eEHIC ako nositeľ údajov urgentnej medicíny
(čipová karta pacienta)

DIPLOMOVÁ PRÁCA

Pavol Marek 2008

eEHIC ako nositeľ údajov urgentnej medicíny

(čipová karta pacienta)

DIPLOMOVÁ PRÁCA

Pavol Marek

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
KATEDRA INFORMATIKY

Informatika

Vedúci diplomovej práce
Ing. František Soviš, CSc.

BRATISLAVA, 2008

Čestne vyhlasujem, že som diplomovú prácu vypracoval samostatne s použitím literatúry a zdrojov uvedených v závere práce.

Bratislava, máj 2008

.....

Pavol Marek

Ďakujem môjmu diplomovému vedúcemu Ing. Františkovi Sovišovi, CSc. za odborné vedenie práce, za cenné rady a pripomienky. Ďakujem mojej rodine a priateľke za podporu pri písaní tejto práce.

Abstrakt

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
KATEDRA INFORMATIKY

Autor: Pavol Marek
Názov diplomovej práce: eEHIC ako nositeľ údajov urgentnej medicíny
Vedúci diplomovej práce: Ing. František Soviš, CSc.
Rozsah práce: 70 strán s prílohami
Bratislava, máj 2008

Diplomová práca sa zoberá dôležitou súčasťou informatizácie zdravotníctva - problematikou poskytovania údajov urgentnej medicíny (emergency data set - EDS). V tejto práci sa nachádza stručný prehľad vybraných zahraničných systémov poskytujúcich EDS, prehľad aktuálnej situácie v problematike informatizácie zdravotníctva v SR, procesná analýza a návrh základnej štruktúry systému poskytujúceho údaje urgentnej medicíny pre SR. Hlavným prínosom tejto práce je návrh skupín údajov umiestnených na čipe pacientskej karty eEHIC, a analýza vybraných bezpečnostných aspektov tohto návrhu. Práca vychádza z medzinárodných štandardov, z platnej legislatívy a rezortných záväzných dokumentov EÚ i SR.

Kľúčové slová: eHealth, emergency data set, EDS, health professional card, HPC, patient data card, eEHIC, údaje urgentnej medicíny, čipová karta pacienta, informatizácia zdravotníctva, národný zdravotnícky informačný systém

Predhovor

Vďaka výhodám ponúkaných informačnými technológiami vo väčšine vyspelých krajín v súčasnosti prebieha informatizácia zdravotníctva. Jej cieľom je predovšetkým zefektívniť procesy v zdravotníctve tak, aby bola poskytovaná lepšia zdravotná starostlivosť, a aby sa zároveň znížili výdavky na zdravotníctvo. Vhodné využívanie informačných technológií má potenciál napomôcť pri dosahovaní týchto cieľov. Slovenská republika, ako jeden z členov Európskej únie, je zaviazaná k informatizácii slovenského zdravotníctva. Ministerstvo zdravotníctva SR zriadilo Národné centrum zdravotníckych informácií – NCZI, ktoré má pôsobiť ako koncepčný, administratívny a výkonný orgán v danej problematike. Toto centrum je poverené riešiť hlavné úlohy týkajúce sa problematiky eHealth na Slovensku, a tiež pôsobiť aj v roli zadávateľa, prípadne riešiteľa v rámci konkrétnych projektov. Táto diplomová práca bola vypracovaná v spolupráci s organizáciou NCZI. Jej cieľom je analyzovať vybrané zahraničné riešenia problematiky poskytovania údajov urgentnej medicíny a navrhnúť riešenie vhodné pre SR, s ohľadom na platné štandardy, legislatívu, požiadavky na bezpečnosť a interoperabilitu. V tejto diplomovej práci navrhujeme obsah pacientskej čipovej karty a rámcovo analyzujeme vybrané bezpečnostné aspekty tohto návrhu. Ide o návrh základnej štruktúry a o procesnú analýzu danej problematiky. Táto práca má slúžiť ako východisko pri podrobnej analýze a návrhu systému poskytujúceho EDS.

Obsah

1. Úvod

Vo vyspelých krajinách v súčasnosti intenzívne prebieha informatizácia zdravotníctva. Hlavnými dôvodmi informatizácie zdravotníctva sú snahy o umožnenie medzinárodnej spolupráce pri poskytovaní zdravotnej starostlivosti, pri zlepšení zdravotnej starostlivosti a riešení problémov spojených so starnutím populácie. Informatizácia zdravotníctva napomáha k zefektívneniu prebiehajúcich procesov, úsporám v zdravotníctve, efektívnejšiemu nakladaniu so zdrojmi, odstraňovaniu redundantných úkonov, vylúčeniu nežiaducich účinkov súčasne užívaných liekov a pod. Ako najväčší problém informatizácie zdravotníctva (okrem nedostatku financií) sa v súčasnosti javí absencia úplných, konzistentných, zrozumiteľných, a najmä relevantných údajov o stave pacienta. Tie by mali plne charakterizovať aktuálne zdravotné problémy pacienta, ako aj poskytovať informácie o jeho zdravotnej histórii. Dôležitou úlohou informatizácie zdravotníctva je preto vytvorenie systému umožňujúceho rýchle poskytovanie relevantných údajov bezpečným spôsobom.

Snahy o kvalitnú medzinárodnú zdravotnú starostlivosť vedú k neprehľadnosti. Tá je spôsobená najmä odlišnosťou právnych pomerov, odlišnou lokálne zaužívanou praxou, neexistenciou príslušných štandardov, nedodržiavaním existujúcich štandardov (XML, HL7, EDIFACT, OpenEHR, ...), existujúce informačné systémy nespolupracujú, prípadne nevyhovujú bezpečnostným normám a mnoho iných faktorov.

V tejto práci sa budeme zaoberať problematikou sprístupňovania údajov urgentnej medicíny. Sú to základné údaje o pacientovi potrebné pre poskytnutie urgentného ošetrenia v prípade ohrozenia života pacienta. Je potrebné navrhnúť spôsob, akým sa k týmto údajom včas dostane zachraňujúci zdravotnícky pracovník tak na území SR, ako aj v zahraničí. Zároveň, keďže sa jedná o mimoriadne citlivé údaje, je potrebné popísať, akým spôsobom budú tieto údaje chránené pred zneužitím nepovolanou osobou.

Cieľom tejto práce je analyzovať vybrané existujúce zahraničné riešenia problematiky poskytovania EDS a v spolupráci s národným centrom zdravotníckych

informácií ponúknuť rámcový návrh riešenia vhodného pre slovenské podmienky, ako aj analýzu vybraných bezpečnostných aspektov tohto riešenia.

V úvodných kapitolách práce zavádzame potrebné pojmy, a vymedzujeme širší kontext tejto práce.

V kapitole 4 sa zaoberáme vybranými zahraničnými riešeniami systémov poskytujúcich údaje urgentnej medicíny. Z dôvodu obrovského množstva informácií a systémov, ktoré bolo treba preskúmať, sú vybrané len niektoré krajiny EÚ a Taiwan. Keď porovnávame legislatívne podmienky v zahraničí s podmienkami u nás, výhodou je, že Európa má v hrubých rysoch spoločné právne základy, a mnohé problémy týkajúce sa tejto problematiky sa snaží riešiť a koordinovať EÚ na európskej úrovni. Taiwanské riešenie uvádzame, pretože je veľmi podobné nemeckému a rakúskemu. Zároveň si v prvej časti práce všímame naplnenie uvedených požiadaviek danými systémami.

V ďalšej časti uvádzame východiskové dokumenty pre informatizáciu zdravotníctva SR a podrobnejšie sa venujeme stavu informatizácie zdravotníctva na Slovensku.

V kapitole 6 čitateľovi objasňujeme pojem elektronický podpis a uvádzame dôvody pre jeho použitie v systéme poskytujúcom EDS.

V kapitolách 7, 8 a 9 uvádzame návrh riešenia problematiky sprístupňovania údajov urgentnej medicíny pre SR. Uvádzame tu rôzne pohľady na rozsah a množiny údajov uložených na pacientskej čipovej karte, a popisujeme prístup k vybraným bezpečnostným aspektom tohto riešenia.

V kapitole 10 uvádzame výsledný návrh údajov umiestnených na čipe eEHIC a zaoberáme sa zabezpečením dôvernosti týchto údajov. Zároveň v tejto kapitole ponúkame približné odhady pamäťovej náročnosti navrhnutého riešenia, a z toho vyplývajúce technické požiadavky na čip pacientskej čipovej karty.

2. Informatizácia zdravotníctva

Pod informatizáciou zdravotníctva môžeme rozumieť proces prehodnotenia a úpravy procesov prebiehajúcich v zdravotníctve, a ich následnú optimalizáciu založenú na výhodách používania IKT technológií. Žiaľ, v praxi to často funguje tak, že informačné technológie sa využívajú na podporu tradičných procesov. Ako synonymum informatizácie zdravotníctva sa používa aj termín eHealth. Najvýznamnejšie dôvody pre ktoré je potrebné zaoberať sa informatizáciou zdravotníctva sú: pokrok v medicíne zdokonalil zdravotnú starostlivosť, čo má za následok vyššiu priemernú dĺžku života obyvateľstva. To spôsobuje značné zvyšovanie finančného zaťaženia zdravotníctva. Druhým dôvodom je celková zložitosť zdravotníckeho systému umožňujúca duplicitu vyšetrení a prípadnú chybovosť. Ďalším dôvodom je rýchly pokrok v medicíne spôsobujúci rýchle zastarávanie vedomostí zdravotníckych pracovníkov. Podrobnejšie sú tieto dôvody rozpracované napr. v štúdiách [1] a [2], ktorých záverom je, že informatizácia zdravotníctva má potenciál tieto problémy riešiť.

eHealth je jednou z desiatich priorít akčného plánu e - Europe, predstaveného Európskou komisiou v máji 2000. Plán zdôrazňuje strategický význam informačných technológií v správe verejného zdravotníctva „pre blaho občanov ako spotrebiteľov zdravotníckych služieb i informácií o zdraví.“ V apríli 2004 bol zverejnený Akčný plán pre eHealth [3]. Aby mohla čeliť problému starnutia svojej populácie, Európa podľa Komisie potrebuje „nový model poskytovania zdravotnej starostlivosti, založený na preventívne a individuálne zameraných systémoch zdravotníctva, čo je možné dosiahnuť iba prostredníctvom správneho využitia IKT.“ Oddelenie Komisie pre Informačné a komunikačné technológie pre zdravie prijalo v júni 2006 novú stratégiu [4] na podporu transformácie európskeho zdravotníctva v súlade s novým politickým rámcom Komisie i2010. Na obdobie do roku 2010 sú pre členské štáty v týchto dokumentoch zakotvené nasledovné ciele:

- Poskytovanie bezpečnej a efektívnej zdravotnej starostlivosti
- Zvyšovanie znalostí občanov o ochrane zdravia a pomoci pri riešení zdravotných problémov prostredníctvom internetu

- Podporovanie cezhraničnej mobility pacientov prostredníctvom elektronického zdravotného záznamu, elektronických zdravotných kariet
- Zlepšenie prístupu k zdravotnej starostlivosti pre znevýhodnených občanov a pre občanov žijúcich v izolovaných oblastiach
- Rozvoj európskeho trhu eHealth (legislatíva, štandardy, bezpečnosť)

Dokumenty EÚ stanovujú dlhodobé stratégie efektívneho rozvoja zdravotníctva a poskytovania zdravotnej starostlivosti. Jedným z cieľov EÚ v oblasti eHealth je podporovanie cezhraničnej mobility pacientov prostredníctvom elektronického zdravotného záznamu, elektronických zdravotných kariet.

Európsky projekt LSP (Large Scale Pilot), do ktorého je zapojených 12 členských krajín EÚ vrátane Slovenska, si kladie za cieľ špecifikovať, implementovať a overiť použiteľnosť myšlienky prepojenia zdravotníckych systémov s cieľom zdieľania pacientskych údajov a elektronickej preskripcie liekov. Základným cieľom projektu je zabezpečenie interoperability v poskytovaní zdravotníckych služieb medzi jednotlivými členskými krajinami EÚ, a to na úrovni organizačnej (identifikácia a autorizácia pacienta aj lekára), sémantickej (spoločné koncepty preložiteľné do jazykov zúčastnených krajín) a technickej (infraštruktúra a ochrana bezpečnosti a spoľahlivosti údajov). Očakávaným výsledkom trojročného pilotného projektu je vytvorenie a overenie nadstavby nad fungujúcimi zdravotníckymi informačnými systémami v jednotlivých členských krajinách EÚ tak, aby bola možná ich cezhraničná súčinnosť pri zabezpečovaní kontinuálnej zdravotníckej starostlivosti.

Z pohľadu pacienta to znamená, že ak musí vyhľadať lekára počas pobytu v ktorejkoľvek zo zapojených členských krajín, lekár aj pri prvom kontakte s pacientom bude mať k dispozícii potrebné informácie o jeho zdravotnom stave (v zodpovedajúcom rozsahu) a liekoch, ktoré užíva. Na základe toho bude mať možnosť poskytnúť pacientovi plnohodnotnú zdravotnú starostlivosť, ktorej záznam sa stane súčasťou pacientovho chorobopisu, rovnako ako záznamy vyšetrení urobených jeho domovským lekárom.

Súčasťou projektu je vymedzenie 3 základných skupín údajov o pacientovi:

- **Emergency data set EDS** (Množina údajov pre urgentnú medicínu) – základné údaje o pacientovi potrebné pre poskytnutie urgentného ošetrenia
- **Patient summary PS** (Pacientsky sumár) – rozšírená množina údajov o pacientovi potrebná pre poskytnutie plnohodnotnej zdravotnej starostlivosti
- **e-Medication eM** (Elektronická medikácia) – zoznam liekov, ktoré pacient aktuálne užíva spolu s uvedením ich účinnej látky klasifikovanej na základe medzinárodného štandardu .

Pod pojmom **elektronický zdravotný záznam** (EHR = electronic health record) rozumieme množinu obsahujúcu Emergency data set, Patient summary a e-Medication jedného pacienta.

Medzi ďalšie kľúčové programy eHealth patria telemedicína, epreskripcia a vzdelávacie portály.

K dokumentom EÚ sa hlási aj Slovenská republika. Východiskové rezortné dokumenty na realizáciu informatizácie zdravotníctva SR sú Koncepcia informatizácie zdravotníctva na roky 2007-2010 a Akčný plán informatizácie zdravotníctva. Hlavné ciele ukotvené v týchto dokumentoch sú dosiahnutie vzájomného zdieľania relevantných informácií bezpečným a spoľahlivým spôsobom, podpora tvorby a aktualizácie zdravotných záznamov s možnosťou vyvodiť z nich súhrn najvýznamnejších zdravotných údajov (MPS), údaje pre urgentnú medicínu (EDS), uchovávanie a aktualizácia predpísaných a užívaných liekov.

3. Údaje urgentnej medicíny

Jednou z najdôležitejších súčastí EHR je množina údajov urgentnej medicíny emergency data set (EDS). Je to vlastne množina zdravotných údajov o pacientovi, potrebná pre bezpečné poskytovanie neodkladnej, resp. urgentnej zdravotnej starostlivosti. Významným cieľom dobrého EHR systému by malo byť riadené, bezpečné súkromie pacienta chrániace dištančné sprístupňovanie EDS na mieste a v čase, keď je to potrebné. V tejto časti uvádzame stručný prehľad problémov spojených s realizáciou systému poskytujúceho EDS.

Prvým a veľmi dôležitým problémom je, že v súčasnosti neexistuje jednoznačná definícia presne určujúca údaje, ktoré do EDS patria a ktoré nie. V každom systéme, ktorý sa zaoberá poskytovaním EDS, do tejto množiny patria rôzne údaje. Toto je skôr problém týkajúci sa poskytovateľov zdravotnej starostlivosti, preto sa v našej práci nebudeme príliš zaoberať otázkou, čo presne by v tejto množine malo alebo nemalo byť.

Ďalším problémom je, komu a za akých okolností tieto údaje budú sprístupnené. Kto bude ich vlastníkom a akým spôsobom budú aktualizované. Jedná sa o mimoriadne citlivé osobné údaje, a preto je zrejmé, že musí existovať presne definovaná politika ich sprístupňovania. To znamená, že musia v rámci systému existovať rôzne roly, a musia k nim byť priradené zodpovedajúce prístupové práva. V súčasnosti ale neexistuje jednotný predpis alebo štandard, ktorý by túto politiku určoval. Túto politiku v SR momentálne upravuje najmä Zákon č.428/2002 Z.z. o ochrane osobných údajov, avšak ani ten ju nedefinuje úplne. S politikou sprístupňovania údajov úzko súvisí aj bezpečnostná politika. Treba definovať, kde budú údaje EDS uložené a ako budú zabezpečené, aby boli splnené bezpečnostné požiadavky (spoľahlivosť, dostupnosť, integrita).

