*Драган Плакаловић* *УДК 004.738.5:621.39:339*

# БЕЗБЈЕДНОСТ ТРГОВАЊА ПУТЕМ МОБИЛНИХ УРЕЂАЈА


## *Резиме*

Трговање путем мобилних уређаја неће бити од интереса нити провајдерима таквих услуга нити клијентима, уколико обављање трансакција не буде безбједно. Да би трговање било безбједно, информациони систем који подржава одвијање трансакција треба да има сљедећа својства: аутентификација, ауторизација, интегритет, повјерљивост, расположивост и непорецивост. Циљ истраживања је да се да преглед технологија које су кандидати за обезбјеђивање наведених особина информационих система трговања путем мобилних уређаја.


**JEL klasifikacija: L86 - Information and Internet Services; Computer Software**

Кључне ријечи: мобилно трговање, информациони системи, заштита трансакција.

## 1. Увод

Увођењем Web сервиса на Интернету појављује се електронско трговање као нови начин продаје и размјене роба и информација. Развојем рачунарских бежичних мрежа и мрежа мобилне телефоније електронско трговање се проширује ка новом подручју, ка мобилном трговању. Овај нови начин трговања се дефинише као размјена или куповање и продаја роба, услуга и информација путем мобилних уређаја, као што су мобилни телефони, персонални дигитални асистенти итд.

Сматра се да је перспектива мобилног трговања добра јер је употреба мобилних уређаја у сталном порасту и што је мобилно трговање ефективан и удобан начин да се електронска трговина обавља било гдје и било када. Међутим, ова очекивања се неће испунити уколико мобилно трговање не буде безбједно, јер у том случају нити купци нити провајдери услуга мобилног трговања неће бити заинтересовани за тај вид трговине.
Са техничке тачке гледишта, мобилно трговање преко бежичних мрежа је инхерентно несигурно у поређењу са електронским трговањем преко жичаних мрежа. Разлози су дати у погледу:

- **поузданости и интегритета**: сметње и опадање сигнала чине да је канал бежичне комуникације подложан грешкама, чести прекиди такође деградирају квалитет безбједоносних сервиса;
- **повјерљивости, тј. приватности**: емитујућа природа радио-канала чини га лакшим за прислушкивање, комуникација може бити прислушкивана и интерпретирана без тешкоћа, ако се не користе безбједоносни механизми као што је криптографија;
- **идентификације**: мобилност бежичних уређаја уводи додатну тешкоћу у идентификовању мобилних терминала
- **капацитета:** бежични уређаји имају ограничену рачунску моћ, величину меморије, комуникациони опсег и снагу батерије, то отежава коришћење безбједоносних шема високог нивоа као што је 256-битно криптовање.

Безбједносна питања иначе прожимају читав систем мобилног трговања, она се протежу с једног краја на други, од врха до дна стека мрежног протокола, од машина до људи. Усредсредићемо се само на питања која су ексклузивно везана за мобилне/бежичне технологије. Недостајање јединственог стандарда бежичне безбједности, различите бежичне технологије подржавају различите аспекте и нивое безбједоносних карактеристика. Овдје ће се приказати само добро познати стандарди бежичних мрежа и њима кореспондентна безбједоносна питања.

## 2. ДЕФИНИЦИЈА БЕЗБЈЕДНОСТИ МОБИЛНОГ ТРГОВАЊА

Безбједност мобилног трговања се дефинише као примјена процедура из области технологије и менаџмента у мобилном трговању ради добијања сљедећих особина информација и система[1]:

- **Аутентичност:** Прије него што се пословање почне вршити, партиципирајући ентитети (обично пошиљалац и прималац) морају да потврде идентитет један другом. Ова особина штити од покушаја маскирања неовлаштеног учесника у легитимног учесника. Аутентичност се обично постиже коришћењем мрежно заснованог протокола аутентификације.
- **Повјерљивост података – тајност:** У трансакцијама електронског пословања, претпоставља се да ће само пошиљалац и примаоци ка којима је комуникација усмјерена моћи да разумију поруке које се преносе. Обезбјеђење тајности података спречава прислушкиваче и пресретаче да не разумију тајну комунукацију. То је обично остварено коришћењем рачунарски заснованог шифровања и дешифровања
- **Интегритет података:** Пренесена порука не смије бити промијењена случајно или злонамјерно, а да то не буде откривено од стране примаоца у систему мобилног трговања. Са овом безбједоносном карактеристиком пресретач није у могућности да превари примаоца промјеном садржаја поруке током преноса. Додавањем електронских потписа порукама обезбјеђује се интегритет података.
- **Ауторизација:** Морају да постоје процедуре које обезбјеђују провјеру да ли корисник може да наручи тражено, у смислу да ли има довољно новца на рачуну, да ли је регистровани корисник за пријем неких врста информација, итд.
- **Непорицање:** Трансакције мобилног трговања су званични пословни договори. Нити пошиљалац нити прималац не смију бити у могућности да порекну постојање легитимних трансакција након што су оне обављене, тј. пошиљалац може доказати да је одређени прималац примио поруку и прималац може доказати да је одређени пошиљалац послао поруку. Ово се обично остварује техникама дигиталног потписа.
- **Расположивост:** Расположивост система мобилног трговања обезбјеђује да легитимни корисници могу приступити пословном сервису поуздано и сигурно. Систем треба да буде дизајниран тако да може да минимизира утицај злонамјерних напада који врше деградацију перформанси система и на тај начин кориснике лишавају сервиса, који могу проузроковати да сервиси мобилног трговања постану нестабилни, па чак и нестабилни у дужим временским периодима. Распоређивање уређаја мрежне безбједности као што су фајерволи и њиховим конфигурисањем са припадајућим протоколима на погодан начин је кључ ка обезбјеђењу расположивости сервиса.

Систем мобилног трговања треба да обезбиједи сигурносне сервисе који ће омогућити да систем има горе наведене особине.

[1] "Advances in Security and Payment Methods for Mobile Commerce"

## 3. ЗАХТЈЕВИ КОЈЕ МАРАЈУ ДА ИСПОШТУЈУ СИГУРНОСНЕ МЕТОДЕ У МОБИЛНОМ ТРГОВАЊУ

Као прво, неопходно је испитати која својства методе сигурности мобилног трговања треба да имају да би проводиле ефективне и ефикасне трансакције мобилног трговања и са којом врстом изазова могу бити суочене у процесу развоја нових метода плаћања и сигурности мобилног трговања. Захтјеви су:

1. Повјерљивост, аутентичност, интегритет, ауторизација, расположивост и непорицање који морају бити ригорозно спроведени.
2. Треба да буду интероперабилни за већину система.
3. Треба да буду прихватљиви од стране садашњих и будућих система који смањују трошак.
4. Треба да дозволе провајдерима добара да обезбиједе приступачне, лаке за употребу, ефикасне и интероперабилне метода плаћања корисницима.
5. Трансакције у мобилном трговању не могу бити одложене током одвијања.

## 4. ОСНОВНЕ ЗАШТИТЕ

Да би постигли безбједоносне циљеве, дигитални подаци су криптују и декриптују на основу алгоритама криптографије. Постоје двије категорије криптографских алгоритама: системи са симетричним кључем и системи са асиметричним кључем.

### 4.1. Системи са симетричним кључем

У овој категорији пошиљалац и прималац повјерљиве сесије имају исти дигитални кључ. Пошиљалац шифрује поруке користећи овај кључ и онда их шаље преко јавне мреже ка примаоцу. Прималац дешифрује примљене поруке користећи исти кључ. Дигитални кључ, међутим, никада се не шаље преко мреже у директном облику. На тај начин се спречава да неко трећи добије кључ и да евентуално угрози безбједност комуникације. Ради постизања споразума о кључу, потребно је да обје стране имају посебне канале, као што је, на примјер, телефонска конверзација или посебно направљен дистрибуциони центар кључева.

