ЗБОРНИК НА ТРУДОВИ

Втора меѓународна научна конференција
„Влијанието на научно – технолошкиот развиток во
областа на правото, економијата, културата,
образованието и безбедноста во
Република Македонија“

Скопје 30-31 октомври 2014

ЗБОРНИК НА ТРУДОВИ: Втора меѓународна научна конференција
„Влијанието на научно – технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија“

Организатор: Институт за дигитална форензика
Универзитет „Евро-Балкан“ - Скопје

Уредник: Проф.д-р Сашо Гелев

Издавач: Универзитет „ЕВРО-БАЛКАН“ Скопје
Република Македонија
www.euba.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

001.3:330/378(497.7)(062)

МЕЃУНАРОДНА научна конференција (2 ; 2014 ; Скопје)
Влијанието на научно-технолошкиот развиток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија : зборник на трудови / Втора меѓународна научна конференција, Скопје 30-31 октомври, 2014 ; [уредник Сашо Гелев]. - Скопје : Универзитет "Евро-Балкан", 2014. - 575 стр. : илустр. ; 24см

Дел од трудовите на англиски јазик. - Библиографија кон трудовите

ISBN 978-608-4714-11-8

а) Научен развиток - Општествени науки - Македонија - Собири
COBISS.MK-ID 97406218

Програмски одбор

- **Проф. Д-р Митко Панов, Универзитет Евро Балкан - Претседател**
- **проф. Д-р Сашо Гелев – Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија копретседател**
- **проф. Д-р Павлина Стојанова, Универзитет Евро Балкан копретседател**
- **Проф. Влатко Чингоски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија**
- **Проф. Д-р Божо Крстајиќ, Електротехнички факултет - Подгорица, Црна Гора**
- **Доц. д-р Роман Голубовски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија**
- **Проф. Д-р Аристотел Тентов, Факултет за електротехника и информациски технологии, Универзитет Св. Кирил и Методиј – Скопје, Република Македонија**
- **Доц. Д-р Марија Календар, Факултет за електротехника и информациски технологии, Универзитет Св. Кирил и Методиј – Скопје, Република Македонија**
- **Доц. Д- Атанас Козарев, Европски универзитет Република Македонија- Скопје**
- **Проф. Д-р Атанас Илиев, Факултет за електротехника и информациски технологии, Универзитет Св. Кирил и Методиј – Скопје, Република Македонија**
- **Проф. Д-р Тони Стојановски, Австралија**
- **Д-р Зоран Нарашанов, Винер осигурување, Скопје, Република Македонија**
- **Проф. д-р Лада Садиковиќ, Факултет за криминалистика, криминологија и безбедност, Универзитет во Сараево;**
- **Проф. д-р Здравко Скакавац, Факултет за правне и пословне студије, Универзитет УССЕ, Нови Сад;**
- **Доц. д-р Марјан Николовски, Факултет за безбедност,**

Универзитет Св. Климент Охридски, Битола, Република Македонија
➢ **Проф. д-р Гордан Калајџиев, Правен факултет, Универзитет Св. Кирил и Методиј – Скопје, Република Македонија**
➢ **Д-р Никола Протрка, Полициска академија, Загреб, Република Хрватска**
➢ **Проф. Д-р Стефан Сименов, Академија за внатрешни работи на Република Бугарија**
➢ **Доц. Д-р Оџаков Фердинанд, Министерство за одбрана на Република Македонија**
➢ **Доц. д-р Лидија Раичевиќ, Основно јавно обвинителство за борба против организиран криминал**

Организацискиодбор

- **Проф. д-р Сашо Гелев, претседател**
- **Проф. д-р Павлина Стојанова, член**
- **Доц. Д-р Мимоза Клековска, член**
- **Доц. Д-р Снежана Черепналковска-Дуковска, член**
- **Доц. д-р Александар Даштевски, член**
- **Доц. д-р Вангел Ноневски, член**
- **Доц. д-р Јорданка Галева, член**
- **М-р Игор Панев, член**
- **М-р Маријана Хрисафов, член**
- **Зорица Каевиќ, член**

П Р Е Д Г О В О Р

Конференцијата се организира да се согледа влијанието на научно - технолошкиот развоток во областа на правото, економијата, културата, образованието и безбедноста во Република Македонија.

Минатата година за прв пат ја организиравме оваа конференција со цел студентите од вториот и третиот циклус на студии да се оспособат за пишување и презентирање научно-стручни трудови, а останатите учесници да ги пренесат своите најнови истражувања во посочените области.

Втората конференција во однос на првата по бројот на презентирани трудови беше поспешна. Презентирани беа повеќе од 60 труда.

За следната конференција ќе се потрудиме најдобрите трудови покрај тоа што ќе излезат во зборникот на трудови од конференцијата, да ги издадеме и во наше списание со интенција тоа да прерасне во меѓународно списание.