Veľmi dôležitou požiadavkou je interoperabilita systémov poskytujúcich EDS. Práve spolupráca rôznych systémov EDS je momentálne centrom záujmu európskych inštitúcií. Je potrebné, aby prebehla terminologická a významová štandardizácia, aby vôbec bola možná spolupráca takýchto systémov. Je potrebné určiť vhodné štandardy určujúce formát dát tak, aby bola možná ich efektívna výmena medzi jednotlivými systémami. Zároveň sa musia dodržať dané sprístupňovacie a bezpečnostné politiky.

Významnou bezpečnostnou požiadavkou na systémy poskytujúce EDS je ich vysoká dostupnosť. To predpokladá dostatočnú technologickú infraštruktúru (hardvérovú, softvérovú ako aj dostatočnú kapacitu prenosových liniek).

Integrita údajov je ďalšou významnou bezpečnostnou požiadavkou. Systém musí zabezpečiť údaje o zdravotnom stave pacientov pred ich neautorizovanou zmenou, pretože takáto zmena môže ohroziť život pacienta. Stačí si predstaviť situáciu, že útočník zmení v pacientovom zázname jeho krvnú skupinu z A+ na B+. Čo sa stane, keď dostane transfúziu na základe svojej množiny EDS je zrejmé.

Autentickosť údajov je ďalším problémom, ktorý je potrebné riešiť. Systém poskytujúci EDS je kvôli dostupnosti v urgentnej situácii otvorený aj pre osoby, ktorých identitu nie je možné fyzicky overiť. Na druhej strane sprístupnenie týchto údajov môže potenciálne viesť k ich úniku a možnému zneužitiu, prípadne k zmene týchto údajov, ktoré môžu následne spôsobiť nesprávne medicínske zásahy. Tento rozpor medzi dostupnosťou a autenticitou si bude vyžadovať certifikáciu potenciálne oprávnených osôb (napr. vydanie digitálnych certifikátov potvrdzujúcich identitu osoby a jej kompetenciu na vykonanie istých zdravotných úkonov) a mechanizmus umožňujúci prístup k pacientovmu EDS bez ohľadu na to, či je pacient pri vedomí alebo nie.

Fyzická realizácia systému musí naplniť všetky uvedené požiadavky. Tu sa uvažuje, kde budú dáta uložené, na akej platforme sa projekt naprogramuje, ako budú dáta posielané. V ideálnom prípade by mala realizácia tohto systému umožňovať jeho rozširovanie v rámci rôznych služieb eHealth. Musí poskytovať vhodné rozhranie pre komunikáciu s inými systémami, ako aj rôzne kontrolné mechanizmy. Systém by mal byť používateľsky príjemný a prehľadný, musí prácu lekárom uľahčiť, nie zbytočne skomplikovať. Inak ho lekári nebudú používať.

4. Existujúce zahraničné riešenia

V tejto časti sa venujeme zahraničným systémom rýchlej zdravotnej starostlivosti. Najpodrobnejšie systému IZIP, ktorý funguje v ČR, keďže naše krajiny majú spoločnú históriu. Český i slovenský právny systém a podmienky v zdravotníctve vyšli z jedného základu, a preto sú práve české našim najbližšie. Systém IZIP dosiahol viacero ocenení a bol vyhlásený za najlepší e-Content projekt na svete v kategórii e-Health za rok 2005, čo naznačuje, že v tejto kapitole ho nesmieme prehliadnuť. Analytik spoločnosti Empirica Alexander Dobrev o IZIP-e povedal: *„IZIP je jednoznačne predlohou dobrého projektu pre ostatné národné zdravotné systémy. S výnimkou dánskeho národného systému je z globálneho pohľadu väčšina zemí len vo fáze plánovania alebo zavádzania podobných projektov. Česká republika dokázala s významne nižšími nákladmi a behom niekoľko málo rokov vybudovať systém, ktorý je schopný veľmi skoro pokryť všetkých obyvateľov a poskytovateľov zdravotnej starostlivosti. Vynaložené náklady sú nepatrné v porovnaní s nákladmi, aké sa diskutujú, alebo aké sú už odsúhlasené v krajinách, ako sú Austrália, Kanada, Nemecko alebo Anglicko, a ktoré sa pohybujú medzi jednou až niekoľko miliardami Euro.“*

Ďalšími systémami opísanými v tejto práci sú nemecký, rakúsky, dánsky a taiwanský.

4.1. Česká republika – systém IZIP

Systém internetovej zdravotnej knižky firmy IZIP, a.s., funguje v Čechách od februára 2002 a ku dňu 14.1. 2008 mal 1 020 213 registrovaných používateľov a 9 021 zdravotníckych pracovníkov. Registrácia poistencov VZP je zdarma a je pomerne jednoduchá. Stačí si vytlačiť vyplnený formulár a podpísaný ho poslať poštou alebo elektronicky podpísaný elektronickým podpisom. Ostatné poisťovne so spoločnosťou IZIP zatiaľ rokujú. IZIP ohlásil že od tohto roku umožní registráciu aj samoplatcom. Následne získa registrovaný prístupový kód, ktorý príde doporučene, a ktorý pozná iba on. Okrem toho si pri aktivácii môže zvoliť aj osobné heslo. Zdravotné knižky na internete sú zabezpečené omnoho lepšie než bežná kartotéka v ordinácii. Všetky informácie sú umiestnené na zabezpečených, vysoko dostupných serveroch, ktoré sú pod neustálym dohľadom. Spoločnosť IZIP, a. s., je držiteľom certifikátu o zhode systému manažmentu bezpečnosti informácií (Information Security Management System – ISMS) s normou ISO/IEC 27001:2005. Takisto je držiteľom značky Good Privacy. Značku v Českej republike udeľuje Sdružení pro certifikaci systémů jakosti (CQS), ktoré je členom medzinárodnej siete IQNet.

Spoločnosť IZIP, a. s., získala súhlas Úradu pre ochranu osobných údajov. S touto inštitúciou zároveň priebežne konzultuje technické i právne otázky. Systém IZIP je v súlade s platnými zákonmi Českej republiky, najmä:

- Zákonom č. 101/2000 Sb., o ochrane osobných údajov
- Zákonom č. 20/1966 Sb., o starostlivosti o zdravie ľudu v platnom znení
- Zákonom č. 258/2000 Sb., o ochrane verejného zdravia
- Zákonom č. 285/2002 Sb., o darovaní, odberoch a transplantáciách tkanív a orgánov
- Vyhláškou č. 552 o poskytovaní osobných a ďalších údajov do NZIS pre potreby vedenia národných zdravotných registrov
- novelou Zákona o starosti o zdravie ľudu z dňa 21.3.2007, ktorá dáva pacientom právo nahliadať do svojej zdravotnej dokumentácie a robiť z nej kópie.

Systém IZIP umožňuje pacientom nazerať do vlastnej zdravotnej dokumentácie, a takisto pripisovať podrobnosti do špeciálnej kolónky. Po dohode

s lekárom, resp. zdravotným pracovníkom mu pacient môže umožniť nazeranie do jeho knižky, a tak má lekár k dispozícii kompletnú zdravotnú dokumentáciu. Výhodami tohto systému sú najmä: vyššia informovanosť, zlepšenie a sprehľadnenie komunikácie medzi pacientom a lekárom i medzi lekármi navzájom, zrýchlenie stanovenia diagnózy a eliminácia prípadných chýb, predchádzanie opakovaných vyšetrení, dávkovanie podobných liekov a nezanedbateľnou výhodou je aj následná úspora vo verejnom zdravotníctve.

4.1.1. Emergentné informácie

IZIP pracuje s emergentnými informáciami, kam patria alergie, krvná skupina, rizikové faktory, očkovanie proti tetanu, liečba za posledné 3 mesiace, diagnózy za posledné 3 mesiace. Tieto informácie sa zobrazujú v úvodnej hlavičke karty pacienta (vidí ich klient a lekár, ktorý má právo ich čítať, v núdzovom prípade pracovník záchrannej služby). Krvná skupina a dátum posledného očkovania proti tetanu sa vyskytuje len raz a novšie zápisy prepisujú staršie (podobne ako anamnéza). Alergie, rizikové faktory a trvalá liečba sa do elektronických zdravotných knižiek zapisuje ako každé iné zápisy.

4.1.2. Emergentné prístupy

V prípade, keď osobné údaje klienta IZIP v jeho elektronickej zdravotnej knižke môžu byť využiteľné na ochranu života alebo zdravia pacienta a ten sa nachádza v takom stave, že nie je schopný komunikovať svoje prístupové heslo, lekár záchrannej služby pomocou núdzového prístupového hesla na základe klientovho súhlasu v prihláške vstúpi do pacientovej dokumentácie. Prístup do zdravotnej dokumentácie pacienta v ohrození života prebieha nasledovne:

1. Centrálny dispečing zdravotnej záchrannej služby príjme telefonát so žiadosťou o rýchlu záchrannú pomoc.
2. Pracovník dispečingu si vyžiada základné údaje pacienta (adresa, meno, priezvisko, rodné číslo). Z dôvodu nedostatku informácií sa nám nepodarilo zistiť, čo sa deje v prípade, že sa nedajú zistiť pacientove údaje alebo sa dajú získať len čiastočne.
3. Zhodnotí, ktorá posádka je najbližšie a vyšle ju na dané miesto.

4. Na základe pacientových osobných údajov (meno a rodné číslo, alebo meno a adresa) zisťuje, či má pacient zriadenú zdravotnú knižku.
5. Ak áno, nasleduje autorizácia pracovníka zdravotnej záchrannej služby do systému IZIP (tú popisujeme v nasledujúcom odseku), čím sa mu umožňuje prístup práve k EDS pacienta.
6. Pomocou vysielačky povie zistené relevantné údaje lekárovi, ktorý smeruje k pacientovi.

Následne sú všetky údaje o zdravotnom stave pacienta v núdzovej situácii uložené v informačnom systéme zdravotnej záchrannej služby, odkiaľ sa automaticky posielajú do pacientovej internetovej zdravotnej knižky. Na príjme v nemocnici teda prijímajúci lekár vie o stave pacienta, poskytnutej prednemocničnej starostlivosti (aké lieky pacient už dostal, ...), prípadnom návrhu na hospitalizáciu, a tak sa môže vyhnúť opakovanému vyšetrovaniu a prípadným pochybnostiam o zásahu vykonanom zdravotnou záchrannou službou.

4.1.3. Autorizácia pracovníka záchrannej služby

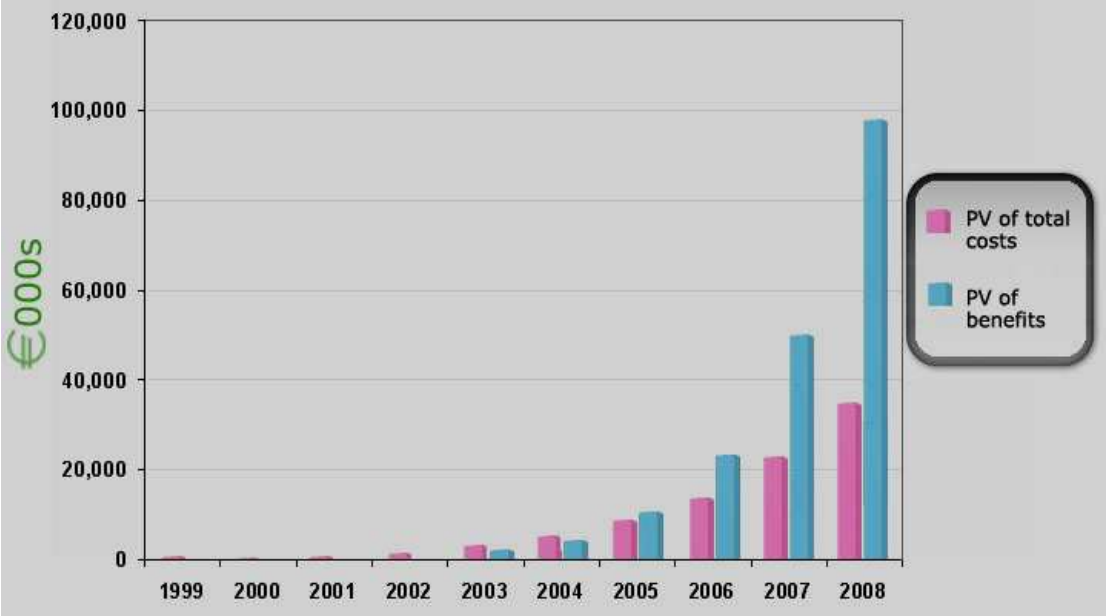
Popis práce pracovníka dispečingu zdravotnej záchrannej služby (ZZS) krok za krokom:

1. Registrácia do programu ZZS
2. Prijatie výzvy na zásah ZZS
3. Určenie zasahujúcej posádky
4. Vloženie čipovej karty do čítačky (každý operátor má svoju vlastnú kartu s jeho biometrickým údajom, pri opustení pracoviska je povinný vybrať kartu z čítačky)
5. Výzva k zosnímaniu odtlačku prsta (prístup operátora sa povolí na základe zhody odtlačku a vzoru uloženého na čipovej karte)
6. Registrácia do systému IZIP (Systém umožňuje prístup k emergentným údajom len v súvislosti s telefonátom. Vstup operátora sa systémom zaznamenáva a dotyčný pacient je o vstupe do jeho karty dodatočne informovaný).
7. Zadanie vyhľadávacích kritérií
8. Otvorenie emergentnej karty pacienta

9. Odovzdanie relevantnej informácie ZZS (vďaka informáciám sa zasahujúci lekár môže pripraviť, napr. ak vie, že ide o diabetika, človeka s kardiovaskulárnym ochorením, astmatika a pod.)

4.1.4. Ekonomický dopad systému IZIP

Správu o ekonomickom dopade podáva spoločnosť Empirica. Podľa výsledkov štúdie prvým rokom, keď hrubý zisk prekročil náklady bol 2005, teda 7 rokov od začatia plánovania projektu. Kumulovaný hrubý ročný zisk prekročil kumulované náklady v roku 2006. Tieto údaje sú zobrazené na obrázku č.1.

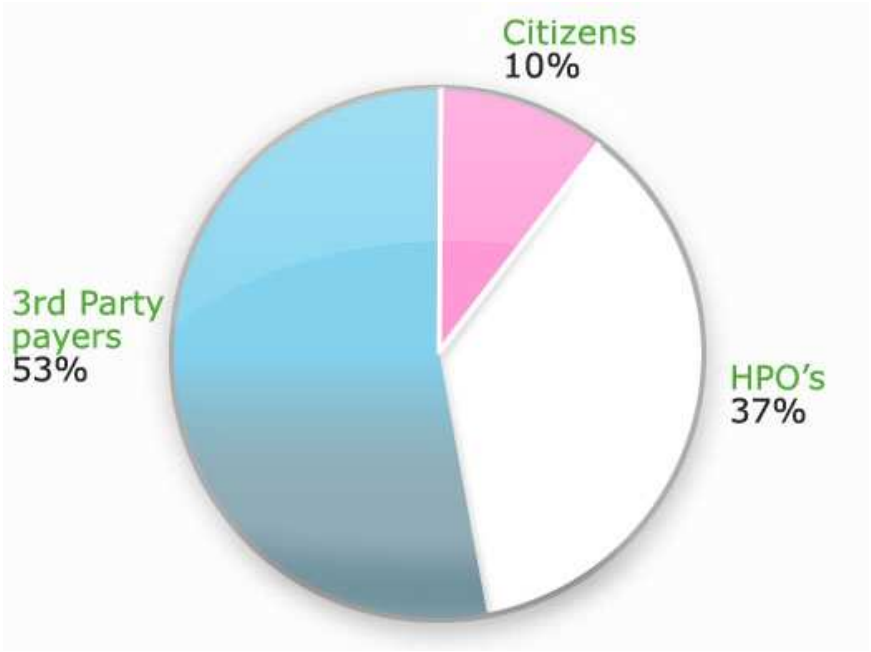


obr. č.1.

Porovnanie nákladov a zisku systému IZIP

zdroj: www.izip.cz

Odhadovaný produkovaný zisk je 74 %. Odhadované rozdelenie zisku v roku 2008 znázorňuje obrázok č.2. Zisk je rozdelený medzi poisťovne, poskytovateľov zdravotnej starostlivosti a obyvateľov.

