УНИВЕРЗИТЕТ СИНГИДУНУМ
ДЕПАРТМАН ЗА ПОСТДИПЛОМСКЕ СТУДИЈЕ
-СТУДИЈСКИ ПРОГРАМ-
Савремене информационе технологије

Заштита здравственог информационог система

- Мастер рад -

Ментор:
Проф. др Младен Веиновић

Студент:
Драго Катић
Бр. индекса: **410035**

Univerzitet Singidunum
Београд, 2015.

Заштита здравственог информационог система

Сажетак

Сажетак: Овај рад описује основне карактеристике здравственог информационог система Републике Србије, затим његове специфичности и разлике у односу на друге такве системе, као и стандарде који дефинишу и одређују такве информационе системе. Поред тога, у овом раду је описано неколико различитих технологија за међусобну аутентификацију клијената и сервера, као и неке од технологија за идентификацију корисника здравственог информационог система. Разматране су различите могућности за имплементацију тих технологија у са идејом да се изгради криптографски систем са инфраструктуром јавних кључева и сопственим сертификационим ауторитетом у изолованом систему који би се реализовао као виртуелна приватна мрежа на инфраструктури Интернета. Поред тога, разматрана је могућност дигиталног потписивања једног дела сервера у оквиру здравственог информационог система са идејом да се на безбедан начин реализују сервиси електронског здравства.

Кључне речи: Здравствени информациони системи, здравствене информационе технологије, здравствени информациони стандарди, аутентификација, чип картице, биометрија, једноструко пријављивање, виртуелне приватне мреже, систем доменских имена са безбедносним проширењима, безбедност података, инфраструктура јавних кључева, е-здравство.

Abstract

Abstract: This article describes main characteristics of the health information system of the Republic of Serbia, then, its specificities and differences compared to other similar systems, as well as standards that define and determine such information systems. Furthermore, in this work are described several different technologies for mutual authentication of clients and servers, as well as some of the technologies for user identification in the health information system. Various options for implementing these technologies have been considered with the idea to build a cryptographic system with a public key infrastructure and its own certification authority in an isolated system that would be realized as a virtual private network on the Internet infrastructure. Besides that, the possibilities of a digital signing on a part of the servers within the health information system have been considered with an idea to safely implement electronic health services.

Keywords: Health information systems, health information technology, health data standards, authentication, smart cards, biometric, single sign-on, virtual private network, domain name system security extensions, data security, public key infrastructure, e-health.

САДРЖАЈ

1. Увод ... 3

2. Здравствени информациони систем ... 6

2.1 Специфичности здравствених информационих система ... 6

2.2 Стратегија развоја здравствених информационих система ... 7

2.3 Информатички стандарди у здравству ... 8

2.4 Уређаји у здравственим информационим системима ... 10

3. Здравствени информациони систем Републике Србије ... 11

4. Електронски сервиси у здравственом информационом систему ... 12

5. Истраживање – прикупљени подаци ... 16

6. Идентификација корисника ... 19

6.1 Заштита података ... 21

6.2 Криптографија ... 22

6.3 Дигитални потпис ... 24

6.3.1 Дигитално потписивање ... 24

6.3.2 Верификација дигиталног потписа ... 25

6.4 Дигитални сертификати ... 26

6.4.1 Структура дигиталног сертификата ... 27

6.5 Инфраструктура са јавним кључевима ... 28

6.6 Безбедносни протоколи ... 29

7. Аутентификација корисника ... 31

7.1 Аутентификација заснована на корисничким именима и лозинкама ... 31

7.2 Аутентификација заснована на чип картицама ... 33

7.2.1 Микропроцесорске картице и инфраструктура јавних кључева ... 36

7.3 Аутентификација (идентификација) заснована на биометрији ... 38

8. Једноструко пријављивање корисника ... 41

8.1 Клијентски и кориснички налози ... 41

8.1.1 Клијентски налози ... 42
8.1.2 Кориснички налози ... 43
9. Аутентификација сервера ... 45
9.1 Систем доменских имена ... 46
9.2 Безбедносни проблеми ... 49
9.3 Безбедносна проширења ... 49
9.3.1 Имплементација у здравственом информационом систему ... 52
10. Виртуелне приватне мреже ... 55
10.1 Значај виртуелних приватних мрежа ... 55
10.2 Тунелска комуникација ... 56
10.3 Point-to-point Tunneling Ptorotocol ... 57
10.4 Layer 2 Tunneling Ptorotocol ... 58
10.5 Безбедносни Интернет протокол и систем доменских имена ... 59
11. Управљање криптографским кључевима ... 61
11.1 Управљање кључевима у симетричној криптографији ... 61
11.2 Управљање кључевима у асиметричној криптографији ... 63
11.3 Протоколи за дистрибуцију криптографских кључева ... 66
11.3.1 Diffie – Hellman протокол ... 66
11.3.2 Needham – Schroeder протокол ... 67
11.3.3 Otway – Rees протокол ... 69
11.4 Управљање криптографским кључевима у здравственом информационом систему ... 70
11.5 Керберос протокол ... 71
11.5.1 Аутентификација на основу Керберос протокола ... 71
11.5.2 Размена кључева на основу Керберос протокола ... 72
12. Закључак ... 75
Литература ... 78
Списак слика ... 80
Списак табела ... 80

1. Увод

Интелектуални капитал, квалитетни и безбедни токови информација и смислено и сврсисходно реализовани информациони системи представљају најзначајније информационе и организационе ресурсе сваке организације. Употреба информационо комуникационих технологија и информационих система у здравству повећава ефикасност и доприноси већој тачности када је у питању скупљање и обрада података, као и већој једноставности када је у питању приступање подацима. Здравствене организације у Републици Србији највећи део својих података чувају у здравственим картонима који су складиштени у картотекама. Тако ускладиштеним подацима се мора приступати физички и само на оном месту где се ти картони чувају, што је веома неефикасан систем. На тај начин се обезбеђује мали скуп података који је доступан на једном месту и који је уско везан за одређену патологију, што не може да пружи увид у ширу слику обољења. То може довести до постављања нетачне дијагнозе и до погрешног лечења. Поред тога, услед бројних догађаја који се одиграју у периоду чувања здравствених картона, некада долази до нестанка или оштећења документације.

Здравствени информациони системи у организацијама које су обухваћене овим истраживањем су у почетним фазама развоја. Они постоје и постоји тенденција да се подаци дигитализују, као и да се учине доступним, али постоје и бројни проблеми који то успоравају и који су највећим делом везани за недостатак финансијских средстава. Увођењем електронских здравствених картона би се значајно изменио начин рада и значајно би се изменио постојећи здравствени систем, а тако би се омогућило брже и тачније постављање дијагнозе, самим тим и квалитетније лечење. То би била директна последица повећане доступности података и тако би сви аутентификовани и ауторизовани корисници здравственог информационог система били у могућности да приступе личним здравственим подацима грађана и могли би да донесу квалитетније одлуке на основу тих података, такође, лекари би, у оквиру свог посла, допуњавали постојеће податке и омогућавали квалитетније постављање нових дијагноза што би омогућило и квалитетније лечење у будућности.

Здравствени информациони систем у Републици Србији чине модули који би у будућности могли постати део јединственог здравственог информационог система. Већ постоји јединствен став о томе који подаци су потребни, у ком облику треба да се чувају и на који начин се шаљу на сервере где су централизовани, али још увек не постоји развијен информациони систем који би могао да обједини све модуле како би се постигло оптимална и функционална организација осталих ресурса у оквиру здравствених организација уз, истовремено, смањење трошкова, ако за то постоји могућност. По угледу на друге сличне информационе системе, а уз поштовање демографских и културних карактеристика нашег поднебља, могуће је направити систем који би објединио све модуле и информатички подржао пословне процесе у здравству. Здравствени информациони систем би на различите начине могао да располаже подацима о нематеријалним ресурсима, о корисницима медицинских услуга, о медицинском и немедицинском особљу и о бројним другим материјалним ресурсима и да као такав допринесе оптимизацији радних задатака и рационалнијем ангажовању постојећих ресурса.

Постојећи информациони систем није предвиђен да прави поделу особља према постојећој систематизацији послова, али би имплементацијом такве пословне логике могао да се направи оптимални распоред рада и дежурства. Поред тога, здравствени информациони систем би могао да се употреби за одређивање оптималних распореда за употребу материјалних ресурса као што су просторије за лечење, или медицински уређаји. Обзиром на то да је посао медицинског особља организован у односу на временске норме за пружање различитих здравствених услуга, могуће би било направити модуле који би уређивали листе чекања на заказане прегледе.

Највећи проблем постојећег здравственог информационог система јесте велика децентрализација података. Уколико постоје медицински подаци који су доступни само у оквиру једне здравствене организације, онда то деградира смисао тог информационог система јер на такав начин не помаже здравственим радницима да донесу квалитетне одлуке, као што би могли када би располагали резултатима квалитативних анализа здравствених података пацијената. Уколико пацијенти, ван свог места пребивања морају да се јаве некој здравственој организацији, најчешће не добију квалитетне здравствене услуге, и поред стручних и искусних здравствених радника, јер нису у могућности да довољно прецизно опишу своје здравствене проблеме, а лекари немају податке на које могу да се ослоне. Веома су стресне ситуације у којима је потребно пружити хитну медицинску помоћ, а једини извор података представљају изјаве пацијента.

Постојање јединственог републичког здравственог информационог система са централизованим подацима би смањило потребну количину прегледа, јер би постојали доступни подаци о претходним прегледима. Поред тога, смањила би се могућност за појаву грешака, повећао би се квалитет дијагностике и терапије, као и могућности за рану дијагностику. Такође, то би омогућило и квалитетну анализу података на основу чега би се могли добити подаци који су значајни за утврђивање здравственог стања комплетног становништва. Постојеће информационо комуникационе технологије пружају бројне могућности, међутим оне нам не представљају користан ресурс уколико не постоји контрола над њима. Комуникација коју не можемо да задржимо у тајности, или Интернет ресурси којима не можемо да располажемо по сопственој вољи не представљају ресурсе на које можемо рачунати. Потенцијал Интернета можемо искористити једину уколико смо у могућности да применимо различите сигурносне механизме за контролу приступа и за заштиту комуникације. Развој здравственог информационог система на инфраструктури Интернета није ни мало лак задатак јер је потребно направити добар систем заштите који би превентивно деловао у случајевима неовлашћеног приступа, или услед намерног нарушавања приватности, компромитовања података, услед појаве малициозних програма, нестручног руковања, неодговорног понашања корисника и слично.

Напади могу настати од стране корисника информационог система, намерно, или случајно. Превентивно деловање када је у питању неки такав сценарио није једноставно јер је ограничено, првенствено због тога што корисници морају располагати одређеним нивоом слободе, односно одређеним привилегијама како би обављали своје радне задатке. Са друге стране, превентивно деловање у случају злонамерних напада из окружења нема таквих ограничења, али ту постоји проблем услед немогућности да се предвиде врсте, начини и учестаности напада и због тога представља област над којом је потребно преузети контролу како би се изградио безбедни информациони систем.

Напади могу бити различити, некада се односе на прислушкивање, односно на надгледање саобраћаја без утицаја на садржај порука, а некада су то напади који се односе на мењање садржаја порука од стране неауторизованих корисника, односно уклањање постојећих, или убацивање нових порука, или једноставно прекидање комуникације. Поред поменутих, постоје напади који се могу реализовати тек након лажног представљања корисника. Ту проблематика постаје сложенија због тога што такав корисник, након што успе да превари систем, може да направити велику штету. Он се може представити као неко ко у стварном свету не постоји, али и као особа која постоји и да при томе направи додатне проблеме особи чији идентитет је искористио за превару. Све ово утиче на стварање бројних предрасуда када је у питању развој и имплементација информационих система заснованих на Интернет инфраструктури. Забринутост је оправдана, али свест о постојању могућих ризика и адекватне мере заштите којима се стварни ризици могу свести на минимум представљају оптимални приступ решавању проблема.

Немогуће је направити информациони систем који би био апсолутно безбедан, али је могуће употребити различите безбедносне механизме и системе и реализовати систем који је веома тешко преварити, или злоупотребити. Тајност комуницирања се може постићи шифровањем, аутентичност, односно идентитет учесника у комуникацији се може утврдити на основу разних система аутентифиакције, могуће је потврдити интегритет поруке и могуће је обезбедити механизме непорецивости, односно механизме који могу спречити пошиљаоца поруке да порекне слање поруке, или да порекне да је креирао садржај те поруке. Дигитални потпис је тренутно најзаступљенији механизам којим се могу имплементирати сви поменути безбедносни механизми и на основу ког се може реализовати контрола приступа уз адекватну идентификацију корисника информационог система.

2. Здравствени информациони систем

Светска здравствена организација (енгл. *World health organization*) здравствене информационе системе дефинише као системе који се баве статистиком у здравству са циљем унапређивања локалне, регионалне и глобалне информисаности у здравству. Поред тога, информације које пружају здравствени информациони системи су значајне за доносиоце одлука у областима постављања дијагноза, затим за ангажовање медицинских ресурса и за праћење и анализирање прикупљених података. Светска здравствена организација даје свој допринос ка унапређењу здравствених информационих система кроз глобалну анализу здравља (енгл. *Global Health Observatory*) и кроз уступање статистичких или аналитичких података другим здравственим организацијама, затим постављањем стандарда, алата и метода за прикупљање података и за њихову употребу, као и кроз унапређење сарадње између различитих земаља у области здравства и усклађивањем карактеристика информационих система како би они могли да коегзистирају.

Светска здравствена организација је посебна организација уједињених нација која, уколико се изузму велике корпорација које послују у области здравства, делује као један од најзначајнијих координатора јавног здравства. Светска здравствена организација у основи има мисију да доведе људе на највиши могући ниво физичког и менталног здравља и спокоја. Обзиром да јој стицање профита није примарно, а ни услов за њен рад, може се претпоставити да су циљеви ове организације исправни и да би требали истовремено бити и циљеви свих здравствених организација. Такође, важно је напоменути да ова организација највећи део средстава којим располаже улаже у истраживања из области здравства и да сви ми директно и индиректно имамо користи од тога, као и то што је један од задатака ове организације обавештавање здравствених радника и људи о новостима и променама у области здравства.

Здравствени радници и корисници здравствених услуга би могли да искористе пун потенцијал здравствених информационих система уколико би настала глобална интеграција свих целина различитих здравствених информационих система. Ови системи би могли да се информативно допуњују па би се на основу великих скупова података и узрочних веза између њих формирале довољно прецизне информације. Такви системи оправдавају своју улогу тек када се у њих интегришу бројни појединачни подсистеми, на пример: истраживачке лабораторије и истраживачки центри, статистички подаци из различитих земаља, подаци добијени из рада лекара, снимци са различитих дијагностичких уређаја и друго. Због тога је важно поштовати стандарде јер то омогућава интеграцију програмских модула у веће целине, подржавање свих процеса медицинске праксе и усклађивање здравствених информационих система са законским прописима Републике Србије у области информатике у здравству.

2.1 Специфичности здравствених информационих система

Значајан развој информационо комуникационих технологија је у великој мери утицао на промену навика у пословању, комуницирању и у међуљудским односима. Интернет технологије су по својој употребној вредности одавно превазишле своју тржишну вредност и постале су неизоставни део наших живота. Међутим, иако је

идеја о предностима употребе савремених информационих система одавно присутна, оне још увек нису заступљене у довољно великој мери. Разлози за то су бројни, али је један од најуочљивијих тај што не постоје стандарди који су општеприхваћени.

Здравствени информациони системи имају бројне специфичности које их карактеришу. Једна од најзначајнијих карактеристика је та што овакви системи треба да подрже пословне процесе на начин који би омогућио здравственим радницима да обављају свој посао без нарушавања принципа професионалне дискреције, односно да принципе професионалне дискреције буду имплементирани у функционалности здравствених информационих система. Складно томе, подела медицинске заштите на целине, која је последица медицинске праксе, треба да буде модел по ком би требало направити логичку поделу функционалности у здравственим информационим системима. Тиме би се добили подсистеми који подржавају примарну медицинску заштиту, затим приватну праксу, апотеке, хитне помоћи, пацијенте, министарства, Републички завод за здравствено осигурање, Републички завод за статистику и друге.

2.2 Стратегија развоја здравствених информационих система

Светска здравствена организација је дефинисала Стратегију развоја здравствених информационих система. На основу те стратегије су у Републици Србији постављени неки од стратешких и оперативних циљева са намером да се реше проблеми који су у вези са развојем здравственог информационог система и да се поставе стандарди којима ће се тежити приликом развоја информационих и комуникационих технологија у здравству. Међутим, још увек нису постигнути жељени стандарди. Најчешће помињани разлози, због којих није више учињено на остваривању циљева, су у вези са недостатком финансијских средстава, затим у вези са одсуством иницијативе у виду пројеката од стране Министарства здравља Републике Србије и у вези са отпором према увођењу електронских картона који у различитим облицима постоји код самих здравствених радника.

Поменута Стратегија претпоставља да би пацијенти требали да буду у фокусу интересовања. Они треба да буду третирани као равноправни и одговорни учесници у процесу бриге о сопственом здрављу и који би требали да буду информисани о питањима везаним за њихово здравље. Ово је нарочито значајно када је у питању превентивно деловање обзиром и на то да су трошкови одржавања доброг здравственог стања мањи од трошкова лечења. Такође, уколико се посвети довољно времена едукацији пацијената, они могу постати корисници бројних сервиса за пружање здравствених услуга на даљину, што би било ефикасно и економично решење у ситуацијама када пацијенти нису у могућности да физички буду присутни у некој од ординација.

Употреба дигиталног потписа од стране медицинског особља је најзначајнији фактор у односу на безбедност здравствених информационих система и у односу на његову функционалност. Дигитално потписивање докумената приликом коришћења здравствених информационих система би омогућило да се свака лекарска активност евидентира и то би представљало доказ о тим активностима, како у информатичком смислу, тако и у правном смислу. То би била велика предност у када је у питању преузимање заслуга и одговорности за обављање лекарског посла.

Један од значајнијих циљева везаних за имплементацију пословне логике у здравствени информациони систем се односи на стандардизацију карактеристика и функционалности које би требале да буду интегрисане у њега: од типова података, шифри лекова, шифри дијагноза, преко лекарских шифри, па до медија који ће се користити за складиштење података. Стандардизација би требала да омогући несметани развој и интеграцију свих делова овог система: амбуланте, хитне помоћи, домове здравља, болнице и клиничке центре, а затим и неке од додатних система у здравству укључујући Министарство здравља Републике Србије, Институте за јавно здравље, агенције за лекове, фондове за здравствено осигурање, апотекарске установе, лабораторије, односно све организације које учествују у пружању здравствених услуга, или на неки други начин учествују у здравственом систему.

2.3 Информатички стандарди у здравству

Обзиром на то да већ дужи низ година постоје различите верзије здравствених информационих система, појавиле су се и различите верзије стандарда који уређују ову област. Одавно постоје специфичне скраћенице које се користе како би се једноставније класификовали подаци: МКБ10, односно домаћи шифрарник болести усклађен са светском класификацијом болести, затим ICPC-2 (енгл. *International Classification of Primary Care, Second edition*), DRG (енгл. *Diagnosis-related group*) систем класификације болести са 467 различитих група болести, или стандардни шифрарник који користи Републички завод за здравствено осигурање. Поред тога у здравству постоји специфична медицинска терминологија и посебна класификација медицинских израза. Најчешће заступљена класификација носи назив SNOMED CT (енгл. *Systematized Nomenclature of Medicine - Clinical Terms*) и представља систематски организован скуп медицинских кодова, термина, синонима, и дефиниција које се користе у медицинској документацији и извештајима.

Здравствени информациони системи се пројектују у складу са стандардима који се односе на информатичке моделе. Најраспрострањенији стандард у Европској Унији је HISA (енгл. *Health Informatics Service Architecture*) стандард који обезбеђује смернице за развој информационих система у здравству, односно смернице за развој апликација и база података кроз дефиницију хардверских, софтверских и комуникационих карактеристика. Поред овог стандарда, заступљен је и openEHR (енгл. *Open Electronic Health Records*). То је стандард који описује организацију, прикупљање, обраду и размену здравствених података. Он је производ истоимене непрофитне организације *openEHR Foundation* и настао је као последица сарадње Европских и Аустралијских стручњака. Он дефинише различите демографске карактеристике, клиничке токове лечења и људске архетипове, али овај стандард нема све значајне карактеристике светског здравственог стандарда и није прихваћен на глобалном нивоу за разлику од стандарда HL7.

Стандард HL7 (енгл. *Health Level Seven*) је креиран од стране непрофитне организације *Health Level Seven International* која је акредитована од стране ANSI (енгл. *American National Standards Institute*). На основу овог стандарда је направљен свеобухватан оквир (енгл. *Framework*) под истим именом. Овај оквир је намењен обради електронских здравствених информација. Њега легално могу да користе сви у временском периоду до три месеца након чега је неопходна лиценца за даљу употребу. Иначе, по речима његових твораца, HL7 је направљен са циљем да буде најбољи и најшире заступљен стандард у здравственим информационим системима.

Овај стандард је пројектован тако да повећа квалитет здравствених услуга, да оптимизује послове и да поспеши трансфер знања и здравствених информација између свих заинтересованих страна.

Сви постојећи стандарди су настали на основу претходних стандарда или система и који су у одређеној мери представљали основу за њихов развој. PACS (енгл. *Picture Archiving and Communication System*) је један од таквих стандарда и он дефинише принципе и правила за економично складиштење и једноставан приступ различитим снимцима са медицинских дијагностичких уређаја у електронској форми, уместо уобичајеног начина чувања папирних, или микрофилмованих снимака. Универзални формат за PACS снимке је DICOM (енгл. *Digital Imaging and Communications in Medicine*), а сви остали подаци који нису снимци чувају се у изворним форматима, на пример *.pdf (енгл. *Portable Document Format*) који су енкапсулирани у DICOM формат.

Поред дефиниција за различите снимке са рендгенске, ултразвучне, или са магнетне резонанце, PACS дефинише и протоколе за размену података о пацијентима путем различитих мрежа, затим хардверске и софтверске компоненте за повезивање дијагностичких медицинских уређаја у здравствени информациони систем, као и хардверске и софтверске компоненте за складиштење и тумачење дијагностичких медицинских података. Наравно, имплементација оваквог система подразумева да медицински уређаји имају одговарајуће интерфејсе у складу са PACS системом. Као и други стандарди, и DICOM стандард обезбеђује компатибилност између различитих информационих система који су реализовани у складу са њим. Власник свих права везаних за овај стандард је *The National Electrical Manufacturers Association* и ова организација је једина која ради даље на његовом развоју и усавршавању.

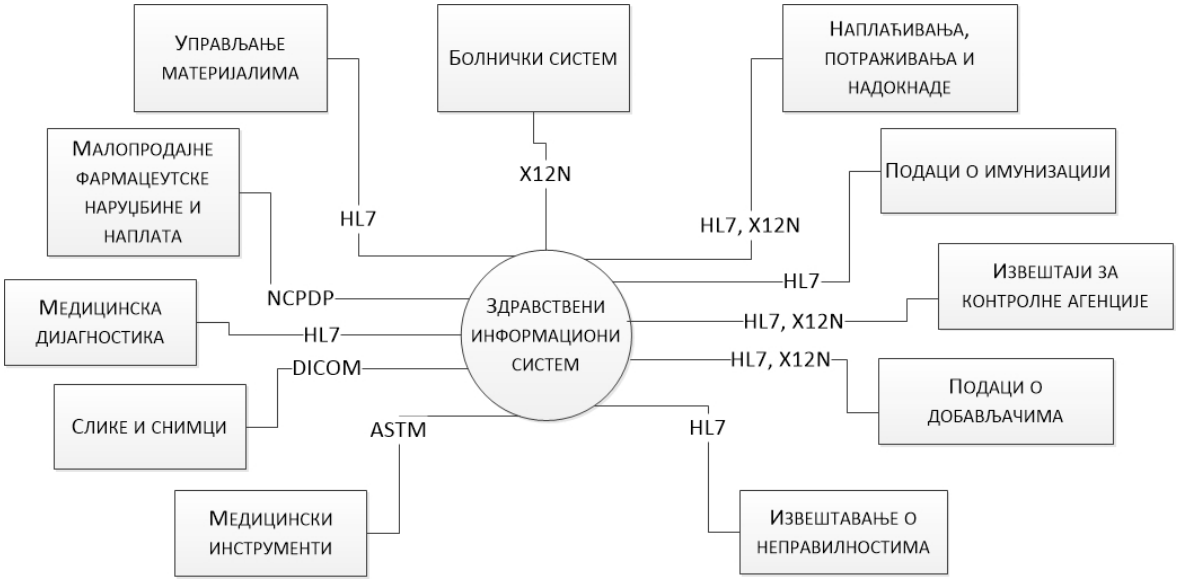
Стандард ASC X12 постоји од 1979. године и представља јединствени индустријски стандард за интерну размену електронских података. Овај стандард је признат од стране Америчког националног завода за стандардизацију (енгл. *American National Standards Institute*). На свом почетку је коришћен у Америци, а данас се користи широм Света. Овај стандард развија организација под називом ASC X12. Он је своју примену нашао у здравственим информационим системима у трансакцијама података који су у вези са здравственим осигурањем што је и логично када је у питању подручје Сједињених америчких држава обзиром да је код њих већ дужи временски период заступљен у комуникацији између осигуравајућих друштава која тамо имају значајан утицај на здравствено осигурање укључујући и обједињавајући све активности у вези са имовином, несрећама, здравственом заштитом, животним осигурањем, пензијама, извештајима намењеним различитим контролним агенцијама и слично.

Највише стандарде у здравству прописује организација под називом *ASTM International*, односно Америчко друштво за тестирање и испитивање материјала, ASTM (енгл. *American Society for Testing and Materials*). Ови стандарди прописују и предлажу широк дијапазон техничких карактеристика за велики број различитих материјала, производа, система, или сервиса. Стандарди које прописује *ASTM International* нису обавезујући, али су свакако стандарди којима треба тежити првенствено због чињенице да је човек, његова безбедност и његово ментално и физичко здравље један од најважнијих циљева приликом њиховог дефинисања. Најзначајнији критеријуми које прописује ова организација су у вези са стандардима

који дефинишу методе научних истраживања, затим стандардима који дефинишу добру праксу кроз редоследе операција уз мерење и упоређивање добијених резултата, стандарде који дефинишу начине и правце сакупљања информација, као и стандарде који дефинишу стручне термине.

2.4 Уређаји у здравственим информационим системима

Стандарди који дефинишу датотеке у којима се чувају дијагностички подаци утичу и на избор потребне опреме и дефинишу техничке карактеристике уређаја. Зависно од типа и области здравствене заштите, потребни су уређаји различитих карактеристика. Станица за примарну дијагностику на радиологији би требала да имају мониторе минималне резолуције 2500 X 2000 пиксела, а приказ снимака би морао бити адекватног квалитета по питању боја, контраста и осветљења. То би требали да буду уређаји са квалитетном софтверском подршком, који би били оспособљени за аутоматско подешавање приказа и за аутоматску калибрацију боја. Са друге стране, некада није пресудно посматрати снимке високе резолуције већ је важније имати више мањих снимака које треба посматрати истовремено, као што је у случају снимака са рендген апарата. Није могуће правити компромисе на рачун квалитета и функционалности због чега је неопходно располагати адекватном информационо медицинском опремом. Опет, није неопходно у свакој ситуацији употребљавати наменске и високо софистициране технологије. Највећи део потреба за информационо медицинском опремом је могуће задовољити уз помоћ стандардне компјутерске опреме.



Слика 1 Здравствени информациони систем

3. Здравствени информациони систем Републике Србије

Република Србија има здравствени информациони систем, али се за њега не може рећи да оправдава свој назив, јер није потпуно имплементиран и делови овог система нису у директној међусобној вези, већ ту везу остварују посредно преко Института за јавно здравље Србије. Институт за јавно здравље Србије „Др Милан Јовановић Батут“, Републички фонд за здравствено осигурање и Републички завод за здравствено осигурање су до сада имали централну улогу у развоју здравственог информационог система код нас. Ове организације су у претходном периоду радиле на развоју овог система са намером да очувају и унапреде јавно здравље и да одрже квалитет здравствене заштите, тако што би, уз бољу информатичку подршку, повећали ефикасност рада здравствених установа и оснажили сарадњу између различитих сектора. Недостатак потребних ресурса и одсуство системске подршке од стране Републике Србије су у великој мери успорили развој и имплементацију здравственог информационог система.

Медицински подаци који се у Републици Србији прикупљају посредством мреже института и завода за јавно здравље, прикупљају се на основу законске и подзаконске регулативе која је углавном неадекватна и застарела. Највећи део података у здравственим установама се прикупља у папирној форми, након чега се доставља окружним институтима и заводима где се врши дигитализација уносом у различите електронске документе, или директно у базе података. Ти подаци се достављају Институту за јавно здравље Србије и на основу њих се формирају републичке здравствене базе података. Од Републичког завода за статистику Србије се преузимају подаци о становништву, о броју рођених и умрлих, а од Републичког фонда за здравствено осигурање подаци о осигураницима и о финансирању здравствене заштите.

На основу тога се развија пет тематски различитих база података. База података о основним ресурсима здравственог система садржи податке о организационој структури, о кадровима и о медицинској опреми, друга база садржи податке о раду здравствених установа и о здравственој заштити становништва, трећа о здравственом стању становништва: морбидитет, морталитет, заразне болести, болести од већег социјално медицинског значаја, четврта податке о квалитету рада здравствених радника и о задовољству пацијената и задовољству запослених у здравственим установама и пета у коју се смештају подаци о различитим медицинским номенклатурама и класификацијама.