Проф. Д-р Сашо Гелев

СОДРЖИНА

удк: 621.395.721.5:004.738.5.056.55

м-р Александар Соколовски
Неотел
д-р Сашо Гелев
Универзитет "Гоце Делчев" - Штип
Електротехнички факултет - Радовиш
Република Македонија

Мобилна автентификација на корисници со модерни криптографски методи

Абстракт
Овој труд ги истражува методите на критпографија и силна автентификација кај корисниците на мобилните телефони, што во денешно време станува еден од главните предизвници со оглет на зголемување на бројот на интернет овозможените мобилните телефони и зголемената употреба за секојдневни активности и мобилни е-плаќања.Примарните цели (objective) е да се истражи и верифицира дали користењето на модерни начини на автентификација на мобилни корисници со користење на модерни криптографски методи како на пример: Силна автентификација (Strong Authentication), мобилна автентификација, НФЦ (Near Feld Communiucaton), ОБЦ (On-Board Credentials), СМС-ОТП (SMS – One Time Password), ќе ја зголеми безбедноста на мобилните телефони.Главна цел е да се одредни најдобрата комбинација на криптографски алатки за зголемента безбедност на афтентификација на корисниците на мобилните телефони. Ова ќе биде постигнато со тестирање на критпографските методи и предлог протоколи со користење на NS-3 мрежниот симулатор.Добиените резултати и донесените заклучоци од анализата можат да послужат како водич за креирање на следната подобра генерација на интернет овозможени мобилни телефони.

Клучни зборови:
Силна автентификација , мобилна автентификација, НФЦ, ОБЦ, СМС-ОТП.

Abstract:
This paper attempts to investigate the methods of cryptography and strong authentication of mobile phones, that is nowadays one of the main challenges having into account the increased number of internet enabled mobile phones and the increased usage of the eveveryday activities in the scope of mobile e-payments.The primary objective is to investigate and verify if the usage of modern authentication of mobile users with the use of modern methods of cryptography like: Strong Authentication, Mobile Authentication, NFC (NearFeldCommuniucaton), OBC (On-Board Credentials), SMS-OTP (SMS - One Time Password), will increase the security of the mobile phones. The main aim is to determine the best compbiation of cryptography tools to achive increased security over the authenification of the mobile phones users. This will

be achieved with testing the cryptography methods and the proposed protocols for usage, using the NS-3 Network Simulator.The results and conclusuons of the analyses may serve as a guide for using the improved next generation of internet enabled mobile phones.

Keywords:
Strong Authentication, Mobile Authentication, NFC (NearFeldCommuniucaton), OBC (On-Board Credentials), SMS-OTP (SMS - One Time Password).

1. Вовед (сложената автентификација – *strong authentication)*

Денес бизнисот се работи највеќе преку Интернет: Банкарски Трансакции, Шопинг инт. Онлине шопингот се повеќе е во пораст, дури и набавката на секојдневни работи како набавка на храна се одвива онлине, преку интернет сервиси кои нудат достава до дома. Поради долгите редици за чекање во Банките се повеќе луѓе во денешно време се одлучуваат за електронско банкарство како побрзо и поефикасно решение но истото иницира дополнилни предизвици. Едно од главните предизвици со Електронстово банкрaство и сите други онлине сервиси кои бараат доверливост на податоците и информациите, бараат зголемена безбедност на трасферот на податокот, тоа се постигнува со зголемено ниво на автентификација. Сложената автентификација е поради заштита на давателот на услугата / провајдерот и за корисникот. Постојат три основни типа на автентификација:

- Првиот и најчестиот тип на автентификација е “според нешто што некој знае”, т.е. постои збор (зборот се врзува со името на корисникот / корисничко име) кој го знае корисникот и збор кој го знае и Провајдерот, тој “збор” може да е шифра / пин код.
- Втор тип на автентификација е “според нешто што некој има” смарт картичка (корисникот има смарт картичка, Провајдерот има начин како според смарт картичката да идентификува дали се работи за автентифициран корисник и за кој точно корисник се работи и секако корисникот каде се има право на пристап).
- Трет начин на идентификација е “според тоа што некој е”, ова се најчесто биометриски начини на идентификација на корисници (преку отисок од прски или скен од ретина од око, дури и ДНК). Овој е најбезбеден начин, но и најсложен за имплементација.

Официјално не постои дефиниција за терминот сложената автентификација, но “неофицијално” во пракса и во најголемиот дел од литературата окулу автентификација во делот на криптографија, под строга автентификација се милси на автентификација која користи 2 од 3 методи за автентификација. Наједноставен пример за сложена автентификација е користењето на кредитната картичка на ATM банкомат. Корисникот се идентификува “според нешто што некој има” кредитна картичка и според “нешто што некој знае” тоа е пин кодот. (Ова е сложена автентификација со комбинација на вториот и првиот тип на автентификација). TUPAS е познат систем за онлине идентификација на клиенти, примарно користен од Банките во Финска / Норвешка / Данска / Шведска, веќе прифатен во најголемиот дел од Банките во цел свет. На пример сценариото за TUPAS се одвива на следниот начин: корисникот се логира на порталот сака да промени на пример вредност за дневен лимит за интернет плаќања, банката генерира еднократен КОД од букви и бројки за едно користење (временски лимитиран од неколку часа до еден ден). КОДОТ банката го праќа преку безбедносно препорачано писмо или нивен курир кој треба истиот да го достави кодот до клиентот во најбрзо можен рок (неколку часа , најмногу еден ден), корисникот по добивање на кодот го користи кодот за да ја направи промената и потоа веќе кодот е навелиден. Во последните неколку години TUPAS КОДОТ наместо преку курир се доставува и преку СМС.