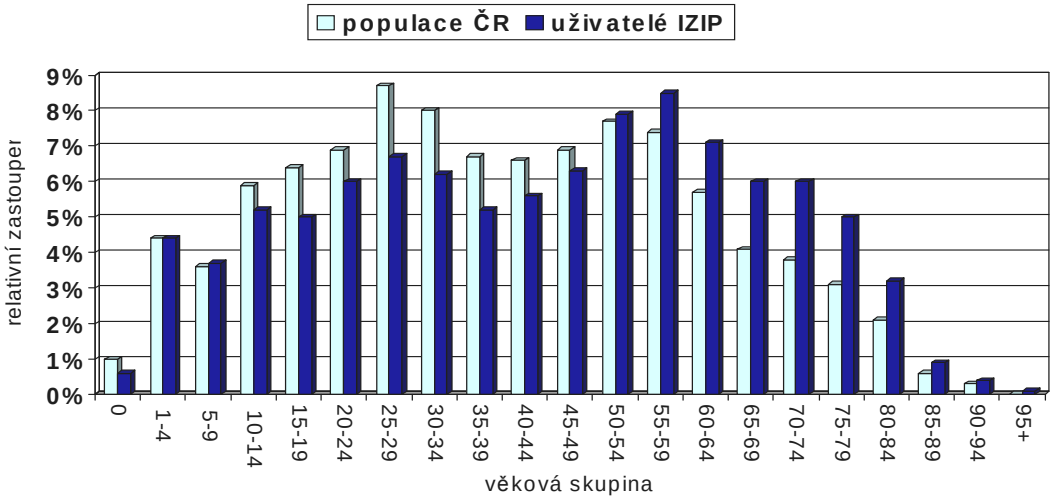


obr. č.2.

ozdelenie zisku

zdroj: www.izip.cz

Užívatelia systému IZIP sú zastúpení rovnomerne zo všetkých vekových skupín. Najvyššie relatívne zastúpenie majú občania vo veku viac ako 50 rokov. To zodpovedá zámeru elektronickej zdravotnej knižky – zamerať sa hlavne na časť populácie, ktorá trpí častejšími ochoreniami. Rozdelenie obyvateľov znázorňuje obrázok č. 3.



obr. č.3.

Relatívne zastúpenie občanov registrovaných v IZIPe

zdroj: www.izip.cz

4.1.5. Bezpečnosť

Zdravotná knižka je výhradne majetkom pacienta. Ak nechce aby tam boli zaznamenané chúlostivé údaje, nemusí to povoliť. Len pacient rozhoduje komu sprístupní svoju zdravotnú dokumentáciu. Ak lekárovi neumožní čítanie, lekár môže jedine zapísať výsledky vyšetrenia. Jedinou výnimkou je emergentný prípad popísaný vyššie.

Ako identifikačné číslo sa so súhlasom pacienta používa jeho rodné číslo. Prístupový kód generuje program náhodne, žiadny z pracovníkov IZIP nemá možnosť ho zistiť. Kód sa vytlačí a zabalí do zvláštnej obálky, ktorá je následne zaslaná klientovi doporučene. Klient má kedykoľvek možnosť požiadať o zmenu kódu. Okrem prístupového kódu má každý klient možnosť sám si vytvoriť ešte druhé, tzv. osobné heslo. Bez prístupového kódu a osobného hesla nie je možné dostať sa k zdravotným informáciám konkrétneho klienta, okrem emergentných prípadov. Po troch neúspešných pokusoch o prihlásenie sa prístup do systému automaticky zablokuje. Vďaka tomuto princípu je tak v podstate jediným možným zlyhaním prezradenie oboch hesiel priamo používateľom. Klientom sú umožnené i ďalšie spôsoby zabezpečenia vstupu do systému, a to pomocou SMS hesla, elektronického prístupového certifikátu, prípadne kombináciou všetkých uvedených spôsobov.

S databázou systému IZIP pracujú administrátori, ktorí pracujú v oddelenom poschodí s elektronicky zaisteným vstupom. Jedná sa o oprávnené a špeciálne vyškolené osoby.

Keď sa užívateľ, či už pacient alebo lekár, pokúša komunikovať so serverom systému IZIP, prebieha kontrola, či je daný užívateľ registrovaný. Túto službu zabezpečuje IZICHECK. Len registrovaný používateľ môže komunikovať so serverom, čo znižuje jeho vyťaženosť a slúži ako bezpečnostné opatrenie.

Údaje pri prechode medzi zdravotným informačným systémom a systémom IZIP vstupujú cez IZIGATE, aplikáciu kontrolujúcu formálnu štruktúru posielaných dát. Tá musí súhlasiť s dátovým štandardom MZ ČR - DS3. Je to komunikačný modul vo forme knižníc DLL alebo spustiteľných súborov pre Windows a Linux.

Komunikačné rozhranie systému IZIP je založené na využívaní SSL 3.0, 128 b šifrovania a serverového certifikátu. Štandardom pre štruktúrovanie dát je XML a DASTA DS3. Tvoria ho dve brány, IZICHECK (overuje existenciu zdravotnej knižky klienta) a IZIGATE (prijíma zápisy do zdravotnej knižky). Využívanie štandardu DASTA má nespornú výhodu v uľahčení komunikácie medzi systémom IZIP a inými zdravotnými informačnými systémami.

4.1.6. Ďalšie účely IZIP

Účelom systému je potom spracovanie zhromaždených údajov, a to pre účely štatistické, vedecké alebo pre účely riadenia zdravotníctva a zdravotníckych zariadení. Spracovanie údajov pre tieto účely je zásadne anonymizované a prebieha na základe klientovho súhlasu s prevádzkovým poriadkom.

4.1.7. Rada systému

Poradný orgán vedenia IZIP zabezpečujúci transparentnosť systému sa nazýva rada systému a je zložená zo zástupcov:

- Ministerstva zdravotníctva
- Ministerstva pre informatiku
- VZP
- Parlamentnej Komisie pre sociálnu politiku a zdravotníctvo

- Odbornej organizácie lekárov a lekárnikov
- Organizácie pacientov
- 1. lekárskej fakulty UK
- Partnerov systému

4.1.8. Zápis a čítanie zdravotnej knižky

Zapisovať môžu všetci poskytovatelia zdravotnej starostlivosti, ktorí sú registrovaní v systéme IZIP. Každý takýto zápis je jasne a jednoznačne identifikovaný, je vždy označený dátumom a časom, menom lekára, jeho odbornosťou a miestom, kde bol záznam spravený. Väčšina lekárskych softvérov v Čechách vytvára zápis do IZIP-u automaticky, čo lekárovi značne šetrí čas a námahu. Pacient užívané voľne predajné lieky (vitamíny, rôzne potravinové doplnky apod.), zapisuje výhradne do sekcie poznámky klienta. Tam sa taktiež zapisuje správa od ošetrujúceho lekára, ktorý ešte nie je zapojený do systému IZIP.

Čítať môžu v núdzovej situácii registrovaní pracovníci záchrannej služby. O každom takomto vstupe systém vytvára záznam a automaticky informuje pacienta. Za bežných okolností môže vlastnú dokumentáciu čítať pacient – majiteľ svojho záznamu. Poskytovatelia zdravotnej starostlivosti môžu čítať pacientov záznam len so súhlasom pacienta. Pacient má pri registrácii možnosť uviesť dôverného lekára (ošetrujúci lekár), ktorému povolia čítanie kedykoľvek. Ten potom má prístup k pacientovej zdravotnej dokumentácii kedykoľvek na základe vlastnej autorizácie do systému.

4.2. Rakúsko

Jeden z dôležitých krokov reformy bolo prijatie zákona o elektronickom prenose dát v zdravotníctve koncom roka 2004. V Rakúsku bola v roku 2005 celoplošne nasadená čipová zdravotná karta. Používa ju viac ako 8 miliónov zdravotne poistených pacientov, 12 000 poskytovateľov zdravotnej starostlivosti a všetky rakúske zdravotné poisťovne. Na karte je uložené meno a číslo poistky občana na základe ktorých sa elektronicky overuje, či a kde je pacient poistený. Na karte nie sú uložené žiadne zdravotné údaje. Tie sú uložené v centrálnej zdravotnej databáze (Zentrales Gesundheitsinformationsnetz). Lekár vlastní tzv. o-kartu – kartu odborného pracovníka. Do databázy pristupuje na základe kombinácie odbornej a klientovej karty.

Využitie karty:

- Je základom autorizovanej komunikácie medzi poistencami a poskytovateľmi zdravotnej starostlivosti prostredníctvom internetu
- Používa sa ako jediný dostatočne bezpečný prostriedok pre prístup k dátam elektronickej zdravotnej knižky
- Platí na území celého Rakúska a u všetkých zmluvných lekárov
- Slúži na sprístupnenie všetkých služieb dostupných v rakúskom zdravotnom systéme
- Kartu získava už novorodenec, platnosť je časovo ohraničená
- Používa sa zároveň ako občiansky preukaz (je nutná registrácia)
- Zadná strana karty je európskou zdravotnou kartou (EHIC), zaručuje nárok na lekársku pomoc v krajinách EU a EWR (Island, Lichtenštajnsko, Nórsko), ako aj vo Švajčiarsku

Karta je navrhnutá tak, aby bola kompatibilná s existujúcimi i budúcimi eHealth orientovanými projektmi. Jednou z požiadaviek na túto kartu bolo, že musí byť rozšíriteľná o budúce aplikácie. Napr. od februára 2007 beží pilotný projekt s názvom Medication safety belt, ktorý na báze dobrovoľnosti kontroluje interakciu užívaných liekov. Medzi plánovanými projektmi sú:

- Zahrnutie out-patient kliník a nemocníc

- Integrácia poskytovateľov zdravotnej starostlivosti
- Electronické referrals a transfer nálezov
- ePrescripcia a eMedikácia
- EDS
- Využitie pre e-government a eSV-portál
- Manažment ochorení používaním karty na autentifikáciu a identifikáciu

4.3. Nemecko

Od roku 2003 majú nemeckí občania čipovú kartu poistenca. Tá zároveň slúži ako EHIC. Od 1.1.2006 bol obsah karty pozmenený. Hlavné úžitky z používania tejto karty sú: vyššia miera akceptovania zdravotnými poisťovňami, okamžité overenie stavu poistenca, zrýchlenie vyplácania poistiek, zníženie byrokracie, výhoda pre cestujúcich do zahraničia. Na prednej strane karty sú tieto údaje:

- Názov poisťovne
- Meno majiteľa
- Fotografia majiteľa
- Číslo poisťovne
- Číslo poistenca
- Platnosť karty
- Stav poistenca

V elektronickej podobe sú na karte uložené tieto údaje:

- Identifikačné a administratívne údaje
- Údaje súvisiace s ePreskripciou
- Údaje o liečbe
- Bezpečnostné funkcie

V súčasnosti sa uvažuje o nasledovnom kategorizovaní týchto údajov:

- Nemenné údaje (administratívne, emergentné)
- Prenosné údaje (ePreskripicia, odporučenie na odborné vyšetrenie)
- Dynamické údaje (menia sa počas pacientovho života: diagnózy, liečba, zdravotná história), ktorých podoba zatiaľ ostáva neurčená, karta bude buď úložisko pointrov na údaje alebo na karte budú tieto údaje priamo

V súčasnosti prebieha testovanie ďalších možností využitia, a to konkrétne ePreskripcia a EDS.

Čipovú kartu majú v Nemecku aj odborníci. Používa sa na určenie práv na čítanie, zápis údajov do pacientovho záznamu. Takisto sa používa aj na autorizáciu a autentifikáciu prostredníctvom elektronického podpisu. Na čipe je uložené ID odborného pracovníka, prístupové práva a digitálny podpis. Technické detaily o nemeckých čipových kartách sú podrobnejšie uvedené napr. v [8].

4.4. Taiwan

Uvádzame aj taiwanský národný systém, pretože patrí medzi prvé celonárodné systémy používajúce čipovú kartu pre pacientov i pre profesionálov. Jeho realizáciu zabezpečovala tá istá firma ako aj pre Rakúsko a časť Nemecka (firma Giesecke-Devrient), takže sa veľmi podobá na európske riešenia. Čipová karta využíva tieto technológie: Sm@rtCafé® Expert: JAVA™ operačný systém, Hitachi AE 450 32 KB mikroprocesorový čip a na šifrovanie sa používajú šifry 3DES a RSA. Na čipových kartách sú fotografie pacientov i profesionálov. Pacientska karta sa využíva aj ako občiansky preukaz.

Na pacientovej karte sú uložené tieto údaje:

- Administratívne údaje
- Údaje súvisiace s poistením
- Anamnéza (chronické a dlhodobé choroby)
- Emergentné údaje
- ID darcu orgánov
- Očkovacie a tehotenské záznamy
- Údaje pre ePreskripciu
- Časť pre sledovanie ceny liečby

4.5. Dánsko

MEDCOM – dánska národná zdravotná sieť má svoje počiatky už v rokoch 1980, úspešne funguje od roku 1994 a používa EDI – Electronic Data Interchange. Táto národná sieť umožňuje rýchlu výmenu spoľahlivých dát vo formáte EDIFACT, neskôr aj XML. Medzi poskytovateľmi zdravotnej starostlivosti sa pošle mesačne približne 3 milióny dokumentov. Ide najmä o záznam ošetrujúceho lekára pre nemocnicu, predpis pre lekáreň, požiadavka o vykonanie diagnostických testov, výsledky testov, prepúšťacie správy, oznámenia o prepustení určené pre poskytovateľov sociálnej starostlivosti. Ekonomický dopad – už v roku 1997 zisk prekročil náklady, odhadovaný zisk na rok 2008 je cca 80 miliónov eur. Od roku 2003 funguje národný portál sundhed.dk, ktorý predstavuje prístup k dánskemu zdravotnému systému pre obyvateľov i profesionálov.

Každý občan má celoživotné identifikačné číslo pod ktorým sa do centralizovanej databázy ukladajú predpísané lieky, laboratórne nálezy a lekárske správy. Databázu spravuje verejnoprávna organizácia MedCom. Každý lekár a lekárnik má právo na základe elektronického podpisu informácie čítať i vkladať. Pacient môže vlastné údaje sledovať cez internet, a takisto vidí, kto ktoré údaje vkladal. Rýchlosť a transparentnosť systému je veľmi vysoká, ale úroveň ochrany dát naopak veľmi nízka. Systém je založený na dôvere a na tvrdení MedComu, že príliš mnoho bezpečnostných obmedzení nie je nutných.

S použitím elektronického podpisu, ktorý majú občania prostredníctvom MedCom – u zdarma, majú obyvatelia dostupné mnohé služby, napr. objednanie sa u lekára, objednanie liekov, obnovenie receptov, náhľad na zdravotné údaje a komunikáciu s poskytovateľmi zdravotnej starostlivosti. Zároveň im portál poskytuje rôzne všeobecné informácie. Takisto im poskytuje prístup k rôznym odborným príručkám.

4.6. Zhrnutie

Z vyššie uvedeného vidíme, že momentálne v zahraničí existujú viaceré varianty realizácie poskytovania EDS. V tomto odseku uvádzame pre zvýšenú prehľadnosť porovnanie výhod a nevýhod jednotlivých modelov.

Český model - čipovú kartu majú iba lekári záchrannej služby. Ostatní odborní pracovníci a pacienti sa do systému prihlasujú pomocou prideleného a osobného hesla. Systém obsahuje kompletnú pacientovu elektronickú zdravotnú kartu, pričom s pacientovým súhlasom do nej odborník môže nahliadať. V urgentnom prípade má pracovník zdravotnej záchrannej služby možnosť pristupovať k EDS pacienta pomocou núdzového hesla v kombinácii s použitím jeho odbornej čipovej karty a biometrickej identifikácie. Pacient je automaticky informovaný o takomto zásahu a systém ukladá záznam o tejto udalosti.

Výhody tohto systému:

- Lacné riešenie
- Odpadajú problémy spojené s čipovou kartou pacienta (réžia, životnosť, strata, konzistencia dát na čipovej karte a zdravotnej karte, bezpečnosť)
- znížené riziko zneužitia čipovej karty (okrem kariet pracovníkov ZZS vlastne neexistuje)

Nevýhody tohto systému:

- nízka predpokladaná kompatibilita so zahraničnými riešeniami (ako sa zahraničný lekár dostane k EDS pacienta, ako bude aktualizovať pacientovu dokumentáciu)
- manuálne vypisovanie administratívnych údajov
- problém overenia, či je pacient poistený
- systém neumožňuje pacientovi podpísať vykonané vyšetrenia
- nie je vyriešené ako sa identifikuje pacient neschopný zadať svoj PIN ak nechce prezradiť svoje osobné heslo lekárovi

Model využívajúci čipové karty poistencov i profesionálov. Zdravotnícki profesionáli majú čipovú kartu odborného pracovníka, tzv. Health Professional Card

(HPC). Vo väčšine materiálov sa uvádza názov European Professional Card – EPC. Tento názov je používanejší, ale je dosť nevhodne zvolený, keďže nič nevraví o tom, o akých profesionálov ide. Rovnako by si mohli takto vydať a označiť svoju kartu aj IT profesionáli alebo profesionálni ekonómovia. Preto v našej práci budeme používať skratku HPC.

