Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 656.8
DOI: https://doi.org/10.24867/14DS02Petrovic

КРИПТОГРАФИЈА И УСЛУГЕ ОД ПОВЕРЕЊА У ПОШТИ

CRYPTOGRAPHY AND TRUSTED SERVICES IN THE POST OFFICE

Ружица Петровић, *Факултет техничких наука, Нови Сад*

Област – САОБРАЋАЈ

Кратак садржај – *Електронско пословање захтева сигурност у комуникацији између корисника. У овом раду презентована је криптографија, безбедност на мрежи сертификациона тела, електронски сертификати и временски жиг.*

Кључне речи: *криптографија, безбедност на мрежи, електронски сертификати, временски жиг*

Abstract – *E-business requires security in communication between users. This paper presents cryptography, online security certification bodies, electronic certificates and timestamp.*

Keywords: *cryptography, network security, electrpnic certiificates, time stamp*

1. УВОД

Време савремене економије и модерног друштва немогуће је замислити без коришћења информационо-комуникационих технологија.

Данашње друштво све више зависи од информационо-комуникационих технологија. Велика количина личних података преноси се путем различитих комуникационих уређаја или се само чува на њима. Из тог разлога, електронске комуникације и информационо-комуникационе технологије постају једна од најрањивијих тачака заштите приватности појединаца.

Да би испунили своју улогу, информациони и комуникациони системи треба увек да буду поуздани и на располагању корисницима, поверљивост информација које се преносе и чувају не сме бити угрожена, а корисници морају бити сигурни и у идентитет пошиљаоца и у то да је примљена информација идентична послатој.

Циљ овог рада јесте да укаже на начине заштита приватности корисника и безбедност на мрежи.

Након увода, у другом поглављу описана је безбедност на мрежи. Дефинисан је циљ безбедности на мрежи, наведене су особине сигурне комуникације, затим су представљене врсте напада на мрежи, како их разликовати и дате су њихове основне карактеристике.

Треће поглавње односи се на историјски развој криптографије, увод у криптографију, принципе криптографије, начину шифровања и алгоритмима за шифровање такође и дистрибуцији кључева у асиметрични и симетричним криптографским системима.

У оквиру четвртог поглавља обрађене су услуге од поверења у пошти и сертификационо тело.

Пето поглавље односи се на електронске сертификате у оквиру кога су описани оперативни захтеви у процесу издавања сертификата, контроле физичког приступа, процедура, овлашћених лица и техничке заштите, као и права и обавезе издаваоца и корисника сертификата.

У шестом поглављу објашње је електронски временски жиг, поступак његовог издавања, животни циклус кључева TSA сервера, физичко обезбеђење, контрола приступа, као и остале процедуре.

У седмом поглављу приказана је детаљна анализа анкете која је спроведена за потребе овог рада. Тема анкете је била Електронски сертификати.

Осмо поглавље односи се на закључна разматрања анализе анкете.

Последње поглавље се односи на закључна разматрања која су донета на основу проучене материје.

2. БЕЗБЕДНОСТ НА МРЕЖИ

Као најзаступљенији медијум за пренос података користе се рачунарске мреже. Као такве логично представљају уско грло по питању сигурности информација које се тим путем преносе, јер може доћи до: крађе података, читања туђих порука, мењања туђих порука, приступ недозвољеним системима, негирање ауторства, лажно представљање. Безбедна комуникација ће бити представљена на следећем примеру.

Особа А шаље поруку особи Б, при томе особа А жели да само особа Б разуме написану поруку, чак и ако се комуникација врши преко небезбедног медијума где постоји могућност да уљез пресретне поруку. Особа Б такође жели бити сигурна да је порука која је примљена заиста послата од особе А. Особе које комуницирају желе бити уверене да се садржај поруке није променио у транзиту [1].

Мере за заштиту података уопште, се заснивају на три принципа:

- Превенција - односи се на предузимање превентивних активности за заштиту података и рачунарских система од могућих напада
- Детекција - откривање како је нарушена заштита, када је нарушена и ко је нарушио
- Реакција - предузимање активности које доводе до рестаурације података или до рестаурације рачунарског система.

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је била др Драгана Шарац, ред. проф.

Сви напади на податке који се преносе мрежом се могу поделити у две групе:

- Пасивни напади - односе на сва прислушкивања и надгледања информација током преноса, без икаквих измена
- Активни напади - сви напади који врше промену садржаја или тока информација.

3. КРИПТОГРАФИЈА

Криптографија је вештина и наука да се одређена информација – порука проследи на тајни начин. Омогућава да се поверљиве информације ускладиште или пренесу преко мреже која је небезбедна, тако да могу бити само прочитане од стране оног коме је намењена порука.

Поступак помоћу кога се изворни текст трансформише у шифрован текст се назива криптовање. Криптовање омогућава да ниједан корисник, осим корисника коме је порука намењена, не може да сазна садржај поруке.

Ако неовлашћени корисници дођу у посед криптованог текста и виде његов садржај не могу га протумачити.