Један од најчешће коришћених симетричних алгоритама за криптовање је DES. Horst Feistel из IBM-а је креирао Луцифер алгоритам , који је изабран као DES и то од стране владе САД и Националне безбједоносне агенције 1970. године. Овај алгоритам користи блок цифарску врсту шифровања. Та врста шифровања врши груписање бита у групе па на таквим групама извршава алгоритам шифровања. Овај алгоритам смањује вријеме коришћења процесорског времена, истовремено одржавајући солидан ниво безбједности. Међутим, због напретка у развоју рачунарских технологија, DES се не сматра више сигурним. Крајем деведесетих година прошлог вијека посебне машине за дешифровање DES шифара су успјеле да за само неколико сати изврше дешифровање података који су шифровани овим алгоритмом. Као резултат свега тога стари стандард је замијењен троструким DES стандардом. Троструки DES су три DES алгоритма постављена у ред (серију) од који сваки има различит кључ, тако да се један податак три пута шифрира заредом. Резлутат једног шифровања је улаз за друго шифровање итд. Мада је 3DES сигурнији, три проласка кроз DES чини да перформансе опадају. Нови стандард којих ће да замијени DES се назива AEC (Advanced Encryption Standard). Код овог стандарда узет је метод двојице Белгијанаца др Joan Deamen и др Vincent Rijmen и назива се Rijndael. Овај алгоритам је изабран на конкурсу међу четири финалиста јер је најбољи у погледу безбједности, високих перформанси, ефикасности, флексибилности и малих меморијских захтјева.

### 4.2. Крипографија јавних кључева

Истраживачи су 1976. године на Стенфорд универзитету развили криптографију јавних кључева да би ријешили питање безбједности размјене тајних кључева. Криптографија јавних кључева је асиметрична. Она користи два кључа са међусобном инверзном зависношћу. Другим ријечима, ако поруку шифрујемо јавним кључем, можемо је дешифровати приватним и обрнуто, ако поруку шифрујемо приватним кључем, можемо је дешифровати јавним кључем. Приватни кључ чува његов власник као тајну, док је јавни кључ доступан свакоме. Ако се јавни кључ користи за шифровање поруке, само одговарајући приватни кључ може извшити дешифровање и обрнуто. Свака страна у трансакцији има тајни и јавни кључ. Да би одаслао поруке на безбједан начин, пошиљалац користи јавни кључ примаоца да би извршио шифровање. Пријемник потом врши дешифровање помоћу свог приватног кључа. Под претпоставком да су власници сачували своје приватне кључеве као тајну, нико други не може дешифровати поруку сем правог примаоца. Тако систем обезбјеђује приватност. Мада су два кључа у математској зависности, „рачунски немогуће" је извести приватни кључ из јавног кључа. Потребно је огромно вријеме да би се извео приватни кључ и то тако велико да потпуно обесхрабрује покушаје да се тако нешто изведе.

И јавни и приватни кључ могу бити употријебљени за шифровање и дешифровање порука. На примјер, ако корисник употребљава јавни кључ трговца од кога купује робу, онда само трговац може дешифровати поруку користећи свој приватни кључ. На тај начин клијент је сигуран у идентитет трговца, јер само трговац има приватни кључ, тј. трговац је аутентификован. Са друге стране, трговац не може бити сигуран у идентитет клијента јер је кључ за криптовање јаван и свима расположив.

Ако се употребљавају као кључеви за шифровање и дешифровање, приватни и јавни кључ, респективно, онда пошиљалац поруке може бити аутентификован. На примјер: претпоставимо да купац шаље трговцу поруку шифровану кориштењем свог приватног кључа, трговац ће да дешифрује поруку користећи купчев јавни кључ. Пошто је купац криптовао поруку својим приватним кључем, трговац може бити сигуран у његов идентитет.

Процес аутентификује пошиљаоца, али не обезбјеђује и повјерљивост, пошто свако може да дешифрује поруку. Овај систем ради све док трговац може бити сигуран да јавни кључ купца који он има је и стварно јавни кључ купца, а не неке друге стране која изиграва да је купац. Проблем доказивања власништва јавног кључа биће описан касније.

Шифровање путем методе јавног кључа може бити употријебљено за аутентификацију и једне и друге стране у комуникацији[2]. Претпоставимо да трговац жели да пошаље повјерљиву поруку купцу, тј да је не може нико прочитати сем купца. Такође претпоставимо да трговац жели да докаже купцу да му он шаље поруку, а не неки преварант. Трговац ће прво шифровати поруку користећи купчев јавни кључ, чиме се гарантује да ће само купац прочитати ту поруку. Потом трговац овако добивену поруку шифрује користећи свој приватни кључ, чиме доказује свој идентитет. Купац дешифрује поруке у обрнутом редосљеду. Прво узима јавни кључ трговца да дешифрује поруку, па потом тако добивени резултат дешифровања подвргава дешифровању путем свог приватног кључа. Прво дешифровање аутентификује трговца, јер се прво дешифрује порука која је шифрована приватним кључем који има само трговац. Друго дешифровање обезбјеђује приватност, нико није могао прочитати поруку изузев купца, јер се дешифрује његовим приватним кључем. Мада овај систем обезбјеђује екстремно безбједне трансакције, трошкови извођења и потребног времена спречавају његову ширу употребу.

Најчешће употребљавани алгоритам код технологије јавног кључа је RSA, систем шифровања развијен 1977. на MIT-u.

[2] "Advances in Security and Payment Methods for Mobile Commerce"

Поред овог алгоритма користи се и PGP (Pretty Good Privacy) који је намијењен за шифровање електронске поште и фајлова. Овај алгоритам се може користити и за дигитални потпис који потврђује аутора електронске поште. PGP је заснован на „мрежи повјерења" у којој сваки учесник јамчи за идентитет другог учесника, а чија је сврха доказивање власништва јавног кључа. Ако корисник зна идентитет власника јавног кључа, путем персоналних контаката или другог безбједног метода, он проглашава кључ важећим потписујући га са властитим кључем. Са порастом корисника који могу да потврде кључеве један другом, мрежа расте. Повремено је потребно мијењати кључеве, јер потенцијални нападачи могу да подрвгну кључеве анализи и ако су они у оптицају дуже времена, повећава се вјероватноћа екстракције садржаја поруке. Такође, уколико неко открије кључ, моћи ће да га користи све док се он не промијени, па је и то још један од разлога да се повремено мијењају кључеви. Коришћењем криптографије јавног кључа могу се размијенити тајни кључеви на безбједан начин што дозвољава да се формира нови кључ за криптовање сваке поруке.

Као недостатак алгоритама јавног кључа може се навести њихова неефикасност код слања велике количине података, јер успоравају комуникацију. То не значи да их треба одбацити, него да се они користе за размјену тајних кључева, а да се потом комуникација одвија путем тајних кључева. Процес у коме двије стране размјењују кључеве преко несигурног медијума, назива се протокол споразума о кључевима. Протокол поставља правила за комуникацију, тј. тачно одређује који су алгоритми за криптовање и који ће се од њих користити.

Најпознатији протокол споразума о кључевима је дигитална коверта. Са дигиталном ковертом порука је шифрована кориштћењем приватног кључа, а приватни кључ је шифрован јавним кључем. Пошиљалац прилаже шифровани тајни кључ уз шифровану поруку и шаље примаоцу. Пошиљалац може да направи и дигитални потпис, да би прималац био сигуран у његов идентитет. За дешифровање поруке прималац прво дешифрује тајни кључ поруке, својим приватним кључем. Потом прималац користи тајни кључ да дешифрује поруку. Пошто само прималац може декриптовати шифровани тајни кључ, пошиљалац може бити сигуран да само жељени прималац чита поруку.

### 4.3. Протокол споразума о кључевима

Један од протокола споразума о кључевима може да буде заснован на систему јавних кључева[3]. По успјешној пријави клијент покушава да успостави комуникациону сесију са серверским процесом. И клијент и сервер имају тајне кључеве Кт и St. Пар кључева који чине тајни и јавни кључ је додијељен и клијенту и серверу (Кт,Кј), (St,Sj). Заједнички кључ за сесију се формира путем размјене кључева који су срачунати примјеном експоненцијалне функције на сљедећи начин:

- Кт и St су 128 битни случајни бројеви
- Кј = $\alpha^{Кт}$ мод М и Cj = $\alpha^{St}$ мод М , гдје су α и М познате константе.

