ZMLUVA O DIELO Č. 003/2013/V

1.	**Objednávateľ:**	**Slovenská zdravotnícka univerzita v Bratislave**
	Sídlo:	Limbová 12, 833 30 Bratislava 37
	V zastúpení:	Dr. h. c. prof. PhDr. Dana Farkašová, CSc.
	Bankové spojenie:	
	Číslo účtu :	
	IČO:	00165361
	DIČ:	2020341895
	IČ DPH:	SK2020341895
	Zriadený zákonom č. 401/2002 Z. z.	
	(ďalej len „Objednávateľ“)	

2.	**Zhotoviteľ:**	**LYNX – spoločnosť s ručením obmedzeným Košice**
	Sídlo	Gavlovičova 9, 040 17 Košice
	V zastúpení**:**	Ladislav Plánka, konateľ
	Bankové spojenie:	
	Číslo účtu :	
	IČO:	00692069
	DIČ:	2020482871
	IČ DPH:	SK2020482871
	Zapísaný v Obchodnom registri	Okresný súd Košice I. , oddiel: Sro, vložka č. 117/V
	(ďalej len „Zhotoviteľ“)	

uzavreli túto **Zmluvu o dielo** v súlade s ustanovením § 536 a nasledujúcich zákona č. 513/1991 Z. z., Obchodný zákonník, v znení neskorších predpisov
(ďalej len “Zmluva”)

Zmluvné strany, vedomé si svojich záväzkov v tejto Zmluve obsiahnutých a s úmyslom byť touto Zmluvou viazané, dohodli sa na nasledujúcom znení Zmluvy:

1. ZÁKLADNÉ USTANOVENIA A ÚČEL ZMLUVY

1.1. Objednávateľ vyhlásil v súlade so zákonom č. 25/2006 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov nadlimitnú zákazku postupom verejnej súťaže na dodávku informačného systému pre podporu výskumu, vývoja a vzdelávania, ktorého cieľom je zaviesť unifikáciu agendy výskumu a vývoja v rámci univerzity a umožniť realizáciu výskumno-vývojových aktivít v oblasti skríningu novorodencov a telemedicíny. Oznámenie o vyhlásení verejného obstarávania na zadanie predmetnej zákazky (ďalej len „verejná súťaž“) bolo uverejnené v Úradnom vestníku Európskej únie S139 zo dňa 21/07/2012 pod značkou 2012/S 139-232629 a vo Vestníku verejného obstarávania č. 138/2012 zo dňa 20.7.2012 pod značkou 08487 – MSS.

1.2. Predmet zmluvy sa realizuje v rámci štrukturálnych fondov EÚ, 2620002 OP Výskum a vývoj, Výskum a vývoj.

a) Prioritná os 1 Infraštruktúra výskumu a vývoja, opatrenie 1.1 Obnova a budovanie technickej infraštruktúry výskumu a vývoja s cieľom zvýšenia schopnosti inštitúcií výskumu a vývoja efektívne spolupracovať s výskumnými inštitúciami v EÚ a v zahraničí, ako aj so subjektmi spoločenskej a hospodárskej praxe prostredníctvom transferu poznatkov a technológií, názov projektu „Modernizácia technickej infraštruktúry výskumu a vývoja na FZ Slovenskej zdravotníckej univerzity v Bratislave s orientáciou na moderné trendy v zdravotníctve.“

b) Prioritná os 4 Podpora výskumu a vývoja v Bratislavskom kraji, opatrenie 4.1 Podpora sietí excelentných pracovísk výskumu a vývoja ako pilierov rozvoja regiónu v Bratislavskom kraji s cieľom zvyšovania kvality výskumných pracovísk a podpory excelentného výskumu v Bratislavskom kraji s dôrazom na oblasti so strategickým významom pre ďalší rozvoj hospodárstva a spoločnosti, názov projektu „Centrum excelentnosti environmentálneho zdravia“

c) Prioritná os 5 Infraštruktúra vysokých škôl, Opatrenie 5.1 Budovanie infraštruktúry vysokých škôl a modernizácia ich vnútorného vybavenia s cieľom zlepšiť podmienky vzdelávacieho procesu, názov projektu „Zvýšenie kvality vzdelávacieho procesu na SZU, prostredníctvom rekonštrukcie a modernizácie hmotnej infraštruktúry“

Zhotoviteľ sa preto zaväzuje:

1.2.1. pristúpiť na zmenu zmluvy o dielo, v prípade, že táto zmena bude vyvolaná neposkytnutím nenávratného finančného príspevku (NFP) pre projekty v zmysle 1.2 bod a) a c), zmenou zmluvy o poskytnutí nenávratného finančného príspevku, ktorú má objednávateľ uzavretú s Agentúrou MŠ SR pre štrukturálne fondy alebo zmenou príručky pre prijímateľa NFP

1.2.2. strpieť výkon kontroly/auditu/overovania súvisiaceho s predmetom plnenia počas platnosti a účinnosti zmluvy o poskytnutí NFP, ktorú má verejný obstarávateľ uzatvorenú s poskytovateľom nenávratných finančných príspevkov, a to oprávnenými osobami v zmysle článku 12 Všeobecných zmluvných podmienok (príloha č. 1 zmluvy o poskytnutí NFP) a poskytnúť im všetku potrebnú súčinnosť.

1.3. Zhotoviteľ sa zaväzuje nezačať s realizáciou časti diela uvedenej v bode 1.2 a) a c) dovtedy, pokiaľ Objednávateľ písomne neoznámi Zhotoviteľovi pridelenie finančných prostriedkov na uvedenú časť Diela. Zhotoviteľ je povinný uvedenú žiadosť akceptovať bez nároku Zhotoviteľa na finančnú náhradu za uvedenú časť. V prípade vzniku takéhoto skutkového stavu sa v zmluve za uvádzaný predmet zmluvy „Dielo“ považuje samostatne časť zodpovedajúca projektu „Modernizácia technickej infraštruktúry výskumu a vývoja na FZ Slovenskej zdravotníckej univerzity v Bratislave s orientáciou na moderné trendy v zdravotníctve.“, samostatne časť zodpovedajúca projektu „Centrum excelentnosti environmentálneho zdravia“ a samostatne časť zodpovedajúca projektu „Zvýšenie kvality vzdelávacieho procesu na SZU, prostredníctvom rekonštrukcie a modernizácie hmotnej infraštruktúry“

1.4. Zhotoviteľ prehlasuje, že spĺňa všetky podmienky a požiadavky v tejto Zmluve stanovené a je oprávnený túto Zmluvu uzavrieť a riadne plniť záväzky v nej obsiahnuté.

1.5. Objednávateľ prehlasuje, že spĺňa všetky podmienky a požiadavky v tejto Zmluve stanovené a je oprávnený túto Zmluvu uzavrieť a riadne plniť záväzky v nej obsiahnuté.

2. PREDMET ZMLUVY

2.1. Zhotoviteľ sa touto Zmluvou zaväzuje vykonať pre Objednávateľa dielo, ktorým sa rozumie dodanie informačného systému pre podporu výskumu, vývoja a vzdelávania na Slovenskej Zdravotníckej univerzite, pričom rozsah funkcionalít je ďalej špecifikovaný v Prílohe č. 1. tejto Zmluvy (ďalej len „Dielo“), a to za cenu a podmienok ďalej stanovených v tejto Zmluve.

2.2. Objednávateľ sa touto Zmluvou zaväzuje uhradiť Zhotoviteľovi za poskytnuté plnenia cenu podľa tejto Zmluvy.

2.3. Objednávateľ sa touto Zmluvou ďalej zaväzuje poskytnúť Zhotoviteľovi súčinnosť potrebnú pre plnenie záväzkov Zhotoviteľa, a to minimálne v rozsahu stanovenom v Implementačnom projekte.

2.4. Súčasťou plnení podľa tejto Zmluvy nie je poskytnutie zdrojových textov k softvéru ani dodanie podkladových materiálov potrebných na jeho prípravu.

3. DOBA PLNENIA

3.1. Plnenia podľa tejto Zmluvy sa Zhotoviteľ zaväzuje odovzdať Objednávateľovi v termínoch špecifikovaných v Implementačnom projekte, ak nie je Zmluvou stanovené inak.

3.2. V prípade omeškania Objednávateľa s úhradou faktúr, alebo v prípade omeškania s poskytnutím potrebnej súčinnosti podľa tejto Zmluvy, je Zhotoviteľ oprávnený po písomnom upozornení Objednávateľa na takéto omeškania pozastaviť práce na zhotovovaní Diela (úplne alebo čiastočne), dokiaľ nedôjde zo strany Objednávateľa k náprave. Ak dôjde k zastaveniu prác podľa tohto odseku, má Zhotoviteľ nárok na úhradu účelne vynaložených nákladov, ktoré mu vznikli v súvislosti so zastavením a následným obnovením prác.

Termíny plnenia zo strany Zhotoviteľa sa predlžujú o dobu zastavenia prác ako aj o ďalšiu primeranú dobu, potrebnú pre opätovné obnovenie plnení Zhotoviteľa.

4. MIESTO PLNENIA

4.1. Miesto plnenia je:

- Stredné Slovensko, Banskobystrický kraj, okres Banská Bystrica, mesto Banská Bystrica;
- Západné Slovensko, Bratislavský kraj, okres Bratislava, mesto Bratislava

5. CENA A PLATOBNÉ PODMIENKY

5.1. Zmluvné strany sa dohodli na nasledovnom spôsobe platenia ceny za Dielo a licencie podľa tejto Zmluvy (ďalej len „cena“).

5.2. Cena za vykonanie Diela je 3 352 083,33 EUR (slovom: Trimiliónytristopäťdesiatdvatisícosemdesiattri EUR, tridsaťtri centov) bez DPH, ktorú objednávateľ uhradí po odovzdaní a prevzatí Diela, resp. po odovzdaní a prevzatí jeho ucelenej časti. Zhotoviteľ má právo na čiastkovú fakturáciu po riadnom odovzdaní a prevzatí časti Diela na základe príslušného protokolu.

5.3. Zmluvné strany sa dohodli, že cena Diela, resp. jeho ucelených častí bude zaplatená na základe faktúr vystavených Zhotoviteľom. K predmetu zmluvy bude fakturovaná DPH v zmysle Zákona č. 222/2004 Z. z. o DPH v platnom znení.

5.4. Splatnosť faktúr je deväťdesiat (90) kalendárnych dní odo dňa doručenia faktúr.

5.5. Faktúra sa považuje za doručenú aj keď bolo jej prevzatie Objednávateľom bezdôvodne odopreté, alebo ak sa ju nepodarilo doručiť aj keď bola zaslaná na adresu sídla Objednávateľa, alebo na dodatočne oznámenú doručovaciu adresu Objednávateľa, a to tretím (3.) pracovným dňom po jej preukázateľnom odoslaní.

5.6. Ak faktúra nebude obsahovať náležitosti v zmysle Zákona č. 222/2004 Z.z. o DPH v znení neskorších predpisov a náležitosti vyplývajúce z tejto Zmluvy, je Objednávateľ oprávnený vrátiť faktúru na prepracovanie Zhotoviteľovi v lehote piatich (5) kalendárnych dní od jej doručenia Objednávateľovi. Objednávateľ uvedie chýbajúce náležitosti alebo nesprávne údaje. V takom prípade sa preruší plynutie lehoty splatnosti a nová lehota začne plynúť doručením opravenej faktúry.

5.7. Ak Objednávateľ faktúru vráti bezdôvodne, bez uvedenia chýb alebo po dohodnutom termíne, lehota splatnosti sa nepreruší. Tým nie je dotknutá povinnosť Zhotoviteľa dodať Objednávateľovi opravenú faktúru.

5.8. Faktúra zhotoviteľa musí obsahovať najmä nasledovné údaje:

- označenie „faktúra“ a jej číslo,
- obchodné meno a sídlo objednávateľa
- obchodné meno a sídlo zhotoviteľa,
- názov projektu a kód ITMS projektu,,
- číslo a názov Zmluvy,
- názov a adresa banky zhotoviteľa,
- číslo účtu zhotoviteľa,
- požadovaná cena bez DPH, výška DPH a cena s DPH v EUR zaokrúhlená na dve desatinné miesta spolu a v členení:
  - jednotková cena druhu tovaru/služby
  - počet jednotiek
  - celková cena druhu tovaru/služby za fakturovaný počet jednotiek
- náležitosti pre účely DPH,
- podpis zodpovednej osoby.

5.9. Faktúry budú uhrádzané bezhotovostných prevodom na bankový účet uvedený na faktúre.

5.10. V prípade omeškania Objednávateľa s úhradou faktúr, môže Zhotoviteľ požadovať zmluvnú pokutu vo výške 0,04 % z dlžnej sumy za každý deň omeškania. Tým nie je dotknutý ani obmedzený nárok oprávnenej strany na náhradu vzniknutej škody.

5.11. V prípade, ak sa Zhotoviteľ vlastným pričinením dostane do omeškania s plnením si svojich povinností podľa tejto zmluvy, Objednávateľ môže uplatniť voči nemu zmluvnú pokutu vo výške 0,04 % z ceny predmetu plnenia z tej časti diela s ktorým je v omeškaní a to za každý aj začatý deň omeškania.

5.12. Zmluvné strany sa dohodli, že v cenách uvedených v tejto zmluve sú už zahrnuté všetky náklady Zhotoviteľa, ktoré v súvislosti s plnením predmetu tejto zmluvy vynaloží.

6. SPÔSOB ZHOTOVENIA DIELA

6.1. Rozsah a spôsob zhotovenia Diela bude špecifikovaný v dokumente Implementačný projekt v štruktúre podľa Prílohy č. 2, ktorý spracuje Zhotoviteľ na základe analýzy súčasnej situácie a špecifikácie požiadaviek Objednávateľa v rozsahu stanovenom touto Zmluvou, Prílohou č.1, ktorý bude vypracovaný v termíne do 60 dní odo dňa účinnosti zmluvy.

6.2. Cieľom Implementačného projektu je špecifikovať spôsob plnenia diela, podrobné časové plnenie a spolupôsobenie objednávateľa ako aj stanovenie akceptačných kritérií pre prevzatie Diela.

6.3. Akceptáciou Implementačného projektu sa Implementačný projekt stáva neoddeliteľnou súčasťou tejto Zmluvy. Termín na akceptáciu Implementačného projektu je zo strany Objednávateľa 15 dní odo dňa odovzdania Implementačného projektu Zhotoviteľom. Akceptácia Implementačného projektu bude potvrdená písomnou formou.

7. ZMENY DIELA V PRIEBEHU PLNENIA

7.1. Ktorákoľvek zo zmluvných strán je oprávnená navrhnúť písomne zmeny Diela pred jeho dokončením. Žiadna zo strán nie je povinná navrhnutú zmenu akceptovať.

7.2. Zhotoviteľ sa na písomnú výzvu Objednávateľa zaväzuje vyhodnotiť dôsledky Objednávateľom navrhnutých zmien Diela, ktoré budú zahŕňať hodnotenie dopadov takých zmien na cenu a rozsahu plnení, dohodnuté termíny odovzdaní a rozsah potrebnej súčinnosti (ďalej len „Špecifikácia dôsledkov“). Ak si podľa Zhotoviteľa vypracovanie Špecifikácie dôsledkov vyžiada dodatočné náklady alebo ak by jej vypracovanie mohlo mať negatívny dopad na plnenie záväzkov Zhotoviteľa podľa tejto Zmluvy, vypracuje Zhotoviteľ Špecifikáciu dôsledkov iba na základe písomnej dohody s Objednávateľom o úhrade nákladov na vypracovanie Špecifikácie dôsledkov a o úprave ďalších zmluvných podmienok, ktorých sa vypracovanie Špecifikácie dôsledkov môže dotknúť.

7.3. Akékoľvek zmeny Diela musia byť dohodnuté formou písomného dodatku k tejto Zmluve, ktorým dôjde k úprave zmluvných podmienok v súlade so Špecifikáciou dôsledkov v súlade s dohodou zmluvných strán, ak nie je v konkrétnom prípade touto Zmluvou stanovené inak.

8. ODOVZDANIE A PREVZATIE DIELA, RESP. JEHO ČASTI

8.1. Odovzdanie a prevzatie Diela, resp. jej častí podľa čl. 2.1 tejto Zmluvy prebieha prostredníctvom akceptačnej procedúry, ktorú tvoria akceptačné testy v súlade s akceptačnými kritériami. Akceptačné kritéria pre Dielo, resp. jeho časti sú stanovené v Implementačnom projekte. Cieľom akceptačných testov je porovnať vlastnosti Diela, resp. jeho časti s dohodnutou špecifikáciou.

8.2. Zhotoviteľ odovzdá Dielo, resp. jeho časti k akceptačnej procedúre v termínoch špecifikovaných v Implementačnom projekte.

8.3. Akceptačné testy vykonáva Objednávateľ. Zhotoviteľ je oprávnený sa ich vykonania zúčastniť. Objednávateľ je povinný oznámiť Zhotoviteľovi termín a miesto vykonania akceptačných testov najneskôr tri (3) pracovné dni vopred.

8.4. Objednávateľ je povinný zahájiť akceptačné testy do piatich (5) pracovných dní od prevzatia diela alebo jeho časti k akceptačnej procedúre. Akceptačná procedúra musí byť ukončená do piatich (5) pracovných dní od jej zahájenia, ak nie je v Implementačnom projekte stanovená iná lehota.

8.5. Dielo, resp. jeho časti sú považované za akceptované bez výhrad, ak nie sú v priebehu akceptačnej procedúry zistené žiadne vady.

8.6. Ak v rámci akceptačných testov nie sú splnené podmienky pre akceptáciu (bez výhrad či s výhradami), oznámi Objednávateľ vady Zhotoviteľovi písomne najneskôr do troch (3) pracovných dní odo dňa uplynutia lehoty pre vykonanie akceptačných testov. V takom oznámení je Objednávateľ povinný vady dostatočne popísať, vrátane ich kategorizácie.

8.7. V prípade, že Objednávateľ oznámil Zhotoviteľovi vady, ktoré bránia akceptácii Diela, resp. jeho časti, v súlade s touto Zmluvou, zaväzuje sa Zhotoviteľ také vady bez zbytočného omeškania odstrániť a odovzdať Dielo, resp. jeho časť k opakovaným akceptačným testom. Predchádzajúce ustanovenia tohto článku sa použijú obdobne. Predmetom opakovaných akceptačných testov je overenie či boli oznámené vady riadne odstránené. Objednávateľ však nie je oprávnený v ich rámci uplatniť vady, ktoré mohol a mal zistiť a oznámiť v rámci predchádzajúcich akceptačných testov.

8.8. Ak v rámci akceptačných testov nebudú zistené vady, brániace akceptácii Diela, resp. jeho časti, považuje sa Dielo, resp. jeho časť za riadne prevzaté, o čom je Objednávateľ povinný Zhotoviteľa písomne informovať bez zbytočného omeškania. O prevzatí podpíšu zmluvné strany akceptačný protokol, ktorého vzor je súčasťou Implementačného projektu, a to najneskôr do troch (3) pracovných dní odo dňa uplynutia lehoty pre vykonanie akceptačných testov.

8.9. Zmluvné strany sa výslovne dohodli, že Dielo, resp. jeho časť budú považovať za riadne prevzaté aj keď:

8.9.1. Objednávateľ začal Dielo, resp. jeho časť používať pre iné účely, ako pre účely vykonania akceptačných testov alebo umožnil také používanie tretej osobe, najmä keď Objednávateľ začal Dielo, resp. jeho časť používať v rámci rutinnej prevádzky,

8.9.2. Objednávateľ riadne a včas neoznámil Zhotoviteľovi vady, ktoré bránia prevzatí Diela, resp. jeho časti.

8.10. Predchádzajúce ustanovenia sa nepoužijú pre prevzatie dokumentácie, ktorú Zhotoviteľ poskytuje v súladu s touto Zmluvou.

9. ODOVZDANIE A PREVZATIE DOKUMENTÁCIE

9.1. Dokumentáciou sa rozumie dokumentácia k Dielu, resp. jeho časti, potrebná pre účelné používanie Diela, resp. jeho časti ako aj dokumentácia k technickému a systémovému vybaveniu, ak je poskytované na základe tejto Zmluvy.

9.2. Dokumentácia pre technické a systémové vybavenie pozostáva z dokumentácie, ktorá je súčasťou dodávky príslušného vybavenia od jeho výrobcu.

9.3. Zhotoviteľ sa zaväzuje dodať Objednávateľovi dokumentáciu k Dielu, resp. jeho časti v papierovej alebo elektronickej podobe.

