VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

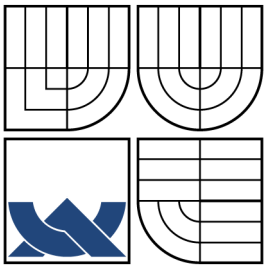
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF BIOMEDICAL ENGINEERING

OBRAZOVÁ DOKUMENTACE V NEMOCNIČNÍM INFORMAČNÍM SYSTÉMU

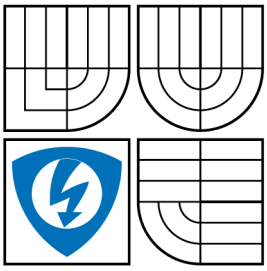
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE TOMÁŠ RÁŠO
AUTHOR

BRNO 2007/2008



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

FACULTY OF ELECTRICAL ENGINEERING AND
COMMUNICATION
DEPARTMENT OF BIOMEDICAL ENGINEERING

OBRAZOVÁ DOKUMENTACE V NEMOCNIČNÍM INFORMAČNÍM SYSTÉMU

IMAGE DOCUMENTATION IN HOSPITAL INFORMATION SYSTEM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — TOMÁŠ RÁŠO
AUTHOR

VEDOUCÍ PRÁCE — ING. PETR FEDRA
SUPERVISOR

BRNO 2007/2008

ZDE VLOŽIT LIST ZADÁNÍ

Z důvodu správného číslování stránek

ZDE VLOŽIT PRVNÍ LIST LICENČNÍ SMOUVY

Z důvodu správného číslování stránek

ZDE VLOŽIT DRUHÝ LIST LICENČNÍ SMOUVY

Z důvodu správného číslování stránek

ABSTRAKT

Tato diplomová práce popisuje nemocniční informační systém (NIS) CLINICOM se zaměřením na oddělení radiologie. Rozebírá problematiku přenosu obrazové dokumentace pacientů prostřednictvím sítě Internet a poskytuje návod pro realizaci rozhraní dálkového přístupu na oddělení radiologie. Kromě toho slouží jako podrobný průvodce instalací a konfigurací programových komponent NIS CLINICOM.

KLÍČOVÁ SLOVA

obrazová dokumentace, NIS, CLINICOM, datový standard, etický kodex, RTG, CareCenter, server Apache

ABSTRACT

This thesis describes the hospital information system (HIS) CLINICOM, focusing on the department of radiology. It analyses the problems linked with Internet transport of patient image documentation and it provides instructions how to create remote access interface on the department of radiology. It gives also a detailed guide describing installation and components configuration of HIS CLINICOM.

KEYWORDS

image documentation, HIS, CLINICOM, data standard, etics code, RTG, CareCenter, server Apache

RÁŠO T. *Obrazová dokumentace v nemocničním informačním systému: diplomová práce*. Brno: Vysoké Učení Technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav biomedicínského inženýrství, 2008. 89 s. Vedoucí práce byl Ing. Petr Fedra.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Obrazová dokumentace v nemocničním informačním systému“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

(podpis autora)

Děkuji vedoucímu diplomové práce Ing. Petru Fedrovi za odbornou pomoc a metodické rady při realizaci této diplomové práce.

V Brně dne 20. května 2008

.....

Tomáš Rášo

OBSAH

Úvod **12**

1 Analýza studentské práce **13**
1.1 Nemocniční informační systém 13
1.1.1 Co se rozumí pod pojmem NIS? 13
1.1.2 Elektronický záznam o pacientovi 14
1.1.3 Obecná struktura NIS 15
1.1.4 Obecná struktura obrazové dokumentace v NIS 20
1.1.5 Nemocniční informační systém CLINICOM 22
1.2 Problematika pacientských dat 25
1.2.1 Etické otázky týkající se ochrany pacientských dat 25
1.2.2 Současná legislativa ČR týkající se ochrany osobních dat v NIS 30
1.3 Problematika přenosu pacientských dat 37
1.3.1 Národní zdravotnický informační systém 37
1.3.2 Datové standardy a jejich využití při komunikaci 38
1.3.3 Zabezpečení přenosu pacientských dat mezi NIS 43

2 Výsledky studentské práce **50**
Průvodce instalací a konfigurací – NIS CLINICOM 50
2.0.4 Server Apache 50
2.0.5 OpenSSL 51
2.0.6 Caché 55
2.0.7 Caché Weblink 56
2.0.8 Program radiologického oddělení (RTG) 56
2.1 Konfigurace Správce zdrojů dat ODBC 58
2.2 CareCenter 62
2.3 Komunikace programů CareCenter a RTG 62
2.4 Webové rozhraní programu RTG 63

3 Závěr **69**

Literatura **70**

Seznam symbolů, veličin a zkratek **74**

Seznam příloh **77**

A Realizace NIS CLINICOM s webovým rozhraním RTG **78**

B Úprava rutin v programu Caché Terminal **79**
B.1 Zavedení rutin ze souboru "mgw.ro" 79
B.2 Zavedení rutiny "mgw1.ro" 80
B.3 Zavedení rutiny "%ZMGW2.rsa" 81
B.4 Zavedení rutiny "mgwstubs.ro" 82
B.5 Zavedení rutiny "ZSTU.rsa" 83
B.6 Zavedení databáze RTG 84

C Obsah přiloženého cd **89**

SEZNAM OBRÁZKŮ

1.1 Koncepce NIS CLINICOM [9] 24
1.2 Ukázka seznamu položek v NLČP [31] 41
1.3 Referenční komunikační model ISO/OSI 43
1.4 Postavení firewallu v síti s NIS 45
1.5 Bitové ekvivalenty šifrovacích metod 47
1.6 Princip programu SafeBoot [38] 48
1.7 Umístnění protokolu SSL v modelu TCP/IP 49
2.1 Základní architektura sítě vzhledem k programu Caché WebLink . . . 57
2.2 Editor nastavení modulu RTG 58
2.3 Správce uživatelů www přístupu k programu RTG 59
2.4 Správce zdrojů dat ODBC – základní rozhraní 59
2.5 Správce zdrojů dat ODBC – nastavení parametrů 60
2.6 Správce zdrojů dat ODBC – test konektivity 60
2.7 Správce zdrojů dat ODBC – test spojení pomocí příkazu ping 61
2.8 SDF nastavení v programu CareCenter 62
2.9 Grafické rozhraní programu CareCenter – seznam pacientů 63
2.10 Přiřazení snímku pacientovi v programu RTG 64
2.11 Komunikace klient – server u programu RTG 65
2.12 Přihlašovací okno na RDO oddělení 66
2.13 Webové rozhraní pro přihlášení na radiologické oddělení ÚBMI 66
2.14 Seznam pacientů v systému RDO 67
2.15 Ukázka záznamu pacienta 67
2.16 Ukázka záznamu pacienta 68
2.17 Prohlížení snímků pacienta 68
B.1 Zavedení rutin ze souboru "mgw.ro" 79
B.2 Zavedení rutiny "mgw1.ro" 80
B.3 Zavedení rutiny "%zmgw2.rsa" 81
B.4 Zavedení rutiny "mgwstubs.ro" 82
B.5 Zavedení rutiny "zstu.rsa" 83
B.6 Vytvoření nového "Namespace" 84
B.7 Pojmenovaní "Namespace" 85
B.8 Načtení nové databáze 85
B.9 Pojmenování nové databáze 86
B.10 Lokalizace nové databáze 86
B.11 Potvrzení vybrané databáze 87
B.12 Přidání databáze do konfiguračního souboru 87
B.13 Kompletně vytvořená databáze 88

ÚVOD

Diplomová práce nazvaná Obrazová dokumentace v nemocničním informačním systému úzce navazuje na předcházející semestrální projekt stejného názvu. Jejím cílem je vytvoření ucelené práce, která svým obsahem a zpracováním pomůže (nejenom) odborné veřejnosti proniknout hlouběji do světa nemocničních informačních systémů (NIS). Práce se zaměřuje na pacientskou obrazovou dokumentaci: její architekturu, zabezpečení a přenos v NIS.

Cílem diplomové práce je vytvoření a popis struktury, základních vlastností a funkcí obecného nemocničního informačního systému. Na základě známé architektury se definuje odpovídající struktura obrazové dokumentace a diskutovat se bude vhodnost přístupu k této dokumentaci pro zdravotnický personál, také způsoby ochrany před neoprávněnými přístupy a zneužitím citlivých pacientských dat. Důležitou součástí práce bude popis nemocničního informačního systému CLINICOM se zaměřením na oddělení radiologie.

Předmětem práce je také problematika pacientských dat, kdy na základě platné legislativy České republiky dojde k nastínění komplexu zákonů, které je potřebné v souvislosti s ochranou osobních dat v NIS zabezpečit. Důležitou součástí jsou i etické otázky týkající se ochrany pacientských dat, kde bude věnován prostor základnímu rozboru ochrany pacientských dat, bude pojednáno o etickém kodexu pacientů i administrativních opatřeních pro bezpečný přenos pacientských dat mezi NIS.

Další součástí práce bude analýza přenosu pacientských dat prostřednictvím sítě Internet při nezměněné bezpečnosti a spolehlivosti systému. Neopomene se ani stručná charakteristika, smysl a využití datových standardů při komunikaci a diskutováno bude také zabezpečení přenosu pacientských dat mezi NIS.

Na základě analýz dojde k návrhu a realizaci rozhraní pro dálkový přístup k obrazové dokumentaci na radiologické oddělení NIS Clinicom na ÚBMI. Součástí práce bude test konektivity k této dokumentaci z pracoviště, které není součástí nemocničního intranetu.

Podrobný popis instalace a konfigurace programových komponent NIS CLINICOM by měl sloužit jako využitelný návod pro realizaci analogického systému v nemocnicích.

1 ANALÝZA STUDENTSKÉ PRÁCE

1.1 Nemocniční informační systém

1.1.1 Co se rozumí pod pojmem NIS?

Nemocniční informační systém je obsáhlý, snadno ovladatelný, ekonomicky a klinicky řízený systém zdravotní péče. Vyznačuje se efektivním zpracováním pacientské dokumentace s využitím podpory pro všechny potřebné činnosti spojené s výkonem lékařské praxe [15]. NIS by měl jako komplexní systém pokrývat všechny oblasti systematického pořizování, ukládání, uchování a zpracování pacientských dat v nemocnici. Stejně tak by měl pomáhat řešit personální, ekonomické a správní problémy a komunikaci s dalšími externími systémy připojenými na Internet [21].

Důležité začátky zdravotnických informačních systémů sahají do 50tých let minulého století, kdy vznikly první systémy orientované na samostatné dílčí oblasti nemocnice (registry pacientů a kartotéky údajů) využívající dávkové zpracovávání pomocí děrných štítků. Od aplikací orientovaných na samostatné dílčí oblasti se vývoj nasměroval až k současným totálním informačním systémům. Cílem je vytváření komplexních informačních systémů pro nemocnice, které disponují dostatkem vnitřní a periferní paměti a dokážou obsáhnout všechny potřeby nemocnic. V závislosti na jejich potřebách dochází neustále k vývoji a vytváření nových modulů či komplexů pro NIS.

Mezi základní požadavky na NIS patří [15]:

- komplexní přístup k řešení zdravotnické informatiky
- respektování pracovních návyků z lékařské praxe
- minimální zátěž uživatele administrativními a jinými vedlejšími činnostmi
- flexibilita systému v měnících se podmínkách lékařské praxe, legislativy včetně harmonizace s normami Evropské Unie
- respektování standardů Všeobecné zdravotní pojišťovny (VZP) a Ministerstva zdravotnictví České republiky (MZ ČR)
- ergonomické ovládání
- snadná orientace v prostředí systému
- odolnost vůči neodborným uživatelským zásahům
- rozsáhlá parametrizovatelnost

- modularita umožňující postupnou implementaci
- snadná administrace
- otevřenost k jiným programovým produktům
- bezpečnost datové základny (selektivní přístup k vybraným úlohám a datům)
- víceúrovňový způsob zálohování
- nezávislost na HW a SW platformě
- využití širokého spektra výpočetní techniky včetně možnosti plnohodnotného využití i nejstarší provozně spolehlivé techniky
- možnost spojení částí sítí na velké vzdálenosti
- možnost připojení vzdálených pracovišť pomocí modemu, telefonních sítí a pod.
- garance údržby systému
- vysoký výkon za přijatelnou cenu

1.1.2 Elektronický záznam o pacientovi

V úzké souvislosti s NIS se užívá termín Elektronický záznam o pacientovi (EPR – Electronic Patient Record). Jedná se o souhrn informací o zdravotním stavu jednotlivce a informací sloužících k jeho identifikaci. Někdy je také definován jako dílčí záznam o pravidelné lékařské péči a je součástí komplexního přehledu péče pacienta (EHR – Electronic Health Record). Používání EPR má oproti klasické formě zdravotního záznamu několik výhod. Snadná přenositelnost umožňuje přístup do zdravotního záznamu odkudkoli a to i více uživatelům najednou. Také odpadají problémy související s manuálním zpracováním a vyhotovením dokumentace a dokladů, což vede k zvyšování kvality zdravotní péče. Při použití elektronického záznamu pacienta neexistuje problém s čitelností oproti klasické papírové kartotéce. Další výhodou je jednoduché vyhledávání v záznamech i v obrovských databázích, kde se vyhledávání omezuje pouze na správnou volbu kriteria hledání. Bezpečnost dat v elektronické podobě je zabezpečována častým zálohováním, distribucemi, archivacemi, takže nemůže dojít k nahodilé destrukci. Elektronický záznam o pacientovi zlepšuje ekonomickou efektivitu léčebného a diagnostického procesu. Finanční a produktivní benefity zavedení EPR jsou nevyvratitelné. Většinou se náklady na vytvoření NIS vrátí za 2 až 4 roky po zahájení provozu (průměrný roční ekonomický přínos je 10 až 25%) [16].

Sdílení dat umožňuje snížit počet nadbytečných vyšetření, zkrátit vyšetřovací i léčebný čas. Sdílení dat minimalizuje opakovaná vyšetření, čímž snižuje zátěž pacienta. Používání EPR má však i své nevýhody, zejména v kompatibilitě různých informačních systémů, které se snaží řešit datové standardy. Jiné problémy vyvstávají v souvislosti s počítačovou gramotností lékařů; v neposlední řadě i ochraně před nedovolenými přístupy a zneužíváním pacientské dokumentace.

1.1.3 Obecná struktura NIS

NIS může být tvořen velkým počtem modulů, které reprezentují specifické požadavky všech potencionálních uživatelů systému. Jedná se o součásti globálního nemocničního systému, které slouží jako samostatné součásti zabezpečující různé funkce v systému. Jinými slovy jde o aplikace řešící funkční celky v rámci nemocnice. Důležitým společným znakem všech modulů NIS je s ohledem k ochraně pacientských dat možnost nastavení potřebných přístupových práv k sdíleným informacím, případně autorské uzamykání dokumentace. Mezi základní moduly patří dle návrhů a realizací existujících systémů modul [15]:

1. evidence
2. ambulance
3. hospitalizace
4. laboratoře
5. pracoviště pro vyšetření zobrazovací technikou
6. operačních sálů
7. fyzioterapeutické péče
8. patologické anatomie
9. rychlé záchranní služby
10. zdravotnického transportu
11. uživatelské služby
12. katalogů
13. pojišťoven
14. statistických výkazů ÚZIS

15. manažerských informací, statistických výkazů NIS
16. lékařského výzkumu
17. skladů
18. hospodářsko-technické, provozní služby
19. administrace NIS

1. Modul evidence

Pokrývá činnost evidence, recepce a přijímací kanceláře. Měl by umožňovat vyhledávání pacientů dle volitelných kritérií, registraci nového pacienta, dále by měl zajišťovat automatickou kontrolu duplicity, úplnosti a korektnosti rodných čísel.

Obecně disponuje osobními údaji pacientů, včetně informací o odpovídajících pojišťovnách; umožňuje objednání hospitalizace, vyšetření, transportu do zdravotnického zařízení, vystavování receptů a další. Měl by zabezpečovat přehled stavů na lůžkových odděleních a poskytovat souhrnné informace o pacientovi.

2. Modul ambulance

Pokrývá činnost odborné a specializované ordinace a poradny, také lékařské služby první pomoci (LSPP). Měl by disponovat částmi jako je seznam žádanek pacientů, umožňovat objednávání vyšetření, obsahovat souhrnné informace o pacientovi s možností editace při dalších vyšetřeních, včetně záznamů o krevní skupině, tělesných údajích, diagnózách, lékařských výkonech, anamnézách, rizikových faktorech a jiných. Při vytváření lékařské zprávy by měl mít lékař možnost importovat libovolné části z předcházejících nebo doplňujících vyšetření.

Modul ambulance by měl obsahovat možnosti objednávání: komplementárních vyšetření jako jsou vyšetření zobrazovací technikou, funkční diagnostiky a pitvy; nejrůznejších operací, hospitalizací, zdravotnického transportu a pod. Dále by měl realizovat tisk libovolných částí lékařských zpráv a různých nemocničních tiskovin, obsahovat aktuální přehled stavů na lůžkových odděleních.

3. Modul hospitalizace

Pokrývá činnost Jednotky intenzivní péče, Anesteziologicko-resuscitačního oddělení, Léčebny dlouhodobě nemocných a zabezpečuje správu ošetřovatelských lůžek. Dále zabezpečuje přehled příjmů a překladů, rezervace lůžek a pokojů, záznamy novorozence a rodičky, souhrnné informace o pacientovi a jeho záznamy z předešlých vyšetření.

Může obsahovat automatický podpis ošetřujícího lékaře, vedoucího lékaře a primáře na dokumentech hospitalizace a může spravovat jednotlivé hospitalizace, upozorňovat na případné chyby či nedostatky v hospitalizaci.

4. Modul laboratoře

Pokrývá komplexní činnost laboratoří klinické biochemie, hematologie a nukleární medicíny. Měl by zabezpečovat bezchybnou návaznost na NIS a mít přístup k souhrnným informacím o pacientovi v závislosti na nastavení přístupových práv ošetřujícím lékařem. Za potřebnou součást modulu lze považovat schopnost dlouhodobé archivace výsledků a jejich (nejenom) statistické vyhodnocování. Modul laboratoře by měl být schopen rozdělit provoz laboratoře do více bloků dle specifických potřeb a umožňovat automatickou integraci a přímý vstup výsledků z analyzátorů a dalších laboratorních zařízení. Velkou pomůckou jsou také možnosti automatických vyhodnocování, testů, srovnávání, kontrola výsledků, také tisk požadovaných částí systému a jiné.

5. Modul pracoviště pro vyšetření zobrazovací technikou

Pokrývá činnosti pracoviště pro vyšetření zobrazovací technikou jako je CT (Computed Tomography), PET (Positron Emission Tomography), SPECT (Single Photon Emission Computed Tomography) a pod. Měl by obsahovat seznam žádanek pacientů o vyšetření (s možností registrace nového pacienta) a plánovací diář. Uživatel modulu by měl mít přístup k souhrnným (osobním) informacím o pacientovi v závislosti na nastavení přístupových práv ošetřujícím lékařem. Dalšími využitelnými funkcemi modulu pracoviště pro vyšetření zobrazovací technikou může být automatické upozorňování na případný rozpor s rizikovými faktory pacienta, různé diagnózy, dávky ozáření, předdefinované formáty snímků, lékařské zprávy, přehledy, statistiky, tisk, archivace přenosu obrazové informace a jiné.

6. Modul operačních sálů

Pokrývá činnost operačních sálů. Obecně disponuje souhrnnými informacemi o pacientovi, zabezpečuje generování seznamu žádanek na operace a s tím související plánování. V modulu operačních sálů musí být odpovědný pracovník schopen vytvořit operační záznam a protokol pacienta s důrazem kladeným na určení diagnózy, vykonaných nebo plánovaných výkonů, anamnézy, rizikové faktory pacienta, očkování, krevní skupiny a pod. Součástí modulu může být také objednávání komplementárních vyšetření, hospitalizace, zdravotnického transportu, operací, různých druhů péče. Vzhledem k předešlým bodům je zde také možné nastavování tisku, přehled stavů na lůžkových odděleních, možnost generace přehledů a statistik.

7. Modul rehabilitace

Pokrývá činnost fyzioterapeutické péče. Obecně poskytuje téměř stejné funkce jako modul operačních sálů, přičemž by měl rozšiřovat jeho funkce o: objednávání vyšetření (s možností registrace nového pacienta), možnost přístupu k osobním údajům pacienta, možnost generace lékařské zprávy (možnost importu předdefinovaných textů, lékařských zpráv, receptů, nálezů a výsledků z minulých nebo doplňujících vyšetření).

8. Modul patologické anatomie

Pokrývá činnost patologické anatomie t. j. biopsie, cytologie, nekropsie, pitvy a přehledu zemřelých. Měl by disponovat možností objednávání vyšetření (s volbou registrace nového pacienta) a automatickým vstupem potřebných údajů z žádanky nebo ze stávající dokumentace pacienta.

Modul patologické anatomie by měl být komplexním systémem pro zpracování vzorku užitých pro biopsii, cytologii a nekropsii. Také by měl obsahovat komplexní systém pro zpracování požadavku na zdravotní pitvu, souhrnné informace a možnost přístupu k osobním údajům pacienta. Tisk, přehledy, statistiky, seznam pitvaných, roční výkaz pro NZIS jsou nezbytným standardem tohoto modulu.

9. Modul RZP

Pokrývá činnost rychlé záchranné služby. Měl by obsahovat seznam a registraci výjezdů, umožnit identifikaci pacienta a získaní jeho základních informací. Modul by měl generovat zprávu o zásahu, potřebné přehledy, statistiky a předdefinované texty.

10. Modul dopravy

Pokrývá činnost zdravotnického transportu. Měl by umět vytvářet a blokovat příkazy, zaznamenávat jednotlivé transporty. Standardně je zde také možné nastavování tisku, zjišťovaní přehledů stavů na lůžkových odděleních, možnost generace přehledů a statistik.

11. Modul uživatelských služeb

Pokrývá činnost uživatelských služeb a měl by sloužit jako osobní záznamník, plánovací diář, zápisník, nástěnka a výrazový kalkulátor. Standardně umožňuje nastavení barev prostředí NIS, poskytuje informace o aktuálním datu, čase, přihlášeném uživateli a slouží jako kontextová nápověda.

12. Modul katalogů

Pokrývá činnost katalogů jako jsou katalogy uživatelské, systémové, MZ ČR, ÚZIS a jiné. Obvykle v sobě obsahuje zabudovaný katalog léků, číselníky ÚZIS, zdravotní pojišťovny, názvy a PSČ měst i obcí, katalog žadatelů pro rozlišení úhrady vyžádané, navržené resp. předepsané péče a další, které jsou součástí konkrétních modulů, např. pro kardiologii, patologii a pod.