Мада су јавни кључеви изведени из тајних кључева, обрнута операција је рачунски скупа јер би се састојала од вршења огромног броја израчунавања инверзне операције тј. дискретних логаритама и процјењивања таквих резултата. Корисници не могу изводити закључке о тајном кључу на лак начин, чак и када је алгоритам познат. На клијентској страни кључ сесије се рачуна кориштењем тајног кључа Кт и серверског јавног кључа Sj тако што се јавни кључ сервера степенује са тајним кључем сервера:

$$SKks = Sj^{Kt} = (\alpha^{St})^{Kt} = \alpha^{St*Kt}$$

Јавни кључ сервера се степенује.

[3] "Internet Security - Criptographic principles, algorithms and protocols"

Симетрично и независно, сервер израчунава кључ сесије SKsk коришћењем свог тајног кључа и клијентовог јавног кључа тако што степенује јавни кључ клијента са тајним кључем сервера:

$$SKsk = Kj^{St} = (\alpha^{Kt})^{St} = \alpha^{Kt*St}$$

Видимо да у оба случајева добијамо исту вриједност кључа сесије:

SKks = SKsk = SK. Кључ сесије је израчунат по модулу M. У овим формулама је операција добивања остатка цјелобројног дијељења изостављена ради јасноће. Након што је сесиони кључ генерисан, тајни кључеви су избрисани из меморије. Сесија заснована на кључу сесије успоставља узајамну аутентичност клијента и сервера пошто она може бити изведена само из тајних кључева

### 4.4. Управљање кључевима

Одржавањем приватних кључева као тајних је круцијално за криптографску безбједност. У већини случајева угрожавања безбједности разлог је лоше управљање кључевима (непажња приликом руковања приватним кључевима која резултује крађом кључа), а не напади који покушавају да открију кључ.

Главна компонента управљања кључевима је генерисање кључева. Злонамјерна страна може да покуша да декриптује поруку сваким могућим декрипционим кључем. Са друге стране, понекад су алгоритми за генерисање кључева конструисани да стварају кључева из мањег подскупа могућих кључева. Ако је подскуп мален,онда су криптовани подаци осјетљивији на овакву врсту напада.Стога је потребно имати програм за генерисање кључева који ће стварати велики број кључева и то што је могуће више на случајан, неодређен начин. Кључеви се праве безбједнијим ако је њихова дужина што већа, тако да је рачунарски немогуће испробати све могуће комбинације.

### 4.5. Дигитални потпис

Дигитални потпис, електронски еквивалент писаних потписа, развијен је у оквиру криптографије јавног кључа ради рјешавања проблема аутентификације и интегритета. Дигитални потпис аутентификује пошиљаочев идентитет и као код писаног потписа тешко га је фалсификовати.

Да би креирао дигитални потпис, пошиљалац прво узима оригиналну поруку и користи је као улаз у хеш функцију (хеш функција – функција сажетка), тј. математску калкулацију која поруци даје хеш вриједност. Безбједни хеш алгоритам (SHA-1) је актуелни стандард за хеш функције. Шанса да двије различите поруке имају исти извод је статистички безначајна. Колизије се дешавају када двије различите поруке имају исту хеш вриједност. Рачунски је немогуће израчунати поруку из њене хеш вриједности или наћи двије поруке које имају исту хеш вриједност.

Даље, пошиљалац користи свој приватни кључ да криптује извод поруке. Овај корак ствара дигитални потпис и аутентификује пошиљаоца. Сада се примаоцу шаље проширена порука која се састоји од дигиталног потписа, сажетка и полазне поруке са корисниковим садржајем која је, наравно, шифрована и то примаочевим јавним кључем. Пријемник користи пошиљаочев јавни кључ да дешифрује дигитални потпис и открије извод поруке. Пријемник потом користи свој приватни кључ да дешифрује оригиналну поруку. На крају, пријемник примјењује хеш функцију на оригиналну поруку и ако тако добивена вриједност одговара сажетку поруке која је добијена у потпису, онда је одржан интегритет поруке, тј. порука није промијењена током преноса.

Фундаментална је разлика између писаног и дигиталног потписа. Својеручни потпис је независан од документа који се потписује. Тако, ако неко на примјер

фалсификује писани потпис, он може користити тај фалсификат за више докумената. Дигитални потпис је створен на основу садржаја документа. Стога је дигитални потпис различит за сваки документ који се потписује.

Дигитални потписи не обезбјеђују доказ да је порука послана. Размотримо сљедећу ситуацију: уговарач шаље компанији дигитално потписан документ, који касније жели да опозове. Уговарач може такође да престане да чува свој приватни кључ као тајну и да тврди да је дигитално потписан уговор дошао од неког другог који је наводно украо његов кључ. Временско означавање, које повезује дигитални документ са датумом и временом, може помоћи да се ријеши проблем порицања. На примјер, претпоставимо да компанија и уговарач преговарају о уговору приликом чега компанија захтијева од уговарача да потпише документ дигитално и да документ добије временску ознаку од стране агенције за временско означавање. Уговарач шаље дигитално потписан уговор овој агенцији. Приватност документа ће бити очувана јер агенција добија шифровани документ, дигитално потписан. Агенција ставља датума пријема на криптовану дигитално потписану поруку и врши дигитални потпис на комплетну поруку са приватним кључем агенције. Сада временска ознака не може бити промијењена ни од кога изузев агенције, пошто нико изузев агенције не посједује њен приватни кључ. Изузев да уговарач извијести да је његов кључ угрожен прије него што је документ добио временску ознаку, уговарач неможе легално доказати да је документ потписан од стране неког другог. Пошиљалац може такође захтијевати од пријемника да потпише поруку дигитално и да је временски означи као доказ пријема.

### 4.6. Инфраструктура јавног кључа, цертификати и цертификациона тијела

Проблем са криптографијом јавног кључа је да свако са сетом кључева потенцијално може да претпостави идентитет друге стране. На примјер, рецимо да купац жели да наручи робу од онлајн трговца. Како ће купац знати да веб сајт припада трговцу, а не неком другом ко се претвара да је трговац да би украо информацију о кредитној картици? PKI обезбјеђује солуцију за такве проблеме. PKI интегрише криптографију јавног кључа са дигиталним цертификатима и цертификационим тијелима да би се аутентификовале стране у трансакцији.

Дигитални цертификат је дигитални документ који се користи за идентификацију корисника и издаје се од стране цертификационих тијела. Дигитални цертификат укључује име субјекта (компаније или индивидуе која се цертификује), субјектовог јавног кључа, серијског броја, датума истека, потписа цертификационих тијела од повјерења и друге релевантне информације. Надлежни за цертификацију су су финансијска институција или нека други повјерљиви учесник као што је Верисигн. Након издавања, дигитални цертификат је јавно расположив и смјештен у бази података које имају цертификациона тијела. Цертификациона тијела потписују цертификате шифровањем или субјектовог јавног кључа или резулата хеш функције гдје је за улаз у ову функцију узет субјектов јавни кључ. Шифровање се врши приватним кључем надлежног за ауторизацију. Надлежни за ауторизацију морају да верификују сваки субјектов јавни кључ. На тај начин корисници морају да вјерују јавном кључу који је издало цертификационо тијело. Обично је свако цертификационо тијело дио хијерархије. Ова хијерархија је слична ланцу повјерења у којој свака веза почива на другој вези ради обезбјеђења потврде идентитета. Врх хијерхије надлежних за цертификацију је Internet Policy Registration Agency (IPRA). IPRA потписује цертификате коришћењем коријенског (полазног, врховног) кључа. Овим кључем се потписују само цертификати за креирање политике надлежних за давање цертификата. Даље, надлежни за постављање правила издавања цертификата потписују дигиталне цертификате за надлежне за давање цертификата. Потом надлежни за давање цертификата потписују организацијама и индивидуама. Надлежни за цертификацију преузимају одговорност,што захтијева од њих опрезност приликом издавања дигиталног цертификата.