9.4. Zhotoviteľ touto Zmluvou poskytuje Objednávateľovi právo celú dokumentáciu k dielu kopírovať a používať iba v nevyhnutnom rozsahu pre vlastnú internú potrebu Objednávateľa.

9.5. Prevzatiu dokumentácie nebránia gramatické, štylistické ani iné podobné chyby, ktoré nemajú vplyv na použiteľnosť dokumentácie k Dielu, resp. jeho časti. Rovnako toto ustanovenie platí aj pre ostatné oznámenia alebo dokumenty vzniknuté v priebehu plnenia Zmluvy.

10. VLASTNÍCKE PRÁVO A PRÁVA POUŽITIA

10.1. Vlastnícke právo k Dielu, resp. jeho uceleným častiam, ktoré sa má podľa tejto Zmluvy stať vlastníctvom Objednávateľa, nadobúda Objednávateľ dňom úplného zaplatenia ceny Diela, resp. jeho ucelených častí podľa tejto Zmluvy. Na dobu od dodania takých vecí do dňa úplného zaplatenia ceny podľa tejto Zmluvy udeľuje Zhotoviteľ Objednávateľovi právo takú vec užívať v rozsahu a k účelu podľa tejto Zmluvy. Toto právo môže Zhotoviteľ kedykoľvek odobrať, pokiaľ bude Objednávateľ v omeškaní so zaplatením ceny.

10.2. Ak je súčasťou plnení podľa tejto Zmluvy autorské dielo v zmysle ust. § 7 zákona č. 618/2003 Z. z., o autorskom práve a právach súvisiacich s autorským právom, v znení neskorších predpisov (ďalej len „autorský zákon"), poskytuje Zhotoviteľ Objednávateľovi licenciu na používanie autorského diela v súlade a s účelom podľa tejto Zmluvy, a to s účinnosťou odo dňa dodania takého autorského diela. Cena za poskytnutie licencie k autorským dielam podľa tohto odseku je zahrnutá v cene Diela podľa tejto Zmluvy.

10.3. Licencie podľa tejto Zmluvy sa udeľujú ako nevýhradné, neprevoditeľné, v rozsahu obmedzenom na územie Slovenskej republiky a na dobu trvania majetkových autorských práv.

10.4. Objednávateľ je oprávnený používať autorské diela v súlade s ich funkčným vymedzením podľa tejto Zmluvy a v súlade s pokynmi poskytnutými formou dokumentácie či v rámci zaškolenia. Ak táto Zmluva nestanoví inak, Objednávateľ nemá oprávnenie zasahovať alebo upravovať autorské dielo s výnimkou zásahov, ktoré v súlade s donucujúcimi ustanoveniami právnych predpisov nevyžadujú súhlas poskytovateľa licencie.

10.5. Predchádzajúce ustanovenia tohto článku sa nevzťahujú na systémové vybavenie, ak je poskytované v súlade s touto Zmluvou. Používateľské práva Objednávateľa vo vzťahu k systémovému vybaveniu sú špecifikované v tejto Zmluve a/alebo v dokumentácii, poskytnuté Zhotoviteľom spoločne s takýmto vybavením.

10.6. V prípade porušenia podmienok licencie zo strany Objednávateľa vzniká Zhotoviteľovi nárok na náhradu vzniknutej škody.

10.7. Zmluvné strany výslovne vyhlasujú, že ak pri vykonávaní Diela vznikne činnosťou Zhotoviteľa a Objednávateľa dielo spoluautorov podľa autorského zákona, dohodnú sa strany na spôsobe vysporiadania vzájomných práv k takému dielu, a to bez zbytočného omeškania odo dňa, kedy k tomu jedna strana druhú strany vyzve.

11. PRÁVA A POVINNOSTI ZMLUVNÝCH STRÁN

11.1. Zhotoviteľ sa touto Zmluvou zaväzuje:

11.1.1. zhotoviť Dielo, resp. jeho časti podľa tejto Zmluvy riadne a včas s potrebnou odbornou starostlivosťou a v súlade s podmienkami určenými:

- zmluvou o poskytnutí nenávratného finančného príspevku v znení jej dodatkov, ktorú má Objednávateľ uzavretú s poskytovateľom nenávratného finančného príspevku (ďalej NFP), t.j. s Ministerstvom školstva Slovenskej republiky pre projekty uvedené v bode 1.2 a) až c);
- príručkou pre prijímateľa NFP 2620002 OP Výskum a vývoj a jej aktualizovaným platným znením.

11.1.2. pri vykonávaní prác v sídle Objednávateľa dodržiavať platné a účinné predpisy o ochrane bezpečnosti práce a zdravia pri práci, požiarnej ochrany, hygieny práce a životného prostredia;

11.1.3. zaistiť, aby jeho pracovníci dodržiavali všetky interné predpisy Objednávateľa, s ktorými boli Objednávateľom vopred oboznámení;

11.1.4. chrániť práva duševného vlastníctva patriace Objednávateľovi ako aj práva tretích osôb, ktoré by mohli byť plnením Zmluvy dotknuté.

11.2. Zhotoviteľ je oprávnený poskytnúť výsledok činnosti, ktorý je predmetom Diela, resp. jeho časti, aj iným osobám než je Objednávateľ.

11.3. Objednávateľ sa touto Zmluvou zaväzuje umožniť Zhotoviteľovi plnenia podľa tejto Zmluvy, spolupracovať so Zhotoviteľom pri plnení tejto Zmluvy, najmä mu s dostatočným predstihom poskytovať vždy súčinnosť,

úplné, pravdivé a včasné informácie potrebné pre riadne plnenie záväzkov Zhotoviteľa, a to v rozsahu najmenej podľa Implementačného projektu.

11.4. Objednávateľ sa zaväzuje pri vykonávaní prác zamestnancami Zhotoviteľa v sídle Objednávateľa a na jeho pracoviskách:

11.4.1. zabezpečiť v zmysle § 6 ods. 4 a nadväzne na § 7 ods. 6 písm. a) až c) zákona NR SR č. 124/2006 Z. z., aby zamestnanci Zhotoviteľa dostali potrebné pokyny pre bezpečnosť a na ochranu zdravia pri práci platné pre jeho pracoviská a informácie o možných ohrozeniach, preventívnych opatreniach, opatreniach na poskytnutie prvej pomoci, na vykonanie záchranných prác a na evakuáciu osôb,

11.4.2. vytvoriť podmienky pre bezpečnosť a na ochranu zdravia pri práci, zároveň v prípade potreby zabezpečiť pre zamestnancov Zhotoviteľa osobné ochranné pracovné prostriedky,

11.4.3. splniť povinnosti uvedené v bodoch 11.4.1 a 11.4.2 pred začatím výkonu práce zamestnancami Zhotoviteľa.

11.4.4. postupovať v zmysle § 17 ods. 6 zákona NR SR č. 124/2006 Z.z. v prípade, že zamestnanec Zhotoviteľa utrpí pracovný úraz.

12. ZÁRUKA

12.1. Zhotoviteľ vyhlasuje, že Dielo, resp. jeho časti má ku dňu prevzatia funkčné vlastnosti uvedené v tejto Zmluve a je oprostené právnych vád.

12.2. Záruka sa poskytuje na dobu dvadsať štyri (24) mesiacov. Záručná doba začína plynúť dňom prevzatia Diela, resp. jeho časti.

13. OPRÁVNENÉ OSOBY

13.1. Každá zo zmluvných strán menuje oprávnené osoby, ktoré za ňu budú jednať v súvislosti s plnením podľa tejto Zmluvy.

13.2. Mená oprávnených osôb, ako aj rozsah ich pôsobnosti, sú uvedené v Prílohe č. 3 tejto Zmluvy. Zmluvné strany sú oprávnené jednostranne meniť oprávnené osoby, a to písomným oznámením druhej strane. Zmena oprávnenej osoby nie je považovaná za zmenu tejto Zmluvy.

13.3. Zmluvné strany sa dohodli, že v prípade, ak sa Zhotoviteľ dostane do styku s osobnými údajmi nachádzajúcimi sa v informačných systémoch Objednávateľa, zaväzuje sa tieto údaje použiť výlučne len na splnenie predmetu tejto Zmluvy a tieto osobné údaje je povinný chrániť pred náhodným, ako aj nezákonným poškodením a zničením, náhodnou stratou, zmenou, nepovoleným prístupom a sprístupnením, ako aj pred akýmikoľvek inými neprípustnými formami spracúvania podľa zákona č. 428/2002 Z.z. o ochrane osobných údajov. Na tento účel je Zhotoviteľ povinný prijať primerané technické, organizačné a personálne opatrenia. Tým nie je dotknutá povinnosť Objednávateľa splniť si všetky ohlasovacie povinnosti podľa zákona a získať súhlas na spracúvanie osobných údajov dotknutých osôb, ak v dôsledku plnenia predmetu tejto zmluvy dôjde k spracovaniu osobných údajov zo strany Zhotoviteľa.

14. RIEŠENIE SPOROV

14.1. Zmluvné strany sa zaväzujú, že vyvinú maximálne úsilie k odstráneniu prípadných sporov vyplývajúcich z tejto Zmluvy vzájomnou dohodou.

14.2. Všetky spory, ktoré vzniknú z tejto Zmluvy, vrátane sporov o jej platnosť, výklad alebo zrušenie, budú riešené príslušným súdom SR.

15. TRVANIE ZMLUVY

15.1. Táto zmluva nadobúda platnosť dňom jej podpísania oboma zmluvnými stranami a účinnosť najskôr dňom nasledujúcim po dni jeho zverejnenia v Centrálnom registri zmlúv. Zmluva sa uzatvára na dobu určitú 36 mesiacov odo dňa nadobudnutia jej platnosti a účinnosti, pričom lehota plnenia diela, resp. jeho časti je 12 mesiacov odo dňa účinnosti zmluvy.

15.2. Zmluvné strany sú oprávnené odstúpiť od Zmluvy iba z dôvodov stanovených touto Zmluvou.

15.3. Ktorákoľvek zmluvná strana môže odstúpiť od tejto Zmluvy z dôvodu podstatného porušenia záväzku druhej zmluvnej strany.

15.4. Za podstatné porušenie záväzku sa považuje omeškanie s plnením záväzku zmluvnej strany, ktoré trvá po dobu viac ako tridsať (30) kalendárnych dní, ak povinná zmluvná strana nezjedná nápravu ani v dodatočnej lehote, ktorú jej poskytne oprávnená zmluvná strana v písomnom oznámení, v ktorom špecifikuje porušenie záväzku, ktorého sa dovoláva. Dodatočná lehota nesmie byť kratšia ako pätnásť (15) kalendárnych dní.

15.5. Ktorákoľvek zmluvná strana môže odstúpiť od tejto Zmluvy aj bez uvedenia dôvodu, a to s účinnosťou uplynutím troch (3) mesiacov odo dňa doručenia písomného oznámenia o odstúpení druhej strane. V takom prípade nadobúda Objednávateľ vlastnícke a používateľské právo k všetkým plneniam, ktoré mu boli Zhotoviteľom poskytnuté do účinnosti odstúpení, a to v rozsahu vyplývajúcom z tejto Zmluvy; a súčasne vzniká Objednávateľovi záväzok uhradiť Zhotoviteľovi cenu za tieto plnenia. Odstúpenie od Zmluvy podľa tohto odseku sa nedotýka tejto Zmluvy v rozsahu, v ktorom upravuje výšku ceny poskytnutých plnení a podmienky jej zaplatenia, nárok na náhradu vzniknutej škody ako aj používateľské práva k poskytnutým plneniam.

15.6. Odstúpenie od Zmluvy nemá vplyv na plnenie Zhotoviteľa, ktoré bolo riadne odovzdané a bolo aj prijaté, alebo malo a mohlo byť prijaté pred nadobudnutím účinnosti odstúpenia. Odstúpením nie je dotknutý ani nárok Zhotoviteľa na zaplatenie ceny za také plnenie podľa tejto Zmluvy ani na prípadnú zmluvnú pokutu.

15.7. Odstúpením Zmluvy nie sú dotknuté ustanovenia týkajúce sa ochrany informácií, voľby práva a riešenia sporov.

15.8. Písomné odstúpenie od zmluvy je účinné dňom jeho doručenia druhej zmluvnej strane.

16. ZÁVEREČNÉ USTANOVENIA

16.1. Pokiaľ by sa ktorékoľvek ustanovenie vyplývajúce z tejto Zmluvy ukázalo ako neplatné či nevymáhateľné, alebo sa takým počas trvania účinnosti tejto Zmluvy stalo, nemá taká skutočnosť vplyv na ostatné ustanovenia, ak nestanoví inak donucujúce ustanovenie zákona. Zmluvné strany sa zaväzujú také ustanovenie nahradiť platným ustanovením, ktoré je svojím obsahom pôvodnému ustanoveniu najbližšie.

16.2. Práva a povinnosti zmluvných strán neupravené touto Zmluvou sa riadia právnymi predpismi Slovenskej republiky, najmä Obchodným zákonníkom a Autorským zákonom.

16.3. Neoddeliteľnou súčasťou Zmluvy sú tieto Prílohy:

Príloha č. 1	Špecifikácia a cena Diela
Príloha č. 2	Štruktúra Implementačného projektu
Príloha č. 3	Mená oprávnených osôb a rozsah ich pôsobnosti

16.4. Táto Zmluva je uzatvorená v štyroch (4) rovnopisoch, z ktorých každá zmluvná strana dostane dva (2).

Strany prehlasujú, že si túto Zmluvu prečítali, že s jej obsahom súhlasia a na dôkaz toho k nej pripojujú svoje podpisy.

Objednávateľ	**Zhotoviteľ**
V Bratislave, dňa 07.02.2013	V Bratislave, dňa 07.02.2013
.....	.....
Dr. h. c. prof. PhDr. Dana Farkašová Rektorka	Ladislav Plánka konateľ

Príloha č. 1 - Špecifikácia a cena Diela

Príloha č. 2 - Štruktúra Implementačného projektu

1. Účel projektu
1.1 Ciele projektu
1.2 Ohraničujúce podmienky a väzby na iné projekty
1.3 Súvisiaca legislatíva, normy, smernice a predpisy
2. Predmet projektu
2.1 Výstupy projektu
3. Súčinnosť zákazníka
4. Organizácia projektu
4.1 Personálne obsadenie funkcií projektového tímu zhotoviteľa
4.2 Personálne obsadenie funkcií projektového tímu zákazníka
4.3 Riadiaci výbor projektu
4.4 Popis funkcií
4.5 Kontrolný mechanizmus
5. Riadenie zmien
5.1 Predkladanie požiadaviek na zmeny
5.2 Riadenie zmien
6. Riadenie rizík
6.1 Oblasti rizík
6.2 Identifikácia rizík
6.3 Preventívne opatrenia
7. Postup zabezpečenia projektu
7.1 Termíny projektu
7.2 Plán etáp projektu
7.3 Popis etáp projektu
7.4 Požiadavky na infraštruktúru
7.5 Požiadavky na podporu
7.6 Definície a ustanovenia
7.7 Fyzické riadenie dokumentácie
8. Prílohy
Príloha č.1 - Matica zodpovednosti
Príloha č.2 - Matica činností
Príloha č.3 - Komunikačný plán
Príloha č.4 – Plán riadenia rizík

Príloha č. 3 Mená oprávnených osôb a rozsah ich pôsobnosti

Zoznam oprávnených osôb Objednávateľa:

Pozícia	Meno a priezvisko
Garant projektu	Dana Farkašová
Osoba oprávnená za zmluvné záležitosti	Oľga Švolíková
Projektový manažér	Jozef Hudák
Vedúci tímu pre časť Enviro	Štefan Kováč
Vedúci tímu pre časť Skríning	Radoslav Suchár
Vedúci tímu pre časť Telemedicína	Radoslav Suchár
Vedúci tímu pre časť Prierezové moduly	Radoslav Suchár

Zoznam oprávnených osôb Zhotoviteľa:

Pozícia	Meno a priezvisko
Garant projektu	Ladislav Plánka
Osoba oprávnená za zmluvné záležitosti	Ľubomír Szabados
Projektový manažér	Róbert Babinský
Architekt bezpečnosti	Dušan Kotora
Vedúci tímu pre časť Enviro	Ľuboš Veselovský
Vedúci tímu pre časť Skríning	Roman Hlubina
Vedúci tímu pre časť Telemedicína	Radoslav Bačár
Vedúci tímu pre časť Prierezové moduly	Ľuboš Modranský

Príloha č. 1 - Špecifikácia a cena Diela

Táto príloha tvorí neoddeliteľnú časť Zmluvy o dielo č. 003/2013/V (ďalej len „Zmluva“) uzavretej medzi zmluvnými stranami:

Objednávateľ: Slovenská zdravotnícka univerzita v Bratislave so sídlom Limbová 12, 833 30 Bratislava 37, v zastúpení rektorkou Dr. h. c. prof. PhDr. Danou Farkašovou, CSc., IČO 00165361, IČ DPH SK2020341895, Zriadenej zákonom č. 401/2002 Z. z. (ďalej len „Objednávateľ“)

a

Zhotoviteľ: LYNX – spoločnosť s ručením obmedzeným Košice so sídlom Gavlovičova 9, 040 17 Košice v zastúpení konateľom Ladislavom Plánkom, IČO 00692069, IČ DPH SK2020482871, zapísanou v Obchodnom registri Okresného súdu Košice I., oddiel: Sro, vložka č. 117/V (ďalej len „Zhotoviteľ“)

Obsahová časť ponuky plne korešponduje s ponukou Zhotoviteľa ponúknutou v rámci Verejnej súťaže č. VO 08487 – MSS zverejnenej vo vestníku č. 138/2012 zo dňa 20.7.2012 pre predmet zákazky “Informačný systém pre podporu výskumu, vývoja a vzdelávania Slovenskej zdravotníckej univerzity“.

V zmysle čl.1 bod 1.3. Zmluvy sa Zhotoviteľ zaväzuje dodať len tú časť Diela, na ktorú ho Objednávateľ písomne vyzve v podobe oznámenia o pridelení finančných prostriedkov pre uvedenú časť Diela (ďalej len Výzva).

1 Špecifikácia Diela

1.1 Bezpečnosť Diela

1.1.1 Analytická bezpečnosť

Vzhľadom k tomu, že informačný systém bude obsahovať a spracúvať osobné údaje, bude súčasťou jeho implementácie bezpečnostný projekt podľa požiadaviek zákona č. 428/2002 Z .z. Bezpečnostný projekt určí, ako bude potrebné údaje informačného systému chrániť a podľa akých kritérií. Bezpečnostný zámer bude ukončený pred začatím detailného návrhu riešenia informačného systému, aby sa jeho výsledky mohli včas zohľadniť a zapracovať. Analýza bezpečnosti informačného systému a bezpečnostná smernica bude súčasťou dokumentov odovzdávaných na akceptáciu.

Základné bezpečnostné princípy použité pre zabezpečenie ochrany osobných údajov budú:

a) Ochrana osobných údajov bude riešená pre informačný systém, v ktorom sa spracúvajú osobné údaje osobitnej kategórie s použitím automatizovaných prostriedkov spracúvania deklarovaním systému dôslednej implementácie bezpečnostných prvkov vo všetkých fázach SDLC, dodržaním princípov pre návrh systémov zabezpečujúcich vysoký stupeň ochrany.

b) Technické opatrenia a riešenie bezpečnosti rámci IS budú navrhované tak, aby chránili osobné údaje pred náhodným ako aj nezákonným poškodením a zničením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením ako aj pred akýmikoľvek inými neprípustnými formami spracúvania.

c) Osobné údaje budú v systéme spracovávané až po ukončení vývoja a to v ostrom, otestovanom a verifikovanom IS.

Nakoľko SZU je univerzitou v zriaďovateľskej pôsobnosti MZ SR, jej informačný systém bude súčasťou informačného systému verejnej správy, a preto sa budú naň vzťahovať všetky požiadavky zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a nadväzných predpisov hlavne výnosu MF SR č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy. Na základe toho splnením legislatívnych požiadaviek

budú splnené aj všetky Minimálne požiadavky verejného obstarávateľa kladené na vytvorenie bezpečnostného projektu vyžadované v súťažných podkladoch.

Viacúrovňová ochrana a rôzne aspekty bezpečnosti budú od začiatku časťou implementovanej architektúry, čo umožní budovať riešenia s primeranou úrovňou bezpečnosti služieb informačného systému. Bezpečnostný model bude flexibilný, podporujúci adaptáciu rôznych súčasných a budúcich bezpečnostných technológií s cieľom minimalizácie nutných budúcich zmien v návrhu integračného riešenia.

1.1.2 Technické prvky informačnej bezpečnosti

1.1.2.1 Východiská

- Modul Telemedicína bude realizovaný ako PoC len na testovacích údajoch t.j. bez ostrých údajov predstavujúcich osobné údaje.