Постојање овог информационог система, и ако још увек некомплетног, је свакако велика предност у поређењу са сакупљањем и обрадом података у некој другој форми. Њега карактерише дуга традиција прикупљања, обраде и употребе здравствено статистичких података. Међутим, постојећи здравствени информациони систем се, претежно, темељи на застарелим методологијама и алатима, уз то, подељен је на мноштво сегмената који нису међусобно усклађени ни компатибилни. Све то заједно не даје довољну количину података и не пружа могућности за квалитетније анализе и добијање квалитетних информација ни пројекција. Поред тога, организација информатичких послова се може окарактерисати као застарела, уз то што ни само информатичко особље није довољно стручно. Такође, мали број запослених здравствених радника је оспособљен за рад на компјутерима.

4. Електронски сервиси у здравственом информационом систему

Електронско здравство подразумева употребу различитих комуникационо информационих технологија у систему здравствене заштите са циљем да се побољша квалитет медицинских услуга путем повећања ефикасности пословних процеса које реализују учесници у том систему. Обзиром на његове карактеристике, е-здравство можемо посматрати као подсистем здравственог информационог система који имплементира уобичајене здравствене процесе тако да се они реализују на даљину, или са удаљених места. То обухвата пружање здравствених услуга на даљину, затим различите видове електронских консултација, даљинску дијагностику, надзор физиолошких параметара код пацијената који се налазе изван здравствених установа, затим конзилијуме између здравствених стручњака путем електронских конференција, као и обуку и образовање медицинских стручњака, ванболничког особља и корисника здравствених услуга.

Имплементација е-здравства смањује трошкове комуникације, транспорта, администрације, едукације, и умањује бројне проблеме и потешкоће које имају корисници здравствених услуга. Е-здравство, такође, повећава транспарентност када је у питању рад здравствених организација чиме се смањује простор за злоупотребу. Међутим, најважнији ефекти е-здравства би се огледали у томе што би пацијенти, путем различитих сервиса и без изласка из куће, могли да стекну увид у расположиве здравствене услуге и да у зависности од здравственог осигурања, или од подршке различитих фондова, пронађу најбољи начин да започну и реализују лечење. Такође, били би у могућности да стекну увид у сопствено здравствено стање и да размотре различите алтернативе за лечење уколико су довољно информисани, односно уколико већ имају слична искуства.

Администрација Сједињених Америчких Држава је 2004. године објавила стратешки план за изградњу здравственог информационог система са циљем да се прикупе медицински подаци о сваком њиховом становнику у форми електронског здравственог досијеа. Убрзо након тога, Америчко министарство здравља (енгл. *Department of Health and Human Services*) је објавило стратегију креирања тог информационог система и започело сарадњу са бројним субјектима који су дефинисали, или донели неопходне стандарде за његов развој и имплементацију. Аналитичари су тренутак за почетак овог пројекта окарактерисали као добар, развој информационо комуникационих технологија је достигао довољан ниво, а у пројекат су биле укључене све релевантне правне и безбедносне институције. Међутим, и тада, као и данас, недостајало је поверење становништва у један такав систем. Крајњи корисници овог система су сумњали у исправност мотива заинтересованих страна (енгл. *Stakeholders*) и поред тога што су у систем биле укључене различите организације за заштиту права грађана.

Здравствени информациони систем Републике Србије се налази пред сличним проблемима као што су се налазили системи из развијенијих земаља. Наш здравствени систем као главни носилац информације подразумева папир који се мора физички преносити са једног места на друго. Чест је случај да особље које треба да преноси здравствену документацију има превише обавеза и да пацијенти чекају сатима на њих. Употреба савремених информационих технологија у здравству би суштински променила положај пацијента и његову улогу у процесу лечења, од пасивног објекта до активног учесника. Уместо традиционалног схватања лечења, где чекање на лечење и излечење зависи од разних утицаја: добре воље медицинског

особља, стручности лекара, или ћудљивости бирократизованог здравственог система, савремено схватање и употреба савремених технологија, први пут у историји човечанства, стварно помажу обичном човеку и омогућавају му да добије квалитетније медицинске услуге и да самостално доноси одлуке о свом лечењу и да прати и контролише ток свог лечења.

Савремени концепт пружања здравствених услуга, где особа сама одлучује о начину свог лечења је велики изазов за све учеснике у овом систему у Републици Србији. Примена савремених информационо комуникационих технологија и разних медицинских технологија значајно утиче на квалитет пружања здравствених услуга, а сада живимо у времену када су се испунили сви потребни услови за реализацију здравственог информационог система. Иницијативом Уједињених Нација, 2010. године је већина савремених држава поставила себи миленијумски циљ да сваком свом становнику обезбеди широкопојасни приступ Интернету, што је код нас већим делом постигнуто. 2013. године је Министарство здравља Републике Србије предложило Влади Републике Србије да измени Закон о здравственом осигурању и да рок за увођење електронских здравствених књижица промери са 2014. године, на 2016. годину. Као разлог за одлагање је наведено то што би сада било физички и финансијски немогуће применити норме Закона о здравственом осигурању.

Остављена је могућност да они који то желе, могу да замене своје папирне здравствене књижице, новим електронским, уз напомену да поседовање електронске здравствене књижице није законска обавеза. Зависно од категорије становништва којој припадају, становници Републике Србије могу преузети електронске здравствене књижице бесплатно, или уз накнаду, уколико немају право на бесплатне књижице. Наравно, то не представља целовито решење, али како наводе представници Министарства здравља, тренутно постоје већи приоритети у здравству на које треба да се одговори и напомињу да ће се поједноставити процедуре употребе папирних здравствених књижица. Са оваквим ставом од стране Министарства здравља пролазе године док се листе чекања повећавају и док се време чекања на неке прегледе мери месецима.

Пракса здравствених организација је показала да се увођењем електронских здравствених књижица и електронских здравствених картона административни пут своди на најмању могућу меру и да се добија тачан увид у пружање здравствених услуга и трошкове које то производи. Такође, смањују се грешке у дефинисању шифри дијагноза и лекова, а Републички завод за здравствено осигурање и друге релевантне организације тренутно могу да приступе свим потребним подацима за обрачун, наплату, анализу, и слично. Обзиром на чињеницу да дигитализација администрације постиже вишу ефикасност уз значајне финансијске уштеде до сада су се независно, најчешће као пилот пројекти, развили различити здравствени информациони системи од којих је најзапаженији информациони систем који развија Дом здравља Врачар.

Дом здравља Врачар поседује здравствени информациони системом и своје медицинске и немедицинске активности свакодневно евидентира употребом различитих информационо комуникационих технологија и свакодневно доприноси даљем развоју електронског здравственог картона и савременог система бележења информација у здравству. Овај информациони систем је резултат заједничког ангажовања Министарства здравља и Републичког завода за заштиту здравља, а настао је према важећим стандардима Европске уније и под покровитељством Европске Уније. Интерно истраживање у овој здравственој организацији је показало

да се велики део радног времена утроши на испуњавање разних образаца, од 30% када су у питању лекари, до 70% када су у питању медицинске сестре што није ефикасно. По новом систему, одмах након пријављивања пацијента на шалтер, податак о томе се евидентира и креира се листа чекања по којој лекар прозива пацијенте и приступа подацима из електронског здравственог картона пацијента.

Овим приступом, у складу са препорукама Европске Уније, створени су тимови лекар – медицинска сестра. То омогућава да лекар интервјуише и прегледа пацијента, док медицинска сестра уноси опште податке, односно да лекар преписује терапију или упуте за даље специјалистичке прегледе, док медицинска сестра обрађује документацију. На овај начин се само једном евидентирају потребни подаци од стране лекара и медицинске сестре у тиму, и то на месту где се одвија сам преглед. Оваквим приступом се пацијентима скраћује период чекања и побољшава се квалитет здравствене услуге. Примена електронског здравственог картона не мења трајање прегледа, већ мења однос у корист ефективног времена које лекар посвећује свом пацијенту.

Проблеми који настају услед дугог чекања на специјалистичке прегледе су делимично решени системом за заказивање прегледа. Међутим, тај систем још увек није заживео у мери у којој би испунио своју сврху. Када су у питању велики болнички центри и специјалистичке болнице, проблем вишемесечног чекања на прегледе је још увек присутан. Недостатак ресурса у виду људства и техничких дијагностичких средстава је највећим делом узрок за то, али уколико би постојала јединствена и транспарентна листа чекања за све пацијенте, постојећи ресурси би могли боље да се искористе. Исто важи и за оне који чекају сложене хируршке захвате, или органе за трансплантацију. Транспарентност је и у овом случају кључан појам јер сви имају право да буду квалитетно информисани, наравно, уз поштовање права пацијената на приватност. Поред тога, људи имају право да буду медицински збринути на најбољи могући начин, а да при томе претрпе што је могуће мање непријатности.

Слика 2 Електронско здравство

Праћење здравственог стања пацијената уз помоћ различитих мобилних уређаја, првенствено уз помоћ савремених мобилних телефона, односно паметних телефона (енгл. *smartphone* или *smart phone*) може значајно допринети ефикасности и успешности лечења пацијената и раној дијагностици уз истовремено смањивање

трошкова лечења и трошкова превентивног деловања. Поред наведених предности, овакви системи значајно олакшавају посао лекарима и значајно смањују време реаговања здравствених радника у хитним ситуацијама. Поред тога, сами лекари огу са удаљених места приступати електронској медицинској документацији својих пацијената путем мобилних мрежа, или путем Интернета. Наравно системи који би омогућили овакве сервисе би морали бити адекватно заштићени како би се омогућила поверљивости и доступност података и безбедна комуникација између система и корисника система у реалном времену. Људи већ имају навику да носе са собом своје мобилне уређаје, а уколико би се ти уређаји искористили у сврху праћења здравственог стања пацијената лекари би могли да једноставно надгледају своје пацијенте и да располажу великом количином података о кључним догађајима и о ситуацијама које повољно или неповољно утичу на здравље пацијената.

Пружање здравствених услуга посредством мобилних уређаја је посебно значајно због веома ниских трошкова који су везани за такав вид лечења. Лични контакт пацијента и лекара је незаменљив, али било каква комуникација у процесу лечења или у процесу одређивања дијагноза је од великог значаја и свакако је боља од одсуства комуникације. Ово је нарочито значајно када су у питању здравствени системи неразвијених земаља, или земаља у развоју. Бројни су уређаји који се могу користити у ову сврху и свима им је заједничко то да морају бити компатибилни са информационим системом и непрестано или периодично повезани на њега. Првенствено су у питању наменски медицински уређаји за евидентирање физичких параметара у сврху праћења здравственог стања пацијената, поред њих су у све већем обиму заступљени мобилни телефони, мобилни компјутери (енгл. *laptop*/*notebook computers*), MP3 уређаји за учење, различити наменски програми за манипулацију медицинским подацима, мобилни оперативни системи и мобилне апликације за медицинске намене.

5. Истраживање – прикупљени подаци

Здравствене организације улажу велике количине средстава у анализу постојећег стања у здравству и у пројектовање будућих потреба. Када је у питању планирање будућих потреба у здравственим организацијама у Србији често су та улагања несразмерна резултатима. Велики и скупи пројекти се завршавају без видљивих резултата, или се непрестано налазе у фази тестирања. Такав приступ не обезбеђује добре резултате јер се здравствене анализе базирају на прегледу малог скупа података што не пружа довољно добар увид у постојеће стање. Ово истраживање је обезбедило скромну количину података на основу којих је могуће направити графичке или табеларне приказе једноставних појава што може пружити увид у околности које постоје у здравству са аспекта информационих система.

Део резултата квалитативног дела истраживања:

- Значај информационо комуникационих технологија у здравству је по мишљењу 80% испитаника веома значајно, исто толико њих сматра да су промене у тој области значајно утицале на квалитет здравствених услуга.
- Мање од 40% испитаника је сматрало да је постигнут задовољавајући ниво опремљености информационо комуникационим технологијама.
- 20% испитаника је одговорило да су се лако прилагодили промени начина рада и преласку са класичног евидентирања података на електронски.
- Што се тиче приступа Интернету захваљујући комуникационој инфраструктури здравствених организација, испитаници су стање окарактерисали као задовољавајуће.
- Администратори који су ангажовани у здравственим организацијама су претежно стање компјутерске писмености медицинског особља окарактерисали као незадовољавајуће, док је значај компјутерске писмености различито третиран у зависности од радних места.
- Сви испитаници сматрају да им је потребна додатна едукација из домена информатике.

Део резултата квантитативног дела истраживања:

- Све обухваћене здравствене организације имају савремене компјутерске мреже које претежно чине компјутери нове генерације.
- Све обухваћене организације имају сервере за контролу корисничких налога и сервере за управљање подацима.
- Све обухваћене организације су користиле различите видове специјализованих компјутерских апликација за прикупљање и обраду података.
- Све апликације су имале једну заједничку карактеристику, све су на исти начин и у истом формату припремале податке за снимање у локалне базе података и за снимање у централне базе података.
- Све организације имају свог информатичара који обавља посао систем администратора, а 50% обухваћених организација ангажује приватна предузећа за одржавање информационог система.

- Све организације користе дигитални потпис у финансијској служби приликом креирања електронске фактуре, али ни једна од обухваћених организација не користи дигиталне сертификате у другим службама.
- Приступ Интернету: *Dail-up* конекције нису заступљене, 80% конекција су ADSL (енгл. *Asymmetric Digital Subscriber Line*) и 20% конекција се реализује бежично.
- Софтверска заштита од претњи са Интернета и из унутрашњости система постоји у свим организацијама, док хардверска заштита не постоји ни у једној.
- Сви медицински и немедицински радници који имају компјутер на располагању посећују друштвене мреже и користе компјутере за личне послове.

Институт за јавно здравље Републике Србије „Др Милан Јовановић Батут“ једанпут годишње публикује „Здравствено статистички годишњак Републике Србије“ и статистичку базу података „Здравствени показатељи у Републици Србији“ као и друге публикације и извештаје у вези са здрављем становништва који се могу преузети са Интернет презентације ове организације. Једна од публикација коју је направио овај Институт, а која је значајна за овај рад је резултат истраживања које је спровео др. Иван Ивановић, Начелник Центра за информатику и биостатистику на овом Институту. Истраживање је посебно интересантно зато што се бавило капацитетима, способностима и спремношћу за рад са електронском здравственом документацијом.

Истраживање је спроведено крајем 2011. године и дало је следеће резултате:

- Болнице врше контролу, анализирају и користе податке који се прикупљају, али само 37% сматрају да су прикупљени подаци адекватни и доброг квалитета.
- Све болнице достављају податке Институту за јавно здравље и Републичком фонду за здравствено осигурање, али не добијају сви повратне информације. 79% болница доставља податке директно Министарству здравља, а 16% локалној управи.
- Једна трећина, односно 32% болница је одговорило да би, ако би били у могућност, прво унапредили свој информациони систем, 26% би прво унапредило опрему за рад и финансијску ситуацију запослених, 11% задовољство пацијената и 5% радни учинак запослених.
- 84% болница имају стручно особље за подршку и одржавање постојећих информационих система, али само 10% сматра да имају довољан број.
- Више од половине, односно 53% болница немају посебну службу, или организациону јединицу, док 58% нема спољну службу (изван установе) за подршку и одржавање постојећих информационих система.
- Веома мали број људи запослених у болницама је прошао неки вид обуке за рад на компјутерима, у 42% болница, мање од 10% запослених.
- Просечно, један компјутер дели 4,25 запослених, а 65% компјутера је набављено у последњих пет година.

- Све болнице имају локалне мреже (енгл. *Local Area Network*), од њих 32% само делимично, а просечан број прикључних места је 317.
- Све болнице користе компјутерски програм у неком облику за рачуноводство (особље, плате и слично), а 95% га користити и за праћење здравствене заштите и рада у болници, с тим што ти програми само делимично подржавају процесе здравствене заштите и рада у здравственим организацијама.
- 63% болница користити одговарајући софтвер за електронску фактуру за Републички фонд за здравствено осигурање, док 26% за извештавање ка Институту за јавно здравље.
- Све болнице се повезане на Интернет, 74% на свим локацијама, а 26% делимично и то углавном преко ADSL 79%, кабловски 21% и бежично 21%.
- 95% болница имају Интернет презентације.

(Напомена: Од 2014. године све јавне организације су у обавези да користе софтвер за електронско фактурисање и електронске сертификате.)

6. Идентификација корисника

Здравствени информациони системи треба да сачувају личне податке корисника здравствених услуга од приступа неауторизованих особа. То је један од разлога због ког је постојећи здравствени информациони систем пројектован тако да се све трансакције података реализују у оквиру локалне компјутерске мреже, док се ретко и на предвиђени начин подаци усклађују са подацима на серверима где су централизовани подаци из свих здравствених организација. Такав приступ, и ако у основи веома безбедан, смањује стварне потенцијале које пружају савремене информационе технологије. Здравствени информациони систем би требао да омогући пружање квалитетних здравствених услуга без обзира на локацију лекара. Он би требао, да на основу разних дијагностичких података из ранијих прегледа, односно, података у облику описа обољења, или дијагностичких снимака, из података добијених консултација са колегама путем порука и видео конференција, омогући лекарима доношење квалитетних одлука.

Закон о заштити права пацијената који је на снази у земљама Европске Уније, као и закони о личним подацима, о електронским комуникацијама, о електронском потпису и други, слични су законима који су на снази код нас, са том разликом што се у Републици Србији већи део законских норми везује за старе начине рада са подацима. Закони који уређују електронско здравство у Европској Унији стварају обавезу да здравствени информациони системи задовољавају високе безбедносне критеријуме када је у питању заштита података и то детаљно дефинишу. Ови закони прописују оптималне видове заштите посматрано кроз слојевитост система у односу на различите референтне моделе. Поред законских норми, постоје и бројне препоруке у вези са различитим хардверским и софтверским решењима. Такође, када су у питању здравствени информациони системи, постоји низ специфичности везаних за њихово пројектовање и реализацију.

Приликом пројектовања информационог система полази се од сврхе коју тај систем треба да оствари. Зависно од тога предвиђају се различите техничке и организационе мере којим се постиже оптимална безбедност будућег информационог система. Тим мерама се превентивно делује и спречава настанак случајних грешака, затим, спречава се неправилно и недозвољено прикупљања, чувања, обраде, или уклањање, односно уништење података, као и њихово фалсификовање и злоупотреба. Ове мере првенствено обухватају правила за организацију просторија у којима ће се налазити различите информационо комуникационе технологије, затим кроз избор медицинске и компјутерске опреме, кроз софтверску подршку, мреже, и кроз едукацију корисника здравственог информационог система. Такође, води се рачуна и о томе да све карактеристике безбедног информационог система не буду нарушене ни у ванредним условима као што су губитак напајања, оштећења на водоводним инсталацијама, оштећења система за климатизацију, у случају елементарних непогода и слично.

Опрема која користи приликом изградње информационог система мора бити адекватна по својим техничким карактеристикама и мора задовољавати све актуелне стандарде и све будуће потребе. Она мора радити поуздано у целом периоду употребе што се постиже оптималним избором квалитета и могућношћу да се благовремено изврши сервис, односно да са набаве потребни резервни делови. Такође, у зависности од сврхе коју треба да испуни тај информациони систем

дефинише се безбедносни принципи и процедуре као и начини на који ће оне бити реализоване.

Уколико се ресурсима информационог система приступа путем Интернета, или путем мрежа мобилне телефоније, пракса је да се користи неки од система за аутентификацију корисника и неки од криптографских система за шифровање, односно за дешифровање података. Наравно, што је виши ниво заштите података, већи су и трошкови који произилазе из тога. Фактор који битно утиче на квалитет заштите, а самим тим и на вредност реализације такве заштите, јесте степен тајности података. Степен и врста тајности података диктирају обавезне и додатне мере обезбеђивања и заштите информационог система. Поред степена тајности, на обавезне и додатне мере заштите утиче и сама сврха организације у оквиру којих се реализује информациони систем и њему адекватан криптографски систем.

Општа болница Лозница, Дом здравља "Др Миленко Марин", Медицина рада Лозница, Дом здравља Савски венац и Дом здравља Врачар у оквиру којих је, једним делом, спроведено истраживање за овај рад су примењивале различите, уобичајене мере заштите. Ове организације су најчешће вршиле неформалну контролу кадрова који су требали да постану администратори здравственог информационих система, затим радне задатке су дефинисали тако да њихова реализација буде безбедна, скоро у свим случајевима је вођено стручно усавршавање кадрова, планирана је и реализована физичка заштита компјутерске опреме и брижно је одабрана компјутерска опрема и услови за чување те опреме. Такође, у складу са важећим законима у Републици Србији, клијентски налози су дефинисани употребом активног директоријума. То је у функционалном и у финансијском смислу било оптимално решење, обзиром на остале карактеристике здравственог информационог система. Свим удаљеним деловима овог система се приступа путем Интернета и уз додатне нивое аутентификације клијената и идентификације корисника.

За разлику од мањих информационих система где постоје две врсте корисника, обични корисници и корисници са администраторским привилегијама, код здравствених информационих система постоји више различитих улога и више различитих комбинација корисничких привилегија. Примера ради, када су у питању медицинске сестре, могу постојати следеће корисничке улоге: главна сестра, сестра за пријем пацијената, сестра у интервенцијама, сестре које дежурају, сестре које су у интервенцијама на терену и слично. Такође, обзиром да се задужења медицинских сестара мењају, потребно је да се и улоге мењају у зависности од локације клијентског компјутера. Слична ситуација је и код лекара где разликујемо лекара специјалисту, одабраног лекара, дежурног лекара и слично. Такође, неретко се наилази на сценарио где је лекар једног пацијента истовремено изабрани лекар неког другог пацијента, а мора постојати разлика у привилегијама над функцијама информационог система јер одабрани лекар има привилегију да приступи већем скупу података својих пацијената и већем броју функција у информационом систему у односу на обичног лекара.

Подаци о пацијентима су организовани и складиштени у базе података, а структура тих база је јединствена на нивоу Републике Србије. Републичке базе пацијената су исте по структури са регионалним и локалним како би сви подаци могли да се централизују. Међутим, корисници здравствених услуга мењају своје личне податке, адресе пребивања, презимена и слично, а обзиром да не постоје аутоматски механизми за ажурирање података, ти подаци често нису ажурни када су у питању здравствене базе података. То прави бројне административне проблеме и

значајно утиче на смањење квалитета здравствених услуга. Поред тога постоје пацијенти који немају здравствене књижице, а могу да остваре право на здравствену заштиту, као и пацијенти који су своје право на здравствену заштиту добили на основу неажурне, или неисправне документације. То су ситуације у којима је потребно донети одлуке за које нема довољно података, документације, па ни формалног покрића. Лекари су тада у ситуацији да доносе одлуке које у оквирима њихових могућности а које су у супротности за мисијом здравства а то је унапређење и очување менталног и физичког здравља људи.

Поред тога, Здравствени информациони систем Републике Србије не поседује механизме који одвајају демографске податке пацијената од њихових медицинских података. Одвајањем тих података се делује превентивно у случајевима злоупотребе. Уколико неко настоји да злоупотреби нечије здравствене податке не би требало да је у могућности да их повеже са личним подацима пацијената. Са друге стране, здравствени подаци су незаменљив извор података за разна истраживања у области здравства. Поред тога, однос лекара и пацијента је поверљив што је уређено и адекватним правним нормама. Раздвајање медицинских и демографских података у великој мери помаже да лични подаци остану тајни и да се обезбеди довољан ниво приватности.

6.1 Заштита података

Посебна проблематика у вези са здравственим информационим системима је заштита података и обезбеђивање тајности информација. Подаци којима се манипулише у оквиру здравствених информационих система су лични подаци грађана и као такви треба да остану тајни за све оне који не треба да располажу тим подацима. Употреба информационих система у здравству подразумева прикупљање и обраду личних података грађана. При томе, то су велике количине података којима свакодневно приступа велики број различитих људи, од немедицинског особља, преко помоћног медицинског особља, па до лекара. Поред тога, ту постоји потреба и оправданост да лекари имају увид у извештаје колега који су специјалисти из других области медицине, због чега постоји потреба за дефинисањем корисничких улога у здравственом информационом систему са адекватним правима и ограничењима како би се омогућила потпуна сагласност информационих просеца и радних задатака.

Приватност је право појединца да одреди које информације о себи третира као тајну и као такве их не дели са другим људима, организацијама или са јавношћу. Етички кодекс здравствених радника подразумева да се све информације које су у вези са корисником здравствених услуга добијене током обављања здравствене делатности сматрају професионалном тајном. Сви лични подаци о појединцу, као и подаци у вези са историјом болести, дијагностичким процедурама, резултатима анализа, прописаном терапијама и слично, морају остати поверљиви и сви здравствени радници морају бити свесни потребе и обавезе поштовања поверљивих информација. Постоје случајеви када се могу открити поверљиви подаци о пацијентима уколико они понуде свој пристанак да се поверљиве информације о њима открију, или уколико се налазе у здравственом стању у ком није могуће да то ураде, а постоји потреба за ти, или ако се установи потреба да се здравствени радник ослободи обавезе чувања професионалне тајне у сврху несметаног обављања лекарског посла, или у сврху полицијске истраге.

Токови информација у здравственом информационом систему су доста слични токовима информација у лекарској пракси, међутим када су у питању токови информација у вези са немедицинским особљем, ту постоје одређене нелогичне ситуације. Информатичара, систем администратори, сервисери и друго информатичко особље је у могућности да управља и надгледа здравствени информациони систем на начин на који то раде и здравствени радници. Информатичком особљу су доступни подаци у истом обиму у ком су доступни и здравственим радницима, али медицинско и немедицинско особље не може располагати истим здравственим подацима и не може их посматрати са истом професионалном дискрецијом. Један део решења за овај и сличне проблеме се налази у додатном обучавању медицинских радника за употребу различитих информационо комуникационих технологија. Други део решења се налази у одвајању здравствених од демографских података о пацијентима.

6.2 Криптографија

Савремени информациони системи омогућавају једноставну и аутоматизовану употребу безбедносних механизама који спречавају да електронски документи буду изложени неовлашћеном читању, копирању, или измени. Савремени стандард у заштити информационих система представљају решења која омогућавају заштиту интегритета порука, односно откривање неовлашћених измена, затим потврду поверљивости комуникације, односно потврду да је садржај комуникације у свом изворном облику доступан само аутентификованим, односно идентификованим странама у комуникацији и институцију непорецивости, односно искључивање могућности да стране у комуникацији порекну своје активности. Ово је нарочито значајно обзиром на чињеницу да би у здравственом информационом систему свакодневно комуницирали корисници који су физички удаљени и који се не познају лично, а који морају да професионално изврше своје радне задатке и да преузму одговорност за сопствене активности.

Подаци који се размењују између страна у комуникацији се преносе у виду пакета који на свом путу пролазе кроз више чворних тачака, односно кроз више различитих информационо – комуникационих уређаја. Уколико се подаци преносе у облику отвореног текста, постоји могућност да ти подаци постану доступни и онима којима нису намењени, или онима који имају намеру да из злоупотребе, па се због превенције таквим ситуацијама подаци шифрују. Криптографски алгоритми се могу окарактерисати као тајни, уколико се безбедност заснива на тајности алгоритма, што представља претечу савремених криптографских алгоритама. Савремени алгоритми своју безбедност заснивају на тајности криптографских кључева па се могу окарактерисати као јавни и често су предмет расправа о њиховој успешности и бројних анализа њихове ефикасности. Данас у употреби симетрични и асиметрични алгоритми с тим што је њихова практична имплементација најчешће хибридно решење које обједињава предности обе врсте алгоритама.

Криптографски системи треба да задовоље неколико критеријума да би се сматрали ефикасним. На првом месту сума новца потребног за откривање отвореног текста од стране нападача, мора бити већа од суме која се троши на шифровање. Временски период потребан за откривање отвореног текста из шифрованих порука мора бити већи од временског периода у ком би шифровани подаци требало да остану тајни. Количина података који су шифровани на основу једног

криптографског кључа мора бити довољно мала како нападач не би имао довољно велики узорак за успешну криптографску анализу. Поступци шифровања и дешифровања порука се реализују на основу истих криптографских алгоритама и на основу истог криптографског кључа. Важно је да време шифровања и дешифровања буде довољно кратко што се постиже комбинацијом адекватних софтверских решења уз додатна хардверска решења.

Симетрична криптографија је најстарији облик криптографије и подразумева да се исти кључ користи за шифровање и за дешифровање порука. Тајност се заснива на кључу и због тога шифроване поруке може дешифровати само онај који поседује криптографски кључ. То је, такође, разлог због ког се криптографски кључ никада не сме слати незаштићеним каналима. Највећа предност симетричног шифровања је висока ефикасност и велика брзина шифровања и дешифровања. Међутим, симетрични криптографски системи подразумева и веома комплексно управљање криптографским кључевима. Криптографски кључеви се морају размењивати сигурним путем, то намеће бројна ограничења, нарочито када су у питању систем са великим бројем корисника и са високим степеном децентрализације. Пракса показује да се виши ниво безбедности постиже када се избегне употреба Интернета за размену криптографских кључева и када се то уради посредством поште, или неких других комуникационих система. Најчешће употребљавани симетрични алгоритми су: DES, 3DES, AES, IDEA, RC5, RC6 и други.