Периодично мијењање парова кључева је неопходно у одржавању безбједности система, пошто приватни кључ може бити угрожен без знања корисника. Што се дуже употребљава исти пар кључева, то су они рањивији. Као резултат дигитални цертификати имају рок трајања, да би натјерали кориснике да мијењају парове кључева. Ако је приватни кључ угрожен прије истека рока трајања, он може бити отказан и корисник може добити нови пар кључева и дигитални цертификат. Отказани и опозвани кључеви се налазе на посебној листи формираној управо ради таквих кључева. Важно је да свако одмах обавијести надлежне за дигиталне цертификате ако примијети да су кључеви угрожени, јер питање непорицања чини власнике цертификата одговорним за све што се деси везано за њихов кључ.

Употребом инфрастуктуре јавног кључа можемо безбједно обављати трансакције. Алгоритми за формирање кључева су тако добри да их је скоро немогуће угрозити. По неким процјенама, алгоритми кључева су тако безбједни да чак ни милиони данашњих компјутера који раде паралелно не може дешифровати кодове ни за сто година. Међутим, како снага рачунара расте, тако алгоритми који се данас сматрају сигурним у будућности бити разбијени.

### 4.7. Паметне картице

Једна од апликација инфраструктуре јавног кључа која је у највећем порасту је паметна картица. Паметна картица изгледа као кредитна картица и служи за многе различите функције, од аутентификације до смијештања података. Најпопуларније паметне картице су меморијске и микропроцесорске картице. Меморијске картице су сличне флопи дисковима. Микропроцесорске паметне картице су сличне малим компјутерима са оперативним системом, безбједношћу и меморијским капацитетом. Паметне картице такође имају различите интерфејсе путем којих међудјелују са читачима. Један тип интерфејса је контакт интерфејс у који су паметне картице убачене и физички контакт између читача и паметне картице је неопходан. Алтернативни метод је интерфејс без физичког контакта код кога се подаци преносе ка читачу преко уграђеног бежичног уређаја у картици.

Паметне картице чувају приватне кључеве, дигиталне цертификате и друге информације неопходне за имплементирање инфраструктуре јавног кључа. Такође могу да садрже број кредитне картице, персоналне контакт информације итд. Свака паметна картица се користи у комбинацији са PIN бројем (personal identification number). Ова апликација обезбјеђује два нивоа безбједности, захтијевајући од корисника да посједује и паметну картицу и да има одговарајући PIN број да би приступио информацијама на картици. Као додатна мјера сигурности, неке микропроцесорске картице бришу погрешне податке ако се деси злонамјерни покушаји кварења података. Паметне картице са PKI су портабилне, дозвољавајући корисницима да приступе информацијама са различитих уређаја користећи исту паметну картицу.

Многи мобилни уређаји користе паметну картицу за аутентификацију. Паметне картице још увијек не гарантују потпуну безбједност, јер ако се мобилни уређај изгуби, дигитални цертификат и приватни кључеви који су смјештени на паметној картици, могу постати доступни прекршиоцу који потенцијално може приступити приватним информацијама. Коришћењем корисничког налога и PIN броја који су неопходни за активирање уређаја, добија се већи ниво безбједности.

Бежични модул идентитета (WIM - Wireless Identity Module) је паметна картица која је укључена у бежични апликациони протокол верзија 2.0. WIM картица штити мобилне комуникације и трансакције са дигиталним потписом.

### 4.8. Мрежна инфраструктура и безбједност

Мрежна инфраструктура обезбјеђује основни капацитет за комуникацију гласом и подацима за клијенте и испоручиоце у сајбер свијету. Развијајући се од електронске

трговине до мобилног трговања, неопходно је за жичану мрежну инфраструктуру, као што је Интернет, да буде проширена бежичним мрежама које подржавају мобилност крајњих корисника. Мобилно трговање је могуће захваљујући расположивости бежичних мрежа. Кориснички захтјеви су испоручени ка најближем бежичном акцес поинту у локалним бежичним мрежама или базној станици у мрежама мобилне телефоније. Мада жичане мреже нису од есенцијалног значаја у системима мобилног трговања, већина сервера мобилног трговања су умрежени у жичане мреже и захтјеви корисника су најчешће усмјерени ка тим серверима коришћењем транспортних и безбједоносних сервиса које обезбјеђују жичане мреже. Међутим, овдје ћемо се задржати само на безбједоносним аспектима бежичних мрежа.

Могућност бежичне комуникације подржава мобилност крајњих корисника у системима мобилног трговања. Бежичне LAN и WAN мреже су главне компоненте које се користе за обезбјеђивање радио-комуникационих канала за стварање мобилних сервиса. У WLAN категорији Wi-Fi стандард са пропусношћу од 11 MBps доминира тржиштем. Очекује се да ће стандарди са много већим брзинама преноса, као што је IEEE 802.11a и 802.11г замијенит Wi-Fi. Технологије мрежа мобилне телефоније се брзо развијају. Њихова предност је широка распрострањеност са већим покривањем радио-сигналом, али им је недостатак мањи пропусни опсег за пренос података (мање од 1МБ)

## 5. БЕЖИЧНЕ МРЕЖЕ

### 5.1. Бежичне локалне мреже и безбједност

Уређаји који се користе у бежичним технологијама локалних мрежа су лагани за преношење и прилагодљиви мрежној конфигурацији. Стога је бежична локална мрежа прикладна за мреже у канцеларији, кућне мреже, персоналне мреже и ад хок мреже. У бежичним локалним мрежама од једног хопа, акцес поинт који дјелује као рутер или свич је дио жичане мреже и мобилни уређаји се директно повезују са акцес поинтом путем радио канала. Ако акцес поинт није расположив, мобилни уређаји могу формирати бежичну ад хок мрежу између себе самих и размијенити пакете података или извршити пословну трансакцију.

**Bluetooth технологија** покрива веома ограничено подручје и има малу пропусност. Прикладна је само за апликације у персоналним мрежама. Wi-Fi 802.11б је сада најпопуларнији систем у бежичним мрежама и користи се у канцеларијама, кућама, јавним просторима као што су аеродроми, трговине и ресторани. Сматра се да ће стандарди са већим брзинама 802.11 а и 802.11г замијенити 802.11б у блиској будућности.

- **Wi-Fi безбједност** Безбједност 802.11 бежичних мрежа обезбијеђена је протоколом на нивоу дата линка који се назива (WEP - Wired Equivalent Privacy). Када је омогућен, сваки мобилни хост има тајни кључ који је дијељен са базном станицом. Алгоритам шифровања који се користи у овом протоколу је ток цифара заснован на RC4. Текст који је кодиран цифрама се генерише помоћу ексклузивног IPI на обичном тексту са RC4 генерисаним током кључева. Међутим, литература која је објављена у задње вријеме открива слабости у начину на који се употребљава RC4 у WEP протоколу. Нова верзија протокола која има ознаку 802.11i, има бољу безбједност која се остварује упошљавањем сервера за аутентификацију који одваја процес аутентификације од акцес поинта, заснованошћу на AES алгоритму и на бољој диструбуцији кључева.[4]
- **Bluetooth безбједност** Bluetooth обезбјеђује безбједност коришћењем фреквентног хоповања у физичком слоју преноса, дијелећи тајне кључеве (тзв. passkeys) између подређеног и надређеног, енкриптујући комуникационе канале и контролишући интегритет. Шифровање у Bluetooth технологији је ток цифара који се назива Ео док се

[4] Real 802.11 Security

за контролу интегритета користи блок цифара такозвани „SAFER+". Међутим Ео има потенцијалну слабост и спорији је од других сличних система са симетричним кључевима и са блок цифрама

### 5.2. Бежичне глобалне мреже и безбједност

Најважнија технологија у овој категорији је бежична мрежа мобилне телефоније. Ова мрежа може спроводити операције мобилног трговања путем мобилних телефона. Код овог сценарија, мобилни телефон се повезује директно са најближом базном станицом, гдје се комуникација преноси до сервисног сајта кроз радио приступну мрежу и друге фиксне мреже.