13. Modul pojišťoven

Modul pokrývá zpracování podkladů pro zdravotní pojišťovny. Standardně se jedná o komplexní systém zpracovávající podklady pro zdravotní pojišťovny, který v sobě obsahuje plně automatický plánovač hromadného vyúčtování, kontroly, chybové výpisy, statistické přehledy a podíly nákladových středisek na vyúčtování.

14. Modul ÚZIS

Pokrývá statistické výkazy Ústavu zdravotnických informací a statistiky ČR (ÚZIS). Mělo by se jednat o komplexní systém pro zpracování podkladů pro povinná hlášení ÚZIS. Zabezpečuje ambulantní a hospitalizační výkazy, kontrolu a chybové výpisy.

15. Modul manažerských informací

Pokrývá manažerské informace a statistické výkazy NIS. Standardně obsahuje systém statistického vyhodnocovaní, který je provázán do všech modulů NIS. Výstupy z modulu lze získávat dle volitelného časového rozmezí. Může umožňovat statistické vyhodnocení podílu nákladových středisek na vyúčtování zdravotních pojišťoven a poskytuje možnost exportu statistických výkazů mimo prostředí NIS, např. do ekonomického subsystému, manažerské nástavby a pod.

16. Modul lékařského výzkumu

Komplexně pokrývá dostupné odborné lékařské statistiky. Na základě vstupních dotazů by měl modul lékařského výzkumu generovat odborné lékařské statistiky sestavované na základě údajů z pacientských záznamů v NIS. Na základě výstupních kritérii se předpokládá určení obsahu, formátu a vzhledu výstupní sestavy.

17. Modul skladů

Zabezpečuje vedení skladového hospodářství. Modul skladů předpokládá vedení příručních skladů na nákladových střediscích různého typu, vytvoření komplexního systému pro vedení skladových karet. Měl by umožňovat standardní operace pro práci

s: příjmem a výdejem zboží, katalogem dodavatelů, odběratelů, výpisem skladové karty a přehledem dokladů, na kterých došlo ke změnám na kartě.

18. Modul HTP

Pokrývá hospodářsko-technické a provozní služby. Univerzálnost tohoto systému by měla umožňovat široké využití pro investiční odbor, provozní odbor, přístrojové zázemí, technický odbor, údržbu a pod. Hlavním prostředkem pro HTP služby je databáze úkonů obsahující požadavky uživatelů, kteří mají k službám HTP přístup prostřednictvím sítě NIS. Cílem modulu HTP by měla být kompletně zpracovaná agenda týkající se požadavků uživatelů.

19. Modul administrace

Pokrývá administraci NIS a měl by poskytovat definice organizační struktury zdravotnického zařízení, jednotlivých kompetencí a přístupových práv uživatelů. Modul administrace standardně umožňuje konfigurace: specifik provozu, stupně ochrany před neúplným vyplňováním pacientské dokumentace, uživatelských a systémových funkcí. Měl bych definovat konfigurační a technické parametry pro jednotlivá pracoviště, porovnávat rodné čísla pacientů a jejich příslušnosti k zdravotním pojišťovnám, aktualizovat číselníky a katalogy. Důležitým prvkem je možnost vykonávaní auditu t. j. kontroly přístupu do systému a také možnost vzdálené správy NIS.

1.1.4 Obecná struktura obrazové dokumentace v NIS

Nemocniční informační systémy jsou navrhovány pro řešení problémů vazby konkrétního pacientského záznamu na příslušnou obrazovou dokumentaci uloženou v archivu. Samotné zpracování a ukládání obrazové dokumentace mají většinou na starosti systémy archivace obrázků a komunikace PACS (Picture Archiving and Communication Systems). Tento přístup k obrazové dokumentaci je způsoben problémy s archivací dat či problematičností přístupu k uloženým informacím. K archivaci dat se používají zejména velkokapacitní disková pole a DVD. Některé systémy neobsahují paměť pro uložení grafické informace (obvykle např. ultrazvukové vyšetření - SONO), některé systémy naopak disponují obrovskou paměťovou kapacitou pro archivaci obrazových a jiných informací i po dobu několika let.

Pro ukládaní obrazové dokumentace u jednoduchých systémů typu SONO, EKG (Elektrokardiogram), EEG (Elektroencefalografie) se řeší archivace často pomocí CD (Compact Disc) nebo DVD (Digital Versatile Disc). Některé systémy umožňují archivaci obrazové dokumentace v řádu několika hodin, poté se informace zpracuje, popíše nález, eventuálně se přesune nebo nahraje jinam. Mezi tyto systémy patří

právě SONO, EKG a EEG. U jiných systémů se archivace provádí po dobu několika dnů (např. CT). U systémů jako RTG, se počítá až s několika měsíci, přičemž vždy záleží na objemu zpracovávaných dat a předpokládané době jejich využívání.

PACS je systém určen pro správu, archivaci a přenos digitálních obrazových informacích ve zdravotnictví. Tyto systémy umožňují oproti klasickým systémům rychlé a levné pořizování digitální obrazové dokumentace, rychlou distribuci, levnější a bezpečnější skladování a téměř konstantní kvalitu obrazu v průběhu času. Je zřejmé, že digitální pořizování a zpracování obrazové dokumentace má oproti klasickým filmům nesporné výhody. Většina systémů PACS se skládá ze čtyř základních modulů, které umožňují různou konfiguraci v závislosti na požadavkách pracoviště. Mezi základní moduly patří:

- server
- klient
- archiv
- modul pro komunikaci

Server zajišťuje komunikaci s ostatními moduly a distribuci informací směrem ke klientům, do dalších serverů, případně do PACS řešení třetích stran. Současně udržuje databázi informací o umístění dat.

Klient umožňuje výběr, třídění a prohlížení uložených dat s možností jejich elektronického zpracování. Zdrojem dat je server. Často umožňuje alternativní prohlížení dat přes webové rozhraní či jejich tisk.

Archiv zajišťuje ukládání dat a obousměrnou komunikaci s úložným velkokapacitním zařízením určeným pro dlouhodobou archivaci dat. Obsahuje v sobě databázi informací o uložených datech (on-line i off-line) a současně udržuje ve vyrovnávací paměti kopie obnovených dat. Výhodou je konzistence dat z hlediska uživatele. Archiv nabízí uživateli jednotný pohled na data bez ohledu na to, kde se data fyzicky nachází. Délku archivace dat lze nastavit libovolně dle požadavků zákazníka tak, aby nedocházelo k rozporům s platnou legislativou České republiky. Další z možností archivačního modulu je selektivní komprese dat pro účely archivace na paměťová média. Pomocí této funkce lze komprimovat různá data nastavitelným poměrem a využívat tak efektivně disponibilní prostor pro archivaci. Komprimovat lze i data uložená on-line na diskovém poli podle nastavených pravidel např. dle stáří nebo podle uplynulé doby od posledního přístupu k datům.

Modul pro komunikaci představuje základní rozhraní pro on-line komunikaci s informačním systémem nemocnic [10, 22, 32].

1.1.5 Nemocniční informační systém CLINICOM

NIS CLINICOM je robustní nemocniční informační systém s modulárním řešením a moderní postrelační databází Caché firmy InterSystems [43]. Implementuje v sobě čtyři základní části:

- správu pacientů
- správu výkonů
- komunikaci
- správu operací

Správa pacientů spočívá v racionalizaci a zefektivnění využívání dat, které byly jednou vloženy do systému. Tím se dosahuje snížení chybovosti v pacientských datech a zvyšuje se rychlost při vybavování pacientů. Správa výkonů se provádí automaticky, bez nutnosti přímé obsluhy personálu. Dané požadavky jsou automaticky zpracovány podle předdefinovaných kritérií. Komunikace spočívá v operacích se žádankami a to především ve vytváření, zasílaní a příjmu. Správa operací zabezpečuje přehled o zákrocích a operacích a odpovídajících nákladech a výnosech.

CLINICOM dále představuje administrativní nástroj lékaře pro usnadnění pořízení a archivaci povinné dokumentace, také k sledování ekonomiky nemocnice. Data z NIS lze dále zpracovat a vyhodnotit prostřednictvím manažerského informačního systému DSS (Decision Support System) [43]. Kromě toho umožňuje komunikaci se systémem internetového přístupu ke zdravotním informacím pacienta (IZIP).

Vzdálený přístup k systému

Vzdálený přístup k systému CLINICOM je realizován prostřednictvím ovladače ODBC. ODBC je aplikačním, API rozhraním, které se využívá k přístupu k datům. Přístup k datům je nezávislý na systému spravování řízením báze dat. Vlastní konfigurace Správce zdrojů dat ODBC je popsána v kapitole 2.1.

Uživatelská rozhraní systému

Existují tři alternativy pro realizaci uživatelského rozhraní systému CLINICOM. První alternativou je přístup pomocí terminálu v textovém režimu (KoalaTerm), který však vzhledem k trendům vývoje zůstává spíše historickým mezníkem. Moderními alternativami je využití grafického uživatelského rozhraní CareCenter anebo využití zabezpečeného externího přístupu NetAccess.

CareCenter je grafické uživatelské rozhraní systému CLINICOM [43], které zabezpečuje přímý přístup k relevantním lékařským datům dle požadavků obsluhujícího personálu. Funguje na principu klient/server a pro komunikaci s databázemi využívá protokol XMS. Po přihlášení do systému poskytuje CLINICOM přehledné informace o zvoleném pacientovi – o jeho zdravotním stavu, vyšetřeních a pod. Platí, že data vložené do programu CareCenter se přenáší do databáze CLINICOMu, čímž se dá práce s těmito modalitami kombinovat dle potřeb lékaře.

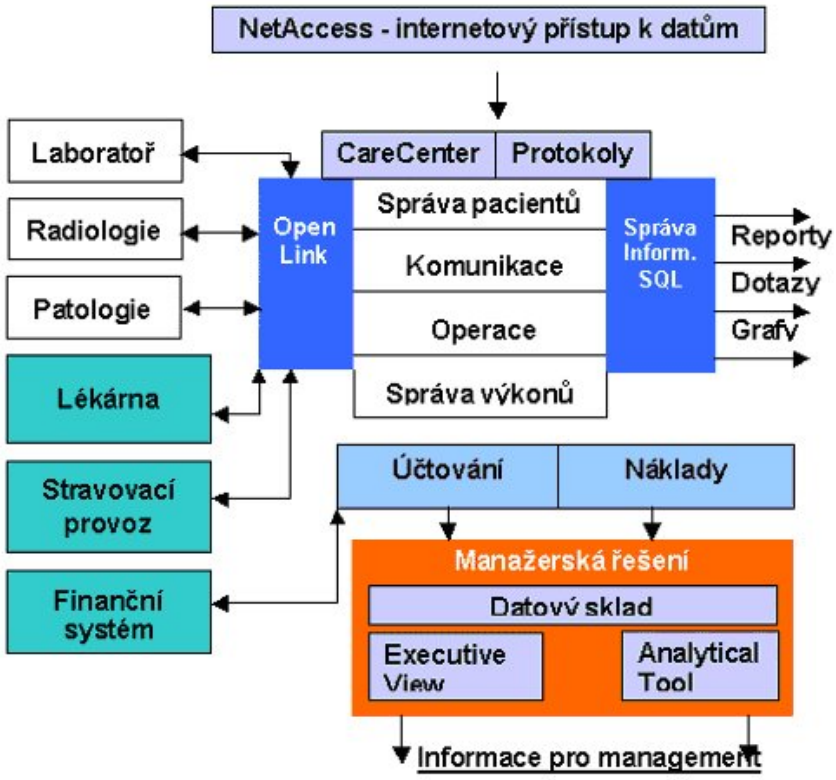
Nastavení systémové funkčnosti programu CareCenter je k nalezení v záznamech SDF (System Definition File). Pro lokální nastavení je nutné přidání funkce přes `Nástroje\SDF nastavení\Počítače\Přidat`. Název odpovídá názvu v operačním systému a upravování SDF nastavení pro specifické položky se provádí pomocí `Nástroje\SDF nastavení\SDF položky`. Změna SDF nastavení je aktualizována pouze po ukončení a opětovném spuštění aplikace. Kontrolu správnosti SDF nastavení lze provést prostřednictvím funkce `Nápověda\Aktuální SDF nastavení` [42].

NetAccess představuje jednoduchý zabezpečený externí přístup k lékařským informacím prostřednictvím Internetu nebo intranetu a umožňuje tak uživatelům přístup k datům NIS nejen z lokální sítě nemocnice, ale také z každého místa, které disponuje připojením na Internet [43]. CareCenter slouží NetAccess k zobrazování přehledných informací o pacientovi a k zadávaní libovolných požadavků, při implementovaném vysokém stupni zabezpečení. Pro ochranu spojení se zde využívá standard SSL.

Modalita oddělení radiologie (RTG)

Modalita oddělení radiologie (RTG) je modalitou využívající vlastní databázový server postavený na databázi Caché. Její nezávislost na databázi CLINICOM umožňuje samostatnou činnost i v případě, že se jedná o diagnostickou jednotku nespadající do většího nemocničního celku. V převažné většině případů jsou však požadavky na komunikaci s databází CLINICOM vyžadovány a komunikace například mezi systémy CareCenter a RTG může probíhat. Popis této komunikace je předmětem kapitoly 2.3.

Samotný program RTG lze využít k vytvoření samostatného lokálního NIS nebo parciální části NIS, která může být součástí globálního NIS odpovídajícímu unikátní struktuře nemocnice. Dochází tak k budování databáze postavené na elektronickém zpracování a archivaci pacientských dat. Jeho úlohou je obsáhnout oblasti příjmu a zpracování požadovaných vyšetření a tomu odpovídající vyhodnocení radiologických výsledků. Program RTG zabezpečuje všechny potřebné operace týkající se pacientských dat a vyžadované práce s nimi. Umožňuje prohlížet a vyhledávat (dle různých kriterii) v záznamech všech registrovaných pacientů na oddělení RTG. Po startu



Obr. 1.1: Koncepce NIS CLINICOM [9]

programu a úspěšném přihlášení se otevře seznam rozpracovaných žádanek, které lze po kliknutí na jméno pacienta dle potřeb upravovat. Je důležité si uvědomit, že každé pracoviště RTG nakládá s unikátním seznamem žádanek t. j. seznamem vlastních pacientů. Aktuální stav jednotlivých žádanek popisují přiřazené zkratky: `*` pro případ, kdy jsou zadány všechny povinné údaje; `V` pro případ, že je zadán minimálně jeden výkon pro zdravotní pojišťovnu, `ZK` v případě provedení kontroly žádanky lékařem a `T` v případě, že dané pacientské údaje jsou vytištěny a jsou součástí provozního deníku. Uvedeným zkratkám odpovídá i proces práce s programem RTG. Po vyplnění všech nezbytných údajů, provedení a zaznamenání výsledků o požadovaném vyšetření je nutno provést lékařskou kontrolu (aktivace tlačítka lékařské kontroly přímo v programu nebo klávesy F7) a v případě potřeby odeslat výsledky zpět na oddělení t. j. odesílateli žádanky. Z důvodu duální archivace (jak v elektronické, tak v papírové formě) je potřebné vytisknout provozní deník a žádanku archivovat.

Provedení a zaznamenání výsledků požadovaného vyšetření v sobě kromě textové informace zahrnuje informace obrazové – digitální. Rentgenologické snímky lze přiložit k dané složce pacienta pomocí tlačítka `Do archivu`, kdy se z pracovního adresáře

vybere odpovídající snímek. Pro korektní fungování programu RTG musí být proto správně nastaven adresář pracovních snímků obsahující všechny vyhotovené snímky RTG a pacientské adresáře snímků, které reprezentují adresáře jménem nebo kódem pacienta a odpovídajícími snímky. Nastavení adresářů se provádí pomocí `Nastavení modulu\Složky pro snímky\Složky pro snímky\Pracovní složka` nebo `...\Pacientská složka`.

Prohlížení žádanek pomocí webového rozhraní vyžaduje definici uživatelů, kterým bude umožněn přístup k citlivým pacientským informacím. Pomocí funkce RTG dostupné přes `Nastavení systému\Přístupová práva www` jsou osoby, nakládající s daným systémem, schopny upravovat seznam uživatelů zadáváním nebo editováním položek: `Jméno`, `Heslo`, `Uživatel` – Obr. 2.3.

1.2 Problematika pacientských dat

1.2.1 Etické otázky týkající se ochrany pacientských dat

Základní rozbor ochrany pacientských dat

Ochrana pacientských dat by ve vzájemném vztahu pacient – nemocnice měla stát na předních místech žebříčku zájmů. Základním důvodem pro ochranu pacientských dat jsou především přirozená lidská práva na ochranu soukromí, přiměřené chování zdravotníků ve vztahu k pacientům, práva na důstojnost a další práva, která jsou garantována v zákonech České republiky, v nadnárodních smlouvách, normách a j.

Problém pacientských dat úzce souvisí s relativně snadnou dostupností a problémy se zabezpečením na půdě nemocnice. Většinou se jedná o rozsáhlé seznamy obsahující množství citlivých informací, které mohou být zneužity jednotlivě nebo jako celek. Je potřebné si uvědomit, že do kontaktu s pacientskými údaji přicházejí kromě zdravotnického personálu také inženýři, fyzici, informatici, dodavatelé a j., což vyžaduje preciznější kontrolu přístupu osob k pacientským záznamům. V tomto kontextu je legislativně dořešeno využívání papírové dokumentace, využívání digitální dokumentace má však zatím četné mezery v legislatívě. Realizace komplexní ochrany pacientských dat dle Seinera [40] vyžaduje ošetření bezpečnosti dat ve všech vrstvách informačního systému: organizační, aplikační a technologické.

Z platných zákonů vyplývá několik klíčových principů [40]:

- Zdravotní údaje (ale i některé další, s kterými NIS pracuje) jsou citlivými osobními údaji ve smyslu zákona a tím požívají nejvyšší možné ochrany.
- Do zdravotnické dokumentace mohou bez souhlasu pacienta nahlížet pouze vyjmenované kategorie osob a to pouze v rozsahu své kompetence a v rozsahu nezbytně nutném pro splnění konkrétního úkolu.

- Osoby, které s údaji pracují, musí zachovávat mlčenlivost.

Důležité je si uvědomit, že každý zdravotník má právo se seznámit se zdravotnickou dokumentací pacienta pouze tehdy, když o něj přímo pečuje a pouze v rozsahu, který odpovídá úkolu, který právě plní. Je zřejmé, že dnes a denně dochází k porušování tohoto principu [40].

Úmyslnému i nedbalému porušování práv pacienta na ochranu soukromí v nemocnici se dá zamezit různými možnostmi NIS. Základ spočívá v zamezení přístupu neoprávněných uživatelů do systému. Pro oprávněné uživatelé NIS je potřebné správné nastavení přístupových práv podle druhu výkonů a činností, čím lze vymezit jejich přístup jenom k některým specifickým informacím. Neméně účinnou metodou pro kontrolu dodržování práv pacientů na ochranu soukromí je monitoring přístupů k jednotlivým pacientským datům. Nemělo by se zapomínat také na ochranu veškerých dat před záměrnou manipulací, modifikací, poškozením či eventuálním zničením. S ochranou pacientských dat také úzce souvisí ochrana osobních, finančních a j. dat zaměstnanců nemocnic.

V těchto ohledech musí provozovatel zdravotnického zařízení, ve kterém je provozován klinický informační systém povinen zajistit minimálně následující [40]:

- Jasné stanovení principů ochrany dat pacientů, dokumentované ve směrnicích a pravidlech.
- Jasné stanovení odpovědnosti pracovníků za jednotlivé činnosti v uskutečňování bezpečnostní politiky s oddělením rolí rozhodovacích, výkonných a kontrolních.
- Motivaci všech kategorií pracovníků k dodržování bezpečnostních zásad a jejich proškolení.
- Realizaci potřebných ochranných opatření na všech úrovních – nastavení aplikace, technické prostředky omezení přístupu k datům a pod.
- Zabezpečení pravidelné kontrolní činnosti.

Problematiku ochrany pacientských dat komplexně rozebírá R. Anderson v článku *A security policy model for clinical information systems* [2], na základě kterého stanovuje devět základních principů, které mají být dodržovány v každém NIS.

1. Každý identifikovatelný lékařský záznam musí být opatřen seznamem přístupových oprávnění vyjmenovávajícím osoby nebo skupiny, které mohou záznam číst či doplňovat další data. Systém nesmí dovolit osobám absentujícím na seznamu práci s údaji.

2. Zdravotník může založit záznam, ve kterém bude na seznamu přístupových oprávnění pracovník zakládající záznam a pacient. Pokud byl pacient doporučen, bude na seznamu přístupových oprávnění zdravotník, pacient a doporučující lékař.

3. Jeden ze zdravotnických pracovníků na seznamu přístupových oprávnění musí být označen jako odpovědný. Pouze pracovník odpovědný může měnit seznam přístupových oprávnění a pouze on může přidávat další pracovníky do seznamu.

4. Odpovědný pracovník musí informovat pacienta o jménech na seznamu přístupových údajů k jeho záznamům v momentě založení, při každém následném přidání a v momentě, kdy předává odpovědnost za správu údajů pacienta. Pacientův souhlas může absentovat v případě neodkladné péče, nebo zákonem vymezených případech.

5. Nikdo by neměl disponovat oprávněním umožňujícím smazání zdravotních záznamů před uplynutím definované doby existence záznamu.

6. Všechny přístupy ke zdravotní dokumentaci musí být označeny na záznamu názvem subjektu, odpovídajícím datem a časem přístupu. Informace auditu musí být také chráněny před mazáním záznamů.

7. Pro informační tok platí, že informace získaná ze záznamu A může být přidána k záznamu B, pokud seznam přístupových oprávnění záznamu B je obsažen v seznamu přístupových oprávnění záznamu A.

8. Musí existovat efektivní prostředky zabraňující agregaci osobních pacientských dat. Pacienti musí obdržet speciální upozornění pokud osoba, která je oprávněná k editaci jejích seznamů přístupových oprávnění, má přístup ke zdravotním údajům velkého množství lidí.

9. Výpočetní systémy zpracovávající soukromé zdravotní údaje musí mít subsystém, který efektivně vynucuje dodržování výše uvedených principů. Efektivita tohoto subsystému musí být vyhodnocena nezávislou expertní komisí.

V souvislosti s pátým bodem Andersonových principů je důležité správné nastavení délky uchovávání pacientských dat. Analyzovaný Andersonův model navrhuje uchovávání základních dat po dobu 8 let, ale například záznamy o rakovině musí být uschovány po celý život pacienta, v případě genetických onemocnění ještě déle. Celospolečenská nebo dokonce celosvětová shoda v délce uchovávaní pacientských dat ale zatím stále neexistuje.

V Evropě má vytváření standardu pro ochranu pacientských dat a jejích kódování na starosti skupina nazvaná *A European standardisation group for Security and Privacy of Medical Informatics*.