Во овој труд правиме истражуваме на различните на методи на автентификација кои можат да се користат со цел да се постигне слично ниво на силна автентификација на тоа со TUPAS. Фокусот на истражување на овој труд е анализа на различните предложени методи и нивна споредба, од аспект на користење на сервисните провајдери како и крајните корисници. Се споредуваат тежината за имплементација, цената, самата имплементација како и корисноста.

Целта на новите системи мора да биде да бидат поефикасни, поефтини, полесни за имплементација, како и полесни за користење (usability) од нивните предходници, со цел да можат да биде прифатени до сервисните провајдери и на крај од крајните корисници.

2.автентификација базирана на сим картичката

Еден валиден пристап кај автентификација на крајните корисници кај мобилните телефони е со користење на СИМ картичка (SIM - Subscriber Identity Module) секоја СИМ картичка содржи ИМСИ (IMSI - International Mobile Subscriber Identity) со кој се идентификува картичката во рамки на глобалните мрежи. ИМСИ е всушност 15 карактерен код со кој мобилните мрежи го идентификуваат претплатникот (дури и во рамки на поврзување на не-домашна мрежа или во рамки на роаминг). Заштита на СИМ картичките постои од страна на сервисниот провајдер, во овој случај мобилниот провајдер, кој не дозволува поврзување на клонирани СИМ картички, бидејќи ако картичката е клонирана мора да се клонира и ИМСИ кодот, мрежите не дозволуваат поврзување на два исти ИМСИ кода во иста мобилна мрежа. Некои обиди се правени мобилните мрежи да го поврзуваат ИМСИ кодот на сим картичката со ИМЕИ (IMEI - **International Mobile Station Equipment Identity**) кодот на телефонот, со цел во случај на клонирана картичка оригинална картичка да не биде блокирана туку само клон картичката (дури да успее некој да ја клонира картичката, ИМЕИ кодот од телефонот е речиси невозможно да се клонира). Последнава фукнционалност не е имплементира и целосно прифатена од сите мобилни провајдери во светот.

Заштита на СИМ картичките постои и од аспект на корисникот, при секое вклучување на телефонот и пред да се активира СИМ картичката мора да се внесе четири цифрен ПИН код (ако пин кодот се згреши повеќе од 10 пати картичката се блокира и истота може да биде одблокирана од страна на сопственикот ако го знае PUK (Pin Unlock Key) или од страна на мобилниот провајдер. Пробивања на СИМ картичките во раните фази се познати во ситуации кога корисникот не го менувал основниот ПИН и го оставал ПИН-от на 0000, поради тоа мобилните провајдери дефинираат нивен ПИН која може да се промени (во поновите СИМ картички се забранува последователните карактери да се повторуваа во еден ПИН). Последнава фукнционалност не е имплементира и целосно прифатена од сите мобилни провајдери во светот.

2.1. SMS-OTP (One time password using SMS)

СМС-ОТП методата е праќање на шифра / пин код за автентификација со цел за една употреба.
Ова често се користи за најава на корисници на некој портал, најава на cloud сервис (Dropbox, iCloud, OneDrive итн.). Банките исто така го практикуваат за правење на промена на одредени параметри без одење физички до банката, на пример промена на дневен лимит за интернет плаќања. Корисникот се најавауува на порталот на банката, ја одбира промената новата вредност за дневен лимит за интернет плаќања, истото барање го “потпишува” (го потврдува идентитетот) со внесување на сајтот на СМС-ОТП кодот кој корисникот го добива на СМС.(TUPAS преку СМС).

Користење
Сервисниот провајдер може да испраќа СМС пораки до корисникот само доколку има база со која може да ги идентификува корисниците според телефонскиот број. Телефонскиот број на мобилен телефон е задолжително барање кога корисникот се пријавува за тој сервис во банката. Првата фаза на идентификација се случува со внесување на стандардни кредицијали (credentials) како пар од

корисничко име и шифра. Со тие стандардни кредицијали сервисниот провајдер го препознава корисникот генерира ОТП (OTP-OneTimePassword) код кој го праќа преку СМС порака до корисникот (СМС-ОТП). Корисникот го внесува ОТП кодот за потребата за која му треба и со тоа се добива силна автентификација, со помош на СМС или попозната како СМС-ОТП.Ова не е единствен начин СМС да се користи за автентификација. На пример Нордеа банка од Финска (со експозитури во Новрешка, Шведска и Данска) користи СМС пораки за конфиркација / потврда на "сомнителни" трансакции и бара од корисникот потврда преку СМС дека истата трансакција на направил тој. На пример вадењето на пари од АТМ банкомат нема да биде процесирано се додека корисникот не врати преку СМС Y или N. Y за да, N за не, корисникот треба да врати ДА Y, со цел да се процесира трансакцијата, во случај корисникот да не врати ништо одреден временски период (10-15 минути), системот автоматски испраќа N не одговор и се известува банкарскиот службеник да го контактира клиентот телефонски, во случај ако е картичката укредена истата да биде блокирана. Сервисните провајдери на пример банките кои сакаат да користат СМС-ОТП автентификација можат тоа да го прават преку нивни СМС gateway или да користат опрема од некој од телеком операторите, банките најчесто поради безбедност имаат нивна опрема. Решение за СМС-ОТП нуди TeleSign (TeleSign's Two-Factor Authentication).TeleSign нудат и постава на ОТП кодот преку аудио или видео повик, видеото е во бета фаза.