Крајем осамдесетих година значајно је повећана употреба разних криптографских система што је била директна последица значајног увећања употребе различитих информационо комуникационих технологија. Симетрични криптографски системи нису више представљали оптимално криптографско решење. Карактеристике компјутерских корисника су се значајно измениле што је довело до појаве асиметричних криптографских система. *Whitfield Diffie* и *Martin Edward Hellman* се сматрају творцима асиметричне криптографије и они су први размотрили предности и недостатке криптографије која се базира на паровима криптографских кључева, односно ја паровима јавних и тајник кључева. Прва и најзначајнија предност оваквих алгоритама јесте постизање тајности комуникације без претходне размене тајног кључа. Сигурност тајности асиметричних алгоритама се темељи на немогућности, или врло малој могућности за израчунавање тајног кључа уз помоћ јавног кључа и шифрованог податка.

Асиметрични алгоритми се заснивају на математичким функцијама које отворени текст на основу одабраног криптографског кључа претварају у шифровани текст. Криптографске функције су направљене тако да је практично немогуће да се уз помоћ шифрованог текста и кључа који је коришћен у процесу шифровања сазна отворени текст. Међутим, уколико је познат тајни кључ за дешифровање, веома је једноставно дешифровати шифровани текст и добити отворени текст. За заштићену комуникацију која се заснива на оваквим алгоритмима потребно је да свака страна поседује по два кључа, јавни и тајни које, иако су различити, повезују математичке функције. Асиметрично шифровање је веома комплексно и веома захтевно када су у питању хардверски ресурси.

1978. године је дефинисан први практични асиметрични алгоритам, под називом RSA. Овај алгоритам је добио назив по почетним словима имена аутора који су га креирали: *Ron Rivest*, *Adi Shamir* и *Leonard Adleman*. Неколико година након тога, овај алгоритам је употребљен за креирање дигиталног потписа (енгл. *Digital*

Signature). 1991. године је усвојен први стандард дигиталног потписа базиран на RSA асиметричном алгоритму, а 1994. године, Америчка Национална Безбедносна Агенција (енгл. *National Security Agency*) је развила и усвојила стандард дигиталног потписа (енгл. *Digital Signature Standard*) како би било могуће генерисање дигиталног потписа у сврху потврђивања аутентичности електронских докумената.

6.3 Дигитални потпис

Дигитални потпис (енгл. *Digital Signature*) је скуп тајних криптографских параметара у електронском облику који се додају електронским порукама са циљем да се недвосмислено идентификује потписник електронске поруке. Поред тога што идентификује потписника електронске поруке, дигитални потпис потврђује и аутентичност садржаја поруке, односно доказ да порука није измењена на путу од пошиљаоца до примаоца. Дигитални потпис је низ бита који се добија применом асиметричног алгоритма на хеш (енгл. *hash*) вредност генерисану из блока података који се штити, а у зависности од приватног, односно тајног кључа пошиљаоца поруке. Обзиром да је порука шифрована приватним кључем пошиљаоца, свака промена поруке доводи до нарушавања интегритета података, а самим тим и до тога да тај електронски документ нема правно дејство.

6.3.1 Дигитално потписивање

Дигитално потписивање подразумева креирање електронског отиска на основу садржаја поруке која се потписује и на основу крипотрафског кључа потписника поруке. Страна која шаље поруку користи свој тајни кључ за шифровање и на основу њега се потписује. Страна која прима поруку користи јавни кључ потписника на основу чега аутентификује потписника и дешифрује поруку. Асиметрични криптографски алгоритми подразумевају да се јавни кључ користи за шифровање, а приватни за дешифровање што је обрнут сценарио у односу на дигитално потписивање. Овакав поступак је неопходан зато што је то начин да се потврди идентитет стране која шаље поруку обзиром да је тајни кључ познат једино страни која дигитално потписује поруку и сертификационом ауторитету.

Уколико трећа страна жели да се лажно представи мора користити тајни кључ стране за коју се представља. Тајни кључ је практично немогуће генерисати на основу шифрованих порука, или на основу јавног кључа. Овим се обезбеђује интегритет порука. Уколико трећа страна покуша да измени део поруке, или један њен део добиће се шифровани текст који је немогуће правилно дешифровати. На овај начин се одржава интегритет порука. За сваку од прослеђених порука се праве копије на основу чега се може реализовати институција непорецивости јер се релативно лако може утврдити да ли је поруку потписала страна која је власник одговарајућег дигиталног сертификата, у које време је послата порука, који је био њен садржај и да ли је дошло до неке измене садржаја поруке од треће стране.

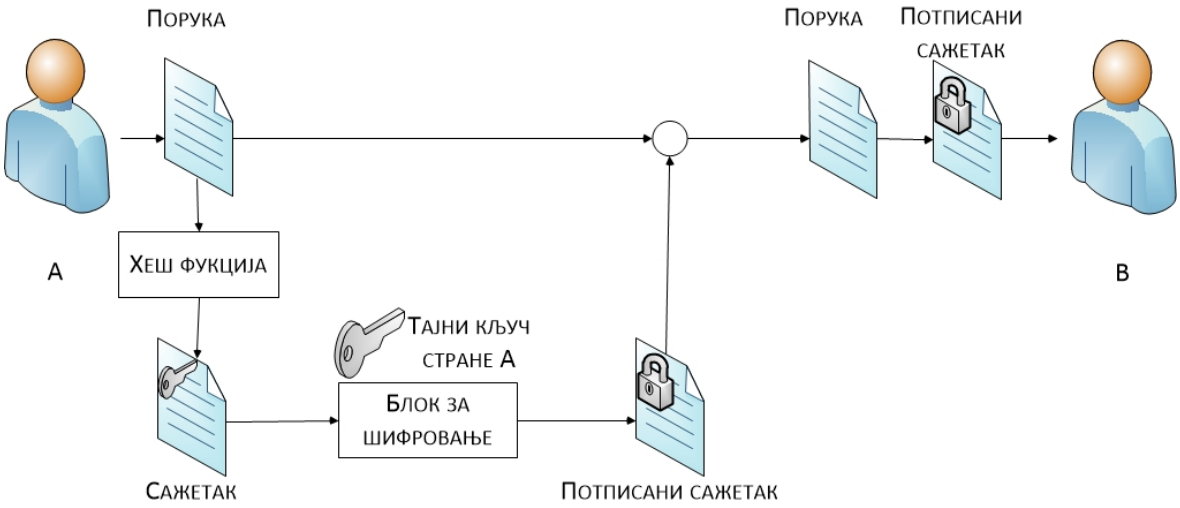
Да би дигитално потписивање докумената било могуће, потребно је да постоје јасно дефинисане границе документа, или дела документа који се потписује. Уобичајено је да се дигитални потпис придодаје поруци, међутим он може бити послан и одвојено докле год постоји недвосмислена веза између поруке и кључа. Некада постоји потреба за потписивањем целе поруке, а обзиром да се поруке

шифрују кључевима великих дужина, генерисани шифрати би такође били великих дужина што би захтевало пуно времена и велику количину ресурса. Пракса је таква да се дигитално потписује сажетак поруке који се генерише на основу неке од криптографских хеш функција. Традиционално су у употреби биле MD5 (енгл. *Message Digest 5*) и SHA-1 (енгл. *Secure Hash Algorithm 1*), међутим у односу на препоруке, период њихове употребе је истекао, или у случају SHA-1, истиче у току 2015. године.

Табела 1 Препоруке за период употребе неких хеш алгоритама

Хеш алгоритам	Препоручени период употребе	Препоручена намена
SHA-1, RIPEMD-160	Крај 2015. године.	Верификација дигиталних сертификата.
SHA-224	Крај 2015. године.	Дигитално потписивање.
SHA-256, SHA-384, SHA-512	Крај 2017. године.	Дигитално потписивање.

Криптографске хеш функције су једносмерне. Отисак поруке се може једноставно креирати, али је практично немогуће креирати полазну поруку из добијеног отиска. То омогућава потврду интегритета поруке уз истовремено очување тајности њеног садржаја. Поред тога, хеш функције су једнозначне, односно применом једне одређене хеш функције на један одређени текст, увек се добија исти отисак. Тако креирани отисак поруке се шифрује, односно дигитално потписује и то се врши уз помоћ тајног кључа стране која шаље поруку. За шифровање се обично употребљавају RSA (акроним имена. *Ron Rivest, Adi Shamir u Leonard Adleman*) и DSA (енгл. *Digital Signature Algorithm*) алгоритми, а ређе ECDSA (енгл. *Elliptic Curve Digital Signature Algorithm).*



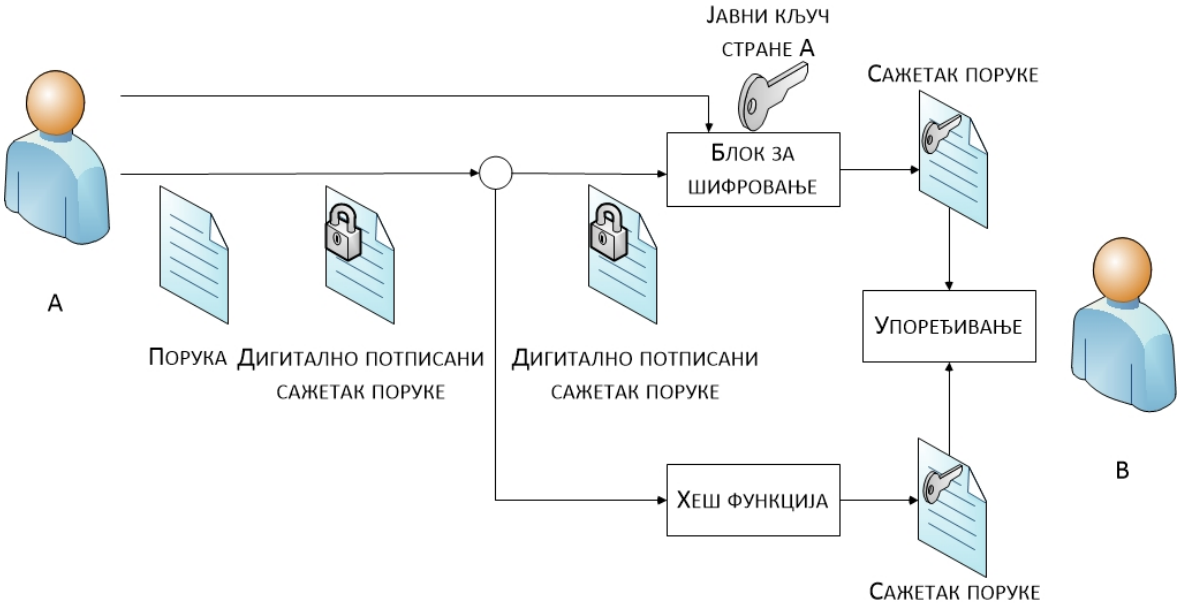
Слика 3 Креирање дигиталног потписа

6.3.2 Верификација дигиталног потписа

Верификација дигиталног потписа се реализује тако што се првенствено из добијене поруке издваја дигитални потпис који се затим дешифрује јавним кључем пошиљаоца поруке. Након пријема, прималац поруке креира отисак добијене поруке идентичном криптографском хеш функцијом, а затим се врши поређење генерисаног отиска поруке и отиска који добијен од стране пошиљаоца поруке. Уколико се након поређења установи да су добијена два идентична отиска, сматра се да је

верификација успешна. Ово потврђује да је порука стигла у неизмењеном облику, а обзиром да је шифрована тајним кључем пошиљаоца, успешно дешифровање се може реализовати само јавним кључем пошиљаоца што недвосмислено указује на то које пошиљалац поруке. Упоређивањем два добијена отиска и успешним дешифровањем се потврђује да порука није модификована на свом путу и да је за садржај поруке је и у правном смислу одговоран њен потписник јер је потписана његовим тајним кључем.

Овако потписани електронски документи недвосмислено указују на њихове творце, па су он правно одговорни за њих, односно нису у могућности да порекну слање тих електронских докумената. Непорецивост осигурава уговоре који су постигнути на основу дигитално потписаних докумената и без употребе других правних средстава, а најчешће и без личног контакта уговорених страна. Институција непорецивости значи да се може потврдити, посебно у правном смислу, да су пошиљалац и прималац електронског документа стварно ентитети који су послали, односно примили поруку. Непорецивост онемогућава ситуацију у којој једна страна у комуникацији негира да учествовала у тој комуникацији.



Слика 4 Верификација дигиталног потписа

6.4 Дигитални сертификати

Усавршавањем технологије дигиталног потписа значајно су се променили правни погледи на ову област што је временом довело до доношења разних законских аката који је уређују. Све земље Европске Уније су почеле са применом Закона о електронском потпису, као и већина осталих земаља на подручју Европског континента које тај закон примењују парцијално са циљем потпуне примене закона. Република Србија је 2004. године донела Закон о електронском потпису (Службени гласник РС бр. 135/2004) и њим је прописана употреба електронског потписа у правним пословима и у другим правним радњама као и права, обавезе и одговорности у вази са електронским сертификатима. Закон о електронском потпису у Републици Србији је у потпуности усклађен са Директивом Европске Уније.

Основна улога Закона о електронском потпису своди се на две функције:

- Да пропише услове под којима је електронски потпис правно еквивалентан својеручном потпису.
- Да пропише услове које морају да испуне сертификациона тела која издају квалификоване сертификате за верификацију квалификованих електронских потписа.

Закон о електронском потпису је већ неколико година на снази у Републици Србији и примењује се у приватном и јавном сектору. Јавни сектор је све промене које су у вези са дигиталним потписивањем и дигиталним сертификатима уводио постепено у зависности од постојеће информационе инфраструктуре и знања и вештина запослених кадрова. Кадрови који су ангажовани у јавном сектору су прилагодили своје радне задатке новим законима који уређују ову област. Обзиром да је у већини случајева употреба компјутера постала начин свакодневног рада, употреба електронског потписа је само један корак више у већ утврђеном начину коришћења постојећих информационих система и уобичајеном начину обављања радних задатака и пријављивања на систем.

Људи који за обављање својих радних задатака користе дигитални сертификат не морају да знају на који начин он функционише јер су информациони системи конципирани тако да су поступци креирања и верификације дигиталног потписа потпуно аутоматизовани. Међутим сви корисници су свесни правне одговорности коју преузимају на себе када обављају своје радне задатке. Такав систем рада, судећи по томе што пракса показује, је веома квалитетан. Вероватноћа отказивања система, или вероватноћа појаве неког безбедносног проблема је веома мала. Ризик је пуно мањи од ризика који је везан за измену неког документа на папиру, или ризика од фалсификовања докумената, или неког другог вида преваре односно злоупотребе.

6.4.1 Структура дигиталног сертификата

Употреба дигиталног потписа, односно креирање и верификација дигиталног потписа, се заснива на асиметричним криптографским системима и на употреби пара криптографских кључева, тајног и јавног кључа. Како би криптографски кључеви недвосмислено указивали на њихове власника, њих мора издавати неко тело од поверења, односно ентитет у кога сви учесници у комуникацији имају поверења. То се реализује издавањем дигиталних сертификата од стране сертификационог тела, односно сертификационог ауторитета. Дигитални сертификат (енгл. *Digital certificate*) је уверење којим се потврђује веза између електронског потписа и идентитета потписника. Обзиром на то, дигиталне сертификате можемо посматрати као електронске личне карте, јер они садрже бројне личне податке о кориснику и податке о издаваоцу сертификата, односно о сертификационом ауторитету (енгл. *Certification Authority*) који гарантује веродостојност тих података.

Дигитални сертификат чини неколико основних елемената:

- Верзија формата која садржи ознаку структуре дигиталног сертификата. Један од најчешће заступљених формата је дефинисан стандардом X.509.
- Серијски број сертификата коју додељује сертификациони ауторитет у тренутку креирања дигиталног сертификата.

- Идентификатор алгоритма који садржи податке о алгоритму који је одређен за дигитално потписивање.
- Назив тела које је издало дигитални сертификат.
- Рок важења дигиталног сертификата, односно период у ком је дигитални сертификат валидан.
- Подаци о власнику сертификата: име власника, назив државе, назив региона, назив места пребивања, адреса електронске поште, назив организације у којој је запослен, назив одељења у ком ради, име власника организације.
- Поље додатних атрибута: број телефона код куће, на послу и слично.
- Подаци о јавном кључу власника који се састоје од јавног кључа и идентификатора асиметричног алгоритма којим се дати кључ примењује.
- Дигитални потпис сертификата од стране сертификационог ауторитета која издаје дигитални сертификат.

Издавање дигиталних сертификата може да врши искључиво трећа страна од поверења (енгл. *Trusted Third Party*), али је чешћи случај да се она појављује у комуникацији као гарант аутентичности. Уколико пријемна страна успешно верификује добијени сертификат, онда је она сигурна у аутентичност пошиљаоца поруке, односно власника одговарајућег тајног кључа. Обзиром да су јавни и тајни кључ повезани одговарајућим математичким функцијама, немогуће је из јавног кључа издвојити приватни кључ. Иако је јавни кључ познат, практично је немогуће открити тајни кључ пошиљаоца и искористити га за лажно представљање и лажно потписивање електронских докумената.

Дигиталне сертификате може, условно речено, издавати било ко. Међутим, већина таквих дигиталних сертификата нема правно дејство. Квалификоване дигиталне сертификате могу да издају само сертификациона тела која имају статус правног лица, таквог да може другим правним и физичким лицима да пружа услуге издавања дигиталних сертификата као и друге услуге повезане са овом делатношћу. У Републици Србији постоји неколико организација које су идентификоване као издавачи квалификованих електронских сертификата у складу са Законом о електронском потпису и одговарајућим подзаконским актима. Њихови дигитални сертификати, са одговарајућим криптографским кључева се могу употребити за креирање квалификованог дигиталног потписа и за квалификовано потписивање дигиталног документа који је по правној снази једнак папирном документу потписаном и овереном на класичан начин, оловком и печатом.

6.5 Инфраструктура са јавним кључевима

Инфраструктура са јавним кључевима (енгл. *Public Key Infrastrukture*) представља комбинацију хардверских и софтверских елемената, људи и процедура неопходних за генерисање, складиштење, дистрибуцију и опозив дигиталних сертификата са сврхом успостављања дигиталног идентитета субјеката у оквиру локалних, или глобалних информационих система. Овим се ствара погодно окружење за реализацију различитих безбедносних и правних сервиса, првенствено оних који су значајни за потврђивање аутентичности субјеката који учествују у комуникацији. Намене су вишеструке, од електронског пословања (енгл. *e-Business*)

укључујући и електронску трговину (енгл. *e-Commerce*) и банкарство (енгл. *e-Banking*), до електронске управе (енгл. *e-Government*) и електронског здравства (енгл. *e-Healthcare*).

За постојање инфраструктуре са јавним кључевима потребно је укључивање сертификационог тела које издаје дигиталне сертификате и регулише начин њихове употребе током периода важности. Поред тога, потребно је доношење документа којим се утврђују правила употребе дигиталних сертификата (енгл. *Certificate Policy*), затим доношење документа којим се утврђују правила рада (енгл. *Certificate Practice Statement),* односно документа који детаљно описују операционе процедуре за реализацију принципа који су наведени у правилима употребе дигиталних сертификата. Ови документи описују како је сертификационо тело формирано, како ради, како се генеришу дигитални сертификати, како се повлаче, како ће кључеви бити генерисани, регистровани и сертификовани, где ће се чувати кључеви и како ће корисници располагати њима. Инфраструктура са јавним кључевима подразумева укључивање ауторитета за регистрацију сертификата (енгл. *Registration Authority*), односно тела ком се подносе захтеви за издавање сертификата. Затим, обезбеђивање инфраструктуре за размену података између регистрационог и сертификационог ауторитета, затим обезбеђивање инфраструктуре за дистрибуцију захтева за издавање и слање дигиталних сертификата, као и саме криптографске системе и сервисе за реализацију криптографских функција инфраструктуре са јавним кључевима.

6.6 Безбедносни протоколи

OSI референтни модел (енгл. *Open Systems Interconnection Basic Reference*), је направљен са циљем да се омогући комуникација између хардверски и софтверски различитих технологија. Идејни творац овог модела је Међународна организација за стандардизацију (енгл. *International Organization for Standardization*) која је 1984. поставила стандарде који дефинишу овај модел. Овај стандард описује и дефинише транспорт података превођењем кроз седам слојева, а прихватањем овог стандарда, различити произвођачи хардвера и софтвера су добили могућност да остваре потпуну комуникацију између различитих уређаја и различитих информационих система без увида у спецификације производа других произвођача, или софтверске карактеристике.

Најзаступљенији транспортни протокол на Интернету је HTTP (енгл. *Hypertext Transfer Protocol*). Међутим, овај протокол подразумева креирање нове везе између клијента и сервера за сваки нови захтев који клијент упути серверу, након чега се веза између сервера и клијента прекида све док се поново не успостави услед новог клијентског захтева. Овај протокол не укључује системе за заштиту података и не користи се у безбедним комуникацијама. Овај недостатак се надомешћује употребом безбедносних протокола од којих је најзаступљенији HTTPS (енгл. *Hypertext Transfer Protocol Secure*). HTTPS је протокол који обезбеђује сигурну комуникацију на Интернету и другим компјутерским мрежама. Он представља надоградњу постојећег HTTP захваљујући безбедносним карактеристикама SSL/TLS (енгл. *Secure Sockets Layer / Transport Layer Security*) протокола. Он представља надоградњу постојећег HTTP захваљујући безбедносним карактеристикама SSL/TLS (енгл. Secure Sockets Layer / Transport Layer Security) протокола. На основу ове безбедносне надоградње, могуће је обезбедити тајност и

интегритет података и проверити аутентичност страна у комуникацији употребом различитих хибридних решења асиметричног шифровања јавним кључем (RSA), симетричним шифровањем (DES, AES, RC5 и други) и дигиталним сертификатима. Ова сигурносна проширења обезбеђују механизме за аутентификацију клијената, за аутентификацију сервера и за безбедну размену података између њих.

HTTPS се, посматрано у односу на референтни OSI модел, реализује на последња три нивоа, односно на нивоима сесије, презентације и апликације и наслеђује све карактеристике SSL/TLS протокола на које се ослања. Инфраструктура са јавним кључевима и сертификациони ауторитети у овом случају су у служби ауентификације сервера и клијената, што пружа довољно добру гаранцију да је комуникација и размена података успостављена са тачно одређеним сервером и Интернет апликацијом, као и да је обезбеђена тајна комуникација између клијента и сервера без могућности да трећа страна протумачи, измени, или фалсификује податке. Највећа предност овог протокола јесте у томе што је веома једноставан за употребу и што је у највећем броју случајева све аутоматизовано.

SSL је дефинисан за две различите опције: прву, која је сигурнија али захтева да и клијент има дигитални сертификат и другу која подразумева да само сервер има свој дигитални сертификат. У оба случаја ниво заштите зависи од софтвера клијентског и серверског компјутера, као и од начина на који су имплементирани криптографски алгоритми. Поред тога, SSL нема податке о протоколима који се реализују на вишим нивоима OSI референтног модела и он постојање дигиталног сертификата везује за одређену комбинацију IP адресе и броја порта. Протоколи за транспорт података на Интернету предефинисано функционишу без безбедносних система па је неопходно да клијент иницира сигурну комуникацију са сервером. Уобичајен начин за то је да клијент користи порт који је намењен безбедној комуникацији, на пример порт број 443 који је предефинисан за HTTPS уместо порта број 80, или порта број 8080, који су предефинисани за обичну комуникацију. Други начин је да клијент, користећи уобичајен порт пошаље захтев серверу у облику команде за покретање сигурне конекције користећи специфичне механизме дефинисане у протоколу, на пример „STARTTLS“ команду у оквиру протокола за електронску пошту којом се покреће TLS или SSL конекција.

7. Аутентификација корисника

Контрола приступа (енгл. access control) се заснива на аутентификацији и ауторизацији и у највећем броју случајева је реализована као систем који обједињава ова два вида контроле. Ауторизација је скуп правила која дефинишу групу права, односно групу ограничења која имају аутентификовани корисници, на основу чега се контролише могућност употребе различитих функција информационог система. Међутим, ко може да приступи одређеним ресурсима информационог система зависи од успешне аутентификације. Аутентификација подразумева одређивање права на приступ жељеним ресурсима информационог система. Можемо направити разлику у зависности да ли је у питању аутентификација човека од компјутерског система, или је у питању процес аутентификације два компјутерска система, односно два софтверска процеса.

7.1 Аутентификација заснована на корисничким именима и лозинкама

Употреба лозинке и корисничког имена у процесу аутентификације је метод који се најчешће примењује обзиром на бројне предности. Највећа предност је у томе што употреба корисничких података не захтева никакве додатне ресурсе у смислу додатних финансијских улагања, или додатних техничких средстава. Кориснички подаци се могу једноставно променити, могу се измислити и не морају да буду стварни одраз личности корисника коме припадају. Обзиром да је ово најједноставнији метод аутентификације, корисничка имена и лозинке се користе у системима где то представља довољно поуздан начин вид потврде аутентичности. То су, најчешће, апликације где се кориснички налози могу самоиницијативно искључивати и креирати и где није потребна додатна провера од стране система, или администратора система.

Постоје ситуације у којима је потребно, поред креирања корисничког налога, имати сагласност система, или администратора система за активирање тог налога. Сагласност система се може реализовати употребом различитих кодова за активирање где се од корисника захтева унос додатних података, као што су број телефона, или адреса електронске поште. Након уноса потребних података, они се користе у даљем процесу активирања корисничког налога тако што се на тај број, или на ту адресу електронске поште шаље код за активирање. Тако се врши верификација тих података, односно утврђује се да је корисник унео тачан број телефона, или тачну адресу електронске поште чиме се додатно обезбеђује кориснички налог и његова будућа употреба. То је, уједно, једини начин да се верификују ови подаци, а они су значајни власницима тих система обзиром да их касније могу употребити за контактирање корисника система, за рекламирање различитих производа или услуга и слично.

Сагласност администратора система за креирање корисничког налога је метод који се употребљава у ситуацијама када је потребна лична процена будућег корисника информационог система. Није ретка ситуација у којој искључиво администратор, или група администратора, има могућност да креира корисничке налоге. Када су у питању велики информациони системи какав је и здравствени информациони систем сагласност администратора је оптимално решење са становишта функционалности и безбедности информационог система. Свака већа

здравствена организација има стално запослене систем администраторе који се могу бавити креирањем и одржавањем корисничких налога. Тако се превентивно делује и штите се ресурси информационог система на више начина. Систем администратори могу креирати корисничке налоге и при томе информисати будуће кориснике о начину на који треба да користе своје налоге. Поред тога, систем администратори могу неформално повезивати корисничке налоге са њиховим власницима па на основу тога пратити активности корисника из чега се може закључити која понашања су штетна за систем и евентуално смислити начин како би се могло позитивно утицати на таква понашања.

Корисници информационих система, када се одлучују за будућу лозинку, најчешће бирају низ карактера који је сувише кратак, сувише једноставан, или сувише предвидив. Са друге стране, дугачки низови случајних карактера који укључују велика и мала слова, бројеве и специјалне карактере се сматрају добрим за избор лозинке, међутим, корисници се никада не одлучују за комплексне лозинке уколико нису приморани на то. Таква пракса представља потенцијални безбедносни проблем, јер уколико је низ карактера који чине лозинку сувише једноставан, повећава се и могућност злоупотребе. Са друге стране, комбинације великог броја различитих карактера се једноставно заборављају што неповољно утиче на функционисање система атутентификације у информационом систему. Лозинке које су настале по узору на имена људи, називе појава, називе објеката, датуме и слично, без обзира на своју дужину, представљају лаку мету за нападаче. Нападачи знају да корисници не бирају случајно своје лозинке и уместо да испитују све могуће комбинације (енгл. *brute-force attack*), напад базирају на садржају „речника“, односно на списку најчешће коришћених комбинација карактера чиме се скраћује време напада.

Табела 2 Време потребно за потпуну претрагу кључева у зависности од врсте напада и броја карактера

Слова: АаБбВвГгДдЂђЕеЖжЗзИиЈјКкЛлМмНнЊњОоПпРрСсТтЋћУуФфХхЦцЧчЏџШш							
Цифре: 0123456789							
Специјални карактери: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~							
Укупан број карактера: 102							
Лозинке		**Време трајања напада у зависности од класе напада**					
Дужина лозинке	**Број комбинација**	**Класа A**	**Класа B**	**Класа C**	**Класа D**	**Класа E**	**Класа F**
2	10.404	Брзо	Брзо	Брзо	Брзо	Брзо	Брзо
3	1.061.208	88½ сек.	9 сек.	Брзо	Брзо	Брзо	Брзо
4	108.243.216	2¼ сат.	14 мин.	1½ мин.	8½ сек.	Брзо	Брзо
5	11.040.808.032	9½ дан.	22½ сат.	2¼ сат.	13½ мин.	1¼ мин.	8 сек.
6	1.126.162.419.264	2½ год.	90 дан.	9 дан.	22 сат.	2 сат.	13 мин.
7	114.868.566.764.928	238 год.	24 год.	2½ год.	87 дан.	8½ дан.	20 сат.
8	11.716.593.810.022.600	22.875 год.	2.287 год.	229 год.	23 год.	2¼ год.	83½ дан.