- Predmetom ponuky je realizácia prác pre návrh a implementáciu dedikovaných bezpečnostných komponentov popisovaných v návrhu a dodávka SW licencií pre dedikované bezpečnostné mechanizmy popisované v návrhu. Pre dosiahnutie čo najvyššej úrovne bezpečnosti budú bezpečnostné mechanizmy realizované nielen dedikovanými (samostatné ucelené HWSW prvky plniace iba bezpečnostnú úlohy) komponentmi bezpečnosti ale aj zdieľanými (ktoré sú súčasťou vyvíjaných a dodávaných komponentov napr. kontrola vstupných údajov) komponentmi, ktoré sú realizované priamo implementátormi týchto komponentov.

- **Súčasťou diela nie je dodávka HW bezpečnostných komponentov** – Zhotoviteľ očakáva súčinnosť zo strany Objednávateľa predstavujúcu dodávku HW podľa špecifikácie realizovanej vo fáze design.

1.1.2.2 Komponenty sieťovej bezpečnosti

Návrh architektúry riešenia sieťovej infraštruktúry taktiež vychádza z generickej koncepcie budovania bezpečných, spoľahlivých a efektívnych dátových centier Cisco Validated Design Táto koncepcia pre dátové centrá používa hierarchický referenčný model sieťového dizajnu dátového centra, ktorý je flexibilný, rozšíriteľný a umožňuje ho aplikovať na potreby konkrétneho dátového centra.

Pre zónovanie komunikačného prostredia, budú použité sieťové komunikačné zariadenia typu firewall s kontrolou protokolových stackov po úroveň L5. Striktne bude oddelené produkčné prostredie od manažmentového.

Pre ochranu sieťovej komunikácie, budú použité štandardné mechanizmy bezpečného pripojenia k web portálom šifrovaním komunikácie a ochranou integrity s pomocou SSL/TLS technológie, resp. IPsec, rovnako aj pre komunikáciu medzi požadovanými IS (napr. SOAP protokolom).

Pre realizáciu sieťovej bezpečnosti budú použité mechanizmy popísané v ďalších častiach kapitoly:

1.1.2.2.1 Firewall – Cisco ASA

Cisco Adaptive Security Appliance (ASA) je multifunkčné vysokovýkonné adaptívne bezpečnostné zariadenie, ktoré kombinuje funkcie firewalu, IDS/IPS a VPN zariadení.

Hlavné vlastnosti:

- L2 – L7 inšpekcia pomocou 30 aplikačných inšpekčných enginov,

- konfigurovateľné politiky môžu byť aplikované na používateľov alebo používateľské skupiny, ďalej na jednotlivé VPN tunely alebo pre dátové toky,

- konfigurovateľný vzdialený prístup cez IPsec VPN,

- možnosť IPsec alebo SSL VPN služieb na jednej platforme,

- podpora VPN konfigurácii typu: remote-to-site alebo site-to-site, IPsec alebo SSL,
- pre site-to-site VPN je možné definovať rozsiahle inšpekčné kontroly, definovateľné QoS, dynamické smerovanie a stavové prebratie služby v prípade poruchy,
- podpora pre H.323 verzie 1-4 a Session Initiation Protocol (SIP).

Robustná bezpečnosť a výkonnosť:
- transparentný firewall na 2 vrstve,
- virtualizácia firewallov (až do 50 virtuálnych firewallov),
- podpora VLAN založených na 802.1q (až 250 VLAN),
- podpora OSPF, EIGRP a RIP (služby dynamického smerovania)
- podpora protokolovo nezávislých multicastov (PIM) tzv. „Sparse mód“ verzia 2 a podpora obojsmerného smerovania pre PIM,
- podpora Stub multicastového smerovania,
- podpora IPv6 ,
- podpora Quality of Service (QoS) z nízko latenčným riadením front tzv. Low-Latency Queuing (LLQ),
- podpora IP telefónie so "zero-touch provisioning" službami,
- architektúra odolná voči výpadku poskytuje možnosti pre Active/Active a Active/Standby služby maximálnej dostupnosti,
- podpora clustrovania (clustering) a rozloženia záťaže (load balancing) pri nasadení ako VPN headend.

Ďalšie vlastnosti
- kontrola HTTP až na úroveň HTTP príkazov, kontrola správnych MIME hlavičiek, kontrola obsahu, kontrola veľkosti Uniform Resource Identifier (URI),
- blokovanie „instant messaging-u“ a „peer-to-peer“ zdieľania súborov,
- silné overovanie užívateľov cez lokálnu alebo vzdialenú databázu užívateľov,
- monitorovanie v reálnom čase cez manažment konzolu alebo externé syslog servery,
- podpora vzdialeného spravovania cez ssh alebo telnet,
- podpora SNMP v3, podpora vytvárania SNMP skupín, SNMP používateľov, kryptovanie,
- zariadenie má samostatné rozhranie na správu,
- podpora NetFlow (v9) Secure Event Logging (NSEL) ,
- uskutočňuje zachytávanie paketov,
- podpora DHCP služieb,
- možnosti podpory širokej množiny multicastových aplikácii a „stub“ multicast smerovaniu.

1.1.2.2.2 Perimeter firewall - McAfee Firewall Enterprise (Sidewinder)

Mcafee Firewall (Sidewinder) je *UTM (Unified Threat Management)* multi-funkčné zariadenie - firewall. Integruje niekoľko bezpečnostných funkcií do jedného systému a vďaka tejto integrácií poskytuje bezpečnosť prostredníctvom silnej a hĺbkovej analýzy prechádzajúcej prevádzky. Mcafee Firewall je najčastejšie používaný ako firewall na aplikačnej vrstve, kde využíva patentovanú technológiu aplikačných proxy.

Aplikačné proxy Mcafee Firewallu zabezpečujú úplné rozdelenie realizovaného spojenia od klienta na server. Komunikácia je realizovaná od klienta na firewall a z firewallu na server.

Mcafee Firewall drží EAL4+ ALC_FLR.3 Common Criteria certifikát pre firewally na aplikačnej vrstve oproti profilu "U.S. Department of Defense Application-level Firewall Protection Profile in Basic Robustness Environments, Version 1.1, July 25, 2007".

Za viac ako 16 rokov CERT nepublikoval „advisory warning" a pre tento firewall nebolo potrebné vydávať bezpečnostnú opravu (emergency security patch).

McAfee Firewall (Sidewinder) obsahuje tieto bezpečnostné funkcie a služby:

- Global Threat Intelligence
  - služby TrustedSource (globálna reputácia, ktorú určujú špecifické zariadenia na Internete),
  - Mcafee Firewall Geo-Location (filtrovanie podľa kódy krajín),
  - McAfee Labs,
- fyzické aj logické oddelenie sietí,
- vlastný operačný systém SecureOS s integrovaným Type-Enforcement systémom,
- protokol a network enforcement,
- podpora NAT,
- integrovaný IPsec server,
- statické aj dynamické smerovanie,
- špecifické bezpečné aplikačné proxy (viac ako 20) ,
- AppPrism (znalosť Web 2) a obmedzovanie web služieb,
- vyhľadávanie aplikácii a kontrola prístupu k nim,
- služby DNS (2 servery),
- Intrusion Prevention Signature (IPS),
- Anti-Virus a Anti-Spyware,
- Anti-Spam a Anti-Fraud,
- SmartFilter,
- URL filtrovanie,
- filtrovanie aplikácií využívajúcich šifrovanie (SSL/HTTPS, SSH, SFTP, SCP),
- podpora high availability,
- podpora externých identít (AD) pomocou McAfee Logon Collector,
- integrovateľné s aplikáciami McAfee Firewall Reporter (real-time monitorovanie, reporty), McAfee Firewall Profiler (prehľad o prevádzke, využívaní pravidiel, zmene prevádzky) a Mcafee Firewall Command Center (ovládacie centrum pre viac produktov Mcafee Firewall).

Mcafee Firewall (Sidewinder) spĺňa kritériá Sorbanes-Oxley (SOX), PCI, GLBA, HIPAA, a FISMA.

1.1.2.2.3 XML firewall - IBM XG45

Umožňuje dobre škálovateľné a efektívne nasadzovanie bezpečných, spoľahlivých a akcelerovaných XML aplikácií a webových služieb. Umožňuje presunúť výpočtovo náročné operácie zo serverov na sieťovú infraštruktúru, čím sa zvyšuje ich výkonnosť. IBM XG45 pomáha pri vytváraní prostredia zdieľaných služieb, redukuje oneskorenie služieb, a zlepšuje ich škálovateľnosť.

IBM XG45 predstavuje integrovaný XML firewall/proxy. Zabezpečuje, že XML správy dosiahnu bezpečne a efektívne ich cieľ. Jednoduchá XML správa môže obísť tradičné ochrany a zneužiť, prípadne úplne zablokovať mission critical aplikácie. XG45 inšpektuje prichádzajúce požiadavky a odpovede a blokuje ohrozujúce alebo podozrivé aktivity a tým pomáha chrániť backend servery od rôznych XML útokov.

IBM XG45 obsahuje tieto bezpečnostné funkcie a služby:

- funkcie ochrany pred hrozbami,
    - XPath injection,
    - SQL injection,
    - kontrola správneho formátovania (formy) XML,
    - kontrola XML schém,
    - ochrana pred buffer overrun,
    - filtrovanie metód na základe WSDL,
    - anti-virusová ochrana pomocou ICAP,
    - XML DoS (XDoS)
        - XDoS nad jedným XML dokumentom (XML parsing problémy, Jumbo payloady, rekurzívne elementy, veľmi veľké tagy, DoS na verejný kľúč,
        - XDoS nad množinou XML dokumentov (XML Flood, resource hijacking),
- všeobecné možnosti spracovania správ
    - XML filtrovanie na základe rôznych vstupov (XPath, premenné, výsledky funkcií, tokeny a pod.),
    - XML transformácie pre akceleráciu XML spracovania (využitie XSLT a EXSLT),
    - wirespeed XML spracovanie,
    - smerovanie správ na základe obsahu,
- funkcie pre service level manažment (SLM),
- realizácia kontroly prístupu na základe informácií zo správy
    - prístup pomocou informácii v správe
        - token,
        - XPath,
        - klientská IP,
        - a ďalšie
    - podpora mechanizmov pre kontrolu prístupu
        - WS-Security,
        - WS-Trust,
        - X.509,
        - SAML,
        - SSL,
        - LDAP,
        - XACML,
        - RADIUS,
- podpora kryptografických operácií
    - podpisovanie správy alebo časti správy,
    - overovanie podpisov,
    - šifrovanie správy alebo časti správy,
    - dešifrovanie správy alebo časti správy,
    - podpora rôznych štandardov pre kryptografické operácie na XML,
    - HSM,
- podpora existujúcich štandardov pre SOAP a XML
    - SOAP 1.1, 1.2,
    - WS-Security,
    - WS-Trust,
    - podpora WSDL definície služieb,
    - WS-Policy,
    - WS-SecurityPolicy,
    - WS-ReliableMessaging,
    - WS-SecureConversation,
    - WS-I Conformance Policy,
    - WS-Addressing.

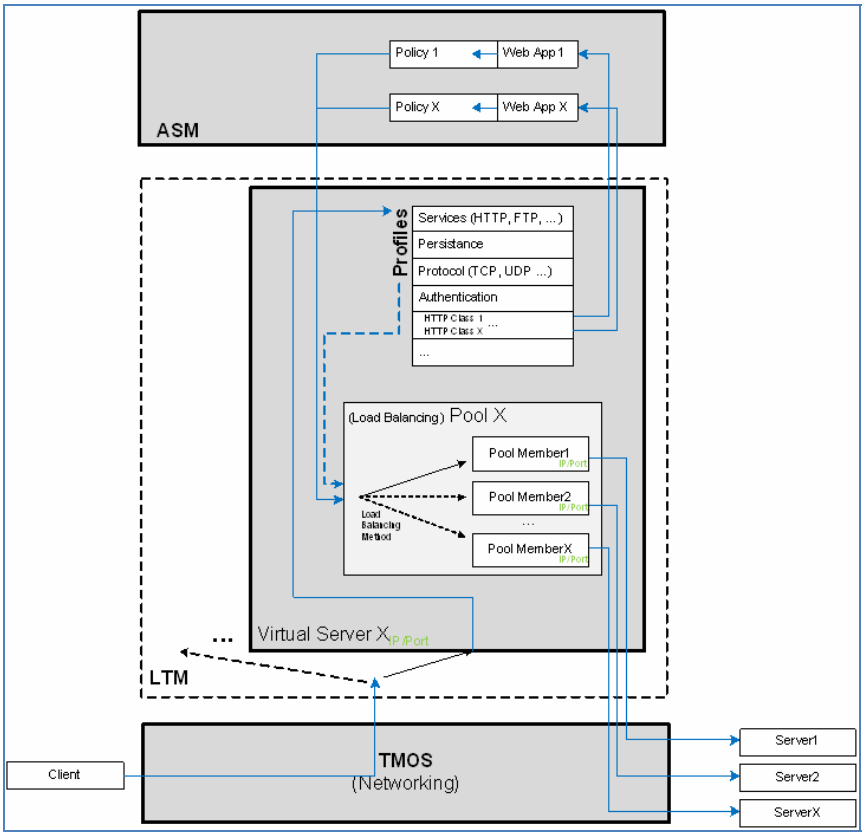
1.1.2.2.4 Web Aplikačný firewall – F5 Big-IP

Rodina produktov F5 Big-IP je systém prepojených modulov fungujúcich na spoločnom hardware. Každý z modulov je plne konfigurovateľný a špecializovaný pre vykonávanie funkcií, pre ktoré bol navrhnutý. Základom F5 Big-IP platformy je TMOS architektúra zabezpečujúca komunikáciu medzi jednotlivými modulmi

ako aj ich komunikáciu so sieťovým prostredím. Pre komunikáciu s externým prostredím TMOS poskytuje otvorené API (iControl).

Pre zabezpečenie funkcionality WAF sú v platforme F5 Big-IP použité moduly:

- TMOS – Traffic Management Operating System
- LTM – Local Traffic Manager
- ASM – Application Security Manager



Obrázok 1 - Štruktúra prepojenia jednotlivých modulov F5 Big-IP platformy

TMOS - Operačný systém vyvinutý firmou F5. Jeho hlavnou úlohou je zabezpečiť komunikáciu medzi jednotlivými modulmi a zároveň celej platformy so sieťovým prostredím.

LTM - Umožňuje meniť prechádzajúcu prevádzku na aplikačnej úrovni. Ovplyvňovanie prechádzajúcej prevádzky v LTM je vykonávané prostredníctvom konfigurovateľných profilov. Každý z týchto profilov ovplyvňuje inú časť prevádzky. Dôležitou funkcionalitou modulu LTM je load balancing, t.j. prichádzajúcu komunikáciu na jednotlivé virtuálne servery je možné distribuovať medzi množinou fyzických serverov.

ASM - Vykonáva aplikačnú inšpekciu prechádzajúcej komunikácie voči vytvoreným profilom aplikácie. Obsahuje súhrn nastaviteľných kontrol, prostredníctvom ktorých sa vykonáva aplikačná inšpekcia. Pri narušení určitej kontroly dochádza k vyvolaniu alarmu a prípadne aj k blokovaniu požiadavky, ktorá ho spôsobila.

Pre aplikačnú kontrolu využíva Application Security Manager viacero kontrolných mechanizmov, ktoré sa navzájom dopĺňajú:

- Negatívny model - je založený na kontrole prechádzajúcej prevádzky voči signatúram, ktoré sú tvorené regulárnymi výrazmi.
- Pozitívny model - popisuje všetko, čo je v aplikácii povolené, na rozdiel od negatívneho modelu, ktorý popisuje všetko to, čo je v aplikácii zakázané. Pozitívny model vyprofiluje každú entitu web aplikácie

s jej vlastnosťami, ktoré sú v tomto modeli popísané. Základné entity kontrolované pozitívnym inšpekčným modelom sú: parametre, URL, hlavičky, cookies a typy súborov.

Detekcia anomálií - poskytuje nástroje, ktoré umožňujú odhaliť neštandardné správanie klientov. Hlavnou úlohou modulu detekcie anomálií je profilovanie štandardnej prevádzky. Každá odchýlka od tohto štandardu je vyhodnotená ako anomália, čo zapríčiní vyvolanie alarmu.

1.1.2.2.5 Cisco Secure Access Control System 5.0

Cisco Secure ACS 5.0 je platforma v kompaktnej forme 1RU zariadenia, ktorá podporuje najnovšie komplexné politiky, ktoré spĺňajú dnešné požiadavky pre prístupový manažment. Cisco Secure ACS poskytuje centralizovaný manažment prístupových politík pre správu zariadení, bezdrôtových sietí a 802.1x sieťových prístupov.

Cisco Secure ACS podporuje Cisco Self-Defending Network technológiu, ktorá chráni prevádzku siete, identifikuje, zabraňuje a prispôsobuje sa rôznym typom hrozieb z vnútra spoločnosti alebo z vonkajšieho prostredia.

Cisco Secure ACS je škálovateľný, vysoko výkonný systém prístupových politík, ktorý centralizuje administráciu a autentizáciu zariadení a užívateľských politík, čo redukuje záťaž administratíve a manažmentu.

1.1.2.2.6 Sieťové prepínače radu Cisco Catalyst 4900M

Catalyst 4900M poskytuje riešenie pre nasadenia s minimom miesta, kde sú napriek tomu požadované vysoký výkon, služby na wire speed, vysoká dostupnosť a modulárna flexibilita nasadenia Gigabit a 10 Gigabit ethernetu. Zariadenie je vo veľkosti 2RU.

Ako súčasť prepínacieho portfólia pre dátové centrá 4900M poskytuje:

- Vysoký výkon
- Nízke oneskorenie
- 10/100/1000 Ethernet
- 10 Gigabit Ethernet
- Riešenie top-of-rack prístupového prepínača

Poskytuje wire-speed služby pre kolapsovanú LAN na úrovni vrstiev core-distribution. Jej unikátna semifixná architektúra umožňuje flexibilne nasadiť Gigabit Ethernet, a neskôr zmigrovať do 10 Gigabit Ethernet.

Catalyst 4900M poskytuje 8 fixných wire-speed 10 Gigabit Ethernet rozhraní a dve polovičné sloty, do ktorých môžu byť zasunuté nasledujúce rozširujúce karty:

- 20-portová wire-speed 10/100/1000 (RJ-45) karta
- 8-portová (2:1) 10 Gigabit Ethernet (X2) karta (kompatibilná s Cisco TwinGig Converter Module)
- 4-portová wire-speed 10 Gigabit Ethernet (X2) karta

1.1.2.2.7 SAN prepínače

Realizujú inteligentné sieťové pripojenie pre fibre-channel (FC) rozhrania a silnú bezpečnosť. Bezpečnostné vlastnosti SAN prepínačov

- podpora RADIUS and TACACS+, port security,fabric binding, Fibre Channel Security Protocol (FC-SP) host-to-switch and switch-to-switch autentizácia,
- Secure FTP (SFTP), Secure Shell Version 2 (SSHv2) a Simple Network Management Protocol Version 3
- (SNMPv3) implementácia Advanced Encryption Standard (AES), a hardvérom vynútené zónovanie,
- broadcastové zóny, a per-VSAN role-based access control (RBAC).

VSANs pre segmentáciu a izoláciu

- VSAN a FC virtualizácia umožnujú vytváranie virtuálnych SAN sieti, vzájomné izolovaných, pričom využívajú spoločnú fyzickú infraštruktúru
- Každá VSAN pritom môže byť segmentovaná do zón s vlastnými fabric službami.

1.1.2.3 Zabezpečenie bezpečnostnej stability prostredia

Podkapitola predstavuje mechanizmy zabezpečujúce monitorovanie a vynútenie integrity, verifikáciu stavu bezpečnosti vzhľadom na definovaný baseline a aktuálne hrozby. Výstupy z fáz SLDC (napr. výstup z testovania) predstavujú podklad (baseline) pre kontrolu.

1.1.2.3.1 Hlavné ciele

- V oblasti zabezpečenia integrity:
  - vytvorenie databázy odtlačkov (fingerprints) súborov filesystému a konfiguračných nastavení komponentov riešenia
  - periodická verifikácia integrity a hlásenie narušení
  - zamedzenie narušenia integrity pre vybrané súbory a servery
- V oblasti verifikácie odolnosti voči bezpečnostným hrozbám
  - automatická kontrola súladu konfigurácie voči best practices a špecifickým konfiguračným štandardom vyvinutým počas SDLC
  - automatická kontrola zraniteľností komponentov voči aktuálnym hrozbám.