Etický kodex pacientů

Etický kodex pacientů upravuje základní práva pacientů ve vztahu ke všem zdravotnickým zařízením. Byl formulován a schválen Centrální etickou komisí Ministerstva zdravotnictví ČR. Tato práva pacientů jsou platná od 25. února 1992.

1. Pacient má právo na ohleduplnou odbornou zdravotnickou péči prováděnou s porozuměním kvalifikovanými pracovníky.

2. Pacient má právo znát jméno lékaře a dalších zdravotnických pracovníků, kteří ho ošetřují. Má právo žádat soukromí a služby přiměřené možnostem ústavu, jakož i možnost denně se stýkat se členy své rodiny či s přáteli. Omezení takovéhoto způsobu (tzv. kontinuálních) návštěv může být provedeno pouze ze závažných důvodů.

3. Pacient má právo získat od svého lékaře údaje potřebné k tomu, aby mohl před zahájením každého dalšího nového diagnostického či terapeutického postupu zasvěceně rozhodnout, zda s ním souhlasí. Vyjma případů akutního ohrožení má být náležitě informován o případných rizicích, která jsou s uvedeným postupem spojena. Pokud existuje i více alternativních postupů nebo pokud pacient vyžaduje informace o léčebných alternativách, má na seznámení s nimi právo. Má rovněž právo znát jména osob, které se na nich účastní.

4. Pacient má v rozsahu, který povoluje zákon, právo odmítnout léčbu a má být současně informován o zdravotních důsledcích svého rozhodnutí.

5. V průběhu ambulantního i nemocničního vyšetření, ošetření a léčby má nemocný právo na to, aby byly v souvislosti s programem léčby brány maximální ohledy na jeho soukromí a stud. Rozbory jeho případu, konzultace a léčba jsou věcí důvěrnou a musí být provedena diskrétně. Přítomnost osob, které nejsou na léčbě přímo zúčastněny, musí odsouhlasit nemocný, a to i ve fakultních zařízeních, pokud si tyto osoby nemocný sám nevybral.

6. Pacient má právo očekávat, že veškeré zprávy a záznamy týkající se jeho léčby jsou považovány za důvěrné. Ochrana informací o nemocném musí být zajištěna i v případech počítačového zpracování.

7. Pacient má právo očekávat, že nemocnice musí podle svých možností přiměřeným způsobem vyhovět pacientovým žádostem o poskytování péče v míře

odpovídající povaze onemocnění. Je-li to nutné, může být pacient předán jinému léčebnému ústavu, případně tam převezen po té, když mu bylo poskytnuto úplné zdůvodnění a informace o nezbytnosti tohoto předání a ostatních alternativách, které při tom existují. Instituce, která má nemocného převzít do své péče, musí překlad nejprve schválit.

8. Pacient má právo očekávat, že jeho léčba bude vedena s přiměřenou kontinuitou. Má právo vědět předem, jací lékaři, v jakých ordinačních hodinách a na jakém místě jsou mu k dispozici. Po propuštění má právo očekávat, že nemocnice určí postup, jímž bude jeho lékař pokračovat v informacích o tom, jaká bude jeho další péče.

9. Pacient má právo na podrobné a jemu srozumitelné vysvětlení v případě, že se lékař rozhodl k nestandardnímu postupu či experimentu. Písemný vědomý souhlas nemocného je podmínkou k zahájení neterapeutického i terapeutického výzkumu. Pacient může kdykoliv, a to bez uvedení důvodu, z experimentu odstoupit, když byl poučen o případných zdravotních důsledcích takového rozhodnutí.

10. Nemocný v závěru života má právo na citlivou péči všech zdravotníků, kteří musí respektovat jeho přání, pokud tato nejsou v rozporu s platnými zákony.

11. Pacient má právo a povinnost znát a řídit se platným řádem zdravotnické instituce, kde se léčí (tzv. nemocniční řád). Pacient má právo kontrolovat svůj účet a vyžadovat odůvodnění jeho položek bez ohledu na to, kým je účet placen.

Administrativní opatření pro bezpečný přenos pacientských dat mezi NIS

Přenos zdravotnických informací mezi různými nebo vícerými NIS si z důvodu plnění legislativy vyžaduje aplikaci specifických administrativních opatření. Požadovanými bezpečnostními funkcemi pro přenos zdravotnických informací jsou důvěrnost, autentizace odesílatele, integrita zpráv a neodmítnutelnost zodpovědnosti odesílatele [32]. Kromě těchto bezpečnostních funkcí je nutné brát ohledy na legislativu příslušného státu, také na technické možnosti jednotlivých zdravotnických pracovišť a komplexní situaci v daném státě.

1.2.2 Současná legislativa ČR týkající se ochrany osobních dat v NIS

Listina základních práv a svobod

Listina základních práv a svobod je součástí Ústavy České republiky a deklaruje základní práva a svobody všem lidem vyskytujícím se na tomhle území. Ochrany osobních údajů pacientů ve zdravotnické dokumentaci se bezprostředně týká Hlava druhá – Oddíl první – Článek 10, který upravuje práva občana v následujících bodech [34]:

1. Každý občan má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.

2. Každý občan má právo na ochranu před neoprávněným zasahováním do soukromého a osobního života.

3. Každý občan má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Dále Hlava druhá – Oddíl první obsahuje Článek 13, který se také přímo dotýká ochrany osobních údajů pacientů ve zdravotnické dokumentaci.

Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením [34].

Občanský zákoník – Zákon č. 47/1992 Sb.

Občanský zákoník definuje ochranu osobních údajů pacientů ve zdravotnické dokumentaci v části Hlava druhá – Oddíl první – Ochrana osobnosti. §11 říká, že fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy [47].

§12 říká [47]:

1. Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením.

2. Svolení není třeba, použijí-li se písemnosti osobní povahy, podobizny, obrazové snímky nebo obrazové a zvukové záznamy k účelům úředním na základě zákona.

3. Podobizny, obrazové snímky a obrazové a zvukové záznamy se mohou bez svolení fyzické osoby pořídit nebo použít přiměřeným způsobem též pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství. Ani takové použití však nesmí být v rozporu s oprávněnými zájmy fyzické osoby.

Trestní zákoník – Zákon č. 412/2002 Sb.

Trestní zákoník v Hlavě třetí – Oddíl šest – §178 nazvaném Neoprávněné nakládání s osobními údaji upravuje také zákony s ohledem k ochraně osobních údajů pacientů ve zdravotnické dokumentaci.

1. Kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném, shromážděné v souvislosti s výkonem veřejné správy, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem [48].

2. Stejně bude potrestán, kdo osobní údaje o jiném získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, byť i z nedbalosti, sdělí nebo zpřístupní, a tím poruší právním předpisem stanovenou povinnost mlčenlivosti [48].

3. Odnětím svobody na jeden rok až pět let nebo zákazem činnosti nebo peněžitým trestem bude pachatel potrestán [48]:

    - Způsobí-li činem uvedeným v odstavci 1 nebo 2 vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se údaj týká.
    - Spáchá-li čin uvedený v odstavci 1 nebo 2 tiskem, filmem, rozhlasem, televizí nebo jiným obdobně účinným způsobem.
    - Spáchá-li čin uvedený v odstavci 1 nebo 2 porušením povinností vyplývajících z jeho povolání, zaměstnání nebo funkce.

Zákon o ochraně osobních údajů – Zákon č. 101/2000 Sb.

Zákon o ochraně osobních údajů definuje v Hlavě jedna v prvním paragrafu předmět úpravy, podle kterého zákon upravuje ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů a stanovení podmínek, za nichž se uskutečňuje jejich předávání do jiných států.

§4 slouží k vymezení pojmů. Pro účely tohoto zákona se rozumí [29]:

1. Osobním údajem jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na

základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu. O osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků.

2. Citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů. . . .

V Hlavě dva jsou také definovány povinnosti osob při zabezpečení osobních údajů. §13 ukládá správci a zpracovateli povinnost:

1. Přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů [29].

2. Zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy [39].

§14 říká, že zaměstnanci správce nebo zpracovatele a jiné osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, mohou zpracovávat osobní údaje pouze za podmínek a v rozsahu správcem nebo zpracovatelem stanoveném [29].

§15 říká, že [29]:

1. Zaměstnanci správce nebo zpracovatele, jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

2. Ustanovením předchozího odstavce není dotčena povinnost zachovávat mlčenlivost podle zvláštních zákonů.

3. Povinnost zachovávat mlčenlivost se nevztahuje na informační povinnost podle zvláštních zákonů.

Hlava sedm Zákona o ochraně osobních údajů je věnována sankcím. Fyzická osoba, která je ke správci nebo zpracovateli v pracovním nebo jiném obdobném poměru; vykonává pro správce nebo zpracovatele činnosti na základě dohody; nebo v rámci plnění zvláštním zákonem uložených oprávnění a povinností přichází u správce nebo zpracovatele do styku s osobními údaji, se dopustí přestupku tím, že poruší povinnost mlčenlivosti (§ 15) [39].

Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů [39]:

1. Nestanoví účel, prostředky nebo způsob zpracování (§5) a nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona.
2. Zpracovává nepřesné osobní údaje (§5).
3. Shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu (§5).
4. Uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování (§5).
5. Zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně (§5, §9).
6. Neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem (§11).
7. Neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem (§11).
8. Odmítne subjektu údajů poskytnout požadované informace (§12, §21).
9. Nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů (§13).
10. Nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů (§13).
11. Nesplní oznamovací povinnost podle tohoto zákona (§16, §27).

Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů některým ze způsobů podle odstavce 2 [39]:

- Ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života.

- Poruší povinnosti pro zpracování citlivých údajů (§9).

Za přestupek podle odstavce 1 lze uložit pokutu do výše 100 000 Kč, podle odstavce 2 pokutu do výše 1 000 000 Kč a za přestupek podle odstavce 3 lze uložit pokutu do výše 5 000 000 Kč.

Podle §46 neodpovídá právnická osoba za správní delikt, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možné požadovat, aby porušení právní povinnosti zabránila. Při rozhodování o výši pokuty se přihlíží zejména k závažnosti, způsobu, době trvání a následkům protiprávního jednání a k okolnostem, za nichž bylo protiprávní jednání spácháno [39].

Zákon o péči a zdraví lidu – 20/1966 Sb.

Paragraf 55 specifikuje povinnosti pracovníků ve zdravotnictví. Zdravotničtí pracovníci jsou povinni vykonávat zdravotnické povolání svědomitě, poctivě, s hluboce lidským vztahem k občanům a s vědomím odpovědnosti ke společnosti. Každý zdravotnický pracovník je povinen zejména [39]:

- Vykonávat své povolání v rozsahu a způsobem, pro něž zásady určuje ministerstvo zdravotnictví ve spolupráci s profesními organizacemi.
- Převzít a řádně plnit i mimořádné zdravotnické úkoly uložené mu dočasně v důležitém obecném zájmu.
- Poskytovat neprodleně první pomoc každému, jestliže by bez této pomoci byl ohrožen jeho život nebo vážně ohroženo zdraví a není-li pomoc včas dosažitelná obvyklým způsobem, a zajistit mu podle potřeby další odbornou péči.
- Zachovávat mlčenlivost o skutečnostech, o nichž se dověděl v souvislosti s výkonem svého povolání, s výjimkou případů, kdy skutečnost sděluje se souhlasem ošetřované osoby nebo kdy byl této povinnosti zproštěn nadřízeným orgánem v důležitém státním zájmu; povinnost oznamovat určité skutečnosti, uložená zdravotnickým pracovníkům zvláštními předpisy, není tím dotčena.

Dvě posledné povinnosti uvedené v odstavci 2 se vztahují i na zdravotnické pracovníky, kteří nevykonávají zdravotnické povolání.

Zpracování osobních údajů souvisejících se zajišťováním zdravotní péče popisuje §67a, který říká, že zpracováním osobních údajů podle tohoto zákona se rozumí zpracování osobních údajů při vedení zdravotnické dokumentace a další nakládání s ní a zpracování osobních údajů v Národním zdravotnickém informačním systému [39].

Zdravotnické dokumentaci se věnuje zákon §67b (nyní upraven také v zákoně č. 111/2007 Sb. – kapitola 1.2.2). Do zdravotnické dokumentace mohou nahlížet, a

to v rozsahu nezbytně nutném pro splnění konkrétního úkolu v rozsahu své kompetence [39]:

- lékaři, zdravotní sestry, rehabilitační pracovníci, lékárníci, kliničtí psychologové a kliničtí logopedové v souvislosti s poskytováním zdravotní péče,
- pověření členové příslušné komory při šetření případů podléhajících disciplinární pravomoci příslušné komory,
- revizní lékaři zdravotních pojišťoven v rozsahu stanoveném zvláštním právním předpisem,
- soudní znalci v oboru zdravotnictví v rozsahu nezbytném pro vypracování znaleckého posudku zadaného orgány činnými v trestním řízení nebo soudy,
- lékaři správních úřadů ve zdravotnictví pověření vyřizováním konkrétních stížností, návrhů na přezkoumání a podnětů ve správním řízení, a to v rozsahu vyplývajícím ze stížnosti, návrhu na přezkoumání nebo podnětu ve správním řízení,
- lékaři Státního úřadu pro jadernou bezpečnost v rozsahu stanoveném zvláštním právním předpisem,
- členové znaleckých komisí,
- pověření zdravotničtí pracovníci orgánu ochrany veřejného zdraví,
- lékaři orgánů sociálního zabezpečení při posuzování zdravotního stavu a pracovní schopnosti pro účely dávek a služeb sociálního zabezpečení, důchodového pojištění, státní sociální podpory, lékaři úřadů práce pro účely zaměstnanosti a lékaři okresních úřadů pro účely odvodního řízení a civilní služby; povinnosti zdravotnických zařízení vůči orgánům sociálního zabezpečení ve věcech zdravotnické dokumentace stanoví zvláštní právní předpis,
- zaměstnanci státu ve zdravotnických zařízeních, zaměstnanci příspěvkových organizací, které jsou zdravotnickými zařízeními, a zaměstnanci provozovatelů dalších zdravotnických zařízení zabezpečující pro tato zařízení zpracování osobních údajů,
- zaměstnanci státu v organizační složce státu (§67c), která zajišťuje plnění úkolů NZIS, kteří zabezpečují zpracování osobních údajů a informací o zdravotním stavu obyvatelstva, a zaměstnanci pověřeného (§67c) nebo stanoveného (§67d) zpracovatele, kteří zabezpečují zpracování osobních údajů a informací o zdravotním stavu obyvatelstva.

Osoby získávající způsobilost k výkonu zdravotnického povolání (§53) mohou nahlížet do zdravotnické dokumentace pouze v rozsahu nezbytně nutném a u pacientů stanovených pověřeným zdravotnickým pracovníkem zdravotnického zařízení, které zabezpečuje praktickou výuku osob získávajících způsobilost k výkonu zdravotnického povolání; k nahlížení do zdravotnické dokumentace takových pacientů je třeba jejich písemného souhlasu, případně souhlasu jejich zákonných zástupců. Souhlasu pacienta není třeba, není-li možné jej získat vzhledem ke zdravotnímu stavu pacienta. Osoby získávající způsobilost podle věty prvé jsou povinny o skutečnostech, o nichž se ze zdravotnické dokumentace dozvěděly, zachovávat mlčenlivost [39].

Pacient má právo na poskytnutí veškerých informací shromážděných ve zdravotnické dokumentaci vedené o jeho osobě a v jiných zápisech, které se vztahují k jeho zdravotnímu stavu; pacient se z informací, které jsou mu sděleny o jeho zdravotním stavu, nesmí dozvědět informace o třetí osobě. Za osoby mladší 18 let nebo osoby zbavené způsobilosti k právním úkonům mají právo na informace podle věty prvé jejich zákonní zástupci [39].

Zákon o péči a zdraví lidu – č. 111/2007 Sb.

Jedná se o zákon, kterým se upravuje zákon č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů, a některé další zákony. §67b odstavec 12 upravuje právo pacienta (znění zákona je kráceno) [37]:

1. na poskytnutí veškerých informací shromážděných ve zdravotnické dokumentaci vedené o jeho osobě nebo v jiných zápisech vztahujících se k jeho zdravotnímu stavu,

2. v přítomnosti zdravotnického pracovníka nahlížet do dokumentů uvedených v prvním bodu,

3. na pořízení výpisů, opisů nebo kopií dokumentů uvedených v prvním bodu,

4. určit osobu, která může být informována o jeho zdravotním stavu, nebo vyslovit zákaz podávání těchto informací jakékoliv osobě, a to při přijetí k poskytování zdravotní péče nebo kdykoliv po přijetí.

Podle zákona č. 111/2007 Sb. [37] a příslušné analýzy M. Seinera [41] vyplývá, že zdravotnická zařízení již nemají právo pacientovi z hlediska dokumentace nic skrývat a nic odepírat. Z nového zákona plyne právo pacienta nahlížet do zdravotnické dokumentace (v přítomnosti zdravotnického pracovníka), právo na její kopii, evidence oprávnění informovat o zdravotním stavu a evidence nahlédnutí a kopií [41].

1.3 Problematika přenosu pacientských dat

NIS se začaly v České republice budovat převážně po roce 1992. Od začátku byla největším problémem kompatibilita mezi různými informačními systémy, což si vyžádalo invenci Ministerstva zdravotnictví ve formě vytvoření standardů pro jejich tvorbu. Sjednocení povinných dat nemocnicemi bylo realizováno pro potřebu Národního zdravotnického informačního systému (NZIS), díky čemuž se podařilo shromáždit množství ekonomických údajů, informací o zdravotnických zařízeních a zdravotním stavu obyvatelstva [44].

Kromě problémů kompatibilit se problematika přenosu pacientských dat týká především bezpečnosti a samotného procesu zabezpečení těchto dat. Komplexní bezpečnost informačních systémů souvisí dle přednášek Ing. M. Dvořáka s:

- technickou bezpečností – zajištění kvalitního technického vybavení, servisních služeb během provozu IS, požadované spolehlivosti, dostupnosti a integrity; dále zajištění neporušenosti informací a řešení problémů nosičů dat (systémy s vysokou redundancí, kterým je vlastní vysoká odolnost vůči chybám).

- empatickou bezpečností – ochrana informačního systému před zneužitím jeho elektromagnetického záření pomocí elektromagnetické ochrany a zvětšením vzdálenosti zářiče od místa potenciálního odposlechu.

- programovou bezpečností – bezpečné operační systémy, aplikační programové vybavení a ochrany operační paměti, přístupových hesel a dalších.

- programovými bezpečnostními prostředky – kontrola přístupu, monitorování činností a hlášení o narušení informačního systému.

Bezpečnost informačních systémů také souvisí se správnou definicí vlastníka objektů, korektním nastavením přístupových práv s dodržením zásad tvorby bezpečných hesel, volbou vhodného šifrování, ověřováním původu zpráv (elektronický podpis), zálohováním, antivirusovou ochranou, ochrannými mechanismy Systému řízení báze dat a dalšími bezpečnostními mechanismy.

1.3.1 Národní zdravotnický informační systém

Národní zdravotnický informační systém (dále NZIS) je systém, určený ke sběru a zpracování zdravotnických údajů a informací, k vedení Národních zdravotních registrů, k poskytování informací v rozsahu určeném právními předpisy při respektování podmínek ochrany dat a k využití informací v rámci zdravotnického výzkumu [45].

Řízení a koordinace plnění úkolů NZIS, včetně činností souvisejících s jeho rozvojem a zdokonalováním, je základním účelem a předmětem činnosti Ústavu zdravotnických informací a statistiky ČR (dále ÚZIS ČR) [45].

Úloha ÚZIS ČR a NZIS je definována v zákoně č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů – § 67c. ÚZIS ČR je též součástí státní statistické služby a tuto činnost vykonává podle zákona č. 89/1995 Sb., o státní statistické službě, ve znění pozdějších předpisů. ÚZIS ČR při nakládání s osobními údaji NZIS zajišťuje úkoly správce a zpracovatele v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, pokud Ministerstvo zdravotnictví nebo ÚZIS ČR nepověří podle tohoto zákona jiného zpracovatele [45].

1.3.2 Datové standardy a jejich využití při komunikaci

Jedná se o metodický návod ministerstva zdravotnictví k datové struktuře přenosu dat mezi informačními systémy zdravotnických zařízení.

Součinnost potřebná při vytváření, ověřování a implementaci standardů klinických dat pacientů by měla zajišťovat dostupnost a smysluplnost dat z jedné části zdravotnického systému vzhledem k nejrůznejším nastavením. Tyto standardy určují pravidla, díky kterým jsou pacientská data elektronicky ukládána a obměňována. Je potřebné si uvědomit jaký smysl mají tyto datové standardy pro pacienty. Klíčovým rozhodnutím proto musí být správná implementace datových standardů v čase a na správném místě, čímž se docílí kvalitní starostlivosti o data pacientů [25].

Správná součinnost standardů a zdravotnických systémů závisí na dvou základních konceptech, kterými jsou syntax a sémantika. Syntax se vztahuje ke struktuře komunikace. Pro výměnu dat a zpráv se využívá zejména standardů Health Level Seven. Sémantika naopak zprostředkovává význam komunikace. Bez sémantické součinnosti můžou být data pozměňována, no není zde žádná záruka toho, že tato data budou smysluplná a využitelná pro příjemce [25]. V současnosti dostupné zdravotnické standardy využívají oba jmenované koncepty. Tyto standardy můžeme dle K. Kim rozdělit do 6 kategorií (platí zejména v USA) [25]:

1. výměna dat/sdělení dat – využívá se HL7 pro administrativní data jako je pacientská demografie nebo pro setkání lékaře s pacientem; DICOM pro radiologické snímky a standard NCPDP (National Council for Prescription Drug Programs) pro elektronické lékárenské předpisy.

2. standardy názvosloví – tato slovní zásoba poskytuje specifické kódy pro klinické koncepty jako jsou nemoci, seznamy problémů, alergie, léčby a diagnózy, které by měly mít různé textové popisy v kartě pacienta nebo na předpisu.

Využívá se LOINC (Logical Observation Identifiers Names and Codes) pro laboratorní výsledky, SNOMED (Systematized Nomenclature of Medicine) pro klinické pojmy a ICD (International Classification of Diseases) pro diagnózy pacientů.

3. standardy dokumentu – indikují typ informace zahrnuté v odpovídajícím dokumentu. Využívá se zde formát SOAP (Subjective, Objective, Assessment, Plan). CCR (Continuity of Care Record) poskytuje standardní formát pro interkomunikaci.

4. standardy konceptuální – umožňují transport dat přes systém bez ztráty smyslu a kontextu (HL7).

5. standardy aplikací – determinují způsob jakým jsou obchodní pravidla implementována do systému a interakci softwaru systému.

6. standardy architektury – definují procesy čítající ukládání dat a jejich distribuce. Nemocniční fungující strukturou je Národní elektronický zdravotní záznam navrhnutý Institutem Mediciny a HL7.