Зависно од снаге компјутера и система за складиштење лозинке, под условом да не постоје додатни системи заштите, време потребно за претраживање 102^5 комбинација карактера варира од 9½ дана до 8 секунди. Уколико је у питању компјутер *Intel Pentium* 100 MHz, а у питању је лозинка која закључава *Microsoft Office* документ, временски интервал износи 9½ дана (Класа A), уколико је у питању систем за закључавања корисничког налога на *Windows* оперативном систему, односно *Windows Password Cache* (.PWL датотека), то време је 22 сата и 30 минута (Класа B), док је време потребно за проверу свих комбинација на компресованим

архивама формата .ZIP или .ARJ износи 2 сата и 15 минута (Класа C). Временски период за потпуну претрагу уз помоћ савремених компјутера са два процесорска језгра износи 22 сата (Класа D). Када су у питању компјутерске радне станице (енгл. *Workstation*) (Класа E) то време је 2 сата, а уз помоћ супер-компјутера (енгл. *Supercomputer*) (Класа F) то време износи 13 минута. Када је у питању претраживање 102^8 комбинација карактера, зависно од снаге компјутера, то време може износити од 83½ дана до 22.875 година.

Корисничке лозинке се чувају у различитим датотекама и то су места на којима потенцијални нападачи очекују да ће их пронаћи, што је у неким случајевима веома једноставно, међутим ове лозинке се никада не чувају у свом изворном облику. Пракса је доказала да је најбоље чувати хеш (енгл. *hash*) вредности лозинке, односно низове карактера који се добијају након примене криптографских хеш функција на вредност лозинке. Ове функције се називају једносмерним обзиром да су направљене тако је немогуће из хеш вредности добити полазну вредност, што је значајно када желимо да снимимо вредност лозинке јер то спречава компромитовање свих корисничких налога и у случају када је један од корисничких налога компромитован. Принцип аутентификације на основу хеш вредности подразумева да се користе једнаки алгоритми за креирање отиска лозинке и у процесу аутентификације како би се добиле исте вредности за упоређивање. Такође, оваквом методом се обезбеђује да корисничка лозинка никада не буде снимљена у свом изворном облику у систему који се штити.

7.2 Аутентификација заснована на чип картицама

Чип картице, или паметне картице (енгл. *smart cards*) у себи имају интегрисано електронско коло, односно електронску компоненту са минијатурним чипом. Захваљујући овој електронској компоненти могуће је реализовати снимање, чување, обраду и ишчитавање различитих података који се користе у процесу аутентификације и другим процесима везаним за намену чип картица. Ове картице се производе у стандардној величини и са неким од стандардних чипова са том разликом што у малој мери постоје и нестандардне, односно специфичне чип картице које се наменски производе за посебне намене и посебне криптографске системе. За производњу чип картица се најчешће употребљавају материјали који су отпорни на оштећења јер се ове картице издају њиховим власницима на периоде дуже од годину дана, док се подаци на картицама се мењају у краћим временским периодима.

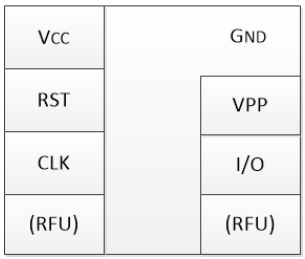
Значај паметних картица се огледа у томе што поред чувања различитих података оне пружају могућност реализације вишег нивоа безбедности приликом процеса аутентификације. Овакав начин провере подразумева испуњавање више неопходних услова: првенствено поседовање чип картице, затим познавање корисничке лозинке, најчешће PIN кода (енгл. *Personal Identification Number*), а неретко и унос додатних података као што су корисничко име, или нека додатна лозинка, или вредност. Поред тога што је поседовање паметне картице услов за аутентификацију, подаци и кључеви који се снимају на њих су доста комплекснији од оних које људи могу да памте, а повећање комплексност повећава ниво безбедности. Поред тога, паметне картице издају организације које том приликом утврђују идентитет будућег власника што индиректно повезује сваку активност за коју је употребљавана картица са идентитетом њеног власника. Ово је нарочито

важно када се чип картице употребљавају као медиј за складиштење података који чине дигитални сертификат, када су у питању електронска лична карта, електронска возачка дозвола или неки други електронски идентификациони документ неког правног или физичког лица.

Чип картице, у безбедносном смислу, представљају оптимално решење јер пружају виши ниво безбедности у односу на системе који се заснивају искључивао на корисничким лозинкама, а коштају мање од система који се заснивају на биометријским методама. Обзиром на њихове карактеристике, паметне картице се могу користити као складишта личних података, на пример: као лична карта, здравствена књижица, или пасош. Оне, такође, представљају одлично криптографско средство у процесу аутентификације, или приликом шифровања при реализацији заштићене комуникације.

Зависно од намене, разликујемо две врсте картица: меморијске, које немају микропроцесор и оперативни систем и микропроцесорске, које имају микропроцесор и потребан хардвер за функционисање оперативног системе као сам и оперативни систем. Поред тога, у зависности од начина на који се повезују са читачем картица разликујемо контактне, које имају металне конекторе и бесконтактне, које комуникацију реализују захваљујући радио таласима. Све постојеће картице су направљене у складу са стандардима ISO 7810, ISO 7816/1 и ISO 7816/2 и обично се састоје од пластичне картице и интегрисаног кола, међутим има и оних које поседују сопствено напајање, па чак и дисплеј и тастере за унос PIN кода као додатне видове аутентификације на нивоу саме картице.

Табела 3 Распоред конектора у односу на ISO7816 стандард



Слика 5 Распоред конектора у односу на ISO7816 стандард

- Vcc (енгл. *IC power-supply pin*) – Конектор задужен за напајање картице.
- RST (енгл. *Reset*) – Конектор задужен за поновно покретање на основу спољних сигнала, или на основу унутрашње логике паметне картице. Уколико сама картица има могућност ресетовања, подразумева се да има сопствено напајање.
- CLK (енгл. *Clock*) – Бројач, или мерач времена на основу кога се одређује радни такт.
- Gnd (енгл. *Ground*) – Уземљење, или маса.
- Vpp (енгл. *Virtual power pin*) – Конектор за регистрацију програмабилног електричног сигнала, односно сигнала вишег напона за програмирање меморије картице.
- I/O (енгл. *Input/Output*) – Улазно излазни конектор за серијски пренос података ка интегралном колу картице.

Микропроцесорске картице поседују различите опције за подешавања од чега зависе њихове могућности. Оне имају процесор који је у највећем броју случајева, или 8 – битни, или 16 – битни и који обично ради на фреквенцији 3 до 5 MHz. Овакви процесори располажу са 256 B до 1024 B оперативне меморије, односно RAM меморије, затим са 1 KB до 16 KB променљиве меморије која чува податке и без напајања, односно EEPROM меморије и са 6 KB до 25 KB сталне меморије, односно ROM меморије. Већина микропроцесорских картица које су данас у

употреби има посебан криптографски процесор. Функције су смештене у ROM или у EEPROM меморију, а RAM се користи за њихово извршење. Оперативни систем на чип картицама подразумева управљање са системом датотека и директоријума који је смештен у EEPROM меморију. Због скучености хардвера, систем датотека и директоријума има одређена ограничења. Називи датотека и директоријума су ограничени на 4 хексадецималне цифре, величина датотека и директоријума је непромењива и задаје се приликом креирања система, а манипулација подацима подразумева да нема померања података на меморијским локацијама јер је меморија организована по принципу „Последњи улазни податак – Први излазни податак“, односно по принципу LIFO (енгл. *Last In - First Out*).

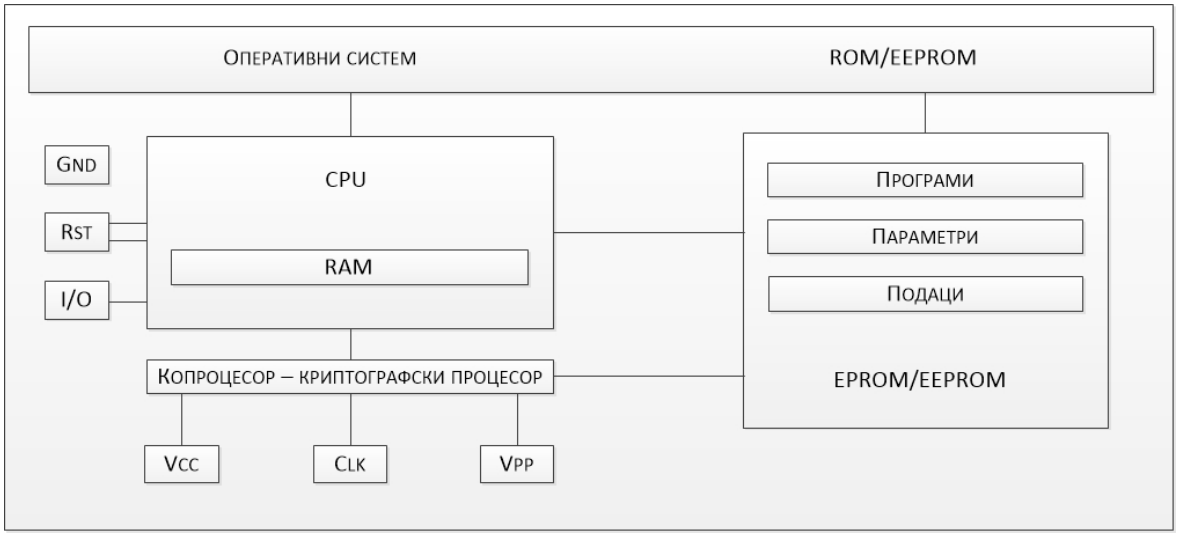
Микропроцесорске картице чувају податке у различитим датотекама које су видљиве само наменским програмима и програмима који се налазе на картици, односно апликацијама које су у оквиру оперативног система. Ове датотеке су организоване тако што постоји једна главна датотека, односно MF (енгл. *Master File*) која се налази у основном (енгл. *Root*) директоријуму који садржи дефиниције, односно заглавља свих осталих датотека. Остале датотеке се називају основним, односно EF (енгл. *Elementary File*) и наменским, односно DF (енгл. *Dedicated File*). Наменске датотеке носе податке о распореду директоријума и датотека, а основне датотеке су оне које садрже податке. Примера ради, PIN код се налази у једној од основних датотека, наменска датотека носи информацију о локацији основне датотеке, а једино картица има приступ вредности тог кода. Ово осликава основни принцип функционисања картице, односно принцип постојања података и постојања правила за приступ подацима. То се реализује захваљујући систему директоријума и датотека, правилима приступа, микропроцесору, RAM, ROM и EEPROM меморији и оперативном систему који њима управља.

Табела 4 Предефинисани називи датотека и директоријума

Датотека	Сврха датотеке
0000	CHV1 (кориснички PIN код)
0001	Унутрашњи кључ
0002	Серијски број картице
0005	Резервисано
0011	Спољни кључ
0012	Приватни кључ
0015	Резервисано
0100	CHV1 (администраторски PIN код)
1012	Јавни кључ
2F01	ATR (енгл. *Answer To Reset*) комуникациони параметри
3F00	Основни (енгл. *root*) директоријум
3F11	Резервисано
3FFF	Резервисано
FFFF	Резервисано

Микропроцесорске картице су, условно речено, сличне компјутерима: имају оперативни систем, могућност за трајно и привремено чување података и централну процесорску јединицу и остали хардвер. Функције оперативног система, зависно до испуњења услова, приступају датотекама, или прихватају комуникацију. Подаци могу бити закључани помоћу PIN кода који се обично састоји од 3 до 8 цифара које су снимљене у одређеној датотеци на картици. Уколико је унети код једнак по вредности коду који се налази на картици, услов је задовољен и комуникација са картицом је дозвољена. Комуникација се реализује преко процесора и не постоји

директна веза између конектора и меморије, односно између читача картица и информација које се налазе у меморији. Ова веза се остварује посредно и оперативни систем је тај који разматра испуњење услова који се заснивају на криптографским алгоритмима и на основу чега се дозвољава, односно забрањује приступ подацима на картици. Обзиром да функције за рад са јавним кључевима захтевају сложена математичка израчунавања, а да постојећи микропроцесори имају радни такт од 3 до 5 MHz, данас већина картица има посебан криптографски процесор, односно чип који убрзава извршење криптографских функција.



Слика 6 Скица компоненти микропроцесорске картице

Највећи број микропроцесорских картица данас има наменски развијен оперативни систем. Обзиром да су намењене за рад на различитим системима, оне морају бити компатибилне са тим системима. Стандард ISO 7816 прописује основне функционалности које морају поседовати паметне картице, међутим захтеви које прописује пракса су доста комплекснији. Један од захтева који је у вези са оперативним системом на картицама јесте могућност динамичке модификације функционалности картица, односно могућност измене функција на картици након њиховог издавања корисницима и активирања. То је важно зато што су честе промене на системима који размењују податке са картицама и који их обрађују, а како корисници не би били приморани да мењају картице, неопходна је могућност аутоматске модификације функционалности.

Међу најпознатијим оперативним системима су JavaCard OS које пружају највиши ниво флексибилности када је у питању развој апликација за њих, затим MULTOS (енгл. *Multi-application Operating System*) који има највиши ниво безбедности у односу на ITSEC (енгл. *Information Technology Security Evaluation Criteria*) и решење које нуди *Microsoft*, за које постоји посебно развијен оквир (енгл. *Framework*) на основу ког се могу даље развијати апликације за картице и за читаче картица.

7.2.1 Микропроцесорске картице и инфраструктура јавних кључева

Микропроцесорске картице представљају одлично место за чување осетљивих података, а у случају здравствених информационих система, оне представљају одлично место за чување личних података медицинских и немедицинских радника са

једне стране и корисника услуга здравствених организација са друге стране. Окружење и радни задаци у овим организацијама захтевају децентрализован информациони систем и честа је појава да запослени требају са различитих локација да приступају подацима и да би их исчитали, изменили или допунили. Постојање дигиталних сертификата и њихова интеграција са чип картицама би омогућило власницима ових картице да могу да приступе жељеним функцијама информационог система, или жељеним подацима са било ког места, при томе преузимајући права и обавезе, као и одговорности у складу са сопственим активностима у оквиру здравственог информационог система.

Да би овакав сценарио био могућ, потребно је реализовати једно од два могућа решења. Прво би било да се у здравствени информациони систем интегрише сервис за додељивање дигиталних сертификата неког другог сертификационог тела, а друго да здравство Републике Србије изгради сопствено сертификационо тело, односно сопствени сертификациони ауторитет (енгл. *Certificate Authority*).

Комплексност здравственог информационог система и специфичност радних задатака његових корисника ствара потребу за увођењем додатног ентитета у систем, регистрационог ауторитета (енгл. *Registration Authority*). Ово тело би било задужено за идентификацију власника дигиталних сертификата, односно за проверу да ли је јавни кључ додељен тачно одређеном појединцу на основу чега би могао да се реализује механизам непорецивости. На основу овога медицински и немедицински радници укључујући и пацијенте би имали личне дигиталне сертификате који би били издати на основу гаранција сертификационог и регистрационог ауторитета. Овај систем би омогућавао аутентификацију посредством валидационог ауторитета (енгл. *Validation Authority*), односно треће стране од поверења.

Сертификат представља јавни кључ власника сертификата који је дигитално потписан тајним кључем којим располаже искључиво сертификациони ауторитет, тако да сви учесници који имају поверење у сертификациони ауторитет, имају поверење и у власника конкретног сертификата. Овакав систем омогућава да дигитални сертификат буде електронска лична карта њеног власника, а микропроцесорска картица је одличан медиј за његово складиштење. Поред јавног кључа, микропроцесорске картице треба да садрже и остале личне податке о власнику, као и податке које повезују дигитални сертификат са организацијом у којој се користи, такође, треба да садрже јединствени идентификатор корисника и његов приватни кључ. Са циљем да приватни кључеви буду довољно комплексни, картице располажу функцијама за генерисање вредности приватних и јавних кључева унутар саме картице због чега не постоји потреба да се приватни кључ напушта оперативни систем картице.

Уколико здравствени радник жели да сними одређену групу података на сервер здравственог информационог система, апликација ће првенствено на картици генерисати шифровану вредност аутентификационих података на основу чега ће започети комуникацију са апликацијом на серверу где корисник информационог система настоји да реализује одређене активности. На овај начин, приватни кључ никада не напушта картицу у свом изворном облику и то значајно повећава безбедносне карактеристике система. Комуникација између клијента и сервера се остварује преко незаштићених линија, али у шифрованом облику што обезбеђује тајност када је у питању слање корисничке лозинке и свих осталих података у даљој комуникацији. Овако се корисник, без обзира на избор клијентског компјутера, може

идентификовати у оквиру информационог система на основу чега може да приступи свом налогу и свим функцијама које његов налог омогућава.

7.3 Аутентификација (идентификација) заснована на биометрији

Биометријска идентификација представља скуп метода које омогућавају идентификацију људи на основу јединствених физичких карактеристика, односно, на основу личног потписа, отиска прста, облика дужица ока, облика лица, вибрација у гласу, мириса и слично. Биометријски уређаји могу потврдити идентитет неке особе тако што снимљене вредности одређених физичких карактеристика упоређују са раније измереним вредностима. Процес аутентификације на основу биометријских података представља најдоследнији вид провере јер су биометријски подаци јединствени па је тај процес истовремено и аутентификација и идентификација корисника. Биометријске методе у процесу аутентификације су заступљене у малој мери, првенствено због потребе за поседовањем специјалних уређаја за мерење природних карактеристика, међутим, и поред комплексности, постоје бројни системи који су данас у употреби, а који користе биометрију, на пример различити уређаји који се откључавају отиском прста, или који реагују на глас. Такође, у последњем периоду масовно се развијају програми за препознавање облика лица, за препознавање покрета тела, тумачење гестова и слично.

Процес биометријска аутентификације може бити веома једноставан, један притисак прстом, или дланом, један снимак ока, изговарање лозинке, или случајне реченице, или једноставан пролазак кроз просторију са сензорима. Биометријске карактеристике се не могу изгубити, украсти, или фалсификовати, али се биометријски подаци могу украсти, а обзиром да су то личне карактеристике које се не мењају, они могу бити злоупотребљени било када у будућности. Због тога је пракса да се ови подаци чувају у шифрованом облику, како не би могли бити злоупотребљени уколико дође до компромитовања тих података. Зависно од потреба система, биометријски подаци могу бити шифровани једносмерним, или двосмерним функцијама. Шифровање двосмерним функцијама омогућава прецизније мерење и прецизнију обраду биометријских података, међутим овакав приступ ствара додатне тешкоће које су у вези са генерисањем и дистрибуцијом криптографских кључева. Шифровање једносмерним функцијама смањује могућност прецизнијег мерења биометријских карактеристика, али пружа могућност квалитетније заштите података.

Највећа предност шифровања једносмерним алгоритмима је у томе што не постоји могућност екстраховања оригиналних података из отисака који се добијају након примене једносмерних функција и у томе што компромитовање биометијских података неће компромитовати читав систем. Идеална биометријска мерења не постоје и није могуће обезбедити потпуно подударање узорака, али је могуће реализовати мерења у складу са одговарајућим биометријским шаблонима што отвара могућност за шифровање једносмерним функцијама. Мерења биометријских карактеристика се реализује на основу предефинисаних скупова биометријских података, односно на основу оног скупа карактеристика које се разматрају приликом снимања и које ће се разматрати приликом упоређивања тих карактеристика. Тако добијени подаци се упоређују на основу биометријских образаца. Постоје две врсте ових образаца, први се користе у системима за препознавање лица, или дужице ока, а други за препознавање карактеристичних тачака на отиску прста, или отиску длана.

Мерење биометријских података на основу великог броја вредности омогућава шифровање једносмерним функцијама јер се упоређује хеш вредност сваке измерене вредности из посматраног предефинисаног скупа, након чега се разматра да ли је подударање довољно велико, односно да ли је број истоветних хеш вредности довољно велик. Упоређивање измереног узорка са сачуваним образацима је подложно грешкама и два узастопна мерења могу дати различите резултате, али се криптографски систем реализује тако да проценат ових грешака буде довољно мали како би било могуће да се за истог субјекта, сваки пут потврди да је онај за кога се представља. Грешке се односе на лажно подударање образаца и на лажно разликовање образаца. Аутентификација је успешна када је мера подударања образаца веће од планиране вредности подударања. Што је задата вредност подударања већа, већа је вредност лажног разликовања, а мања вредност лажног подударања. Зависно до потреба система, дефинишу се различите вредности обе врсте грешака па се у зависности од тога дефинише вредност успешних подударања.

Подаци који су потребни за биометријску аутенификацију се разликују у зависности од технике прикупљања података. Примера ради, приликом мерење биометријских карактеристика ока, подаци се могу поредити методом Хаминговог растојања. Снимљене вредности се претварају у бинарне низове предефинисаних дужина које се упоређују. Ти бинарни низови су карактеристично организовани у зависности од биометријксих образаца, а измерене вредности се снимају након што се коригују уз помоћ система за проверу грешака, односно система који упоређује снимљене вредности са предефинисаним скуповима вредности. Тако се формирају скупови података које је могуће шифровати једносмерним криптографским алгоритмима, а да се не наруши могућност каснијег упоређивања вредности. Након извршене корекције и након шифровања података, добија се довољно велики број хеш вредности које представљају биометријске карактеристике које се упоређују. Уколико је удаљеност за исти субјекат мања од потребне вредности успешних подударања, онда се број потребних хеш вредности коригује док се не добију задовољавајући резултати, односно док не изједначе лажно подударање и лажно одступање образаца.

Имплементација биометријских технологија у здравственом информационом систему још увек не проналази своје место, првенствено због високих трошкова који су у вези са тим технологијама, техникама и самом употребом, али када се у разматрање узме све могућности, наслућују се предности које је могуће искористити. Делује као далека будућност, али системи у којима би присуство у одређеној просторији, или поседовање неког од мобилних уређаја били довољни за идентификацију, аутентификацију и дијагностику би били врхунац у развоју здравственог информационог система. Аутентификација корисника би могла да се реализује креирањем система који би обједињавао унос корисничког имена и лозинке, мерењем биомтеријских података и упоређивањем њихових вредности са постојећим подацима и употребом адекватног криптографског подсистема.

Питања везана са сакупљање личних података и њихову употребу су делимично решена и формалним путем, односно Законом о заштити података о личности, међутим тај закон још увек не уређује довољно прецизно питања која се тичу биометијских метода у процесу идентификације што је неодвојиви део процеса аутентификације. Због тога је пракса да се биометријске методе идентификације могу реализовати у оквиру организација које су надлежне за то, као што су Министарство одбране Републике Србије и Министарство унутрашњих послова

Републике Србије, где постоје адекватни системи заштите. Наравно, то не представља довољно добро решење јер онемогућава друге организације да се баве сакупљањем и обрадом биометријских података, односно не дефинише довољно прецизно права и обавезе, што представља ограничење. Са друге стране, велика количина личних података се обрађује на основу „сагласности“људи што се не може сматрати ваљаним основом јер у великом броју ситуација, на пример када је у питању видео надзор, нико не утврђује да ли постоји сагласност субјеката.

Здравствене организације би, уколико би постојала оправдана потреба, могле да користе биометријске методе у процесу аутентификације. Такав систем аутентификације би могао контролисати физички приступ просторијама, затим, приступ разним медицинским уређајима, односно могућност употребе тих уређаја, онда могућност приступа медијима са аналогним подацима, или дигиталним подацима и слично. Највећа предност биометријске аутентификације је у томе што је могућност злоупотребе веома мала, јер особа која је одговорна за одређени ресурс мора бити физички присутна уколико се приступа том ресурсу. Такође, јединствене биолошке карактеристике стварају недвосмислену везу између корисника и корисничког налога што смањује и могућност преваре. На пример, уколико би се читач отисака прстију поставио на улазима у просторије неке здравствене организације, било би могуће контролисати приступ просторијама и могло би се тачно утврдити где су запослени боравили, у ком временском периоду, па и шта су тада радили. Ово је ситуација у којој не би било могуће регистровати присуство у одређеној просторији посредством неке друге особе, као што је могуће код система са меморијским, или микропроцесорским картицама, већ би идентификација запослених недвосмислено указивала на њихово присуство.

8. Једноструко пријављивање корисника

Једноструко пријављивање корисника, односно SSO (енгл. *Single Sign-On*) представља систем који омогућава клијенту да се пријави на систем и да се након успешне аутентификације читав низ пријављивања на друге системе, односно сервисе, или апликације реализује аутоматски. Овакав вид пријављивања је једна од карактеристика коју мора да поседује здравствени информациони систем Републике Србије. Зависно од имплементације, овакав вид пријављивања може бити реализован привременим чувањем корисничких података у датотекама, у базама података, или у вредностима сесије. Привремено чување ових података представља безбедносну претњу, међутим корисници се пријављују само једанпут, што значајно смањује безбедносни ризик који настаје услед многобројних пријављивања корисника. Овакав систем поједностављује пријављивање јер корисници не морају да памте велики број различитих корисничких података за сваку апликацију посебно. Такође овакав систем штеди време корисника и у мањој мери оптерећује компјутерске ресурсе.

Код овакве аутентификације, обзиром да се само једанпут уносе кориснички подаци, смањује се могућност да неко други види корисничку лозинку и да је касније злоупотреби. Такође, обзиром да се процес пријављивања одвија једнократно ово је идеална околност за комбиновање стандардних начина пријављивања са сложеним као што су употреба чип картица, или примена разних биометријских метода. Сам процес пријављивања на систем је јединствен што, истовремено, представља, и ману и предност. Уколико корисник није аутентификован, он нема могућност приступа ни једном од система, односно, ни једном од сервиса, или апликација. То може бити проблем, уколико је у питању стандардни корисник, али ако је у питању злонамерни корисник, то је предност у смислу безбедности јер тај корисник неће бити аутентификован ни за један од система.

8.1 Клијентски и кориснички налози

Клијентске налоге, као што је до сада и била пракса, треба везати за компјутерске ресурсе. Свака радна станица треба да има свој клијентски налог, а у оквиру системских подешавања треба да се дефинишу сва права у вези са употребом осталих компјутерских ресурса који су повезани за ту радну станицу, односно на друге компјутере, штампаче, скенере и на специјализовану медицинску опрему и слично. Ови налози се могу подесити захваљујући различитим *Single Sign-On* системима и *Single Sign-On* серверима. Са друге стране, једноструко пријављивање и обједињавање пријављивања клијента и корисника ствара бројне безбедносне ризике. Такође, није потребно, па ни оправдано, да сваки корисник има сопствени кориснички налог за сваки систем, или сервис који користи. Такође, везивање корисничких налога за радне станице узрокује ограничење приступа информационом систему, обзиром да је честа ситуација у којој се здравствени радници распоређују на оне радне задатке где постоји потреба за њима. Ово је ситуација у којој је потребно размотрити три врсте фактора: безбедносне, економске и практичне и на основу тога предложити оптимално решење.

8.1.1 Клијентски налози

Аутентификација клијената у здравственом информационом систему која је реализована на принципима једноструког пријављивања, а која је истовремено одвојена од аутентификације корисника тог система, може бити добро решење. Свака радна станица која се пријављује на мрежу, у зависности од системских подешавања, приступа и користи различите ресурсе у тој мрежи. На тај начин се избегава конфузија у обављању радних задатака у оквиру различитих организационих целина, истовремено се прави подела одговорности везана за употребу компјутерске и здравствене опреме. Сви запослени временом схвате на који начин могу да приступе различитим уређајима које сви користе као што су штампачи, скенери, или нека друга уобичајена компјутерска опрема. Са друге стране, када је у питању софистицирана здравствена опрема, здравствени радници који су обучени за употребу те опреме, могу чувати у тајности приступне податке и тако обезбедити да само стручно особље користи ту опрему.

Single Sign-On системи и сервери нуде могућност аутентификације клијената који се налазе у оквиру радних група, у оквиру локалних компјутерских мрежа, или у оквирима глобалне компјутерске мреже, Интернета. Обзиром на то, овакви сервиси пружају значајне могућности. Они се првенствено се базирају на обједињавању свих система аутентификације, и на нивоу апликација за управљање опремом и на нивоу апликација за управљање подацима. Те предности треба искористити селективно и омогућити једноструко пријављивање корисника када су у питању апликације за употребу различитих мрежних уређаја уз истовремено изоловано једноструко пријављивање корисника када су у питању апликације за управљање подацима. Тако би се, уз смањене трошкове, омогућила квалитетна аутенитификација и ауторизација корисника јер би се користила постојећа решења, које у зависности од потреба могу бити и нека од бесплатних решења отвореног кода. Истовремено би се остварио довољно висок ниво безбедности обзиром да би систем једноструког пријављивања корисника на нивоу апликација за манипулацију подацима био изолован.

Single Sign-On системи се понашају ако апликације средњег нивоа посматрано у односу на апликације које приступају различитим ресурсима, које се налазе изнад и разних постојећих система за аутентификацију, као што су *Windows Active Directory*, IBM *Resource Access Control Facility* и слично, који су испод. Њихов основни задатак је синхронизација корисничких налога. Ова синхронизација се реализује централизацијом шифрованих података за приступање систему, који се налазе у бази података са налозима (енгл. *Credential Database*) и транспортом ових података, такође у шифрованом облику, у оквиру информационог система, без обзира на врсту компјутерске мреже на којој је тај систем реализован. Зависно од потреба, у информационим системима се може налазити и *Single Sign-On* сервер који је задужен за генерисање, чување и безбедан транспорт главног кључа за шифровање (енгл. *Master Encryption Key*). *Single Sign-On* сервис користи главни кључ како би се на основу њега шифровали и дешифровали подаци о налозима. Системским подешавањима на том серверу могу приступити искључиво *Single Sign-On* администратори и једино они могу генерисати вредност главног кључа, или је заменити новом, након одређеног временског периода.