1.1.2.3.2 Použité technológie

Tripwire Enterprise umožňuje:

- vytvorenie a správu baseline jednotlivých systémov prostredníctvom kryptografických odtlačkov:
  - konfigurácií sieťových zariadení
  - konfigurácie a vybraného obsahu databáz
  - súborov a adresárov na súborových systémoch
  - kľúčov a hodnôt registry
  - objektov Active Directory
- pravidelná kontrola stavu systémov oproti schválenému baseline
- alerting a reporting v prípade zmeny

McAfee Change Control ako prvok nezávislý od správcov OS zabezpečí pre servery detekciu, prevenciu a logging nežiaducich zmien vybraných komponentov viditeľných z pohľadu OS vrátane spustiteľných súborov, knižníc, konfiguračných súborov aplikácií a databáz.

McAfee Application Control pomocou mechanizmu „dynamic whitelisting via a trusted source“ zabezpečí, že na určených serveroch bude môcť byť spustený iba autorizovaný softvér (vrátane DLL, skriptov...). Autorizované kódy sú chránené pred zmenou, zmazaním, nahradením a pod., pričom súčasťou je ochrana kódov v operačnej pamäti pred ich odstránením, zmenou, hijackingom.

McAfee Risk Advisor na základe informácií zozbieraných o monitorovanom systéme publikovaných renomovanými organizáciami v oblasti informačnej bezpečnosti vykonáva vyhodnotenie stavu zraniteľnosti

McAfee Policy Auditor periodicky verifikuje súlad konfigurácie komponentu voči stanovenému konfiguračnému profilu prostredníctvom partikulárnych testov vykonávaných Policy Auditor agentom podľa centrálne definovanej politiky. Umožňuje automatickú kontrolu verzií softvérových komponentov voči informáciám o dostupných aktualizáciách publikovaných výrobcom komponentu

Súčasťou mechanizmov pre zabezpečenie bezpečnostnej stability prostredia je aj patch management a configuration/change management, ktorý je realizovaný prostriedkami IT architektúry a vynucovaný a kontrolovaný technológiami uvedenými v tejto kapitole, ako aj sieťovými bezpečnostnými technológiami (napríklad schválená a otestovaná zmena aplikačného komponentu je zanesená do konfigurácie bezpečnostných mechanizmov na kontrolu integrity, čím sa zabezpečí okrem odolnosti voči útokom aj znemožnenie implementácie komponentu, ktorý neprešiel príslušným procesom).

1.1.2.4 Bezpečnostné komponenty na serveroch

1.1.2.4.1 Hardening komponentov

Zvýšenú ochranu operačných systémov a aplikácií, ktoré nie sú primárne bezpečnostné, bude realizované aplikovaním bezpečnostných nastavení podľa doporučení výrobcov a renomovaných organizácií v oblasti informačnej bezpečnosti (NIST, DISA, CIS, ...) pomocou ich natívnych funkcií.

1.1.2.4.2 McAfee VirusScan Enterprise

Pozn.: napriek komplexnosti ponuky v oblasti ochrany proti malware, ponúkané riešenie dokáže zohľadniť existujúce produkty používané SZÚ.

McAfee VirusScan Enterprise (VS) zabezpečuje komplexnú, proaktívnu systémovú ochranu pracovných staníc a serverov pred vírusmi, červami, trójskymi koňmi a ďalším malware. Vďaka heuristickej analýze a pokročilej antimalware technológii Artemis, je VS schopný odhaliť a zablokovať aj nové, zatiaľ neznáme škodlivé kódy. Výborná manažovateľnosť a škálovateľnosť umožňuje zabezpečenie všetkých chránených systémov na vysokej úrovni, pri súčasne minimálnych požiadavkách na správu celého AV systému. V spojení s inteligentnou auto-update technológiou a centrálnym manažmentom prostredníctvom aplikácie ePolicy Orchestrator Server je možné zabezpečiť presadzovanie a udržiavanie aktuálnych bezpečnostných politík a vírusových databáz pre všetky chránené systémy. Inštaláciou Add-On modulu Antispyware Enterprise sa rozšíria detekčné schopnosti VS o schopnosť detekcie potenciálne nebezpečných, resp. nechcených programov typu adware, cookies a pod. a umožní sa kontrola a liečenie Windows Registry databázy.

Vlastnosti produktu:

- Integrácia s ePolicy Orchestratorom (ePO) – VS sa integruje s ePolicy Orchestrator (ePO) serverom, nástrojom pre centralizovanú správu McAfee produktov, zabezpečujúcim centrálne vytváranie a presadzovanie politík, spracovávanie udalostí získaných z manažovaných systémov a generovanie notifikácii, a poskytujúcim rozsiahly grafický reporting.

- Komplexná ochrana - je zabezpečená rezidentným skenerom kontrolujúcim vopred nadefinované aktivity (spúšťanie, kopírovanie, premenovávanie súborov a podobne) a tiež nerezidentným skenerom, ktorý môže byť spúšťaný buď v reálnom čase (lokálne užívateľom, vzdialene administrátorom), alebo pomocou schedulera vo vopred nadefinovaných intervaloch.

- Likvidácia počítačových infiltrácií v operačnej pamäti – vyhľadávanie a likvidácia počítačových infiltrácií priamo v operačnej pamäti, v bežiacich procesoch (napríklad CodeRed a SQL Slammer).

- ScriptScan – funkcia umožňuje detailnú analýzu a vyhodnocovanie nebezpečnosti všetkých spúšťaných skriptov v reálnom čase. Na rozdiel od klasického debugovania kódu, ktoré je ľahko ošetriteľné a tým neúčinné, funkcia ScriptScan zabezpečí spustenie kontrolovaného skriptu v chránenom virtuálnom móde a analyzuje až výsledok jeho činnosti a potenciálny dopad na chránený systém.

- Rýchlosť skenovania – použitá technológia a architektúra výrazne znižuje negatívny vplyv na produktivitu užívateľa pri súčasnom zachovaní vysokej úrovne zabezpečenia antimalware ochrany.

- Inteligentný proces aktualizácii – služba “Nearest Server Updates” umožňuje vykonávať aktualizáciu z najbližšieho nadefinovaného servera, ktorý je automaticky zvolený na základe fyzického umiestnenia, prípadne rýchlosti spojenia. Ak dôjde k prerušeniu sťahovania aktualizácie, ďalšie sťahovanie

automaticky pokračuje od miesta kde došlo k prerušeniu. V prípade aplikovania chybnej aktualizácie VS umožňuje vykonanie návrat k poslednej funkčnej aktualizácii.

- Skenovanie na základe miery rizika – Aplikácie a procesy je možné rozdeliť do 3 kategórií - na High risk, Low Risk a Default aplikácie, pričom pre každú kategóriu je možné nadefinovať rôzne parametre skenovania a tiež rôzne akcie v prípade detekcie škodlivého kódu.

- Regulácia využitia CPU – funkcia "CPU utilization" umožňuje veľmi jednoducho prideliť systémové prostriedky plánovanému skenovaniu, vďaka čomu je možné zvoliť optimálny pomer medzi potrebami užívateľa a vyhľadávaním škodlivých kódov.

- Uzamknutie nastavení – administrátor môže pomocou centrálne nadefinovaného hesla uzamknúť, buď celé užívateľské rozhranie, alebo len jeho vybrané časti, čím ochráni vopred nadefinované politiky pred akýmikoľvek neoprávnenými zmenami.

- Pokročilá „samoochrana" – VirusScan je schopný chrániť svoje súbory, adresáre a procesy pred všetkými neautorizovanými zmenami (snahy užívateľa alebo škodlivého softvéru o deaktiváciu AV, vzdialené útoky a podobne).

- Podpora 64-bit. prostredia – VS bol prvý AV produkt na svete, ktorý podporoval 64 bitovú technológiu.

- Integrovaný Firewall - umožňuje monitorovanie aplikácií a blokovanie nepovolenej in/out komunikácie.

- Integrované IPS techniky - buffer overflow ochrana pre cca 20 najpoužívanejších a z bezpečnostného hľadiska najrizikovejších aplikácii (Word, Excel, Outlook, Internet Explorer, SQL server a podobne). Ochrana súborov, adresárov a zdieľaných zložiek pred neautorizovanými zmenami.

- Rozšírená detekčná schopnosť pre Adware, Spyware a iné potenciálne nebezpečné alebo nechcené programy.

- Pokročilá ochrana pred rootkitmi – vyhľadávanie a likvidácia rootkitov priamo v operačnej pamäti.

- Automatické zisťovanie IP adresy zdroja nákazy - v závislosti na nastavení je možné zabezpečiť trvalé alebo dočasné zablokovanie všetkej komunikácie so zdroja infiltrácie.

- Podpora najrozšírenejších VPN klientov (napr. Cisco) zabezpečuje možnosť zablokovania pripojenia do siete počítačom bez aktuálnej verzie AV programu alebo vírusových databáz.

- Ochrana VMWare prostredia – VS umožňuje zabezpečiť VMWare procesy pred neautorizovanými zmenami, zastavením a pod.

- Centrálne spravovaná karanténa – VS karanténa poskytuje možnosťou vzdialenej manipulácie s položkami ktoré sa v nej nachádzajú (zmazanie, preskenovanie, uvoľnenie) (dlhodobo uložené položky môžu byť v pravidelných intervaloch automaticky premazávané).

1.1.2.4.3 McAfee Host Intrusion Prevention for Servers

Program McAfee Host Intrusion Prevention (HIPS) je softvérové riešenie, určené pre proaktívnu ochranu pracovných staníc, prenosných počítačov a serverov používajúcich operačné systémy MS Windows, Linux a Sun Solaris pred známymi a aj novými zero-day zraniteľnosťami a útokmi, ktoré nedokážu odhaliť a zastaviť bežné antimalware systémy a ani sieťové IDS/IPS sondy. HIPS zabezpečuje monitorovanie a blokovanie nechcených, resp. nepovolených aktivít a tým chráni samotný operačný systém, bežiace aplikácie, užívateľské dáta, databázy a podobne. Kvôli zosilneniu ochrany IS a zabezpečeniu čo najefektívnejšej a najspoľahlivejšej detekcie potenciálnych hrozieb HIPS vykonáva analýzu a vyhodnocovanie sledovaných aktivít pomocou kombinácie viacerých metód, zahŕňajúcich využitie klasických signatúr, behaviorálnu detekciu neštandardných aktivít, a využitie integrovaného sieťového a aplikačného firewallu. HIPS umožňuje detailnú profiláciu

štandardného správania aplikácie (vrátane špecifických pre prostredie MZ) a automatické vygenerovanie ochrannej politiky, ktorá umožní automaticky zasiahnuť pri detegovaných odchýlkach.

Vlastnosti produktu:

- Integrácia s ePolicy Orchestrator serverom – McAfee HIPS sa integruje s ePolicy Orchestrator (ePO) serverom, nástrojom pre centralizovanú správu McAfee produktov, zabezpečujúcim centrálne vytváranie a presadzovanie politík, spracovávanie udalostí získaných z manažovaných systémov a generovanie notifikácii, a poskytujúcim rozsiahly grafický reporting.

- Jednoduchosť nasadenia – inštalácia produktu je vykonávaná centrálne, prostredníctvom ePO servera, príp. iného manažovacieho systému schopného distribuovať MSI balíky. Nasadenie McAfee HIPS v „učiacom“ móde poskytuje zároveň správcom možnosť centrálneho zberu detailných informácii o monitorovaných systémoch, pričom výstupy sú generované vo forme návrhov pravidiel, ktoré správca môže následne využiť pri vytváraní, resp. úprave centrálne definovaných politík. McAfee HIPS umožňuje tiež využiť výrobcom predpripravené sady politík, ktoré sú optimalizované tak, aby vyhovovali čo najväčšiemu počtu zákazníkov.

- Filtrovanie paketov - McAfee HIPS poskytuje Firewall na paketovej úrovni, ktorý dokáže filtrovať všetku prichádzajúcu a odchádzajúcu sieťovú komunikáciu. Pre blokovanie alebo povolenie určitej komunikácie sa využívajú už preddefinované pravidlá a tiež pravidlá definované administrátorom.

- Aplikačný Firewall - McAfee HIPS poskytuje aplikačnú vrstvu umožňujúcu filtrovanie všetkých aplikácií, ktoré generujú sieťovú komunikáciu.

- Kontrola inštalácií nových aplikácií - McAfee HIPS umožňuje zabrániť inštalácii nových aplikácii, vytvoreniu, premenovaniu, zámene alebo kopírovaniu spustiteľných súborov a zabezpečí, že na chránenom počítači bude možné spúšťať len administrátorom povolené aplikácie.

- Multiprotokolová podpora - McAfee HIPS podporuje viac než 120 IP protokolov. Administrátor môže definovať politiky aj pre iné ako IP protokoly, vrátane WiFi, NetBEUI, IPX a Apple Talk.

- Monitoring aplikácií – funkcia monitoringu zabraňuje neautorizovaným aplikáciám v spúšťaní a pripájaní k iným aplikáciám. Pravidlá pre aplikácie môžu byť zadané manuálne, prípadne môžu byť získané pomocou automatického učenia.

- Intrusion Detection System – je založený na signatúrach a vychádza z pravidiel definovaných v definičnom súbore signatúr. IDS signatúry môžu byť aktualizované automaticky alebo ručne. o Karanténny mód – tento mód umožňuje preskúmanie počítača ePO serverom skôr, než je manažovaný systém úplne pripojený k sieti. V prípade detekovania neaktuálnych politík, MS patchov alebo vírusových databáz AV programu je prístup k sieti zakázaný až dovtedy, kým nedôjde k náprave (komunikácia s ePO serverom, príp. so serverom obsahujúcim aktualizácie ostane povolená).

- Samoučiaci mód - McAfee HIPS sa automaticky učí podľa prichádzajúcej a odchádzajúcej sieťovej a aplikačnej aktivity. V tomto režime sa McAfee HIPS dotazuje užívateľa alebo administrátora, či má danú činnosť alebo aktivitu povoliť alebo zakázať. Takto vytvorené pravidlá je možné ďalej distribuovať na ostatné chránené systémy.

- Ochrana pred neautorizovanými zmenami – McAfee HIPS je chránený pred všetkými nepovolenými zmenami, bez ohľadu na prístupové práva momentálne prihláseného užívateľa. Povolenie lokálnych zmien centrálne nadefinovaných politík je možné iba po zadaní administrátorského hesla.

- Vytváranie profilov - McAfee HIPS umožňuje definovanie rôznych sád politík, ktoré sú následne automaticky aplikované na základe typu pripojenia (LAN, WIFI, VPN, dial-up), IP adresy, DNS alebo DHCP servera, Default Gateway a WINS. o Kompatibilita s VPN - McAfee HIPS je navrhnutý tak, aby posilňoval ochranu virtuálnych privátnych sietí a bol testovaný so všetkými rozšírenými VPN klientmi

- vrátane Cisco, Checkpoint, Nortel a Microsoft.
- Podpora IPV6
- Multiplatformná podpora - McAfee HIPS umožňuje zabezpečiť ochranu pracovných staníc, prenosných počítačov a serverov používajúcich operačné systémy MS Windows, Linux a Sun Solaris.

1.1.3 Aplikačná bezpečnosť

Na aplikačnej úrovni budú realizované bezpečnostné mechanizmy v oblastiach:

SDLC – Aplikovanie bezpečnosti vo všetkých fázach životného cyklu vývoja softvéru využitím metodiky, ktorá bude vytvorená špeciálne SZU pomocou uznávaných SDLC metodík s dôrazom na:

- maximálnu možnú ochranu osobných údajov,
- identifikáciu a implementáciu bezpečnostných požiadaviek od začiatku vývoja systému,
- využívanie analýzy rizík a modelovania hrozieb,
- aplikovanie bezpečnostných doporučení a vzorov pre návrh architektúry s vysokým stupňom bezpečnosti,
- identifikovanie údajov, údajových tokov a komponentov vo fáze návrhu a ich klasifikácia podľa charakteru spracovávaných údajov a miery dôveryhodnosti,
- aplikovanie doporučení pre bezpečné kódovanie, aplikovanie bezpečnostných doporučení a vzorov pre návrh architektúry s vysokým stupňom bezpečnosti,
- maximálnu možnú verifikáciu bezpečnosti riešenia.

Vytvorenie architektúry riešenia v maximálnej možnej miere implementujúce nasledujúce princípy:

- Logické a fyzické oddelenie demografických a zdravotných informácii navzájom a od okolia a oddelenia aj na úrovni osôb realizujúcich správu.
- Ochrana najzraniteľnejšieho miesta (Securing the Weakest Link) – Celková miera bezpečnosti systému je významne ovplyvnená najmenej zabezpečeným miestom v systéme. Potenciálny útočník vyhľadáva najslabšie miesta a na tie sa bude snažiť zaútočiť. Od začiatku životného cyklu softvéru budú preto systematicky identifikované takéto zraniteľné miesta a hrozby a budú prijímané opatrenia na ich zabezpečenie.
- Implicitná nedôvera (Reluctance to Trust) – Dizajnéri systému budú implicitne predpokladať, že prostredie, v ktorom bude systém nasadený, je nezabezpečené. Dôvera voči existujúcim externým systémom a komponentov bude založená na hlbšej znalosti ostatných súčastí prostredia. Vzhľadom na to, že nie je možné predpokladať absolútnu bezpečnosť spolupracujúcich systémov, budú rozhrania s týmito systémami jasne definované a zabezpečené do najvyššej možnej miery. V prípade nesprávnej funkčnosti komunikujúceho systému budú prijaté operatívne riešenia (od upozornenia až po separáciu systému).
- Najvyšší stupeň nedôvery bude uplatnený na prvkoch realizujúcich spájanie demografických údajov (údajov, identifikujúcich zainteresované osoby – pacientov, zdravotných profesionálov, ako aj organizácie, s ktorými sú vo vzťahu – PZS a pod.) so zdravotnými údajmi a na komponentoch priamo interagujúcich s prostrediami mimo SZU. Spájanie údajov zahŕňa demografické a zdravotné údaje, ale aj väzby medzi pacientmi a lekármi resp. PZS). Vzájomne budú oddelené aj databáz/servery jednotlivých aplikačných domén.