Предности

СМС-ОТП автентификација има многу предности: покриеност и достапност до корисниците, едноставно користење. Најголем дел од луѓето во целиот свет поседуваат мобилен телефон без разлика дали се работи за паметен телефон (smartphone) или телефон од генерација 1 или 2, сите мобилни телефони имаат сим картичка и имаат можност за примање и испраќање СМС пораки. Од аспект на едноставноста за користење на СМС-ОТП, овој начин на автентификација не бара дополнителна инсталација на софтвер на мобилниот телефон или користење на дополнителен уред и не бара обука на корисникот за нејзино користење, обична СМС порака е.

Со ова СМС-ОТП како метода го покрива секој корисник со мобилен телефон, без дополнителна потреба од нов хардвер или софтвер или без потреба од дополнителна обука на корисникот.

Цената

цената за имплементација на СМС-ОТП сервисот од аспект на сервисниот провајдер е ниска споредено со другите начини на автентификација, во поглед на инфраструктурите трошоци (најчесто е доволно најниска класа на сервери, доволен е и еден сервер каде може се да биде). Праќањето на СМС пораките е ниска споредено со другите начини на автентификација. Цената за имплементација на СМС-ОТП од аспект на корисникот е еднавна на нула (нема ништо плус).

Проблеми

Проблемите најчесто се повеќе од кориснички аспект: губење на мобилен телефон и ненавремено пријавување (злоупотреба на украдениот телефон), блокирана СИМ картичка ненавреме пријавена (напаѓач ја користи клонирана СИМ картичка). Постари телефони кои не подржуваат интернет сообраќај и немаат можност за подршка на интернет прегледник, па корисникот користи втор уред за најава компјутер лаптоп таблет итн, во меѓу време кодот од пораката го запишува на лист (со лист од 5-10 последователни кодови може да се погоди следниот код), последното е ретка појава но се има сличувано.Проблеми се појавуваат и од аспект на сервисниот провајдер, СМС пораките се испраќаат до корисникот преку одредена мобилна мрежа на со еден мобилен провајдер (најчесто банките имаат посебен СМС gateway за секој мобилен оператор посебно), но кога се работи за роаминг СМС-ОТП автентификација во тој случај бројот на мобилни оператори е повеќе од еден и со тоа се зголемува можноста за напад од трета страна која може да ја пресретне СМС пораката.

2.2. Мобилен Сертификат

Мобилниот сертификат е дополнителен сервис на претплатниците на мобилните телефони.

Оваа услуга не е бесплатна ниту за сервисниот провајдер ниту за корисникот. Овој тип на автентификација е базиран на принципот на ПКИ - Криптирање со јавен Клуч (PKI – Public Key Infrastructure) и клучевите и сертификатите се зачувани во СИМ картичката на корисникот. Мобилниот сертификат содржи уникатен персонален идентификатор, на пример ЕМБР или

перманентни лични податоци како: датум на раѓање, пол, пационалност. Мобилниот оператор служи како ПКИ-ЦА Авторитет за сертификатот (PKI CA – Certification Authorities).
Постои и мобилен сертификат кои се користи преку апликација и истиот е сместен во апликацијата наместо во СИМ картичката, се друго и исто користењето и автентификацијата.

