byl mobilní telefon SGH-i900 s operačním systémem Windows Mobile Professional 6.1, na který byl nainstalován Afaria klient pro Windows Mobile, který byl rovněž vytvořen pomocí aplikace Create Client Installation.

All Clients			
Cli...	Client type	Last connection date	First connection date
WS03R2EE	Windows	11/11/2009 7:49:24 AM	6/11/2009 11:34:01 AM
DUKAT-PC	Windows	11/15/2009 10:18:07 AM	11/8/2009 9:41:30 AM
SGH-i900	Windows Mobile Professional	11/8/2009 7:58:07 PM	11/8/2009 5:19:41 PM

obrázek č. 17 – Použitá klientská zařízení v

Pro komunikaci klientů se serverem byla na lokální síti použita nezabezpečená verze protokolu XNET.

Client communication

Protocols and ports

Configure protocols and ports to use for client communication. XNET is always used. Ensure your firewall allows bidirectional traffic for each port used.

<input checked="" type="checkbox"/> XNET (TCP/IP)	Port	3007	Reset to default
<input type="checkbox"/> XNETS (TCP/IP over SSL)	Port	3008	Reset to default
<input type="checkbox"/> HTTP	Port	8088	Reset to default
<input type="checkbox"/> HTTPS	Port	443	Reset to default

SSL certificates

To use the XNETS and HTTPS protocols, you must associate the certificate obtained from a Certificate Authority (CA) with the corresponding private key.

[Associate certificate and key...](#) [View certificates...](#) [Generate certificate request...](#)

Address for Client communication

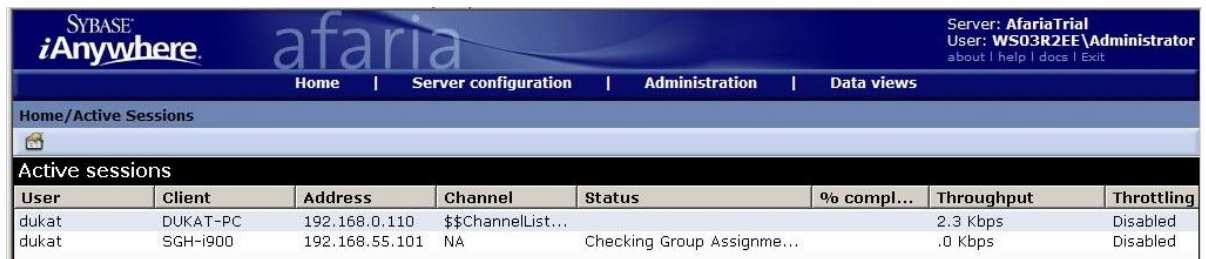
Define the default server address for Clients to use when contacting the server. This value is used to seed client installations, XEC generation, and outbound notifications. Resetting the default address will select the port number from above.

Syntax: [protocol://]Address[:port]
Example: 10.24.23.13
Example: xnets://server1.example.com:3008

[Reset to default...](#)

obrázek č. 18 – Nastavení komunikace s klienty [printscreens autora]

Veškerá komunikace mezi serverem a klienty se odehrává pomocí kanálů (channels). Kanál je sada úkolů a instrukcí, které klient vykoná, když se připojí k serveru. Pomocí kanálů lze měnit nastavení zařízení, stahovat data apod. Druhy kanálů jsou specializované, jsou využívány jednotlivými komponenty systému Afaria, např. Document Managerem, Data Security Managerem a dalšími. V případě, že je některý z kanálů aktivní, probíhá tzv. „session“ – spojení mezi klientem a serverem.



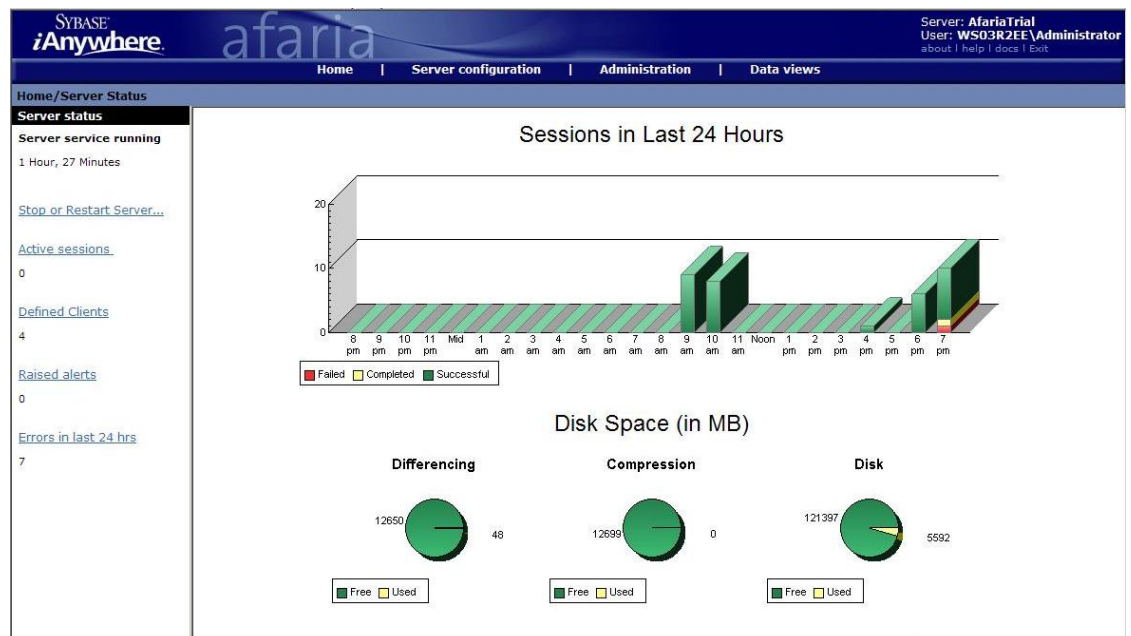
The screenshot shows the Afaria administrator interface. At the top, there is a navigation bar with 'Home', 'Server configuration', 'Administration', and 'Data views'. Below this, the 'Active sessions' section is displayed as a table with the following data:

User	Client	Address	Channel	Status	% compl...	Throughput	Throttling
dukat	DUKAT-PC	192.168.0.110	\$\$ChannelList...			2.3 Kbps	Disabled
dukat	SGH-I900	192.168.55.101	NA	Checking Group Assignme...		.0 Kbps	Disabled

obrázek č. 19 – Active session [printscreen autora]

Během testování aplikace byly vyzkoušeny základní kanály pro zjišťování konfigurace HW klienta, SW klienta, Backup Manager (zálohování dat a nastavení), přenos souborů, obnova hesla apod.

Afaria administrator nabízí přehledné menu pro sledování systémových událostí serveru, menu pro konfiguraci serveru, administrační část pro definování komunikačních kanálů, správu uživatelů a automatických akcí a část pro sledování logů systému.



obrázek č. 20 – Status serveru [printscreen autora]

System lze hodnotit jako velice robustní a výkonný. Výhodou jsou jeho nízké HW nároky, podpora různých typů mobilních zařízení včetně notebooků a různých operačních systémů.

6 Správa mobilních zařízení – možnosti implementace a hodnocení

V předchozích kapitolách byly prakticky testovány SW pro správu mobilních zařízení. Tato kapitola se zabývá případovou studií projektu mobilní výukové sítě, jejímž cílem je navrhnout mobilní síť pro výukové účely na střední škole (SŠ) za použití aplikace Afaria nebo Mobile Device Manager a uvést možnosti implementace.

Porovnání kladů a záporů aplikací Mobile Device Manager (MDM) a Afaria v podmínkách střední školy:

klady MDM

- kompatibilita s dalším software od spol. Microsoft
- GUI typická pro Microsoft software
- propracovaná správa mobilních zařízení se systémem Windows Mobile

zápory MDM

- vysoké HW nároky a pouze 64 bit architektura
- kompatibilita pouze se zařízeními Windows Mobile

klady Afarie

- kompatibilita s mobilními zařízeními založenými na různých platformách vč. Blackberry, Linuxu a možnost správy nejen mobilních zařízení jako jsou smartphony a PDA, ale i notebooků apod.
- oproti MDM má nižší HW nároky – vhodnější i pro menší organizace (pro běh aplikace stačí i jeden fyzický server resp. virtuální)

zápory afarie

- netypické GUI (oproti MS softwaru), je nutné více času pro seznámení se s veškerými funkcemi a ovládáním aplikace

Po porovnání výše uvedených kladů a záporů je pro výukové účely na středních školách - obor Informační technologie a obdobné obory vhodnou aplikací Afaria, vzhledem ke své univerzálnosti, nárokům na hardware a zároveň i poměr cena/výkon.

6.1 Návrh mobilní sítě pro výukové účely na SŠ

Mobilní výuková síť je navrhována pro potřeby výuky na Střední průmyslové škole na Proseku pro oblast mobilních technologií, která bude obsažena v předmětech Mobilní technologie a Praktická cvičení, které jsou součástí aktuálně připravovaného školního vzdělávacího programu oboru Informační technologie. Tyto předměty se budou zabývat zejména praktickou výukou mobilních technologií a budou navazovat na teoretické znalosti, které studenti získají v předmětech Počítačové sítě, Technické vybavení a Operační systémy a praktické dovednosti získané v Praktických cvičeních. Výuka mobilních technologií začne ve školním roce 2011/2012. Tematický plán výuky předmětu Mobilní technologie bude vypracován autorem této práce v návaznosti na tematické plány dalších souvisejících předmětů, které jsou v současné době vypracovávány a také na základě úrovně skutečně získaných znalostí studentů v ostatních předmětech. Zvažuje se také zavedení výuky mobilních technologií do dalších oborů, např. do oboru Mechanik elektronik - kde se vyučují oblasti elektronika, informatika a zabezpečovací technika. Všechny výše uvedené oblasti úzce souvisí s mobilními technologiemi.

Mobilní síť bude studentům sloužit zejména k získání praktických dovedností při správě a ovládání mobilních zařízení a administraci mobilní sítě. Mobilní výuková síť bude nadstavbou projektu nové školní laboratoře IT technologií.