Pacienti majú pacientsku čipovú kartu, tzv. Patient Data Card – PDC. Bezpečnostné pravidlá, ako aj údaje uložené na čipovej karte sa líšia v jednotlivých riešeniach. Prístup k pacientovým údajom získava odborník na základe prístupových práv definovaných na jeho HPC. Uvedené príklady (Nemecko, Rakúsko, Taiwan a Dánsko) demonštrujú, že neexistuje univerzálne riešenie. Pri riešení problematiky EDS je potrebné brať do úvahy miestne legislatívne pomery, rovnako aj pomery v zdravotníctve.

Výhody tohto systému:

- kompatibilita s väčšinou doteraz implementovaných systémov tohto typu
- pacienti i odborníci majú možnosť elektronicky podpisovať jednotlivé úkony
- ďalšie možnosti využitia čipovej karty pacienta (OP, ePreskripcia, využívanie zaručeného elektronického podpisu v úradnom styku)
- zvýšená bezpečnosť
- možnosť definovať prístupové práva profesionála na jeho karte
- administratívne údaje sú k dispozícii v elektronickej podobe

Nevýhody tohto systému:

- drahšie riešenie
- nutnosť zabezpečenia manažmentu životného cyklu karty
- riziko straty alebo poškodenia karty

5. Východiská riešenia v SR

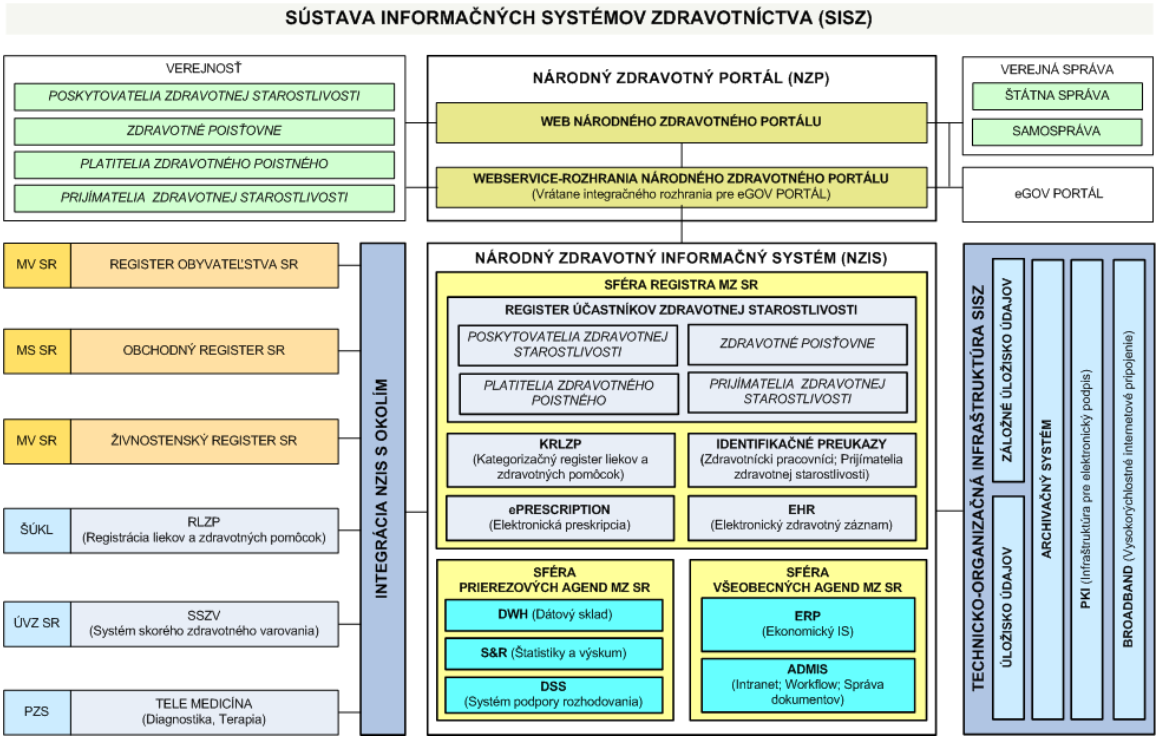
V porovnaní so situáciou v zahraničí, Slovensko sa nachádza v ranom štádiu informatizácie zdravotníctva. Vzhľadom na viaceré faktory (chorobnosť populácie, mobilita obyvateľov v európskom priestore, rozvoj diagnostických a liečebných technológií, demografické ukazovatele) stále rýchlejším tempom rastú požiadavky na poskytované zdravotnícke služby. Zároveň ale zdravotníctvo naráža na limity financovateľnosti. Riešením tohto problému je práve racionalizácia procesov, ktorá by sa mala opierať o efektívne využívanie informačných technológií. Bezpečne a rýchlo poskytnuté relevantné informácie o zdravotnom stave pacientov majú potenciál napomôcť k významnej úspore v zdravotníctve, a najmä k omnoho kvalitnejším službám pre pacienta. Ministerstvo zdravotníctva SR na základe dokumentov EÚ iniciovalo program pod názvom Nové zdravotníctvo, v rámci ktorého sa má venovať pozornosť informatizácii zdravotníctva. Viď [10]. Východiskami pre informatizáciu zdravotníctva na Slovensku sú nasledovné dokumenty:

- Programové vyhlásenie vlády SR (júl 2006)
- Dodatok k národnému programu reforiem SR na roky 2006-2008
- Národná eHealth stratégia 2005
- Výhľadový plán eHealth (road map) 2006
- Akčný plán informatizácie zdravotníctva 2006
- Koncepcia informatizácie zdravotníctva na roky 2007-2010

5.1. Perspektíva eHealth na Slovensku

Kľúčové elementy naznačené v slovenskom Výhľadovom pláne (Road Map) sú základom pre funkčné služby eHealth na Slovensku. Ich štruktúra je názorne zobrazená na obr. č. 4 – ide predovšetkým o:

- Národný zdravotný informačný systém
- Národný zdravotnícky portál pre profesionálov a laikov
- Národná sieť poskytovateľov zdravotnej starostlivosti pre domácu a medzinárodnú súčinnosť (na základe štandardu HL7, v3)
- Občianske a profesionálne elektronické zdravotné/identifikačné karty EHIC a HPC
- Elektronický multimediálny zdravotný záznam (SNOMED-CT nomenklatúra v schvaľovacom procese) smerujúci k optimálnemu využitiu klinických ciest
- Telemedicína a nezávislé žitie
- ePreskripcia/Medikácia smerujúca k použitiu medikačnej histórie pacienta
- Domáce systémy zdravotnej a sociálnej starostlivosti podporované informačnými a komunikačnými technológiami
- Poradenské podporné vedomostné systémy pre praktických, klinických lekárov a manažment
- Vývoj a zavedenie systémov podporujúcich opatrenia na prevenciu ochorení a zlepšujúcich kvalitu údajov a ich ukladanie na podporu verejného zdravia
- Zavedenie systémov na hodnotenie a kontrolu bezpečnosti a kvality klinických postupov
- Certifikácia klinických návodov
- Aplikovanie IKT a medzinárodných zdravotníckych štandardov (napr. CEN TC251, ISO 215, SNOMED, HISA, DICOM atď.)
- Ustanovenie univerzitného vzdelania v zdravotníckej a medicínskej informatike v súlade s odporúčaniami IMIA



obr. č. 4

Sústava informačných systémov zdravotníctva podľa NCZI

zdroj www.nczisk.sk

5.2. Koncepcia informatizácie zdravotníctva SR

K funkčnému Národnému zdravotníckemu informačnému systému (NZIS) vedú podľa Koncepcie nasledovné kroky:

- Zavedenie štandardov pre zdravotnícku informatiku na báze európskych štandardov. Ich prostredníctvom sa vytvoria predpoklady pre interoperabilitu rôznych zdravotníckych informačných systémov v celej EU
- Informatizácia zdravotníckych zariadení a ďalších subjektov v zdravotníctve v súlade s definovanými štandardami
- Definovanie a naplnenie národných zdravotníckych registrov
- Vybudovanie hardvérovej a softvérovej infraštruktúry pre komunikáciu a uchovávanie zdravotníckych informácií

Ministerstvo zdravotníctva SR vo februári 2006 zriadilo Národné centrum zdravotníckych informácií - NCZI. Jeho súčasťou je Centrum pre informatizáciu zdravotníctva, ktoré je poverené riešiť hlavné úlohy týkajúce sa problematiky eHealth na Slovensku. Druhou súčasťou je aj Centrum pre štandardy informačnej sústavy zdravotníctva, ktorého cieľom je zavádzať a uplatňovať štandardy pre informácie v zdravotníctve. Poslaním organizácie NCZI je, okrem iného, pôsobiť ako koncepčný, administratívny a výkonný orgán v danej problematike, a tiež pôsobiť aj v roli zadávateľa, prípadne riešiteľa v rámci konkrétnych projektov. Úlohou NZIS je prepojenie existujúcich systémov poskytovateľov zdravotnej starostlivosti, zber, spracovávanie a poskytovanie relevantných zdravotných údajov na národnej úrovni, ako aj zabezpečenie výmeny zdravotníckych informácií so zahraničím. NZIS je charakterizovaný rozsahom, použitou architektúrou, štandardmi zabezpečujúcimi integráciu a spôsobom jednoznačnej identifikácie poskytovateľa i prijímateľa zdravotnej starostlivosti.

5.2.1. Rozsah NZIS

V súčasnosti organizácia NCZI predpokladá v systéme NZIS integráciu nasledovných okruhov:

- Bezpečná elektronická komunikácia
- Elektronická preskripcia
- Elektronické zdravotné záznamy (obsahujú EDS, elektronický chorobopis a elektronickú zdravotnú kartu)
- Vykazovanie výkonov pre poisťovne
- Zber a spracovanie údajov pre štatistiku

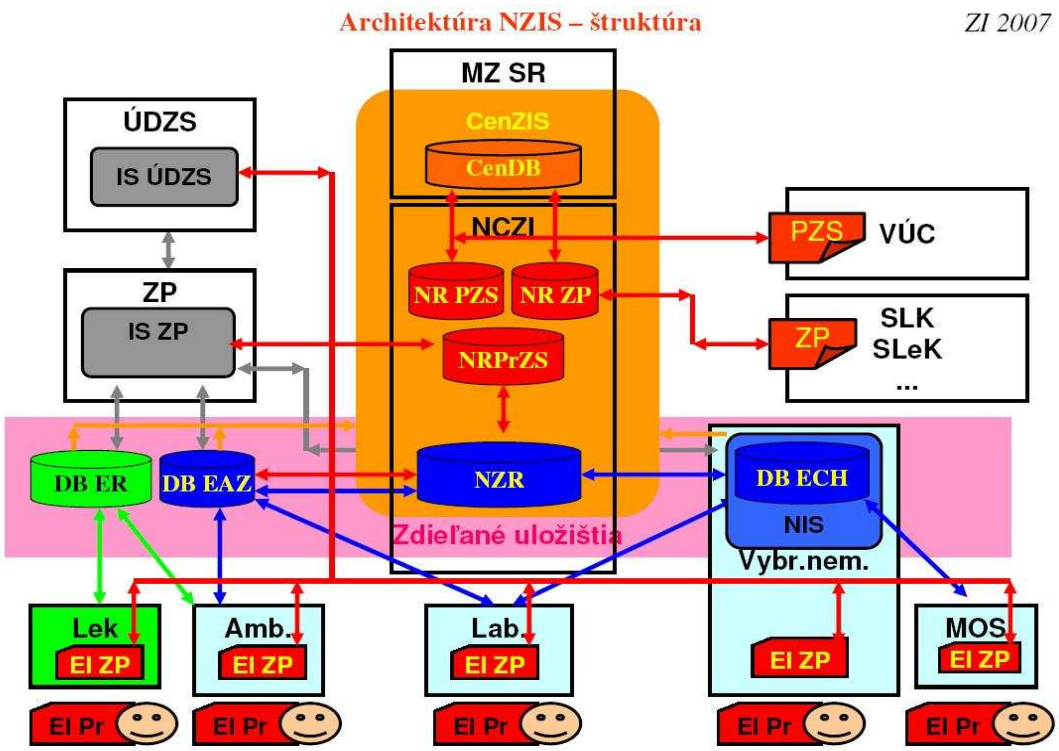
5.2.2. Architektúra NZIS

Architektúra NZIS sa predpokladá na 3 úrovniach, a to:

- základná úroveň:
  - informačné systémy poskytovateľov zdravotnej starostlivosti
  - elektronické identifikátory zdravotníckych pracovníkov a pacientov/poistencov
- stredná úroveň:

  databázy v zdieľaných úložiskách
  - elektronických receptov (DB ER)
  - elektronických ambulantných záznamov (DB EAZ)
  - elektronických chorobopisov (DB ECH)
- najvyššia úroveň:
  - národné zdravotnícke administratívne registre (NR PoZS, NR ZP, NR PrZS)
  - národné zdravotné registre (NR ZZU, NOR, …)

Navrhnutú architektúru zobrazuje obr. č. 5.



obr. č. 5

Architektúra NZIS navrhnutá NCZI

zdroj: www.nczisk.sk

5.2.3. Štandardy NZIS

Pri budovaní NZIS je potrebné dodržať nasledovné medzinárodne platné štandardy:

- Komunikačná kompatibilita (TCP/IP, …, XML)
- Interoperabilita (DICOM, HL7, HISA, EN 13606, SNOMED-CT)
- Bezpečnosť (EN 12251, EN 13606-4, EN 13608-1, ISO/IEC 17799, ISO 27001, ...)

5.2.4. Bezpečná identifikácia v NZIS

Základom pre autorizovanú a autentifikovanú komunikáciu je jednoznačná identifikácia profesionálov i pacientov a realizovaného výkonu v konkrétnom čase na konkrétnom mieste v spojení s princípmi zaručeného elektronického podpisu.

Vytvorenie systému autorizovanej komunikácie je podmienené vznikom bezpečného elektronického preukazu zdravotníckeho profesionála HPC (čo ukazujú

aj zahraničné riešenia). Tento preukaz je identifikačným a autentifikačným predmetom s funkciami vytvárania zaručeného elektronického podpisu, čiže slúži ako kľúč pre sprístupnenie zdravotných údajov. Týmto podpisom sa podpisujú všetky informácie o poskytnutej zdravotnej starostlivosti, ako aj elektronické správy (výsledky laboratórnych vyšetrení, postupov) vymieňané medzi zdravotníckymi profesionálmi.

Druhou dôležitou súčasťou tohto systému (a zároveň aj predpokladom) je, že každý občan SR (resp. v širšom kontexte každý občan EÚ) má bezpečný a jednoznačný elektronický predmet - preukaz pacienta PDC. Ten sa využíva ako identifikačné médium pacienta a kľúč na autorizáciu a verifikáciu poistného vzťahu. Zároveň ponúka priestor na uloženie administratívnych údajov, smerníkov na miesta, kde je fyzicky uložená pacientova zdravotná dokumentácia a uloženie limitovaných zdravotných dát pacienta – EDS.

Treťou časťou je služba overovania elektronických preukazov a transakcií, ktorá prepája informačné systémy jednotlivých poskytovateľov zdravotnej starostlivosti. Táto vytvára bázu pre bezpečnú a dôveryhodnú vzájomnú komunikáciu poisťovní a poskytovateľov zdravotnej starostlivosti.

Súčasné systémy identifikujú pacienta väčšinou prostredníctvom rodného čísla alebo identifikačného čísla poistenca. Tieto čísla sú uvedené na preukaze poistenca. Tento preukaz pacienta neumožňuje priame načítanie identifikačného čísla do elektronického systému. Použitie rodného čísla upravuje Zákon č. 428/2002 Z. z. o ochrane osobných údajov a jeho využívanie v systémoch elektronického zdravotníctva je preto bez úpravy tohto zákona problematické. Ošetrujúci lekár sa v súčasnosti identifikuje napríklad pri predpisovaní liekov 13 miestnym kódom, kde 4 miesta predstavuje kód jednotlivých poisťovní a 9 miest je pridelený lekárov kód. Tento identifikačný systém je zastaraný. V súčasnosti je na Slovensku 7 zdravotných poisťovní, a preto je 4 miestny kód na ich určenie zbytočný. Takisto kód pre lekárov sa prideľuje nesystematicky. Tento kód obsahuje dve miesta na určenie odbornosti lekára, tieto kódy ale nie sú kompatibilné so zoznamom odborností pre preskripčné obmedzenia. Jeho použitie v žiadnom prípade preto nemožno odporučiť.