8.1.2 Кориснички налози

Један од важних фактора утицаја на безбедност једног информационог система јесте понашање корисника тог система. Начин на који корисници употребљавају постојећи здравствени информациони систем указује да се мало пажње посвећује едукацији запослених, а то узрокује бројне безбедносне ризике. Систем је имплементиран тако да се запослени пријављују приликом учитавања оперативног система, са том разликом што се један део запослених додатно пријављује када покреће неку од специјализованих апликација. Овако реализован систем пријављивања корисника није потпуна имплементација једноструког пријављивања корисника и не задовољава постављене критеријуме, односно имплементацију *Single Sign-On* система.

Корисници постојећег здравственог информационог система често за корисничке лозинке бирају низове од малог броја карактера, некада два или три карактера, поред тога, честа је ситуација да они остају пријављени на систем и када нису присутни, односно када заврше са радом, такође, често се дешава да више различитих корисника употребљава исти налог, тако да се мало може закључити о активностима корисника. Управо због тога, постојање система једноструког пријављивања представља добро решење. Пуна реализација *Single Sign-On* сервиса у оквиру здравственог информационог систем Републике Србије треба да укључи и дигиталне сертификате након чега би било могуће потпуно реализовати овакав систем. Тако би се достигао довољно висок ниво безбедности, сви корисници би имали јасно дефинисане привилегије и одговорности које су у складу са тим привилегијама.

Најједноставније техничко решење за једноструко пријављивање корисника је синхронизација корисничких налога, односно систем који обједињава све корисничке лозинке тако што промена једне лозинке, аутоматски повлачи промену свих осталих. Овакав систем подразумева да корисник има кориснички налог креиран за сваку апликацију посебно и потребу да се посебно пријављује за сваку апликацију. Другачије и комплетније решење за једноструко пријављивање представља аутоматско пријављивање на различите апликације. Сви подаци о корисничким налозима се налазе на једном месту и њима располаже апликација која је намењена аутентификацији корисника. Корисник се пријављује само једанпут док апликација, у зависности од привилегија корисника, одређује за које апликације је корисник аутентификован, односно за које функције је ауторизован.

Највећи број *Single Sign-On* система је развијен на *Kerberos* протоколу. Овај протокол је намењен аутентификацији клијентских и серверских компјутера у компјутерским мрежама са клијент – сервер архитектуром. *Kerberos* функционише захваљујући тикетима (енгл. *tickets*) који се размењују између мрежних уређаја у оквиру одређене мреже, а који садрже податке на основу којих је могуће реализовати аутентификацију и шифровану комуникацију између учесника у комуникацији путем мреже која није заштићена. Овај протокол обезбеђује сервисе интегритета и поверљивости података који се размењују у мрежи. *Kerberos* се заснива на комбинацији симетричне и асиметричне криптографије при чему у комуникацију укључује друге ентитете од поверења, односно сервер за аутентификацију и сервер за додељивање тикета на основу којих је могуће реализовати различите системе за једноструко пријављивање корисника.

Аутентификација клијената захваљујући овом протоколу се реализује на бази симетричних кључева где сваки корисник има свој кључ. То се реализује тако што у комуникацији посредује центар за дистрибуцију кључева, односно KDC (енгл. *Key Distribution Center*) који додељује кључеве клијентима и самим тим, се у комуникацији појављује као трећа страна од поверења, односно TTP (енгл. *Trusted Third Party*). Успостављање оваквог ауторитета у комуникацији подразумева имплементацију асиметричне криптографије и успостављање инфраструктуре јавних кључева, односно PKI (енгл. *Public Key Infrastructure*). То је посебно значајно обзиром да центар за дистрибуцију кључева поседује симетричне кључеве свих учесника у комуникацији и као такав представља најрањивије место у ланцу комуникације.

Имплементација овог протокола подразумева да се након аутентификовања сервера и клијента, успоставља кључ сесије након чега сервер конкретном клијенту додељује тикет који садржи кључ за ту сесију, након чега се успоставља и сама сесија. Сваки тикет је шифрован од стране центра за дистрибуцију кључева и то кључем који познат само њему. То обезбеђује да се центар за дистрибуцију кључева у комуникацији појављује као ауторитет који гарантује тајност комуникације, односно као трећа страна од поверења. Центар за дистрибуцију кључева омогућава посредно симетрично шифровање комуникације између клијената на основу базе података коју дистрибуира свим клијентима која је такође шифрована симетричним алгоритмима.

9. Аутентификација сервера

Интернет протокол (енгл. *Internet Protocol*) управља адресирањем чиме се постиже да сваки уређај који је повезан на Интернет, или на неку мању компјутерску мрежу, има јединствену адресу. Поред тога, Интернет протокол управља усмеравањем података на основу чега се они шаљу са предајног на пријемно место уз одређивање оптималне путање за њихов пренос. Међутим, овај протокол не подразумева успостављање везе пре слања података и не подразумева међусобну идентификацију предајне и пријемне стране. Такође, пренос података је непоуздан јер не постоје гаранције за испоруку и исправност испоручених података. Подаци се приликом транспорта могу оштетити, може се догодити да пакети података не стигну по редоследу, да се дуплирају, или да се потпуно изгубе приликом транспорта.

Обзиром да је Интернет протокол ослобођен бројних механизама који обезбеђују поузданост транспорта и безбедност података, адресирање уређаја и усмеравање пакета (енгл. *Routing*) је релативно брзо. Поред овог, постоје и други мрежни протоколи од којих сваки има своју улогу, а Интернет протокол увек функционише у сарадњи Протоколом за контролу преноса, односно TCP (енгл. *Transmission Control Protocol*). Овај пар, односно TCP/IP, се налази у самој основи функционисања Интернета и он представља стандард чије поштовање омогућава успостављање и успешно контролисање комуникације путем Интернета. Међутим, ови протоколи подразумевају адресирање уређаја помоћу њихових IP адреса што је веома непрактично када су у питању крајњи корисници. Корисницима је једноставније да памте симболичка имена ресурса до којих желе да дођу, уместо њихових нумеричких адреса, па је због тога уведен Систем доменских имена, односно DNS (енгл. *Domain Name System*).

DNS је систем превођења Интернет домена појединачних компјутера, компјутерских мрежа, или група компјутера у њихове IP адресе (енгл. *Internet Protocol Address*). Сваки ресурс на Интернету има јединствену IP адресу, а DNS памти и повезује те адресе са симболичким именима тако што их поистовећује. Подаци о томе се налазе у бази података која је дистрибуирана на серверима који су задужени за превођење IP адреса у имена домена и обрнуто. DNS у основи чине подаци о именима домена и одговарајућим IP адресама и скупови функција које су задужене за превођење. Захваљујући томе, уколико клијент, на пример: Интернет претраживач, пошаље захтев за неким јавним Интернет доменом, или јавном IP адресом, он једноставно и аутоматски долази до жељених Интернет зона, односно до жељених Интернет ресурса.

DNS чине хијерархијски повезани DNS сервери. За сваки од домена, односно за сваку од зона постоји један, или више надлежних DNS сервера који чувају и манипулишу информацијама о доменима, такође, један DNS сервер може бити задужен за више независних домена. Основу хијерархије DNS сервера чине корени сервери (енгл. *Root Servers*) који су задужени за домене највишег нивоа (енгл. *Top Level*), односно домене који се налазе у самој основи хијерархије, а на њих се надовезују сервери задужени за више нивое. Након слања захтева за неким Интернет доменом, део серверског софтвера за разрешавање тог захтева (енгл. *DNS Resolver*) започиње процес у ком настоји да разреши тај захтев. Уколико DNS сервер нема податке о жељеном домену, он прослеђује захтев другом DNS серверу који се налази на следећем хијерархијски вишем нивоу у односу на њега. Након што се захтев

неколико пута проследи кроз хијерархију DNS сервера, жељени Интернет домен се разрешава, а резултат је IP адреса жељеног ресурса.

DNS у комбинацији са TCP/IP протоколима чини основу на којој почива Интернет, међутим он не поседује безбедносне механизме и не може реализовати безбедносне функције. Одсуство безбедносних функција отвара бројне могућности за превару или злоупотребу. Различите нерегуларне измене DNS кеша на DNS серверима могле би омогућити нападачима да пошаљу разне нетачне податке другим корисницима са циљем да их погрешно информишу, или да прикупљају њихове личне податке са циљем да их касније злоупотребе. Ово би било нарочито штетно када је у питању здравствени информациони систем. Уколико би неко неовлашћено прикупљао податке о пацијентима, о медикаментима које троше, или дијагностичке податке пацијената ако је у питању надзирање биолошких параметара на даљину, он би могао да их злоупотреби у сврху стицања конкурентске предности на тржишту, или на неки други начин. Како би се то предупредило, осмишљена су и имплементирана бројна проширења којим се овакве активности онемогућавају, или своде на мању меру.

9.1 Систем доменских имена

Седамдесетих година прошлог века, Америчко Министарство одбране (енгл. *United States Department of Defense*) је донело одлуку за креирање компјутерске комуникационе мреже. Реализација те мреже је поверена организацији Министарства одбране Сједињених Америчких Држава за развој нових војних технологија, односно DARPA (енгл. *Defense Advanced Research Projects Agency)* по чијем имену је, након реализације, та мрежа добила име: ARPAnet. Данас се ова мрежа сматра претечом Интернета јер је њеном реализацијом направљен и нови протокол који је дефинисао пакетски пренос података, адресирање мрежних уређаја на основу IP адреса, одређивање оптималних путања за слање података, комуницирање између различитих компјутерских мрежа и између различитих типова уређаја повезаних на мрежу. Убрзо након реализације ове мреже постале су очигледне њене могућности и бројне предности које пружа овакав вид комуникације. То је довело до њеног наглог развоја, а затим и до реализације Интернета, мреже коју данас познајемо.

Први проблем на који је наишао ARPAnet био је у вези са наглим порастом броја уређаја које је требало повезати, односно адресирати. Тај проблем је превазиђен захваљујући решењима које је понудила организације под називом IANA (енгл. *Internet Assigned Numbers Authority*). Ова организација је проблеме адресирања уређаја на мрежи решила кроз достизање неколико циљева. Ти циљеви су били у вези са глобалним надзором расподеле IP адреса, затим у вези са реализацијом и управљањем системом доменских имена и доношењем и реализацијом бројних стандарда везаних за бројеве и симболе у Интернет протоколу. Почетно су уређаји били адресирани искључиво нумеричким адресама, међутим то није било адекватно решење обзиром на промену типа корисника Интернета, односно на пораст боја корисника и обзиром на то да је Интернет, поред едукативне и истраживачке сврхе, све више добијао на значају као средство у пословном посредовању, рекламирању, забави и слично. Ускоро након тога, 1984. године је реализован DNS чиме је адресирање уређаја на мрежи добило данашњи облик.

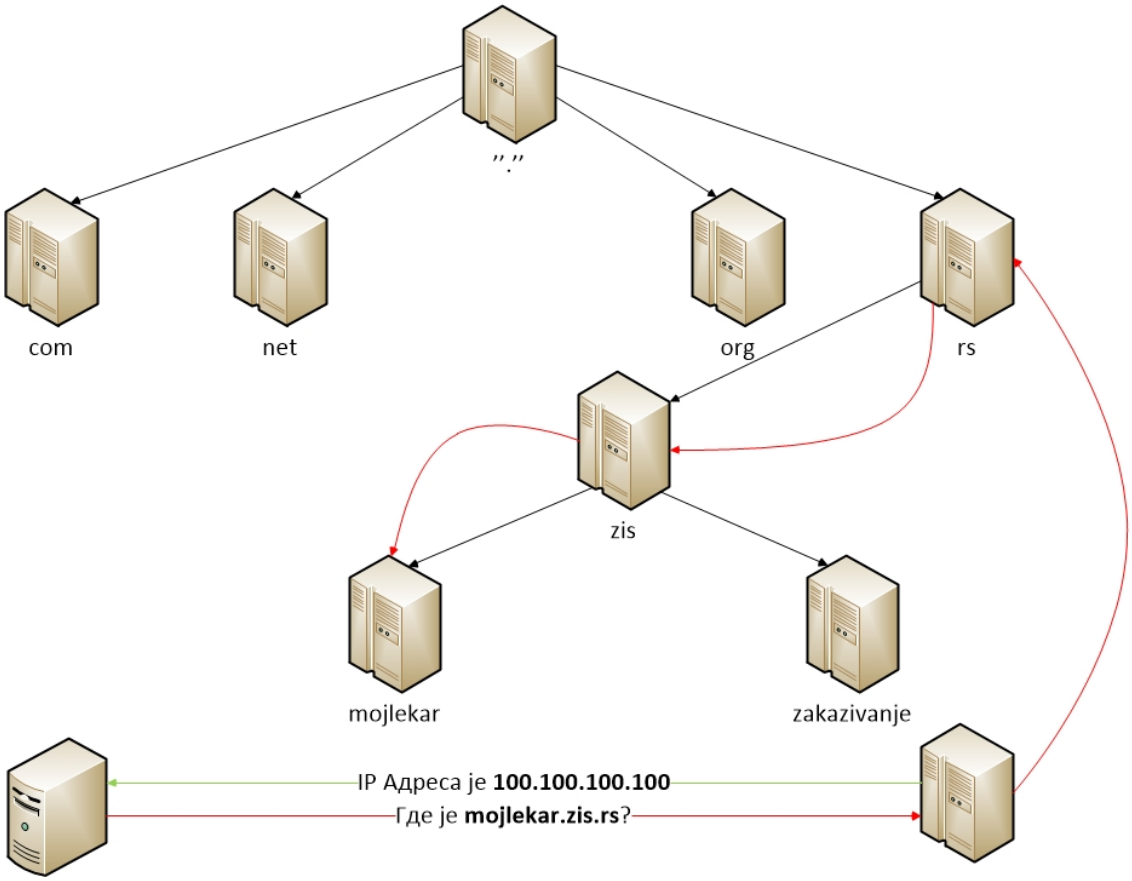
Даљи развој Интернета је омогућен појавом приватних Интернет провајдера, 1991. године, и појавом приватних организација за регистрацију Интернет домена, 1992. године, које су пословале по законима тржишне економије што је довело до значајног смањења цена услуга. Након формирања компаније под називом ICANN (енгл. *Corporation for Assigned Namesand Numbers*), 1998. године, централизована је координација функционисања и развоја Интернета на глобалном нивоу. Њеним оснивањем је, у институционалном смислу, омогућена сарадња заинтересованих страна да учествују у стварању и да спроводе регулативу у вези са функционисањем и развојем Интернета. Такође, ICANN је омогућио акредитовање великог броја организација које корисницима омогућавају регистрацију нових домена. Тако је створен Заједнички систем за регистрацију домена (енгл. *Shared Registration System*) и омогућено је децентрализована регистрација домена у складу са регулативном политиком и у складу са законима тржишне економије.

Адресирање мрежних уређаја на Интернету се реализује захваљујући IP адресама тих уређаја. Обзиром да је тешко памтити нумеричке адресе, реализован је систем додељивања имена уређајима који су повезани на мрежу, односно Систем доменских имена где су сви компјутери били именовани у мрежи уз помоћ *host* фајлова који су били снимљени на тим компјутерима. Овај систем су заменили дељени, односно дистрибуирани *host* фајлови, а затим дистрибуиране базе података. Ови фајлови још увек могу бити алтернативно решење за DNS и могу се применити у мањим локалним мрежама и уз аутоматске софтверске, или мануелне, односно ручне измене садржаја тих фајлова. Међутим, адресирање компјутера уз помоћ *host* фајлова је непрактично. Поред тога што је потребно мењати њихов садржај на свим компјутерима уколико дође до промене броја компјутера, њиховог назива, или адресе у мрежи, овакав систем је доста спорији од система доменских имена. Данас у великим мрежама попут Интернета, систем за именовање уређаја чине хијерархијски повезани DNS сервери од којих је сваки појединачно, или свака група задужена за чување, обраду и давање информација о наведеним доменима.

Систем доменских имена је организован хијерархијски тако да за сваку ставку и сваки ниво постоји запис у DNS серверу надлежном за ту зону. Сваки надлежни DNS сервер (енгл. *Authoritative Name Servers*) располаже подацима за ту зону и за зоне које се налазе на хијерархијски нижем нивоу. Приликом слања захтева за неким доменом, серверски софтвер за разрешавање тог захтева (енгл. *DNS Resolver*) рекурзивно покушава да дође до података које чувају сервери, а након тога их повезује у комплетан назив домена, односно повезује име жељеног ресурса на Интернету са његовом IP адресом. Назив домена (енгл. *Domain Name*) се састоји од, најмање, два дела раздвојених тачкама. Посматрано са десне стране ка левој, први део представља назив највишег домена, а сваки наредни део представља назив поддомена највишег домена, односно поддомен првог надређеног домена.

На самом врху хијерархије домена се налази основни домен (енгл. *Root Domain*) који се означава тачком. На њега се надовезује домен највишег нивоа, односно TLD (енгл. *Top Level Domain*) који, у зависности од прихваћене поделе, може бити TLD везан за државе, на пример: *rs* – Република Србија, *ru* - Руска Федерација, или *de* - Савезна Република Немачка, затим генерички TLD који се користи за одређену категорију организација, на пример: *com* – за комерцијалне организације, *edu* – за едукативне организације, *coop* – за невладине организације, или *museum* – који је предвиђен за музеје. Поред наведених постоји и инфраструктурни домени највишег нивоа. Следеће, ниже подручје у односу на TLD

представљају домени другог нивоа, односно SLD (енгл. *Second Level Domain*) и те домене могу регистровати правна и физичка лица под условом да ти домени нису већ у употреби. На следећем, најнижем подручју у односу на домене другог нивоа, налазе се поддомени (енгл. *Subdomain*). Поддомен се може произвољно додати испод већ регистрованих домена.



Слика 7 Разрешавање имена домена

Једини инфраструктурни домен највишег нивоа је *arpa*. Његови домени другог нивоа имају различите функције, na пример *in-addr.arpa* и *ip6.arpa* омогућавају обрнуто мапирање (енгл. *Reverse DNS Lookup*), односно проналажење имена компјутера на основу његове IP адресе. Обрнуто мапирање је практично у борби против слања нежељене поште (енгл. *Anti Spam techniques*). Техника филтрирања се заснива на провери логичности назива домена добијених из IP адреса сервера који шаљу пошту. Примера ради, домен *dynamic-ip.com*, не би задовољио очекиване критеријуме. Такође, обрнуто мапирање омогућава да се направи верификација која проверава да ли постоји унапред дефинисан пар доменског имена и одговарајуће IP адресе, односно FCrDNS (енгл. *Forward Confirmed Reverse DNS*). Иако оваква провера не представља вид идентификације сервера, довољно је добар начин да се сервер нађе на листи привилегованих, односно пожељних (енгл. *Whitelist*). Поред домена који служе обрнутом мапирању, постоје *uri.arpa* и *urn.arpa* за апликације које користе DNS заснован на DDDS (енгл. *Dynamic Delegation Discovery System*) најчешће у Интернет телефонији, или *e164.arpa* за мапирање бројева телефона.

9.2 Безбедносни проблеми

Систем доменских имена је у периоду од петнаест година функционисао без већих проблема, ако се изузме недовољно брзо ажурирање података DNS записа и уколико се изузме рањивост система на измену података о DNS записима. Подаци који се транспортују путем Интернета се усмеравају зависно од полазишта и коначног одредишта. При томе су датотеке које се транспортују подељене у мање целине, односно у пакете података који се транспортују независно и који не морају ићи изворним редоследом и једнаким путањама од полазишта до одредишта. Обзиром да је DNS имплементиран тако да аутоматски регулише повезивање предајне и пријемне стране и обзиром да у основи нема безбедносне механизме, потенцијални нападачи, релативно лако, могу искористити његове безбедносне пропусте.

DNS напади се односе на компромитовање система којим се врши превођење словног записа назива неке станице на Интернету, односно имена домена, у бинарни запис, односно Интернет протокол адресу. Интернет клијенти комуницирају са дистрибуираном базом података на DNS серверима и када неки од сервера нема податке, односно нема могућност мапирања жељеног захтева, односно повезивања имена домена и IP адресе, он прослеђује тај захтев другом блиском DNS серверу. Том приликом, север који је упутио захтев архивира нову путању мапирања као би се она могла користити у наредном временском периоду. Одсуство аутентификације сервера и клијента представља безбедносни ризик и омогућава нападачима да убеђују или да убеде клијенте да је повратна порука аутентична и да их тако усмере ка лажним Интернет ресурсима.

DNS напад се може извести на разним местима у комуникационом ланцу. Када нападач приступи DNS бази података он је у могућности да измени одређени запис, или групу записа и да преусмери будуће клијентске захтеве на лажну Интернет адресу ка лажној Интернет апликацији која у свему подсећа на оригиналну и да тако злоупотреби поверење корисника те апликације. Наравно, Интернет се заснива и на другим системима који у одређеној мери повећавају ниво безбедности, првенствено на SSL (енгл. *Secure Socket Layer*) протоколу и на његовом наследнику TLS (енгл. *Transport Layer Security*) протоколу, међутим тиме није решен проблем аутентификације сервера и клијената који учествују у комуникацији. DNSSEC, и ако није у потпуности имплементиран, може се размотрити као једно од решења за овај проблем.

9.3 Безбедносна проширења

Потенцијални нападачи могу, уз релативно мало знања и уз мала улагања, пресрести неки од захтева који је прослеђен DNS серверу и преузети контролу над сесијом, након чега је могуће посматрати комуникацију и прикупљати, па и злоупотребити осетљиве податке о корисницима. Наравно, могуће је и открити такве активности, али оптимално решење за отклањање оваквих безбедносних претњи се налази у превентивном деловању, односно у развоју и имплементацији безбедносних проширења за DNS. Та проширења у комбинацији са Системом доменских имена чине Систем доменских имена са безбедносним проширењима, односно DNSSEC (енгл. *Domain Name System Security Extensions*). Ова технологија је развијена да

делује превентивно када су у питању овакви и слични безбедносни ризици и она се заснива на дигиталном потписивању података.

DNSSEC представља оптимално решење за аутентификацију Интернет сервера. Обзиром да ова технологија не подразумева шифровање података већ само дигитално потписивање одговора добијених од DNS сервера, а на основу захтева упућених од стране клијената, она обезбеђује добре перформансе уз мале трошкове. Међутим, у односу на DNS без безбедносних проширења, за функционисање DNSSEC – а је потребно више ресурса и више времена за одговор, односно за обраду и слање података. Дигитално потписивање је захтевно када је у питању процесорска снага. Количина података коју је потребно обрадити и транспортовати је од три до шест пута већа у односу на систем доменских имена без безбедносних проширења, поред тога, дистрибуција кључева је такође веома захтевна обзиром на велики број кључева и на њихову комплексност. На то се надовезују проблематика администрације и проблематика контроле над тим ресурсом, односно контроле над DNSSEC – ом.

DNSSEC омогућава потврду аутентичности порекла податка и интегритет податка помоћу криптографије са јавним кључевима и шифровањем употребом елиптичних кривих (енгл. *Elliptic Curve Cryptography*). Потпуна имплементација DNSSEC – а обезбеђује верификацију сервера и омогућава крајњим корисницима да се повежу на жељени сервер, или да дођу до жељених ресурса на основу доменског имена. Корисници при томе могу бити сигурни да одговор потиче од ауторитативног сервера задуженог за конкретну зону и да су добили тачну IP адресу. Такође, захваљујући дигиталном потписивању, ова технологија омогућава да се постигне интегритет одговора, односно потврда да одговор DNS сервера није мењан на свом путу. Са друге стране, DNSSEC не поседује систем заштите од онеспособљавања сервера или неких других виталних делова комуникационе инфраструктуре, односно не поседује систем заштите од DDoS (енгл. *Distributed Denial of Service*) напада који узрокују закрчење пропусног опсега. Такође, DNSSEC ни на који начин не поседује систем за проверу тачности DNS података, па иако је могуће сачувати интегритет података, то не мора нужно значити да су подаци тачни и да су DNS сервери правилно подешени.

Безбедносна проширења имплементирана у DNSSEC подразумевају додавање података у већ постојећи систем, у DNS. Потпис, односно SIG (енгл. *Signature*) је запис који је предвиђен за чување дигиталног потписа у Систему доменских имена. Он обухвата криптографско повезивање Интернет ресурса који је дигитално потписани, затим податке о томе ко потписује тај ресурс, односно име домена и податке о временском периоду у ком је тај потпис валидан. Уколико сервер подржава DNSSEC он ће на захтев клијента покушати да одговори адекватним одговором у виду релевантног записа и одговарајућег потписа. Потпис конкретног записа садржи податке о алгоритму који је коришћен, периоду валидности, потписнику и дигиталном потпису. Поред података о алгоритмима за дигитално потписивање и за криптографију са јавним кључевима, резервисан је простор за дефинисање разних приватних алгоритама који се могу подешавати локано, што може представљати основни извор безбедности за информационе системе који су реализовани уз подршку Интернета. Обзиром да је име потписника истовремено и име домена, на тај начин се обезбеђује једнозначна идентификација DNS записа и SIG записа.

Кључ, односно KEY (енгл. *Key*) је запис који садржи јавни кључ из пара јавног и приватног кључа и он је генерисан на основу DNS имена домена. Власник кључа (енгл. *The Owner*) може бити DNS зона, клијент који приступа Интернет ресурсима, сервер на ком се физички налазе Интернет ресурси, или неки други ентитет. Запис о Интернет домену, или о неком другом Интернет ресурсу може бити здружен са више различитих записа са дигиталним потписима у зависности од власника кључа. KEY запис садржи кључ, затим алгоритам са којим је кључ третиран, и индекс протокола у зависности од намене кључа. Додатно, овом рекорду се може додати и индекси симетричних кључева, односно алгоритама за размену симетричних кључева. Индекс протокола се разликује у зависности од тога да ли се кључеви користе у TLS протоколу (енгл. *Transport Layer Security*), за шифровање електронске поште, DNSSEC – у или IPSec (енгл. *Internet Protocol Security*) протоколу, такође он носи и податак о томе да ли се кључ може користити у свим протоколима. Поред овога, KEY запис располаже резервисаним простором за нове протоколе које је могуће додати у будућности.

DNS има могућност да кешира (енгл. *Cache*) негативне одговоре. Негативан одговор значи да не постоји запис о Интернет ресурсу који је дефинисан у клијентском захтеву. DNSSEC обезбеђује дигиталне потписе и у случају непостојећег имена (енгл. *Nonexistent Name*), како би одређена зона могла бити аутенификована. NXT (енгл. *Nonexistent*) запис указује на опсег непостојећег DNS имена, или на записе који су из различитих разлога недоступни за постојеће DNS име. Да би DNS могао да пошаље позитиван одговор, односно да би занемарио неслагање између имена власника и имена Интернет ресурса, DNS користећи концепт првог следећег имена. Када клијент пошаље захтев за непостојећим именом, сервер одговара клијенту одговором у виду NXT записа који садржи DNS име првог следећег DNS записа по канонском редоследу. Када недостаје запис за постојеће DNS име, NXT запис садржи DNS име и адекватни потпис који је генерисан на основу дигиталног потписа постојеће зоне.

Дигитални сертификат за сервере, односно CERT (енгл. *Certificate*) је запис који садржи податке о алгоритмима који су коришћени, затим типовима сертификата и о врсти конкретног сертификата. Додатно, овај запис може садржати податке о алгоритмима који су коришћени приликом генерисања вредности које су смештене у KEY и SIG записе, а који нису предефинисани за употребу у оквиру DNSSEC – а. То омогућава да дигитални сертификат буде креиран уз помоћ алгоритама који нису стандардни за DNSSEC, док су уобичајени типови сертификата дефинисани X.509 стандардом. Један део CERT записа садржи путању до Интернет локације, односно апсолутни URI (енгл. *Uniform Resource Identifier*) на којој се може наћи детаљна документација конкретном формату сертификата. Та документација, такође, подразумева и листу повучених сертификата, односно CRT (енгл. *Certificate Revocation List).* Безбедност података је разлог за постојање CERT записа. То је важно због тога што се тако омогућава да DNS приступи јавним кључевима разних Интернет ресурса, а да при томе не приступа директно KEY запису, већ да само упоређује вредности након примене криптографских алгоритама на податке који су стигли у оквиру конкретног захтева.

Употреба јавних кључева приликом дигиталног потписивања сервера, односно DNSKEY (енгл. *Domain Name System Public Key)* и употреба низова дигитално потписаних података у сврху делегирања потиса, односно DS (енгл. *Delegation Signer*) омогућава да се докаже да је подређена зона дигитално потписана

и тиме се експлицитно дефинише делегација. Ови додаци не шифрују податке и не мењају постојећи систем датотека и директоријума што омогућава потпуну компатибилност са постојећим DNS апликацијама. Они, такође, не утичу на постојећи протокол који је задужен за адресирање већ се на њега надовезују низом дигиталних потписа за сваки ниво у DNS хијерархији, тиме градећи ланац поверења. Приликом провере аутентичности, DNSSEC прати ланац поверења до основног домена (енгл. *Root Domain*) аутоматски проверавајући сваки подређени домен. Обзиром да је за сваки ниво аутентичност делегирана од стране надређеног нивоа, једина вредност коју је потребно проверити у целом домену јесте аутентичност најнижег домена јер се подразумева аутентичност свих надређених домена.