Informační technologie		18-20-M/01				
		Platný od 1.9.2010 - předběžný				
Předmět		Zkratka	Ročník			
Název předmětu			1	2	3	4
Všeobecné vzdělání						
Jazykové vzdělání						
Cesky jazyk	CJ	4	3	3	3	3
Anglický jazyk/Německý jazyk	AJ	3/3	3/3	3/3	3/3	3/3
Anglický jazyk/Německý jazyk	NJ	2/2	2/2	2/2	2/2	2/2
Společenskovědní vzdělání						
Základy společenských věd	ZSV	2	1	1	1	1
Přírodovědné vzdělání						
Fyzika	F	2	2	-	-	-
Chemie	CH	1	-	-	-	-
Základy ekologie	ZEK	-	1	-	-	-
Matematické vzdělání						
Matematika	M	3	3	3	3	3
Vzdělání pro zdraví						
Tělesná výchova	TV	2/2	2/2	2/2	2/2	2/2
Lyžařský výcvik	ZVK	1 týden	-	-	-	-
Sportovní kurz	LVK	-	-	1 týden	-	-
Ekonomické vzdělání						
Ekonomika	E	-	1	2	-	-
Odborné vzdělání						
oblast hardware						
Technické vybavení	TVy	2	2	2	2	2
Mobilní technologie	Mt	-	-	-	-	1
oblast základního programového vybavení						
Operační systémy	OS	-	-	3/2 ^A	3/2 ^A	-
oblast aplikačního programového vybavení						
Programové vybavení	PVy	4/3	2,5/2	-	-	-
Databázové a informační systémy	Dat	-	-	3/2	3/3	-
Počítačová grafika	PGM	-	2,5/2	-	2/2	-
oblast počítačových sítí						
Počítačové sítě	PSi	-	-	3	2	-
oblast programování a vývoje aplikací						
Programování	Prg	-	-	3/3	3/3	-
Webové stránky	Web	3/2	2/2	-	-	-
Umělá inteligence	UI	-	-	-	1/1	-
oblast elektrotechniky, elektroniky						
Elektronická technická dokumentace	ETD	2	3/3	-	-	-
Elektrotechnika	Elt	2	-	-	-	-
Elektronika	Eln	-	2	-	-	-
Automatizace	Au	-	-	2	-	-
Oblast praktického vyučování						
P r a v i t ě l e c n i k i á	Programování mikroprocesorů	PCv	-	2/2	-	-
	Elektrotechnika, elektronika a fyzika		-	0,5/0,5 [*]	1/1 [*]	-
	Hardware a počítačové sítě		-	0,5/0,5 ^{*A}	1/1 ^{*A}	1/1 ^{*A}
	Automatizace		-	-	1/1 [*]	-
	Správa mobilních zařízení		-	-	-	1/1 ^A
	Souvislá praxe		-	2 týdny	2 týdny	-
Celkem			32	35	35	33

Legenda: počet hodin - X/Y = celkový počet hodin/cvičení
cvičení s * jsou děleny na 1/3, cvičení označené ^A budou vyučovány v laboratoři IT

obrázek č. 21 – Učební plán oboru Informační technologie [17]

6.1.1 Hadwarové zabezpečení mobilní sítě

Výuka předmětu bude probíhat maximálně v 16ti členných skupinách. Bude zakoupeno 8 mobilních zařízení.

Technické specifikace a parametry zvažovaných zařízení:

MDA Mivvy Zero

Podporované sítě:

GSM (850/ 900/ 1800/ 1900 MHz)

GPRS/ EDGE třídy 12

Operační systém:

Windows Mobile 6.5

Displej:

Dotykový TFT QVGA (240 × 320 bodů), 65 536 barev, úhlopříčka 2,8 palce

Procesor:

Marvell PXA300 s frekvencí 624 MHz

Paměť:

128 MB RAM, 256 MB Flash ROM

Slot pro paměťové karty: microSDHC (max. 32 GB)

Digitální fotoaparát:

Rozlišení dva megapixely; možnost nahrávání videa

Další vlastnosti:

GPS (SiRFstar III)

Pohybový senzor

Vibrace

FM rádio

Stavová LED dioda (zelená/červená/modrá)

Java Virtual Machine

SIM Toolkit

Nativní česká lokalizace

Rozhraní:

miniUSB 1.1

Datové funkce: Wi-Fi 802.11 b/g,

Bluetooth 2.0 včetně EDR (podporované profily: DUN, HFP, HSP, HID, OPP, PAN, A2DP, AVRCP, PBAP, GAP, GOEP a SPP)

Napájení:

Li-Pol akumulátor s kapacitou 1100 mAh

Pohotovostní režim: 150 hodin

Max. doba hovoru: 240 minut

Rozměry:

103 × 54 × 14,5 mm

Váha:

81/104 g (bez/ včetně baterie)

Dodávané příslušenství:

Baterie

Stylus

Nabíječka

Stereo headset

USB kabel

Příručka pro rychlý start

CD-ROM s Uživatelským manuálem a SW ActiveSync

Cena zařízení: 5 873 Kč. [18]

Samsung Omnia II i8000

Podporované sítě:

GSM 850/ 900/ 1800/ 1900 MHz

UMTS 900/ 1900/ 2100 MHz

Operační systém:

Windows Mobile 6.5 Professional

Paměť:

256 MB RAM

Slot pro paměťové karty microSD

Uživatelská paměť 2 GB

Procesor:

Samsung S3C6410 s frekvencí 800 MHz

Displej:

Dotykový AMOLED displej s úhlopříčkou 3,7 palce

Rozlišení WVGA (480 x 800 bodů), 65 tisíc barev

Speciální ovládací prostředí TouchWiz 2.0

Fotoaparát:

Digitální fotoaparát s rozlišením 5 megapixelů

Automatické ostření, LED blesk

Natáčení videa v rozlišení 720 x 480 bodů (30 sn./s.)