Nová identifikácia odborníkov ako aj pacientov by mohla prebiehať pomocou čipovej karty pacienta, resp. profesionála. Jej rozmery a dátová štruktúra, zapísaná na čipe vrátane bezpečnostných a šifrovacích nástrojov sú predmetom štandardizácie -

ISO norma 7810. V súvislosti s PDC vydala organizácia ISO normu EN ISO 21549 Health informatics – Patient healthcard data. Norma má 8 častí:

- Všeobecná štruktúra
- Spoločné prvky
- Limitované klinické údaje
- Rozšírené klinické údaje
- Identifikačné údaje
- Administratívne údaje
- Údaje o medikácii
- Prepojenie

Z praktických príčin bude užitočné, ak by pacientska karta bola vydávaná jednotne a centrálne - a nie každou poisťovňou zvlášť, nakoľko väčšina údajov na karte nesúvisí s poisťovňou (prakticky ide len o jeden údaj). Profesijnú kartu HPC by mala vydávať stavovská organizácia. Zoznam odborností povoľuje príslušná stavovská organizácia a platnosť zmluvného vzťahu poskytovateľa zdravotnej starostlivosti k zdravotnej poisťovni zdravotná poisťovňa. Profesijná karta by mala spĺňať medzinárodný štandard pre profesijné karty. Táto karta potom držiteľa oprávňuje pristupovať k zdravotným záznamom uložených v elektronickom zdravotnom zázname, resp. k údajom EDS z pacientskej karty. Karta HPC umožní príslušnému profesionálovi predpisovať lieky, zapisovať výsledky vyšetrení do pacientovho záznamu, ale najmä potvrdí identitu pracovníka. Každý zdravotnícky profesionál - fyzická osoba - by mala mať pre svoj konkrétny výkon práve jeden profesijný preukaz, ktorý mu príslušná komora vydá na základe zápisu v profesijnom registri (lekár, gynekológ, zubár, atď.). Napr. lekár, ktorý má dve špecializácie bude mať dve karty HPC.

6. Elektronický podpis

V tejto kapitole uvedieme základné informácie o elektronickom podpise a uvedieme dôležité pojmy použité v ďalších kapitolách.

Pri klasickej komunikácii prostredníctvom papierových dokumentov sa spoľahlivé určenie totožnosti autora realizuje najčastejšie jeho vlastnoručným podpisom, pri dôležitejších dokumentoch sa podpis overuje dôveryhodnou inštitúciou – napr. notárom.

Elektronické podpisy sú kryptografickou konštrukciou umožňujúcou spoľahlivo zabezpečiť autentickosť a integritu elektronického dokumentu, ako aj nepopretie autorstva. Sú digitálnou analógiou vlastnoručných podpisov pri klasickej komunikácii. Zakladajú sa na asymetrických šifrovacích algoritmoch, v súčasnosti napríklad algoritmy RSA, DSA [11]. To znamená, že na šifrovanie a dešifrovanie sa používajú dva rôzne kľúče - verejný a súkromný kľúč (ten sa niekedy uvádza aj pod názvom privátny kľúč). Verejný kľúč používateľ zverejní a súkromný ponechá v tajnosti.

Keďže asymetrické šifrovacie algoritmy majú pomerne vysokú časovú náročnosť, v praxi sa súkromným kľúčom nepodpisuje celý dokument, ale len jeho odtlačok. Ten sa vypočíta z pôvodného dokumentu hašovacou funkciou. V súčasnosti sa na hašovanie používa napríklad skupina algoritmov SHA. Navyše vlastnosti kryptografických hašovacích funkcií – jednosmernosť a odolnosť voči kolíziám, pomáhajú chrániť bezpečnosť elektronického podpisu pred niektorými útokmi. Viac podrobností je možné nájsť napríklad v [11].

V súčasnosti teda podpísanie dokumentu D prebieha nasledovne: odosielateľ vytvorí z elektronického dokumentu D odtlačok pomocou hašovacej funkcie H. Následne použije svoj súkromný kľúč na podpísanie odtlačku H(D). Prijímateľ podpísanej správy dostane dokument D a k nemu pripojený podpis T(H(D)). Prijímateľ vypočíta z dokumentu D odtlačok H(D) a z podpisu T(H(D)) pomocou odosielateľovho verejného kľúča vypočíta H(D). Ak sa tieto dva odtlačky zhodujú, odosielateľ vie, že dokument sa nezmenil a je podpísaný osobou, ktorá pozná súkromný kľúč odosielateľa.

Keď sa k dokumentu pripojí elektronický podpis, ktokoľvek, kto pozná verejný kľúč autora si môže ľahko overiť, že dokument nebol po podpísaní modifikovaný a podpísal ho niekto, kto súkromný kľúč autora pozná. Elektronické podpisy poskytujú dostatočnú ochranu komunikácie medzi vlastníkmi príslušných kľúčov. Neriešia však sami problém väzby verejného kľúča na konkrétnu osobu alebo iný objekt. Pokiaľ adresát správy nemá možnosť spoľahlivo zistiť verejný kľúč autora, nemôže overiť, že správu naozaj poslal ten, kto sa vydáva za autora. Teda je potrebné mať dôveryhodný zdroj verejných kľúčov a spoľahlivú metódu prístupu k nemu.

Certifikačná autorita (Certification Authority – CA) je dôveryhodná inštitúcia, ktorá pre potreby elektronickej komunikácie plní podobné úlohy ako notár pri overovaní podpisov. Úlohou CA je udržiavať databázu verejných kľúčov a ich vlastníkov, poskytovať tieto verejné kľúče všetkým žiadateľom prostredníctvom certifikátov. Certifikát je dokument, ktorým CA potvrdzuje väzbu verejného kľúča na konkrétnu osobu alebo iný objekt.

Zákon č. 215/2002 Z. z. o elektronickom podpise rozoznáva dva druhy elektronických podpisov. Elektronický podpis a zaručený elektronický podpis. Úlohou elektronického podpisu je preukázať, že dokument bol podpísaný osobou, o ktorej predpokladáme, že tento dokument podpísala a zároveň poskytnúť možnosť overenia, či počas prenosu nedošlo k modifikácii tohto dokumentu. Nemá právnu silu podpisu overeného notárom. A práve na tento účel slúži zaručený elektronický podpis. Takýto podpis má zaručovať:

- Autentifikáciu – tzn., že adresát (prijímateľ), ktorému je určený dokument má istotu, že adresant (odosielateľ) je skutočne tá osoba, za ktorú sa vydáva. Ide o rozpoznanie a jednoznačnú identifikáciu podpisujúceho.
- Integritu – tzn., že to, čo adresant odoslal, je skutočne to, čo adresát dostal. Ide o zaručenie toho, že poslaný dokument sa dostal k adresátovi v nepozmenenej podobe.

Zaručený elektronický podpis je z bezpečnostných dôvodov vytváraný pomocou zariadenia na vyhotovenie elektronického podpisu a pomocou softvérovej aplikácie spĺňajúcej prísne bezpečnostné kritériá stanovené Zákonom č. 215/2002 Z. z. o elektronickom podpise. Na verejný kľúč je vydaný kvalifikovaný certifikát CA.

Certifikát CA obsahuje nasledovné údaje:

- sériové číslo
- ID vlastníka certifikátu (údaje identifikujúce osobu, ku ktorej sa dvojica kľúčov viaže)
- ID certifikačného centra
- rozsah platnosti certifikátu
- typ verejného kľúča (algoritmus, pre ktorý je určený)
- verejný kľúč
- digitálny podpis CA

Keď príjemca dostane takýto certifikát a pozná verejný kľúč príslušnej CA, môže overiť, že sa obsah certifikátu na ceste z CA k nemu nezmenil. Prípadný útočník, ktorý nepozná súkromný kľúč CA nemôže zmeniť obsah tak, aby digitálny podpis CA zodpovedal obsahu. Takže bezpečnosť zaručeného elektronického podpisu je založená na sile použitého algoritmu, sile hašovacej funkcie a na utajení súkromného kľúča CA. Ak by unikol súkromný kľúč CA, všetky ním podpísané certifikáty sa stávajú nedôveryhodnými.

6.1. Elektronický podpis zdravotníckeho profesionála

Každý zdravotnícky profesionál bude môcť vďaka svojmu zaručenému elektronickému podpisu podpisovať vykonané vyšetrenia, ako aj rôzne pracovné dokumenty, napr. aj elektronický recept. Zákon č. 215/2002 Z. z. o elektronickom podpise v §7, odseku 2, písmene c) uvádza: „Kvalifikovaný certifikát fyzickej osoby je certifikát, ktorý má v sebe uvedené obmedzenia na jeho použitie, ak tretia strana také obmedzenia rozlišuje“. V prípade zaručeného elektronického podpisu pre zdravotníckeho profesionála je rozumné v kvalifikovanom certifikáte uviesť také obmedzenia, ktorými bude jasne vymedzené, kedy môže profesionál používať svoj zaručený elektronický podpis. Tento podpis bude profesionál využívať výhradne vtedy, keď bude vystupovať vo svojej profesijnej role.

Ak by sme chceli uchovávať súkromný kľúč zdravotníckeho profesionála na jeho PC, narazíme na viaceré problémy. V operačných systémoch a sieťových programoch sa často nachádzajú chyby, ktoré potenciálne umožňujú neoprávnený prístup. Nemožno očakávať, že si bežný zdravotnícky profesionál bude schopný zabezpečiť svoj systém tak, aby tam mohol mať bezpečne uložený svoj súkromný kľúč. Preto musíme pre účely uchovávania súkromného kľúča zdravotníckeho profesionála zvoliť iné riešenie. Z ekonomického hľadiska je najvýhodnejšie uložiť súkromný kľúč priamo na čip jeho karty zdravotníckeho profesionála HPC.

6.2. Elektronický podpis pacienta

Jeden z problémov v súčasnom systéme zdravotnej starostlivosti v SR je, že neposkytuje možnosť dostatočnej kontroly lekárskych výkonov. Následkom tohto stavu sú napr. poisťovňami preplácané nevykonané lekárske úkony.

Tento problém môže byť značne obmedzený práve povinným používaním čipovej karty zdravotníckeho profesionála a pacientskej čipovej karty. Každý výkon, ktorý má byť lekárovi uznaný, bude musieť lekár podpísať svojím zaručeným elektronickým podpisom pomocou súkromného kľúča uloženého na jeho karte zdravotníckeho profesionála. Podobne každý úkon lekárovi podpíše pacient svojím zaručeným elektronickým podpisom. Súkromný kľúč na vyhotovenie tohto podpisu bude uložený na čipe pacientovej čipovej karty. Tým zabezpečíme, že systém neumožní lekárovi vykazovať výkony pacientovi, ktorý u neho nebol.

Zaručený elektronický podpis pacient teda využije na podpísanie vykonaných úkonov, čím lekárovi potvrdí, že ich skutočne vykonal. Zároveň ho použije u lekárnika, kde ním potvrdí prevzatie predpísaných liekov.

Pri realizácii narazíme na viaceré problémy. Prvým je, že čipovú kartu pacienta budú mať všetci občania SR, čiže aj trojročné dieťa bude mať svoju pacientsku čipovú kartu a svoj zaručený elektronický podpis. Problémom je, že používanie zaručeného elektronického podpisu je ohraničené pre osoby spôsobilé právnych úkonov. Spôsobilosť občana pre právne úkony vyplýva z občianskeho zákonníka.

Druhým problémom je, že je tu vysoké riziko zneužitia pacientovho zaručeného elektronického podpisu lekárom. Nie je ťažké predstaviť si situáciu, keď ochotný lekár pomôže staršiemu človeku, aby sa nemusel trápiť s novou technológiou, ale zároveň podpíše pacientovým elektronickým podpisom obsah iného dokumentu nesúvisiaceho so zdravotníctvom, napr. priznanie dlžoby 10 000 SK.

Preto sa javí ako rozumné využiť už zmienený §7, odsek 2, písmeno c) Zákona č. 215/2002 Z. z. o elektronickom podpise a v kvalifikovanom certifikáte k dvojici kľúčov pacienta uviesť také obmedzenia, ktoré používanie tohto súkromného

a verejného kľúča určia výhradne len na účely potrebné v systéme zdravotnej starostlivosti. To znamená, že pomocou tohto pacientovho súkromného kľúča bude technicky možné podpísať napríklad aj predaj vlastného domu, ale z právneho hľadiska tento podpis nebude platný kvôli obmedzeniu uvedenému v kvalifikovanom certifikáte pre túto dvojicu kľúčov. Pri tomto riešení bude pravdepodobne potrebná taká úprava legislatívy, ktorá zakotví pre neplnoleté osoby spôsobilosť podpisovať lekárovi úkony pomocou ich pacientskej čipovej karty, resp. pre osoby do istého veku, napr. do 10 rokov v prípade potreby môžu podpísať aj rodičia.

Týmto prístupom umožníme lekárom vykazovať výkony jedine pacientovi, ktorého čipovú kartu majú práve v čítačke. Zároveň minimalizujeme riziko zneužitia pacientovho zaručeného elektronického podpisu.

Pri výbere konkrétneho algoritmu použitého na vytváranie elektronického podpisu je nutné brať do úvahy kompatibilitu riešenia so zahraničnými riešeniami. V prípade, ak EÚ vydá smernicu upravujúcu túto problematiku, bude nutné takúto smernicu dodržať. V súčasnosti zoznam šifrovacích algoritmov a podpisových schém na realizáciu zaručeného elektronického podpisu uvádza NBÚ v prílohe k vyhláške č. 537/2002 Z. z. Pri výbere algoritmu použitého v navrhovanom systéme by bolo výhodné spolupracovať s NBÚ. Podľa informácií z NCZIS sa na realizáciu zaručeného elektronického podpisu v systéme pre poskytovanie EDS plánuje použiť algoritmus RSA s kľúčom dĺžky 2048 bitov a hašovacia funkcia SHA II. [11]

7. Návrh systému pre poskytovanie EDS

Na základe uvedených zahraničných riešení, súčasných okolností, legislatívnych podmienok SR, ale predovšetkým s ohľadom na vydané záväzné dokumenty EÚ, považujeme za najschodnejšie riešenie problematiky EDS v SR obdobu českého modelu, upravenú na slovenské pomery a doplnenú o čipovú kartu pre profesionálov aj pacientov. Z praktického hľadiska sa na úlohu pacientskej čipovej karty - PDC výborne hodí elektronický zdravotný preukaz poistenca – eEHIC. Európska únia definuje len jednu stranu preukazu EHIC, pričom údaje z tejto strany preukazu budú potrebné aj na PDC. Druhá strana preukazu by teoreticky mohla zároveň slúžiť ako občiansky preukaz (viď Rakúsko). V tom prípade by ale bolo nutné uvažovať o umiestnení ochranných prvkov na PDC, čo by zrejme výrazne zvýšilo jej cenu. Prístup k dátam na eEHIC bude možný len v kombinácii s čipovou kartou profesionála. V súčasnosti existujú dvojštrbinové čítačky čipových kariet, ktoré umožnia vložiť eEHIC a HPC naraz.

Znamená to teda, že profesionál bude mať čipové karty dve. Profesijnú kartu HPC s možnosťou používať zaručený elektronický podpis zdravotníckeho profesionála a svoju „občiansku“ kartu eEHIC s možnosťou používať zaručený elektronický podpis v roli pacienta.

Z dôvodu čítania údajov na čipovej karte zahraničnými lekármi v ich materinských jazykoch a čítania údajov zahraničných pacientov slovenskými lekármi v slovenčine je potrebné úspešne vyriešiť problematiku štandardizácie lekárskych pojmov a ich jedinečnej reprezentácie. Je nutné, aby bol zostavený oficiálny tím odborníkov, ktorý by dokončil spracovanie jestvujúcich podkladov uplatňujúc oficiálne slovenské názvoslovie zosúladené so SNOMED CT a jeho následné schválenie slovenskými lekárskymi inštitúciami.

7.1. Typy EHIC preukazov

Plastový EHIC – klasický identifikačný doklad. Je to vlastne plastová kartička s vytlačenými údajmi. Tie sú definované nariadeniami EHS č. 189/2003, č. 190/2003 a č. 191/2003 (viď [13]) jednotne pre štáty EÚ a EFTA.

Elektronický EHIC (eEHIC) – plastová karta s čipom, ktorá obsahuje rovnaké vizuálne informácie ako plastový EHIC. Čip obsahuje tieto informácie v elektronickej podobe. Okrem toho umožňuje na kartu umiestniť rôzne ďalšie údaje, napríklad práve EDS. Elektronický EHIC by potenciálne mohol slúžiť ako pacientska čipová karta. Jej prostredníctvom môže byť jednoznačne identifikovaná osoba, ktorá je držiteľom tejto karty. Z bezpečnostných dôvodov je samozrejme nutné túto kartu chrániť pred zneužitím. Implementáciou a koordináciou týchto kariet sa zaoberá konzorcium NETC@RDS, ktoré vyvíja systém umožňujúci v rámci krajín EÚ a EFTA overovanie platnosti eEHIC preukazov v reálnom čase.