Првобитно замишљене за комуникацију гласом, ћелуларне мреже су се развиле од аналогних до дигиталних, од виртуелних кола до пакетских, да би се прилагодиле апликацијама мобилног трговања.

- **Безбједност GSM мрежа** SIM (Subscriber Identification Module) картица у GSM мрежи садржи информације претплатникове аутентификације, као што су кључеви за шифровање и јединствени идентификатор који се назива међународни мобилни претплатнички идентитет (IMSI – International Мобиле Subscriber Identification). SIM је обично имплементиран као паметна картица која се састоји од микропроцесора и меморијских чипова. Исти аутентификациони кључ и IMSI су смјештени на GSM страни мреже у аутентификационом центру и локационом регистру, респективно. У GSM-у, кратке поруке су смјештене у SIM и позиви су усмјерени радије ка SIM-у него мобилном терминалу. То својство дозвољава GSM претплатницима да дијеле терминал са различитим SIM картицама. Безбједоносне карактеристике које су на располагању између GSM мреже и мобилне станице укључују повјерљивост и аутентификацију IMSI, повјерљивост корисничких података и повјерљивост сигналног информационог елемента. Једна од слабости у безбједности GSM мрежа је једносмјерна аутентификација, тј. мобилна станица је аутентификована, а мрежа није. То може бити пријетња безбједности, јер се може појавити станица у средини и извршити напад а да мобилна станица то не открије.
- **UMTS (Universal Mobile Telecommunications System) безбједност** UMTS је технологија треће генерације мрежа мобилне телефоније. UMTS је дизајниран да се користи и развија од постојећег језгра мрежних компоненти GSM и GPRS система и да поправи безбједоносне слабости као што су једносмјерна аутентификациона шема и опционално шифровање. Аутентификација у UMTS је узајамна и шифровање је обавезно, да би се спријечила реприза поруке и модификација. Уз све то, UMTS користи дуже криптографске кључеве и новије цифарске алгоритме, који га чине безбједнијим од GSM-а и GPRS-а.

### 5.3. Бежични апликациони протокол и безбједност

Поред комуникационих механизама на нивоу дата линка које обезбјеђују безичне локалне мреже, бежични апликациони протокол (WAP – Wireless Aplication Protocol) је дизајниран да ради са свим бежичним мрежама. Најважнија технологија која се користи у овом протоколу је WAP gejtvej, који преводи захтјеве од WAP протокол стека ка WWW стеку, тако да могу бити прослијеђени ка Веб серверима. На примјер, захтјеви од мобилних станица се шаљу као URL адресе кроз мрежу ка WAP gejtveju, одговори се шаљу од Веб сервера ка WAP gejtveju у HTML-у и преводе се у WML и шаљу се ка мобилним станицама. Мада WAP подржава HTML и HML његов језик је WML, који је језик заснован на HML и направљен је да се користи у спецификацији садржаја и корисничких интерфејса за мобилне уређаје. WAP такође подржава WML skript, који је сличан Java scriptu али чини минималне захтјеве у меморијском погледу и снази процесора јер не садрже неке непотребне функције које су присутне у другим скрипт језицима.

WAP безбједност је дата кроз бежичну безбједност транспортног нивоа (WTLS) Овај протокол обезбјеђује интегритет података, приватност и аутентификацију. Један безбједоносни проблем у овом протоколу је узрокован постојањем WAP gejtveja када се поруке обрађују. Једна солуција је да се направи WAP gejtvej резидентним унутар мреже предузећа, гдје би се користили јачи безбједоносни механизми.

## 6. Закључак

Без безбједне размјене пословних информација и сигурних електронских финансијских трансакција на мобилним мрежама, нити ће сервис провајдери нити потенцијални клијенти вјеровати мобилном пословању. Различите процедуре за обезбјеђивање безбједности у раду са мобилним уређајима су предложене и примијењене на мобилно пословање и овај рад покушава да представи њихов преглед на разумљив начин. Сигурни системи за мобилно трговање морају да задовољавају сљедећа својства: повјерљивост, аутентичност, интегритет, ауторизацију, расположивост и непорицање. Ова својства се данас постижу у првом реду рјешењима заснованим на технологији јавних кључева, дигиталних потписа и дигиталних цертификата, која се једним именом називају инфраструктура јавних кључева. Недостатак инфраструктуре јавних кључева код њене примјене у мобилним уређајима је захтјевност алгоритама шифровања у погледу процесорске моћи и меморијских капацитета, а познато је да су ти ресурси код ових уређаја оскудни. Због тога су у употреби и неки други механизми заштите који праве компромис у смислу повећане употребљивости, а на рачун тврдоће и непробојности алгоритама шифровања. При томе се врши опредјељивање за алгоритме са краћим кључевима (56 битним) у односу на кључеве инфраструктуре јавних кључева (128 бита), а да је и даље такав поступак заштите непробојан за постојеће рачунарске капацитете. Стога на подручју безбједности извођења трансакција путем мобилних рачунара постоји шароликост технологија, док у случајевима трансакција електронске трговине у жичаним мрежама то није случај.

## ЛИТЕРАТУРА:

Hu, W., Lee, C., Kou, W., (2004). Advances in Security and Payment Methods for Mobile Commerce, Idea Group Publishing

Deitel, H., M., Deitel, P., J., Nieto, T., R., Steinbuhler, K., (2002). Wireless Internet & Mobile Business How To Program, Prentice-Hall

Peikari, C., Fogie, S., (2002). Maximum Wireless Security, Sams Publishing

Edney, J., Arbaugh, W., (2003). Real 802.11 Security: Wi-Fi protected Access and 802.11i, Addison Wesley

Tara,M., Elden, C., (2002) Wireless Security and Privacy: Best Practices and Design Techniques, Addison Wesley

Rhee, M., Y., (2003) Internet Security - Criptographic principles, algorithms and protocols, Wiley

---

Безбједност трговања путем мобилних уређаја
Драган Плакаловић,
дипл. инж. ел.
Информациони системи, архитектура апликативног софтвера за рачунарске мреже
Економски факултет Универзитета у Источном Сарајеву, Алексе Шантића 3, 71420 Пале, БиХ
057/224-945, 065/306-640, dplakalovic@yahoo.com

# СТРУЧНИ ЧЛАНЦИ

- ***супституцију у плаћању*** ( када је страна валута у употреби као средство плаћања);
- ***финансијску супституцију*** ( када домаћи резиденти држе финансијску активу у страној валути);
- ***реалну супституцију*** ( када су цијене или плате у домаћој привреди изражене у страној валути);

Што се тиче земаља у развоју, асиметрична валутна супституција је широко распрострањена, међутим, разлике се јављају у валути за коју се домаћа валута веже. Тако се у земљама Латинске Америке јавља амерички долар ($), као и у Русији и Азији, док се валуте земаља Балкана вежу за евро (€) ( или њемачку марку прије увођења евра). Због широко прихваћеног долара као „боље" валуте у земљама Латинске Америке, појава валутне супституције се често у литератури може срести и под називом доларизација (*dollarization*).

У овом раду највише ће бити ријечи о асиметричној супституцији као појави која је карактеристична за земље у развоју и која негативно утиче на макеоркономију и привреду.

## *1. Фактори валутне супституције*

Валутна супституција се обично јавља у земљама са дужом историјом макроекономске неравнотеже, односно, гдје се јавља висока стопа инфлације која је таква дужи временски период. Тада се домаћи резиденти више окрећу коришћењу стране валуте ( која је стабилнија и сигурнија) од домаће, која губи куповну моћ и на тај начин смањује своју куповну моћ. На другој страни, страна валута је стабилнија и није под утицајем високе инфлације. Управо из тога разлога се приликом доларизације узимају валуте земаља чија привреда нема веће промјене осцилације.