Detakce obličeje a úsměvu, geotagging

Další vlastnosti:

Rychlá data HSUPA, HSDPA

Prohlížeč Pocket Internet Explorer, Opera 9.5

GPS (aGPS, 20 kanálů)

JAVA MIDP 2.1

Hudební přehrávač

Přehrávač videa s podporou DivX a XViD

Widgety na pohotovostní obrazovce

YouTube, Facebook

Synchronizace s PC i serverem

Podpora práce s dokumenty

Organizační funkce

FM rádio s RDS

Světelný a pohybový senzor, senzor přiblížení

Napájení:

Li-Ion akumulátor s kapacitou 1500 mAh

Výdrž až 430 hodin v poh. režimu nebo 10 hodin hovoru

Rozhraní:

USB 2.0 (microUSB)

Bluetooth 2.0 (A2DP)

Wi-Fi 802.11b/g

3,5 mm audio jack

Barevné provedení:

Černé

Rozměry:

118 x 59,6 x 11,9 mm

Hmotnost:

129 g

Cena zařízení: 10 599 Kč. [19]

MDA GIGABYTE GSmart MS802

Podporované sítě:

GSM 900/ 1800/ 1900 MHz

HSDPA 2100 (3.5G)

Operační systém:

Windows Mobile 6.1 Professional

Procesor:

Marvell PXA 270 s frekvencí 520 MHz

Paměť:

256 MB ROM, 128 MB RAM

Slot pro paměťové karty microSDHC

Displej:

Dotykový displej s úhlopříčkou 2,8 palce

Rozlišení 240 x 320 bodů, 65 tisíc barev

Fotoaparát:

Rozlišení 3.15 megapixely, automatické ostření

Záznam videa, CMOS fotoaparát na čelní straně

GPS:

Vestavěná GPS navigace

Další vlastnosti:

Windows Mobile Direct Push E-Mail

Windows Live Messenger

Multimediální přehrávač

FM rádio s RDS

Funkce pro organizaci času

Internetový prohlížeč

Hry

Kalkulačka, poznámky

GPS (SirfStar III)

Hudební přehrávač (MP3, AAC, WMA, AMR, WAV, MIDI)

Přehrávač videa (MPEG4, 3GPP, WMV)

Rozhraní:

USB 2.0 (miniUSB)

Bluetooth 2.0 + EDR a A2DP

Wi-Fi 802.11b/g

3,5 mm audio jack

Napájení:

Li-Pol akumulátor s kapacitou 1300 mAh

Výdrž až 4 hodiny hovoru nebo 150 hodin v poh. režimu

Obsah balení:

PDA MS802

Sluchátka s mikrofonem

Nabíječka

2x stylus

USB kabel

Český manuál

CD se softwarem

Rozměry:

117 x 59,8 x 14,8 mm

Hmotnost:

130 g

Cena zařízení: 6323 Kč. [20]

Z těchto tří zvažovaných typů zařízení bylo autorem vybráno jako nejvhodnější na základě poměru cena/výkon MDA Mivvy Zero. Celková cena za 8 mobilních zařízení bude činit 46 984 Kč.

Dalším hardwarem, který bude začleněn v mobilní výukové síti je několik notebooků, které jsou součástí projektu laboratoře IT technologií. Server, na kterém bude spuštěna aplikace pro správu mobilní sítě bude virtuální. Fyzický hardware, na kterém bude virtuální stroj spuštěn a další síťové prvky potřebné pro běh sítě budou rovněž využity z infrastruktury laboratoře IT a školní Wi-Fi sítě. Projekt laboratoře IT technologií bude specifikován v kapitole 6.2 Implementace.

6.1.2 Softwarové zabezpečení mobilní sítě

Potřebným softwarem pro mobilní síť bude:

- Kernel Virtual Machine – nástroj pro virtualizaci založený na linuxové distribuci Proxmox VE
- MS Windows Server 2003 R2 Enterprise Edition SP2 – serverový operační systém
- Microsoft .NET Framework – prostředí pro běh aplikací
- SQL Anywhere 11 – databázový systém
- Afaia 6.0 – systém pro správu mobilní sítě skládající se z jednotlivých součástí:
 - Afaia Backup Manager
 - Afaia Configuration Manager
 - Afaia document manager
 - Afaia Inventory Manager
 - Afaia Licence Manager
 - Afaia Security Manager
 - Afaia Session Manager
 - Afaia Software Manager
 - Patch Manager
 - OTA device provisioning

6.2 Implementace

Projekt laboratoře IT technologií a mobilní výukové sítě bude realizován ve školním roce 2010/2011. Mobilní výuková síť bude nadstavbou projektu laboratoře IT technologií, která je navrhována s následujícími parametry:

Část 1 – nábytek a hardware [17]:

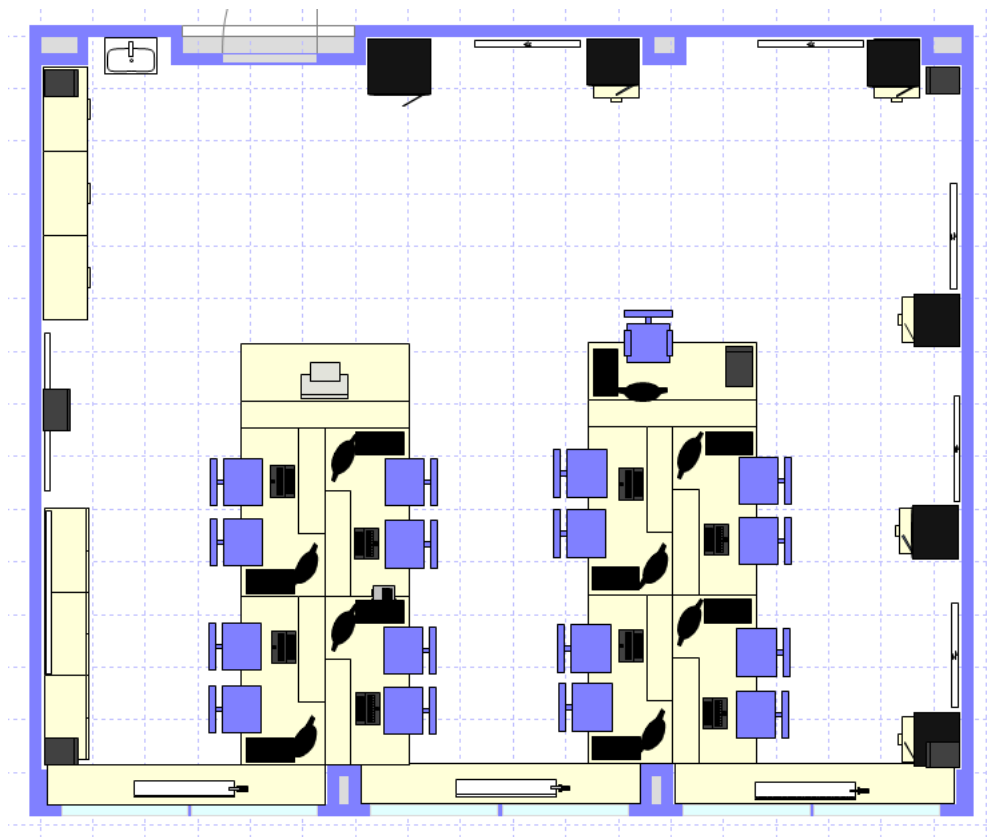
<i>položka</i>		<i>rozměry</i>	<i>barva</i>	<i>kusů</i>	<i>cena (s DPH)</i>	<i>cena celkem(Kč)</i>
Počítačový stůl		1600x800	dub	10	5000	50000
Stolová nástavba		1200x250	dub	8	2000	16000
Stolová nástavba		1600x250	dub	2	2000	4000
Židle DREAM				17	2450	41650
šuplík pod stůl				1	1500	1500
Skříň s dveřmi				1	7300	7300
Skříň prosklená				2	14000	28000
						0
Tabule bílá		1500x1200		1	7000	7000
					2600	0
Plátno el.				1	10000	10000
				0	18000	0
Projektor Benq				1	26000	26000
držák projektoru + lišty + VGA kabel				1	3000	3000
Rack hlavní:						0
19" rozvaděč stojanový 42U		600x800		1	13000	13000
ATEN přepínač s 17" LCD do racku + kabely				1	27000	27000
vyvazovací panel - kovový				3	300	900
rozvodný panel 230V				1	900	900
SWITCH HP ProCurve 2510-24				3	8500	25500
patch panel 5e UTP 24 portů				3	600	1800
APC Smart-UPS SC 450VA, 1U	4x 1ks		alternativa	4	5500	22000
Ližiny pro server				4	2000	8000
Rack student:						0
19" rozvaděč nástěnný 18U		600x515	45kg	5	5500	27500
rozvodný panel 230V				5	900	4500
vyvazovací panel - kovový	5 x 4ks			20	300	6000
patch panel 5e UTP 24 portů	5x 2ks			10	600	6000
patch panel 5e neosazený	5x 1ks			5	200	1000

osazení	5x 24ks	max 120	50	34	1700
CCNA Discovery and CCNA Exploration Standard POD (Rackmountable)			90000	3	270000
SWITCH HP ProCurve 2510-24	5x 1ks		5	8500	42500
					0
montážní sada (šrouby)			50	45	2250
Počítač - Core 2 Duo, 2-4GB, 160GB HDD, DVD-RW, s WIFI			9	11000	99000
					0
Samsung 943N (nahrazen 911NT - tenký klient)			9	3600	32400
KVM Switch ATEN CS-64U (USB)			9	450	4050
Klávesnice Genius KB-120e, USB, black			9	150	1350
Myš Genius XSCROLL, USB, black			9	100	900
Notebook - HP Pro 4515			8	13000	104000
					0
Server -XEON QUAD-CORE, 12GB DDR3,Velocity, 4x LAN			4	32000	128000
M1522nf - T+K+S+F - 8200,-Kč			1	8500	8500
NAS server			1	16000	16000
					0
Vybudování lokální sítě			1	150000	150000
Úprava učebny			1	20000	20000
				celkem	1219200