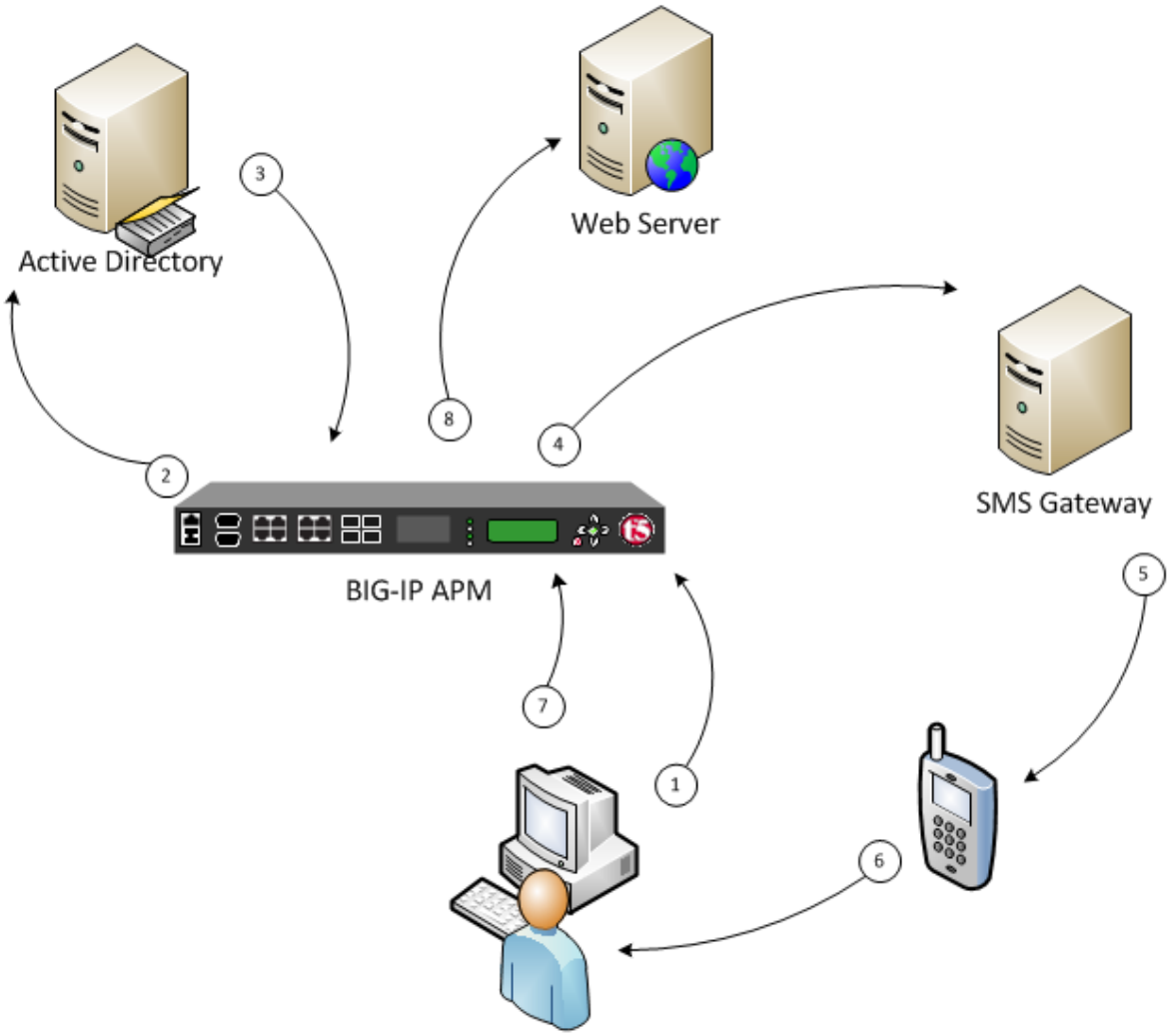
Користење
Автентификација со мобилен сертификат се одвива на многу сличен начин како и СММ-ОТП автентификацијата.
Начинот на автентификација е следниот. Прво корисникот се автентицира со комбинација на корисничко име побрзано со соодветна шифра, ако е ова успешно Сервир Провајдерот потоа бара од ПКИ-ЦА (во случајот мобилниот оператор на корисникот) бара да се направи автентикација преку мобилен сертификат. Тоа се одвива на следниот начин: По добието барање од Сервисниот провајдер за идентификација со мобилен сертификат, ПКИ-ЦА-то праќа challenge до мобилниот телефон од телефонскиот број од кој истото е иницирано. Корисникот го внесуваСПИН-от за идентификација кој го отклучува приватниот клуч зачуван во СИМ картичката. Challenge е потпишан со употреба на приватниот клуч на корисникот и истиот е вратен назад до ПКИ-ЦА-то. По примањето на challenge назат ПКИ-ЦА-то или мобилниот провајдер може да провери дали challenge е потпишан со точниот сертификат или не.
Мобилниот провајдер го има јавниот клуч на корисникот и со користење на јавниот клуч го декриптира challenge и ако challenge има иста содржина со пратениот до мобилниот корисник, тогаш корисникот е успешно идентификувам и мобилниот операторот во оваа ситуација ПКИ-ЦА-тоиспраќа пораката до сервисниот провајдер дека корисникот е успешно идентификуван и истиот може да продолжи со своите активности на порталот или интернет страната која ја посетува.

Мобилните сертификати исто така може да се користата за автентификација на корисниците за време на телефонски повик. Исто така многу честа ситуација е користење на друг втор уред (компјутер или лаптоп) за најава на сервисниот провајдер, со користење на идентификација на корисникот преку мобилниот сертификат. Сценариото е идентично како и погоре објаснето, разлика е што корисничкото име и шифра за иницијална најава и по целосно успешната автеникација корисникот користи друг уред за интернет не мобилниот.

Предности
Како што спомнавме предходно сервиси поврзани со автентификација преку СИМ картички е едноставна. Исто се однесува и на автентификацијата со користење на мобилен сертификат. Корисникот се што треба да направи е да побара нова СИМ картичка од операторот која подржува мобилен сертификат и да си генерира (внесе иницијално СПИН кодза користење на мобилниот сертификат) или да се инсталира соодветна апликација на мобилниот телефон без промена на СИМ картичката. Во голем дел од државите во ЕУ мобилниот сертификат со апликација е прифатлив начин на идентификација на корисните од БАНКИТЕ, некои го користат паралелно со TUPAS системот. Користењето на идентификација со мобилен сертификат е одличен начин корисничките подршки на банките да ги идентификуваат своите корисници (без тие да мора на глас да ги кажуваат своите лични податоци како ЕМБР). Мобилните сертификати преку апликација немаат гласовна подршка но работат на идентификација на корисниците преку отисок од прст (моментално во тест фаза и подржано од мал број фирми).Оваа технологија сеуште официјално не е прифатено од банките и мобилните оператори, но голем дел од нив прават тестови за корсиње и начин како да се имплементира. Слика бр.1