DNSSEC подразумева дигитално потписивање са две врсте криптографских кључева: дугорочни кључеви за дигитално потписивање краткорочних кључева како би се омогућила њихова провера, односно KSK (енгл. *Key Signing Key*) и краткорочни кључеви за дигитално потписивање DNS записа, односно ZSK (енгл. *Zone Signing Key*). Сви криптографски кључеви се морају мењати у оптималним року како би се спречило њихово компромитовање. Уколико би потенцијални нападач имао довољно времена да примени напад грубе силе и да открију приватни кључ од пара кључева за шифровање, овај систем не би био безбедан. DNSSEC превентивно делује заменом и повлачењем кључева у оптималним временским периодима што смањује могућности напада. Тај временски период је кратак када су у питању краткорочни кључеви за потписивање зона, а дужи, најчешће годину дана, када су у питању дугорочни кључеви. Обзиром да се са KSK потписују ZSK, а са ZSK потписују DNS записи, једино је KSK потребан како би се проверила аутентичност DNS записа.

9.3.1 Имплементација у здравственом информационом систему

Практично, DNSSEC није у потпуности реализован. Када би сви домени највишег нивоа били дигитално потписани, било би потребно да се дигитално потпишу и сви остали домени који се налазе на другом нивоу, а из чега би могла да се потврди и аутентичност њихових поддомена. То је једини начин да се креира ланац поверења за све домене на Интернету, а у том процесу је дигитално потписивање домена највишег нивоа само почетак. Поред тога, да би DNSSEC могао да потврди аутентичност DNS записа и да би могао да обезбеди интегритет тих података, он мора бити доследно тестиран како би се избегла појава случајних, или злонамерних грешака. Порастом поверења у сигурност коју омогућава DNSSEC и превазилажењем проблема који настају услед недоследности приликом његове реализације могуће је да DNSSEC постане најзначајнији систем за проверу валидности и аутентичности ресурса на Интернету.

Потпуна реализација овог система подразумева његову интеграцију у само језгро Интернета и то, сигурно, није процес који је могуће реализовати нагло и скоковито, већ постепено и безбедно. Најсложенија проблематика је у вези са управљањем криптографским кључевима. Такође, да би се креирао комплетан ланац поверења, дигитално потписивање мора бити централизовано и ту настаје један од важнијих проблема, обзиром на то да онај који дигитално потписује DNS записе, држи кључеве Интернета. Владе моћних држава Света и руководства великих светских корпорација желе да преузму контролу над кључевима за потписивање Интернет зона, а самим тим и над информацијама.

Овакве организације су највећи заговорници потпуне имплементације DNSSEC – а. Оне су, истовремено, и највећи спонзори његовог развоја. Такво понашање је логично обзиром на чињеницу да контрола Интернета на овај начин, представља извор моћи и могућност утицаја на даљи развој Интернет технологија и на обезбеђивање информационе и економске предности. Наравно, потпуна имплементација DNSSEC – а није услов за креирање система за аутентификацију сервера. Здравствени информациони систем треба да има свој интерни систем међусобне аутентификације клијента и сервера. Реализација таквог система би била могућа захваљујући бројним програмима који су креирани у ту сврху. Велики број тих програма је бесплатан и отвореног кода (енгл. *Opensource*), међутим, то најчешће представља и њихову ману, јер ако је неки софтверски производ бесплатан то значи да није довољно добар, а када је у питању безбедност информационог система, ту се не смеју правити компромиси.

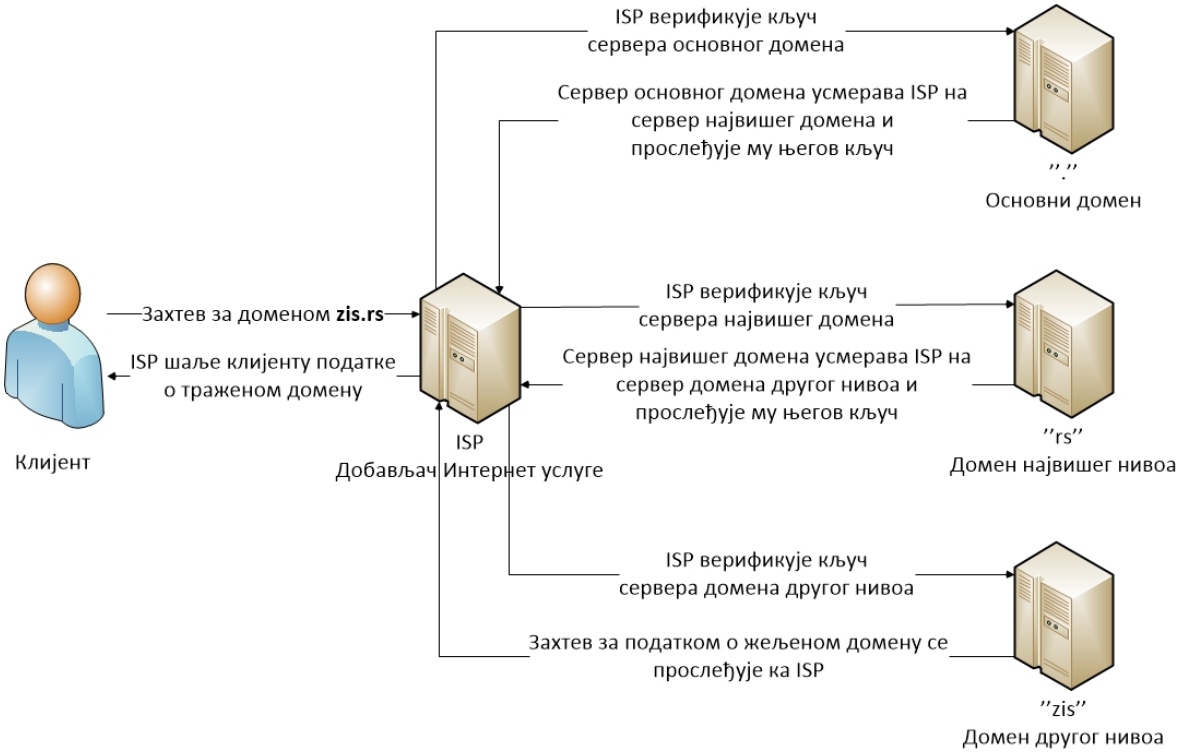
Поступак потписивања Интернет зона подразумева примену криптографије са јавним кључевима и употребу асиметричних алгоритама. Почетни корак је генерисање два криптографска кључа: први за потписивање Интернет зоне, а други за потписивање тог кључа, односно генерисање пара кључева, јавног и тајног за сваки од њих. Софтвер за потписивање је често конципиран тако да корисницима омогућава да изаберу између неколико понуђених алгоритама за креирање отиска поруке. Након креирања парова јавних и тајних кључева, њихове вредности се смештају у одговарајуће датотеке, првенствено у две датотеке од којих једна садржи јавни, а друга тајни кључ, а затим и у датотеку која је везана за конкретну Интернет зону (енгл. *DNSSEC Zone File*) и која, између осталих података садржи и вредности овог пара кључева.

Након окончања поступка генерисања кључева може се реализовати дигитално потписивање Интернет зоне. Процес потписивања је, такође, потпуно аутоматизован и најчешће захтева унос имена домена и унос путање до датотека које садрже вредности кључева. Комплетна Интернет зона се потписује кључем за потписивање зоне, а DNSKEY запис са кључем за потписивање Интернет зоне и кључем за његово потписивање, након чега DNSKEY запис постаје јавни кључ те зоне. Овај поступак резултира креирањем нове датотеке која садржи податке о потписивању комплетне Интернет зоне и која је релевантна у поступку аутентификације. Како би овај систем задовољио безбедносне критеријуме потребно је развити систем за управљање криптографским кључевима који би издавао и повлачио кључеве у оптималним временским периодима.

Поступак замене кључева започиње генерисањем новог пара кључева чије вредности се додају у датотеку конкретне Интернет зоне, док се та зона поново потписује текућим, односно старим и још увек важећим кључевима. Овај поступак укључује креирање новог DNSKEY записа на основу новог пара кључева. Подаци о дигиталном потписивању Интернет зоне ће бити доступни свим DNS серверима. Обзиром да подаци којима располажу DNS сервери имају ограничен период важења, односно TTL (енгл. *Time To Live*), ти сервери ће се у предвиђеним временском периоду изменити податке у односу на нове вредности. DNS сервери покушавају да реализују процес аутентификације на основу свих доступних кључева, а успешна аутетификација је могућа обзиром на постојање старих, важећих кључева. Након истека периода важења, обзиром да су сви DNS сервери изменили податке, врши се потписивање Интернет зоне новим кључем. Након истека још једног TTL периода сви DNS сервери имају податак о новом дигиталном потпису Интернет зоне, након

чега је могуће повући стари кључ за потписивање те Интернет зоне.

Здравствени информациони систем, и ако би већим делом био реализован захваљујући инфраструктури Интернета, из безбедносних разлога треба да остане изолована целина. Обзиром на то, DNSSEC технологија може да се парцијално имплементира у овај информациони систем. Делимично решење може представљати безбедностно проширење које омогућава аутентификацију сервера и без креирања ланца поверења (енгл. *Chain of Trust*). Чињеница је да нису сви домен највишег нивоа дигитално потписани, па самим тим није могућа аутентификација њихових поддомена, односно није могуће формирање ланца поверења, али технологија парцијалног потписивања (енгл. DNSSEC *LookasideValidation*) омогућава потписивање једног дела сервера. По узору на то, могуће је направити систем за дигитално потписивање свих сервера у здравственом информационом систему, који би уместо да проверава дигиталне потписе свих домена проверавао само дигитални потпис конкретне DLV (енгл. *DNSSEC LookasideValidation*) зоне, односно доменске мреже здравственог информационог система.



Слика 8 Креирање ланца поверења у здравственом информационом систему

10. Виртуелне приватне мреже

Савремени здравствени информациони систем Републике Србије се мора простирати на територији читаве земље. Он треба да обухвата целу територију, укључујући и она подручја која данас немају ни техничке могућности за повезивање на Интернет. Ово је нарочито важно због тога што је у овим подручјима ниво квалитета здравствених услуга мањи у односу на ниво који би те области могле да имају када би постојала информациона и комуникациона повезаност са базама података, или са базама знања. Поред проблема који су у вези са техничком реализацијом такве компјутерске мреже, постоје проблеми који су у вези са заштитом података и безбедношћу комуникације. Све поменуте групе проблема је могуће решити употребом различитих технологија које су обједињене у технологији Виртуелних приватних мрежа, односно VPN (енгл. *Virtual Private Network*).

Технологија виртуелних приватних мрежа подразумева безбедно повезивање клијентских компјутера, односно других компјутерских мрежа које се налазе на удаљеним локацијама са матичном компјутерском мрежом, односно са конкретним клијентским компјутером. Ова технологија омогућава да се креира децентрализована компјутерска мрежа употребом јавне инфраструктуре Интернета, а да се при томе постигне тајност података и њихов интегритет. То се остварује тако што се сви мрежни уређаји, односно све групе мрежних уређаја, третирају као тачке између којих су реализовани безбедни комуникациони тунели, односно између којих се одвија шифрована комуникација. Повезивање тачака и шифровање података се може остварити на основу PPTP (енгл. *Point to Point Tunneling Protocol*) и L2TP (енгл. *Layer 2 Tunneling Protocol*) и на основу MPPE (енгл. *Microsoft Point-to-Point Encryption*) и IPSec (енгл. *IP Security Protocol*), односно на основу безбедносних функција које су имплементиране у ове системе.

10.1 Значај виртуелних приватних мрежа

Безбедност података здравственог информационог система је један од најзначајнијих критеријума по којима можемо сагледати степен остварења његове сврхе. Уколико постоји информациона и комуникациона повезаност свих корисника овог система, а не постоји могућност да се обезбеди тајност и интегритет података, можемо сматрати да тај информациони систем не остварује своју сврху. Здравствени подаци пацијената се морају чувати у складу препорукама здравствених организација и у складу са Законом о заштити података о личности Републике Србије. Због тога информациони систем мора бити реализован тако да је број могућих напада сведен на меру за коју се сматра да даје оптималан однос између трошкова заштите података и потребе за безбедношћу тог система. Напади могу бити разни, превара система за аутентификацију корисника, напади на тајност и интегритет података, преусмеравања пакета података, ускраћивање услуга информационог система, пасивно посматрање и прикупљање података и слично.

Виртуелне приватне мреже омогућавају висок ниво децентрализације информационог система уз исте безбедносне карактеристике, а без повећавања трошкова. Ова технологија представља решење које пружа безбедносне карактеристике сличне оним које пружају приватне комуникационе линије и ако подразумева употребу јавне Интернет инфраструктуре. Имплементација оваквих

мрежа може бити искључиво софтверска, или комбинована, укључујући наменске уређаје и специјализована софтверска решења. Без обзира на имплементацију виртуелних приватних мрежа, све врсте ових мрежа имају системе за адресирање клијената, или за адресирање компјутерских мрежа које су део ове мреже и системе за генерисање и дистрибуцију криптографских кључева.

10.2 Тунелска комуникација

Виртуелне приватне мреже за пренос података користе технологију тунелске комуникације, односно технологију преноса података у оквиру једне мреже која је изграђена на инфраструктури неке друге мреже, укључујући и протоколе на којима се заснива комуникација у тим мрежама. Тунелска комуникација подразумева размену података који су енкапсулирани у пакете који се размењују кроз тунеле којима се спајају комуникационе тачке. Тако енкапсулиране јединице података, односно пакети, могу бити у различитих формата у зависности од протокола на ком се заснива тунелска комуникација. Сваки пакет поред података има карактеристично заглавље. Пакети којима се шаљу подаци у тунелској комуникацији се разликују од уобичајених, између осталог, и по томе што садрже податке намењене усмеравању пакета чиме се постиже да пакети стижу на тачно дефинисано одредиште и тачно утврђеним путањама. Након доласка на одредиште, енкапсулирани подаци се распакују и прослеђују на циљано одредиште у приватној мрежи. Помоћу протокола за тунелску комуникацију, могуће енкапсулирати податке у пакете карактеристичне за тунелску комуникацију, на пример PPTP (енгл. *Point-to-Point Tunneling Protocol*) и проследити их путем јавне мреже некој приватној мрежи у којој се комуникација заснива на другом протоколу, на пример TCP/IP (енгл. *Transmission Control Protocol / Internet Protocol).*

Када је у питању тунелска комуникација која се заснива на PPTP, или L2TP, тунел је сесија успостављена између две тачке у комуникацији. Обе тачке учествују у успостављању тунела између њих и при томе се усаглашавају о вредностима адреса учесника у комуникацији, о вредностима кључева, односно алгоритама за шифровање, о вредности параметара којима се дефинише компресија и количина података и о вредности параметара на основу којих се гаси комуникациони канал након завршетка комуникације. Након успостављања тунела, клијент започиње комуникацију и обраћа се серверу који је задужен за тунелску комуникацију и од ког добија одговор на основу ког се пакети података шаљу до другог сервера, такође, задуженог за тунелску комуникацију, који их након пријема ослобађа од мета - података за тунелску комуникацију, па их са заглављем предвиђеним за протокол у приватној мрежи, прослеђује до циљаног мрежног уређаја, односно компјутера.

Тунелску комуникацију можемо окарактерисати као добровољну (енгл. *Voluntary Tunneling*), или као обавезну (енгл. *Compulsory Tunneling*) у зависности од начина на који се успоставља тунел и у зависности од карактеристика комуникације. Добровољна тунелска комуникација постоји у ситуацији када клијент може самостално иницирати креирање и конфигурисање комуникационог тунела на основу параметара које поседује. Оваква комуникација подразумева да је клијент крајња тачка у комуникацији и да поседује специјализовани софтвер за тунелску комуникацију као и вредности параметара на основ којих се дефинише комуникациони тунел. Овакав вид тунелске комуникације подразумева да се сервери укључују у комуникацију једино због усмеравања енкапсулираних пакета до

одредишта. Обавезна тунелска комуникација подразумева да је сервер крајња тачка у комуникацији и да је он тај који учествује у креирању тунела док је на клијенту да податке, који се шифрују на основу вредности параметара којим располаже сервер, достави серверу.

10.3 Point-to-point Tunneling Ptorotocol

PPTP (енгл. *Point-to-Point Tunneling Protocol*) се заснива на енкапсулирању PPP (енгл. *Point-to-Point Protocol*) фрејмова у IP пакете (енгл. *Internet Protocol Datagram*) који се транспортују путем јавних мрежа које се заснивају на Интернет протоколу. Овај протокол користи TCP конекцију (енгл. *Transmission Control Protocol Connection*) да би креирао, користио и угасио комуникациони тунел. Пакети намењени тунелској комуникацију су карактеристично енкапсулирани PPP фрејмови који су шифровани, на основу чега се обезбеђује тајност и интегритет података. Тунелска комуникација која се заснива на овом протоколу подразумева да тачке које учествују у комуникацију буду повезане на IP мрежу и да буду доступне пре успостављања тунела који ће их повезивати у тунелској комуникацији.

Спецификација PPTP – а не дефинише механизме за аутентификацију, или механизме за шифровање, али сваку имплементацију тунелске комуникације на основу овог протокола је могуће додатно проширити на основу других протокола који обезбеђују механизме за очување тајности и интегритета података. PPTP безбедност (енгл. *PPTP Security*) је безбедносна надоградња овог протокола којом се омогућава аутентификација, шифровање и филтрирање пакета. Пре успостављања тунела у VPN конекцији потребно је аутенификовати потенцијалне учеснике у комуникацији. Механизми аутентификације су имплементирани у бројне протоколе као што су: EAP (енгл. *Extensible Authentication Protocol*), затим CHAP (енгл. *Challenge Handshake Authentication Protocol*), PAP (енгл. *Password Authentication Protocol*) и други. Филтрирање пакета је могуће дефинисати аутоматски, или уз помоћ једноставних подешавања што употребу софтвера за тунелску комуникацију чини једноставнијом, а не утиче на смањење безбедности.

PPTP поседује мали избор механизама за шифровање. Механизам за шифровање, који је везан за овај протокол, се назива *Microsoft Point-to-Point Encryption* и он подржава искључиво шифровање везе (енгл. *Link Encryption*), односно шифровање порука између пријемног и предајног рутера, или сервера. Обзиром да је за безбедну комуникацију потребно аутентификовати клијенте, потребно је реализовати шифровану комуникацију између крајњих тачака у комуникацији, односно између крајњих тачака. Ово је могуће реализовати захваљујући безбедном Интернет протоколу, односно IPSec - у (енгл. *Internet Protocol Security*). IPSec омогућава шифровање са краја на крај (енгл. *End-to-End Encryption*) па је могуће остварити безбедну комуникацију између два краја. *Microsoft* оперативни системи поседују аутоматско подешавање VPN конекције. Предефинисана подешавања подразумевају PPTP и MPPE, а уколико није могуће креирати такву конекцију по аутоматизму се покушава са L2TP у комбинацији са IPSec шифровањем.

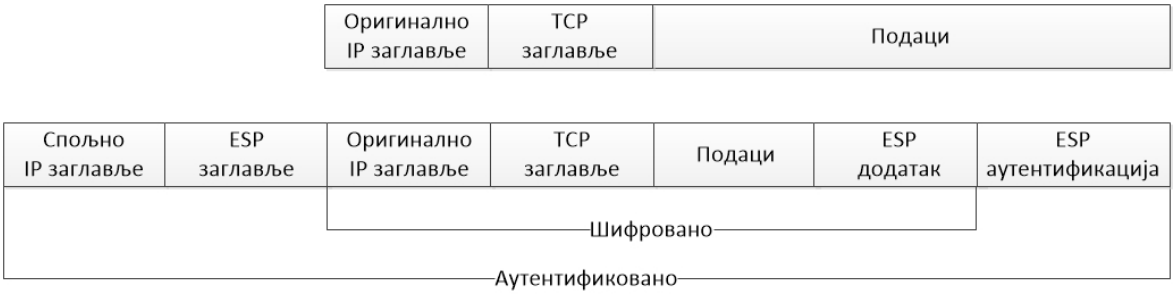
10.4 Layer 2 Tunneling Ptorotocol

L2TP је настао на иницијативу IETF – а (енгл. *Internet Engineering Task*) као тенденција да се два постојећа и некомпатибилна протокола за тунелску комуникацију обједине у један. Овај протокол је развио *Cisco Systems, Inc*. и у њему је објединио најбоље карактеристике PPTP – а и L2F – а (енгл. *Layer 2 Forwarding*) протокола. L2TP енкапслулира PPP фрејмове које касније, у зависности од протокола, енкапсулира у друге пакете. Захваљујући тој карактеристици, овај протокол је могуће искористити за креирање тунелске комуникације на неколико различитих протокола. Када је у питању мрежна инфраструктура изграђена на основи Интернет протокола, L2TP фрејмови су енкапсулирани у UDP (енгл. *User Datagram Protocol*) поруке. Енкапсулирани PPP фрејмови су и шифровани и компресовани, а шифровање се реализује енкапсулацијом у ESP (енгл. *Encapsulating Security Payload*) пакете.

Сигурни Интернет протокол, односно IPSec омогућава безбедну комуникацију на основу аутентификације порекла података, а затим и на основу шифровања, чим се постиже тајност и интегритет података. Овај протокол предвиђа и заштиту од дуплирања шифрованих пакета (енгл. *Anti Replay Protection*) на основу податка о броју пакета које обезбеђује пријемна страна. IPSec почиње комуникацију на основу међусобне аутентификације предајне и пријемне стране. Након тога се успоставља сесија између две стране у комуникацији тако што се размењују криптографски кључеви, односно криптографски алгоритми. Овај протокол поседује бројне функције и разне врсте различитих порука на основу чега се може реализовати безбедна тунелска комуникација.

IPSec се заснива на технологији која користи разне алгоритме и параметре, односно кључеве како би се послао низ аутентификованих и шифрованих пакете са предајне на пријемну страну. Сви пакети у тунелској комуникацији имају модификована заглавља у односу на стандардне IP пакете. Поред параметара који су карактеристични за IP заглавља, ови пакети имају и друге додатне параметре који се налазе између стандардног IP заглавља и података. Зависно од намене разликујемо две врсте пакета са две врсте карактеристичних заглавља: AH (енгл. *Authentication Headers*) и ESP (енгл. *Encapsulating Security Payloads*). AH обезбеђује интегритет података, аутентификацију IP пакета и заштиту од понављања пакета, док ESP обезбеђује тајност и интегритет података, аутентификацију IP пакета и заштиту од понављања пакета.

Слика 9 Authentication Header (AH)



Слика 10 Encapsulating Security Payload (ESP)

Тунелска комуникација са оваквом заштитом пакета може да се реализује тек након креирања тунела, односно, тек након усаглашавања пријемних и предајних страна о алгоритмима и параметрима потребним ESP операције. Креирање комуникационих тунела подразумева постојање система за аутентификацију и размену криптографских кључева која може бити различита у зависности од безбедносних карактеристика које треба да задовољи тај комуникациони канал. Зависно од тога може постојати мануелна размена кључева која је веома захтевна и скупа јер подразумева ручно пуњење криптографског системе криптографским кључевима, затим размена кључева путем Интернета посредством центра за дистрибуцију криптографских кључева, размена кључева на основу неког од система за управљање кључевима, или размена која је имплементирана у систем доменских имена која укључује аутентификацију и управљање криптографским кључевима размену кључева на основу функција имплементираних у IPSec.

Независно до технологије, процес креирања тунела започиње формирањем комуникационог пара слањем порука за аутентификацију учесника у комуникацији и за размену криптографски кључева између њих. Аутентификација се реализује захваљујући асиметричним алгоритмима и инфраструктури јавних кључева, односно на основу инфраструктуре приватних и јавних кључева уз посредовање сертификационих ауторитета. Процес размене кључева и других комуникационих параметара се може реализовати на основу RSA Diffie–Hellman методе (RSA-2048, RSA-3072, или RSA-4096), или криптографијом заснованом на елиптичним кривим Diffie–Hellman методе, ECC (енгл. *Elliptic curve cryptography*) (ECC-256k1, ECC-256r1, или ECC-521). Интегритет података се обезбеђује употребом криптографских функција за хеширање података: SHA-160, или SHA-256, а тајност шифровањем података уз помоћ симетричних алгоритама: AES-128 и AES-256.

10.5 Безбедносни Интернет протокол и систем доменских имена

Систем доменских имена који је данас у употреби располаже са ресурсима који се могу употребити у спрези са функцијама сигурног Интернет протокола са циљем да се направи хибридно решење које би обједињавало адресовање, аутентификацију и шифровање, односно решење које би се заснивало на наменски направљеним функцијама које би које би биле сличне функцијама које обједињава DNSEC (енгл. *Domain Name System Security Extensions*). DNS располаже записима који се могу употребити за чување јавних кључева како би могла да се реализује атуентификација клијената или сервера који учествују у комуникацији. Приступање жељеном ресурсу на Интернету се може реализовати адекватним адресирањем на основу имена домена, или експлицитним навођењем IP адресе, међутим, то не

гарантује аутентичност тих ресурса. Такође, уколико је потврђена аутентичност мрежних ресурса, то не гарантује да ће комуникација бити заштићена јер ће и даље постојати могућност да се пресретне комуникација и злоупотреби поверење.

Аутентификација учесника у комуникацији се може реализовати на основу јавних кључева након чега је могуће креирати комуникациони тунел, а један од система који ово омогућава користи запис под називом IPSECKEY за складиштење потребних информација. Овај запис, између осталих података, чува вредности јавних кључева који су у вези са називима домена у сигурној комуникацији која се заснива на IPSec протоколу. Зависно од врсте комуникационог тунела, то могу бити јавни кључеви клијената, сервера, компјутерских мрежа, или апликација. Поред вредности јавних кључева, овај запис служи за складиштење осталих информација на основу којих се реализује шифровање и дешифровање података.

Уобичајено је да безбедносни мрежни пролаз (енгл. *Gateway*) остварује приступ одређеној тачки само на основу IP адресе и да поред тог податка не располаже са другим подацима за адресирање. Због тога, повезивање ресурса на основу IPSECKEY записа захтева употребу обрнутог мапирања, односно *.arpa* (енгл. *Addressand Routing Parameter Area*) домена (конкретно *in-addr.arpa* за IPv4 и *ip6.arpa* за IPv6) и сервиса за обрнуто мапирање које нуде апликације развијене над њима. Претраживање се врши на начин карактеристичан за обрнуто мапирање и PTR записе, односно на записе који садрже канонска имена Интернет ресурса. Аутентификацију ресурса на основу IPSECKEY записа треба реализовати на основу DNSEC функција. Уколико се појави више IPSECKEY записа са истим именом, то указује на постојање дуплирања података о мрежним пролазима, што покреће процес повлачења кључева.

Прва вредност коју садржи IPSECKEY запис се назива предност (енгл. *Precedence*) служи да се одреди редослед, односно приоритет по ком ће мрежни пролаз преузимати IPSECKEY записе. Ова вредност је нумеричка и за њу је резервисан простор од осам бита. Записи са мањом вредношћу имају већи приоритет. Затим следи вредност типа мрежног пролаза (енгл. *Gateway Type*) која указује на формат података које је потребно привремено сачувати у меморији резервисаној за тај мрежни пролаз, односно вредност IP адресе, или вредност домена. Тип алгоритма (енгл. *Algorithm Type*) представља идентификатор алгоритма јавног кључа и формат јавног кључа који је у складу са тим, односно да ли је кључ DSA, или RSA формата. Мрежни пролаз (енгл. *Gateway*) је поље које садржи адресу чворишта, односно мрежног пролаза посредством ког се остварује комуникација између крајњих тачака. Поље које је резервисано за вредност јавног кључа је у складу са постојећим форматима јавних кључева са том разликом што су алгоритми IPSECKEY другачији од алгоритама који се користе у DNSSEC – у.

11. Управљање криптографским кључевима

Са становишта безбедности здравственог информационог система постоји оправдана потреба за имплементацијом наменског криптографског решења која ће бити у потпуности ново, или које ће се развијати на постојећим основама неких претходних решења. Обзиром да се безбедност електронских комуникација своди на комплексност криптографских кључева, поред алгоритама за шифровање, постоји потреба за системом који ће омогућити квалитетно и безбедно управљање криптографским кључевима. Управљање криптографским кључевима представља један од најделикатнијих задатака у реализацији криптографских система. Иако постоје бројни алгоритми за генерисање кључева и за њихову размену, очување њихове тајности није лак задатак. Приликом напада, највећа је вероватноћа да ће криптоаналитичар напасти систем за управљање кључевима, па је због тога највећа пажња усмерена на његово обезбеђивање.

Управљање криптографским кључевима подразумева њихово генерисање, дистрибуцију и чување. Очување тајности кључева је од пресудног значаја за смисао постојања једног криптографског система јер у супротном, нападач који дође у посед криптографских кључева, може дешифровати поруке које су шифроване тим кључевима. Опет, учесници у комуникацији морају бити у могућности да генеришу кључеве и да их несметано користе, па уколико дође до компромитовања кључева, они морају бити повучени што ствара потребу за генерисањем нових кључева. Без обзира на комплексност криптографског система, његова употреба у здравственом информационом систему треба да буде једноставна, односно аутоматска, а све криптографске функционалности аутоматизоване тако да његови корисници немају потребе да утичу на функционисање криптографског система. Такође, корисници информационог система не би требали да примете кашњења до којих ће неминовно доћи услед повећавања комплексности комуникације и услед повећавања количине података.