Datový standard MZ ČR 03. 09. 02

Datový standard pro předávaní pacientských dat mezi zdravotnickými informačními systémy a Národním číselníkem laboratorních položek (dále NČLP) umožňuje praktickému lékaři především elektronickou komunikaci s LIS, elektronické zasílání výsledků (v plném rozsahu a maximální kvalitě) a základní informace o problematice, kterou řeší NČLP (nomenklatura, položky, objednávání, preanalytická fáze, interpretace a jiné).

Komunikace mezi informačními systémy probíhá tak, že informační systém odesílatele připraví datový soubor, který je určen pro jednoho konkrétního příjemce a soubor mu vhodnou a bezpečnou formou předá. V tomto souboru mohou být informace od několika odesílajících subjektů, které jsou součástí informačního systému odesílatele – například několik oddělení může posílat současně v jednom datovém souboru své požadavky na laboratorní analýzy do laboratorního informačního systému v laboratoři příjemce, přičemž každé z oddělení může posílat požadavky a data od více svých pacientů. V rámci předávaného datového souboru je jednoznačně určen jeden příjemce, jeden nebo více odesílatelů a v rámci jednotlivých odesílatelů jsou jednoznačně určeni jednotliví pacienti [30].

Název souboru je konstruován podle jednoznačných pravidel, která jsou popsána v datovém standardu: odesílatel připraví soubor a odešle jej. Vzhledem k možnostem komunikace každého s každým, nelze vytvářet návrh s ohledem na jednoznačnost

názvu z hlediska příjemce. Pokud by to na straně příjemce vadilo, může příjemce zařídit přejmenování došlých souborů ještě před jejich vložením do složky příjmového místa nebo vhodně soubory zařazovat do připravených složek. Odesílatel zajistí vytváření jmen souborů, které nebudou po určitou vhodnou dobu duplicitní [30].

Jméno datového souboru má strukturu:

UTTXXXXX.KKK pro soubory pakované nebo UTTXXXXX.xml pro soubory nepakované, kde:

U – představuje určení t. j. typ přenášených dat a v případě pacientských dat také urgentnost.

TT – určuje typ odesílajícího místa.

XXXXX – libovolný řetězec neobsahující mezery, který je sestavený z číslic a běžných písmen anglické abecedy.

KKK – určuje program, kterým bylo zapakováno (arj, zip, rar).

Nepakované (a rozpakované) soubory mají vždy extenzi XML [30]. V případě XML se jedná o programovací (značkovací) jazyk, pomocí kterého se vytváří struktura pacientských dat v NIS. Časté využívání jazyka XML souvisí právě s jeho jednoduchou strukturou, jednoduchým čtením a dobrou srozumitelností, dále také kvůli příbuzné struktuře s populárním jazykem HTML a celosvětovému rozšíření.

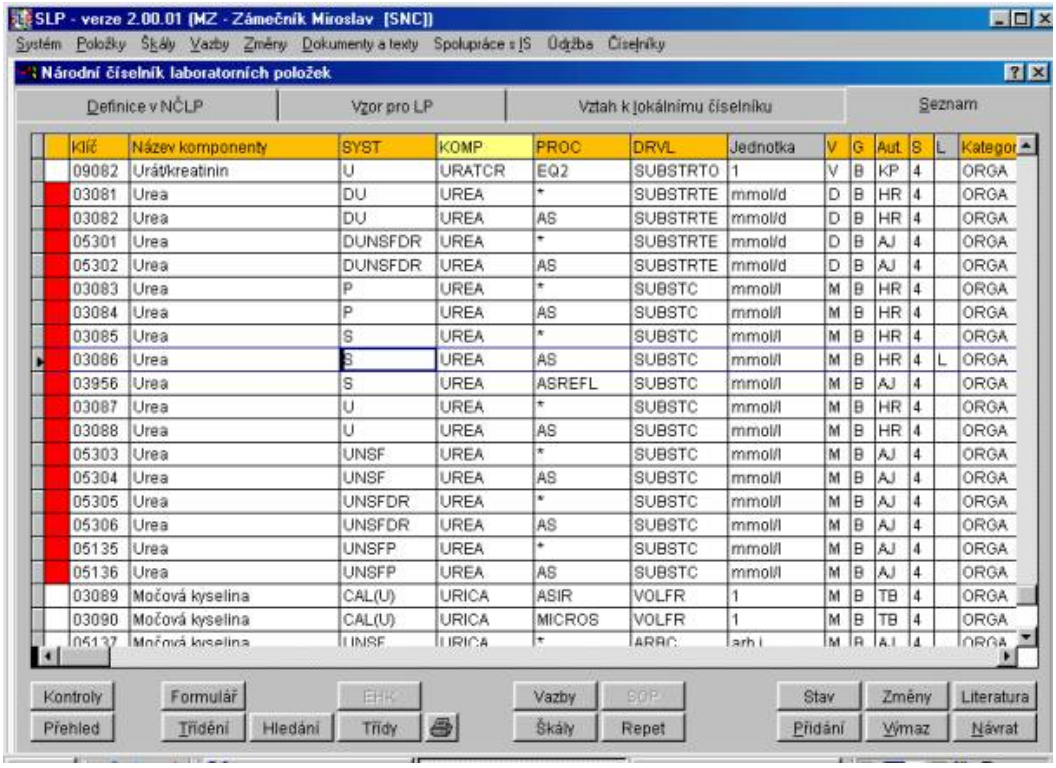
Národní číselník laboratorních položek je také důležitou součástí Datového standardu MZ ČR 03. 09. 02. NČLP je z hlediska informatického datovým souborem, obsahujícím základní definice a popisy laboratorních položek v rozsahu potřebném pro Datový standard MZ ČR. Dále obsahuje základní definice a informace potřebné pro tvorbu standardů efektivní lékařské péče i pro tvorbu standardů managementu kvality v klinických laboratořích a je potřebný pro mnohé zdravotnické informační systémy (LIS, NIS a jiné) [31].

NČLP je sestavován za pomoci elementů, uložených v interních číselnících jako jsou číselníky systémů, komponent, procedur, druhů veličin a jednotek [31].

Datový standard DICOM

DICOM (Digital Imaging and Communications in Medicine) je datový standard navržen pro přenos, ukládání, tisk a přenášení medicínských obrazů jako například grafické výstupy z CT, MR a ultrazvuku. Byl vytvořen asociací The National Electrical Manufacturers Association (NEMA).

Formát obsahuje obrazová data a záhlaví. Hlavička slouží k ukládání textových dat, obrazová data reprezentuje kompletní obrázek uložený do jednoho souboru. Soubor DICOM může obsahovat informace o obrázku ve třech různých dimenzích. Jeho součástí je také definice formátu souborů a popis síťových komunikačních protokolů. Je důležité si uvědomit, že pro komunikaci mezi nemocničními systémy dle



Klíč	Název komponenty	SYST	KOMP	PROC	DRVL	Jednotka	V	G	Aut	S	L	Kategor
09082	Urát/kreatinin	U	URATCR	EQ2	SUBSTRTO	1	V	B	KP	4		ORGA
03081	Urea	DU	UREA	*	SUBSTRTE	mmol/d	D	B	HR	4		ORGA
03082	Urea	DU	UREA	AS	SUBSTRTE	mmol/d	D	B	HR	4		ORGA
05301	Urea	DUNSFDR	UREA	*	SUBSTRTE	mmol/d	D	B	AJ	4		ORGA
05302	Urea	DUNSFDR	UREA	AS	SUBSTRTE	mmol/d	D	B	AJ	4		ORGA
03083	Urea	P	UREA	*	SUBSTC	mmol/l	M	B	HR	4		ORGA
03084	Urea	P	UREA	AS	SUBSTC	mmol/l	M	B	HR	4		ORGA
03085	Urea	S	UREA	*	SUBSTC	mmol/l	M	B	HR	4		ORGA
03086	Urea	S	UREA	AS	SUBSTC	mmol/l	M	B	HR	4	L	ORGA
03956	Urea	S	UREA	ASREFL	SUBSTC	mmol/l	M	B	AJ	4		ORGA
03087	Urea	U	UREA	*	SUBSTC	mmol/l	M	B	HR	4		ORGA
03088	Urea	U	UREA	AS	SUBSTC	mmol/l	M	B	HR	4		ORGA
05303	Urea	UNSF	UREA	*	SUBSTC	mmol/l	M	B	AJ	4		ORGA
05304	Urea	UNSF	UREA	AS	SUBSTC	mmol/l	M	B	AJ	4		ORGA
05305	Urea	UNSFDR	UREA	*	SUBSTC	mmol/l	M	B	AJ	4		ORGA
05306	Urea	UNSFDR	UREA	AS	SUBSTC	mmol/l	M	B	AJ	4		ORGA
05135	Urea	UNSFP	UREA	*	SUBSTC	mmol/l	M	B	AJ	4		ORGA
05136	Urea	UNSFP	UREA	AS	SUBSTC	mmol/l	M	B	AJ	4		ORGA
03089	Močová kyselina	CAL(U)	URICA	ASIR	VOLFR	1	M	B	TB	4		ORGA
03090	Močová kyselina	CAL(U)	URICA	MICROS	VOLFR	1	M	B	TB	4		ORGA

Obr. 1.2: Ukázka seznamu položek v NLČP [31]

datového standardu DICOM se využívá protokol TCP/IP.

Standard DICOM napomáhá součinnosti zařízení:

- Specifikuje skladbu a sémantiku příkazů a souvisejících informací.
- Specifikuje sémantiku souborových složek, souborových formátů a informačních složek nutných pro offline komunikaci.
- Explicitně definuje souhlasné požadavky na implementaci DICOM standardu.
- Usnadňuje operace v síťovém prostředí.
- Je strukturován pro využití nových služeb, také ulehčuje podporu budoucích medicínských zobrazovacích aplikací.
- Využívá existující mezinárodní standardy tam, kde je to využitelné.

Standard DICOM byl vyvinutý se zaměřením se na diagnostické zobrazování využívané v radiologii, kardiologii a obdobných disciplínách; je využitelný také pro široký rozsah obrazových a neobrazových informací, které jsou součástí klinických a jiných systémů.

Hlavní model komunikace standardu obsahuje síťovou komunikaci (komunikaci online) a komunikaci střídaní uložených kapacit (komunikaci offline). Servis vyšších vrstev zabezpečuje nezávislost od podpory fyzické síťové komunikace a protokolů jako např. TCP/IP. Základní DICOM servis souborů zabezpečuje přístup na úložné medium nezávisle od různých datových formátů a datových struktur [33].

Datový standard HL7

Health Level Seven (zkráceně HL7) je společnost akreditovaná Americkým normalizačním a standardizačním institutem (ANSI) pro standardizaci klinických a administrativních údajů ve zdravotnictví. Jejím úkolem je poskytovat standardy pro výměnu, správu a integraci dat sloužící péči o pacienta, související administrativě, poskytování a hodnocení zdravotnických služeb. Konkrétně jde o vytvoření pružných a cenově efektivních přístupů, standardů, doporučení, metodologií a souvisejících služeb pro spolupráci informačních systémů ve zdravotnictví [17].

Nejvíce využívaným standardem HL7 je verze 2. 5. Jde o relativně jednoduchý model zasílání zpráv mezi informačními systémy ve zdravotnictví a jednotlivými zařízeními. Nejnovější verze HL7 2. 5. 1 byla schválena v únoru 2007. Již od konce 90. let 20. století se vyvíjí HL7 verze 3, která usiluje namodelovat veškeré relevantní informace, vztahy a procesy ve zdravotnictví. HL7 verze 3 užívá objektového přístupu; pro modelování využívá UML (Unified Modeling Language) a pro přenos informací XML [17].

Datový standard HL7 verze 3. 0 je reprezentován výraznou změnu oproti předešlým datovým standardů HL7. Poskytuje širokou nabídku voleb a je flexibilní; řady zpráv již byly implementovány v sérií V2.x a byly úspěšně využity. Tyto zprávy se v průběhu let rozvíjely na principu zpětného přístupu, který plnil individuální požadavky prostřednictvím rozvinuté ad-hoc metodologie. Nová verze obsahuje množství nastavitelných datových elementů, které ji dělají schopnou adaptovat se na téměř jakoukoliv stránku. Verze 3 používá objektově-orientovanou vývojovou metodologii a model RIM (Reference Information Model) pro vytvoření zpráv. RIM je základní částí metodologie HL7 verze 3. 0, jak to provádí explicitní reprezentace sémantického a jazykového spojení, které existuje mezi informacemi uloženými uvnitř zpráv HL7 [14].

Datový standard HL7 definuje parametry komunikace na aplikační (nejvyšší) vrstvě v komunikačním modelu ISO/OSI (Obr. 1.3). Standardizuje struktury zpráv, kódovací pravidla pro přenos zpráv a aplikační, spouštěcí události.

Obr. 1.3: Referenční komunikační model ISO/OSI

1.3.3 Zabezpečení přenosu pacientských dat mezi NIS

Síť Internet je v současnosti nejvýznamnějším nástrojem pro přenos (nejen) obrazové dokumentace pacientů mezi NIS, v důsledku čehož dochází k akutní potřebě spolehlivého zabezpečení a s tím související ochraně pacientských dat. Bezpečnost pacientských dat spočívá v zajištění [13]:

- důvěrnosti – zajištění autorizace osob, které disponují přístupem k údajům.
- integrity a autenticity – možnost modifikace informací pouze osobou autorizovanou, přičemž musí zůstat původ informací ověřitelný.
- dostupnosti – přístupnost služeb autorizovaným subjektům.
- prokazatelnosti a nepopíratelnosti odpovědnosti
- spolehlivosti

Jednou z metod řešení těchto problémů může být využívání digitálního podpisu, pomocí kterého se dá docílit zajištění autenticity a integrity dokumentu, také zodpovědnosti konkrétního autora za jeho konání. Vzhledem k podstatě digitálního podpisu se zde využívají biometrické nebo šifrovací technologie, kterým odpovídá biometrický resp. digitální podpis. Biometrický podpis však na rozdíl od digitálního podpisu nezaručuje integritu dokumentu.

Na vytváření digitálního podpisu se využívají šifrovací algoritmy. Z asymetrických šifrovacích algoritmů s veřejným klíčem se nejčastěji uplatňují metody RSA (Rivest-Shamir-Adleman) a DSA (Digital Signature Algorithm). Tyto metody jsou silným autentizačním mechanizmem, kdy za ověřování autenticity odpovídá certifikační autorita. Z bezpečných šifrovacích jednocestných algoritmů se nejčastěji využívá metod MD5 (Message Digest 5) ve spolupráci s RSA, také SHA (Secure Hash

Algorithm) ve spolupráci s DSA. Digitální podpis však kvůli slabé průkaznosti na soudu neznamená zrušení papírové dokumentace.

Základními operativními kroky při ochraně NIS jsou dle autorů knihy *The Practice of System and Network Administration* [18]:

1. Umístění a následná konfigurace firewallu dohlížejícího na rozhraní privátní počítačové sítě s veřejnou počítačovou sítí. Tímto krokem se zabezpečí ochrana lokální počítačové sítě před vnějšími útoky.

2. Nastavení ochranných opatření u všech prvků v počítačové síti, čímž se docílí zvýšení ochrany i v rámci počítačové sítě.

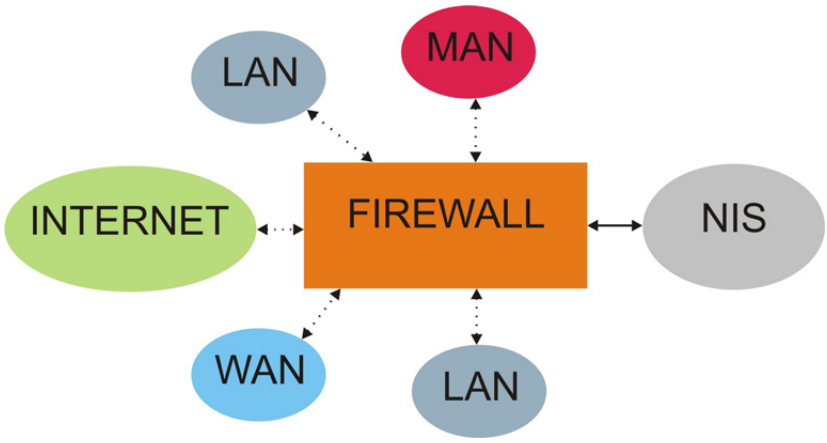
Rozšířená ochrana spočívá v:

- ochraně před viry, trojskými koni a červy – pravidelná antivirová kontrola a aktualizace, kontrola příloh emailů, zablokování HTML v příchozích emailech
- neotevíraní příloh podezřelých, nevyžádaných emailů; nestahování a neinstalování programů z neznámých serverů; nepřipojování neznámých USB klíčů, CD, DVD a pod.
- ochraně pomocí antiadwarů a antispywarů – Ad-aware, Spybot Search a pod.
- ochraně pomocí firewallů
- kódované komunikaci pomocí SSL resp. TLS
- využívání SFTP (Secure File Transfer Protocol) nebo SSH (Secure Shell)
- využívání proxy serverů pro zabezpečení anonymity
- využívaní kódů ne kratších než 3000 bitů v případě šifrování pomocí veřejných klíčů a kódů ne kratších než 128 bitů v případě symetrického šifrování [8]

Firewall

Firewall je zařízení zabezpečující bezpečnost sítě oddělením částí s různým stupněm ochrany. Jedná se o komponentu, která primárně tvaruje komunikaci a přenos mezi sítí a Internetem, nebo dalšími sítěmi [19] – Obr. 1.4. Ochrana spočívá v rozumném nastavení pravidel pro konkrétní síť a firewall chrání porty od neautorizovaného přístupu. Je důležité, aby byl firewall schopen před útokem ochránit sám sebe a také síť, kterou chrání.

Kromě toho zabezpečuje firewall řadu dalších funkcí zvyšujících bezpečnost dané sítě. Umožňuje [46]:



Obr. 1.4: Postavení firewallu v síti s NIS

- sledovat a udržovat stav procesů,
- podporovat nízce postavené protokoly pro multimédia vyžadující UDP nebo broadcastové protokoly,
- autentizaci individuálních uživatelů využívajících znaky pověření v síti nebo jednorázové hesla,
- šifrování nebo dešifrování přenosů směrujících přes firewall,
- vytváření bezpečnostních privátních tunelů a virtuálních sítí v nezabezpečených sítích,
- podporu překladu IP adres: poskytuje jinou vrstvu zabezpečení připoutáním počítačů k intranetu nepřístupným na Internet (využíváním privátních adres) a adresováním malého počtu IP adres,
- ochranu před viry, ActiveX a Javou.

Vedle dovedností se firewally dělí na 4 základní druhy [8]:

- firewall využívající paketovou filtraci – pakety jsou filtrovány na základě uživatelem zvoleného kriteria, např. odkud a kam pakety směrují. Nevýhodou je poměrně jednoduchá modifikace hlavičky paketů při přenosu sítí a tím klesá kvalita zabezpečení.
- firewall využívající inspekci stavů – odstraňuje nedostatky firewallů využívajících paketovou filtraci sledováním sekvencí paketů a rozhodováním se na jejich základě.

- firewall využívající proxy – je implementován v aplikační vrstvě síťového modelu. Srovnává příchozí požadavky se seznamem povolených operací, čímž filtruje a chrání komunikaci.

- firewall pracující na relační vrstvě – identický s firewallem využívajícím proxy. Firewall nejprve ověří koncové body spojení protokolem TCP a následně povolí přenos TCP a UDP (User Datagram Protocol) dat mezi těmito body.

Důležité je si uvědomit, že firewall a kvalita jeho poskytované ochrany závisí na zvolené konfiguraci správcem nebo uživatelem systému. Také netvoří uspokojivou ochranu před viry, které se do počítače dostávají různými cestami. Firewall neposkytuje ochranu před hrozbou z vnitřku sítě.

Problém může nastat v případě, že je umožněn přístup uživatelů NIS do sítě Internet. Podle americké studie *Why Enterprises Need More than Firewalls and Intrusion Detection Systems* [46] je prvním problémem e-mailová komunikace. V případě neuváženého spuštění souboru z přílohy e-mailu, který chybně prošel spamovým filtrem, hrozí reálné riziko narušení bezpečnosti systému. Druhým problémem může být přítomnost JavaScriptu, který se obvykle spouští automaticky a může kontrolovat webové rozhraní a obsah stránek. Útok může spočívat v alternaci uživatelského rozhraní webovým serverem. Jednoduchým řešením je manuální zablokování JavaScriptu v užívaných internetových prohlížečích. Dalším typem útoku je útok založen na využití Java apletu. Uživatel je nalákán na určenou webovou stránku, která je schopna získat informace o přistupujícím uživateli (IP adresu, proxy server, informace o firewallu). Dochází k aktivitám, jejíž snahou je oklamat uživatele naváděním k nesprávné reakci na používané certifikáty, pomocí kterých lze modifikovat systém uživatele a získávat citlivé informace (podrobnější informace o popisovaném problému jsou dostupné z [46]). Konfigurace webového prohlížeče by tak měla být znemožněná koncovým uživatelům NIS a správce NIS by měl zablokovat používání Javy a JavaScriptu.

Šifrování

Cílem šifrování je znemožnit čitelnost citlivého dokumentu neoprávněnými osobami. Tato ochrana nemusí trvat věčně, v některých případech stačí chránit data jenom po definovanou dobu.

Symetrické metody šifrování využívají stejný klíč pro zakódování i rozkódování přenášených dat. Proto je pro rozšifrování zprávy zapotřebí použít stejný klíč, jakým byla zpráva šifrována. Přenos šifrovacího klíče je tedy základem bezpečného

přenosu a úspěšného kódování. Klíč je předáván na začátku komunikace bezpečnostním kanálem, z čeho vyplývá poměrně vysoká rychlost symetrického šifrování, ale také nebezpečí odhalení klíče.

Nejznámějším algoritmem využívaným pro konvenční (symetrické) šifrování je DES. Jedná se o zabezpečovací kód užívající 56bitový klíč. Vylepšenou verzí kódu DES je kód Double DES využívající 112bitový klíč a kód Triple DES využívající 168bitový klíč. Kromě DES klíčů se v praxi objevuje kód IDEA (International Data Encryption Algorithm) využívající 128bitový klíč, kód Blowfish s proměnnou délkou klíče od 32 do 448 bitů, silný kód Twofish a rychlý kód RC4 s libovolnou délkou klíče [8].

Asymetrické metody šifrování využívají dva rozdílné klíče pro zakódování a pro rozkódování zprávy. Šifrování se provádí pomocí veřejného klíče, který je dostupný všem uživatelům dané sítě. Dešifrování se provádí pomocí soukromého klíče, který jediný umožňuje dešifrování přenášené zprávy. Výhodou této metody šifrování je skutečnost, že nedochází k přenosu veřejného klíče jak při symetrických metodách šifrování. Jeho nevýhoda spočívá ve výrazné pomalosti procesu šifrování-dešifrování.