Ниво валутне супституције се може изразити као однос депозита у страној валути у односу на укупне депозите. Одређена стопа валутне супституције се јавља у већини земаља па је тако у развијеним земљама у 2002. години износила 6,6% док је у економијама у транзицији била 47,7% а у земљама Јужне Америке 55,9% ( табела 1 )[2]

| *РЕГИОН* | *БРОЈ ЗЕМАЉА У РЕГИОНУ* | *ГОДИНА 2001.* | *ГОДИНА 2002.* |
|---|---|---|---|
| *Јужна Америка* | 8 | 54 | 55,9 |
| *Економије у транзицији* | 26 | 46,9 | 47,7 |
| | | | |
| *Развијене земље* | 14 | 7 | 6,6 |

***Табела 1. Просјек учешћа страних депозита у укупним депозитима***

На валутну супституцију утичу сви они фактори који утичу и на тражњу новца, односно, ниво релане имовине, институционални фактори и разлика између очекиваних стопа приноса на домаћи и страни новац.

[2] G.D.Nicolo, P. Honohan, A.Ize, *Dollarization of The Banking sistem: Good od Bad*?, IMF working paper 03/146, July 2003

***Ниво реалне имовине*** представља оквир, односно представља лимит за тражњу како домаћег тако и страног новца. Што је већи обим реалне активе, односно дохотка, већа је тражња за новцем.

***Институционални фактори*** предсатвљају још један од фактора који утичу на валутну супституцију и они се односе на могућност држања различитих облика имовине као што су реалне активе, хартије од вриједности и девизне пласмане.

Одабир одређене врсте имовине која ће се преферирати при инвестирању првенствено зависи од финансијске моћи домаћих резидената, али и каматних стопа и нивоа инфлације у земљи. Наиме, уколико је цијена реалних актива већа и брже расте од стопе инфалције, улагање у реалне активе је врло атрактивно и исплативо инвестирање. Исто тако, ако је развијено финансијско тржиште и ако оно обезбјеђује довољан степен ликвидности, улагање у хартије од вриједности може бити једна од повољнијих могућности за инвестирање. Међутим, земље у развоју углавном или немају развијена финансијска тржишта или нису развијена до степена који обезбјеђује висок ниво ликвидности, па тако ова врста улагања није толико заступљена у овим земљама. Најраспрострањенији начин који резиденти користе код валутне супституције јесте држање депозита у страној валути.

***Алтернативно држање новца и других финансијских актива у домаћој или страној валути*** је одређено разликом каматних стопа на једну или другу валуту у односу на стопу инфлације. Бира се валута која има позитивну реалну каматну стопу, односно, валута код које је каматна стопа виша од стопе инфлације. Исто тако очекивања у погледу девалвације опредјељују трансакторе да бирају валуту у којој ће држати своју финансијксу активу. Уколико су очекивања да ће депресијација једне валуте бити већа у односу на депресијацију друге валуте, а при томе каматне стопе не компензују ту очекивану депресијацију, онда ће се средства усмјеравати ка стабилнијој валути.

## *II ЕФЕКТИ И УТИЦАЈ ВАЛУТНЕ СУПСТИТУЦИЈЕ*

### *1. Губитак традиционалних функција новца*

Свака земља настоји да путем одређених привредних активности побољша своју привреду и економију. Самим тим постиже се и веће повјерење у државне органе и власт, али и у домаћу валуту. У таквим условима, домаћа валута обавља све своје функције, односно она је средство размјене, трансакционо средство и средство за чување имовине. У неким земљама валутна супституција је и формално уведена, односно страна валута је и законско средство плаћања, формална валутна супституција постоји у мањем броју земаља као што су Еквадор, Панама, Црна Гора и неким другим земљама, док је неформална валутна супституција заступљена у много већем броју земаља.

У условима валутне супституције домаћи новац почиње да губи своје традиционалне функције, односно престаје да буде јединица обрачуна или средство у коме се држи штедња. У ком обиму ће домаћи новац губити своје битне функције, зависи прије свега од висине и дужине трајања инфлације.

Наиме у периоду од 1990. до 1999. године, већина земаља у развоју је имала високе стопе инфлације, а самим тим и високу валутну супституцију ( табела 2)[3].

| РЕГИОН | 1990 – 1994. | 1995 – 1999. | 2000 – 2003. |
|---|---|---|---|
| Азија | 7,3 | 11,2 | 4,4 |
| Латинска Америка | 365,6 | 14,8 | 9,3 |
| Земље у транзицији | 873,0 | 44,1 | 10,4 |
| Развијене земље | 4,6 | 2,1 | 2,2 |

*Табела 2. Просјечна инфлација по регионима ( у процентима годишње)*

Почетком 90-их година висок ниво инфлације је забиљежен у Латинској Америци, Африци и земљама у транзицији, па се до 2001 године у тим земљама јавила и висока стопа валутне супституције, гдје је скоро пола вриједности укупних депозита банака било у страној валути.

Почетком 2000. године стопа инфлације у већини поменутих земаља је била на прихватљивом нивоу и стабилна, очекивана реакција на смањење стопе инфлације је била да домаћи резиденти користе домаћу валуту и смање количину стране валуте у свом посједу путем држања штедње, приликом трансакција и сл.

Међутим, и у таквим условима степен валутне супституције се није промијенио сразмјерно са опадањем стопе инфлације. Ова појава се јавља из простог разлога што је већина поменутих земаља била дужи временски период под високом стопом инфлације, па тако домаћи резиденти немају повјерење у домаћу валуту и не желе да је користе у свакодневној употреби као ни при чувању штедње, тако да, иако је стопа инфлације ниска, стопа валутне супституције је висока.

Очигледан примјер ове појаве је БиХ, гдје је стопа инфлације на релативно ниском нивоу, али је стопа валутне супституције мјерена односом депозита у страној валути у односу на укупне депозите, изразито висока. У табели 3 и графикону 1 се може видјети кретање депозита у страној валути у односу на депозите у домаћој валути и у односу на укупне депозите банака од 1998. до 2006. године у БиХ.[4]

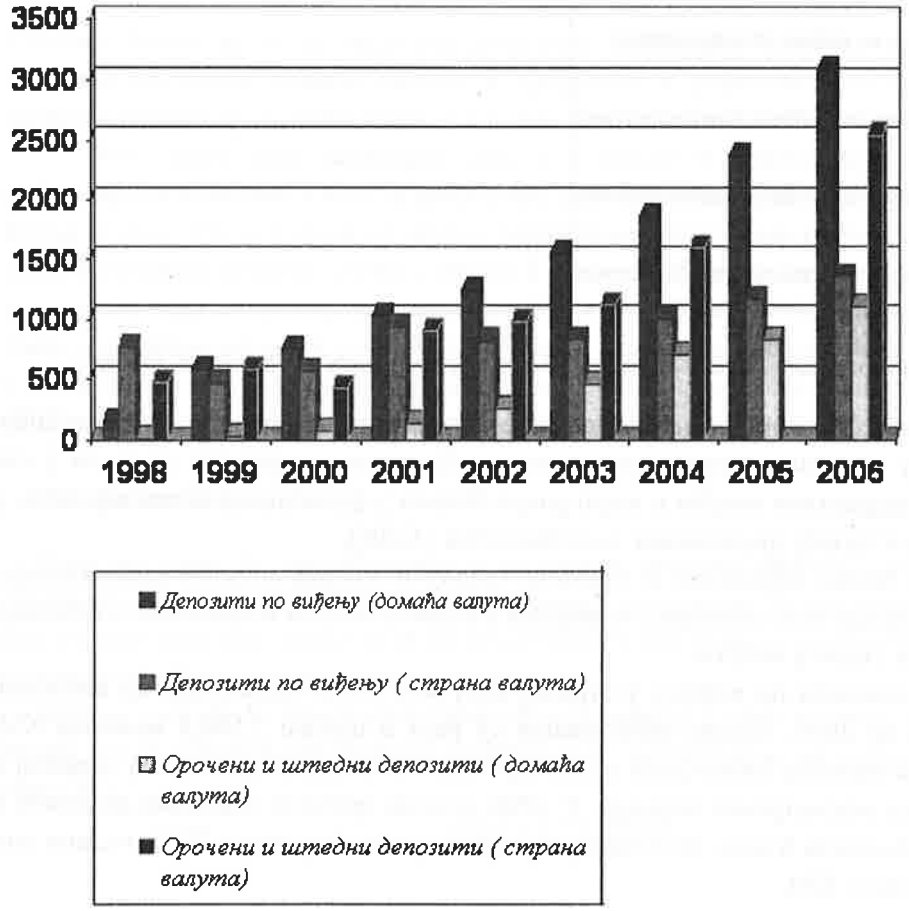
| ГОДИНА | 1998. | 1999. | 2000. | 2001. | 2002. | 2003. | 2004. | 2005. | 2006. |
|---|---|---|---|---|---|---|---|---|---|
| Депозити по виђењу у домаћој валути | 147,5 | 584,5 | 750,0 | 1.018,4 | 1.232,3 | 1.553,1 | 1.863,9 | 2.373,6 | 3.092,3 |
| Орочени и штедни депозити у домаћој валути | 8,0 | 23 | 77,9 | 140,9 | 261,2 | 462,2 | 705,5 | 818,8 | 1.098,8 |
| Депозити по виђењу у страној валути | 762,1 | 465,5 | 559,5 | 928,5 | 817,1 | 818,7 | 988,1 | 1.154,8 | 1.358,8 |
| Орочени и штедни депозити у страној валути | 467,0 | 577,3 | 428,2 | 907,7 | 974,4 | 1.118,9 | 1.604,0 | 1.999,4 | 2.544,4 |