Проблеми
Како што спомнавме погоре, мобилните сертификати не се бесплатни ниту за корисниците ниту за сервисните провајдери, овој тип на сервис сеуште е во рана фаза за да може точно да се прецизира цена поради многу малата застапеност споредено со СМС-ОТП но целата секако ќе биде повисока бидејќи се потребни најмалку 1-2 сервери и кај мобилниот оператор и кај сервисниот провајдер (цената може да се намали со виртуелизација, но секогаш проблемите кои може да се јават кога има комуникација помеѓу 2-4 сервери кај две различни компании – мобилниот оператор и сервисниот провајдер, тоа сепак останува). Дополнително одржување и развирање на апликација на серверската страна и развој на соодветна апликација за клиентот (тука ако се земе предвид дека не постои само

еден мобилен оперативен систем и само еден серверски оперативен систем, потенцијалот за проблеми секако е во пораст).
Проблемите со користење се зголемуваат ако се користи апликација за идентификација на корисникот, ако е мобилен сертификат истата апликација мора да помине безбедности тестови. Ако се работи за биометриска идентификација како отисок од прист или ако се чуваат било какви други лични податоци, мора да постојат соодветни механизми и кај мобилниот оператор и кај сервисниот провајдер за заштита на идентитот на корисниците. Сите овие правила и процедури мора да бидат во склоп со законите за заштита на лични податоци на соодветната држава како и ИСО стандарите за безбедност за заштита на информации 2700. Сеуште отворено прашање останува за земјите кои не се членки во ЕУ, ако корисникот прави биометриска идентификација или идентификација со користење лични податоци во рамки на роаминг мрежа каде се разликуваат законите за заштите на личните податоци помеѓу двете држави. Најголем дел од државите имаат слични закони со ЕУ за тоа, но не сите држави.



Слика бр.1

3. НФЦ (NFC – Near Field Communication)

НФЦ (NFC – Near Field Communication) е безжична комуникациска технологија која работи на кратки растојанија, која е базирана на RFID (Radio Frequency Identification) технологијата. НФЦ технологијата почна да се применува во тест фази од 2005 година прво од VODAFONE, потоа NOKIA

со моделот С7.Мобилните телефони со НФЦ отвораат многу интересни можности. Такви уреди може да се употребат во иднина да ги заменат физичките клучеви и бонус картички, како и најважно кредитните картички. Најинтересниот аспект од НФЦ автентификацијата е тоа што мобилниот телефон може да се користи во замена на кредитна картична итн, но исто така може да се користи како РФИД читач за новиот тип на кредитни картички (така наречените contactless credit cards кои имаат РФИД код секако).

Користење

Можноста мобилниот телефон да се користи како смарт карт читач исто така отвара можност да се користи мобилниот телефон со НФЦ како автентификациски метод при најава на портал за електроско банкарство.

- Прво корисникот ја посетува страната за електорско банкарство и по внесување на корисничкото име и шифра и по успешната најава, корисникот добива challenge на неговиот мобилен телефон.
- Корисникот ја чита картичката со допирање на картичката на крајниот дел од телефон
- НФЦ-то може да се користи за повеќе финкции корисниот од апликацијата одбира дека прави идентификација / внесување на картичка.
- Потоа challenge започнува кој корисниот го добива од банката.
- Корисниот го внесува ПИНОТ на картичката (можно е да треба прво да се внесе СПИН при стартурвање на апликацијата ако се прави криптирање на сообраќајот со мобилен сертификат).
- Ако ПИНОТ на картичката е успешно внесе се продолжува понатаму, банката испраќа КОД на мобилниот на корисникот, тој код корисникот го користи за да продложи со работа на порталот за електронско банкарство.

Предности

Главната идеја за НФЦ не е идентификацијата, тоа е една од работите за која се користи НФЦ. НФЦ е одлично решение бидејќи може да се користи за многу работу, поради тоа има големи шанси да успее како нова технологија и да биде прифатена од корисниците и сервис провајдерите.

Проблеми

НФЦ како и секоја друга нова технологија има проблеми, во моментов три се најбележителни:

- Корисноста (usability) аспектот е на многу ниско ниво споредено со мобилните сертификати, како и СМС-ОТП технологиите. Корисниците без упатство не би се снашле, исто така постарите генерации кои не се навикнати на паметните телефони тешко дека ќе го прифатат овој начин за автентикација.
- Втор проблем е достапноста, многу мал број на модели на мобилни телефони подржуваат НФЦ технологија, тие што подржуваат се најчесто најскапите телефоните кај сите производите, пред НФЦ биде достапна како Wifi на сите телефони ќе помине време.
- Трет проблем е безбедноста на информациите кога се работи за RFID уреди, ова е отворена тема и ќе помине многу врем додека се разрешат сите проблеми окулу тоа.