Nejznámějším algoritmem využívaným pro asymetrické šifrování je algoritmus RSA. V současnosti je za spolehlivě zabezpečující považován klíč RSA délky nejméně 2048 bitů. Dalším známým algoritmem využívajícím asymetrické šifrování je algoritmus PGP. PGP využívá silné konvenční symetrické šifrování (typicky 128bitový kód IDEA) pro zašifrování textu se specifickým klíčem, následně se šifruje veřejným klíčem určeným pro zašifrování daného klíče. Z toho plyne, že dvě šifry, stejného textu a určené stejnému uživatelovi budou navzájem rozdílné [8].

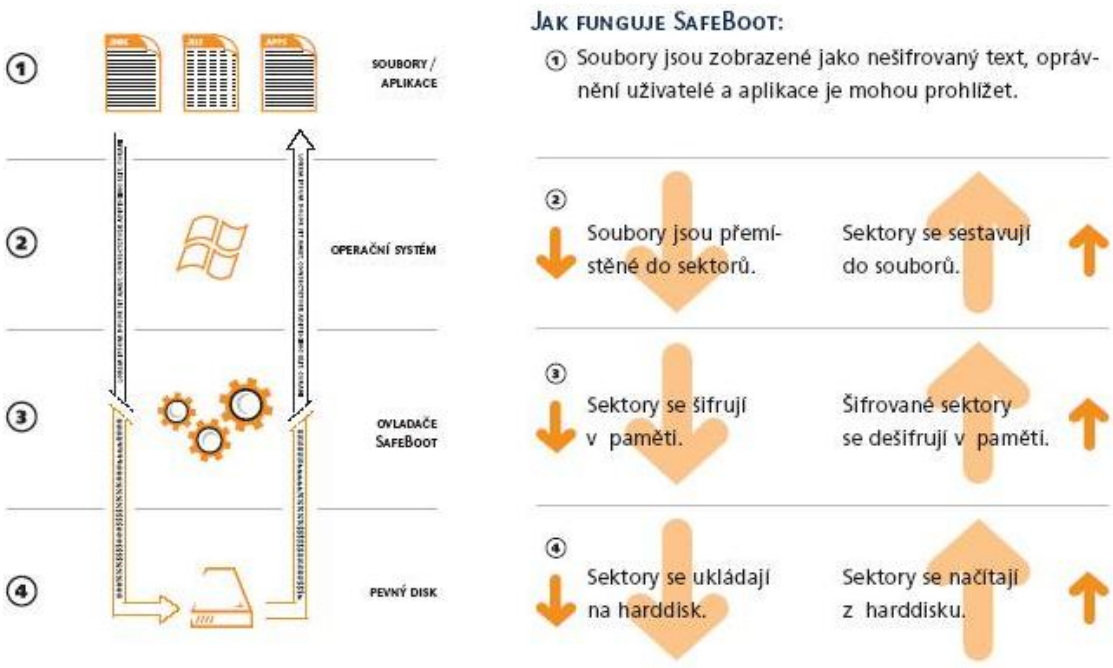
velikost symetrického klíče	velikost asymetrického klíče
56 bitů	384 bitů
64 bitů	512 bitů
80 bitů	768 bitů
112 bitů	1792 bitů
128 bitů	2304 bitů
256 bitů	15000 bitů

Obr. 1.5: Bitové ekvivalenty šifrovacích metod

Šifrování e-mailů pomocí PGP je velmi účinnou metodou ochrany při přenosu dat sítí. Co však může zcela zničit účinnost ochrany je ponechání kódovaného souboru na harddisku. Je potřebné dodržet standardní bezpečnostní zásady při tvorbě hesla a zaručit, aby se v počítači nenacházely viry, trojské koně a pod., které narušují

bezpečnost komunikace. Také je vhodné nepoužívat šifrovací plug-iny v emailových softwarech. Uživatelé by se měli vyvarovat pojmenování veřejného klíče osobními údaji (jméno, e-mail a pod.). Klíč PGP by se neměl ukládat na žádný server a po ukončení komunikace by měl být zmazán.

Pro šifrování disků se využívají programy jako SafeBoot, SecureDoc, Drive Crype Plus Pack (DCPP). SafeBoot Device Encryption zařízení (Obr. 1.6) využívá přísnou kontrolu přístupu a předbootovací ochranu k identifikaci uživatelů a zároveň podporuje jednoduché přihlášení. K šifrování dat na veškerých paměťových discích využívá algoritmy jako RC5-1024 a AES-256 [38]. Na podobném principu pracují i další šifrovací programy.

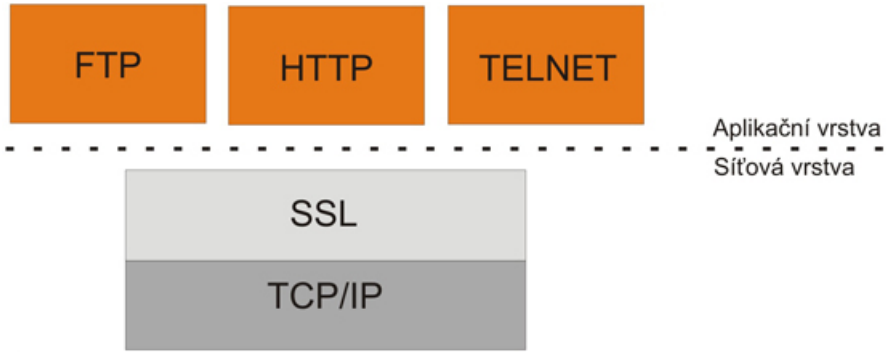


Obr. 1.6: Princip programu SafeBoot [38]

SSL

SSL je protokol vyvinutý firmou Netscape zajišťující bezpečnou komunikaci mezi aplikační a transportní vrstvou. Pro tyto účely se nejčastěji využívá zabezpečeného protokolu HTTPS (Hypertext Transfer Protocol over Secure Socket Layer). Šifrování přenosové cesty na odpovídající vrstvě je zajištěno pomocí digitálních certifikátů a je tvořeno protokoly:

- Record Protocol – zajišťuje šifrování a přenos aplikačních dat.
- Handshake Protocol – zajišťuje sestavení spojení a ověření stran při spojení na základě ověření a odsouhlasení šifrovacího algoritmu a klíčů.



Obr. 1.7: Umístnění protokolu SSL v modelu TCP/IP

Hlavními pozitivy zabezpečení pomocí SSL je dle [35]:

- bezpečnost šifrování – po výměně bezpečnostního klíče inicializačním algoritmem, je používáno symetrické šifrování.
- spolehlivost – kontrola integrity dat pomocí MAC (Message Authentication Code).
- interoperabilita – úspěšná výměna parametrů bez znalosti kódu aplikace druhé strany.
- rozšířitelnost – implementace nových metod šifrování a výměna veřejných klíčů.
- relativní efektivita – snaha o kompenzaci zátěže procesoru.

SSH

SSH je software, který umožňuje bezpečné připojení k jinému počítači přes nezabezpečenou síť jakou je Internet [8]. Tvoří standard připojení se k vzdálenému počítači t. j. vzdálené správě. SSH řeší v podstatě tři klíčové problémy připojení založeném na Telnetu [8]:

1. Slabou autentizaci založenou na adresách IP, která může být zkreslená nebo můžou být vystopovány opakovaně použité hesla.
2. Žádné osobní data jako jsou pakety nemůžou být vystopovány. Obsah komunikace, při přihlášení uživatele s uživatelským jménem a heslem, musí zůstat utajený před neoprávněnými osobami.
3. Ochrana integrity připojení nemůže být napadena.

SSH nikdy nedůvěřuje síti a pro autentizaci využívá veřejné klíče RSA.

2 VÝSLEDKY STUDENTSKÉ PRÁCE

Průvodce instalací a konfigurací programových komponent NIS CLINICOM

2.0.4 Server Apache

Apache je jednoduchý, přitom velmi výkonný web server, který je dostupný jak pro operační systém Windows, tak i pro platformu Unix/Linux [6]. Pomocí naprogramovaných modulů je možné upravovat nebo přidávat postradatelné vlastnosti jako je například podpora zabezpečení OpenSSL a pod.

K zprovoznění spolupráce serveru Apache a databázového programu Caché byla potřebná instalace programu Weblink. Program Weblink je z důvodu zastavení vývoje použitelný jenom s Apache verzemi 1. 2. x a 1. 3. x, takže aktuální, stabilní verze druhé řady serverů nemůžou být použity. Z tohoto důvodu bylo pro plně funkční spolupráci nutné využít např. Apache verzi 1. 3. 37.

Instalační balík `Apache_1.3.34-Mod_SSL_2.8.25-Openssl_0.9.8a-Win32.zip` byl nainstalován do adresáře `c:\apache`. Spolupráce serveru Apache s databází Caché nebyla automatická a bylo proto potřebné modifikovat konfigurační soubor `httpd.conf` nacházející se v adresáři `c:\apache\conf\`. Soubor `httpd.conf` slouží k nastavení hodnot, které říkají vše o tom, jak se server bude jmenovat, kolikrát bude spuštěn, jak velkou zvládne zátěž uživatelů, definují způsob spojení, umístění konfiguračních souborů, chybová hlášení, umístění serveru, a mnoho dalších [7].

V konfiguračním souboru `httpd.conf` se provedou následující změny v nastavení serveru:

```
Port 80
ServerType standalone
ServerAdmin rasotomas@gmail.com
ServerName PC-E218-163.ubmi.feec.vutbr.cz:80
```

Nastavení adresářové struktury:

```
ServerRoot c:\apache
DocumentRoot c:\apache\www
<Directory c:\apache\www>
```

Nastavení přihlašovacích souborů:

```
ErrorLog logs\error.log
CustomLog logs\access.log common
```

```
PidFile logs\httpd.pid
```

kde:

`Port` – nastavení portu, který bude server využívat pro komunikaci (naslouchání)
`ServerType` – hodnota standalone značí, že server bude běžet pořád a nezastaví se
`ServerAdmin` – emailová adresa správce serveru, na který jsou směrovány všechny chybové hlášení ze strany serveru
`ServerName` – název serveru
`DocumentRoot` – adresář, do kterého se ukládají soubory HTML, které mají být umístněny do adresářové struktury serveru
`ServerRoot` – adresář, do kterého byl www server nainstalován
`ErrorLog` – přihlašovací soubor, do kterého server zapisuje své chybové hlášení
`CustomLog` – přihlašovací soubor pro nastavení druhu prohlížečů (`agent.log`), přístupů na server (`access.log`), referenci přístupů (`referer.log`). Příkaz obsahuje 3 parametry. Prvním je příkaz CustomLog, druhým cesta k přihlašovacímu souboru a třetím je způsob zápisu přihlašovacího souboru.
`PidFile` – obsahuje informace o záznamech PID jednotlivých procesů, které se můžou využít při restartu nebo kolapsu serveru.

2.0.5 OpenSSL

OpenSSL je šifrovací soubor nástrojů, který v sobě implementuje síťový protokol SSL (Secure Sockets Layer), transportní protokol TLS (Transport Layer Security) a potřebné šifrovací standardy. Bezpečná komunikace s internetovými servery je zabezpečená prostřednictvím protokolu HTTPS.

Balík OpenSSL není standardně obsažen v programu Apache a proto je nutná jeho samostatná instalace. Volně dostupný instalační balík, např. `Openssl-0.9.8a--Win32.zip` je potřebné extrahovat do adresáře `c:\apache\openssl\` a do této složky následně přidat konfigurační soubor `openssl.conf` dostupný z [3, 4].

Zdrojový kód `"openssl.conf"`:

```
RANDFILE = .rnd
```

[*ca*]
`default_ca = CA_default` – počáteční ca sekce

[*CA_default*]
`certs = certs` – kde sou drženy všechny vydané certifikáty (certs)
`crl_dir = crl` – kde jsou drženy všechny vydané crl
`database = database.txt` – databázový index souboru

`new_certs_dir = certs` – počáteční místo pro nové certifikáty

`certificate = cacert.pem` – CA certifikát
`serial = serial.txt` – aktuální sériové číslo
`crl = crl.pem` – aktuální CRL

`private_key = private\cakey.pem` – privátní klíč
`RANDFILE = private\private.rnd` – privátní náhodné číslo souboru
`x509_extensions = x509v3_extensions` – rozšíření přidáno do cert

`default_days = 365` – platnost certifikátu
`default_crl_days = 30` – délka doby k dalšímu CRL
`default_md = md5` – který md se má použít
`preserve = no` – podržení uplynulého DN řazení

#Pro CA metodu:
[*policy_match*]
```
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = match
commonName = supplied
emailAddress = optional
```

#Pro různé metody:
[*policy_anything*]
```
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
```

[*req*]
```
default_bits = 1024
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
attributes = req_attributes
```

```
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_min = 2
```

```
countryName_max = 2
stateOrProvinceName = State or Province Name (full name)
localityName = Locality Name (eg, city)
0.organizationName = Organization Name (eg, company)
organizationalUnitName = Organizational Unit Name (eg, section)
commonName = Common Name (eg, your website's domain name)
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 40
```

[*req_attributes*]

```
challengePassword = A challenge password
challengePassword_min = 4
challengePassword_max = 20
```

[*x509v3_extensions*]

```
#pod ASN.1, bit 0 bude kódovaný jako 80
# nsCertType = 0x40
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName
#nsCertSequence
#nsCertExt
#nsDataTypeRANDFILE=.rnd
```

Následně je potřebné zavést knihovny `ssleay.dll` a `libeay32.dll` do adresáře `c:\WINDOWS\system32\`. V adresáři `c:\apache\openssl\` je třeba spustit program `openssl.exe` a vygenerovat certifikát a privátní klíč.

Nejprve je potřebné vytvořit žádost (server.req) a privátní klíč (privkey.pem) obsahující heslo a další hodnoty, které budou předmětem certifikátu.

```
req -config openssl.conf -new -out server.req
```

Odstraněním passphrase z privátního klíče se umožní serveru Apache přistupovat k tomuto klíči.

```
rsa -in privkey.pem -out server.key
```

Vytvoření vlastního certifikátu ze žádosti:

```
x509 -in server.req -out server.cer -req -signkey server.key -days 365
```

kde:

`req` – práce s certifikační žádostí
`new` – vytvoření nové žádosti
`config - openssl.conf` – konfigurace zadaného souboru `-openssl.conf`
`rsa` – práce s RSA klíčem
`x509` – vytvoří certifikát podepsaný sám sebou (self-signed certificate)
`nodes` – soukromý klíč nebude šifrován
`out server.req` – zapíše certifikát do souboru `server.req`
`out server.key` – klíč zapíše do souboru `server.key`
`days 365` – platnost certifikátu 365 dní

Dodatečně je možné nastavit:

`Country Name` – kód státu (CZ)
`State or Province` – název státu nebo provincii (Czech republic)
`Locality Name` – název města (Brno)
`Organization Name` – název organizace (VUT)
`Organizational Unit Name` – název sekce organizace (DBME)
`Common Name` – název užívané domény (PC-E218-163.ubmi.feec.vutbr.cz)
`Email Address` – emailovou adresu (rasotomas@gmail.com)

Na závěr se certifikát (server.cer) a privátní klíč (server.key) nakopírují do nově vytvořené složky `c:\apache\conf\ssl\` a je potřebná opětovná konfigurace souboru `http.conf` programu Apache.

Příkaz `Port 80` je nahrazen příkazem:

```
Port 443
Listen 443
```

Příkaz `ServerName PC-E218-163.ubmi.feec.vutbr.cz:80` je nahrazen příkazem `ServerName PC-E218-163.ubmi.feec.vutbr.cz:443`.

Následně je nutné doplnit zdrojový kód o řádky, pomocí kterých dojde k přidání SSL modulu:

```
LoadModule ssl_module modules\mod_ssl.so
AddModule mod_ssl.c
```

A na konec zdrojového kódu přidat:

```
SSLMutex none
SSL RandomSeed startup builtin
SSLSessionCache none
```

```
<VirtualHost PC-E218-163.ubmi.feec.vutbr.cz:443>
SSLEngine On
SSLCertificateFile c:/apache/conf/ssl/server.cer
SSLCertificateKeyFile c:/apache/conf/ssl/server.key
</VirtualHost>
```

Apache server je tak nakonfigurován a připraven pro komunikaci s OpenSSL.

2.0.6 Caché

Postrelační databáze Caché se v zdravotnictví využívá především kvůli velké rychlosti přístupu k vícerozměrným datům a její dobré spolupráci s ostatními technologiemi. Jedná se o objektovou databázi postavenou na jazyku SQL (Structured Query Language), která podporuje přístup prostřednictvím rozhraní ODBC a JDBC. Caché zahrnuje také aplikační server s progresivními možnostmi objektového programování, schopnost snadné integrace se širokou paletou technologií a databázový stroj s technologií vyrovnávacích pamětí [32].

Program Caché (přesně Caché 5. 0. 20.) je nutné instalovat až po úspěšné instalaci serveru Apache. Pro správnou funkci programu je v případě operačního systému Windows nezbytná verze Professional, nikoli Home edition!

Do zdrojového kódu programu Apache je po instalaci Caché potřebné přidat následující řádky:

```
ScriptAlias \RTG\ c:\CacheSys\weblink\i386\
<Directory c:\CacheSys\weblink\i386\>
AllowOverride None
Options ExecCGI
Order allow,deny
Allow from all
</Directory>
```

A na závěr zdrojového kódu definovat vlastní virtuální CSP (Caché Server Pages) server [28]:

```
#LoadModule cspsys_module_sa c:\CacheSys\Objects\i386\CSPapSys.dll
#LoadModule csp_module_sa c:\CacheSys\Objects\i386\CSPap.dll
<Location \csp\bin\Systems\>
SetHandler cspsys-handler-sa
<\Location>
<Location \csp\bin\RunTime\>
SetHandler csp-handler-sa
```

```
<\Location>
AddHandler csp-handler-sa csp cls
Alias \csp\ c:\CacheSys\CSP\
<Directory c:\CacheSys\CSP\>
AllowOverride None
Options MultiViews FollowSymLinks ExecCGI
Order allow,deny
Allow from all
</Directory>
```

2.0.7 Caché Weblink

Caché Weblink poskytuje vysoce výkonnou výměnu dat mezi databázemi Caché, internetovými servery a webovými prohlížeči. Obsluhuje jenom Internet nebo prostředí Intranetu a obsahuje 2-bytovou kódovou podporu [20].

Funkce Caché WebLink jsou následující:

- Caché Weblink přijímá požadavek
- Caché Weblink předá požadavek Caché systému na zpracování
- Caché Weblink vrátí Caché výstup webovému klientu

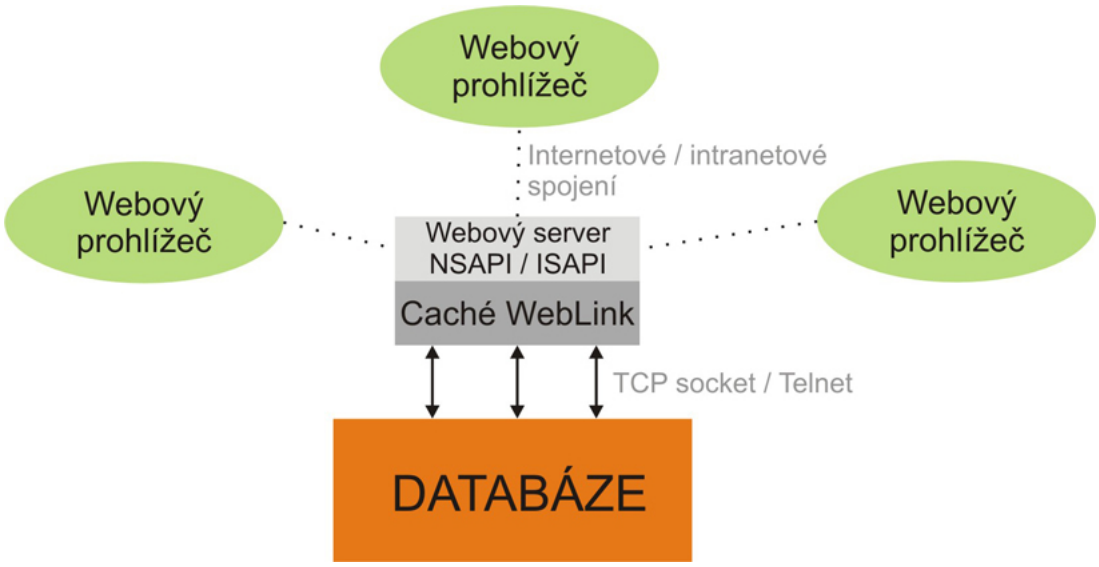
Model architektury pro tyto funkce zobrazuje Obr. 2.1. Program Caché Weblink však není obsažen v základní instalaci databázového programu Caché a proto je potřebné tuto komponentu doinstalovat dodatečně. Je bezplatně dostupný ze stránek `http://weblink.intersys.com`.

Celou složku Caché Weblink je potřebné zkopírovat do adresáře `\c:\CacheSys\` a následně pomocí Caché terminálu zavést důležité rutiny a knihovny pro komunikaci se serverem Apache. Ze souboru `mgw.ro` je nutné zavést rutiny `%mgw`, `%mgw0`, `%mgw3`, `%mgwa`, `%mgwb`, `%mgwd`, `%mgwe`, `%mgwj` (Příloha B.1), následně zavést rutiny `mgw1.ro` (Příloha B.2), `%ZMGW2.rsa` (Příloha B.3) a `mgwstubs.ro` (Příloha B.4). Nakonec se přepíše rutina `%mgw3` na `%ZMGW2` pomocí příkazu `ZL %mgw3 ZS %ZMGW2`.

2.0.8 Program radiologického oddělení (RTG)

Zavedení databáze

Databázi RTG (`Cache.dat`) je vhodné zkopírovat do nově vytvořeného adresáře `c:\CacheSys\Mgr\RTG\`, následně aktivovat samotnou databázi a vytvořit nový `Namespace`.



Obr. 2.1: Základní architektura sítě vzhledem k programu Caché WebLink

Instalace programu

V adresáři `c:\CacheSys\` je potřebné vytvořit složku RTG, která je určena pro samotnou instalaci programu RTG.

Pro správnou komunikaci databáze Caché s programem RTG je nutné nejprve spustit program `EditReg.exe`, který je součástí balíku RTG. Je dostupný z adresáře `c:\CacheSys\RTG\util\`.