[3] R.Rennhac, M. Nozaki, Financial Dollarization in Latin Amerika, IMF working paper 06/7. 2004
[4] Билтен бр. 3 и 4, Централна банка БиХ, 2004. и 2006. година

***Табела 3 Депозити у страној и домаћој валути у периоду од 1997. до 2006. године у милионима КМ***

| ГОДИНА | 1998. | 1999. | 2000. | 2001. | 2002. | 2003. | 2004. | 2005. | 2006. |
|---|---|---|---|---|---|---|---|---|---|
| Депозити по виђењу у страној валути | 9,6 | 11,0 | 29,9 | 21,8 | 24,6 | 27,96 | 27,27 | 29,5 | 30,7 |
| Орочени и штедни депозити у домаћој валути | 0,5 | 1,1 | 3 | 3 | 5,2 | 8,32 | 10,32 | 10,1 | 10,9 |
| Депозити по виђењу у страној валути | 49,25 | 21,5 | 22,65 | 19,87 | 16,19 | 14,86 | 14,46 | 14,3 | 13.5 |
| Орочени штедни депозити у страној валути | 30,18 | 26,65 | 17,34 | 19,4 | 19,21 | 20,05 | 23,84 | 24,7 | 25,3 |

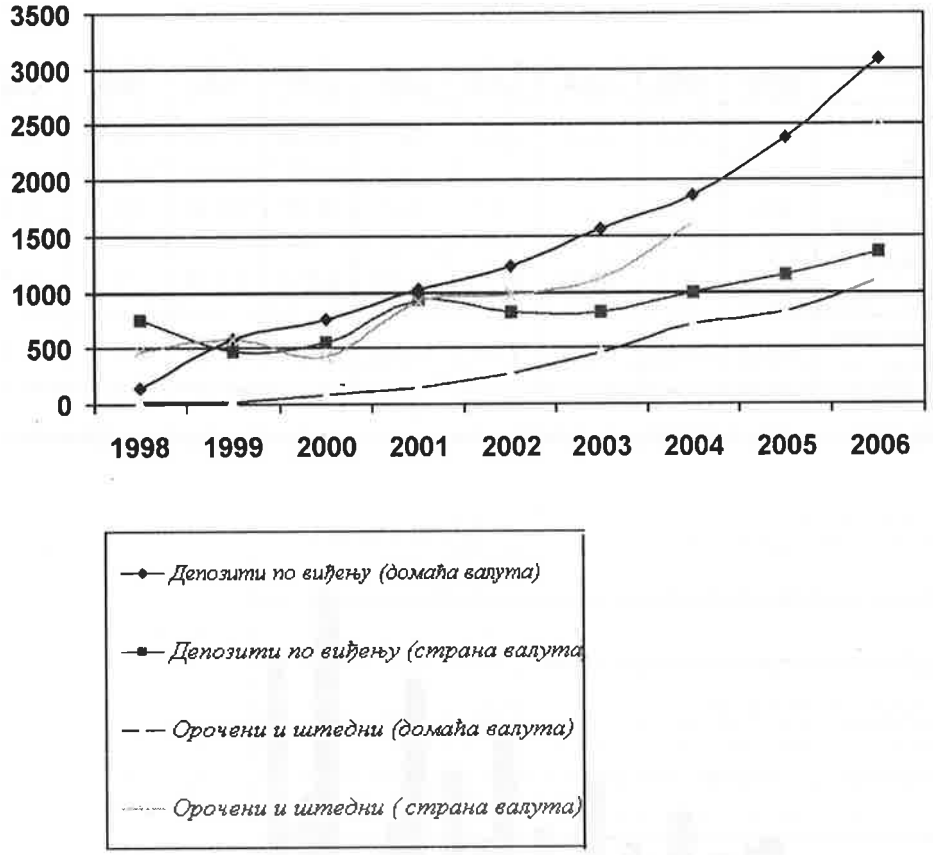
***Табела 4 Процентуално учешће посматраних депозита у укупним депозитима по годинама***




***Графикон 1 Депозити у домаћој и страној валути у периоду 1998 – 2006. година***

| ГОДИНА | 1998. | 1999. | 2000. | 2001. | 2002. | 2003. | 2004. | 2005. | 2006. |
|---|---|---|---|---|---|---|---|---|---|
| Валутна супституција | 79,43 | 48,15 | 39,99 | 39,27 | 35,4 | 34,91 | 38,3 | 39 | 38,8 |

***Табела 5 Валутна супситуција у периоду 1998 – 2006. године***




***Графикон 2. Депозити у домаћој и страној валути у периоду 1998 – 2006. године***

Као што се може примијетити, што се тиче депозита по виђењу од 1998. до 2006. године они показују константан раст, што се може објаснити чињеницом да су се у све већем броју почели користити текући и жиро рачун банака у функцији платног промета, у односу на пријашњу Службу друштвеног књиговодства ( СДК).

Међутим, да бисмо објаснили и пратили појаву и утицај валутне супституције, обратићемо пажњу на кретање депозита по виђењу у страној валути и орочених и штедних депозита у домаћој и страној валути.

Што се тиче депозита по виђењу у страној валути у 1998. године они су износили 467 милиона КМ и до 2006. године забиљежили су раст и износе 2.544,4 милиона КМ. Међутим, оно што је посебно битно јесте однос орочених и штедних депозита у домаћој и страној валути у току посматраног периода. У 1998. години орочени и штедни депозити у домаћој валути су износили 8 мил. И од тада константно расту, па тако у 2006. години они су износили 1.098,8 мил. КМ.

Оно што се може закључити на основу презентованих података јесте да грађани и даље више штеде у страној валути, мада и штедња у домаћој валути није занемарљива. Пораст штедње у домаћој валути се видно поправио у посматраним годинама, што говори у прилог чињеници да домаћи резиденти све више имају повјерења у монетарне власти и домаћу валуту.

Прва функција која је на удару при појави валутне супституције је функција новца као чувања вриједности, затим функција обрачунског средства и на крају и функција новца као трансакционог средства.