Поступак који омогућава да се од криптованог текста добије оригинални изворни текст назива се декриптовање.

Декриптовање односно дешифровање представља инверзни поступак од криптовања [2].

3.1. Кратак историјски преглед

Криптографија као средство за заштиту информација датира још од појаве првих писама, када је било неопходно пренети поруку на даљину и то сачувану од туђих нежељених погледа.

У 5. веку п.н.е. Спартанци су користили направу за шифровање која се називала скитал. То је био дрвени штап око којег се намотавао лист папируса на који се дуж штапа писала порука.

Након уписивања поруке, папир се одмотавао, а на њој би остали измешани знакови које је могао прочитати само онај ко је имао штап једнаке дебљине.

У 6. веку п.н.е. у делу Библије, Књиге о Јеремији, коришћена је једноставна шифра која изврће абецеду наопако. Шифра је позната под именом Атбаш.

Грцки писац Полибије у 2.века п.н.е. објаснио је замену слова бројевима употребом табеле. Данас је тај систем познат под називом шаховска плоча. Она се састојала од 5 редова и 5 колона, односно од 25 поља у која су уношена слова.

Прве методе криптовања је користио Јулије Цезар када је слао поруке својим војсковођама. Он је те поруке шифровао тако што је слова у тексту померао за три места у алфабету. Такву поруку могли су да дешифрују само они који су познавали правило померања.

Године 1518. Јоханес Тритемијус је написао прву штампану књигу о криптографији.

Око 1790. Томас Џеферсон је уз помоћ математичара Др. Роберта Патерсона изумео шифарник с точком, 1861. у патентном заводу у САД пријављен је први изум везан за криптографију а 1923. Артур Шербиус производи свој најславнији производ - широко познату Енигму [3].

3.2. Методе шифровања

Супституционо шифровање је шифровања код кога се свако слово или група слова замењује другим словом или групом слова за прикривање. Супституционо шифровање обухвата следеће врсте замена:

- Моноалфабетска замена
- Полиалфабетска замена
- Полиграмска замена

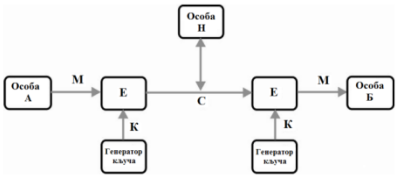
Транспозиционо шифровање не скрива слова отвореног типа али им мења распоред. Оваква шифра као кључ има реч или фразу у којој се не понављају ни једно слово.

3.3.Симетрична криптографија

Симетрична криптографија је најстарији облика криптографије.

Основна карактеристика симетричних алгоитама је коришћење истог (јединственог) кључа за шифровање и дешифровање. То значи, да и пошиљалац и прималац поруке поседују идентичан кључ који међусобно размењују посебно безбедним каналом. Сигурност система зависи од квалитета алгоритма за трансформацију, дужине и начина генерисања кључа и од тајности кључа. Због тога се ови криптографски системи зову и системи са тајним кључевима.

Особа А има за циљ слање поруке М особи В преко незаштићеног комуникационог канала. Особа А најпре генерише поруку М (изворни текст) која се упућује у блок за шифровање Е. У овом блоку се врши шифровање поруке М уз коришћење кључа К добијеног уз помоћ генератора кључа. На тај начин се креира шифрована порука С. Потом се тако добијена порука комуникационим каналом шаље до особе В. Поступак дешифровања се обавља инверзним поступком од шифровања у блоку за дешифровање. Дешифровање поруке С се врши помоћу истог кључа К који је коришћен приликом шифровања. Након дешифровања се добија изворна порука М. Уколико на каналу за пренос постоји особа N (нападач) која може да пресретне шифровану поруку и уколико дође у посед кључа може прочитати или злоупотребити изворну поруку. (Слика 1).



Слика 1. Блоковски приказ симетричног криптосистема

3.4. Асиметрични криптографски алгоритми

Главни проблем криптографије одувек је био дистрибуција кључева, уколико непријатељ открије кључ и најбољи алгоритми били су бескорисни, због тога научници развили нову идеју која се заснивала на два кључа, тајном и јавном кључу.

Основна разлика у односу на симетричне алгоритме који користе исти кључ за шифровање и дешифровање јесте да се код асиметричних алгоритама користе различити кључеви за шифровање и дешифровање. Шифровање се врши јавним кључем који је доступан свима, док се дешифровање врши

тајним кључем који поседује само одговарајућа особа. Јавни и тајни кључ су повезани једносмерном функцијом која омогућава да посредством приватног кључа добије јавни кључ, док обрнута веза није могућа.

3.5. Хибридни криптосистеми

Принцип рада хибридних криптосистема: Прво се врши шифровање изворног текста употребом кључа (понекад назван и session кључ), а затим се тај кључ заједно са шифрваном поруком пакује и поново врши шифровање са јавним кључем особе којој се шаље порука. Поступак дешифровања целе поруке се остварује обрнутим редоследом операција: Особа која је примила поруку прво дешифрује исту са својим тајним кључем, проналази запаковани session кључ и користи га да би прочитала изворну поруку.