Nastavení parametrů po startu RTG (Obr. 2.2):

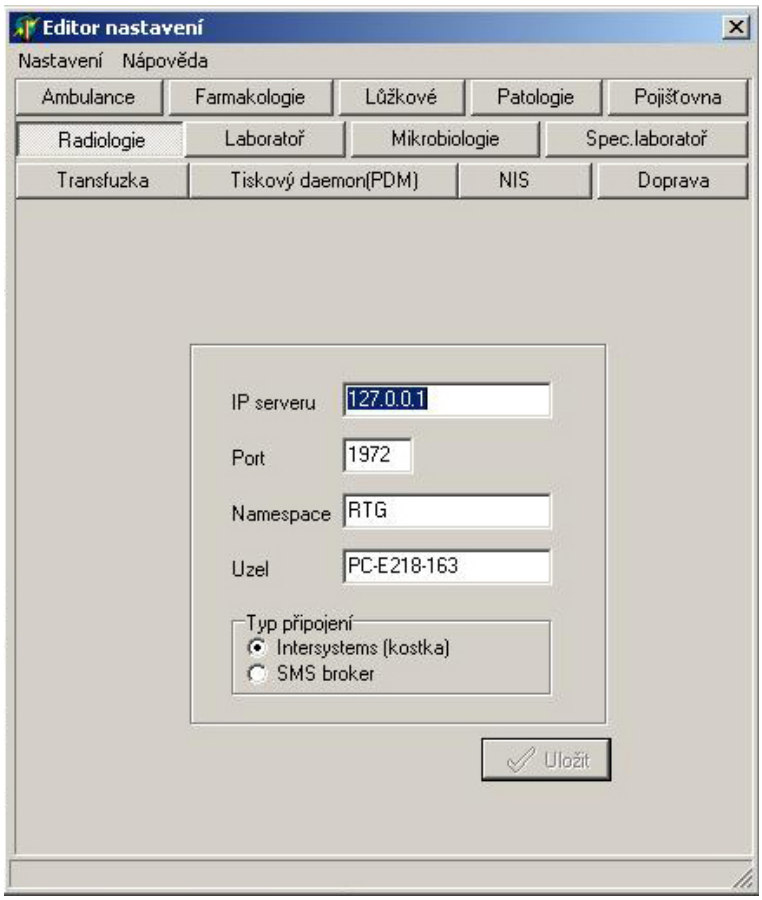
IP server: 127.0.0.1
Port: 1972
Namespace: RTG
Uzel: PC-E218-163

Pomocí součásti Caché Terminal je potřebné přidat do `Namespace %SYS` rutinu `ZSTU.rsa` (Příloha B.5). V programu RTG je možné zvolit složky pro snímky, konkrétně v nabídce `Nastavení modulu\Složky pro snímky`. Pro správnou funkci webového rozhraní je nutné aby se cesta nastavená v aplikaci RTG shodovala s cestou uloženou v databázi na místě `FIS\T\SET\cesta` [32].

Aktuálně nastavené složky:

Pracovní složka: `c:\CacheSys\RTG\OBR\All`
Pacientská složka: `c:\CacheSys\RTG\OBR\Pacient`

Dále zbývá nastavit uživatelská práva uživatelům přistupujícím k pacientským datům přes Internet, což je možné udělat v nabídce `Nastavení systému\Přístupová`

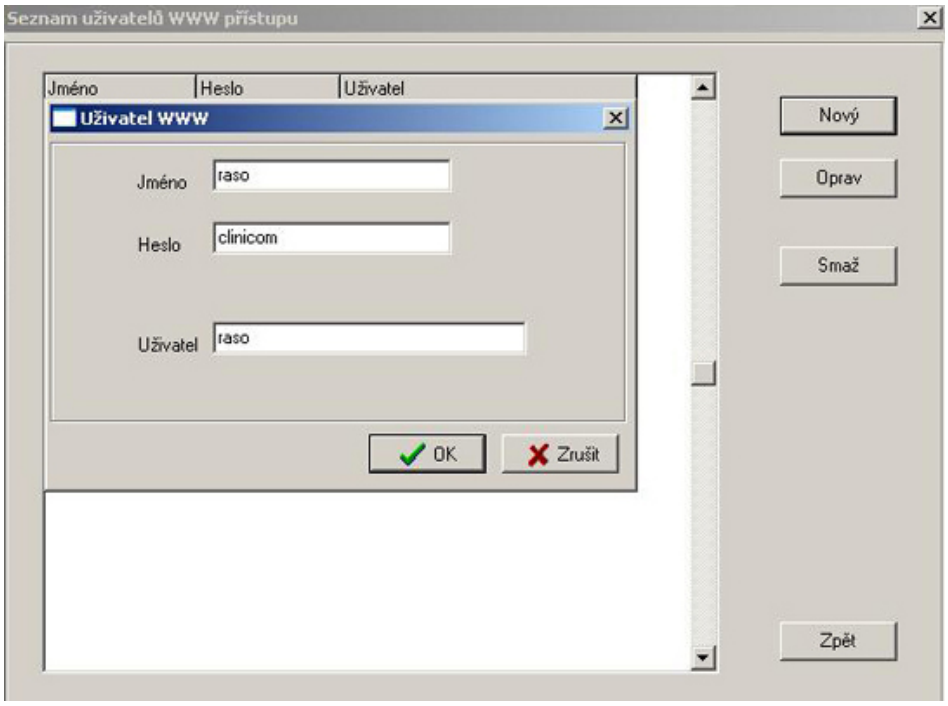


Obr. 2.2: Editor nastavení modulu RTG

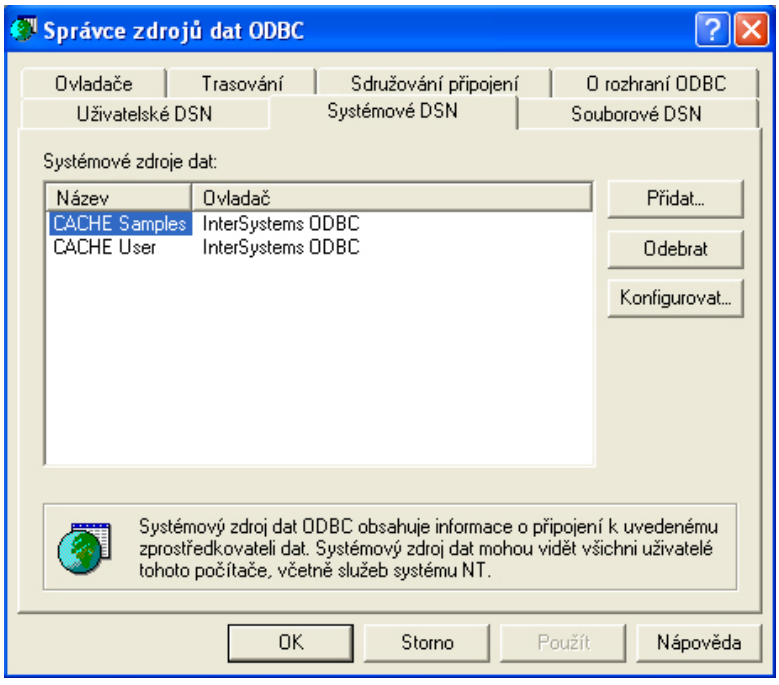
`práva www` – Obr. 2.3.

2.1 Konfigurace Správce zdrojů dat ODBC

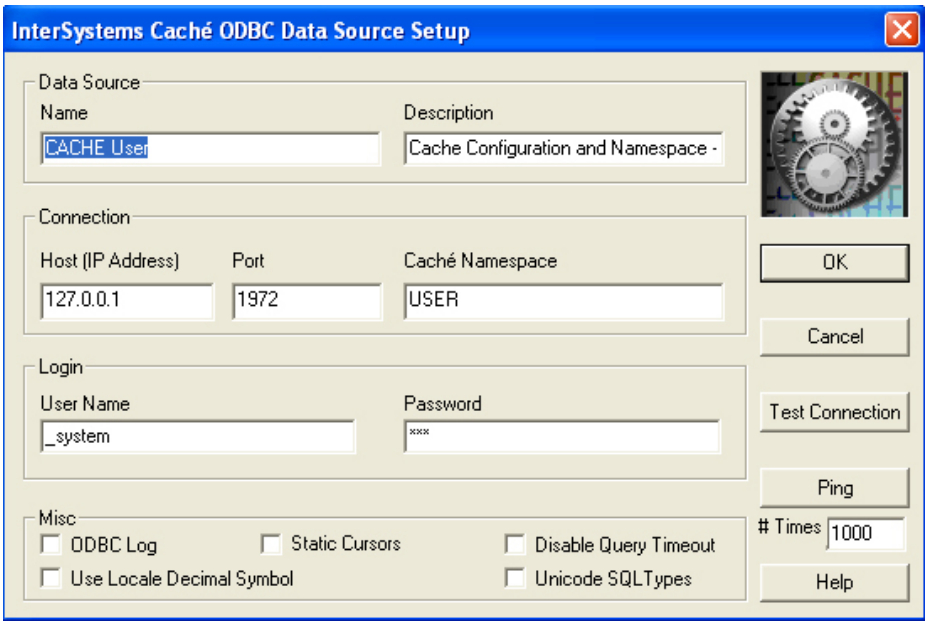
Pro správnou funkci programů Apache, Caché Weblink a Caché je nutná konfigurace ovladače ODBC. V adresáři `Ovládací panely\Nástroje pro správu\Datové zdroje (ODBC)` je dostupný Správce zdrojů dat ODBC. Konfigurace a správné nastavení Správce zdrojů dat ODBC dokumentují Obr. 2.4 a Obr. 2.5. Na průběh testování připojení jsou zaměřené Obr. 2.6 a Obr. 2.7. Heslem, ukrytým na Obr. 2.5 za hvězdičkami je `sys`.



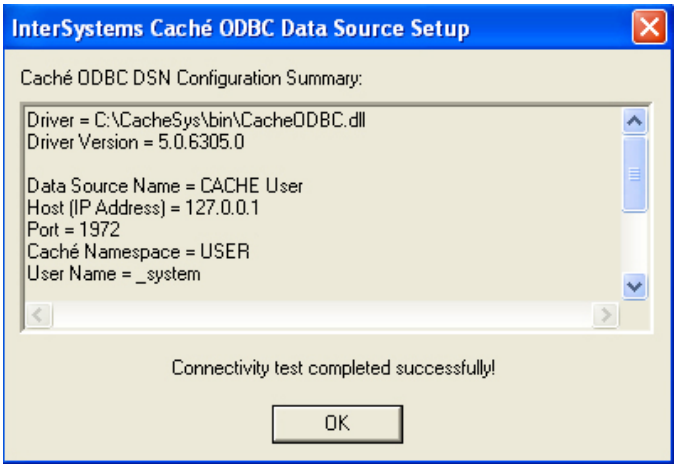
Obr. 2.3: Správce uživatelů www přístupu k programu RTG



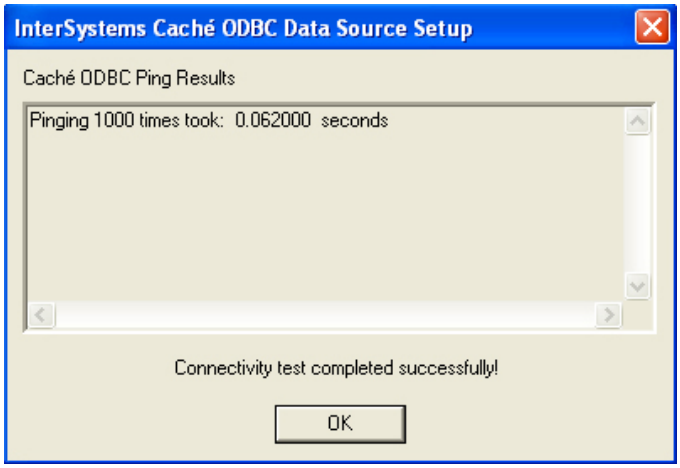
Obr. 2.4: Správce zdrojů dat ODBC – základní rozhraní



Obr. 2.5: Správce zdrojů dat ODBC – nastavení parametrů



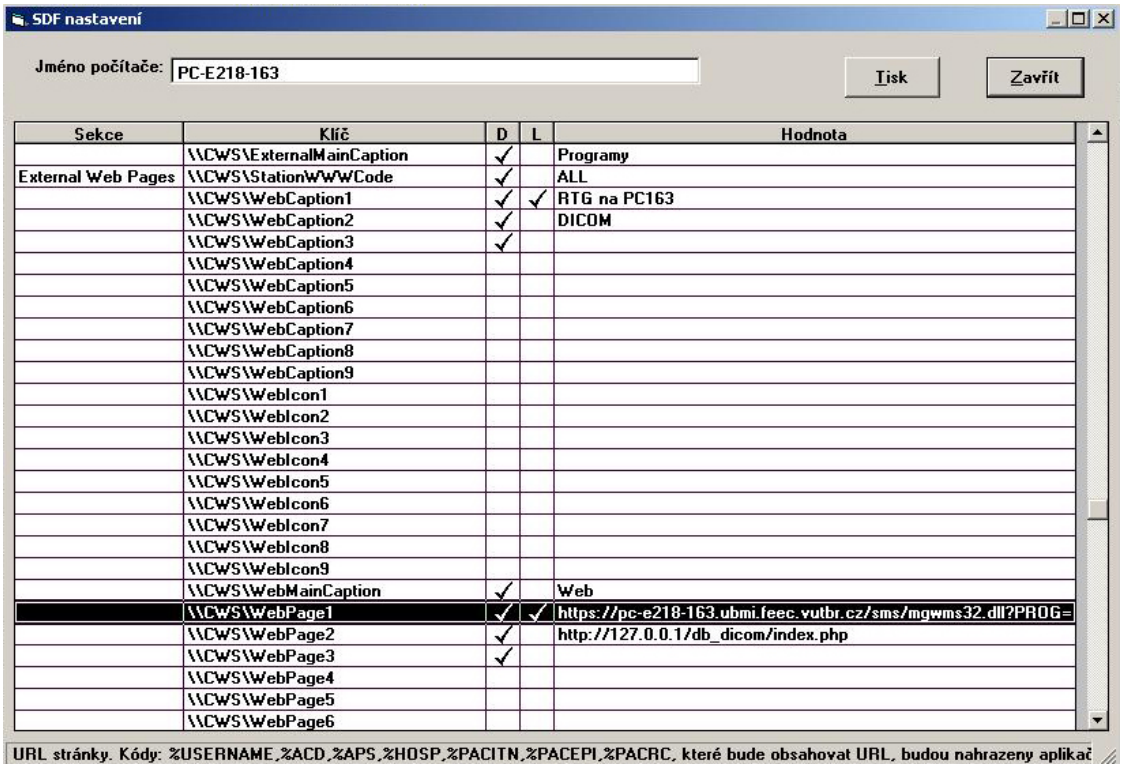
Obr. 2.6: Správce zdrojů dat ODBC – test konektivity



Obr. 2.7: Správce zdrojů dat ODBC – test spojení pomocí příkazu ping

2.2 CareCenter

Pro nastavení přístupu uživatele do systému je zapotřebí přidání položky `RTG na PC163` v hlavním menu programu (`Nástroje\SDF nastavení\SDF položky`). V otevřeném okně pro úpravu SDF záznamů se do volného klíče `\\CWS\WebCaption` uloží název položky `RTG na PC163` a do klíče `\\CWS\WebPage` adresa serveru ve tvaru `https://PC-E218-163.ubmi.feec.vutbr.cz/sms/mgwms32.dll?PROG=^Wini&ZN==RTG` resp. IP adresa počítače provozujícího server `https://147.229.77.201/sms/mgwms32.dll?PROG=^Wini&ZN=RTG`. Tímto zápisem, včleněným do adresy serveru se zavolá knihovna `mgwms32.dll` a parametr `PROG` určí program, který bude knihovnou zavolán. Pro aktualizaci provedených nastavení je potřeba program CareCenter restartovat.

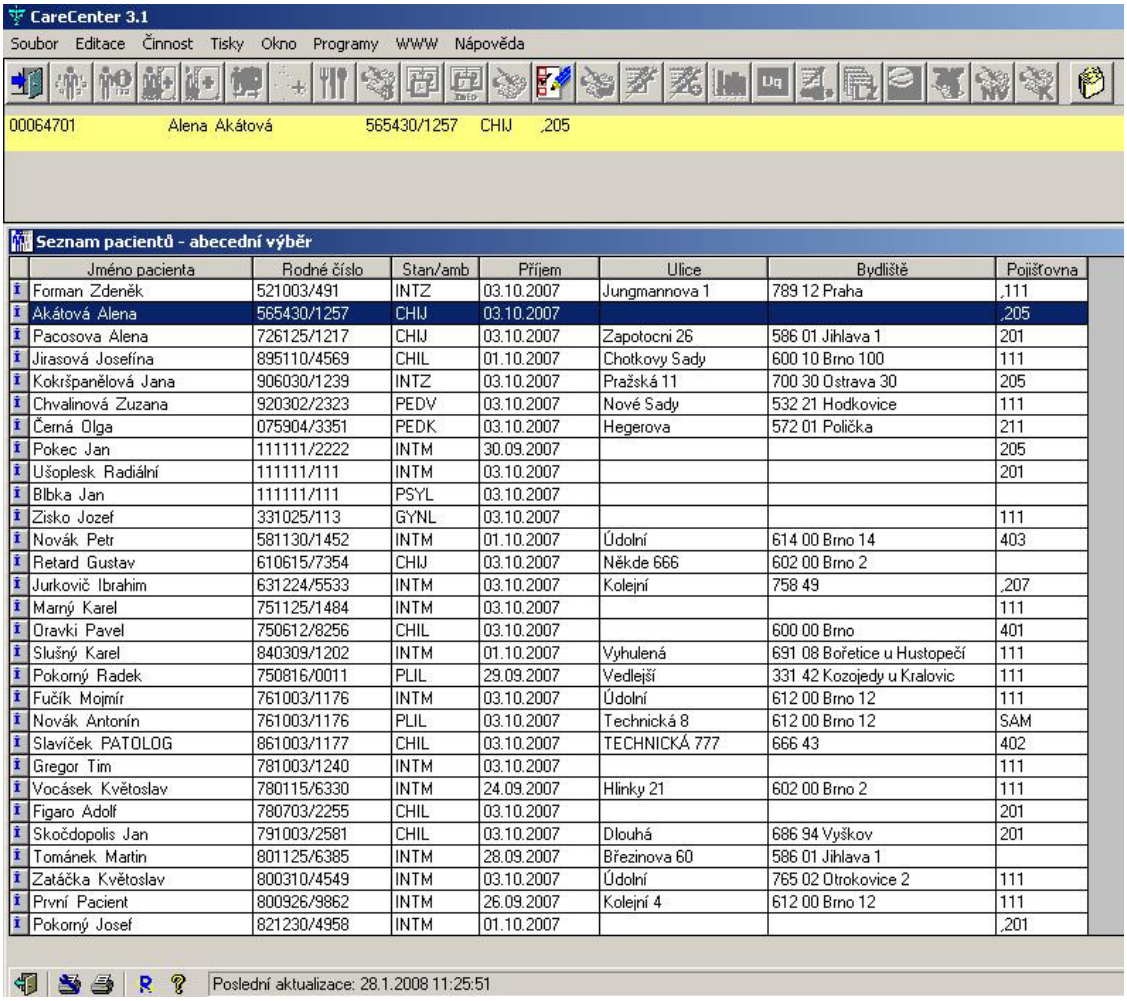


Obr. 2.8: SDF nastavení v programu CareCenter

2.3 Komunikace programů CareCenter a RTG

Při spuštění programu CareCenter 3. 1. se automaticky otevře databáze a vygeneruje se odpovídající seznam pacientů (Obr. 2.9). Při žádosti lékaře o vyšetření pacienta je potřebné vyplnit žádanku, v které je potřebné definovat požadovaný výkon včetně způsobu vyšetření, typu pracoviště a také části těla pacienta požadované k vyšetření.

Pro korektní vystavení žádanky je nutné definovat prioritu, čas, datum, anamnézu, způsob transportu, jméno lékaře a předpokládanú diagnózu. Po úspešném zaslání žádanky je žádanka doručena a přijata RTG systémem. Po převedení žádanky do systému RTG je danému pacientovi po absolvování vyšetření přiřazen odpovídající snímek (Obr. 2.10). Vyšetřující lékař doplní výsledný obrázek popisem nálezu, z něho plynoucího závěru a doplní informace o typu výkonu pro zdravotní pojišťovnu. Po lékařské kontrole je zpracovaná žádanka odeslaná zpět na oddělení, které vyšetření iniciovalo.



Obr. 2.9: Grafické rozhraní programu CareCenter – seznam pacientů

2.4 Webové rozhraní programu RTG

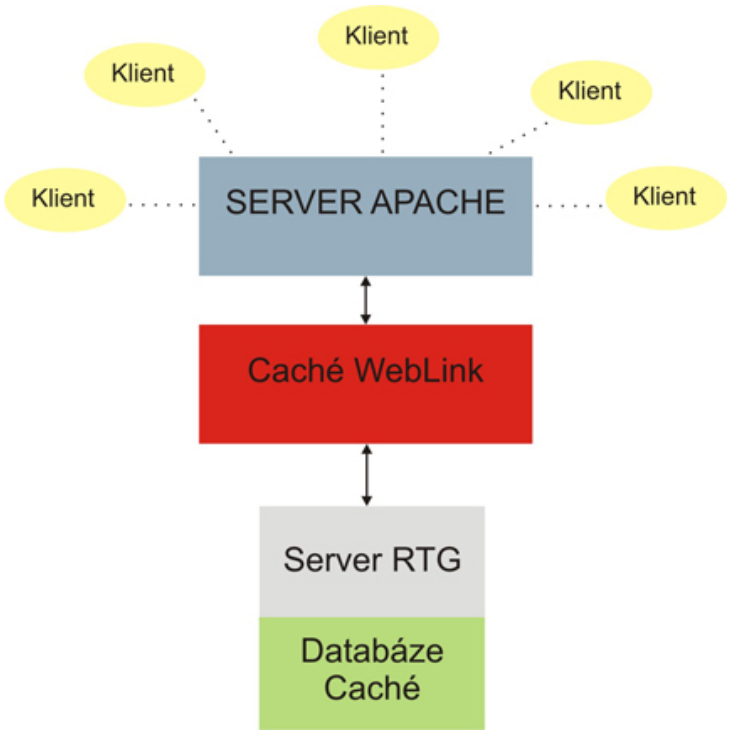
Úlohou webového rozhraní programu RTG je umožnit rychlý přístup odpovědného personálu nemocnice k rentgenologickým datům pacientů. Výsledkem je časově úsporný přístup k potřebným datům, který je kromě uvedených pozitiv schopen přinést

Obr. 2.10: Přiřazení snímku pacientovi v programu RTG

úsporu finančních prostředků a zvýšit dynamiku celého nemocničního informačního systému.

Klient přistupuje k databázi RTG prostřednictvím serveru Apache, se kterým komunikuje přes zabezpečený protokol HTTPS (port 443). Apache získává potřebné informace z databáze RTG prostřednictvím databázového serveru Caché. Komunikace je zprostředkována rozhraním Caché Weblink přes knihovnu `mgwms32.dll`. Přímé připojení k databázovému serveru zabezpečuje aktuálnost dat v aplikaci RTG. Popsaný komunikační proces zobrazuje Obr. 2.11.