- Vzájomné podozrievanie (Mutual Suspicion) – Komponenty systému si budú navzájom dôverovať len v prípadoch, ktoré boli vopred definované ako povolené scenáre vzájomnej spolupráce. V opačných prípadoch bude komponent pripravený na ochranu pred útokom prichádzajúcim z iného komponentu. Komponenty systému budú rozdelené do vrstiev a skupín, pričom budú definované scenáre spolupráce jednotlivých vrstiev a skupín. Počet komponentov, ktorým je potrebné v rámci systému dôverovať, bude minimalizovaný.
- Najnižšie možné oprávnenia (Least Privilege) – Každému subjektu, ktorý bude využívať služby poskytované systémom (používateľ, proces alebo zariadenia) bude udelený najviac obmedzujúci súbor oprávnení nevyhnutný na plnenie jeho všetkých úloh. Jednotlivé subjekty budú kategorizované do skupín(rolí), pre ktoré budú definované najslabšie oprávnenia na základe analýzy požiadaviek pre činnosti vykonávané skupinou.
- Úplné sprostredkovanie (Complete Mediation) – Pred každým sprístupnením zdroja alebo vykonaním činnosti bude subjekt žiadajúci o zdroj resp. vykonanie činnosti autorizovaný. V prípade, že subjekt nemá príslušné oprávnenie, bude požiadavka na zdroj resp. vykonanie činnosti zamietnutá.
- Bezpečný pri poruche (Fail-Safe Defaults) – Na základe tohto princípu bude vo všetkých bezpečnostne relevantných situáciách predvoleným správaním odmietnutie prístupu namiesto povolenia. Predvoleným spôsobom reakcie na požiadavku nespĺňajúcu stanovené kritériá teda bude v systéme odmietnutie.
- Separácia oprávnení (Separation of Privilege) – Vykonanie činností vyžadujúcich vysokú mieru zabezpečenia bude podmienené splnením viacerých požiadaviek súčasne. Potenciálny útočník je tak nútený splniť všetky definované požiadavky súčasne ešte pred prístupom k chránenému zdroju (resp. vykonaním činnosti). Systém bude na základe tohto pravidla rozdelený na viacero samostatných komponentov zabezpečujúcich kontrolu prístupu. Takéto rozdelenie systému na množinu nezávislých, ale vzájomne spolupracujúcich komponentov umožňuje viacnásobnú kontrolu prístupu. V prípade výskytu bezpečnostného incidentu a splnenia iba jednej z definovaných požiadaviek (resp. neúplnej množiny požiadaviek) na prístup k zdroju (resp. vykonaniu činnosti), bude prístup odmietnutý.
- Otvorený dizajn (Open Design) – Bezpečnosť systému nebude založená na princípe utajenie jeho dizajnu. V prípade prezradenia utajeného dizajnu by systém nemohol byť viac považovaný za zabezpečený. Ak nie je bezpečnosť systému založená na utajení, môže byť dizajn navyše podrobený revízii odborníkmi bez rizika zneužitia znalostí o utajenom dizajne.
- Zaznamenávanie kompromitácie (Recording of Compromises) – Systematické sledovanie činnosti systému a vytváranie záznamov je kľúčové pre objasnenie bezpečnostných incidentov a zvyčajne vedie k pochopeniu vzorov útokov vrátane spôsobu ich realizácie. Systém bude zaznamenávať vykonávané činnosti, pričom dôraz bude kladený na minimalizáciu možnosti ich modifikácie.
- Ochrana do hĺbky (Defense in Depth) – Ochrana do hĺbky je stratégia, pri ktorej sú ľudské, technologické a operačné kapacity zahrnuté v systéme integrované s cieľom vytvorenia ochranných mechanizmov z pohľadu všetkých vrstiev a dimenzií systému. Takáto organizácia zabezpečuje, že útočník musí prekonať viacero bariér, aby bol systém kompromitovaný. Rôznorodosť ochranných mechanizmov zvyšuje náročnosť realizácie útokov, ako aj celkovú cenu útoku a tým odrádza potenciálneho útočníka. V systéme budú implementované ochranné mechanizmy na viacerých vrstvách s cieľom zabezpečenia do hĺbky (ochrana na úrovni sieťovej komunikácie, údajovej vrstvy, vrstve biznis komponentov a procesov, vrstve používateľského rozhrania).
- Ekonomika mechanizmu (Economy of Mechanism) – Dizajn systému bude realizovaný tak, aby bol čo najjednoduchší za podmienky splnenia požadovanej funkčnosti. Jednoduchosť dizajnu je podstatná z hľadiska pravdepodobnosti výskytu chýb a má priamy vplyv na analyzovateľnosť systému. Toto pravidlo bude aplikované aj na komponenty realizujúce bezpečnostné mechanizmy.
- Analyzovateľnosť systému (Analyzability) – Systém, ktorého správanie je možné podrobiť analýze na základe existujúcej dokumentácie a zdrojových artefaktov (návrhová dokumentácia, zdrojový kód, konfigurácie), má väčšiu pravdepodobnosť správnej funkčnosti, pretože relevantné aspekty jeho správania sa je možné vopred predpovedať. Systém bude počas svojho celého životného cyklu analyzovaný z pohľadu aplikácie bezpečnostných princípov a spôsobu realizácie bezpečnostných mechanizmov. Okrem revízie odborníkmi z oblasti bezpečnosti budú použité na revíziu nástroje na

automatickú revíziu systému (bezpečnostné testovanie, statická analýza zdrojových kódov, aplikácia bezpečnostných vzorov a odporúčaní a podobne).

- Spracovanie chýb a výnimiek s ohľadom na bezpečnosť (Security-Aware Error- and Exception Handling) – Výnimky v systéme budú systematicky spracovávané tak, aby prípadný výskyt výnimky spôsobený útokom nespôsobil pád systému, resp. odmietnutie služby. Systém bude do maximálnej možnej miery overovať všetky vstupy, aby nedošlo k nesprávnej interpretácii vstupu a následnému výskytu bezpečnostného incidentu (napr. prepis údajov, transformácia údajov na vykonávanie činnosti). Počas životného cyklu budú realizované testy zamerané špecificky na túto oblasť s dôrazom na komponenty spájajúce demografické a zdravotné údaje.
- Obmedzenie a izolácia nedôveryhodných procesov (Isolation and Constraint of Untrusted Processes) – V systéme budú procesy, ktoré nie sú považované za dôveryhodné a predstavujú riziko z pohľadu vykonávania, mať obmedzené možnosti, resp. budú izolované od iných procesov. Táto stratégia vedie k zníženiu rizík z dôvodu nemožnosti vykonávania kritických operácií nedôveryhodnými procesmi, ktoré sú vykonávané v kontrolovanom prostredí.
- Izolácia procesov kritických pre bezpečnosť (Isolation of Trusted/High Consequence Processes) – Procesy kritické pre zabezpečenie funkčnosti bezpečnostných mechanizmov budú oddelené od ostatných procesov s cieľom zachovania ich integrity a dostupnosti.

1.1.4 Hlavné bezpečnostné opatrenia pre ochranu dát

Cieľom je:

- V oblasti dôvernosti uchovávaných údajov
  - Zabezpečiť utajenie obsahu vybraných položiek (častí záznamov)
- V oblasti integrity uchovávaných údajov:
  - Zabezpečiť riadenie prístupu do databázy, resp. jej oddelených častí, minimálne na úrovni aplikačných komponentov (I&A komponentu)
  - Zabezpečiť nepopierateľnosť akcií vytvorenia, resp. modifikácie záznamov ,resp. položiek
- V oblasti dostupnosti uchovávaných údajov
  - Zabezpečiť odolnosť voči strate údajov, výpadku, zlyhaniu HW, SW
  - Zabezpečiť odolnosť voči enormnej záťaži voči databáze generovanej napr. v rámci útoku typu DOS

Bezpečnostné mechanizmy pre ochranu dát budú realizované:

- využitím možností DB a OS platformy databázových serverov
- inherentné bezpečnostné mechanizmy platforiem
- striktné granulárne riadenie prístupu (minimálne na úrovni aplikačných komponentov - I&A komponentu)
- minimalizácia množiny oprávnení pre osoby, ktoré pristupujú priamo k databázovým serverom (operátori, správcovia), s dôsledným zachovávaním princípu segregation of duties (zahŕňa aj oddelenie rolí bezpečnostného správcu o správcov OS a databázy)
- auditovaním aktivít na databázovom serveri,
- ochranou údajov v rámci ich životného cyklu (vrátane zabezpečenia dôvernosti a integrity záložných a archívnych kópií)
- rozdelením aplikačnej logiky medzi databázový a aplikačný server s využitím granulárnej úrovne riadenia prístupu k údajom a službám (napr. Využívanie uložených procedúr - stored procedures)
- ochranou údajov šifrovaním s využitím nasledovných typov šifrovania podľa požiadaviek vyplývajúcich z bezpečnostnej analýzy (projektu):
  - šifrovanie dát aplikáciou
  - šifrovanie na úrovni súborového systému OS
  - šifrovanie ovládačom sieťovej karty resp. sieťovým adaptérom
  - šifrovanie sieťovou infraštruktúrou

- o šifrovanie kontrolérom úložiska
- o šifrovanie samotným úložiskom na transparentné šifrovanie diskov sa môže použiť technológia Storage Media Encryption (SME), ktorá zabezpečí zašifrovanie dát pred ich uložením na úložisko (diskové pole alebo pásku).
- o Šifrovanie správ na všetkých úrovniach je v SOAP správe umožnené používaním WS-Security. Je možné šifrovať celú správu alebo iba vybrané časti.

- Pre ochranu exportovaných dát navrhujeme použiť anonymizačné služby – odstraňujú z dát identifikovateľné osobné elementy, čo dáta transformuje do menej citlivej formy a potenciálne do podoby keď nie sú predmetom prísnej regulácie. Umožňujú teda zachovať hodnotu dát pre legitímne sekundárne použitie ako je výskum a výkazníctvo. Anonymizácia je nezvratný, jednosmerný proces, ktorý spôsobí nemožnosť vrátiť dáta späť do identifikovateľnej podoby,

Podľa požiadaviek bezpečnostného projektu budú navrhnuté rôzne úrovne autentizácie pre osoby podľa citlivosti údajov ku ktorým je možné v danej roli pristúpiť. Pre prístup k osobným údajom osobitnej kategórie odporúčame použiť dvoj-faktorovú autentizáciu realizovanú pomocou HW apliance ktoré značne zjednodušujú správu a prevádzku.

Autentizácia služieb bude realizovaná v závislosti od typu:

- Inherentné vlastnosti protokolu (MS doména, WS-Security)
- Autentizácia peerov komunikačného kanála (VPN)

Pre zabezpečenie logovania prístupov k dátam bude vypracovaný logovací štandard ktorý bude obsahovať minimálnu množinu povinných atribútov auditného záznamu a typy udalosti, ktoré je potrebné auditovať v aplikáciách.

1.1.5 Identifikácia a autentizácia pre modul Skríning

Nakoľko modul skríning bude obsahovať osobné údaje osobitnej kategórie, plánujeme preň využiť systém viacfaktorovej autentizácie.

SafeNet eToken je univerzálnym USB tokenom, ktorý je určený primárne pre účely PKI (práca s certifikátmi), SSO (Single Sign-On) a Windows Logon. Token je použiteľný pre všetky bežné kryptografické funkcie vďaka bohatej zásobe šifrovacích algoritmov "on board". Podporuje najširšie spektrum operačných systémov (Win, Linux, Mac).

1.1.5.1 Vlastnosti tokenu

Veľkosť pamäte	72 K	
Max. počet write/erase cyklov	min 500 000, read neobmedzene	
Rozmery	16.4 x 8.4 x 40.2mm (5100-mini) 16.4 x 8.4 x 53.6mm (5105-midi)	
Algoritmy v hardware	RSA (1024, 2048bit key), DES, 3DES, DH, SHA-1, SHA-256	
Kryptografické API	PKCS#11 v.2.01, MS CryptoAPI (CAPI, CNG), PC/SC, X.509v.3 certificate storage, SSLv3, IPSec/IKE	
Výkonnosť	Generovanie RSA kľúča+ verifikácia	<18s (1024-bit) <40s (2048-bit)
	Digitálny podpis	<0.45s (1024-bit), 1.23s (2048-bit)

Podporované OS	Windows (32- a 64-bit) 2003, 2008, XP, Vista, Windows 7
	Mac OS 10.6 (Snow Leopard)
	Linux (Ubuntu, RHEL, CentOS, Fedora, Suse)
Certifikácie (bezpečnosť)	FIPS 140-2 level 3 (pre nové HW revízia v procese), Common Criteria EAL 4+ (nové HW revízia)
Kompatibilita	ISO 7816, RoHS, FCC Part 15, CE, USB 1.1/2.0

1.1.5.2 Typické použitie

- digitálny podpis dokumentov a e-mailov
- generovanie a ukladanie kľúčov, hesiel a digitálnych certifikátov
- hardvérové šifrovanie pomocou symetrických a asymetrických algoritmov
- Windows logon, autentifikácia a přístup do aplikácií, VPN, SSL
- on-line bankovníctvo, Public Key Infrastructure (PKI)
- Single Sign-On

K produktu je nutné zakúpiť middleware SafeNet Authentication Client 8.0 a vyšší, ktorý obsahuje ovládače k tokenu, kryptografické knižnice a podporné utility pre management tokenu.

Tokeny sa inicializujú centrálne pomocou SafeNet Authentication Managera (SAM), alebo je možné využiť tzv. Remote Enrollment Portal (súčasť SAM), čo je vlastne vopred nakonfigurovaná web-stránka, kde si používateľ vzdialene inicializuje token. Pri tom sa automaticky nahrávajú potrebné certifikáty a ďalšie dáta potrebné pre prihlasovanie.

1.2 Modul Enviro

1.2.1 Architektúra riešenia

Riešenie je založené na centralizovanom uskladnení a poskytovaní údajov pre zainteresované subjekty v rámci definovaného rozsahu projektu modulu Enviro. Architektúra navrhovaného riešenia vychádza z požiadaviek a modul Enviro je navrhnutý tak, aby zabezpečil ukladanie štruktúrovaných a aj neštruktúrovaných údajov. Centrálne úložisko a aj iné konfiguračné či systémové údaje modulu sú pravidelne zálohované. Archivácia je navrhovaná pre centrálne úložisko za predpokladu využitia externých prostriedkov v rámci SZU.

Architektúra je postavená na viacvrstvovom návrhu a to využitím vrstvenia modulu na:

- dátovú vrstvu,
- aplikačnú vrstvu,
- prezentačnú vrstvu a
- vrstvu zabezpečujúcu integráciu údajov z externých systémov.

1.2.2 Návrh dátovej vrstvy

Podľa požiadaviek na modul je predmetom správa nasledujúcich typov údajov:

- vlastné údaje,
- registre,
- popisné údaje,
- dokumenty a
- externé údaje aj offline kópie.

Pre realizáciu požiadaviek na správu údajov je navrhovaný cluster MS SQL 2008 R2 databázových serverov ako centrálne úložisko modulu vrátane údajov (vlastné údaje, registre a externé údaje), dokumentov a popisných údajov. Clusterové riešenie je navrhnuté najmä z dôvodu vysokej dostupnosti v režime Aktív-Pasív a teda ide aj o zálohu centrálneho úložiska medzi SQL serverami prostredníctvom replikácie údajov medzi databázovými serverami.

1.2.3 Návrh aplikačnej vrstvy

Aplikačná vrstva pozostáva z viacerých logických komponentov. Pre evidenciu projektov je navrhovaný ako kolaboračný nástroj platforma MS Sharepoint Server 2010. Samotná platforma MS Sharepoint je navrhovaná a delená z pohľadu požiadaviek na:

- authoringovú farmu slúžiacu na zadávanie a riadenie údajov kolaborácie a
- publikačnú farmu slúžiacu na prezentovanie verejne dostupných informácií.

Súčasťou platformy MS Sharepoint je vyššie spomínaný MS SQL server ako dátové uložisko. Ďalej je navrhovaný v rámci platformy MS Search Server pre indexáciu vyhľadávania.

Aplikačná vrstva ďalej podporuje a zároveň realizuje:

- integráciu s registrami pracovísk SZU, číselníkov, klasifikácií a údajov z meracích prístrojov prostredníctvom dátových adaptérov/púmp platformy,
- správu popisných údajov,
- pravidelnú aktualizáciu popisných údajov prostredníctvom schedulovaných jobov,
- verzovací systém nad zvolenou množinou údajov (dokumenty, textové súbory a multimediálny obsah),
- workflow (riadenie procesov) mechanizmy,
- prístupový modul ACL (Access control list) pre správu prístupov a riadenia práv v rámci celej platformy,
- validačné kritéria (rozsahy hodnôt, prípustné hodnoty a pod.),
- vyhľadávanie skrz štruktúrované a aj neštruktúrované údaje,
- import/migrácia existujúcich údajov do systému prostredníctvom adaptérov/púmp platformy,
- export údajov formou XML podľa požiadaviek s prihliadnutím na anonymizáciu osobných údajov,
- taxonómiu,
- administrátorské rozhranie pre správu obsahu, formulárov, WF, prístupov a pod.

Na štruktúrovaný obsah je navrhované použitie Sharepoint listy a na neštruktúrovaný obsah Sharepoint dokumentové knižnice.

1.2.4 Integrácia údajov do IS s externého okolia

Pre prepojenie na externé zdroje, import existujúcich údajov a automatický zber je navrhovaný middleware BOND, ktorý:

- je plne konfigurovateľný (frekvencia zberu, rôzne dátové adaptéry – FTP, SFTP, File, DB a webové služby, transformácie údajov, popisná vrstva k integrovateľnému obsahu a štruktúre a k cieľovému úložisku),
- automaticky zbiera požadované údaje,
- minimalizuje záťaž na zdrojové IS,
- bezstratovo spracováva získané údaje (zotavenie po prerušení),
- archivuje zdrojové údaje ako offline kópia a
- vylučuje duplicity.

Middleware BOND zabezpečuje plne automatický prenos dát z rôznych typov zdrojov údajov do cieľovej databázy. Systém bol vyvinutý s ohľadom na:

- možnosť konfigurácie zberu údajov zo zdroja
- nepostihovanie okolitých systémov (s tým spojenie časovanie prístupu k zdrojom)
- požiadavku na bezstratovosť prenosu a vylúčenie duplicity (korektné zotavenie po prerušení činnosti)
- potrebu archivácie údajov (s nezmeneným obsahom)

Systém pozostáva z nasledujúcich modulov:

- DataReader – zabezpečuje zber dát zo zdrojových systémov a ich zápis do dočasných súborov bez zmeny hodnôt
- DataWriter – zabezpečuje čítanie dát z dočasných súborov (vytvorených DataReader-om) a ich zápis do cieľovej databázy
- ITIMSynchronizer – zabezpečuje synchronizáciu údajov o používateľských účtoch a identitách
- Archivator – zabezpečuje archiváciu dočasných súborov vytvorených DataReader-om
- ProcessManager – spravuje beh inštancií ostatných modulov

Databázová logika Middleware BOND systému pozostáva z 5 základných častí:

- Údaje zo spracovaných súborov
- Log aktivity procesov
- Synchronizácia používateľských účtov a identít (ITIM)
- Log chýb
- Údajové tabuľky – tvoria rozhranie medzi BOND MW a cieľovým systémom

1.2.4.1 DataReader

- Modul zabezpečuje získavanie údajov z externých informačných systémov. Získané údaje sú buď v CSV štruktúre / formáte alebo sú DataReader-om do tohto formátu transformované. Celý tento proces prebieha cyklicky nasledujúcim spôsobom:
- Na základe konfigurácie sa DataReader pripojí príslušným protokolom (FTP, DB, WebService, ...) k externému IS.
- Z externého IS je stiahnuté príslušné množstvo údajov.
- V prípade potreby sú tieto údaje transformované do CSV štruktúry / formátu a uložené lokálne do jedného súboru so špecifickým názvom.
- Finálny CSV súbor je presunutý do príslušného adresára, odkiaľ bude následne spracovaný DataWritter-om.
- Je vygenerovaný príznak pre DataArchivator na archiváciu CSV súboru.

1.2.4.2 DataWriter

Modul zabezpečuje čítanie dát z CSV súborov (vytvorených DataReader-om) a ich zápis do cieľovej tabuľky v databáze. Proces spracovania modulom prebieha nasledovne:

Modul sa pokúsi vložiť do databázy údaje zo všetkých súborov zo série tzn. skupinu súborov z ktorých každý pochádza z iného dátového zdroja pre daný IS. Na to využíva zoznam, kde si ukladá zdroj práve spracovávaného súboru. Súboru sú spracovávane podľa času ich vytvorenia až pokiaľ nedôjde k spracovaniu súboru, ktorý pochádza zo zdroja ktorý sa už v sérii vyskytol (a teda sa úž nachádza v zozname).

1.2.5 GIS

Pre spracovanie geografických informácií plánujeme využiť produkt ArcView v požadovanej kvantite, ktorý v plnej miere spĺňa požiadavky stanovené v opise predmetu zákazky. ArcView je najpoužívanejšou desktop GIS aplikáciou na svete, ponúka jednoduchý prístup k využívaniu GIS údajov. Je vybavený intuitívnym užívateľským rozhraním, prepracovaným systémom kontextového návodu a obsažnou dokumentáciou, čím umožňuje jednoduchý a rýchly štart v práci s geografickými údajmi.

ArcView umožňuje tvoriť mapy, ktoré pomôžu zviditeľniť pravidelnosti, trendy a výnimky z nich. Obsahuje sprievodcov, vopred definované mapové šablóny, široký výber mapových prvkov, ktoré šetria čas a zjednodušujú tvorbu máp profesionálnej kvality. Vytvorené mapy je možné tlačiť, exportovať a vkladať do iných dokumentov a aplikácií. ArcView poskytuje aj nástroje na vizualizáciu údajov v podobe tabuliek, grafov a správ.

ArcView poskytuje nástroje na riešenie priestorových otázok, testovanie teórií a predpovedí a skúmanie vzájomných vzťahov. Implementované nástroje na priestorové spracovanie údajov obsahujú hotové analytické nástroje pripravené na použitie ako aj schopnosti na tvorbu procesných modelov, skriptov a kompletných pracovných postupov.

ArcView zjednodušuje integráciu rôznych dátových formátov a ich využitie na vizualizáciu a analýzu. Obsahuje nástroje na tvorbu, spracovanie a organizovanie geografických, tabuľkových údajov a metadát a podporuje široký výber dátových formátov - demografické údaje, údaje o zariadeniach, CAD údaje, rastrový obraz, webové služby a multimédiá. Do ArcView môžete priamo načítať alebo importovať viac než 70 rôznych dátových formátov.

Ako mapový podklad plánujeme využiť digitálnu vektorovú mapa SVM 50. Na tvorbu geografickej databázy slúžili ako podklad tlačové podklady ZM50. Tieto boli snímané na skeneroch KartoScan FBIII a SGI 906C. Obe zariadenia majú maximálne rozlíšenie 1000 DPI, použité boli rozlíšenia od 400 až po 1000 DPI v závislosti od kvality snímaných podkladov. Pred skenovaním boli do podkladov dokreslené vlícovacie krížiky, po naskenovaní bola uskutočnená kontola kvality každého rastrového obrázku.