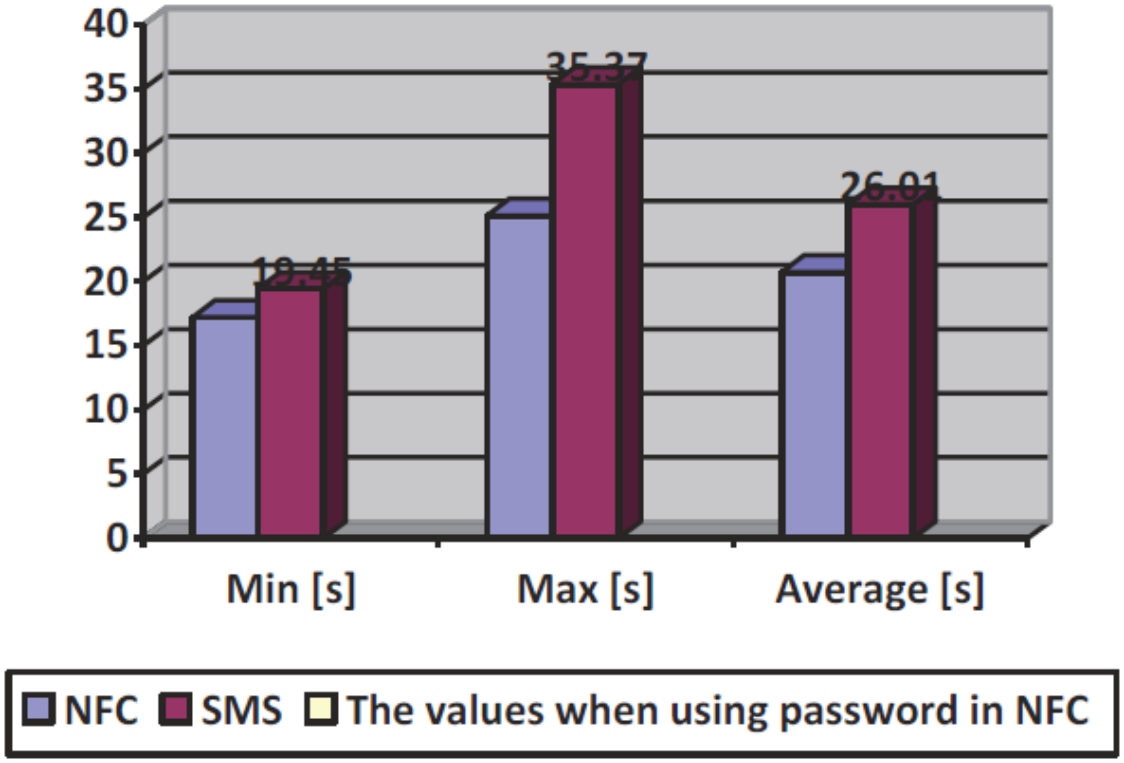
Од експериментот направен на СМС (СМС-ОТП / Мобилен сертификат) и НФЦ онлине трансакции, со и без користење на шифра, со користење на шифра, автентификацијата при користење на шифра е минимално подобра од СМС (СМС-ОПТ / Мобилен сертификат), но кога не се користи шифра НФЦ афтентификациајата е многу пати побрза од СМС (СМС-ОПТ / Мобилен сертификат). Ова е прикажано на сликите Слика Бр.2 и Бр.3

4. Споредба

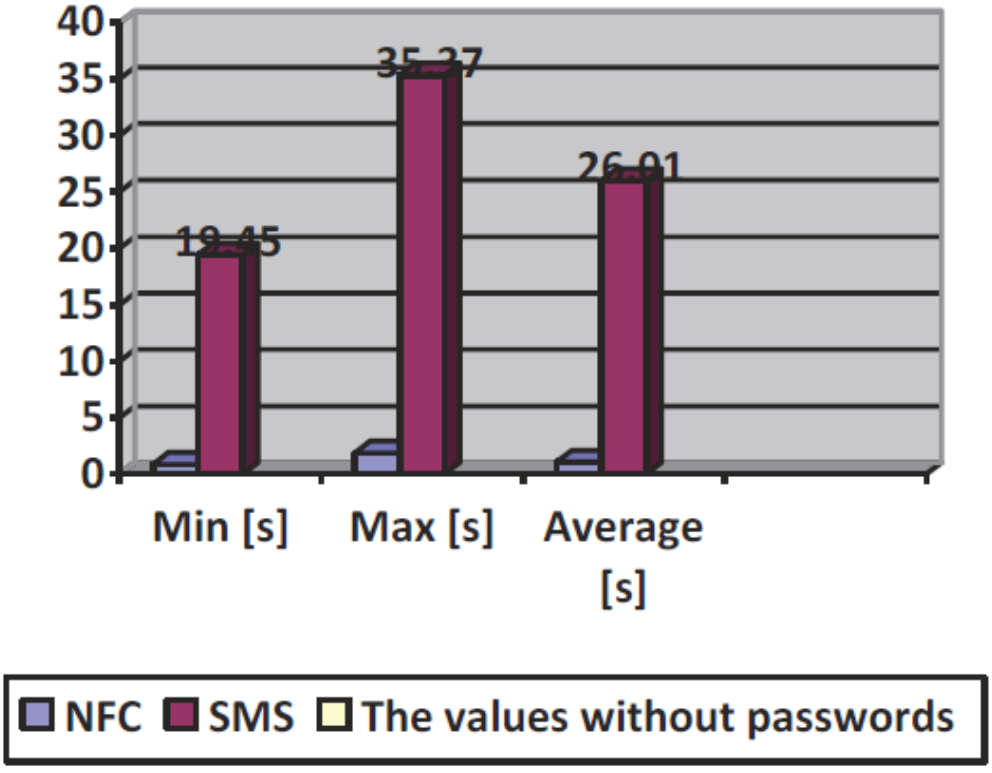
Споредба	Побарувања (Requirments)	Инсталација (Deployment)	Цени (Pricing)	Корисност (Usability)
TUPAS	Да биде корисник и да има соодветно корисничко име и шифра	Се користи во Финска, Данска, Норвешка, Шведска и Друго ЕУ држави.	Цените се слични на цените за користење на телефон, со договор 12/24 месеци	Лесен за користење, корисникот треба да ја знае само својата шифра
Мобилен Сертификат	Нова СИМ картичка што подржува мобилен сертификат	Не е прифатено како технологија од банките и мобилните оператори, се очекува имплементација	Цените се слични на цените за користење на телефон, со договор 12/24 месеци	Лесен за користење, ако се користи само со телефон. Може да е сложено со користење на втор (таблет,лаптоп) уред.
СМС-ОТП	корисникот треба кориснкот да има само СИМ картичка и телефон мобилен	Многу често користена услуга најчесто од банките за електронско банкарство	Цените се слични на цените за користење на телефон, со договор 12/24 месеци	Лесен за користење, ако се користи само со телефон. Може да е сложено со користење на втор (таблет,лаптоп) уред.
НФЦ	Мобилен телефон со НФЦ чип	Многу слаба покриеност, сеуште се води како експериментална технологија	Цените се слични на цените за користење на телефон, со договор 12/24 месеци	Најсложен за користење, бара одлична обука и добри предзнаења.