### 2. Вођење монетарне политике

Појава валутне супституције у некој земљи утиче и на монетарну политику, односно, онемогућава монетарним властима да је спроведе и да се покажу ефекти које она може да има. У нормалним условима, односно, у привреди гдје не постоји валутна супституција, тражња за домаћим новцем зависи од каматне стопе. Ако је каматна стопа висока, тражња за новцем опада јер становништво и привреда не желе да имају готов новац који не доноси профит, за разлику од ороченог новца, на који иде камата. Супротан ефекат се добија ако је каматна стопа ниска.

При валутној супституцији, поред каматне стопе, на тражњу за новцем утичу и очекивања у погледу промјене девизног курса.

Ако се очекује да ће девизни курс стране валуте порасти, односно апресирати, онда тржња за домаћом валутом опада. На тражњу за домаћом валутом утиче и стопа њене девалвације. Ако домаћа валута девалвира у мањем проценту, онда ће и тражња за страном валутом бити мања, док у супротном, све воше домаћих резидената ће да тражи страну валуту.

У овим случајевима долази до повећања ризика ликвидности централне банке. Уколико банка жели да води рестриктивну монетарну политику, она ће утицати на смањење количине домаће валуте, а предузећа и становништво ће претварати страна средства плаћања у домаћи новац, па монетарна политика неће имати ефекта.

Исто тако, када монетарне власти у земљи А повећавају домаћу понуду, стопа инфлације се повећава а валута депресира, што ће утицати на повећање тражње за валутом земље Б. Ако земља Б води политику одржавања таргетираног монетарног раста, то значи да ће бити више каматне стопе у земљи Б него што би биле да нема валутне супституције, али ако се води политика везивања домаће каматне стопе то ће повећати понуду новца. Тако у условима валутне супституције акције политике у земљи А води ка сличној акцији у земљи Б чак и у условима флексибилних девизиних курсева, односно, монетарне власти не могу водити независну монетарну политику.

### 3. Девизни курс

Девизни курс је нестабилнији у условима валутне супституције и тада утиче на промјене домаћих цијена. У тим условима, централна банка нема много утицаја на формирање девизног курса па је он под утицајем различитих шпекулативних фактора који га чине несатбилним али и неодређеним.

Што се тиче БиХ, Централна банка функционише у режуму валутног одбора (currency board), па је установљен фиксан девизни курс конвертибилне марке ( КМ) у односу на евро ( € )

1КМ = 0,51 ЕВРО

### 4. Преваљивање ефеката валутне супституције

Појава и ниво валутне супституције је под директним утицајем инфлације, која се код земаља у развоју често јавља као резултат буџетског дефицита.

Самим тим новац губи своју куповну моћ што, у ствари, представља инфлациони порез којег имаоци новца плаћају држави, а валутном супституцијом настоје да избјегну плаћање овога пореза. У оваквој ситуацији, преваљивање ефеката валутне супституције настаје због већих могућности богатијег слоја становништва да изврше валутну

супституцију, односно, да домаћи новац замијене страном валутом, од сиромашнијег слоја, па самим тим они сносе већи терет плаћања инфлационог пореза. [5]

## III ЕЛИМИНАЦИЈА ВАЛУТНЕ СУПСТИТУЦИЈЕ

Супституција домаће валуте страном може да има и неке позитивне ефкете као што су усмјеравање токова капитала, повећање девизних резерви земље и смањење ризика диверзификацијом портфолија. Међутим, без обзира на ове позитивне ефекте, свака земља и њена монетарна власт жели да има јаку и стабилну домаћу валуту. У већини земаља у развоју то је много теже постићи него у развијеним земљама, из више разлога, од којих су само неки: макроекономска равнотежа и слаба привреда и неразвијеност, ратови, слаба државна управа и сл, тако да је већина земаља у развоју суочена са проблемом валутне супституције. Њени грађани не желе да чекају када ће се инфлација смирити, или када ће се покренути привредна производња. Чим се појаве било какве назнаке да би домаћа валута могла изгубити куповну моћ, односно, ако сте стопа инфлације у земљи повећа, они ће настојати да своју валуту замијене страном, било у трансакцијама, или као средство чувања вриједности.

Међутим, валутна супституција као појава коришћења стране валуте у неким фукцијама које би требало да обавља домаћа валута је често само резултат макроекономске равнотеже, односно појаве фискалног дефицита и већих стопа инфлације, а није узрок таквог стања.

Неке земље Латинске Америке ( Бразил, Чиле, Колумбија) су увеле одређене вјештачке мјере против доларизације као што су индексирани финансијски инструменти, присиљавање на конверзију стране у домаћу валуту и слично[6]. Овим мјерама се настојала спријечити валутна супституција, али се не може утицати на срж проблема, односно отклонити они фактори који су и довели до појаве валутне супституције. Све док постоји висок ниво инфлације, али и висок ризик од могућег повећања стопе инфлације, домаћи резиденти ће више тражити страну него домаћу.

Да би се валутна супституција елиминисала, потребно је утицати на проблеме који су довели до њене појаве, да би се на дуги рок повећала сигурност у домаћу валуту и спријечило њено поновно јављање.

***Слабе државне институције и повјерење у државни апарат*** један су од разлога за постојање валутне супституције и смањење стопе инфлације. Домаћи резиденти ће држати страну валуту све док се не поврати повјерење у државу и монетарне власти.

Земље у развоју су се дуго времена бориле са инфлациојом, која је била резултат повећања новчане масе од стране централне банке, а ради финансирања јавног дуга. Стабилизациојом инфлације ситуација се поправила, али се није вратило повјерење у државу, па се страна влата задржала у неким функцијама новца. И све док резиденти немају повјерења у државу и док су очекивања у погледу промјене стопе инфлације велика, до тада ће се валутна супституција задржати у већини земаља у транзицији. Оно што је потребно урадити јесте ојачати привреду и успоставити стабилну монетарну политику, која неће финансирати државу путем повећања новчане масе, што би само довело до повећања инфлације и до све веће појаве валутне супституције.

---

[5] Др Ново Плакаловић, Монетарна економија – Теорија, и нституције и политика, Завод за уџбенике и наставна средства Српско сарајево, 2004. год.

[6] Financial dollarization in Latin America, R. Rennhack, M.Nozaki, IMF workig paper, 06/7, 2006.

## РЕЗИМЕ

Као што се може примијетити, валутна супституција је карактеристична за земље са високим стопама инфлације и недовољно развијеном привредом. Основни фактор који утиче на ниво валутне супституције је, прије свега, ниво реалне имовине, који представља њену горњу границу, а ту су , даље, и институционални фактори, односно могућност држања различитих облика имовине ( реалне активе и хартије од вриједности) те развијеност и дубина финансијског тржишта. С обзиром да је валутна супституција у директној вези са инфлацијом, у ове факторе спада и разлика између каматних стопа на валуте у односу на инфлацију, гдје се, наравно, узима она валута која има позитивну релану каматну стопу. Међутим, оно што је најбитније код питања валутне супституције јесте могућност њене елиминације. Као што је и у раду споменуто, неке земље су се користиле вјештачким мјерама елиминације (индексирани финасијски инструменти, присиљавање на конверзију у домаћу валуту и сл), гдје се није утицало на отклањање проблема због којих је и дошло до појаве валутне супституције, већ су се настојали смањати њени појавни облици, што није препоручљиво ни за једну земљу која жели на дуги рок повећати сигурност у домаћу валуту и спијечити њену поновну супституцију.

### ЛИТЕРАТУРА:

1. Билтен Централне банке БиХ, 2004. и 2006. година
2. G.D.Nicolo, P.Honohan, A. Ize, *Dollarization of The Banking sistemy: Good or Bad?,* IMF working paper 03/146, July 2003.
3. R. Rennhac, M.Nozaki, *Financial Dollarization in Latin Amerika*, IMF working paper 06/7. 2004.
4. др Ново Плакаловић, *Монетарна економија – Теорија, институције и политика*, Завод за уџбенике и наставна средства С. Сарајево, 2004. год.
5. др Александар Живковић, др Градимир Кожетинац, *Монетарна економија*, Економски факултет Београд, 2005. год.