7.2. Čipová karta profesionála (HPC)

V tejto časti uvádzame základné informácie o predpokladanej podobe HPC. Karta HPC bude slúžiť ako autentifikačný a autorizačný prostriedok pre zdravotníckeho profesionála. Bezpečnosť čipovej karty HPC je veľmi dôležitým predpokladom bezpečnosti celého systému. Je nutné chrániť HPC pred zneužitím, autenticitu karty HPC a integritu údajov na čipe HPC. Určite by bolo vhodné riešiť zabezpečenie HPC pred zneužitím minimálne pomocou PIN-u alebo pomocou biometrických údajov, prípadne kombináciou týchto spôsobov. Pri troch neúspešných pokusoch o zadanie PIN-u by sa karta mala z bezpečnostných dôvodov zablokovať. Zabezpečenie autenticity zabráni aby si mohol útočník vyrobiť vlastnú platnú kartu HPC, pomocou ktorej by pristupoval k pacientovým údajom či už EDS, alebo k celému pacientovmu EHR. Integrita údajov na HPC je dôležitá, aby si žiaden útočník nemohol ľubovoľne pozmeniť napr. prístupové práva, či dobu platnosti karty HPC. Naplnenie týchto bezpečnostných požiadaviek je nutným predpokladom bezpečnosti celého systému. Podrobnejšia analýza, a riešenie bezpečnostných požiadaviek na kartu HPC je mimo rozsahu tejto práce.

7.2.1. Elektronické údaje uložené na HPC

Podľa informácií z NCZI na čipe budú uložené nasledovné údaje:

- Identifikačné údaje
- Administratívne údaje
- Aplikácia umožňujúca vytváranie zaručeného elektronického podpisu zdravotníckeho profesionála
- Definícia prístupových práv profesionála
- Aplikácia overujúca PIN, prípadne totožnosť na základe biometrických prvkov
- V prípade zabezpečenia karty biometrickými údajmi bude vzorka týchto údajov uložená na karte
- Iné

7.2.2. Vizuálne informácie na HPC

Podľa informácií z NCZI sa aktuálne uvažuje o umiestnení nasledovných vizuálnych údajov na HPC:

- Národný kompetenčný úrad (kto vydáva kartu a vedie zoznam profesionálov)
- Národné registračné číslo (National Identification Number)
- výrobné číslo karty
- dátum expirácie karty
- Meno
- Fotografia držiteľa HPC
- Farebný horný a dolný okraj podľa príslušnosti ku komore (lekári, sestry, ...)

8. Čipová karta pacienta eEHIC

Čipová karta pacienta bude slúžiť ako autentifikačný a autorizačný prostriedok pre pacienta. Na základe vlastníctva eEHIC bude môcť pacient vstupovať do svojej zdravotnej dokumentácie a čítať ju, prípadne v časti vyhradenej pre jeho poznámky doplniť užívané voľne predajné lieky alebo poznámky týkajúce sa liečby.

Zároveň poskytnutím karty zdravotníckemu profesionálovi oprávni pacient profesionála k vstupu k jeho zdravotným údajom uloženým na eEHICu i v databáze. Bezpečnosti čipovej karty venujeme samostatnú kapitolu. Na čipe tejto karty budú uložené údaje v digitálnej podobe. Tu je možné zvážiť viacero rôznych prístupov k otázke, aké údaje budú na čipe uložené.

Zároveň bude možné údaje urgentnej medicíny získať aj z databázy prostredníctvom núdzového hesla profesionála. Toto heslo môže použiť len profesionál autentifikovaný prostredníctvom svojej HPC. Pomocou tohto hesla má profesionál možnosť dostať sa k údajom zachraňujúcim život aj v prípade, že je karta eEHIC poškodená, alebo ju pacient nemá so sebou, alebo je z iných príčin nedostupná. Vhodným príkladom je havarovaný autobus kde cestujúci majú svoje doklady v batožinovom priestore, odkiaľ ich nie je možné vybrať kvôli poškodeniu autobusu, ale zranený je schopný poskytnúť záchranárom svoje identifikačné údaje alebo je nablízku niekto, kto je schopný spoľahlivo identifikovať pacienta v bezvedomí. Z bezpečnostných dôvodov musí systém automaticky ukladať podrobný záznam o každom použití tohto núdzového prístupového mechanizmu. Zároveň bude automaticky informovať pacienta zaslaním emailu v prípade, že uviedol adresu na ktorú má byť správa v tomto prípade doručená. Identita profesionála vykonávajúceho tento vstup bude zistená práve vďaka jeho HPC.

8.1. Údaje využiteľné na čipe pacientskej karty eEHIC

8.1.1. Minimálna množina údajov

Prvým možným prístupom je uložiť na čip minimálnu množinu osobných údajov, ktoré by mohli byť zneužité. Všetky údaje o zdravotnom stave budú uložené v centralizovanej databáze NZIS spravovanej NCZI. Karta eEHIC bude slúžiť ako token pre elektronický podpis a ako kľúč umožňujúci vstup do pacientovho zdravotného záznamu v databáze. Identifikačné a administratívne údaje budú uvedené v elektronickej podobe, aby sa lekár vyhol manuálnemu vypisovaniu týchto údajov. V tomto prípade budú na čipe uložené tieto údaje:

- Identifikačné údaje
- Administratívne údaje
- Aplikácia umožňujúca vytváranie zaručeného elektronického podpisu pacienta
- Aplikácia overujúca PIN, prípadne totožnosť na základe biometrických prvkov (ak budú použité)
- V prípade zabezpečenia karty biometrickými údajmi bude vzorka týchto údajov uložená na karte
- Iné

Výhodou tohto prístupu je značné zjednodušenie réžie údajov uložených na čipe. Všetky údaje pacienta totiž musia byť pre prípad poškodenia alebo stratenia karty uložené aj v databáze NZIS, a teda ak by zdravotné údaje boli uložené aj na čipe, bude nutné zabezpečiť aktualizáciu údajov na čipe a ich konzistenciu s údajmi na karte. Potrebné údaje pacienta profesionál získa z databázy NZIS na základe autentifikácie a autorizácie pomocou vlastného HPC a súčasne pacientovho eEHIC.

8.1.2. Rozšírenie o nemenné zdravotné údaje

Druhým možným prístupom je rozšírenie vyššie uvedených údajov o množinu nemenných zdravotných údajov. V tomto prípade budú na čipe pridané nasledovné údaje:

- Krvná skupina
- Neliečiteľné ochorenia
- Chronické ochorenia
- Liekové alergie
- Vrodené
- Iné

Významnou výhodou získanou týmto prístupom je možnosť dostať sa k základným nemenným zdravotným údajom pacienta aj v miestach, ktoré nie sú pokryté signálom. V takomto prípade údaje na čipe môžu zachrániť ľudský život, čo je ich hlavným zmyslom. Týmto prístupom sa zároveň vyhneme problémom s aktualizáciou zdravotných údajov na čipe.

8.1.3. Rozšírenie o všetky údaje zachraňujúce život

Keď pripustíme možnosť občasnej neschopnosti prístupu do databázy so zdravotnými údajmi, je na mieste ďalší prístup. Čo ak nemenné zdravotné údaje nepostačujú a na záchranu života by pomohli aj údaje, ktoré sa menia? Napríklad lieky užívané počas posledných troch mesiacov alebo zoznam ochorení za posledný polrok. Logicky sa nám núka rozšírenie zdravotných údajov uložených na čipe na množinu všetkých údajov zachraňujúcich život. Tu je miesto pre štandardizáciu množiny týchto údajov. Kompetentná organizácia musí v spolupráci s odborníkmi jasne definovať, ktoré údaje do tejto množiny patria, či už na národnej, alebo európskej úrovni.

Problémom tohto prístupu je práve aktualizácia premenlivých údajov na čipe. Aby mohol zahraničný lekár aktualizovať zdravotné údaje pacienta, musel by byť kompatibilný hardvér i softvér týchto systémov a jasne definované medzinárodne platné prístupové práva pre profesionálov. Resp. musel by existovať systém overujúci profesionalitu odborníka podľa jeho národnej HPC a primerane k jeho odbornosti by

mu pridelil právo na aktualizáciu údajov na čipe eEHIC. Zároveň by bolo nutné zabezpečiť konzistenciu údajov uložených na čipe a v databáze.

8.1.4. Rozšírenie na všetky zdravotné údaje

Ďalším možným prístupom je, aby pacient nosil so sebou neustále svoju kompletnú zdravotnú dokumentáciu. V tomto prípade by to musela byť kópia celej dokumentácie, pretože ak by pacient stratil svoje zdravotné záznamy, bez zálohy by bolo nemožné tieto dôležité údaje získať znovu. Výhodou tohto prístupu je dostupnosť kompletnej pacientovej zdravotnej dokumentácie aj v prípade neschopnosti pripojiť sa k databáze. Nevýhodou je veľké navŕšenie potrebnej pamäťovej kapacity. Starší pacienti majú často rozsiahly zdravotný záznam obsahujúci mnoho výstupov rôznych odborných vyšetrení, napr. CT, RTG snímky, atď. Zároveň sa pri tomto prístupe zvyšuje riziko zneužitia. Úplná zdravotná dokumentácia je zbierka veľmi citlivých osobných údajov. Výhoda tohto prístupu je v porovnaní s cenou za toto riešenie neadekvátna, a preto tento prístup neodporúčame.

8.1.5. Rozšírenie o iné údaje

Čipová karta pacienta ponúka ďalšie možnosti využitia. Môže slúžiť ako občiansky preukaz (viď Rakúsko). Veľmi významným spôsobom využitia je elektronická preskripcia. Podľa Štúdie uskutočniteľnosti elektronickej preskripcie na Slovensku [28] existujú tri spôsoby, ako sa dostane elektronický recept od lekára k lekárnikovi.

- Lekár – verejné úložisko – lekáreň
- Lekár – eEHIC – lekáreň
- Lekár – vopred zvolená lekáreň

Pri prvom a treťom spôsobe sa eEHIC využíva ako nosič kupónu, ktorý sa používa ako identifikátor receptu v úložisku, resp. na mailovom serveri lekára. Pacientska čipová karta eEHIC je preto jedným z predpokladov pre funkčnosť elektronickej preskripcie.

9. Bezpečnostné obmedzenia údajov na čipe eEHIC

V tejto kapitole pojednávame o vhodnom rozsahu údajov na eEHIC z pohľadu bezpečnosti a o prístupe k ich zabezpečeniu. Dôvernosť údajov, čiže povolenie prístupu k nim len pre autorizované entity zabezpečíme v závislosti od konkrétnych údajov uvedených na karte. Preto popis zabezpečenia dôvernosti údajov uvádzame v neskoršej kapitole. Dostupnosť systému je založená na predpoklade, že si pacienti budú nosiť eEHIC so sebou a pre prípad potreby bude možné k údajom EDS pristúpiť aj prostredníctvom databázy obsahujúcej EHR bez vloženia čipovej karty pacienta, pričom sa uloží presný záznam, ktorý profesionál a do koho dokumentácie kedy nazeral. Daný pacient bude o takomto prístupe automaticky informovaný. Toto riešenie predpokladá realizáciu databázy sprístupňujúcej EHR takým spôsobom, že umožní profesionálom spomenutý núdzový vstup k EDS pacienta.

9.1. Integrita údajov na čipovej karte pacienta

Integrita všetkých údajov uložených na čipe je nutnou bezpečnostnou požiadavkou. Keďže ide o údaje, ktoré budú využívané v kritických situáciách na záchranu života je zrejmé, že je potrebné minimalizovať riziko, že niekto tieto údaje omylom alebo úmyselne pozmení. Zmena krvnej skupiny či zoznamu alergií alebo vrodených chorôb, by mohla spôsobiť vážnu ujmu na zdraví, či prípadnú smrť pacienta. Takisto prípadné neautorizované zmeny doby platnosti karty či poisťovne by potenciálne mohli viesť k podvodom. Keďže narušenie integrity údajov na karte eEHIC sa javí ako významné riziko navrhujeme, aby bola čipová karta pri vydaní občanovi uzamknutá na zápis. Znamená to, že po vydaní karty nebude fyzicky možné zapisovať ani meniť údaje na čipe.

Keďže údaje na karte sa nebudú meniť počas jej životnosti, je možné ich podpísať súkromným kľúčom CA, čím sa zabezpečí ich integrita, ako aj ich autentickosť (v prípade potreby zmeny alebo doplnenia údajov je potrebné vydať novú kartu). Vďaka tomuto prístupu nikto, kto nepozná súkromný kľúč CA nebude schopný vytvoriť pacientsky čip s vlastnými údajmi tak, aby bol považovaný za platný.

Ak by sme zvolili rovnaký prístup k zabezpečeniu integrity HPC, mohli by sme predpokladať nasledovný tvar údajov na oboch kartách: U | TCA(H(U)). U je

množina údajov na čipe, H(U) je odtlačok údajov U získaný ako výstup hašovacej funkcie H so vstupom U a TCA(H(U)) je H(U) podpísaný súkromným kľúčom CA.

Na vzájomné overenie integrity kariet HPC a eEHIC je možné používať nasledovný protokol. Lekár vloží svoju HPC do dvojštrbinovej čítačky a autentifikuje sa voči HPC. Ak sa autentifikuje úspešne, pri príchode pacienta vloží do druhej štrbiny jeho eEHIC. Nasleduje overenie integrity oboch kariet navzájom:

1. Čip HPC zráta H(U) zo svojich údajov U
2. Následne pošle čipu eEHIC vyrátaný odtlačok H(U)
3. HPC pošle svoj TCA(H(U))
4. Čip karty eEHIC použije na ňom uložený verejný kľúč CA na overenie zhody prijatého odtlačku H(U) a odtlačku H(U) z prijatého podpisu TCA(H(U))

Ak sa zhodujú, následne prebehne analogický postup na overenie integrity čipu eEHIC voči HPC. Ak aj toto overovanie prebehne úspešne, bola zachovaná integrita údajov na oboch čipoch.

9.2. Autenticita čipových kariet HPC a eEHIC

Na vzájomné overenie autenticity kariet HPC a eEHIC je možné používať protokol Secure Sockets Layer - SSL [12]. Aby sa mohol využívať, na oboch čipových kartách musí byť uložený certifikát CA overujúci ich autentickosť.

Pri pristupovaní do databázy s EHR pacienta je potrebné zabezpečiť, aby lekár mohol vstúpiť iba do EHR pacienta, ktorého eEHIC má v čítačke. Je potrebné overenie autenticity aj medzi kartou HPC a databázou a eEHIC a databázou. Keďže na oboch čipoch je uložený certifikát CA, na overenie autenticity oboch kariet voči databáze je možné využiť opäť protokol SSL [12], ak aj databáza bude certifikovaná dôveryhodnou CA. Vďaka tomuto prístupu máme zaručenú požadovanú autenticitu a nie je problémom overiť, že sa jedná o čipovú kartu pacienta, ktorého EHR sa požaduje z databázy.

10. Údaje na čipe eEHIC

Z výsledkov predchádzajúcich kapitol vyplýva, že čip eEHIC bude uzamknutý pre zápis. Preto navrhujeme na čipe eEHIC umiestniť množinu údajov popísaných v odseku 8.1.1. Minimálna množina údajov, rozšírenú o nemenné zdravotné údaje relevantné pri záchrane života, popísané v odseku 8.1.2. Vďaka tomuto prístupu môžeme zabezpečiť integritu a autenticitu karty popísaným spôsobom a zároveň na čipe budú uložené najdôležitejšie údaje urgentnej medicíny. Na čipe teda budú uložené nasledovné údaje:

- Identifikačné údaje
- Administratívne údaje
- Nemenné údaje urgentnej medicíny
- Certifikát CA na overovanie autenticity
- Aplikácia na vytváranie zaručeného elektronického podpisu pacienta
- Súkromný kľúč pacienta
- Zaručený podpis CA

10.1. Dôvernosť údajov na čipe eEHIC

Identifikačné a administratívne údaje na karte eEHIC budú aj vo vizuálnej podobe. Preto nemá zmysel tieto údaje v elektronickej podobe chrániť pred neautorizovaným čítaním. Každému, kto by tieto údaje chcel zistiť, sa to ľahko podarí aj bez toho, aby kartu PDC musel vkladať do čítačky.

Údaje urgentnej medicíny budú chránené vyššie spomenutým protokolom SSL na zaistenie autenticity karty HPC voči karte eEHIC a protokolom na vzájomné overenie integrity oboch kariet. Ak profesionál má platnú svoju HPC a úspešne prebehnú oba protokoly, môžeme zvoliť nasledovné prístupy.