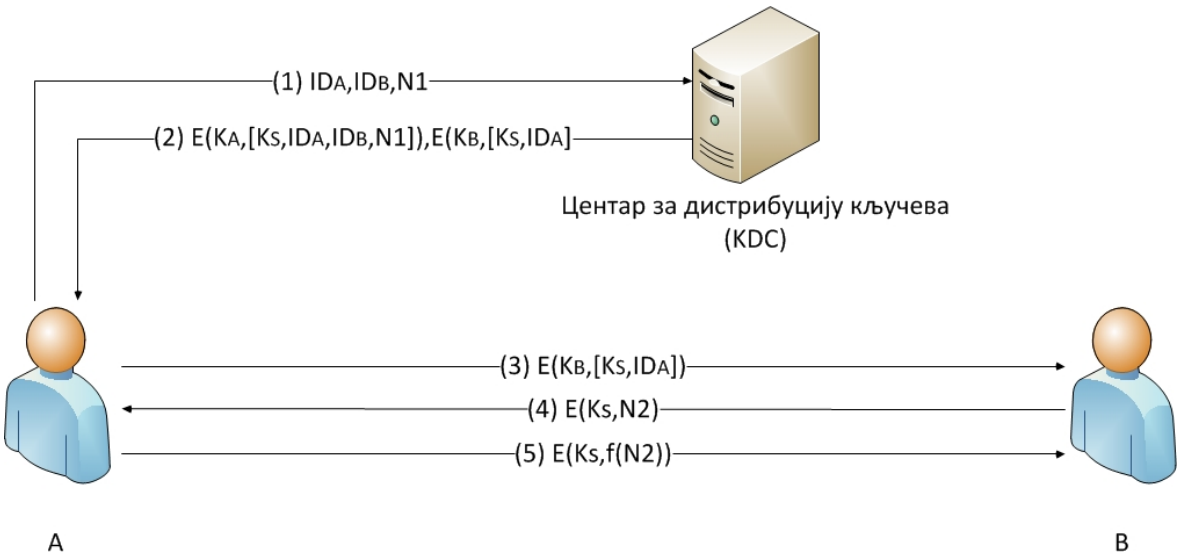
Криптографски кључеви се користе у ограниченом временском периоду чиме се умањује могућност успешне криптоанализе. Криптографски кључеви се употребљавају приликом шифровања порука, а нападачи су у могућности да прикупљају шифроване податке који су неопходни за криптоанализу. Време валидности кључева се процењује у односу на време потребно за дешифровање текста, па дужина и комплексност кључева утиче на тај период. Препоручене минималне дужине криптографских кључева који су данас у употреби су од 256 бита за привремене кључеве који се користе неколико дана па до 4096 бита за кључеве који се користе у дужем временском периоду. Дужина кључа такође утиче на перформансе криптографског система па се она бира у зависности од жељеног нивоа безбедности и у зависности од избора криптографских алгоритама и криптографских техника. Препоручене дужине за RSA алгоритам су од 2048 бита до 4096 бита у зависности од планираног периода валидности.

11.1 Управљање кључевима у симетричној криптографији

Симетрична криптографија подразумева да све стране у комуникацији деле исте кључеве и да користе исте алгоритме у процесима шифровања и дешифровања. Симетрични криптографски системи се одликују високом ефикасношћу јер је потребно релативно мало ресурса за успешну реализацију шифроване комуникације.

Међутим, уколико би се у здравствени информациони систем имплементирао овакав криптографски систем, управљање кључевима би представљало потенцијални проблем. Реализација ефикасног система за управљање кључевима не би била једноставна обзиром да су кључеви у симетричној криптографији мање комплексни од оних намењених асиметричној криптографији, а рад криптографског система са становишта запослених који би користили здравствени информациони систем треба да буде аутоматизован, односно не треба да укључује њих у процесе размене, или уноса криптографских кључева. Поред тога, управљање криптографским кључевима не би представљало велики проблем уколико би број учесника у комуникацији био мали, али када су у питању велики информациони системи као што је здравствени информациони систем, оно би било сувише компликовано и неефикасно.

Један од начина за реализацију управљања кључевима у симетричним криптографским системима јесте увођење дистрибутивног центра за кључеве, KDC (енгл. *Key Distribution Center*). Овакав систем подразумева да сваки учесник у комуникацији дели тајни кључ са дистрибутивним центром и уколико учесници желе да успоставе комуникацију, она се реализује посредно путем дистрибутивног центра.



Слика 11 Управљање кључевима посредством центра за дистрибуцију кључева

Страна која иницира комуникацију, страна A, генерише иницијални идентификатор сесије N1 и шаље га заједно са својим идентификатором ID_A и идентификатором стране B, ID_B, и све то шифрује кључем K_A, који деле страна A и центар за дистрибуцију кључева KDC. KDC генерише одговор који садржи једнократни кључ K_S, ID_A, ID_B, N1 што шифрује кључем K_A и податке које ће страна A проследити страни B који се састоје од кључа K_S, и идентификатора ID_A који су шифровани кључем K_S. Након овога, и страна A и страна B поседују кључ за ту сесију K_S, а страна B зна да је страна A иницирала комуникацију. Страна B одговара идентификатором N2 шифрованим сесијским кључем K_S и чека одговор од стране A, односно поруку f(N2) шифровану сесијским кључем K_S што представља доказ да страна B комуницира са страном A.

11.2 Управљање кључевима у асиметричној криптографији

Асиметрични криптографски системи пружају бројне могућности које комуникацију чине једноставнијом са становишта учесника у њој. Кључеви за шифровање порука се креирају динамички са сваку сесију и након ње се уништавају. Такав приступ, првенствено, решава недостатке дељења криптографских кључева јер, за разлику од симетричне криптографије, свака страна креира по два кључа: један тајни који чува и други јавни који размењује са другим странама у комуникацији. Такав систем омогућава свим странама висок степен независности у остваривању и реализацији шифроване комуникације. Такође, асиметрични криптографски системи захтевају мање криптографских кључева у односу на симетричне. На пример, информациони систем са асиметричним криптографским системом са 100.000 корисника би требао да располаже са 200.000 кључева, за разлику од симетричног криптографског система где би било потребно око 5 милијарди кључева.

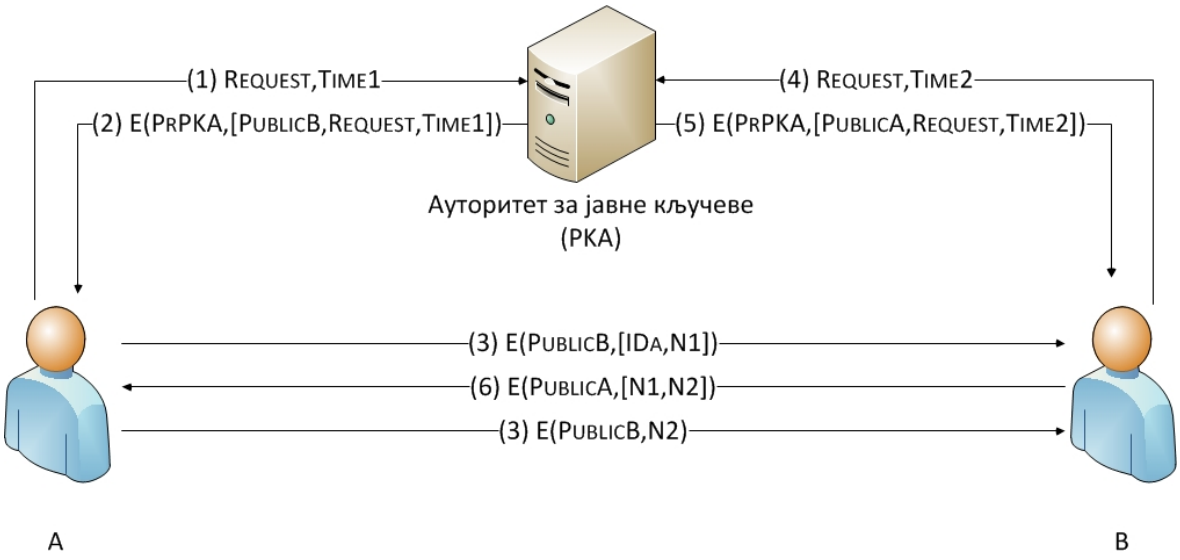
Асиметрични алгоритми су веома комплексни и користе дугачке кључеве приликом шифровања и дешифровања због чега су доста спорији у односу на симетричне алгоритме. Операције са великим бројевима захтевају много времена и много компјутерских ресурса па ови алгоритми нису погодни за рад са великим количинама изворних података, већ за рад са кратким порукама, криптографским кључевима, кодовима и слично. Кључеви се могу дистрибуирати јавним објављивањем, излагањем у јавном директоријуму, посредством ауторитета за јавне кључеве, PKA (енгл. *Public Key Authority*) и на основу дигиталних сертификата.

Комуникација у којој учесници јавно објављују криптографске кључеве се реализује тако што сваки учесник шаље јавни кључ учеснику са којим намерава да комуницира. Међутим, овакав начин размене кључева омогућава да се било који учесник у комуникацији представи као неко други и да наведе друге учеснике у комуникацији да поверују у то, односно овакав систем не предвиђа повезаност јавног кључа и идентитета његовог власника.

Већи степен сигурности се постиже објављивањем кључева путем јавног директоријума, првенствено због тога што је одржавање оваквог директоријума у надлежности ентитета у кога сви учесници у комуникацији имају поверења, а и због тога што се поред кључа у овом директоријуму чувају и подаци о власницима тих кључева. Приступ овом директоријуму је могуће остварити, или непосредно, односно лично, или путем Интернета, а учесници су у могућности да након идентификације, или аутентификације, мењају своје кључеве уколико сматрају да су компромитовани, или уколико сматрају да је истекао период важења кључа. Овај начин је безбеднији од јавног објављивања, али ту постоји ризик од компромитовања свих кључева уколико дође до откривања приватног кључа ентитета који одржава овај директоријум, или уколико дође до преузимања контроле над директоријумом и кривотворења јавних кључева учесника у комуникацији.

Управљање јавним кључевима посредством ауторитета за јавне кључеве, PKA (енгл. *Public Key Authority*) пружа виши ниво безбедности у односу на објављивање кључева у јавном директоријуму јер овакав систем подразумева да ауторитет за јавне кључеве дигитално потписује јавне кључеве свих учесника у комуникацији на основу приватног кључа којим само он располаже. Сви учесници у комуникацији

морају познавати јавни кључ директоријума и на основу тога могу добити јавне кључеве свих осталих учесника у комуникацији. Захтев за неким јавним кључем се може упутити директоријуму у сваком тренутку.

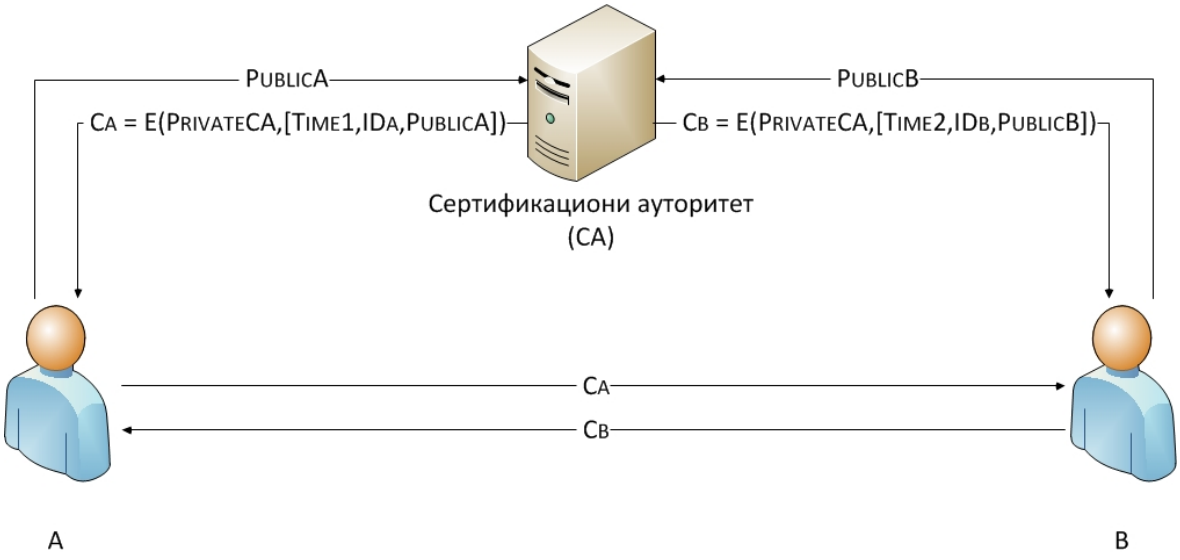


Слика 12 Управљање кључевима посредством ауторитета за јавне кључеве

Размена кључева између два учесника се реализује у седам корака:

1. Страна А шаље поруку ауторитету за јавне кључеве која садржи временску ознаку TIME1 и захтев за јавним кључем стране B.
2. Ауторитет за јавне кључеве шаље јавни кључ стране B и оригинални захтев стране A, а одговор шифрује својим приватним кључем PRPKA.
3. Страна А шаље поруку страни B и шифрује је јавним кључем стране PUBLICB, а у поруци се налази податак о идентитету учесника A, IDA и једнократни идентификатор за ту сесију N1 који је генерисала страна A и који је само њој познат.
4. Након пријема те поруке, страна B шаље поруку ауторитету за јавне кључеве која садржи временску ознаку TIME2 и захтев за јавним кључем стране A.
5. Ауторитет за јавне кључеве одговара шаљући јавни кључ стране A, PUBLICA и оригинални захтев стране B шифроване својим приватним кључем.
6. Након пријема те поруке, страна B шаље поруку која се састоји од једнократних идентификатора N1 и N2 који су шифровани употребом јавног кључа стране A. Једнократни идентификатор N2 је генерисала страна B и он је само њој познат.
7. Страна А из добијене поруке издваја једнократни идентификатор N2 одговара шаљући тај идентификатор шифрован јавним кључем стране B, PUBLICB, након чега су обе стране уверене у то да је заснована шифрована комуникација између страна чију аутентичност гарантује ауторитет за јавне кључеве.

Управљање јавним кључевима на основу дигиталних сертификата захтева мање ресурса у односу на управљање посредством ауторитета за јавне кључеве обзиром да стране у комуникацији, након додељивања дигиталних сертификата од стране сертификационог ауторитета, могу самостално размењивати властите јавне кључеве без приступа ауторитету за јавне кључеве у тренутку када желе да започну комуникацију. Дигитални сертификати садрже личне податке о власнику сертификата и бројне техничке податке. Најважније својство дигиталног сертификата је то што он повезује идентитет власника и његов јавни кључ. Целокупни садржај сертификата се дигитално потписује од стране сертификационог ауторитета што омогућава да свакој заинтересованој страни да провери идентитет власника сертификата уколико познаје јавни кључ сертификационог ауторитета.



Слика 13 Размена дигиталних сертификата

Управљање јавним кључевима на основу дигиталних сертификата омогућава свакој страни да на основу дигиталних сертификата осталих страна виде њихове јавне кључеве и неке од њихових личних података, такође, увек се могу уверити у веродостојност сертификата јер се сертификациони ауторитет у комуникацији појављује као страна од поверења и једино он може да издаје и да повлачи сертификате што се доказује тако што је дигиталне сертификате могуће дешифровати само јавним кључем сертификационог ауториета. Издавање дигиталних сертификата се најчешће реализује личним контактом уз давање на увид личних докумената а често и додатне документације уколико је подносилац захтева правно лице. Након тога је власник дигиталног сертификата у могућности да започне шифровану комуникацију када то њему одговара и то на следећи начин:

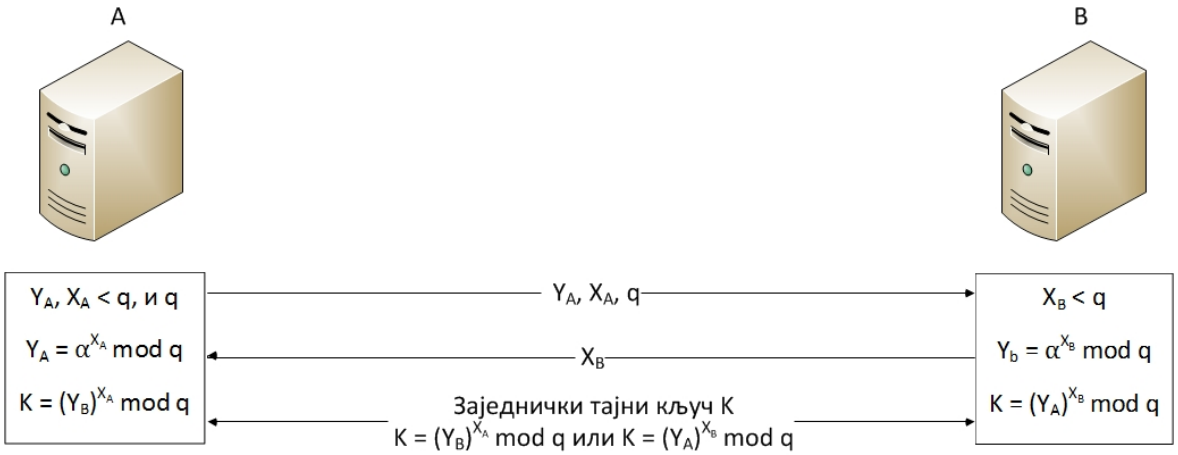
1. Страна А шаље свој јавни кључ и захтев за креирањем дигиталног сертификата.
2. Сертификациони ауторитет са страну А креира дигитални сертификат CA који садржи временску одредницу TIME1, идентификацију стране А, IDA и њен јавни кључ PUBLICA које шифрује својим приватним кључем PRIVATECA.
3. Након тога, страна А је у могућности да проследи свој дигитални сертификат који је јединствено идентификује а за шта гарантује сертификацони ауторитет.

4. Такође и страна B, којој је исто тако креиран дигитални сертификат, је у могућности да се представи сопственим дигиталним сертфикатом након чега је могуће да започну шифровану комуникацију.

11.3 Протоколи за дистрибуцију криптографских кључева

11.3.1 Diffie – Hellman протокол

Творци асиметричне криптографије *Whitefield Diffie* и *Martin Hellman* су 1976. године представили своју идеју која је поставила стандарде и постала основ за даљи развој криптографије са приватним (тајним) и јавним кључевима. D-H метода је у времену након тога искоришћена у великом броју комерцијалних криптографских решења. Тајни и јавни кључ повезују математичке функције које омогућавају израчунавање у једном смеру, односно омогућавају израчунавање јавног кључа на основу тајног, док је израчунавање тајног кључа на основу јавног немогуће, односно немогуће у разумном времену. D-H метод за размену криптографских кључева омогућава странама које нису раније биле у контакту да остваре тајну комуникацију преко незаштићених комуникационих линија на основу заједничког тајног кључа који генеришу помоћу D-H алгоритма.



Слика 14 Diffie – Hellman протокол

D-H алгоритам за размену кључева је веома комплексан и захтеван када су у питању компјутерски ресурси па се као такав не може користити за размену порука између страна у комуникацији, али се успешно користи за успостављање заједничког тајног кључа. Вредност заједничког тајног кључа се добија степеновањем природног броја производом два велика проста броја по модулу простог броја, а зависи од података о јавном и тајном кључу које имају или одређују стране у комуникацији, док се сигурност ослања на тежину израчунавања дискретних логаритама, односно на комплексност проналажење дискретног логаритма по модулу простог броја који је одређен приликом успостављања кључа. Приликом успостављања јавног кључа уз помоћ овог алгоритма користе се две познате вредности: прост број q и природни број који је примитивни корен простог броја q.

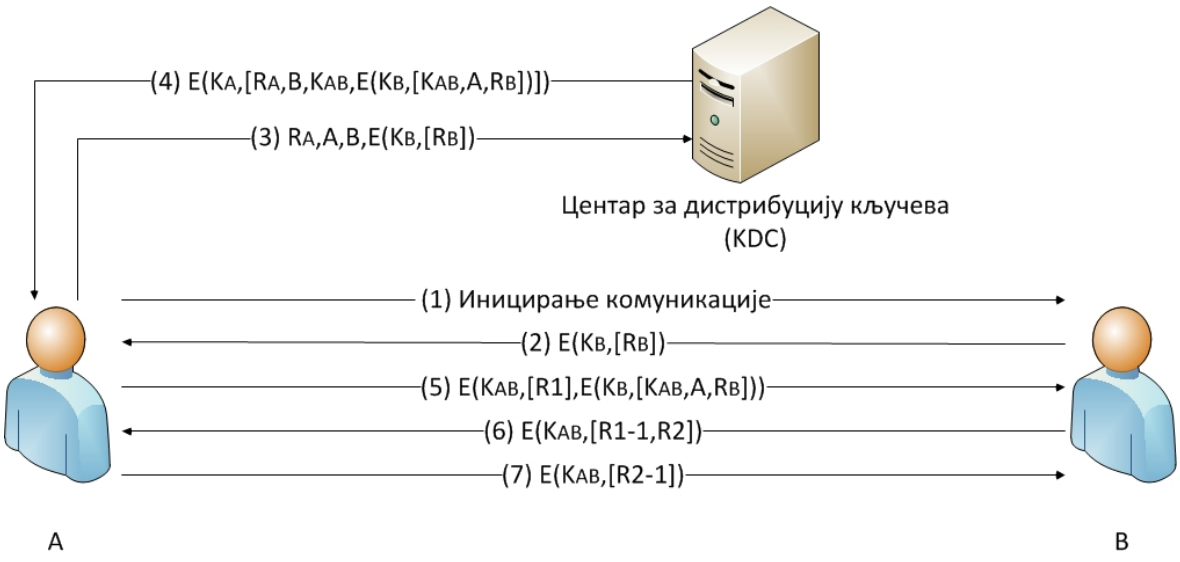
D-H поступак успостављања дељеног тајног кључа:

1. Страна А псеудо случајном методом бира бројеве q и $X_A < q$ и израчунава $Y_A = \alpha^{X_A} \bmod q$, након чега добијене вредности шаље страни В.
2. Након пријема поруке, страна В бира псеудо случајан број $X_B < q$ и израчунава $Y_B = \alpha^{X_B} \bmod q$.
3. Обе стране у комуникацији задржавају вредност X као приватну (тајну) а вредност Y представљају као јавну другој страни у комуникацији.
4. Страна А израчунава кључ К, $K = (Y_B)^{X_A} \bmod q$.
5. Страна В израчунава кључ К, $K = (Y_A)^{X_B} \bmod q$.
6. Обе стране у комуникацији познају заједнички тајни кључ К.

D-H метод не подразумева постојање система за аутентификацију, или за идентификацију страна у комуникацији тако да постоји могућност напада и злоупотребе услед лажног представљања, односно постоји могућност реализовања MiM (енгл. *Man in the Middle*) напада. Са друге стране, ако је заједнички тајни кључ успешно успостављен веома је тешко извршити криптоанализу и доћи до отвореног текста. Уколико вредности X_A и X_B остану тајне, потенцијални нападач има на располагању вредности α, q,Y_A и Y_B и могућност да користи дискретне логаритме како би пронашао вредност кључа. Ако жели да израчуна вредност X_B потенцијални нападач треба да израчуна вредност дискретног логаритма $X_B = \log \alpha,q\ (Y_B)$, а затим да добијену вредност искористи за израчунавање вредности кључа К попут стране В, $K = (Y_A)^{X_B} \bmod q$. Релативно лако се могу наћи експоненти по модулу простог броја, али је веома тешко наћи вредности дискретних логаритама, нарочито када су у питању велики прости бројеви где то постаје практично немогуће.

11.3.2 Needham – Schroeder протокол

Needham – Schroeder протокол омогућава безбедну размену кључева путем јавне компјутерске мреже, односно путем Интернета. Постоје две верзије N-S протокола. Први је заснован на инфраструктури јавних кључева и подразумева међусобну аутентификацију између страна у комуникацији, али је у пракси доказано да није довољно безбедан. Други протокол је базиран на симетричним криптографским алгоритмима и омогућава успостављање сесијског кључа између две стране у комуникацији путем Интернета како би се реализовала шифрована комуникација. Овај протокол је представљао основу за реализацију Керберос протокола, на основу које су настали многи други протоколи. Процес размене криптографских кључева на основу N-S протокола се реализује кроз седам корака у чему учествује центар за дистрибуцију кључева.



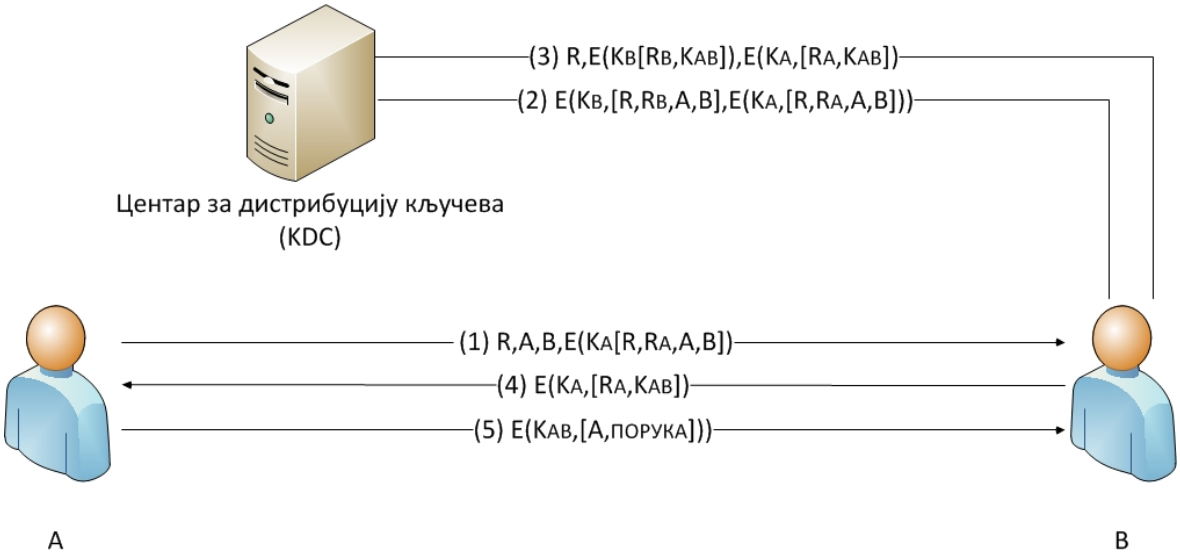
Слика 15 Needham – Schroeder протокол

Needham – Schroeder протокол:

1. Страна А започиње комуникацију шаљући страни В своју идентификацију.
2. Страна В на основу свог тајног кључа KB шифрује претходно генерисани псеудо случајни број RB који шаље страни А као би га она касније проследила центру за дистрибуцију кључева чиме се доказује да ће стране А и В учествовати у комуникацији.
3. Страна А шаље центру за дистрибуцију кључева поруку која садржи псеудо случајни број RA, идентификацију стране А, идентификацију стране В, и број RB шифрован кључем KB који прослеђује у истом облику у ком га је добила од стране В.
4. Центар за дистрибуцију кључева враћа страни А поруку која садржи број RA, идентификацију стране В, кључ сесије KAB и шифровани тикет који је намењен страни В. Овај тикет је шифрован тајним кључем стране В и садржи кључ сесије KAB, идентификатор стране А и псеудо случајни број који је генерисала страна В, RB.
5. Страна А прослеђује страни В добијени тикет и нови псеудо случајни број R1 који шифрује заједничким кључем за ту сесију KAB како би верификовала страну В.
6. Страна В одговара слањем броја R1 – 1 и новог псеудо случајног броја R2 који су шифровани заједничким кључем за ту сесију KAB. Уколико је страна А у могућности да дешифрује поруку употребом заједничког кључа и добије очекивани број R1 – 1 то значи да је страна В верификована као учесник у комуникацији који је био у могућности да применом тајног кључа KB дође до вредности заједничког кључа KAB.
7. Последњи корак верификује страну А тако што она шаље поруку која садржи број R2 – 1 који је шифрован на основу заједничког кључа KAB.

11.3.3 Otway – Rees протокол

На основу *Otway – Rees* протокола могуће је реализовати безбедну тунелску комуникацију између два компјутера или две компјутерске мреже на основу успостављања заједничког дељеног кључа на инфраструктури Интернета, а уз помоћ центра за дистрибуцију кључева. Примарна сврха овог протокола је повезивање и аутентификација ентитета у компјутерским мрежама, успостављање заједничког сесијског кључа и реализација шифроване комуникације између њих. Данас постоје бројне модификације O-R протокола и могућност успешне превенције бројних напада, од спречавања прислушкивања, преко онемогућавања злонамерног понављања података или злонамерног одлагања слања података, па до детектовања модификације података. Овај протокол, такође, у процес размене кључева укључује центар за дистрибуцију кључева.



Слика 16 Otway – Rees протокол

Otway – Rees протокол:

1. Страна A шаље поруку страни B која садржи псеудо случајни број R, идентификацију страна A и B и шифровани тикет намењен центру за дистрибуцију кључева који садржи број RA, копију броја R и идентификације страна A и B.
2. На основу добијених података, страна B генерише тикет намењен центру за дистрибуцију кључева који чине број RB, број R, идентификације страна A и B који шифрује на основу кључа KB који заједно са тикетом који је генерисала страна A шаље центру за дистрибуцију кључева. На основу ове поруке, KDC доказује идентитет, односно аутентификује стране A и B.
3. KDC генерише поруку која садржи два шифрована тикета који се састоје од заједничког случајног броја R, по два генерисана броја која потврђују идентитет, односно аутентичност страна у комуникацији RA и RB, затим њихове идентификационе ознаке A и B и заједнички дељени кључ за ту сесију KAB.
4. Страна B прослеђује тикет страни A који јој је намењио KDC.

5. Након тога су обе стране у могућности да размењују поруке које ће шифровати и дешифровати на основу заједничког дељеног кључа K_{AB}.