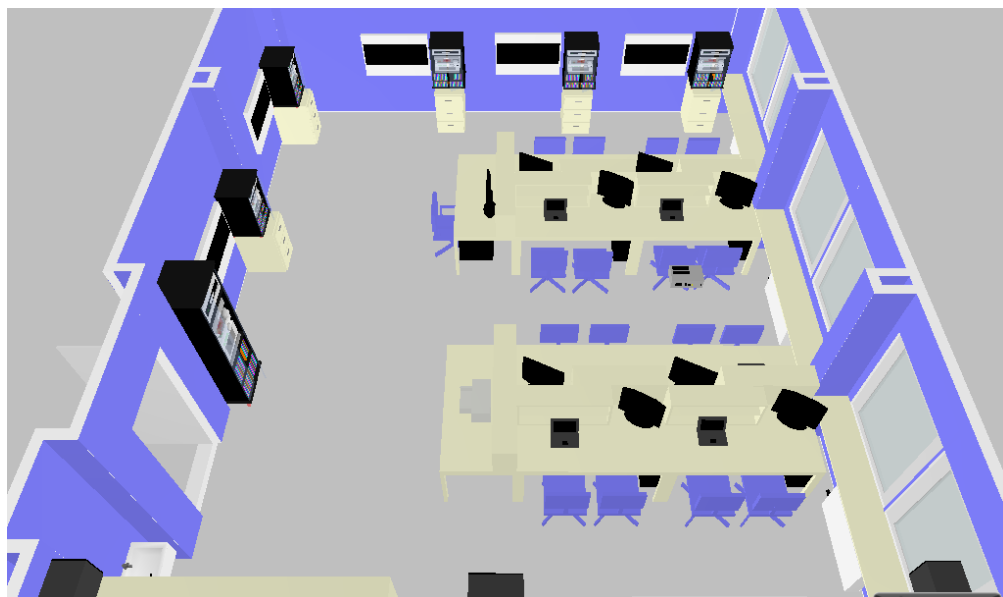
Část 2 – testery, kabeláž a ostatní vybavení [17]:

<i>položka</i>			<i>rozměry</i>	<i>barva</i>	<i>kusů</i>	<i>cena (s DPH)</i>	<i>cena celkem(Kč)</i>
WIFI tester					5	7700	38500
Tester UM NT-955					1	46000	46000
Tester optických kabelů - ST - měření útlumu					1	4500	4500
Tester optických kabelů - ST - měření průchodnosti					1	3800	3800
Multimetr HC-MT-1280					6	500	3000
Tester RS-232					6	250	1500
Tester sítě - testuje po párech					6	250	1500
WIFI router - na panel					5	2200	11000
							0
Bluetooth - mikro USB					9	250	2250
optický kabel - ST					5	120	600
optický kabel - LC					5	160	800
síťový kabel 3m -šedý					4	45	180

síťový kabel 5m -šedý		52	65	3380
síťový kabel 7m -šedý		4	80	320
síťový kabel 2m -šedý		10	35	350
síťový kabel 1m - šedý		10	25	250
síťový kabel 0.5m - šedý		20	20	400
síťový kabel 3m - Z, M, Č, Č, O, Ž	10ks každý	60	45	2700
síťový kabel 2m - Z, M, Č, Č, O, Ž	10ks každý	60	35	2100
síťový kabel 1m - Z, M, Č, Č, O, Ž	10ks každý	60	25	1500
prodlužovací kabel s vypínačem 5 zásuvek 3m		4	150	600
prodlužovací kabel s vypínačem 5 zásuvek 5m		6	200	1200
prodlužovací kabel bez vypínače 3 zásuvky 1,5m		8	100	800
držák prodlužovacího kabelu		18	20	360
koncovky RJ45 - lanko		300	2,5	750
koncovky RJ45 - drát		300	3,6	1080
krytka RJ45 - modrá		300	1	300
krytka RJ45 - bílá		300	1	300
koncovky RJ11		180	1	180
koncovky RJ12		180	1,5	270
kabel LAN - lanko		1	1700	1700
kabel LAN - drát		1	1500	1500
držák kabelů		600	5	3000
deska - výuková	0,96 m ²	360	5	1800
adapter USB-->IDE, SATA		650	6	3900
lampa s lupou		1	900	900
antistatický pásek na ruku		10	60	600
antistatická podložka 100x50cm		18	180	3240
demagnetizér a magnetizér		1	250	250
tester baterie		1	150	150
			celkem	147510
			projekt celkem	1366710



obrázek č. 22 – laboratoř IT technologií [17]



obrázek č. 23 – laboratoř IT technologií – 3D [17]

6.3 Ekonomická analýza

Společnost Sybase nabízí v České republice program Business partner, který obsahuje také EDU licence zdarma. Business partner program je zpoplatněn 13 000 Kč za kalendářní rok. V rámci EDU programu dostane SPŠ na Proseku licence pro SQL Anywhere Studio a iAnywhere Afaria pro 20 pracovišť. Součástí EDU programu jsou další benefity např. 3 dny školení atd.

Za licenci pro MS Windows Server 2003 R2 Enterprise Edition SP2 zaplatí SPŠ na Proseku v rámci licenčních podmínek firmy Microsoft 1200 Kč.

Celkové náklady za 8 mobilních zařízení MDA Mivvy Zero budou činit 46 984 Kč (kalkulace na základě maloobchodní ceny Alza.cz).

Zbýlý hardware nutný pro chod mobilní sítě je již zahrnut v celkové cenové kalkulaci projektu laboratoře IT technologií.

Sybase Software	Veškeré licence	13 000 Kč
MS Windows Server 2003	1 licence	1200 Kč
MDA Mivvy Zero	8 ks	46 984 Kč
Celková cena mobilní sítě		61 184 Kč
Celková cena včetně celé laboratoře IT tech.		1 427 894 Kč

7 Závěr

V rámci diplomové práce bylo prakticky otestováno programové vybavení pro správu mobilních zařízení Afaria od společnosti Sybase a Mobile Device Manager od společnosti Microsoft. Vzájemné porovnání obou aplikací proběhlo na základě jejich vhodnosti pro nasazení v projektu mobilní výukové sítě. Pro realizaci sítě byla na základě vyhodnocení vlastností obou testovaných řešení vybrána aplikace iAnywhere Afaria.