- Každý zdravotnícky profesionál bude mať prístup ku všetkým údajom urgentnej medicíny uloženým na čipe eEHIC. V tomto prípade je problém dôvernosti údajov vyriešený.
- Zdravotnícki profesionáli budú mať pridelené práva na čítanie časti, prípadne celej skupiny údajov EDS. Definícia a realizácia rôznych prístupových práv

profesionálov je mimo rozsahu tejto práce. V tomto prípade bude potrebné zabezpečiť dôvernosť údajov na čipe eEHIC tak, aby každý profesionál mal prístup práve k tým údajom, ku ktorým ich má mať na základe svojich prístupových práv.

K zabezpečeniu aplikácie vyhotovujúcej zaručený elektronický podpis pacienta proti zneužitiu možno zaujať nasledovné prístupy:

Keďže tento podpis bude určený výhradne na účely potvrdzovania výkonov vykonaných zdravotníckym profesionálom a jeho využívanie na iné účely bude obmedzené, nie je nutné chrániť túto aplikáciu tak prísne, ako aplikáciu vyhotovujúcu zaručený elektronický podpis bez obmedzení.

Jedným prístupom teda je chrániť túto aplikáciu iba spomínanými protokolmi SSL a protokolom overujúcim integritu, ktoré určia, či sa naozaj jedná o platnú kartu HPC. Pri tomto prístupe nie je možné eliminovať riziko, že si lekár pacientovou kartou podpíše aj nevykonané výkony bez toho, aby o tom pacient vedel. Všetky výkony ale budú uvedené v pacientovom zdravotnom zázname EHR v databáze spravovanou organizáciou NCZI. Každý pacient si bude môcť kontrolovať, aké údaje má uvedené vo svojej karte a v prípade nekonzistencií bude môcť situáciu riešiť v rámci legislatívnych možností.

Druhým prístupom je aplikáciu vyhotovujúcu pacientov podpis chrániť osobným heslom pacienta - PIN-om . Týmto prístupom umožníme pacientovi, aby podpísal iba tie výkony, ktoré lekár naozaj vykonal. Pri tomto prístupe žiaľ narážame na iný problém. Keďže kartu eEHIC bude mať každý občan SR, dá sa predpokladať častý vznik nasledovných situácií: pacient zabudol svoj PIN, lekár už vyšetrenia vykonal, avšak nebude možné, aby pacient lekárovi podpísal výkony. Mnoho občanov nie je dostatočne vzdelaných v medicínskej oblasti, aby naozaj rozumeli vykonaným vyšetreniam a aby vedeli, čo podpisujú. Toto môže viesť k dvom konfliktom. Lekár si nahodí výkony, ktoré nevykonal a pacient na to nepríde. Alebo pacient odmietne lekárovi podpísať vykonané výkony (buď preto, že nebude rozumieť aké výkony mu lekár naozaj vykonal alebo zo zlomyseľnosti). Kým by lekári vysvetlili pacientom, čo a prečo majú podpísať, strácali by oveľa viac času a námahy, než im celý systém

ušetrí. Zároveň eliminácia rizika, že si lekár nechá podpísať nevykonaný výkon je nedostatočná.

Ďalším prístupom je aplikáciu vyhotovujúcu pacientov podpis chrániť biometrickými údajmi. V súčasnosti je toto riešenie finančne a technologicky náročnejšie. Tu je na zváženie pomer cena / benefit.

Z uvedeného vyplýva, že je zrejme jednoduchšie a praktickejšie nechrániť aplikáciu vyhotovujúcu pacientov podpis PIN-om, ale zvoliť prvý prístup. Zároveň je potrebné ponechať možnosť reklamácie, prípadne sťažností pre pacientov, ktorí zistia nezrovnalosti vo svojich záznamoch EHR.

Karta eEHIC má slúžiť aj ako kľúč umožňujúci profesionálom prístup k databáze so všetkými pacientovými zdravotnými údajmi EHR. Úloha určiť kto bude mať práva na čítanie a zápis do pacientovho EHR a v akom rozsahu, je mimo témy tejto práce. Pri sprístupňovaní pacientovho EHR zdravotníckemu odborníkovi sú možné viaceré prístupy.

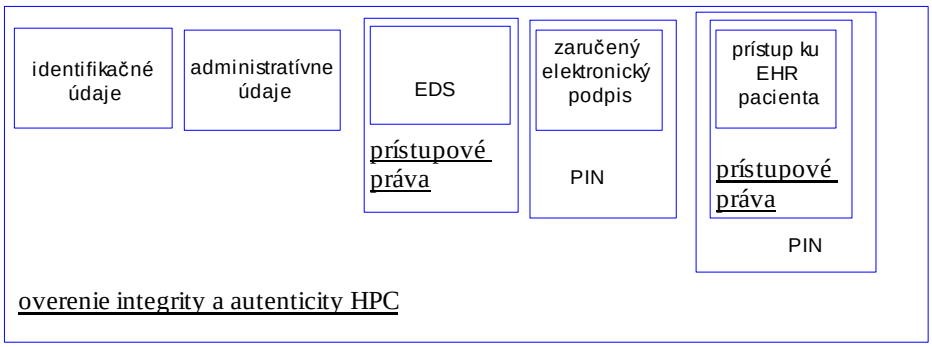
Podobne ako v Českej republike, môžeme ponechať pacientovi možnosť rozhodnúť, koho oprávni nahliadať do svojej dokumentácie. V tom prípade bude prístup k pacientovmu EHR vhodné chrániť osobným heslom pacienta – PIN-om. Toto riešenie opäť naráža na problém zabudnutého PIN-u, resp. neschopnosť značnej časti pacientov používať PIN zodpovedne (nepísať si ho na papier, nediktovať ho lekárovi,...)

Druhou možnosťou je definovať prístupové práva na základe odbornosti zdravotníckych profesionálov centrálne. To by znamenalo, že napr. lekárnici nebudú mať oprávnenie na zápis diagnóz do pacientovho EHR, ale budú mať právo na čítanie zoznamu liekov, ktoré pacient užíval. V tomto prípade bude systém postavený na dôvere, že každý odborník bude mať prístup ku všetkým relevantným údajom potrebným pre správne vykonávanie jeho profesie (preto je potrebné, aby návrh prístupových práv ponúkli odborníci v tejto oblasti), ale zároveň nezneužíva informácie, ku ktorým má na základe svojej odbornosti prístup. Pri tomto riešení nie je nutné používať PIN pacienta. Na zabezpečenie karty eEHIC proti zneužitiu na prístup k databáze s EHR pacienta postačí spomínaný protokol overujúci vzájomnú

autenticitu kariet HPC a eEHIC. Tým vylúčime útok pomocou falošnej karty HPC. Zároveň vieme, že každý profesionál má definované svoje prístupové práva vďaka čomu sa nedostane k údajom, ktoré majú pred ním ostať utajené.

Pre ochranu tejto funkcionality karty eEHIC biometrickými údajmi platí, že v súčasnosti je toto riešenie finančne a technologicky náročnejšie. Tu je na zváženie pomer cena / benefit.

Návrh údajov umiestnených na čipovej karte eEHIC a návrh zabezpečenia dôvernosti týchto údajov a ich ochrana pred zneužitím je znázornený na obr. č 6. Nami zvolený návrh zabezpečenia dôvernosti údajov a ich ochrana pred zneužitím je vyznačený podčiarknutím jednotlivých častí. Pre úplnosť sú na obrázku aj ďalšie spomenuté možnosti zabezpečenia dôvernosti týchto údajov.



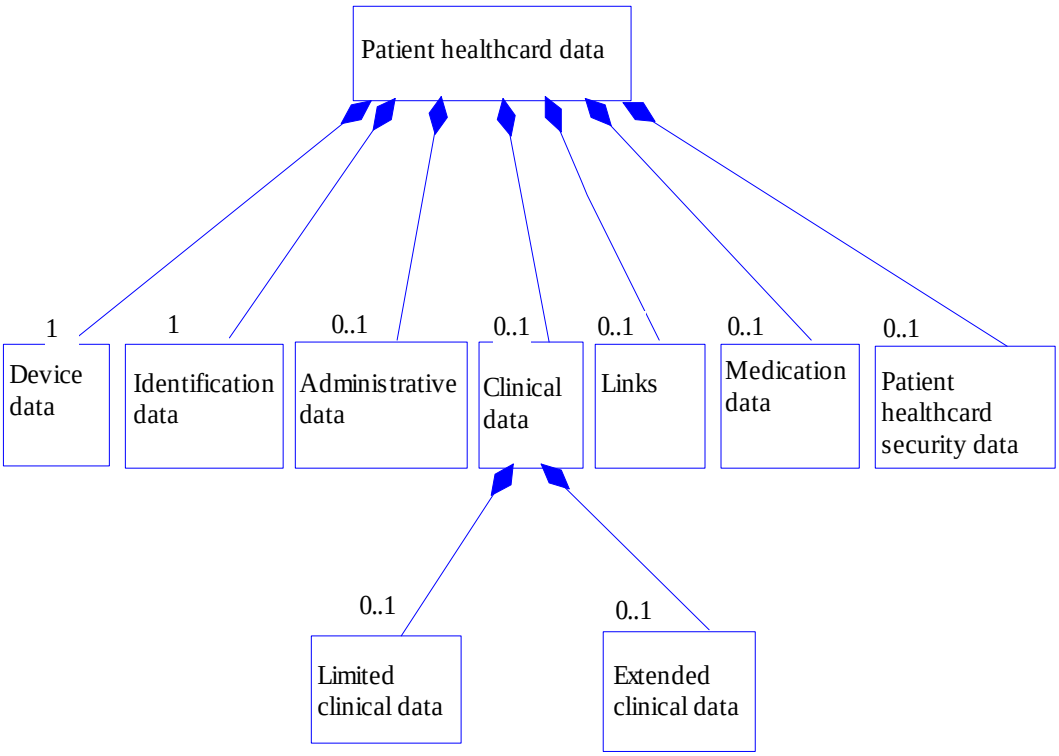
obr. č. 6

návrh zabezpečenia dôvernosti údajov na eEHIC

10.2. Štruktúra údajov

Keďže jednou z hlavných požiadaviek na systém poskytujúci EDS je jeho interoperabilita, je potrebné dodržiavať existujúce štandardy. Štruktúru údajov uložených na čipe PDC stanovuje norma EN ISO 21549 Health informatics Patient healthcard data, a preto navrhujeme jej dodržanie aj pri realizácii systému poskytujúceho údaje EDS prostredníctvom karty eEHIC. Táto norma má 7 častí, pričom 5 z nich je na Slovensku uznaných ako Slovenská Technická Norma.

Kvôli zvýšenej prehľadnosti štruktúru údajov stanovenú normou uvádzame v grafickej podobe na obr. č. 7.



obr. č. 7

Štruktúra údajov uložených na čipe eEHIC

10.3. Odhad pamäťovej náročnosti

V tejto časti práce podávame približný odhad pamäťovej náročnosti zvoleného návrhu.

10.3.1. Identifikačné údaje

- Meno :String[20]
- Priezvisko :String[20]
- Rodné priezvisko :String[20]
- Tituly :Set of Titul, kde Titul je vymenovaným typom obsahujúcim všetky používané tituly (predpokladáme že ich nie je viac ako 63) reprezentované kladnými celými číslami 1 – 63
- Dátum narodenia: Date, kde Date je reprezentovaný osemmiestnym číslom podľa ISO 8601 v tvare RRRRMMDD, kde DD je deň narodenia, MM je mesiac narodenia a RRRR je rok narodenia
- Rodné číslo :Rodnecislo, kde Rodnecislo je 10 miestne číslo vyhovujúce normalizovanému tvaru rodného čísla, pre zahraničného obyvateľa SR, ak nemá RČ, treba jednoznačný osobný kľúč zodpovedajúceho tvaru
- Pohlavie :Boolean
- Iné napr. národnosť, miesto narodenia, telefónne číslo, mailová adresa (na automatickú notifikáciu o núdzovom vstupe profesionála)

Ak predpokladáme, že jedno písmeno sa dá zakódovať pomocou 8 bitov, meno, priezvisko a rodné priezvisko zakódujeme pomocou 60 B.

Na zakódovanie jedného titulu bude stačiť 6 bitov. Ak predpokladáme, že jednotlivec nebude mať viac ako 8 titulov, bude na zakódovanie titulov na eEHIC stačiť 6 B.

Dátum narodenia môžeme zakódovať pomocou 5 bitov pre deň, 4 bity pre mesiac a na zakódovanie roka nám určite postačí 15 bitov, teda na určenie dátumu budú určite stačiť 3 B.

Na zakódovanie rodného čísla nám postačí 31 bitov. 7 bitov pre rok, 5 bitov pre mesiac (ženám sa pripočítava 50 k číslu mesiaca, preto ten bit navyše), 5 bitov pre deň a 14 bitov pre posledné 4 miesta. Ak pridáme bit pre určenie pohlavia dostávame 4 B.

Z uvedeného vyplýva, že pre identifikačné údaje pacienta nám postačí 73 Bytov.

10.3.2. Administratívne údaje

- Poisťovňa :Poistovna, kde Poistovna je vymenovaným typom obsahujúcim všetky slovenské poisťovne
- Adresa trvalého bydliska :Adresa, kde Adresa je zloženým typom obsahujúcim:
    - Ulica :String [50]
    - Číslo domu :Cislo, kde Cislo je kladné celé číslo od 0 po 4000
    - Mesto :String[50]
    - PSČ :PSC, kde PCS je 5 miestne kladné celé číslo
- Právne obmedzenia držiteľa :set of Obmedzenie, kde Obmedzenie je vymenovaným typom možných právnych obmedzení (nesvojprávna osoba, osoba menej ako 18 ročná, a pod.). Ak je táto množina neprázdna, posledný prvok množiny bude usporiadaná dvojica typu Osoba, kde Osoba je v tvare [meno, priezvisko]
    - meno je krstné meno zodpovednej osoby :String [20]
    - priezvisko je priezvisko zodpovednej osoby :String [20]
- osoby ktoré majú byť vyrozumené :set of Osoba
- dátum vydania eEHIC :Date
- dátum expirácie eEHIC :Date
- Iné napr. vydávajúci štát, inštitúcia

Keďže v SR je momentálne 7 poisťovní, na určenie tej, kde je pacient poistený, prípadne na určenie, že nemá platný poistný vzťah budú stačiť 3 bity. Treba rátať s potenciálnym príchodom novej poisťovne na trh, prípadne s možnosťou registrácie v zahraničnej poisťovni, preto na zakódovanie rezervujeme 24 bitov.

Na zakódovanie adresy budeme potrebovať 50 B pre ulicu, 12 bitov pre číslo domu, 50 B pre mesto a na PSČ 17 bitov. To je spolu po zaokrúhlení nahor 104 B.

Právne obmedzenia, ak predpokladáme, že možných obmedzení je nanajvýš 16, pomocou 4 bitov jedno. Ak by mal niekto všetky obmedzenia naraz, bude potrebovať 16 * 4 bity, teda 8 B. Okrem toho pridáme 40 B pre zodpovednú osobu. Výsledkom je teda 48 B.

Ak predpokladáme nanajvýš tri uvedené osoby, ktoré majú byť vyrozumené, budeme potrebovať 3 * 40 B, teda 120 B.

Pre oba dátumy bude stačiť 3 + 3 B.

Pre administratívne údaje teda bude potrebné vyhradiť minimálne 300 B.

10.3.3. Zhrnutie pre identifikačné a administratívne údaje

Z uvedeného je zrejmé, že obe tieto skupiny údajov majú malú pamäťovú náročnosť. Pri veľkostiach pamäte dnešných čipov je oveľa rozumnejšie na reprezentáciu týchto údajov použiť vhodný existujúci štandard, napr. XML. Ani pri takejto reprezentácií údajov sa nedá očakávať, že by presiahli veľkosť 4 kB.