Табела Бр.1

5. Експерименти



Слика бр.2



Слика бр.3

6. Заклучок

СМС-ОТП е наједностава технологија за користење со најмала безбедност, мобилниот сертификат е технологија која е лесна за користење и има големо ниво на безбедност. НФЦ е најдобра од сите технологии но треба време додека биде прифатена од корисниците и додека има соодветен пазар за неа, како и соодветни и економски достапни уреди за сите. (Прикажано на Слика бр.2 и бр.3).

Според ова може да се види дека НФЦ е технологија која ќе помине доста време додека биде достапна и прифатена, но можностите со НФЦ се сеуште нова и "неосвоена територија".

Со експериментот се покажува дека НФЦ технологијате е супериорна споредена со предходниците, поради брзината на автентификација и поради нивото на сигурност што доаѓа со НФЦ (Attribute Based Access Control).

7. Литература

[1] Andrew S. Tanenbaum, David J. Wetherall, Computer Networks - 5th Edition, 2010
[2] Yi-Bing Lin, Imrich Chlamtac, Wireless and Mobile Network Architectures Paperback, 2000
[3] I.A.Dhotre V.S.Bagad, Information Security, 2009
[4] V. S. Corporation. MobileKey (Mobile Authen¬tication Server). http://www.visualtron. com/products_mobilekey.htm.
[5] Digitoday -Jukka Lehtinen. Sähköinen tunnis¬tusfloppi on käynyt kalliiksi. http://www. digitoday.fi/tietoturva/2008/04/21/ sahkoinen-tunnistusfloppi-on-kaynyt¬kalliiksi/200811104/66
[6] Ericsson. Mobile subscriptions hit 5 billion mark. http://www.ericsson.com/thecompany/ press/releases/2010/07/1430616, July 2010.
[7] J. erik Ekberg, N. Asokan, K. Kostiainen, P. Eronen, A. Rantala, and A. Sharma. NRC-TR-2008-001 On-Board Credentials Platform Design and Implementation, 2008.
[8] IBM Zurich Research Lab -Diego A. Ortiz-Yepes. Enhancing Authentication in eBank¬ing with NFC-Enabled Mobile Phones. http://ercim-news.ercim.eu/en76/rd/ enhancing-authentication-in-ebanking¬with-nfc-enabled-mobile-phones.
[9] K. Kostiainen, J.-E. Ekberg, N. Asokan, and A. Rantala. On-board credentials with open provi¬sioning. In ASIACCS '09: Proceedings of the 4th In¬ternational Symposium on Information, Computer, and Communications Security, pages 104–115, New York, NY, USA, 2009. ACM.
[10] Network System Architects, Inc. What is a Subscriber Identity Module (SIM)? .
[11] http://www.gsm-security.net/faq/ subscriber-identity-module-sim. shtml.
[12] NFC Times -Dan Balaban. Nokia Begins Shipping C7 Smartphone with NFC Chip In¬side. http://www.nfctimes.com/news/ nokia-prepares-introduce-first-nfc¬smartphone.
[13] Nordea. Strong End-user Authentication for Online Banking with NFC Handsets. http://www.mobilemondayoulu.com/wp-content/uploads/Strong_End-user_Authentication_for_Online_Banking_ with_NFC_310809.pdf.
[14] RFID - Consortium for Security and Privacy. Vulnerabilities in First-Generation RFID-Enabled Credit
[15] Cards. http://www.rfid-cusp.org/blog/blog-23-10-2006.html.
[16] RSA. Security Information Security Glossary - Strong authentication. http://www.rsa.com/
[17] glossary/default.asp?id=1080.
[18] TeleSign. Two-Factor Authentication. http://www.telesign.com/solutions_
[19] twofactor_auth.php.
[20] TeleSign. TeleSign's SMS Identification Stops Phishing and Online Fraud! http://www.prlog.org/ 10626763-telesigns-sms-identificationstops-phishing-and-online-fraud.html.
[21] Yahoo. What is Flash SMS. http://in.content.mobile.yahoo.com/new/flash/.