Parametre SVM 50	
Vrstvy	• Hranice územno-správnych jednotiek • Sídla a jednotlivé objekty • Pozemné komunikácie • Železnice • Vodstvo • Lesy • Výškopis • Popis
Cieľová mierka	1: 50 000
Polohová presnosť	
Polohová presnosť prvkov vektorovej databázy je ovplyvnená kvalitou použitého podkladu ZM50, ktorého presnosť je ovplyvnená spôsobom tvorby tohto mapového diela.	
Georeferenčné umiestnenie a transformácia rastra	max. stredná štvorcová chyba 10m
Presnosť digitalizácie	0.1 mm
Tolerancie	
generalizačná tolerancia	5m
tolerancia prichytávania	5m
tolerancia fuzzy (splynutie prvkov)	1m
tolerancia dangle (spájanie konc. uzlov)	0m
Kódová stránka	
SO 8859-2 - pre formát coverage	
WIN1250 – pre formát ShapeFile a Geodatabáza	
Súradnicový systém	
Štandardný	S-JTSK
Voliteľný	podľa dohody s koncovým užívateľom (S-42, UTM,...)
Dátový formát	
Štandardný	ArcInfo coverage, ArcView Shapefile, Personálna Geodatabáza (MDB geodatabáza alebo súborová geodatabáza pre v9.2 a vyššie)
Voliteľný	podľa dohody s koncovým užívateľom (napr. DXF, DGN, VPF...)

Posledná aktualizácia	
vrstva hraníc	stav podľa roku 2006 (zdroj najnovšie údaje GKÚ a ZM 1:10 000)
polohopisné vrstvy	stav podľa roku 2004
vrstva výškopisu	stav podľa roku 1999

1.2.6 Návrh prezentačnej vrstvy

Prezentačná vrstva je navrhnutá tak aby spĺňala výnos IS pre verejnú správu a je poskytovaná a prezentovaná publikačnou farmou Sharepoint technológie. Prostredníctvom prístupových práv je delená na tieto dva hlavné používateľské skupiny, a to:

- pracovníci SZU a poverené osoby,
- externé inštitúcie

Okrem používateľského rozhrania prezentovaného internetovým prehliadačom poskytuje táto vrstva aj možnosť poskytovať obsah formou webových služieb prostredníctvom SOAP protokolu.

1.2.7 Návrh podporných modulov

1.2.7.1 Riadenie prístupu používateľov

Identity Access Management (IAM) bude realizovaný prostredníctvom Sharepoint platformy, ktorý zabezpečí prístup a overovanie používateľov voči aplikačným procesom a údajom v IS. Jednotlivé identity používateľov budú do platformy synchronizované cez protokol LDAP alebo s Active Directory štruktúr.

1.2.7.2 Aplikačná bezpečnosť

Pre zabezpečenie vysokej úrovne bezpečnosti aplikácie je navrhované aplikácia bezpečnostnej metodiky SDL (Secure development lifecycle) v rámci celého vývojového cyklu SDLC (Software development lifecycle). Aplikačná bezpečnosť bude pozostávať najmä z týchto bezpečnostných aktivít vykonávaných priebežne:

- statická analýza kódu – vykonávaná vo vývojovom nástroji MS Visual Studio 2010 aplikovaním bezpečnostných pravidiel pri vývoji a
- fuzz testovanie – vykonávané v špecializovanom nástroji pre fúzovanie požiadaviek na webové služby.

1.3 Modul Skríning

Modul Skríning bude realizovaný prostredníctvom vzájomne kompatibilných aplikačných komponentov.

1.3.1 Skríningový portál

Komponentom riešenia, ktorý zabezpečuje elektronizáciu procesu skríningu je „Skríningový portál (SP)“, ktorý bude tvoriť prezentačnú vrstvu celého modulu. Je riešením pre automatizáciu tvorby výskumnej údajovej základne skríningu novorodencov a ich štruktúrovanú prezentáciu. Používateľmi systému budú všetky strany zúčastnené procesu skríningu a výskumnej a vzdelávacej činnosti. SP bude poskytovať privátnu a verejnú zónu.

a) Privátna časť portálu bude zabezpečovať funkcionality pre autentifikovaných používateľov:

- Registrácia používateľa SP
- Spracovanie elektronického formulára a jeho odoslanie na ďalšie spracovanie
- Pred vyplnenie osobných údajov používateľa, ktoré tvoria súčasť spracovávaných dokumentov
- Evidencia spracovaných a odoslaných formulárov a ich prezeranie
- Pripojenie a odoslanie dokumentov súvisiacich s protokolom
- Generovanie čiarového kódu do dokumentu protokolu a jeho tlač na pracovnej stanici používateľa
- Správu elektronických formulárov a ich verzií
- Správu údajov používateľov

Komponenty ktoré tvoria privátnu časť portálu sú:

i. <u>iPodateľňa</u>

SP zabezpečí funkcionality systému riadenia podaní tak, aby príslušný elektronický formulár bol sprístupnený v portálovej aplikácii. Tá umožní po autentifikácii užívateľa jeho elektronické podanie. S podaniami má možnosť pracovať so štandardnými webovými prehliadačmi bez nutnosti akejkoľvek dodatočnej inštalácie podporného softvéru. Pre pridelenie autentifikačných údajov užívateľ vyplní žiadosť ako registračný formulár. Po schválení žiadosti mu je odoslaný dokument s vyjadrením a autentifikačnými údajmi. Po svojej autentifikácii má užívateľ v prívetivom užívateľskom prostredí, možnosť výberu konkrétneho elektronického formuláru, ktorým bude realizovať svoje podanie. SP vytvorí každému užívateľovi svoje profilové konto. Vo svojom profilovom prostredí následne môže uložiť rozpracovaný formulár pre jeho neskoršie dopracovanie a odoslanie. V užívateľskom prostredí portálu má tiež dostupný zoznam zrealizovaných podaní. V daných zoznamoch si môže prezerať detailne informácie o podaniach, ich stavy, prípadne prílohy. Daný komponent obsahuje prehľadne usporiadané viacvrstvové stromové menu, v ktorom má na výber definované formuláre „Protokolu, Žiadosti, Výsledku vyšetrenia a ďalších“. Po vyplnení a odoslaní podania, sa môže spustiť generický proces elektronickej služby. Vyplnený a odoslaný elektronický formulár sa následne vygeneruje do elektronického dokumentu vo formáte PDF

resp. PDF/A. Nasleduje ďalej integrácia, ktorá pre vybavenia daného podania vytvorí príslušnému pracovníkovi úlohu pre spracovanie podania v komponente CMS vytvorenej na platforme MS SharePoint 2010. V tomto systéme môžu byť tiež riešené workflow ako WFM modul a všetky dokumenty sú taktiež vedené v komponente DMS. Užívateľ má k dispozícií aj štandardné funkcie na úpravu hesla, zobrazenie stránkovaných zoznamov uložených a odoslaných podaní, prehľad svojich profilových údajov a osobných údajov. Osobná schránka registrového užívateľa bude obsahovať autentifikovanú zónu pre možnosť prezerania všetkej doteraz uskutočnenej komunikácie (podaní) a ich prípadných výstupov. Toto prostredie umožňuje ukladanie aj rozpracovaných formulárov ak nebude možné všetky dáta získať ihneď. Umožňuje postupnú organizáciu práce s dátami formulárov a ich priebežné uchovávanie.

Riadenie prístupu užívateľov **-** Identity Access Management (IAM) bude zabezpečovať prístup a overovanie užívateľov voči službám uchovávajúcim identitu užívateľa, prípadne voči vlastným registrom. Spracovatelia podaní môžu byť autentifikovaný voči LDAP alebo Active Directory štruktúram.

Odporúčania ku konsolidácii technologickej infraštruktúry **-** Tento komponent slúži na priamy kontakt s užívateľom. Vzhľadom na to, je potrebné zabezpečiť vysokú dostupnosť.

Systémová a aplikačná bezpečnosť **-** Vnútorná architektúra modulu je tvorená tak aby spĺňala kritéria ochrany proti SQL injection a CODE injection. Užívateľský prístup do modulu je prostredníctvom „tenkého klienta“ – webový prehliadač. Zabezpečenie tohto prístupu je prostredníctvom šifrovaného HTTPS spojenia.

Licencie tretích strán **-** Vlastný produkt. Dodatočné licencie nie sú požadované.

Metódy integrácie **-** Daný komponent v integračnej architektúre bude využívať pre komunikáciu s ostanými systémami webových služieb a štandardov pre vzájomnú funkčnú spoluprácu, medzi ktoré patria jazyk XML a protokol SOAP (Simple Object Access Protocol). S integračnou platformou bude komunikovať a integrovať sa do generických procesov prostredníctvom správ, ktorých štruktúra a aj samotná sprava, bude popísaná štandardom jazyka XML.

ii. <u>iFormuláre</u>

Elektronické formuláre predstavujú základný nosič údajov o skríningu pri elektronizácii procesov skríningu. Vytvorené sú na technológií Microsoft InfoPath formulárov vo formáte XSN. Dané formuláre sú následne spracovávané v module systém riadenia podaní a renderované do webového prehliadača ako html výstup. InfoPath formuláre sa použijú na získavanie, zdieľanie, opätovné použitie a spravovanie informácií. InfoPath formuláre môžu byť využívané pre:

- Priamu integráciu s portálom. Novo vytvorené formuláre sa ukladajú do knižnice v SP, a ich dáta sú plne prístupné na ďalšie spracovanie.
- Priamu integráciu so Sharepoint Serverom. Novo vytvorené formuláre sa ukladajú do knižnice v Sharepoint, a ich dáta sú plne prístupné na ďalšie spracovanie.

- InfoPath formuláre sa budú zobrazovať vo webovom rozhraní a užívatelia môžu podávať jednotlivé podania, bez nutnosti inštalovania akejkoľvek aplikácie.
- Konvertovanie dokumentov na šablóny formulárov InfoPath, aby sa zabezpečila integrita údajov a zdokonalila kontrola verzií.
- Na základe prihláseného používateľa sa budú dať pred vyplniť vybrané údaje, čo umožní zminimalizovať počet chybných formulárov.
- Formuláre sa budú dať jednoducho navrhnúť vrátane možnosti vytvárania viacerých pohľadov toho istého formulára, čo sa dá využiť, pri spracovaní formulárov pracovníkmi na rôznych pozíciách.

Rôzne číselníky sa budú dať čerpať z rôznych zdrojov (databáza, webové služby, Xml súbory), čo umožní ľahšie zachovanie integrity dát, pri ich úprave.

Riadenie prístupu užívateľov **-** Identity Access Managment bude zabezpečovať prístup a overovanie užívateľov voči službám uchovávajúcim identitu užívateľa, prípadne voči vlastným registrom.

Systémová a aplikačná bezpečnosť **-** Užívateľský prístup do modulu je prostredníctvom „tenkého klienta“ – webový prehliadač. Obsah elektronických formulárov bude renderovaný do html formátu. Zabezpečenie tohto prístupu je prostredníctvom šifrovaného HTTPS spojenia.

Licencie tretích strán **-** Microsoft Office InfoPath 2010

Metódy integrácie **-** Daný komponent v integračnej architektúre bude využívať pre komunikáciu s ostanými systémami webových služieb a štandardov pre vzájomnú funkčnú spoluprácu, medzi ktoré patria jazyk XML a protokol SOAP (Simple Object Access Protocol). S integračnou platformou môže komunikovať a integrovať sa do generických procesov prostredníctvom správ, ktorých štruktúra a aj samotná sprava, bude popísaná štandardom jazyka XML.

b) Verejná časť portálu bude určená pre neautentifikovaných používateľov. Zabezpečovať bude prístup k štandardným funkcionalitám web portálov ako sú:

- Všeobecné informácie o skríningu a platnej legislatíve
- Novinky a oznamy
- Diskusné fóra
- FAQ
- Sprístupnenie štatistických a špecifických zostáv skríningu
- Filtrovanie obsahu zostáv podľa kritérií
- Správu informačných častí portálu prostredníctvom personalizovaných nástrojov na správu obsahu

c) Tlač dokumentu na pracovnej stanici používateľa bude zabezpečená komponentom SP, ktorý umožní konvertovať výstupný dokument do formátu vhodného na tlač a zabezpečí jeho vytlačenie na zariadení pripojenom k pracovnej stanici používateľa. Max. rozmer tlačenej stránky bude A4.

d) Notifikáciu používateľov bude zabezpečovať funkcionalita portálu formou zaslania štruktúrovanej e-mailovej správy používateľom, ktorí budú určení ako odberatelia týchto notifikácií. Obsah správy a štruktúra odberateľov notifikácií bude určená na základe implementačnej analýzy. Podľa aktuálnych technologických možností, implementovaný systém umožní v prípade potreby aj zasielanie SMS notifikácií použitím web služieb, https rozhrania, zaslaním štruktúrovanej e-mailovej notifikačnej správy vybranému telekomunikačnému operátorovi.

Presný rozsah implementovaných funkcionalít SP bude určený na základe implementačnej analýzy.

1.3.2 Reporting a monitoring

Pre zabezpečenie výskumných a vzdelávacích úloh riešenie predpokladá vytvorenie výskumnej databázy, ktorá je synchronizovaná s produktívnou skríningovou databázou vedenou v DFNBB. Mechanizmus jej tvorby bude zabezpečovať systém SQL Server Replication, ktorý zabezpečí replikáciu dát a databázových objektov medzi produktívnou lokalitou v DFNBB a výskumnou lokalitou na SZÚ. Parametrizácia replikácie bude definovaná na základe konkrétnych požiadaviek SZÚ na obsah databázy s ohľadom na ochranu osobných údajov.

Prístup k dátam bude používateľom umožnený na základe preddefinovaných pohľadov na dáta v prostredí SP. Používateľ bude môcť vo vybranom pohľade využiť nástroje, ktoré mu umožnia bližšiu špecifikáciu výstupnej vzorky dát. Služba Microsoft SQL Server Reporting Services ponúka komplexnú serverovú platformu navrhnutú pre podporu celého životného cyklu zostáv v organizácií. Zdrojom údajov môžu byť transakčné, analytické a iné štruktúrované dáta (OLTP, OLAP, XML), ku ktorým existuje prístup pomocou ADO .NET a OLE DB / ODBC (SQL Server, Oracle, DB2, SAP NetWeaver BI, Hyperion Essbase, a pod.). Reporty môžu byť tradičné aj interaktívne, môžu sa vytvárať na požiadanie i automaticky a môžu mať rôzne formáty - webový (HTML), tlačový (TIFF, RTF, PDF) alebo dátový (Excel, Word, XML, CSV). Na grafický návrh a vývoj reportov bude možné využiť Report Designer, ktorý je integrovaný do vývojového prostredia Visual Studio .NET, alebo nástroje tretích strán, ktoré budú vývoj reportov podporovať. Reporty sa definujú v jazyku RDL (Report Definition Language), ktorý sa zapisuje vo forme XML dokumentu.

1.3.2.1 Riadenie prístupu užívateľov

Autentifikačná vrstva podporuje nasledovné spôsoby autentifikácie:

- NTLM
- Basic
- Forms
- Custom authentication
- Anonymous (podporovaná jedine prostredníctvom rozšírenia custom authentication)

1.3.2.2 Odporúčania ku konsolidácii technologickej infraštruktúry

SQL server je najdôležitejší server z hľadiska rýchlosti všetkých modulov.

1.3.2.3 Systémová a aplikačná bezpečnosť

Reporting Services poskytujú flexibilný role-based bezpečnostný koncept na udeľovanie administrátorského prístupu a na zabezpečenie prístupu k zdieľaným dátovým zdrojom, reportom, adresárom a zdrojom. Administrátori môžu používať či už vstavané, alebo customizované definície rolí na vyladenie bezpečnosti ich reportovacích aplikácií. Používateľ môže patriť pod rôzne typy rolí pre rôzne položky. Napríklad, užívateľ môže

byt členom Content Manager role pre report manažovaný jeho oddelením, a zároveň byť členom Browser role pre report vyvíjaný pre iné oddelenie vo firme. Administrátor môže neskôr vylepšiť bezpečnosť administrácie prostredníctvom SharePoint integrácie. Keď Reporting Services beží v SharePoint-Integrated Mode, oprávnenia Sharepointu môžu byt použité na manažovanie reportov a adresárov v knižnici Sharepointu.

1.3.2.4 Licencie tretích strán

Služba Microsoft SQL Server Reporting Services je súčasťou balíka „The Business Intelligence components" produktu Microsoft SQL Server.

The Business Intelligence components pre SQL Server zahŕňa Analysis Services, Reporting Services, a Integration Services. Na používanie hociktorého z týchto komponentov, potrebuje server, na ktorom je nainštalovaný Business Intelligence, platnú licenciu na SQL Server. Ak tieto komponenty sú na samostatnom serveri ako databázový server, vyžadujú dodatočnú licenciu na každý takýto samostatný server, kde sú nainštalované.

1.3.2.4.1 Správa obsahu – CMS

CMS (Content management system - CMS), alebo systém pre manažment správy obsahu je komponent vnútornej infraštruktúry, ktorého úlohou je podpora správy portálových stránok modulu a ich prezentácie na portáli. Tento komponent zabezpečuje pre rôzne role používateľov možnosti spravovať obsah na portáli prostredníctvom dostupného používateľského rozhrania. Daný komponent je prístupný iba v rámci vnútornej infraštruktúry organizácie, nie je prístupný prostredníctvom voľne dostupnej siete internet.

Systém pre riadenie podaní – je komponent určený pre preberanie a extrahovanie dát z formulárovej podoby, do štruktúrovanej bázy dát, ktorá bude tvoriť súčasť dátovej základne pre výskum. Nad touto agregovanou množinou dát budú môcť byť tvorené a dopĺňané reportovacie zostavy pre účely výskumu nad danou bázou dát. Elektronický obsah v integrovanom intranetovom riešení umožní organizácií zlúčiť rozmanitý obsah z viacerých zdieľaných súborov alebo osobných jednotiek do centrálne spravovaného odkladacieho priestoru s pevnou kategorizáciou. Integrované možnosti vyhľadávania potom umožnia používateľom vyhľadať a zdieľať tieto informácie. Organizácia môže tiež zabezpečiť obsah v tomto centrálne spravovanom odkladacom priestore pred neoprávneným prístupom. Integrované možnosti spolupráce, ako je napríklad automatizovaný pracovný tok, umožnia ľuďom lepšie spolupracovať a štruktúrovanejším spôsobom vytvárať, prezerať a schvaľovať obsah. Pracovníci nebudú musieť využívať výhradne emailové správy pre zdieľanie dokumentov. Mobilní pracovníci môžu tieto dokumenty používať aj v režime offline, keď nie sú pripojení na sieť. Taktiež bude obsahovať nástroje pre definovanie, správu a prehľad úloh. Zoznam úloh bude zobrazovať kolekciu úloh, ktoré sú súčasťou projektu. V tomto zmysle bude úloha samostatnou pracovnou položkou, ktorá môže byť priradená jednej osobe. Projekt bude reprezentovať sériu činností, z ktorých pozostávajú jednotlivé parciálne časti práce. V projekte budú efektívne a prehľadne organizované jednotlivé úlohy a činnosti. Po vytvorení zoznamu projektových úloh bude možné pridať úlohy, priradiť úlohám prostriedky, aktualizovať priebeh úloh a zobraziť informácie o úlohách na čiarach, ktoré sa zobrazia po celej dĺžke časovej osi.

1.3.2.4.2 Riadenie prístupu užívateľov

Osobná lokalita WWW (personálna stránka) poskytuje používateľom úplne prispôsobené prostredie s dedikovanou personálnou stránkou pre každého používateľa. Každú personálnu stránku je možné použiť na ukladanie, prezentáciu, zobrazenie a správu obsahu, informácií a aplikácií kontrolovaným spôsobom. Jednotlivé personálne stránky je možné použiť taktiež na zobrazenie informácií o používateľovi, napríklad o schopnostiach a rolách, spolupracovníkoch, skupinách a distribučných zoznamoch, do ktorých používateľ patrí, a dokumentoch, na ktorých pracuje. Jednotlivé personálne stránky taktiež zahŕňajú priame mechanizmy kontroly osobných údajov a zabezpečenia, takže sa každý používateľ môže rozhodnúť, koľko informácií poskytne a komu. Personálnu stránku je možné taktiež plne prispôsobiť, aby vyhovovala požiadavkám jednotlivých používateľov.