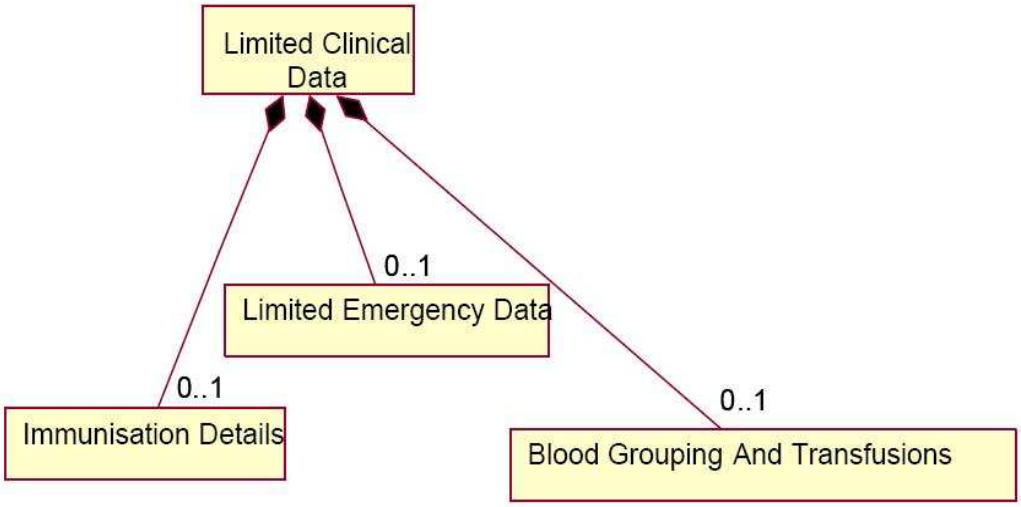
Výber vhodného štandardu na reprezentáciu týchto údajov je mimo rozsahu našej práce. Pri výbere tohto štandardu by bolo vhodné pamätať na to, že je potrebné, aby boli čipové karty občanov SR použiteľné aj v zahraničí. V súčasnosti norma EN ISO 21549 v častiach 5 a 6 rieši priamo problematiku identifikačných a administratívnych údajov na pacientskej čipovej karte. Tieto dve časti v súčasnosti nie sú platnými slovenskými technickými normami (veľmi pravdepodobne však aj tieto budú časom akceptované ako STN).

Zároveň by bolo užitočné, aby Ministerstvo zdravotníctva SR, prípadne iný kompetentný orgán vydal štandard ekvivalentný k Dátovému štandardu Ministerstva zdravotníctva Českej republiky [9] (vzhľadom na blízkosť problematiky odporúčame prevziať tento štandard vcelku, resp. ho prispôsobiť na slovenské podmienky). Tento štandard by slúžil na zjednotenie formátu údajov vo vznikajúcich systémoch eHealth aj v existujúcich systémoch v súčasnosti používaných lekármi, napr. na vykazovanie

výkonov zdravotným poisťovniam. Prijatím takéhoto štandardu by sa zaručila možnosť jednoduchej spolupráce týchto systémov.

10.3.4. Limitované medicínske údaje

Štruktúra navrhovaných údajov v tejto časti podľa STN EN ISO 21549 - 3 je graficky znázornená na obrázku č. 8. Rozdelenie týchto údajov na tri časti umožní nastaviť rozdielne prístupové práva k jednotlivým častiam.



obr. č.8.

Štruktúra limitovaných medicínskych údajov

zdroj: EN ISO 21549-3

Trieda Immunisation Details bude slúžiť na uchovávanie pacientových očkovacích záznamov.

Trieda Limited Emergency Data bude slúžiť na uchovávanie limitovaných údajov urgentnej medicíny. Štruktúra navrhnutá v STN EN ISO 21549 - 3 reprezentuje tieto údaje ako množinu dvojíc: názov alergie (ochorenia, poruchy) a príznak typu boolean určujúci, či pacient je, alebo nie je alergický (trpí daným ochorením, má danú poruchu...).

V prípade, že je príznak pravdivý a sú potrebné podrobnosti, uvedú sa v triede Extended Clinical Data. Presný rozsah a tvar urgentných medicínskych údajov je

mimo rozsahu tejto práce. Preto neuvádzame ani presnejší popis pre triedu Extended Clinical Data. Štruktúra tejto triedy je stanovená normou STN EN ISO 21549 – 4.

Trieda Blood Grouping And Transfusions bude slúžiť na uchovávanie údajov o krvi a transfúziách.

Presnejší popis jednotlivých tried je uvedený v norme STN EN ISO 21549 - 3, a preto ho tu neuvádzame. Na základe štruktúry uvedenej v spomínanej norme predpokladáme, že pamäťová náročnosť limitovaných medicínskych údajov nepresiahne 4 kB pre očkovacie záznamy, 1kB pre údaje o krvi pacienta a 3 kB pre údaje urgentnej medicíny, čo je dokopy 8 kB pre limitované medicínske údaje.

10.3.5. Pamäťová náročnosť pre údaje CA

Na čipe eEHIC bude uložený súkromný kľúč slúžiaci na vyhotovovanie zaručeného elektronického podpisu pacienta. Veľkosť kľúča bude pravdepodobne 2 kB. Na čipe bude uložený aj certifikát CA využívaný v protokole SSL a verejný kľúč CA, aby bolo možné overiť certifikát CA v protokole SSL aj bez pripojenia na internet (aby bolo možné používať čipové karty aj v miestach, kde nie je signál). Z uvedeného vyplýva, že očakávaná pamäťová náročnosť pre údaje CA bude 8 kB.

10.3.6. Celková pamäťová náročnosť

Približná minimálna pamäťová náročnosť na základe výsledkov z predošlých odsekov je 20 kB. Ak aj vezmeme do úvahy možnosť neskoršieho rozširovania údajov na karte, prípadne použitie podrobnejšieho popisu ochorení v triede Extended Clinical Data predpokladáme, že pamäťová náročnosť čipu nepresiahne 64 kB.

10.4. Technické parametre čipu eEHIC

Z dôvodu kompatibility čipu s čítačkami u nás i v zahraničí je nutné, aby čip vyhovoval štandardu ISO/IEC 7816 - 2. Z bezpečnostných dôvodov neodporúčame realizovať eEHIC ako bezkontaktnú čipovú kartu, keďže obsah takejto karty sa dá ľahko skopírovať. Aby mohla byť karta aktívna pri podpisovaní dokumentov je potrebné, aby mala vlastný mikroprocesor a kryptografický koprocesor na urýchlenie výpočtov. Ako sme uviedli v závere kapitoly o pamäťovej náročnosti, bude potrebný čip s kapacitou pamäte 64 kB. Čip by mal byť odolný voči bežným klimatickým podmienkam (rádovo -25 až + 60 stupňov Celzia, odolnosť voči vlhkosti). V prípade, že štruktúra údajov na karte bude založená na štandarde EN ISO 21549, bolo by vhodné použiť operačný systém JAVA^{TM} z dôvodu jednoduchšej implementácie a narábania s objektmi, ako pri súborovo orientovanom operačnom systéme popísanom v ISO/IEC 7816 – 4. Zároveň by mala čipová karta eEHIC spĺňať technickú špecifikáciu uvedenú v [13].

10.5. Životný cyklus karty eEHIC

Z bezpečnostných a aj praktických príčin je potrebné stanoviť dobu platnosti karty eEHIC. Karta sa časom mechanicky opotrebuje, čo by mohlo viesť k problémom v prípade potreby údajov z karty. Zároveň by ale doba platnosti z finančných i praktických dôvodov nemala byť príliš krátka. Navrhujeme preto životnosť karty na 5 rokov. Životný cyklus karty bude vyzerať nasledovne:

1. Nákup kariet od výrobcu
2. Personalizácia karty
3. Distribúcia kariet do regionálnych centier
4. Vydanie karty vlastníkovi
5. Blokovanie (pri strate, na základe oznámenia CA), prípadne expirácia karty
6. Likvidácia (mechanická, aj dátová)

Personalizácia kariet (minimálne jej časť) bude vykonaná certifikačnou autoritou, aby bola zabezpečená väzba medzi dvojicou kľúčov pre zaručený elektronický podpis, a vlastníkom karty. Treba navrhnúť, ako sa identifikačné, administratívne a medicínske údaje dostanú k CA, prípadne treba navrhnúť vhodnú infraštruktúru zabezpečujúcu personalizáciu kariet, s ohľadom na všetky relevantné požiadavky. Karta bude vydaná vlastníkovi v regionálnom centre na základe predloženia dokladov overujúcich jeho totožnosť. Vlastník si kartu bude musieť odblokovať zadaním špeciálneho hesla určeného na tento účel.

Je potrebné zabezpečiť všetky fázy životného cyklu karty eEHIC. Keďže ide o kartu pre približne 5 miliónov používateľov, je potrebné zriadiť potrebnú infraštruktúru a jasne určiť zodpovednosti účastníkov tohto procesu. Návrh a opis tejto infraštruktúry je mimo rozsahu tejto práce.

11. Záver

Naším prvým cieľom bolo analyzovať problematiku poskytovania EDS a poskytnúť prehľad relevantných zahraničných riešení. Ucelený pohľad na túto problematiku sme ponúkli v prvej časti práce v kapitole 4. V rámci piatej kapitoly uvádzame východiskové rezortné dokumenty SR a koncepciu NZIS podľa NCZI. Prínosom tejto časti práce je vytvorenie celkového kontextu pre ďalšie časti práce a bližšie oboznámenie čitateľa s touto širokou problematikou.

Ďalším cieľom bolo navrhnúť základnú štruktúru vhodného riešenia pre sprístupňovanie údajov EDS. V kapitolách 7,8,9 a 10 uvádzame návrh riešenia a podrobnejšie sa venujeme rozsahu a štruktúre údajov uložených na čipe eEHIC. V týchto kapitolách sa zaoberáme vybranými bezpečnostnými a realizačnými aspektmi tohto návrhu. Analyzovali sme problémy, ktoré sa môžu vyskytnúť pri implementácii navrhnutého riešenia a sformulovali sme niekoľko odporúčaní a riešení pre identifikované problémy.

V tejto práci sme narazili na mnoho netriviálnych otvorených problémov, ktorých vyriešenie je mimo rozsahu tejto práce, ale zároveň je nevyhnutným predpokladom, aby mohol byť na Slovensku realizovaný systém poskytujúci EDS. Za najdôležitejšie problémy považujeme nasledovné.

V blízkej budúcnosti je potrebné určiť, ktoré údaje o zdravotnom stave pacienta patria do EDS a navrhnúť, ako budú profesionálom pridelené prístupové práva k týmto údajom. Keďže EDS je súčasťou EHR, nami zvolený návrh vychádza z predpokladu, že pri realizácii systému pre správu EHR občanov SR bude implementovaný mechanizmus umožňujúci spoluprácu nášho riešenia s týmto systémom.

Potrebné budú i legislatívne zmeny, ktoré napomôžu realizácii celého projektu. Nevyhnutným predpokladom pre medzinárodnú interoperabilitu tohto systému je vypracovanie a schválenie oficiálneho slovenského názvoslovia zosúladeného so SNOMED CT.

Za veľmi dôležitú úlohu považujeme definovanie obdoby českého štandardu DASTA [9]. Tento štandard by napomohol zjednoteniu formátov údajov už existujúcich medicínskych systémov a uľahčil by realizáciu nových systémov eHealth, pričom by umožnil ich vzájomnú interoperabilitu.

Ďalšou významnou úlohou je určenie podrobnej infraštruktúry pre zabezpečenie životného cyklu karty eEHIC.

Táto práca má slúžiť ako východisko pre ďalší postup v tejto oblasti. Najbližšími krokmi by mali byť podrobná analýza bezpečnosti, štúdia o finančnej návratnosti, a podrobný návrh systému poskytujúceho EDS.

Stanovené ciele teda považujeme za splnené a veríme, že táto práca bude cenným prínosom k riešeniam v širokej a zatiaľ veľmi otvorenej oblasti informatizácie zdravotníctva na Slovensku. Zároveň táto práca bude prínosom aj pre organizáciu NCZI, ktorá je zastrešovateľom aktivít a iniciatív v oblasti informatizácie zdravotníctva - eHealth.

12. Literatúra

[1] Global eHealth survey 2005, WHO 2005, Geneve

[2] Revolutionizing Health Care Through Information Technology, President's Information Technology Advisory Committee June 2004

[3] e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area dostupná na: http://ec.europa.eu/information_society/doc/qualif/health/COM_2004_0356_F_EN_ACTE.pdf

[4] ICT for Health and i2010 Transforming the European healthcare landscape Towards a strategy for ICT for Health

[5] Sdělovací technika 3/2007 Elektronické zdravotní záznamy a sdílení informací ve zdravotnictví, Ing. Jan Lexa

[6] Domovská stránka spoločnosti IZIP, dostupná na: www.izip.cz

[7] Stránka Európskej komisie pre štúdie o ekonomických dopadoch eHealth systémov, dostupná na: www.ehealth-impact.org

[8] Technické informácie o Health Care Cards od spoločnosti Giesecke-Devrient, dostupné na: http://www.gi-de.com/portal/page?_pageid=42,55042&_dad=portal&_schema=PORTAL.

[9] Domovská stránka pre dátový štandard Ministerstva zdravotníctva ČR, dostupná na: http://ciselniky.dasta.mzcr.cz/

[10] Nové zdravotníctvo: súčasný stav a perspektívy zdravotníckej informatiky v SR. MZ SR 2006

[11] Základy kryptológie, Martin Stanek, v elektronickej podobe na adrese: http://www.dcs.fmph.uniba.sk/~stanek/crypto/main2.pdf

[12] The SSL Protocol**,** Version 3.0 Internet Draft dostupný na: http://wp.netscape.com/eng/ssl3/ssl-toc.html

[13] Official Journal of the European Union 27.10.2003; DECISION No 190 of 18 June 2003 concerning the technical specifications of the European health insurance card

[14] Domovská stránka spoločnosti euser, dostupná na: www.euser-eu.org

[15] Domovská stránka rakúskeho systému ecard, dostupná na: www.chipkarte.at

[16] Domovská stránka dánskej inštitúcie National Board of Health, dostupná na: www.sst.dk

[17] Domovská stránka nemeckého systému gesundheitskarte, dostupná na: www.die-gesundheitskarte.de

[18] Domovská stránka konferencie o eHealth 2006, dostupná na: www.ehealthconference2006.org

[19] Domovská stránka konferencie o eHealth 2007, dostupná na: www.ehealth2007.de

[20] eHealth priorities and strategies in European countries, eHealth ERA report, marec 2007, dostupná na: www.ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf

[21] Domovská stránka dánskeho systému MEDCOM, dostupná na: www.medcom.dk

[22] Domovská stránka dánskeho národného zdravotného portálu, dostupná na: www.sundhed.dk

[23] eHealth – zdravie na internete, I-Europa s.r.o., dostupné na: www.euractiv.sk/lisabonska-strategia/zoznam_liniek/ehealth---zdravie-na-internete

[24]Domovská stránka verejného zdravotného portálu EÚ, dostupná na: http://ec.europa.eu/health-eu/index_en.htm

[25] Domovská stránka Ministerstva zdravotníctva SR, dostupná na: http://www.health.gov.sk/

[26] Stránka Európskej komisie pre najlepšie prebiehajúce projekty v oblasti eHealth, dostupná na: http://ec.europa.eu/information_society/eeurope/ehealth/best_practices/ongoing_projects/index_en.htm

[27]Ľubomír Vlčák, prezentácia NZIS, ITAPA 2007, dostupná na: http://www.itapa.sk/2007/ehealth/Presentation3.pdf

[28] Štúdia uskutočniteľnosti elektronickej preskripcie na Slovensku, Krchňák Š., Sukeľ O., dostupná na: http://www.nczisk.sk/buxus/docs/eHealth/studie/e-Prescription_Krchnak.pdf

[29]Domovská stránka organizácie Europen Health Telematics Observatory, dostupná na: http://www.ehto.org/

[30] Domovská stránka slovenskej koreňovej certifikačnej autority, dostupná na: www.nbusr.sk

[31] Domovská stránka slovenskej akreditovanej certifikačnej autority, dostupná na www.disig.sk

13. Prílohy

13.1. Príloha 1: obsah údajov na priloženom CD

Keďže sme čerpali z mnohých materiálov umiestnených na internetových stránkach, ktoré môžu neskôr daný dokument odstrániť, alebo premiestniť, najdôležitejšie materiály prikladáme na CD v prílohe 2. V tejto prílohe uvádzame pre lepšiu prehľadnosť ich štruktúru. V nasledovných odrážkach stručne popisujeme obsah jednotlivých adresárov.

- Dan – materiály o dánskom národnom systéme
- EC – materiály Európskej komisie
- EDXL – emergency data Exchange language
- EHR – základné informácie o electronic health record
- EU – materiály z rôznych portálov EÚ
- HL7 – základné materiály o štandarde HL7
- ISO – materiály international standardisation organisation
- IZIP – materiály o českom systéme IZIP
- MZSR – materiály získané zo stránok Ministerstva zdravotníctva SR
- NBÚ - zákon o elektronickom podpise a vyhlášky NBÚ týkajúce sa danej problematiky
- NCZI - materiály národného centra zdravotníckych informácií
- Nem – materiály o nemeckom národnom systéme
- Netriedené – netriedené materiály, ktoré sa nedali inde zaradiť
- Rak – informácie o rakúskom národnom systéme
- WHO – materiály World Health Organisation

Okrem toho sa na CD nachádza táto práca v digitálnej podobe.

13.2. Príloha 2: CD s elektronickými materiálmi