Navigace v systému je analogická s klasickým přístupem do systému; kromě pacientských snímků disponuje základními informacemi o pacientovi, jménem lékaře požadujícího a realizujícího vyšetření, parametry vyšetření, výkony pro zdravotní pojišťovny a pod. Vstup do systému je chráněn přihlašovacím jménem a heslem,



Obr. 2.11: Komunikace klient – server u programu RTG

které zabezpečují selekci přistupujícího personálu do systému. Komunikace klient – server je zabezpečena pomocí šifrování protokolem SSL. Každý přístup do systému je kromě toho zaznamenáván do souboru `RTG.log`, který je součástí adresáře `c:\apache\logs\`. Zpětnou analýzou tohoto souboru je možné určit přihlašovací jména, IP adresy a čísla pacientů, s kterými přihlášená osoba nakládala.

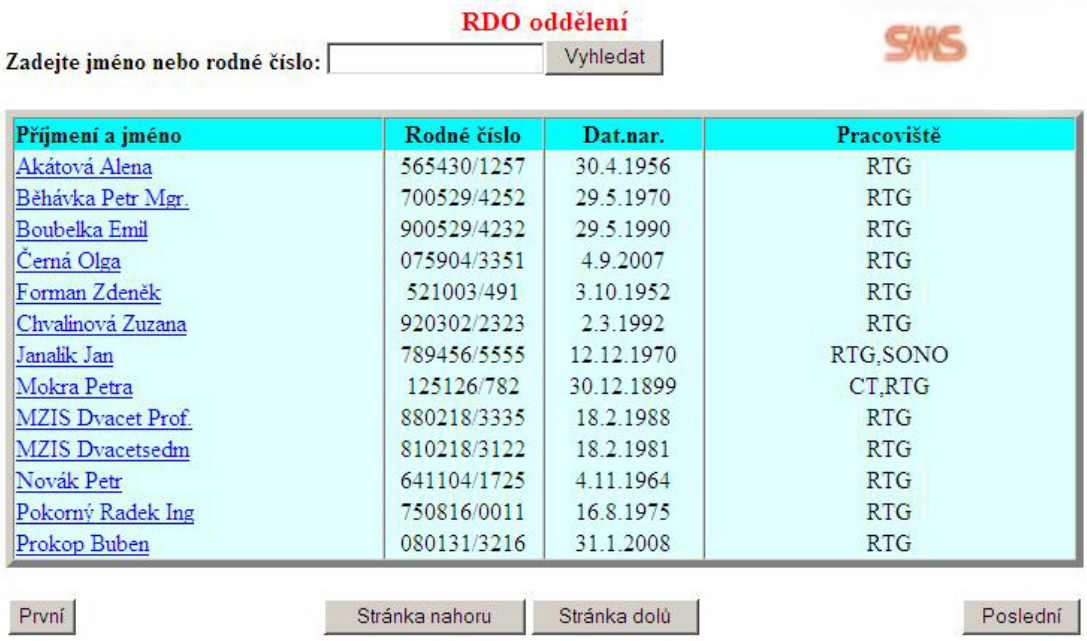
Po aktivaci položky `RTG na PC163` v hlavním menu programu CareCenter se otevře okno s hlášením o zabezpečení stránky a výzva k přijetí certifikátu vygenerovaného přímo užívaným serverem. Po přijetí certifikátu následuje otevření samotné přihlašovací stránky (Obr. 2.12), prostřednictvím které může uživatel vstoupit do databáze pacientů. Tím je funkčnost spojení programů CareCenter a RTG prostřednictvím sítě Internet z části ověřená.

Z externého prostředí se dá do RTG systému přistoupit pomocí webového prohlížeče, kliknutím na odkaz `Přihlašení do RDO`, který je součástí naprogramovaného webového rozhraní sloužícího k připojení na radiologické oddělení instalovaného na ÚBMI (Obr. 2.13). Rozhraní, podobně jako program CareCenter, využívá k přihlašení do radiologického systému odkaz `https://PC-E218-163.ubmi.feec.vutbr.cz/sms/mgwms32.dll?PROG=^Wini&ZN=RTG`, který zavolá knihovnu `mgwms32.dll` a následně i spustí program RTG. Analogicky s předešlým postupem platí, že po přijetí certifikátu dojde k otevření přihlašovací stránky (Obr. 2.12) a uživatel může vstoupit do databáze pacientů.

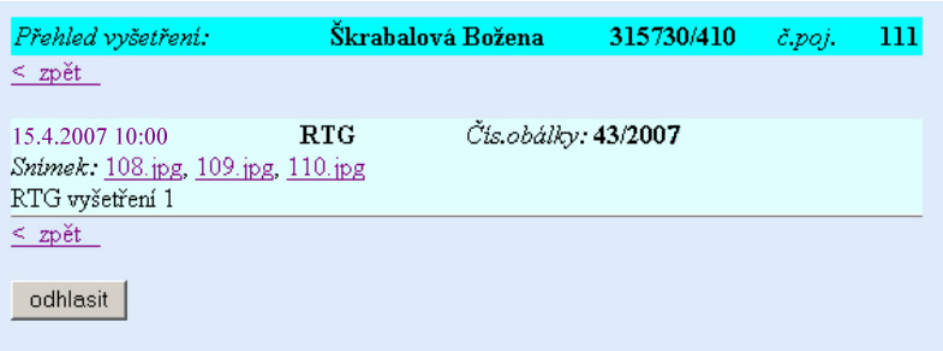
Obr. 2.12: Přihlašovací okno na RDO oddělení

Obr. 2.13: Webové rozhraní pro přihlášení na radiologické oddělení ÚBMI

Přímo po přihlášení do databáze se otevře stránka obsahující seznam pacientů s aktivní žádankou na radiologické oddělení (Obr. 2.14). Seznam pacientů obsahuje základní informace čítající jméno pacienta, rodné číslo, datum narození a druh pracoviště, kde byl záznam pořízen. Program umožňuje prohlížet seznam pacientů, vyhledávat pacienty dle různých kriterií či vyhledávat informace v archivu, který obsahuje dokončené vyšetření z minulosti.



Obr. 2.14: Seznam pacientů v systému RDO



Obr. 2.15: Ukázka záznamu pacienta

Přehled vyšetření: **Boubelka Emil** **900529/4232** *č.poj.* **111**

< zpět

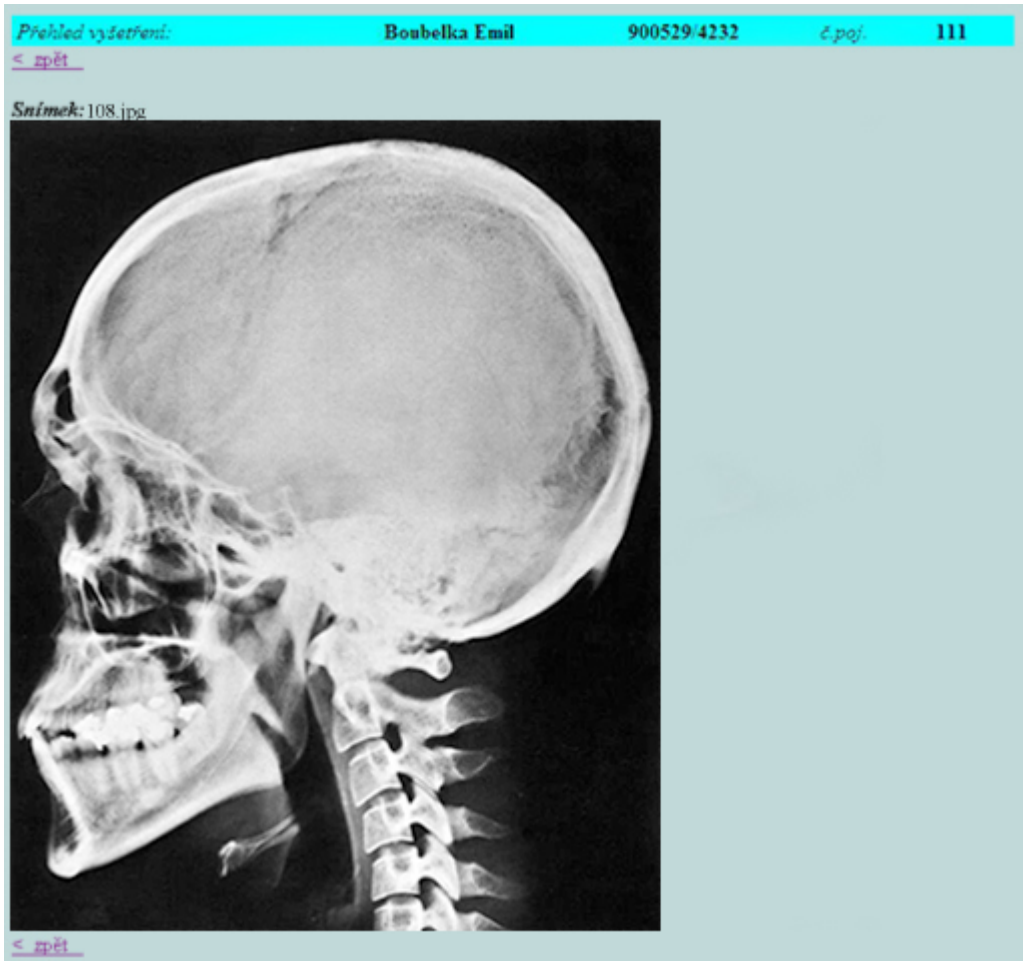
Datum vyšetření: 31.1.2002 13:14 Pracoviště: RTG Diagnóza: P92.4,H00.0
Žadatel:
Oddělení: NIS IČP: 68001406

Popsal: Cučelik A.

Nález:
Normálně velká lebka bez známek nitrolební hypertenze. Strukturální změny nejsou patrné. Frontální endokranioza. Sella ostře konturovaná bez tlakových změn. Skelet bez prokazatelných traumatických změn.Dobře vytvořená pneumatizace beze změn struktury a transparence. Vnitřní zvukovody souměrné, bez tlakových změn.
Závěr:
mas to tam
Výkony ZP:
- 89115 RTG LEBKY; PüEHLEDNÉ SNÖMKY (89115) Provedl: Cučelik Alois

< zpět

Obr. 2.16: Ukázka záznamu pacienta



Obr. 2.17: Prohlížení snímků pacienta

3 ZÁVĚR

Žijeme v době Internetu, což se odráží ve většině technických oborů, nevyjímaje nemocniční informační systémy. Čím dál tím více jsou diskutovány možnosti využití sítě Internet k přenosu obrazové dokumentace pacienta a i z tohoto důvodu se snaží text diplomové práce přispět k rozšíření diskuze v oboru lékařské informatiky. Navzdory zřetelné podpoře využití sítě Internet pro přenos obrazové dokumentace pacientů je zde věnována nemalá pozornost právě její ochraně.

Diplomová práce nazvaná Obrazová dokumentace v nemocničním informačním systému se zaobírá pacientskou obrazovou dokumentací, konkrétně její architekturou, zabezpečením a přenosem uvnitř i vně NIS.

Práce popisuje strukturu, základní vlastnosti a funkce obecného nemocničního informačního systému. Na základě známé architektury definuje odpovídající strukturu obrazové dokumentace a vhodnost přístupu k této dokumentaci pro zdravotnický personál, také způsoby ochrany před neoprávněnými přístupy a zneužíváním citlivých pacientských dat. Obsahuje popis nemocničního informačního systému CLINICOM s důrazem věnovaným oddělení radiologie.

Tato práce také odkazuje na platné zákony České republiky, které je potřebné v souvislosti s ochranou dat splnit. Důležitou součástí jsou etické otázky týkající se ochrany pacientských dat. Pojednává se zde o etickém kodexu pacientů i administrativních opatřeních potřebných pro bezpečný přenos pacientských dat mezi NIS.

Diplomová práce dále obsahuje analýzu přenosu pacientských dat prostřednictvím sítě Internet s ohledem na bezpečnost a spolehlivost systému. Stručně se věnuje smyslu a využití datových standardů pro komunikaci, také zabezpečení přenosu pacientských dat mezi NIS.

Na základě analýz popisuje návrh a realizaci rozhraní pro dálkový přístup k obrazové dokumentaci radiologického oddělení NIS CLINICOM na ÚBMI. Součástí práce je úspěšná realizace testu konektivity k této dokumentaci ze vzdáleného pracoviště. Podrobný popis instalace a konfigurace programových komponent NIS CLINICOM může být využit jako užitečný návod pro opětovnou realizaci obdobného systému vzhledem k účelům výuky na ÚBMI.

Programy, jejichž obrazová dokumentace a výstupy tvoří součást této diplomové práce, byly licencovány firmou SMS s. r. o. [43] pro potřeby ÚBMI na VUT v Brně. Ostatní použité programy jsou volně dostupné z Internetu ve verzi freeware. Snímky pacientů použity v této diplomové práci byly zbaveny identity a jsou dostupné z rentgenologického virtuálního atlasu [12].

LITERATURA

[1] ANDERSON, R. *Security in clinical information system.* Cambridge: University of Cambridge, 1996. ISBN 0-7279-1048-5

[2] ANDERSON, R. *A security policy model for clinical information systems.* In Proc. of the 15th IEEE Symp. on Security and Privacy. IEEE Comp. Society Press, 1996.

[3] BÁRÁNY, B. *The Apache + SSL on Win32* [online]. Leden 2007 [cit. 1. dubna 2007]. Dostupné z WWW: <http://tud.at/programm/apache-ssl-win32-howto.php3>.

[4] BEATTIE, D. *Openssl* [online]. Únor 2003 [cit. 4. března 2007]. Dostupné z WWW: <http://www.dylanbeattie.net/docs/openssl.conf>.

[5] BELLOVIN, S. M.; CHESWICK, W. R.; RUBIN, A. D. *Firewalls and Internet Security.* Addision-Wesley 2003. 433 s. ISBN 0-201-63466-X

[6] BROŽEK, E. *Server Apache, co je vlastně zač a co dokáže* [online]. Říjen 1998 [cit. 4. března 2007]. Dostupné z WWW: <http://www.zive.cz/h/Uzivatel/AR.asp?ARI=3277>.

[7] BROŽEK, E. *Konfigurujeme Apache - soubor httpd.conf* [online]. Listopad 1998 [cit. 4. března 2007]. Dostupné z WWW: <http://www.zive.cz/h/Programovani/AR.asp?ARI=3626>.

[8] CALOYANNIDES, A., M. *Privacy Protection and Computer Forensics Second Edition.* Boston: Artech House 2004. 366 s. ISBN 1-58053-830-4

[9] CVIS *DICOM* [online]. Září 2006 [cit. 19. února 2007]. Dostupné z WWW: <http://www.cvis.cz/hlavni.php?stranka=novinky/clanek.php&id=487>.

[10] DOSTÁL, O. *Využití vysokorychlostní sítě pro potřeby přenosu medicínských aplikací.* Olomouc: Univerzita Palackého v Olomouci 2000. s. 31-33. ISBN 80-244-0095-2

[11] ENGELSCHALL, S. R. *User manual mod_SSL* [online]. 1998 - 2000 [cit. 9. března 2008]. Dostupné z WWW: <http://www.modssl.org/docs/2.1/>.

[12] FOLBER, F. *RenTGenový atlas* [online]. 2001- [cit. 10. prosince 2007]. Dostupné z WWW: <http://rtg.misto.cz/>.

[13] HANÁČEK, P. *Definice bezpečnostních funkcí pro předávání dat ve zdravotnictví* [online]. Česká společnost zdravotnické informatiky a vědeckých informací, 2002- [cit. 8. prosince 2007]. Dostupné z WWW: <http://cszivi.cls.cz/dokumenty.htm>.

[14] Health Level Seven. *Specifications of HL7* [online]. 2005- [cit. 4. prosince 2007]. Dostupné z WWW: <http://www.hl7.org/>.

[15] HICOMP SYSTEMS CZ. *NIS* [online]. 2007- [cit. 1. dubna 2007]. Dostupné z WWW: <http://www.nis.cz/nis.htm>.

[16] HIPPISLEY-COX, J. *The electronic patient record in primary care – regression or progression? A cross sectional study.* London: British Medical Journal 2003. 326 s.

[17] HL7 Česká republika. *HL7 a standardy HL7* [online]. 2005- [cit. 27. listopadu 2007]. Dostupné z WWW: <http://www.hl7.cz/cz/hl7/about.html>.

[18] HOGAN, Ch. J., CHALUP, S. K., LIMONCELLI, T. A. *The Practice of System and Network Administration.* Boston: Addision-Wesley 2007. s. 272 ISBN 0-321-49266-8

[19] CHAPMAN, D., ZWICKY, E. *Building Internet Firwalls.* O'Reilly & Associates, Inc. 1995.

[20] INTERSYSTEMS. *Caché Documentation* [online]. 2007- [cit. 12. března 2007]. Dostupné na WWW: <http://docs.intersystems.com>.

[21] JECHOVÁ, H. *Definice nemocničního informačního systému a jeho subsystémů.* In Sborník: Nemocniční informační systémy ve výuce informatiky na lékařských fakultách. Praha: I lékařská fakulta Univerzity Karlovy 2000. s. 54-55.

[22] JELÍNEK, P. *StaproTomocon PACS.* Pardubice: STAPRO s. r. o. 2005.

[23] KASAL, P., SVAČINA, Š. a kol. *Internet a medicína.* Praha: Grada 2001. 224 s. ISBN 80-247-0119-7

[24] KASAL, P. *Lékařská informatika.* Praha: Karolinum – nakladatelství Univerzity Karlovy 1998. ISBN 80-7184-594-9

[25] KIM, K. *Clinical Data Standards in Health Care: Five Case Studies.* Oakland: California Healthcare Foundation 2005. ISBN 1-932064-94-X

[26] KOSINER, I., PAPP, R., SEINER, M, ZÁMEČNÍK, M. *Problematika ochrany zdravotnických dat, klasifikace citlivosti zdravotnických dat a doporučené bezpečnostní funkce pro jejich přenos.* Příručka Ministerstva zdravotnictví ČR, verze 1.

[27] KRÁL, J. *Informační systémy.* Veletiny: Science 1998. 356 s.

[28] KUTÁČ, D. *Tipy a triky pro Caché XI. – definování virtuálních CSP serverů* [online]. Únor 2006 [cit. 9. března 2008]. Dostupné z WWW: <http://www.dbsvet.cz/view.php?cisloclanku=2006020901>.

[29] Ministerstvo vnitra ČR. *Sbírka zákonů* [online]. Duben 2007 [cit. 25. října 2007]. Dostupné na WWW: <http://www.mvcr.cz/sbirka/2000/sb032-00.pdf>.

[30] Ministerstvo zdravotnictví ČR. *Datový standard MZ ČR 03. 09. 02* [online]. Duben 2005 [cit. 27. listopadu 2007]. Dostupné z WWW: <http://www.mzcr.cz/index.php?kategorie=31>.

[31] Ministerstvo zdravotnictví ČR. *Základní informace k národnímu číselníku laboratorních položek* [online]. Duben 2005 [cit. 4. prosince 2007]. Dostupné z WWW: <http://www.mzcr.cz/data/c764/lib/mzaia.htm>.

[32] MUSIL, P. *Obrazová dokumentace v nemocničním informačním systému Clinicom: diplomová práce.* Brno: FEKT VUT v Brně, 2006. s. 31-33., příl. 3

[33] National Electrical Manufacturers Association. Digital Imaging and Communications in Medicine (DICOM). *DICOM* [online]. Leden 2007 [cit. 1. prosince 2007]. Dostupné z WWW: <http://medical.nema.org/dicom/2007/07_01pu.doc>.

[34] Parlament ČR. *Listina základních práv a svobod* [online]. Prosinec 1992 [cit. 24. října 2007]. Dostupné na WWW: <http://www.psp.cz/docs/laws/listina.html>.

[35] ODVÁRKA, P. *SSL protokol - princip a přínosy* [online]. Duben 2002 [cit. 15. března 2008]. Dostupné z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=171>.

[36] OpenSSL. *Keys* [online]. 2008- [cit. 9. března 2008]. Dostupné na WWW: <http://www.openssl.org/docs/HOWTO/keys.txt>.

[37] SAGIT. *Listina základních práv a svobod* [online]. Květen 2007 [cit. 13. listopadu 2007]. Dostupné na WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb07111&cd=76&typ=r>.

[38] SafeBoot©Device Encryption^{TM}. *Bezpečnostní řešení pro PC, laptopy a tablet PC* [online]. 2005- [cit. 31. března 2008]. Dostupné na WWW: <http://www.safeboot.cz/device>.

[39] SEINER, M. *Legislativa, týkající se ochrany osobních údajů pacientů ve zdravotnické dokumentaci* [online]. Září 2005 [cit. 25. října 2007]. Dostupné z WWW: <http://www.infomed.cz/ps/article.php?arid=43>.

[40] SEINER, M. *Ochrana osobních údajů ve zdravotnické dokumentaci* [online]. Září 2005 [cit. 11. listopadu 2007]. Dostupné z WWW: <http://www.infomed.cz/ps/article.php?arid=44>.

[41] SEINER, M. *Zákon č. 111/2007Sb. – zásadní změny v právu na informace o zdravotním stavu – jak se projeví v klinických informačních systémech?* [online]. Květen 2007 [cit. 13. listopadu 2007]. Dostupné z WWW: <http://www.infomed.cz/ps/article.php?arid=106>.

[42] SMS. *Funkční specifikace CareCenter*. Brno: SMS Brno s.r.o., 1999.

[43] SMS. *Nemocniční informační systém CLINICOM* [online]. 2008- [cit. 1. února 2008]. Dostupné z WWW: <http://www.smed.cz/>.

[44] ÚSTAV ZDRAVOTNICKÝCH INFORMACÍ A STATISTIKY ČR. *Národní Zdravotnický Informační Systém stav k 1. 1. 2004* [online]. 2004- [cit. 13. března 2007]. Dostupné z WWW: <http://www.uzis.cz/cz/nzis04/nzis_vykazy2004.htm>.

[45] ÚSTAV ZDRAVOTNICKÝCH INFORMACÍ A STATISTIKY ČR. *Národní Zdravotnický Informační Systém stav k 1. 1. 2004* [online]. 2007- [cit. 18. listopadu 2007]. Dostupné z WWW: <http://www.uzis.cz/info.php?article=12&mnu_id=7100&mnu_action=select>.

[46] VANDENWAUVER, M., CLAESSENS, J., MOREAU, W., VADUVA, C., MAIER, R. *Why Enterprises Need More than Firewalls and Intrusion Detection Systems*. California: In Proceedings of the Eighth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'99) 1999. s. 152 – 157. Dostupné z WWW: <http://citeseer.ist.psu.edu/vandenwauver99why.html>.

[47] Zákony ČR. *Zákon č. 47/1992 Sb.* [online]. 1992- [cit. 24. října 2007]. Dostupné na WWW: <http://www.zakonycr.cz/seznamy/0401964Sb.html>.