11.4 Управљање криптографским кључевима у здравственом информационом систему

Проблематика управљања криптографским кључевима у здравственом информационом систему је специфична због величине тог система и због великог броја различитих улога које могу имати његови корисници. Сигурно је да постоји потреба да се неким деловима овог система криптографски кључеви уносе ручно, али већи део система као приоритет има једноставност употребе па је у тим случајевима неопходно направити компромис којим ће се смањити безбедност на рачун поједностављења употребе тако што ће се аутоматизовати одређен број активности и функција. Симетрично шифровање комуникације је најбоље реализовати на основу симетричних кључева које би дистрибуирао центар за дистрибуцију, а обзиром на величину овог информационог система то би требало реализовати тако што би се у њега имплементирало више таквих центара између којих би постојала хијерархија у зависности од нивоа безбедности и у зависности од логичких целина за које су одређени.

Обзиром на број и врсту различитих корисничких улога у здравственом информационом систему и обзиром на чињеницу да би због доступности и функционалности овај систем требао бити реализован на инфраструктури Интернета, највећи део управљања криптографским кључевима би се ослањао на асиметричну криптографију и инфраструктуру јавних кључева. То би подразумевало укључивање дистрибутивних центара који би корисницима додељивали криптографске кључеве на основу дигиталних сертификата. Тиме би се омогућила заштићена комуникација између страна у комуникацију уз аутентификацију и идентификацију. Како је пракса доказала, овако се постижу оптималне перформансе јер се користе комплекснији алгоритми за успостављање заједничких дељених кључева и мање комплексни алгоритми којима се шифрује комуникација.

Време трајања кључева треба да буде јасно дефинисано у зависности од нивоа тајности и начина на који се кључ користи, односно од алгоритама који га употребљавају у процесу шифровања. Редовном заменом кључева се смањује могућност злоупотребе јер се смањењем времена употребе криптографског кључа смањује могућност успешности напада на криптографски систем. Криптографски систем који би за сваку трансакцију користио другачији криптографски кључ би у том смислу био безбеднији од оних који успостављају нови криптографски кључ за сваку нову сесију, али је управљање кључевима у таквим системима је сувише сложено што би негативно утицало на комуникационе перформансе нарочито када су у питању комплексни криптографски кључеви карактеристични за инфраструктуру јавних кључева.

Криптографски систем у здравственом информационом систему треба да поседује механизме за повлачење кључева за које се сматра да нису валидни, или за које се претпоставља да су компромитовани. Обзиром на то да би управљање кључевима требало да се реализује посредством центара за дистрибуцију њихова провера би била централизована и самим тим једноставна за реализацију. Време важења криптографских кључева би било дефинисано на основу дигиталних

сертификата, док би за остале криптографске кључеве време било одређено у зависности од њихове врсте и намене.

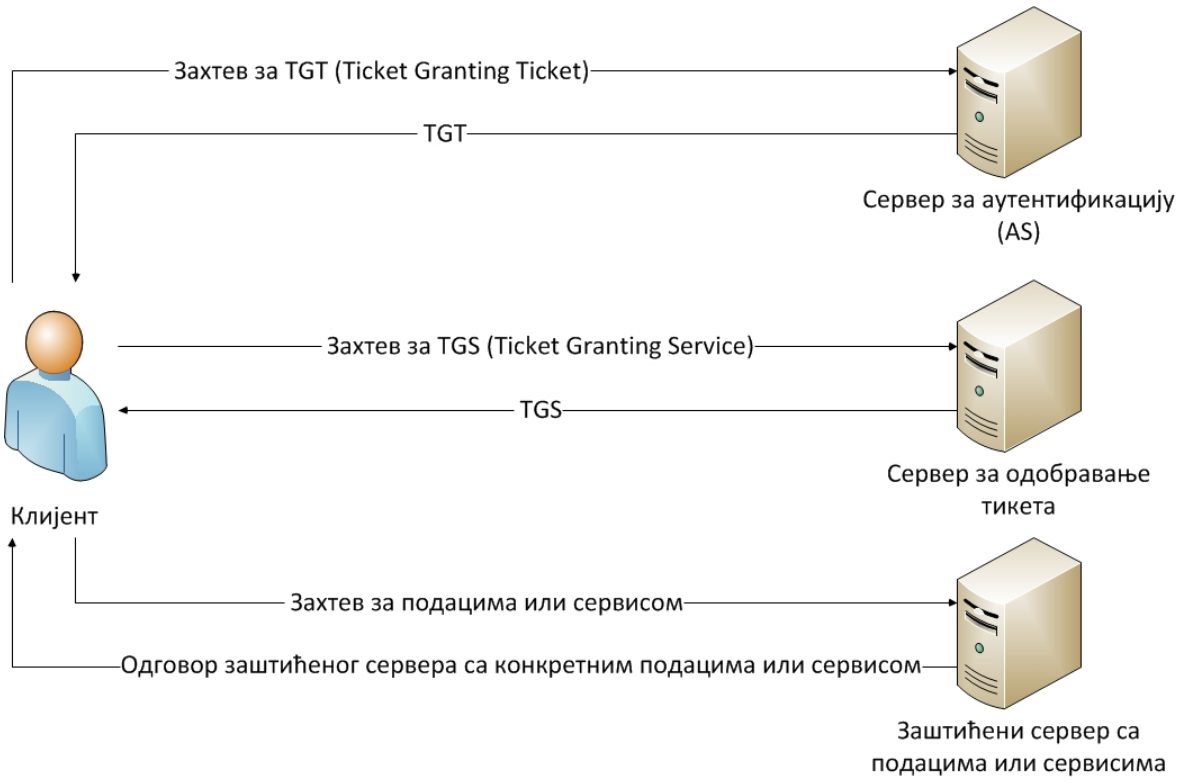
11.5 Керберос протокол

Керберос је протокол намењен аутентификацији у клијент – сервер компјутерским мрежама. Створен је од стране инжењера MIT – а (енгл. *Massachusetts Institute of Technology*) који су имали намеру да реше безбедносне проблеме сопствене компјутерске мреже. Овај протокол се ослања на криптографски систем који омогућава клијентима да се акредитују пред серверима за аутентификацију на основу чега су касније у могућности да се идентификују у комуникацији. Овај протокол, поред функција за атутентификацију обезбеђује и друге функције на основу којих је могуће реализовати тајну комуникацију између различитих страна чиме обезбеђује тајност порука и интегритет података. Основна верзија овог протокола, коју обезбеђује MIT, је бесплатна и доступна свима који коју имају намеру да је користе у складу са правима и обавезама које прописују њени власници. Поред тога, овај протокол је имплементиран у бројна друга криптографска решења где је индиректно доступан као интегрални део тих решења.

11.5.1 Аутентификација на основу Керберос протокола

Керберос протокол је пројектован тако да одговори захтевима карактеристичним за компјутерске мреже средњих величина па као такав има бројне предности када су у питању потребе здравственог информационог система у односу на друга решења. Аутентификација се реализује у неколико корака између клијента и сервера где сервер акредитује корисника при чему не тражи додатне податке од осталих тачака у комуникацији, односно од домен контролера. Провера клијента подразумева проверу сервера, односно аутентификација је узајамна. Такође, овај протокол поседује своје функције за дигитално потписивање домена што омогућава креирање ланца поверења између сервера који се налазе у истој зони и домена који су повезани преко те зоне поверења. Поред тога, овај протокол је заснован на стандардима које прописује IETF (енгл. *Internet Engineering Task Force*) што омогућава његову имплементацију у бројне различите криптографске системе.

Специфичност Керберост протокола су функције које креирају наменске пакете података познате под називом тикети (енгл. *tickets*) помоћу којих се, у облику шифрата, размењују криптографски подаци. Ови тикети представљају потврду аутентичности која обезбеђује успостављање комуникације са одговарајућим сервером. Криптографски систем који се заснива на Керберос протоколу, поред постојања клијената који иницирају комуникацију и сервера који реализује сервисе које захтевају клијенти, подразумева постојање сервера за аутентификацију и сервера за додељивање тикета, као имплементацију центра за дистрибуцију кључева. Приликом шифровања тикета, или прокука, старије верзије Керберос протокола користе DES алгоритам, док новије 3DES и AES. Пета верзија овог протокола користи искључиво AES алгоритам.



Слика 17 Керберос протокол – сервери

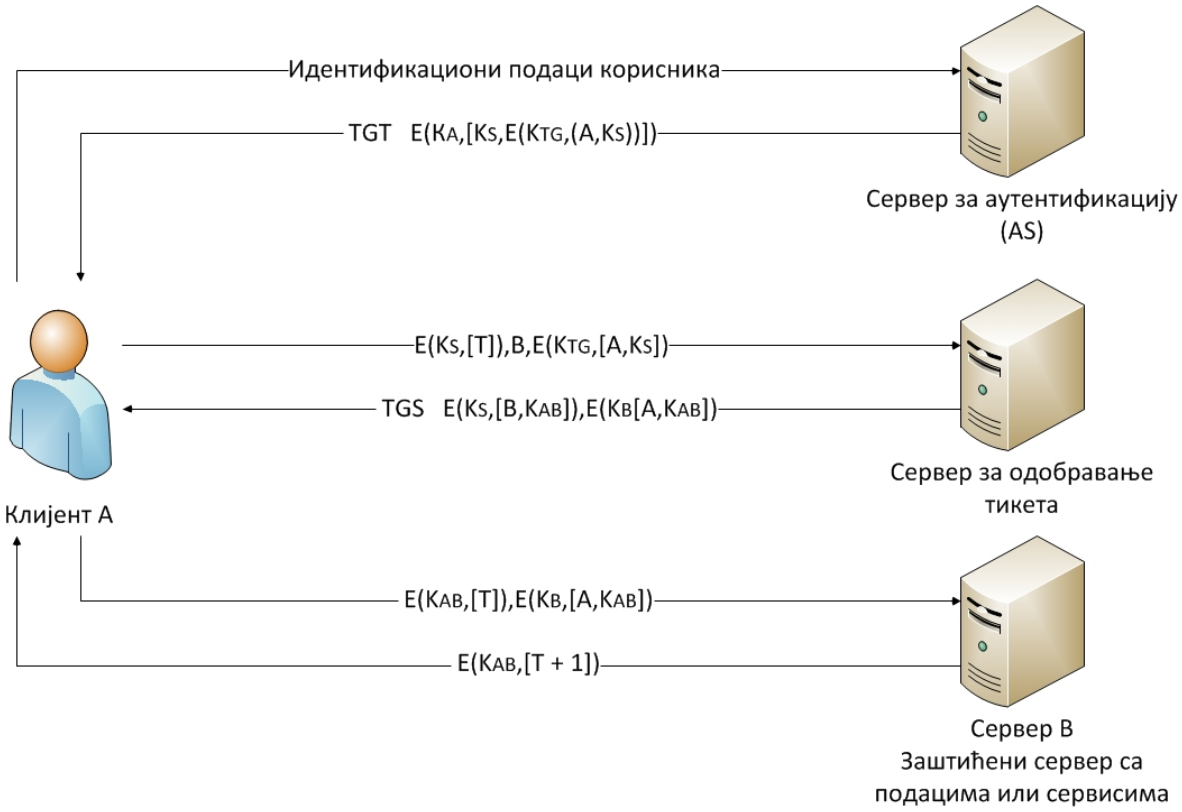
Основно окружење криптографског система који се реализује на Керберос протоколу подразумева укључивање три ентитета: први је сервер за аутентификацију (енгл. *Authentication server*), затим сервер за издавање тикета где је доступан сервис за издавање тикета (енгл. *Ticket Granting Service*) и сервер на коме се чувају подаци, или на ком се реализују клијентски сервиси. Сервер за аутентификацију у овом протоколу има улогу центра за дистрибуцију кључева и сваки субјекат који се појављује у комуникацији мора бити регистрован на том серверу, односно овај сервер мора поседовати рекорд о сваком субјекту који ће између осталог садржати и дугорочни кључ за тај субјект. Након што сервер за атутентификацију добије клијентски захтев, он проверава акредитиве након чега издаје TGT (енгл. *Ticket Granting Ticket*) на основу ког ће се клијент обратити серверу за издавање тикета. Сервер за издавање тикета издаје TGS (енгл. *Ticket Granting Service*) намењен клијенту и обезбеђује сесијски кључ који ће користити клијент у комуникацији са сервером.

11.5.2 Размена кључева на основу Керберос протокола

Овај протокол омогућава клијенту да након што добије тикет који обезбеђује приступ заштићеним серверима може да приступи одређеном сервисима или функцијама на већем броју различитих сервера. Ово је нарочито повољно обзиром на карактеристике здравственог информационог система где је корисницима потребно да користе одређени број различитих сервиса и да обрађују већи скуп података које је због перформанси и због безбедности потребно чувати на различитим серверима.

Сваки заштићени сервер који клијентима обезбеђује сервисе или податке

реализује комуникацију на основу различитих клијент – сервер апликација и предвиђен је за реализацију на инфраструктури Интернета. Друге предности овог протокола се односе на његову поузданост обзиром да је у употреби дужи временски период и да је у том периоду тестиран у великом броју различитих ситуација, такође, обзиром на његову флексибилност могуће га је имплементирати у комбинацији са другим системима. Поред тога, велики број оперативних система и серверских апликација већ има имплементиране функције које се заснивају на овом протоколу.



Слика 18 Керберос протокол – процес размене кључева

Поступак размене кључева и аутентификације клијента на основу Керберос протокола се реализује у штест корака:

1. Комуникацију иницира клијент који шаље шифровани захтев ка аутентификационом серверу који садржи идентификационе податке корисника, које шифрује на основу криптографског кључа који генерише на основу своје корисничке лозинке.
2. Након пријема овог захтева и након акредитације, аутентификациони сервер шаље клијенту поруку у виду тикета, односно TGT. TGT (енгл. *Ticket Granting Ticket*) је шифрован помоћу KA, односно симетричног кључа клијента који садржи кључ сесије KS који ће клијент користити у комуникацији са сервером за одобравање тикета и тикет који је намењен серверу за дозволу тикета који је шифрован симетричним кључем KTG који садржи идентификациоју клијента и кључ за ту сесију KS. Након пријема ове поруке клијент је поново генерише криптографски кључ KA којим дешифрује добијену поруку, односно TGT, после чега се тај кључ уклања.

3. Након успешног дешифровања поруке клијент шаље поруку серверу за одобравање тикета која садржи тикет добијен од аутентификационог сервера, домен, или име заштићеног сервера који чува податке или обезбеђује жељене сервисе и временску одредницу T коју шифрује кључем сесије KS.
4. Сервер за одобравање тикета шаље одговор клијенту у виду новог тикета који обезбеђује приступ сервисима, или подацима, TGS. TGS (енгл. *Ticket Granting Service*) садржи два тикета, по један за обе стране у комуникацији, односно један за клијента а други са сервер, или за групу сервера. Оба тикета садрже кључ сесије KAB и идентификаторе страна у комуникацији, A и B, са том разликом што је тикет намењен клијенту A шифрован сесијским кључем добијеним од сервера за аутентификацију, док је тикет намењен серверу B шифрован уз помоћ тајног кључа сервера, KB.
5. Након успешног дешифровања, клијент шаље тикет жељеном серверу који је шифровано сесијским кључем KAB, који садржи временску одредницу T и тикет добијен од сервера за одобравање тикета који садржи идентификацију клијента A и сесијски кључ KAB који је шифрован тајним кључем сервера B, KB.
6. Последњи корак у процесу размене кључева и аутентификације клијента је порука коју враћа сервер B која потврђује успешност успостављања заједничког кључа и тајност комуникације. Ова порука садржи временску одредницу коју је сервер примио у претходном кораку увећану за један која је шифрована сесијским кључем KAB.

12. Закључак

Радни задаци у здравственим организацијама у Републици Србији су организовани по принципима који су у складу са потребама тог система, међутим, ти радни задаци нису адекватно подржани када је у питању здравствени информациони систем. То узрокује значајне тешкоће у раду здравствених радника и значајне финансијске губитке. Имплементација савременог здравственог информационог система би позитивно утицала на продуктивност и на повећање квалитета здравствених услуга уз, истовремено, смањење трошкова, што би била последица боље информисаности и рационалније употребе постојећих ресурса. Поред тога, тај систем би омогућио здравственим радницима да свој посао обављају и са удаљених локација, као и да се информишу и размењују идеје са својим колегама. Наравно, реализација таквог информационог система подразумева оптималну имплементацију различитих информационо комуникационих технологија и адекватних система за заштиту података, контролу приступа и заштиту комуникација.

Резултати истраживања указују да околности у здравству не задовољавају све потребне услове за развој здравственог информационог система. Комуникациона инфраструктура задовољава потребне критеријуме, постојећа компјутерска опрема такође, али када је у питању софистицирана дијагностичка опрема, то није случај. Здравствене организације у Републици Србији располажу добром, али застарелом медицинском опремом коју није могуће интегрисати у здравствени информациони систем. Уколико нека од ових организација располаже са неким од савремених дијагностичких уређаја, услед недовољног стручног знања, недовољне техничке компатибилности тог и других уређаја, или услед кварова, ти уређаји су ван функције, односно употребљавају се, али уз бројна ограничења. Недостатак знања и вештина за употребу и одржавање савремених дијагностичких апарата се најчешће јавља у ситуацијама када здравствена организација добије на поклон неки такав уређај. Видео конференције, или видео упутства би значајно могла да помогну приликом оспособљавања и стављања у функцију ових уређаја.

Поред недостатка вештина за употребу софистицираних техничких уређаја, присутан је проблем недостатка вештина и знања за употребу стандардне компјутерске опреме. Едукација се реализује посредством пројеката различитих здравствених организација, затим посредством програмерских фирми које развијају модуле здравственог информационог система који је сада у функцији, кроз пројекте локалних заједница и непосредним контактом медицинског особља са особљем које је задужено за одржавање информационог система. Овакав начин не даје довољно добре резултате и не представља системско решење, али обзиром да не постоји стратегија са јасно дефинисаним циљевима, могуће је да су оваква делимична решења за сада најбоља.

Стратегија опремања здравствених установа и обучавања запослених у тим установама је сложен и дуготрајан процес који значајно утиче на развој здравственог информационог система, е-здравства и употребе информационо комуникационих технологија у здравству уопште. Постојеће стање је одраз устаљених навика које имају корисници здравствених услуга, међутим корисници би могли стећи бројне нове навике уколико би се појавили Интернет апликације где би могли квалитетно да се информишу, да закажу прегледе, да се консултују у вези са симптомима које имају и слично. То би смањило трошкове лечења и остале трошкове који настају у том процесу. Такође, здравствено особље би могло да путем Интернета стално буде

у току са новим информатичко здравственим достигнућима и да без додатних трошкова допринесу квалитету здравственог система.

Обзиром на постојећу ситуацију, здравствени информациони систем Републике Србије не задовољава потребе и захтеве које пред њега поставља друштво. Прикупљање података није организовано систематски, не постоје јасно дефинисана правила која налажу како треба да обрађивати прикупљене податка и није могуће направити довољно квалитетне анализе података, а самим ти ни квалитетне извештаје. Здравствене организације имају велики број високо мотивисаних радника са идејом да унапреде постојећи здравствени информациони систем, али без стратешких решења није могуће остварити значајније резултате јер се у постојећим оквирима не пружају такве могућности.

Уколико би здравствени информациони систем стварно подржавао процесе у здравственој делатности, стрес ком су изложени здравствени радници би се значајно умањио и они би могли да се у потпуности посвете пацијентима и да испуне своју правну и моралну обавезу, односно да помогну пацијенту. Важно је да здравствени радници на најбољи начин изађу у сусрет потребама пацијената и да им укажу на све оно што је њима важно. Нереално је очекивати да ће старији људи моћи да користе савремене информационо комуникационе технологије, али здравствено особље ће моћи, на основу чега ће информисати кориснике здравствених услуга о томе када их лекар може примити, односно, где би требали да се јаве и слично. То би, између осталог, утицало на рационалнију употребу постојећих ресурса.

Техничка реализација здравственог информационог система би обухватила развој информационо комуникационе мреже на територији Републике Србије на постојећој инфраструктури Интернета, имплементацију система за обезбеђивање тајности и интегритета података уз имплементацију инфраструктуре јавних кључева, едукацију медицинског, немедицинског и информатичког особља за употребу, одржавање и даљи развој здравственог информационог система.

Свака од ових целина је област којој је потребно прићи систематски, што није лак задатак када је у питању развој овако комплексног информационог система, али обзиром да је здравствени информациони систем Републике Србије мање развијен од сличних постојећих система у окружењу и у Свету, већ постоји искуство које може бити од великог значаја у том послу. Када су у питању безбедносни системи, домаћи стручњаци у овој области већ имају довољно знања и искуства стеченог у раду на сличним системима, што омогућава оптималну реализацију безбедносних система и њихову квалитетну имплементацију у здравствени информациони систем.

Министарство здравља је задужено за развој и координацију развоја здравственог информационог система који је до сада реализован кроз различите мање пројекте, најчешће финансиране и организоване од стране органа и организација Европске уније. Резултати тих пројеката су била парцијална софтверска решења која су једноставно реализована обзиром да није било потребе за реализацијом посебних криптографских система. На пример, постојећи здравствени информациони систем је организован тако да се здравствени подаци не снимају директно у централне базе података од стране здравствених радника, већ индиректно посредством систем администратора који прикупљене податке у локалним базама података шаљу путем Интернета захваљујући посебним Интернет апликацијама које су реализоване за ту намену. Такав начин манипулације подацима значајно умањује ефикасност здравственог информационог система.

Здравствени информациони систем би требао да поседује јединствени систем аутенитфикације и идентификације корисника. Зависно од врста корисника, врста медицинских уређаја, функција којима приступају ентитети тог информационог система и зависно од степена тајности података, потребна је имплементација различитих технологија и техника контроле приступа. Приступ неким од ресурса би могао бити једноставно контролисан захваљујући аутентифијацији корисника на основу корисничког имена и лозинке, док би приступ здравственим подацима пацијената захтевао идентификацију здравствених радника на основу дигиталног сертификата чији су власници. Уколико би се јавила потреба за реализацијом система идентификације на основу природних карактеристика, овоме би се могао додати и подсистем који би укључивао биометријске методе провере корисника. Ради једноставности и уштеде у времену, потребно је реализовати систем једноструког пријављивања корисника, који би након успешне аутентификације или идентификације, омогућио корисницима приступ свим оним подацима, функцијама и здравственим уређајима за које су ауторизовани.

Поред аутентификације корисника, здравствени информациони систем би требао да поседује систем за аутентификацију сервера. Идеално решење би представљало централизовано управљање кључевима и централизовано дигитално потписивање свих сервера у здравственом информационом систему. То би омогућило креирање великог децентрализованог информационог система који би се простирао на територији Републике Србије, а који би био изолован од остатка Интернета. Овакав вид контроле не би имао негативних ефеката, а била би могућа интеграција здравственог информационог система Републике Србије у глобални здравствени информациони систем. Трошкови који би настали услед реализације оваквог вида контроле не би били високи у поређењу са безбедношћу података и сигурношћу комуникације и у поређењу са могућностима и које би овакав систем пружао здравственим радницима и корисницима здравствених услуга.

Информационе технологије уносе револуционарне промене у све сфере наших живота и нормално је да велики друштвено технички системи као што је здравство имају своје наменски створене информационе системе. Ови системи пружају бројне предности, а свака од њих представља разлог за дигитализацију медицинских процеса у здравству и за увођење електронских здравствених картона. Имајући у виду интерес корисника здравствених услуга, будућност дијагностике и прописивања терапије неће моћи да се замисли без подршке здравственог информационог система. Уколико размотримо савремену дијагностику, познато је да постоји више од 100.000 симптома који могу да укажу на око 10.000 обољења, а дијагноза може представљати комбиновану појаву више обољења истовремено. Уместо листања књига ради постављања дијагнозе, упоређивања шифара обољења, шифара лекова и третмана, употреба компјутера у здравственом информационом систему може да једноставно реши тај проблем. Поред тога, савремене информационе технологије омогућавају да непрестано будемо у контакту и да стално надзиремо своје здравствено стање, па да на основу сакупљених података направимо квалитетне анализе и тако повећамо квалитет лечења. Здравствени информациони систем треба да омогући лекарима да део својих обавеза и део стреса ком су свакодневно изложени пренесу на тај систем, како би могли да се посвете ономе што је њихова примарна делатност, очувању здравља људи.

Литература

[1] Веиновић, М., Јевремовић, А., **Рачунарске мреже**, прво издање, Универзитет Сингидунум, Београд, 2011. године.

[2] Веиновић, М., Адамовић С., **Криптологија I**, прво издање, Универзитет Сингидунум, Београд, 2013. године.

[3] Милосављевић М., Адамовић С., **Криптологија II**, прво издање, Универзитет Сингидунум, Београд, 2014. године.

[4] Password Recovery Speeds, http://www.lockdown.co.uk/?pg=combi

[5] Smart Card HOWTO, http://tldp.org/HOWTO/Smart-Card-HOWTO/index.html

[6] Павловић Наташа, **Биометријска аутентификација базирана на пресјеку скупова**, Универзитет Црне Горе, Природно математички факултет, Подгорица, 2013. године.

[7] Understanding Enterprise Single Sign-On, http://msdn.microsoft.com/en-US/library/aa745042(v=bts.10).aspx

[8] The Kerberos Network Authentication Service (V5), http://www.ietf.org/rfc/rfc4120.txt

[9] VPN Technical Reference, http://technet.microsoft.com/en-us/library/cc780737(v=ws.10).aspx

[10] A Method for Storing IPsec Keying Material in DNS, http://www.ietf.org/rfc/rfc4025.txt

[11] Портал еУправа Републике Србије, http://www.euprava.gov.rs/.

[12] Педагошко друштво информатичара Србије, http://www.pdis.org.rs/.

[13] Министарство унутрашњих послова Републике Србије, http://www.mup.gov.rs/.

[14] Управа за заједничке послове републичких органа, http://www.uzzpro.gov.rs/.

[15] Републички завод за статистику, http://webrzs.stat.gov.rs/WebSite/.

[16] Управа за трезор Републике Србије, http://www.trezor.gov.rs/.

[17] Закон о електронским комуникацијама, http://www.paragraf.rs/propisi/zakon_o_elektronskim_komunikacijama.html

[18] Закон о електронском потпису, http://www.paragraf.rs/propisi/zakon_o_elektronskom_potpisu.html

[19] Закон о правима пацијената, http://www.zdravlje.gov.rs/downloads/2013/Jun/Jul2013ZakonOPravimaPacijenata.pdf

[20] Закон о заштити података о личности, http://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html

[21] Правилник о садржини технолошких и функционалних захтева за успостављање интегрисаног здравственог информационог система, http://www.rfzo.rs/download/pravilnici/mz/Pravilnik_integrisanizdrsistem.pdf

[22] Етички кодекс коморе медицинских сестара и здравствених техничара Србије, http://www.paragraf.rs/propisi/eticki_kodeks_komore_medicinskih_sestara_i_zdravstvenih_tehnicara_srbije.html

[23] Ивановић, И., **Здравствени информациони систем Републике Србије**, Институт за јавно здравље „Др Милан Јовановић Батут“, 2011. године.

[24] Опачић, М., **Информационе технологије у медицини**

[25] Продановић, Р., Кршљанин, Д., **Инфраструктура јавних кључева Министарства одбране и Војске Србије,** Центар за примењену математику и електронику, Војска Србије

[26] Ђорђевић, Д., **Дигитални потпис и дигитални сертификат**, Телекомуникациони форум ТЕЛФОР 2007. године, Београд 2007.

[27] Веиновић М., Бркић Б., Ћајић М., **Дистрибуција криптографских кључева у мобилним уређајима под андроид оперативним системом**, Инфотех – Јахорина, 9. део, Ref. E-VI-2, p. 823-826, Март 2010. године.

[28] Пајчин Б., Иваниш П., Софтверска реализација система за дигитално потписивање са хеш фунцијама и RSA алгоритмом, Инфотех – Јахорина, 10. део, Ref. E-III-3, p. 596-600, Март 2011. године.

[29] Петковић Л., Стефановић Д., Благојевић Д., **Креирање и аланиза безбедних Site-to-Site и Client-to-Site VPN конекција**, Инфотех – Јахорина, 10. део, Ref. B-III-5, p. 210-214, Март 2011. године.

Списак слика

Слика 1 Здравствени информациони систем 10
Слика 2 Електронско здравство 14
Слика 3 Креирање дигиталног потписа 25
Слика 4 Верификација дигиталног потписа 26
Слика 5 Распоред конектора у односу на ISO7816 стандард 34
Слика 6 Скица компоненти микропроцесорске картице 36
Слика 7 Разрешавање имена домена 48
Слика 8 Креирање ланца поверења у здравственом информационом систему 54
Слика 9 Authentication Header (AH) 58
Слика 10 Encapsulating Security Payload (ESP) 59
Слика 11 Управљање кључевима посредством центра за дистрибуцију кључева 62
Слика 12 Управљање кључевима посредством ауторитета за јавне кључеве 64
Слика 13 Размена дигиталних сертификата 65
Слика 14 Diffie – Hellman протокол 66
Слика 15 Needham – Schroeder протокол 68
Слика 16 Otway – Rees протокол 69
Слика 17 Керберос протокол – сервери 72
Слика 18 Керберос протокол – процес размене кључева 73

Списак табела

Табела 1 Препоруке за период употребе неких хеш алгоритама 25
Табела 2 Време потребно за потпуну претрагу кључева у зависности од врсте напада и броја карактера 32
Табела 3 Распоред конектора у односу на ISO7816 стандард 34
Табела 4 Предефинисани називи датотека и директоријума 35