V rámci řešení diplomové práce byl vytvořen návrh mobilní sítě pro výukové účely na střední škole a uvedena možnost jeho implementace jako nadstavby projektu laboratoře IT technologií. Byla také provedena ekonomická analýza finanční náročnosti celého projektu.

V diplomové práci byla také uvedena charakteristika operačního systému Windows Mobile.

Pro vybudování laboratoře IT technologií a mobilní výukové sítě se rozhodla Střední průmyslová škola na Proseku z důvodu potřeby nabídnout svým studentům možnost seznámit se s co největším spektrem informačních technologií. Všeobecné znalosti IT technologií dovolí absolventům získat větší uplatnění na trhu práce. Autor diplomové práce je pedagogem na Střední průmyslové škole na Proseku a bude studenty oblast mobilních technologií vyučovat. V teoretické výuce budou studenti seznámeni s následujícími tématy: 1. Historie mobilních zařízení 2. SW a HW mobilních zařízení 3. Mobilní zařízení v praxi (m-commerce, m-business) 4. Správa mobilních zařízení (mobilní sítě) 5. Technologie GPS, GIS a GSM. V praktické výuce studenti získají zkušenosti s administrací mobilních zařízení a správou mobilní sítě. Celkové vyhodnocení projektu a jeho přínosu pro výuku bude možné až po skončení školního roku 2011/2012.

8 Seznam literatury

- 1) ŠILHÁN, J.: Operační systém Windows Mobile. [online]. 2008, http://www.silhan.net/wp-content/uploads/2009/10/xsilj101_BP.pdf
- 2) YAVAGAL, R. - TALUKDER A.: Mobile computing. 1. vydání. United States: McGraw-Hill, 2006. 672 s. ISBN 0071477330 / 9780071477338
- 3) ADELSTEIN, F. - GUPTA, S. - GOLDEN, R. - SCHWIEBERT, L.: Fundamentals of Mobile and Pervasive Computing. 1. vydání. United States: McGraw-Hill, 2004. 404 s. ISBN 0071412379 / 9780071412377
- 4) MICROSOFT CORPORATION. Microsoft System Center Mobile Device Manager 2008. [online]. <http://msdn2.microsoft.com/en-us/library/bb847932.aspx>
- 5) SYBASE. [online]. <http://www.sybase.com/>
- 6) BURLING, D.: Defining a Security Policy for Windows Mobile Pocket PCs. [online]. 2007, http://www.pocketpcmag.com/_archives/May0/securitypolicy.aspx
- 7) HUGHES, S.: Microsoft System Center Mobile Device Manager. [online]. 2008, <http://www.smartphonemag.com/cms/node/1327?page=0%2C0>
- 8) MICROSOFT CORPORATION. Microsoft System Center Mobile Device Manager 2008 Product Reference Guide. 2008. 43 s.
- 9) MICROSOFT CORPORATION. Microsoft System Center Mobile Device Manager 2008 Service Pack 1. [online]. <http://www.microsoft.com/windowsmobile/en-us/business/solutions/enterprise/mobile-device-manager.aspx>
- 10) MICROSOFT CORPORATION. System Center Mobile Device Manager Product Documentation. [online]. 2008, <http://technet.microsoft.com/en-us/scmdm/cc304592.aspx>
- 11) MB MAGAZÍN. Windows Mobile 7 (Photon) pro nedočkavé spekulanty. [online]. 2008, <http://magazin.softimage.cz/windows-mobile-7-photon-pro-nedockave-spekulanty/>
- 12) SYBASE. Using Afaia trial Virtual Machine. 2009. 21 s.
- 13) SYBASE. Getting to Know Afaia 6.0. 2008. 113 s.
- 14) SUNNYSOFT. [online]. <http://www.sunnysoft.cz/>
- 15) WINDOWS MOBILE TODAY. [online]. <http://www.pocketpccity.com/>
- 16) ŽIVNÝ, P.: Historie Pocket PC. [online]. 2006, <http://www.pdasoft.cz/>
- 17) Procházka L.: Projekt laboratoře IT technologií. 2009
- 18) ALZA.CZ. MDA Mivvy Zero. [online]. 2010, <http://www.alza.cz/mivvy-zero-d148245.htm>
- 19) ALZA.CZ. Samsung Omnia II i8000. [online]. 2010,

- <http://www.alza.cz/samsung-omnia-ii-i8000-d144154.htm>
20) ALZA.CZ. MDA Gygabyte GSmart MS802. [online]. 2010,
<http://www.alza.cz/gigabyte-gsmart-ms802-d142777.htm>