1.3.2.4.3 Odporúčania ku konsolidácii technologickej infraštruktúry

Nie je potrebné, aby pre MS SharePoint bol vyčlenený separátny SQL server, ale môže byť zdieľaný s ostatnými komponentmi. Minimálna požiadavka na edíciu MS SQL servera je „Standard". MS Sharepoint musí byt na samostatnom serveri.

1.3.2.4.4 Systémová a aplikačná bezpečnosť

Daný komponent je komplexný balík nástrojov pre správu a riadenie elektronického obsahu zjednodušuje dodržiavanie podmienok licencií a udržuje dôležité informácie zabezpečené. Zabezpečené je aj výkonné monitorovanie systému, sledovanie používania a nástroje monitorovania. Tieto nástroje uľahčujú rýchlejšie rozpoznávanie a riešenie problémov a zvyšujú efektivitu prevádzky infraštruktúry systému.

1.3.2.4.5 Licencie tretích strán

- Microsoft Office SharePoint Server 2010
- Office SharePoint Server 2010 Standard Client Access Licenses (CAL)
- Office SharePoint Server 2010 Enterprise Client Access Licenses (CAL)

1.3.2.4.6 Udržateľnosť riešenia

Udržateľnosť riešenia z hľadiska technologickej podpory, definuje pre produkt SharePoint 2010 spoločnosť Microsoft 10 rokov podpory.

1.3.2.4.7 Metódy integrácie

CMS na platforme MS SharePoint je založený na škálovateľnej architektúre s podporou webových služieb a štandardov pre vzájomnú funkčnú spoluprácu, medzi ktoré patria jazyk XML a protokol SOAP (Simple Object Access Protocol). Daný komponent obsahuje taktiež otvorené rozhrania API s mnohými funkciami a obslužné rutiny udalostí pre zoznamy a dokumenty. Tie umožňujú integráciu s existujúcimi systémami a poskytujú flexibilitu pre pridávanie nových technológií iných spoločností. Podpora integrácie protokolu LDAP pre ďalších pripojiteľných sprostredkovateľov overovania uľahčuje spoluprácu so zdrojmi adresárových služieb iných než Active Directory. Integrovaná webová časť WSRP Consumer umožňuje integráciu s ďalšími portálovými riešeniami kompatibilnými s technológiou WSRP.

1.3.2.5 Riadené úložisko dokumentov

Modul skríningu v rámci procesu skríningu bude poskytovať funkcionality DMS (Document management systém). Počas procesu skríningu vznikajú elektronické dokumenty, ktoré je nevyhnutné systémovo chrániť a riadene ukladať. Za týmto účelom bude riešenie obsahovať systémový komponent riadeného úložiska, ktoré zabezpečí nasledovné funkcionality:

- Poskytne rozhranie prostredníctvom WS(web services) pre integráciu s ostatnými komponentmi modulu skríningu
- Umožní indexovať a uložiť indexačné údaje do štruktúrovanej databázy
- Umožní štruktúrovane uložiť objekt elektronického dokumentu
- Umožní vyhľadať a poskytnúť dokument podľa kritérií oprávnenému používateľovi na prezeranie
- Zabráni neoprávnenej manipulácii s dokumentom

Riadené úložisko dokumentov bude riešené ako systémový komponent poskytujúci svoje služby ostatným komponentom modulu, bez vlastnej prezentačnej vrstvy. Jeho hlavnou úlohou je centralizovať úložisko dokumentov, ktoré vznikajú pri procese skríningu a chrániť uložené dokumenty pre neoprávnenou manipuláciou.

Riadenie prístupu používateľov – Ide o systémový komponent, ktorý nemá prezentačnú vrstvu a poskytuje služby ostatným komponentom modulu skríningu. Tieto komponenty na prístup k službe úložiska využijú vlastný systém riadenia oprávnení na úrovni použitia funkcií ukladania a prezerania dokumentov.

1.3.2.5.1 Odporúčania ku konsolidácii technologickej infraštruktúry

Nie je potrebné aby pre komponent bol vyčlenený separátny server. Pre uloženie indexačných údajov používa databázu SQL a objekty dokumentov ukladá na FS (file system).

1.3.2.5.2 Systémová a aplikačná bezpečnosť

Vzhľadom k tomu, že systém neposkytuje prezentačné rozhranie, oprávnenia na manipuláciu s dokumentom a dátami, ktoré spravuje sú riadené oprávnením používateľa použiť službu, ktorú cieľový komponent používateľovi poskytuje.

1.3.2.5.3 Licencie tretích strán

Vlastný produkt, nie sú potrebné dodatočné licencie pokiaľ bude databáza modulu centralizovaná na platforme SQL.

1.3.2.5.4 Udržateľnosť riešenia

Udržateľnosť riešenia z hľadiska technologickej podpory, je definovaná podporou DB SQL spoločnosťou Microsoft.

1.3.2.5.5 Metódy integrácie

Daný komponent v integračnej architektúre bude využívať pre komunikáciu s ostanými systémami webových služieb a štandardov pre vzájomnú funkčnú spoluprácu, medzi ktoré patria jazyk XML a protokol SOAP (Simple Object Access Protocol). S integračnou platformou bude komunikovať a integrovať sa do generických procesov prostredníctvom správ, ktorých štruktúra a aj samotná sprava, bude popísaná štandardom jazyka XML.

1.4 Modul Telemedicína

Modul telemedicína je založený na vlastnostiach produktu Ericsson Mobile Health (EMH). Navrhovaná architektúra modulu Ericsson Mobile Health zohľadňuje požiadavky pre výskum a vývoj, ale nie je vhodná pre reálnu prevádzku pre telemonitoring pacientov, nakoľko pre tento modul nie je počítané s plnohodnotnými bezpečnostnými mechanizmami (odporúčane vykonávať zber monitorovaných údajov nad vzorkou anonymizovaných pacientov).

1.4.1 Popis systému

Produkt Ericsson Mobile Health pozostáva z nasledovných komponentov:

- Senzory
- Komunikačné zariadenia
- Servery
- Prezentačné zariadenia

Senzory sa používajú na medicínske merania, komunikačné zariadenia sú pri senzoroch a slúžia na zber a prenos nameraných hodnôt cez IP sieť na servery. Servery sú úložiskom nameraných údajov, ale aj údajov o pacientoch, organizáciách a procesoch. Prezentačné zariadenia slúžia na zobrazovanie uložených informácií.

1.4.1.1 Podpora meraní - senzory

Systém je dodávaný s niekoľkými pred-integrovanými senzormi, ktoré je možné objednať a používať okamžite. Zároveň je tu možnosť integrácie ďalších senzorov.

Predintegrované senzory sú určené najmä na merania pre kardiovaskulárne choroby a diabetes. Stručný popis predintegrovaných senzorov je v nasledujúcej tabuľke. Tieto senzory sa používajú pri najbežnejších oblastiach chronických chorôb: kardiológia a diabetes[1].

Typ senzora	Názov nodelu senzora
ECG1	Corscience ECG CorBELT
ECG 1	Vitaphone 100 BT
ECG 3/6	Corscience ECG BT3_6
ECG 12	Corscience ECG BT12
Tlakomer	Boso Medicus Prestige BPM
Tlakomer	Foracare D40b[2]
Tlakomer	Manuálne zadávanie
Astma monitor	Asthma Monitor ERT AM1+ BT
Astma monitor	Manuálne zadávanie
Pulse oximeter	Onyx II Nonin Model 9560
Váha	Boston Life Labs BS2.4
Váha	Manuálne zadávanie
Glucometar	Foracare G31b
Glukomer	Foracare D40b2
Glukomer	Manuálne zadávanie

[1] Väčšinu senzorov je možné použiť so všetkými komunikačnými zariadeniami, ale sú určité obmedenia (napr. senzory Vitaphone nemožno použiť s jednoúčelovým Komunikačným zariadením, manuálne zadávanie je možné len v prípade Android aplikácii.)

[2] Toto je kombinovaný senzor na meranie tlaku a tiež glukózy.

Okrem predintegrovaných senzorov systém podporuje integráciu ďalších senzorov[3]. Integráciu je možné dodať ako službu alebo je možné nové senzory integrovať pomocou API , ktoré poskytuje systém EMH.

1.4.1.2 Jednoúčelové komunikačné zariadenie

Komunikačné zariadenie je vyvinuté na mieru pre účel telemedicíny a slúži ako komunikačná gateway. Zariadenie zbiera výsledky meraní a posiela ich na serverovú časť systému EMH.

Zariadenie bolo navrhnuté s tým, aby ho mohol používať ktokoľvek, takže je extrémne jednoduché na používanie**.** Zariadenie je ovládané jediným tlačidlom (zapnúť/vypnúť). Naviac, grafické používateľské rozhranie je celé založené na symboloch, takže je jazykovo neutrálne.

Zariadenie používa na komunikáciu so senzormi spojenie Bluetooth, a na komunikáciu so serverovým systémom EMH používa GPRS/3G sieť. Zariadenie automaticky vyhľadáva senzory a tiež sa automaticky pripája na mobilnú sieť a odosiela merania. Zariadenie je vybavené dostatočne veľkou pamäťou, takže si môže dočasne uložiť namerané údaje v prípade, že je mimo pokrytia mobilnej siete.

Zariadenie je možné automaticky a na diaľku konfigurovať zo serverovej časti systému EMH.

1.4.1.3 Komunikačný klient pre PC

PC klient je softvérová verzia Komunikačného zariadenia, ktorú je možné používať na PC vybavenom bluetooth a prístupom na sieť4. Poskytuje všetky funkcie Komunikačného zariadenia. Okrem toho PC klient môže používať ľubovoľnú IP sieť pripojenú k PC a teda môže pracovať aj v podmienkach, kde nie je pokrytie mobilnej siete.

Aplikácia sa spúšťa v operačnom systéme Windows ako štandardná PC aplikácia. Má okno, v ktorom sa zobrazuje úplne rovnaké používateľské rozhranie ako ma Komunikačné zariadenie.

1.4.1.4 Aplikačná gateway a prehliadač pre Android

Aplikácia pre Android je gateway a zároveň aj prezentačná aplikácia. Môže teda zbierať merania zo senzorov a posielať ich na server, ale môže tiež pristupovať k údajom uloženým na serveri a zobrazovať ich používateľovi. Aplikácia je určená smartfóny so systémom Android 2.3 (a vyšším)5.

Android aplikácia bola navrhnutá pre osoby so základnou znalosťou používania smartfónov. Aplikácia sa ovláda cez dotykový displej a štandardne tlačidlá systému Android. Aplikačné rozhranie používa symboly a jednoduchý jazyk. Okrem toho používa sprievodcu používateľa pre uľahčení procesu merania.

Aplikácia používa na komunikáciu so senzormi spojenie Bluetooth, a na komunikáciu so serverovým systémom EMH používa dostupnú IP sieť (GPRS/3G, Wi-Fi). Zariadenie používa manuálne zadávanie typu merania, ktoré sa má vykonať a následne vyhľadá príslušné senzory. Aplikácia používa dostupnú pamäť zariadenia na dočasné uloženie meraní v prípade, že IP sieť je nedostupná, takže môže pracovať aj samostatne.

Aplikácia podporuje niekoľko typov autentifikácie v závislosti na požadovanej úrovni bezpečnosti. Používatelia sa môžu autentifikovať pomocou hesla alebo PIN-u, alebo automaticky.6

Aplikácia sa konfiguruje automaticky zo servera systému EMH.

Aplikácia poskytuje možnosť manuálneho vyplnenia dotazníkov, ktoré sú zaregistrované na EMH. Dotazníky sa vypĺňajú pomocou rozhrania dotykového displeja.

Aplikáciu je možné použiť na merania pre viacerých pacientov pomocou jedného zariadenia. Napríklad sestra v teréne môže používať smartfóne na meranie a vyplňovanie dotazníkov pre viacerých pacientov.

Aplikácia umožňuje filtrovanie SMS správ. Správy odoslané od lekára neskončia v schránke správ, ale sú presmerované do aplikácie. Týmto spôsobom sú správy o zdravotnom stave oddelené od ostatných a tým je chránené súkromie pacienta.

Aplikácia poskytuje prístup do osobného zdravotného záznamu uloženého na serveroch systému EMH. Prehliadač je možné použiť na zobrazenie všetkých uložených meraní, poznámok, a tiež na prezeranie v minulosti vyplnených dotazníkov.

---

[3] Integrácia ďalších senzorov môže mať vplyv na celkovú MDD certifikáciu systému.
[4] PC nie je súčasťou ponuky EMH.
[5] Vzhľadom na nekonzistencie medzi rôznymi verziami Android zariadení odporúčame otestovať aplikácie s konkrétnymi zariadeniami pred tým, než ich budú používať pacienti.
[6] Všetci používatelia majú pridelené heslá a môžu sa rozhodnúť, či použijú heslo, PIN alebo automatickú autentifikáciu.

1.4.2 Mobilná jednotka

Mobilná jednotka je súčasťou dodávky systému EMH. Obsahuje sadu senzorov a komunikačnú jednotku. Od verzie EMH 3.3 sú podporované tzv. Flexibilné Mobilné Jednotky. Flexibilné mobilné jednotky môžu pozostávať z ľubovoľnej kombinácie podporovaných senzorov a hubov. Výsledná sada senzorov môže byť zostavená presne podľa špecifických požiadaviek konkrétneho zákazníka.

1.4.3 Centrálna jednotka EMH

1.4.3.1 M2M Platforma

Centrálna jednotka EMH poskytuje M2M platformu, ktorá slúži na:

- manažment vzdialených senzorov a hubov
- ukladanie nameraných údajov
- prístup a filtrovanie uložených nameraných údajov

V systéme EMH je M2M platforma použitá na manažment a senzorov a hubov a na ukladanie nameraných údajov zo všetkých senzorov. M2M platformu je možné rozšíriť tak, aby podporovala aj ďalšie typy meraní z medicínskej oblasti ale aj z iných oblastí.

1.4.3.2 Osobný zdravotný záznam

Osobný zdravotný záznam je časť centrálneho systému EMH, kde sú uložené rôzne osobné údaje pacientov. Osobné údaje pozostávajú zo statických údajov, ktoré sa zadávajú pri vytvorení záznamu (demografické údaje) a z dynamických údajov, ktoré sa ukladajú, keď pacient systém používa. Dynamické údaje sú z meracích zariadení, od pacienta samotného a zo zdravotných exportov. Dynamické údaje môžu byť nasledovného typu:

- Merania – údaje získané zo senzorov a hubov
- Dotazníky – rôzne dotazníky, ktoré vypĺňajú pacienti, zdravotnícky personál a lekárski experti
- Uložené dokumenty – rôzne dokumenty ktoré môžu do systému uložiť pacienti, zdravotnícky personál a lekárski experti, napríklad to môžu byť naskenované obrázky EKG.
- Poznámky – poznámky, ktoré môžu poskytovať vysvetlenia k meraniam, dokumentom, stanovovať diagnózy, hovoriť o tom, ako sa pacient cítil v určitom čase, a podobne. Zadávajú sa ako text s jasným označením času a autora.

Ku všetkým údajom osobného zdravotného záznamu je možné zistiť autora. Systém umožňuje filtrovanie údajov. (Napríklad, lekár môže odfiltrovať všetky údaje zadané samotnými pacientmi a sústrediť sa len na objektívne informácie.)

1.4.3.3 Prahové hodnoty a inteligencia

Osobný zdravotný záznam umožňuje nastavenia prahových hodnôt meraní individuálne pre každého pacienta. Nastavené prahové hodnoty sa zobrazia po prihlásení do systému a porovnajú sa so skutočnými nameranými hodnotami. Okrem toho systém môže posielať SMS a emailové notifikácie pri prekročení prahových hodnôt.
V systéme sú zapracované referenčné tabuľky pre funkcie pľúc, ktoré môžu byť použité pri analýze funkcie pľúc pacientov, pričom funkcia pľúc pacienta je vyjadrená ako % referenčnej hodnoty.

1.4.3.4 Rozhodovací komponent

Rozhodovací komponent (CDSS) poskytuje vhodné užívateľské rozhranie, integráciu s externými repozitármi dát (tlak, SpO2, EKG, glykémia, váha), na základe ktorých detekuje anomálie vo vstupných dátových obrazcoch, generuje klasifikáciu a predikciu vývoja zdravotného stavu pacienta a umožňuje adresné poskytovanie informácií za účelom podpory rozhodovania medicínskeho personálu.

Charakteristika CDSS:

- Oddelenie rozhodovacej logiky od aplikačného kódu
- Vývoj a implementácia rozhodovacej logiky nezávisle od aplikácie
- Vyjadrenie rozhodovacej logiky pomocou produkčných pravidiel vo forme “if-then” výrokov
- Formovanie doménového slovníka za účelom popisu objektov a vzťahov pomocou produkčných pravidiel

- Implementácia rozhodovacej logiky ako nezávislej entity vo forme vykonateľnej množiny pravidiel volanej priamo aplikáciou
- Prostredníctvom vhodného užívateľského rozhrania je umožnená implementácia pravidiel priamo doménovými expertmi/analytikmi bez potreby podpory zo strany IT expertov
- Vyjadrenie pravidiel v prirodzenom jazyku
- Rozšírené možnosti vyhľadávania jednotlivých pravidiel alebo skupín pravidiel vo viacerých projektoch súčasne
- Prehľad histórie vývoja pravidiel a verzií rozhodovacieho systému
- Testovanie a simulácia rozhodovacích a predikčných scenárov a algoritmov

CDSS umožňuje zlúčenie výsledkov práce aplikačného a znalostného tímu, ktoré môže prebiehať aj v externých nástrojoch. Týmto je umožnené modelovanie znalostí pomocou diskrétnych štruktúr (logické a fuzzy znalosti), ontológií (podpora OKBC protokolu, OWL), Arden Syntax, GLIF. Jednotlivé formalizmy je možné ľubovoľne voliť v závislosti od požadovaných výstupov (na základe presného procesného modelu telemedicínskej služby) a požadovanej miery zdieľateľnosti modelovaných znalostí medzi CDSS systémami.

V rámci užívateľského rozhrania poskytuje rozhodovací komponent generovanie prehľadných preddefinovaných grafických výstupov (3D grafy, mapy atď.) ako aj možnosť začlenenia vlastných Java vizualizačných formátov pre desktop alebo JSF, Dojo webových užívateľských rozhraní.

1.4.3.5 Plánovanie meraní

Systém umožňuje nastavovať rozvrh meraní. Po nastavení rozvrhu meraní môže systém posielať upozornenia pacientom a/alebo lekárom o tom, že meranie nebolo urobené v súlade s rozvrhom.

1.4.3.6 Webový prehliadač

Systém poskytuje webovú aplikáciu, ktorá umožňuje správu systému. Nasledujúci zoznam obsahuje najdôležitejšie funkcie webového prehliadača.

- Administrácia pacientov, lekárov a sestier
- Zobrazovanie údajov zo senzorov
- Písanie poznámok o pacientoch a meraniach
- Nastavovanie rozvrhu meraní
- Správa stavu pacienta zdravotníckym personálom ako podpora procesu vzdialeného monitorovania
- Špecifikácia prahových hodnôt meraní a prehľad o tom, kedy boli prekročené
- Zobrazenie hodnôt funkcie pľúc ako % referenčných hodnôt

1.4.4 Režimy prevádzky

Systém EMH umožňuje tri režimy prevádzky, ktoré sú popísané nižšie:

1.4.4.1 Jeden používateľ

V režime jedného používateľa je Mobilná Jednotka priradená len jednému pacientovi, ktorý ju dlhodobo používa. Preto v tomto prípade nevzniká potreba administrácie a rekonfigurácie zariadenia. Primárne je tento režim určený pre liečenie chronických chorôb, kde jeden pacient používa jednu mobilnú jednotku dlhší čas.

1.4.4.2 Viacerí používatelia

V režime viacerých používateľov sa jedna Mobilná jednotka používa na merania viacerých pacientov. Tento režim podporuje rýchlu zmenu priradenia mobilnej jednotky k inému pacientovi na serverovej časti.

1.4.4.2.1 Sestra v teréne

Sestra v teréne je jednou z možností použitia systému v režime viacerých používateľov. V tomto prípade je jedna mobilná jednotka priradená sestre v teréne, ktorá navštevuje pacientov a robí merania.

Zmena priradenia pacienta ej možná cez web prehliadač alebo pomocou Android aplikácie[7].

1.4.4.2.2 Režim Off-line a sestra v teréne

Android aplikácia umožňuje použitie režimu sestra v teréne aj v oblastiach, kde nie je pokrytie. V tomto prípade je ale nutné, aby mala Android aplikácia voppred uložený zoznam pacientov, ktorých merania sa budú robiť.