[48] Zákony ČR. *Zákon č. 412/2002 Sb.* [online]. 2002- [cit. 25. října 2007]. Dostupné na WWW: <http://www.zakonycr.cz/seznamy/1401961Sb.html>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ANSI American National Standards Institute – Americký normalizační a standardizační institut

API Application Programming Interface – rozhraní pro programování aplikací

CCR Continuity of Care Record

CD Compact Disc

COSTAR Computer Stored Ambulatory Record – ambulantní systém COSTAR

CSP Caché Server Pages

CT Computed Tomography – počítačová tomografie

DCPP Drive Crype Plus Pack

DICOM Digital Imaging and Communications in Medicine – datový standard DICOM

DSA Digital Signature Algorithm

DVD Digital Versatile Disc

DSS Decision Support System

EEG Electroencephalography – Elektroencefalografie

EKG Elektrokardiogram

EHR Electronic Health Record – elektronický záznam péče o pacienta

EPR Electronic Patient Record – elektronický záznam o pacientovi

HIS Hospital Information System – nemocniční informační systém

HL7 Health Level Seven – datový standard HL7

HTP modul hospodářsko-technických a provozních služeb

HTTPS Hypertext Transfer Protocol over Secure Socket Layer – zabezpečený protokol HTTP

ICD International Classification of Diseases – mezinárodní klasifikace nemocí

IDEA International Data Encryption Algorithm

ISO/OSI International Standards Organization / Open System Interconnection – referenční komunikační systém ISO/OSI

IZIP internetový přístup ke zdravotním informacím pacienta

LIS Local Information System – lokální informační systém

LOINC Logical Observation Identifiers Names and Codes

LSPP lékařská služba první pomoci

MAC Message Authentication Code

MD5 Message Digest 5

MR magnetická rezonance

MZ ČR Ministerstvo zdravotnictví České republiky

NCPDP National Council for Prescription Drug Programs

NČLP Národní číselník laboratorních položek

NEMA The National Electrical Manufacturers Association – asociace NEMA

NIS Nemocniční informační systém

NZIS Národní zdravotnický informační systém

ODBC Open Database Connectivity

PACS Picture Archiving and Communication Systems – systémy archivace obrázků a komunikace

PET Positron Emission Tomography – pozitronová emisní tomografie

RDO radiologické oddělení

RIM Reference Information Model – model RIM

RSA Rivest-Shamir-Adleman

RTG rentgen

RZP rychlá záchranná služba

SDF System Definition File – soubory systémových definic

SFTP Secure File Transfer Protocol

SHA Secure Hash Algorithm

SNOMED Systematized Nomenclature of Medicine

SOAP Subjective, Objective, Assessment, Plan

SONO ultrazvukové vyšetření

SQL Structured Query Language

SSH Secure Shell

SPECT Single Photon Emission Computed Tomography – jednofotonová emisní tomografie

SSL Secure Sockets Layer

TCP/IP Transmission Control Protocol/Internet Protocol – síťový protokol TCP/IP

TLS Transport Layer Security

UDP User Datagram Protocol

UML Unified Modeling Language – jazyk UML

ÚZIS Ústav zdravotnických informací a statistiky ČR

VZP Všeobecná zdravotní pojišťovna

XML Extensible Markup Language – jazyk XML

SEZNAM PŘÍLOH

A Realizace NIS CLINICOM s webovým rozhraním RTG **78**

B Úprava rutin v programu Caché Terminal **79**

B.1 Zavedení rutin ze souboru "mgw.ro" 79

B.2 Zavedení rutiny "mgw1.ro" 80

B.3 Zavedení rutiny "%ZMGW2.rsa" 81

B.4 Zavedení rutiny "mgwstubs.ro" 82

B.5 Zavedení rutiny "ZSTU.rsa" 83

B.6 Zavedení databáze RTG 84

C Obsah přiloženého cd **89**

A REALIZACE NIS CLINICOM S WEBOVÝM ROZHRANÍM RTG

1. Instalace a konfigurace serveru Apache.
2. Konfigurace modulu OpenSSL v programu Apache.
3. Instalace programu Caché a rekonfigurace serveru Apache.
4. Instalace Caché Weblink a zavedení potřebných rutin a knihoven pomocí terminálu Caché.
5. Instalace programu RTG a zavedení databáze RTG do programu Caché.
6. Konfigurace parametrů připojení v programu Caché pomocí Editoru nastavení.
7. Konfigurace Správce zdrojů dat ODBC.
8. Instalace programu CareCenter a nastavení přístupových práv uživatelů.
9. Nastavení uživatelských práv připojení přes Internet pomocí programu RTG.
10. Návrh a realizace webového rozhraní pro přístup k programu RTG.

B ÚPRAVA RUTIN V PROGRAMU CACHÉ TERMINAL

B.1 Zavedení rutin ze souboru "mgw.ro"

```
USER>ZN

ZN
^
<SYNTAX>
USER>ZN "%CACHELIB"

%CACHELIB>d ^%RI

Input routines from Sequential
Device: c:\CacheSys\Weblink\mgw.ro   Parameters: "R"=>

File written by Cache for Windows NT using %RO on 01 Nov 2002   1:16 PM
with extension INT and with description:
WebLink Version 4.30.605

( All Select Enter List Quit )

Routine Input Option: All Routines

If a selected routine has the same name as one already on file,
shall it replace the one on file? No => Yes
Recompile? Yes => Yes
Display Syntax Errors? Yes => Yes

^ indicates routines which will replace those now on file.
@ indicates routines which have been [re]compiled.
- indicates routines which have not been filed.


%mgw.INT@       %mgw0.INT@      %mgw3.INT^@     %mgwa.INT@      %mgwb.INT@
%mgwd.INT@      %mgwe.INT@      %mgwj.INT@

8 routines processed.
```

Obr. B.1: Zavedení rutin ze souboru "mgw.ro"

B.2 Zavedení rutiny "mgw1.ro"

```
%SYS>ZN "%CACHELIB"

%CACHELIB>d ^%RIMF

Load routines from a %ROMF file.

WARNING: This routine will delete the source code (if any)
         for existing object routines that are being replaced.


Device: c:\CacheSys\Weblink\mgw1.ro
           file format: ("UR") =>

M/WNT wrote this file on Jan 09 2003  5:26 PM.
File Comment: WebLink Version 4.30.605

( All Select Enter List Quit )

Routine Input Option: All Routines

If a selected routine has the same name as one already on file,
shall it replace the one on file? No => Yes
Building existing routine list ... done.


@ indicates routines which have been saved to disk.
. indicates routines which already exist in this directory.

Loading Routines ...
%mgw1@.

   1 routine in  0 minutes,   0 seconds
none of them skipped.
```

Obr. B.2: Zavedení rutiny "mgw1.ro"

B.3 Zavedení rutiny "%ZMGW2.rsa"

```
%CACHELIB>ZN "%SYS"

%SYS>d ^%RI

Input routines from Sequential
Device: c:\CacheSys\Weblink\%ZMGW2.rsa   Parameters: "RS"=>

File written by Cache for Windows NT using %RO on Apr 25 2005   2:45 PM
with extension INT and with description:
Export of 1 routines from namespace %SYS

( All Select Enter List Quit )

Routine Input Option: All Routines

If a selected routine has the same name as one already on file,
shall it replace the one on file? No => Yes
Recompile? Yes => Yes
Display Syntax Errors? Yes => Yes

^ indicates routines which will replace those now on file.
@ indicates routines which have been [re]compiled.
- indicates routines which have not been filed.


%ZMGW2.INT@

1 routine processed.
```

Obr. B.3: Zavedení rutiny "%zmgw2.rsa"

B.4 Zavedení rutiny "mgwstubs.ro"

```
%SYS>d ^%RI

Input routines from Sequential
Device: c:\CacheSys\Weblink\mgwstubs.ro   Parameters: "R"=>

File written by Cache for Windows NT using %RO on 01 Nov 2002   1:11 PM
with extension INT and with description:
WebLink Version 4.30.605 - Stub routines

( All Select Enter List Quit )

Routine Input Option: All Routines

If a selected routine has the same name as one already on file,
shall it replace the one on file? No => Yes
Recompile? Yes => Yes
Display Syntax Errors? Yes => Yes

^ indicates routines which will replace those now on file.
@ indicates routines which have been [re]compiled.
- indicates routines which have not been filed.


%MGW.INT@       %MGWJ.INT@

2 routines processed.
%SYS>
```

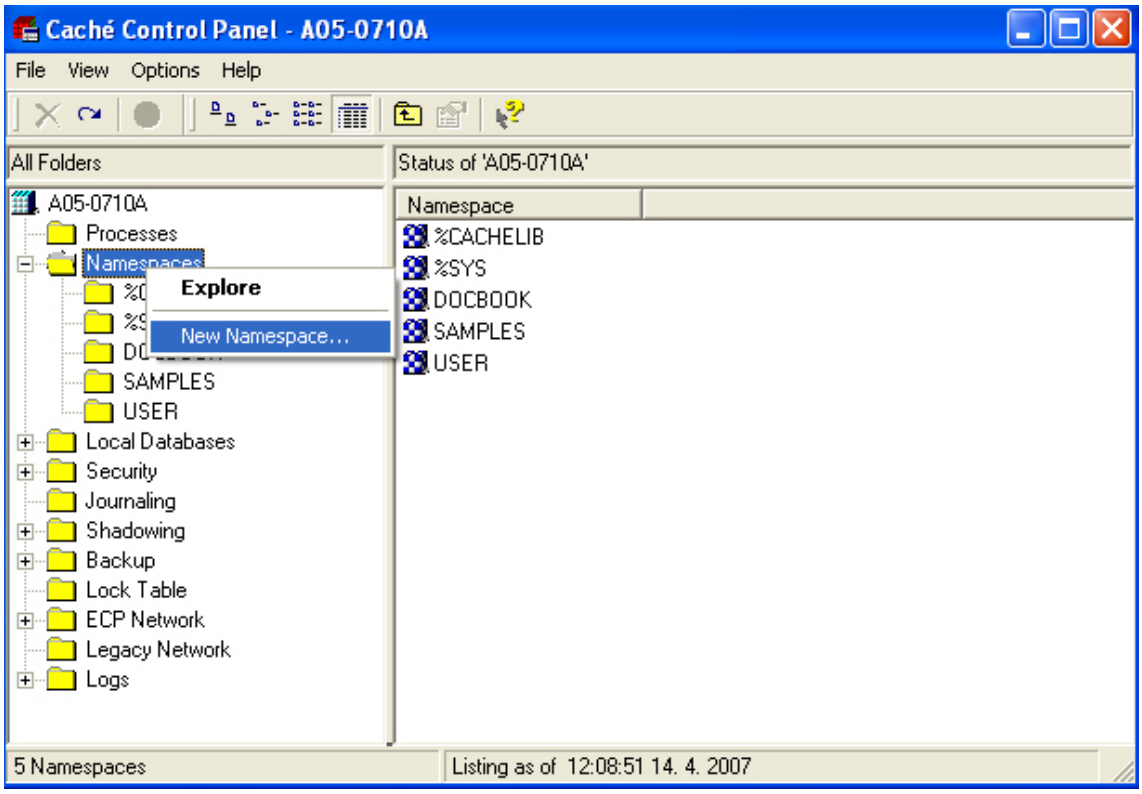
Obr. B.4: Zavedení rutiny "mgwstubs.ro"

B.5 Zavedení rutiny "ZSTU.rsa"

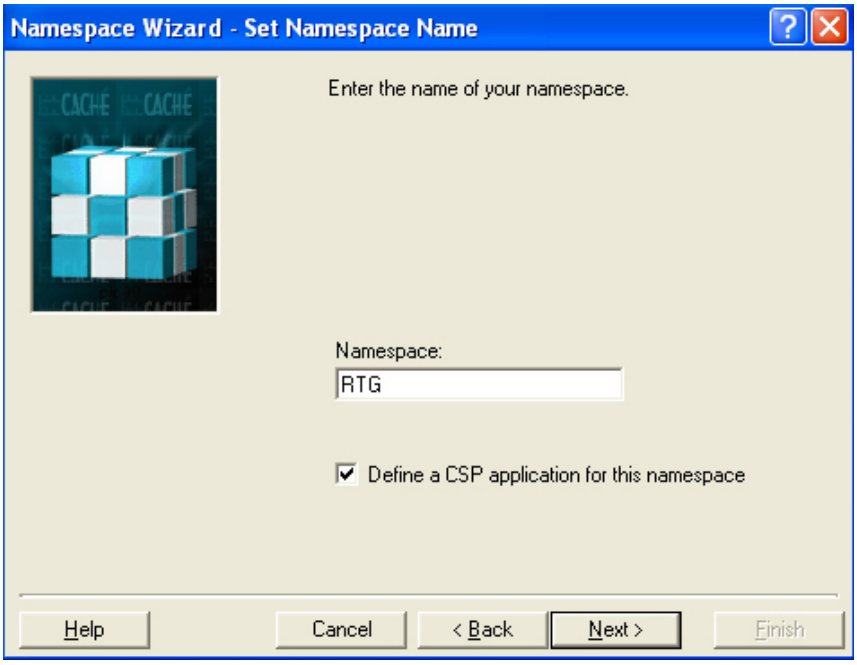
```
USER>ZN "%SYS"

%SYS>d ^%RI

Input routines from Sequential
Device: c:/CacheSys/SMS/ZSTU.rsa   Parameters: "RS"=>

File written by Cache for Windows NT using %RO on May 2 2005  10:53 AM
with extension INT and with description:
Export of 1 routines from namespace %SYS

( All Select Enter List Quit )

Routine Input Option: All Routines

If a selected routine has the same name as one already on file,
shall it replace the one on file? No => Yes
Recompile? Yes => Yes
Display Syntax Errors? Yes => Yes

^ indicates routines which will replace those now on file.
@ indicates routines which have been [re]compiled.
- indicates routines which have not been filed.


ZSTU.INT^@

1 routine processed.
```

Obr. B.5: Zavedení rutiny "zstu.rsa"

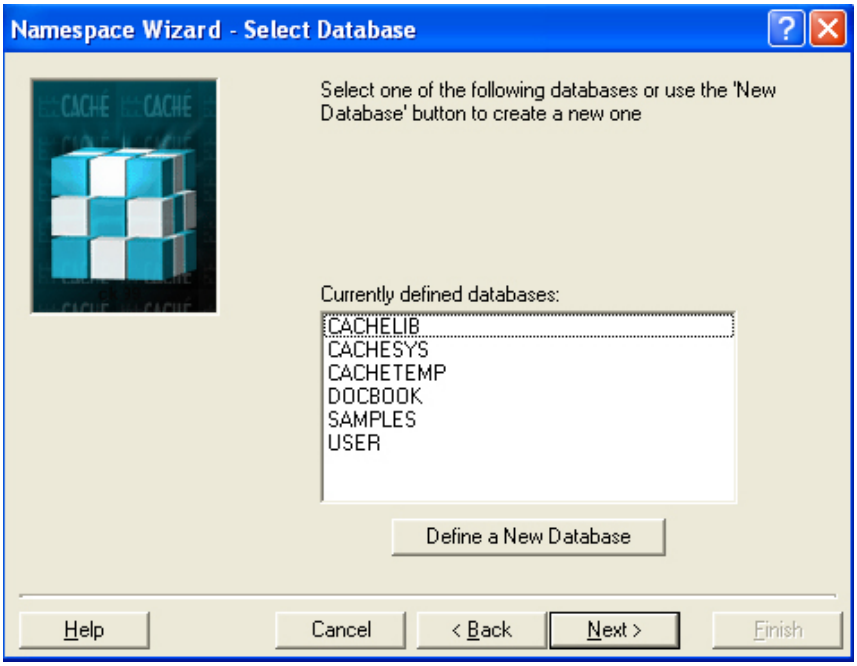
B.6 Zavedení databáze RTG



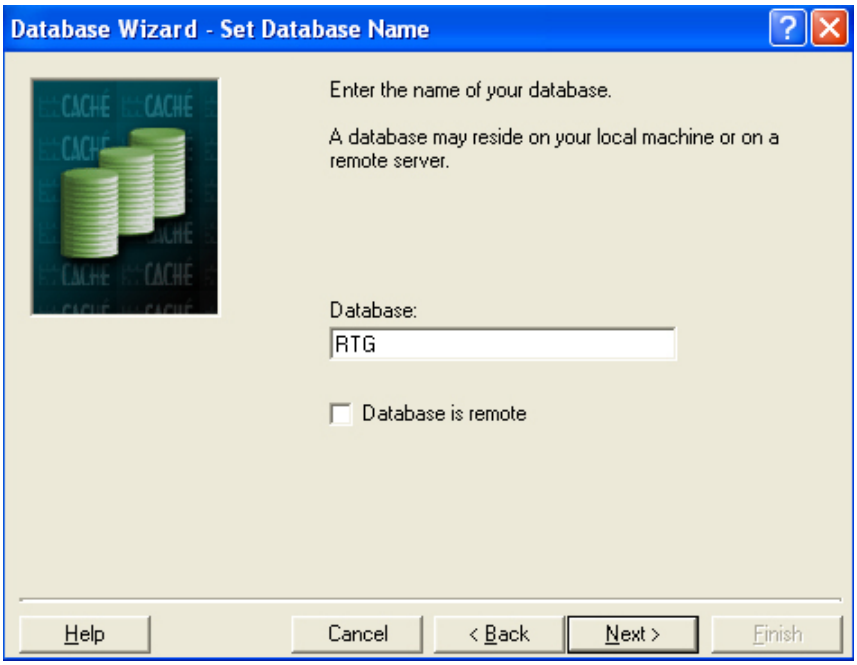
Obr. B.6: Vytvoření nového `"Namespace"`



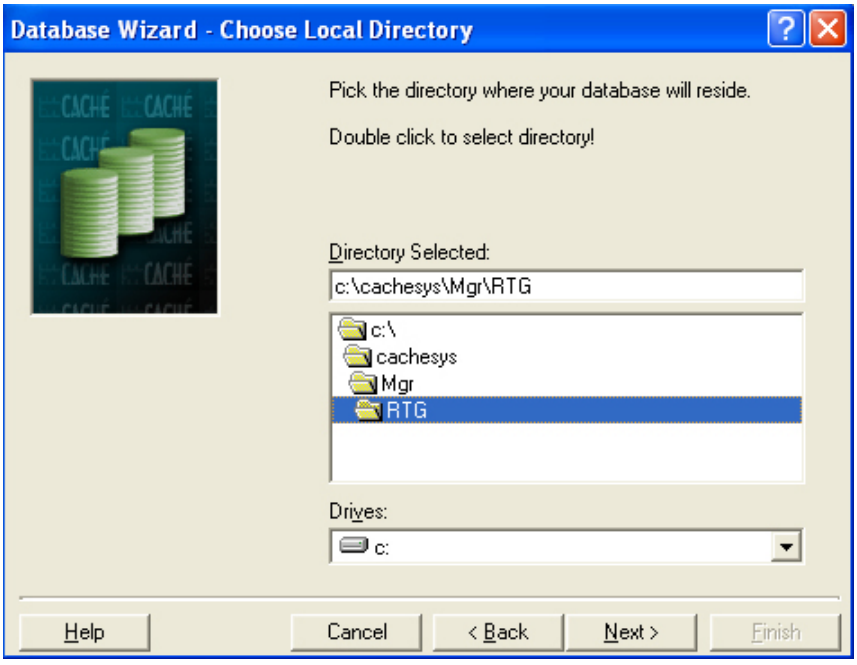
Obr. B.7: Pojmenovaní `"Namespace"`



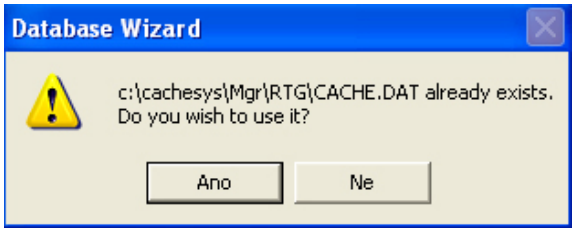
Obr. B.8: Načtení nové databáze



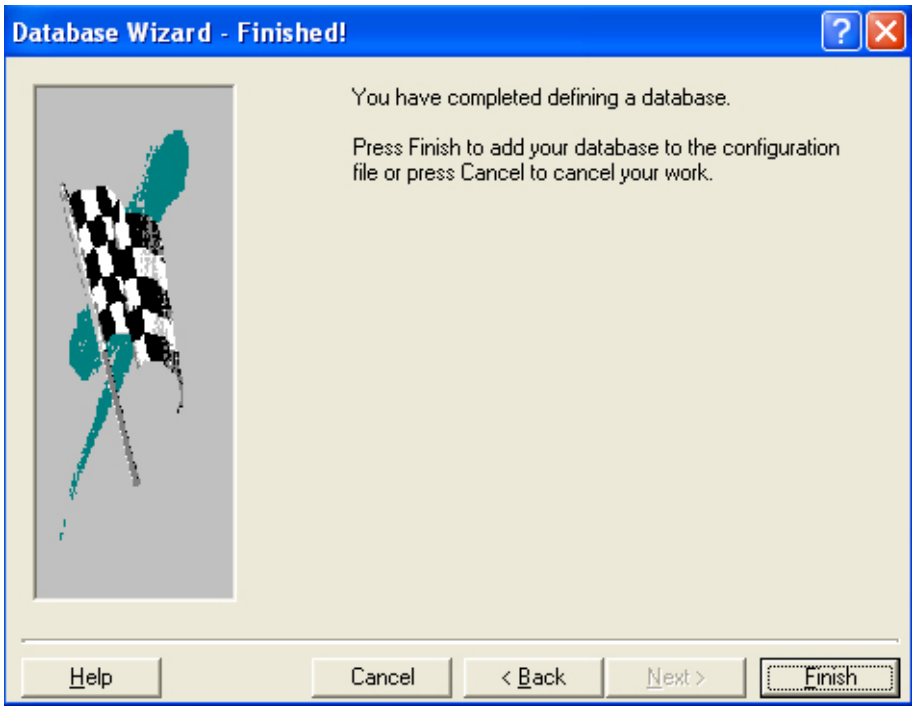
Obr. B.9: Pojmenování nové databáze



Obr. B.10: Lokalizace nové databáze



Obr. B.11: Potvrzení vybrané databáze



Obr. B.12: Přidání databáze do konfiguračního souboru

Obr. B.13: Kompletně vytvořená databáze

C OBSAH PŘILOŽENÉHO CD

- text diplomové práce vysázen v programu LaTeXve formátu *.pdf a *.dvi
- instalační balík `Apache_1.3.37-Mod_SSL_2.8.25-Openssl_0.9.8a-Win32`
- instalační balík `Openssl-0.9.8a-Win32.zip`
- program Caché Weblink
- konfigurační soubor httpd.conf
- soubor openssl.conf
- soubor index.html
- pacientské obrázky použitelné v programu CareCenter (dostupné z [12])