9 Seznam zkratek

- ARM** – Advanced RISC(Reduced Instruction Set Computer – Procesor s omezenou instrukční sadou) Machine - je RISC procesor založený na Von Neumannově architektuře
- CMOS** – Complementary Metal – Oxide – Semiconductor – technologie používaná pro integrované obvody
- COM** – Seriový port
- CSV** – Comma separated values – jednoduchý tabulkový formát pro výměnu tabulkových dat
- EDGE** – Enhanced Data Rates for Global Evolution – technologie pro přenos dat na paketovém principu
- FAT** – File allocation table – souborový systém používaný mnoha operačními systémy
- FTP** – File Transfer Protocol – protokol pro přenos dat mezi počítači
- GB** - Giga Bajt – jednotka velikosti informace
- GPRS** – General Pocket Radio Service – mobilní datová služba
- GPS** – Global Position System – družicový navigační systém
- GSM** – Global System for Mobile communications – světový standard pro mobilní telefony
- GUI** - Graphic User Interface – uživatelské grafické rozhraní
- HP** – Hewlett Packard – firma zabývající se výrobou hardware zařízení včetně kapesních počítačů
- HTTP** – Hypertext Transfer Protocol – internetový protokol pro přenos a výměnu dat
- HVGA** – Half-size Video Graphics Array – rozlišení 480*320 pixelů
- IP** – Internet Protocol – IP adresa identifikuje určité zařízení v internetu
- IrDA** – Infrared Data Association – infračervený port
- LAN** – Local Area Network – místní síť
- LCD** – Liquid Crystal display – monitor z tekutých krystalů
- MDA** – Mobile Digital Assistant – PDA obsahující GSM modul
- MIPS** – Microprocessor without Interlocked Pipeline Stages – architektura procesorů RISC
- MMC** – Multi Media Card – paměťové karty založené na paměti typu flash
- MS** - Microsoft
- OS** – Operační systém
- PC** – Personal Computer – Osobní počítač
- PCMCIA** – Personal Computer Memory Cards International Association – rozšiřující slot pro přídatné periferie
- PDA** – Personal Digital Assistant – kapesní počítač
- QWERTY** – počítačová klávesnice – název podle pořadí kláves v první řadě
- RAM** – Random Access Memory – paměť jejíž obsah je závislý na napájení

RDA - Remote Data Access – služba, která umožňuje vzdálený přístup k datům

ROM – Read Only Memory – paměť jejíž obsah je nezávislý na napájení

SD – Secure Digital – formát paměťových karet s pamětí typu flash

SDIO – Secure Digital Input Output – slot pro mobilní periferie

SQL – Structured Query Language – dotazovací jazyk pro práci s daty v relačních databázích

TCP/IP – Transmission Control Protocol/ Internet Protocol – sada protokolů internetu

USB – Universal Serial Bus – univerzální sériová sběrnice

VGA - Video Graphics Array – rozlišení 640*480 pixelů

VOIP – Voice Over Internet Protocol – protokol pro IP telefonii (volání přes internet)

WAN – World Area Network – světová síť

Wi-Fi – Wireless LAN – bezdrátová lokální síť

WM – Windows Mobile

OTA – Over The Air - zapsání zařízení do systému bezdrátového připojení

WSUS - Windows Software Update Services

OMA DM - Open Mobile Alliance Device Management – protokol pro správu mobilních zařízení

VPN – Virtual Private Network – virtuální privátní síť

DMZ – „demilitarizovaná zóna“ – okrajová síť, která chrání před útokem podnikovou síť.

SSL – Secure Socket Layer – je vrstva vložená mezi transportní a aplikační vrstvu, která poskytuje zabezpečení komunikace šifrováním.

IPSec – je bezpečnostní rozšíření IP protokolu založené na autentizaci a šifrování každého datagramu.

POP – Post Office Protocol – protokol pro přenos e-mailových zpráv

IMAP – Internet Message Access Protocol – protokol pro vzdálený přístup k e-mailové schránce.

UDP – User Datagram Protocol – protokol pro přenos dat, je nespolehlivý a nespojovaný.

MDM – Mobile Device Manager

LOB application– Line of Business aplikace – jsou aplikace, které jsou důležité pro chod organizace.

LDAP - Lightweight Directory Access Protocol – protokol pro přístup k datům na adresářovém serveru.

10 Seznam obrázků

obrázek č. 1 – Architektura Windows CE [1]	15
obrázek č. 2 – Obrazovka Dnes [1]	18
obrázek č. 3 – architektura Mobile Device Manageru 2008 SP1 [8]	27
obrázek č. 4 – Pre-Enrollment wizard [8]	29
obrázek č. 5 – Konfigurace serverů [8]	31
obrázek č. 6 – Autentizace mobilního zařízení [8]	32
obrázek č. 7 – Instalační CD MDM 2008 SP1 [printscreens autora]	36
obrázek č. 8 – Instalace databáze [printscreens autora]	37
obrázek č. 9 – Zablokování připojení zařízení [printscreens autora]	38
obrázek č. 10 – architektura Afarie [13]	41
obrázek č. 11 – Channel Viewer user interface [printscreens autora]	44
obrázek č. 12 – Create client Installation [printscreens autora]	45
obrázek č. 13 – Software catalog editor [printscreens autora]	45
obrázek č. 14 – Afaria OTA Publisher [printscreens autora]	45
obrázek č. 15 – Afaria Administrator [printscreens autora]	46
obrázek č. 16 – schéma spojení Relay serveru [13]	48
obrázek č. 17 – Použitá klientská zařízení v	54
obrázek č. 18 – Nastavení komunikace s klienty [printscreens autora]	54
obrázek č. 19 – Active session [printscreens autora]	55
obrázek č. 20 – Status serveru [printscreens autora]	55
obrázek č. 21 – Učební plán oboru Informační technologie [17]	59
obrázek č. 22 – laboratoř IT technologií [17]	70
obrázek č. 23 – laboratoř IT technologií – 3D [17]	70