1.4.4.3 Režim kiosk

V tom tomto prípade je mobilná jednotka poskytnutá skupine používateľov a umiestnený v kiosku, stánku alebo v miestnosti. Miestnosť je vybavená mobilnou jednotkou a PC. Pacient pomocou mobilnej jednotky urobí merania a pošle ich na server. PC pacient používa na komunikáciu s lekármi a na prezeranie výsledkov vlastných meraní cez web rozhranie EMH.

V režime kiosk:

- je aplikácia EMH integrovaná s rezervačným systémom eBooking. Systém eBooking používajú operátori aj pacienti. Operátori ho používajú na plánovanie Operátori návštev pacientov v kiosku a pacienti ho používajú na to, aby si skontrolovali čas, kedy majú navštíviť kiosk.
- V režime kiosk poskytuje sysém EMH integráciu s jednoduchým video call systémom. Video hovor sa vždy zostavuje medzi zamestnancom a operátorom. Iniciátorom hovoru je vždy zamestnanec. Zvyčajne sa hovor robí z PC umiestneného v kisoku, stánku alebo vyhradenej mestnosti.

1.4.5 Aplikačné rozhrania (APIs)

Systém EMH 3.3 poskytuje množinu aplikačných rozhraní, ktoré sa používajú na integráciu so systémami a produktmi tretích strán. API poskytujú nasledovnú funkcionalitu:

- Integráciu s novými senzormi a hubmi
- Integráciou nových prehliadačov
- Použitie EMH ako integrálnej súčasti externých zdravotných záznamov
- Možnosť integrácie pomocou rozhrania Parlay X 2.1 in pre posielanie SMS

Aplikačné rozhrania sú založené na ľahkých **HTTP protokoloch,** ktoré majú širokú podporu v rôznych aplikačných programovacích prostrediach.

1.4.6 Zdravotnícka certifikácia

Celý systém je zdravotnícky certifikovaný v súlade s EU Medical Device Directive (MDD). Takže ho je možné používať na zdravotnícke účely v zdravotníckych zariadeniach aj mimo nich.

1.4.7 Integrácia s NZIS a Národným telemedicínskym centrom

Navrhované riešenie je otvorené pre vytvorenie komunikačného rozhrania systému Ericsson Mobile Healt s národnými inštitúciami poskytujúcimi informatické služby pre zdravotníctvo. Predpokladmi pre zriadenie takéhoto prepojenia sú:

- legislatívne zmeny umožňujúce zriadenie takéhoto prepojenia,
- zriadenie a vypublikovanie informatických služieb ich poskytovateľmi, na základe ktorých bude možné takého prepojenie zrealizovať,
- technická dokumentácia a testovacie prostredie pre umožnenie overenia tejto funkcionality.

[7] Vzhľadom na limitované používateľské rozhranie komunikačné zariadenie neumožňuje priradenie inému pacientovi. Priradenie je nutné urobiť vo web rozhraní alebo pomocou Android aplikácie.

1.5 Prierezové moduly

1.5.1 Architektúra riešenia

Riešenie bude koncipované ako moduly Modulárneho akademického informačného systému (MAIS) - systému pre správu pedagogických procesov. Modul bude využívať spoločné rozhrania pre riadenie prístupu vedeckovýskumných pracovníkov k jednotlivým vedeckým úlohám.

Architektúra modulu bude vychádzať zo štandardnej architektúry modulov v MAISe - viacvrstvá architektúra obsahujúca:

- dátovú vrstvu,
- aplikačnú vrstvu a
- prezentačnú vrstvu

1.5.1.1 Návrh dátovej vrstvy

Ako systém riadenia báze dát bude použitý systém PostgreSQL 8.4, v ktorom bude modul využívať tabuľkový priestor aplikácie MAIS. Toto riešenie je navrhnuté najmä z dôvodu úzkej spolupráce s aplikáciou MAIS a použitie jej zálohovacích mechanizmov

1.5.1.2 Návrh aplikačnej vrstvy

Na postavenie aplikačnej vrstvy bude použitý aplikačný server JBoss AS, ktorý využíva architektúru na báze tzv. Microkernel komponentov postavených na báze Java Management Extensions – JMX. V rámci aplikačnej vrstvy bude pre prácu s dátami použitá technológia Hibernate a pre spojenie s databázou vrstvou budú použité technológie založené na štandardoch JTA a JDBC.

1.5.1.3 Návrh prezentačnej vrstvy

Modul bude koncipovaný ako web-based aplikácia s interentovým prehliadačom ako klientským rozhraním. Na prezentáciu údajov sa bude využívať technológia JSP a JSF s podporou JSTL knižnice a Spring. Ako kontainer pre túto vrstvu bude použitý servlet kontainer TOMCAT. Výmena údajov bude prebiehať prostredníctvom objektového protokolu RMI (Remote Method Invokation) pre Java-to-Java komunikáciu, ktorá umožňuje bezpečne oddeliť server prezentačnej vrstvy od servera s aplikačnou logikou.

1.5.1.4 Návrh podporných modulov

1.5.1.4.1 Riadenie prístupu používateľov

Riadenie prístupu používateľov bude realizované pomocou rozhraní v systéme MAIS. Systém MAIS umožňuje definovať prístup a overovanie používateľov pre prácu s jednotlivými modulmi, definíciu skupiny práv (rolí) pre jednotlivých používateľov a samostatný webový modul pre ich manažment.

1.5.1.4.2 Aplikačná bezpečnosť

Modul využíva zabezpečený protokol (HTTPS) pri komunikácií medzi klientom (internetovým prehliadačom) a serverom a rozhranie pre prístup k dátam je overované oproti používateľskému tokenu. Prístup na dátovú vrstvu bude obmedzený iba pre aplikačný server.

1.5.2 Funkcionalita prierezových modulov

1.5.2.1 Modul Podpora komunikácie vedeckovýskumných pracovníkov v rámci plnenia vedeckých úloh

Modul Podpora komunikácie vedeckovýskumných pracovníkov v rámci plnenia konkrétnych vedeckých úloh – komunikácia vedeckovýskumných pracovníkov medzi sebou za účelom konzultácií v rámci výskumu a plnenia čiastkových cieľov projektov /výskumov/, komunikácia vedeckovýskumných pracovníkov so zazmluvnenými partnermi na projektoch za účelom zadávania konkrétnych vedeckovýskumných úloh, bližšie popisy predstáv o výsledkoch výskumu a pod.

Funkcionalita modulu:

- online komunikácia ,
- komunikácia na základe autorizovaného prístupu ,
- možnosť exportovať úlohy, zadania, popisy, komunikačné jednotky vo formátoch ako napr. pdf, doc, xls, rtf,
- možnosť publikácie exportovaných údajov na web,
- zabezpečenie prenosu poznatkov formou e-mailu alebo krátkej správy jednotlivým adresátom, alebo skupine vybratých adresátov,
- modul musí zabezpečiť podporu komunikácie aj s partnermi zo zahraničia,

Komunikácia na zabezpečenie plnenia výskumných úloh by mala prebiehať vo forme:

- zverejňovania na web,
- zverejňovania v rámci systému IS VVV,
- zverejňovania prostredníctvom e-mailu.

1.5.2.2 Modul Zabezpečenie prenosu poznatkov v súvislosti s využívaním výskumných zariadení

Modul umožní každému výskumníkovi jednotlivo prenos poznatkov o jeho výskume, podporu spolupráce pri výskume možnosťou zadefinovať viacerých pracovníkov na výskume, pričom každému umožní priradiť jeho rolu (úlohu) na vedeckom zadaní. Každý výskumník musí mať do modulu samostatný prístup na základe autentifikácie. Jeho osoba je previazaná s konkrétnym projektom, v rámci projektu s konkrétnou výskumnou úlohou a na toto je naviazaný prenos poznatkov o priebehu jeho výskumu. Potrebné je zadefinovať osoby spolupracujúce na výskumnej úlohe, ich pracovné povinnosti v rámci vedeckej úlohy a umožniť im prenos poznatkov o nameraných hodnotách a získaných poznatkoch medzi spolupracovníkmi.

Funkcionalita modulu:

- online komunikácia,
- možnosť obmedzenia cieľových skupín, tzn. možnosť označiť komu budú čiastkové ciele výskumu sprístupnené,
- možnosť nadefinovať externých spolupracovníkov na výskume – keďže na výskume sa nepodieľajú len zamestnanci verejného obstarávateľa, ale aj výskumníci z hospodárskej praxe, resp. z partnerských spoločností. Týmto výskumníkom bude umožnené zadať čiastkové vedeckovýskumné úlohy a zabezpečiť možnosť spolupráce s výskumníkmi z radov verejného obstarávateľa bez potreby osobnej prítomnosti v zariadeniach obstarávateľa.

1.5.2.3 Modul Podpora práce výskumníkov – „Záznamník výskumníka“

Modul „Záznamník výskumníka“ umožní zaznamenávať merania a čiastkové výsledky vedeckej činnosti a vytvárať databázu výsledkov, ktorá bude ďalej používaná na ďalší výskum. Údaje v databáze musia byť ďalej analyzované a vyhodnocované v rámci výskumnej činnosti. Medzi záznamami je potrebné vyhľadávať, triediť a musí byť možnosť ich ďalšieho spracovania. Výsledky meraní musí byť možné priamo importovať do systému a následne ich priradiť ku konkrétnym vedeckým úlohám na ďalšiu analýzu a pripomienkovanie.

Čiastkové výsledky výskumu a merania budú evidované v rámci projektov, resp. konkrétnych výskumných úloh. Ku výskumnej úlohe je potrebné priradiť výskumníkov, ktorí musia mať k nej prístup a budú tiež môcť do nej zaznamenávať výsledky svojich parciálnych úloh.

Konkrétna vedecká úloha bude v záznamníku rozdelená na čiastkové úlohy, ktoré budú priradené na skúmanie ďalším výskumníkom. Vedecká úloha bude rozdelená na teoretickú časť a praktickú časť. Teoretická časť bude

slúžiť na zaznamenávanie podkladov ku výskumu, spracovanie teoretickej časti výskumnej úlohy, pripomienkovanie spracovaného textu v rámci výskumu a to osobami priradenými ku vedeckej úlohe. Praktická časť vedeckej úlohy bude slúžiť na nahrávanie a ďalšie skúmanie konkrétnych výsledkov meraní. Údaje budú uložené na jednom mieste, aktuálne, prístupné z ktoréhokoľvek miesta s prístupom na internet. Tým bude umožnená jednoduchá a rýchla komunikácia výskumníkov bez potreby osobných stretnutí. Priložené súbory s výsledkami meraní je možné sprístupniť na čítanie, alebo aj na editáciu, takže sa zanikne potreba tlače a posielania nameraných údajov, čím bude možné skrátiť čas na reakciu a tým pádom na výskum samotný.

Pre úlohu sú požadované stavy: Vytvorená, Priradená, Akceptovaná, Hotová. Čiastková úloha bude priradená výskumníkovi, jemu príde notifikačná správa o priradení úlohy, v systéme si ju skontroluje. Poznačí si poznámky ku výskumu, akceptuje úlohu. Zadávateľ vidí, že úloha bola akceptovaná. Výskumník plní vedeckú úlohu, píše k nej poznámky, priradí súbor s meraniami. Zadávateľovi, alebo všetkým členom pracovnej skupiny príde notifikačná správa, že k čiastkovej úlohe bol priradený výsledok merania (iba na čítanie, na editáciu). Zadávateľ kontroluje plnenie čiastkových úloha dáva dohromady výsledok výskumu, sleduje, koľko a akých čiastkových úloh ostáva na spracovanie, sleduje priebeh spracovania úloh. Zadávateľ úloh musí mať možnosť pridať poznámku, resp. komentár ku úlohe a ku výsledku merania. Poznámky zostávajú v systéme, ku vybranej časti poznámok je potrebné mať možnosť pridať komentár, vyjadriť sa.

1.5.2.4 Modul Podpora vzdelávania a komunikácie pre semestrálne, bakalárske a diplomové prace

Modul poskytuje nástroje pre podporu vzdelávania a komunikácie pri tvorbe semestrálnych a záverečných prác. Umožňuje komunikáciu medzi zadávateľmi, riešiteľmi a konzultantmi nad rôznymi verziami práce vo forme poznámok, návrhov a doporučení, čím zefektívňuje tvorbu práce a umožňuje zadávateľom mať prehľad o tvorbe práce v každej jej fáze. Ku jednotlivým prácam je možné pripájať externé zdroje v elektronickej podobe ako citácie, referencie, študijné materiály a pod. Modul musí umožňovať zadávať úlohy súvisiace z tvorbou práce (napr. ohodnotenie vedúcim, vyžiadanie doplnenia a pod.) pre používateľov participujúcich na práci a k tomu obsahuje aktívnu podporu pri kontrole termínov s možnosťou upozornení vo forme exportov alebo pripomienok v elektronickej podobe. Modul podporuje a automatizuje v procese tvorby práce nasledujúce fázy:

- podpora definície vzťahov pre používateľov v kontexte vytváranej práce,
- podpora pridávania rôznych verzií práce s možnosťou ich porovnávania pre vybrané formáty,
- podpora možnosti definície poznámok, návrhov a doporučení používateľmi pre rôzne verzie práce i jednotlivé časti práce,
- podpora definície prepojenia s inými elektronickými zdrojmi informácií vo forme referencií,
- podpora zadávania úloh pre participantov tvorby práce s možnosťou definície časových obmedzení pre jednotlivé úlohy,
- automatizácia kontroly časových obmedzení s možnosťou upozornení v elektronickej podobe.

1.5.2.5 Modul Testovanie formou tlačených testov

Modul predstavuje aplikáciu umožňujúcu rýchle a efektívne vyhodnotenie písomných testov a písomných dotazníkov čím predstavuje vysoko efektívny nástroj pre testovanie veľkého počtu osôb bez potreby prostriedkov IKT vo fáze vypracovania samotného testu. Z hľadiska celého procesu testovania aplikácia podporuje a v rôznej miere automatizuje jeho nasledovné fázy:

- podpora prípravy testovacích otázok, definícia správnych odpovedí a stanovenie obtiažnosti a ohodnotenie otázky,
- podpora prípravy testov s viacerými prístupmi pri generovaní testov ako napríklad rôzne testy pre viaceré skupiny študentov – mutácie testov, premiešanie otázok, jedinečné testy pre každého študenta a pod.,
- príprava skúšobných hárkov,

- príprava štítkov na skúšobné hárky zabezpečujúce anonymitu preskúšavaných študentov,
- automatické vyhodnotenie odovzdaných testov.

Modul prostredníctvom špecializovaných štítkov zabezpečuje anonymitu skúšaných študentov, čím eliminuje riziko ovplyvňovania procesu vyhodnotenia na rôznych úrovniach. Ďalším faktorom je eliminácia ľudského faktoru z procesu vyhodnotenia písomných testov čím odpadá riziko chybovosti pri vyhodnocovaní písomných testov.

1.5.2.6 Modul Testovanie formou elektronického testovania

Modul má slúžiť na umožnenie plnohodnotné elektronického preskúšanie študentov v učebni IKT, podporu plnej automatizácie vyhodnotenia skúšania a elimináciu ľudského faktoru v tejto fáze, čím sa výrazne zníži riziko chybovosti vyhodnotenia testov, čo predstavuje nemalú úsporu času pedagógov. V procese preskúšania a testovania je požadovaná podpora a automatizácia jeho nasledovných fáz:

- podpora prípravy testovacích otázok, definícia správnych odpovedí a kategorizácia otázok podľa ich obtiažnosti,
- podpora tvorby multimediálneho obsahu otázok,
- podpora prípravy testov s viacerými prístupmi pri generovaní testov,
- podpora férového priebehu online preskúšania evidovaním dĺžky trvania testu, blokovaním počítača v prístupe na internet a pod.,
- podpora distančného preskúšania online,
- automatické vyhodnotenie výsledkov testov,
- štatistické vyhodnotenie preskúšania podľa zvyklostí vyučujúcich na univerzite.

K požadovaným funkcionalitám modulu patrí aj zaznamenávanie postupov študenta pri skúšaní, čím je možné získať pohľad na vedľajšie aspekty preskúšania (ako napríklad rýchlosť odpovede, rozhodnosť študenta pri voľbe odpovede a podobne), ako aj podpora diferencovaného preskúšania využívaného v rámci inovatívnych diferencovaných vyučovacích metód.

1.6 Cena Diela

Číslo		Počet [ks]	Jednotková cena v EUR bez DPH	Cena spolu v EUR bez DPH	Cena spolu v EUR s DPH
1	**Informačný systém pre podporu výskumu, vývoja a vzdelávania**			**3 352 083,33**	**4 049 500,00**
1.1	**Modul Enviro**			**554 166,00**	**664 999,20**
1.1.1	Architektúra, implementácia, testovanie, dokumentácia softvérových komponentov evidencia projektov, kontrola údajov, export, import existujúcich údajov, automatizovaný zber údajov, prepojenie na externé zdroje, GIS, evidencia informačných zdrojov SZU, systémové nástroje	1	554 166,00	554 166,00	664 999,20
1.2	**Modul skríning**			**341 666,00**	**409 999,20**
1.2.1	Architektúra, implementácia, testovanie, dokumentácia softvérových komponentov skríningový portál (riadenie prístupu používateľov, elektronické formuláre, generovanie čiarového kódu, tvorba a tlač dokumentu, prístup k informáciám, notifikácia), integračné komponenty, DMS (Document Management System), reporting a monitoring, Content management system (CMS)	1	341 666,00	341 666,00	409 999,20
1.3	**Modul telemedicína**			**910 420,33**	**1 119 504,40**
1.3.1	**Mobilné jednotky**			60 064,00	99 076,80
1.3.1.1	Mobilná jednotka - Cardio 1 (EKG 1, pulzný oximeter, tlakomer, komunikačná jednotka)	4	3 625,00	14 500,00	17 400,00
1.3.1.2	Mobilná jednotka - Cardio 2 (EKG 6, pulzný oximeter, tlakomer, váha, komunikačná jednotka)	4	3 833,00	15 332,00	18 398,40
1.3.1.3	Mobilná jednotka - Diabetes 1 (Glukomer, komunikačná jednotka)	4	1 750,00	7 000,00	8 400,00
1.3.1.4	Mobilná jednotka - Diabetes 2 (Glukomer, tlakomer, váha, komunikačná jednotka)	4	2 250,00	9 000,00	10 800,00
1.3.1.5	Mobilná jednotka - Diabetes 3 (Glukomer, tlakomer, váha, EKG 1, komunikačná jednotka)	4	3 558,00	14 232,00	17 078,40
1.3.1.6	SW komponenty pre mobilné jednotky	20	1 125,00	22 500,00	27 000,00
1.3.2	**Centrálna jednotka**			850 356,33	1 020 427,60
1.3.2.1.	Architektúra, implementácia, testovanie, dokumentácia, komponentov komunikačný hub, úložisko údajov, zdravotný záznam pacienta, generátor upozornení, rozhodovací komponent, prezentačný portál	1	742 156,33	742 156,33	890 587,60
1.3.2.2	Dodatočné analytické a programátorské práce (v jednotkách človekodeň)	200	541,00	108 200,00	129 840,00
1.4	**Prierezové moduly**			**1 141 665,00**	**1 369 998,00**
1.4.1	Modul - Podpora komunikácie vedeckovýskumných pracovníkov v rámci plnenia konkrétnych vedeckých úloh	1	183 000,00	183 000,00	219 600,00
1.4.2	Modul - Zabezpečenie prenosu poznatkov v súvislosti s využívaním výskumných zariadení	1	237 333,00	237 333,00	284 799,60
1.4.3	Modul - Podpora práce výskumníkov (záznamník výskumníka)	1	288 000,00	288 000,00	345 600,00
1.4.4	Modul - Testovanie formou tlačených testov	1	129 404,00	129 404,00	155 284,80
1.4.5	Modul - Testovanie formou elektronického testovania	1	154 239,00	154 239,00	185 086,80
1.4.6	Modul - Podpora vzdelávania a komunikácie pre semestrálne, bakalárske a diplomové práce	1	149 689,00	149 689,00	179 626,80
1.5	**Bezpečnostný projekt**			**404 166,00**	**484 999,20**
1.5.1	Bezpečnostný zámer, analýza bezpečnosti, bezpečnostné smernice	1	41 666,00	41 666,00	49 999,20
1.5.2	Technické komponenty bezpečnosti (design, implementácia)	1	362 500,00	362 500,00	435 000,00

Objednávateľ

V Bratislave, dňa 07.02.2013

.....
Dr. h. c. prof. PhDr. Dana Farkašová
Rektorka

Zhotoviteľ

V Bratislave, dňa 07.02.2013

.....
Ladislav Plánka
konateľ