3.6. Дигитални потпис

Дигитални потписи се користе за идентификацију извора информације који може бити нека особа, организација или рачунар. Идеја дигиталног потписа је слична класичном потписивању докумената. Уколико се неки документ жели послати електронским путем, такође се мора потписати. За разлику од класичног потписа, дигитални потпис је готово немогуће фалсификовати.

Потписивањем докумената особа која их шаље гарантује аутентичност, интегритет и немогућност порицања особи која их прима.

Аутентичност многих законских, финансијских и других докумената одређује се присуством или одсуством овлашћеног писаног потписа. За компјутеризоване системе поруке које могу заменити физички транспорт докумената писаних на папиру, мора се наћи метода која омогућава електронским документима да се потпишу на адекватан начин. Дигитални потпис је криптографска техника за постизање ових циљева у дигиталном свету [4].

Области у којима се дигитални потписи највише користе су електронска трговина, електронска пошта и разне финансијске трансакције, мада се ова техника може наћи и у другим областима у циљу решавања многих проблема који се односе на безбедност информација.

4. СЕРТИФИКАЦИОНА ТЕЛА

Регистрована сертификациона тела, до данашњег дана, за издавање квалификованих електронских сертификата у Републици Србији су:

- Јавно предузеће ПТТ саобраћаја „Србија” РЈ за електронско пословање - СЕРР
- Привредна комора Србије - PKS CA
- МУП РС - Сертификационо тело MUP RS
- Привредно друштво Halcom а.д. Београд – HALCOM BG CA
- „E- Smart Systems“ d.o.o

Сертификационо тело Поште Јавно предузеће ПТТ саобраћаја „Србија” изградило је PKI систем под именом Сертификационо тело Поште, према решењу компаније Entrust. Сертификационо тело Поште користи у својој инфраструктури за издавање квалификованих електронских сертификата хијерархију више CA сервера. Инфраструктуру Сертификационог тела Поште чине два сертификациона тела [5]:

- „Posta CA Root” сервер, као Root сертификационо тело
- „Posta CA 1” сервер, као подређено сертификационо тело.

Корисници Сертификационог тела Поште могу да буду:

- физичка лица – индивидуални корисници,
- правна лица / државни органи / организације.

5. ЕЛЕКТРОНСКИ СЕРТИФИКАТИ

Електронски сертификати омогућавају потврду идентитета учесника у електронској комуникацији. Они повезују податке о идентитету учесника у комуникацији са паром асиметричних кључева који се користе за шифровање и потписивање дигиталне информације чиме потврђује нечије право на коришћење пара криптографских кључева. Дакле, потврђује се да одређени јавни кључ припада одређеном крајњем ентитету (крајњем кориснику, али и корисничком серверу). На тај начин се спречава злоупотреба кључева и да се неко неовлашћено представља туђим идентитетом.

Електронски сартификат садржи податке о власнику, јавни кључ власника, период важења сертификата, име издавача (сертификационо тело које је издало сертификат), серијски број сертификата, дигитални потпис издавача.

5.1.Оперативни захтеви у процесу издавања сертификата

Захтев за издавање сертификата може да поднесе физичко или правно лице које испуњава одређене услове.

За издавање сертификата потребно је обавити идентификације и потврђивања аутентичности. Сертификационо тело Поште идентификује корисника на основу докумената за идентификацију које корисник подноси (важећа лична карта, пасош). Корисник мора лично да поднесе целокупну документацију.

Сертификационо тело Поште корисника обавештава о издавању сертификата коришћењем контакт података које је он навео приликом регистрације.

Корисник квалификовани сертификат преузима лично на изабраној локацији на територији Републике Србије. Првом употребом квалификованог сертификата од стране корисника, сертификат се сматра прихваћеним.

Обнова квалификованог сертификата, замена јавног кључа у квалификованом сертификату и промена података у квалификованом сертификату се не врше. Цео процес се извршава издавањем новог квалификованог сертификата [6].

6. ЕЛЕКТРОНСКИ ВРЕМЕНСКИ ЖИГ

Сертификационо тело Поште је изградило систем за издавање временских жигова и постало је издавалац временских жигова (Time-Stamping Authority - TSA) у Републици Србији, у складу са Законом о електронском документу и Правилником о издавању временског жига. Временски жигови Поште намењени су

свим учесницима електронског пословања у Републици Србији, и физичким и правним лицима (државна управа, локална самоуправа, јавне службе, предузећа, банке, осигуравајућа друштва, организације, институције,...) [7].

TSA тело Поште осигурава да временски жиг буде издат на сигуран начин и да садржи тачно време. TSA тело Поште издаје само једну врсту временског жига, у складу са Политиком. Сваки жиг садржи идентификациони број Политике издавања временског жига (OID) и јединствени серијски број издатог жига [8].

Временски жиг је електронски потписан тајним (приватним) кључем TSA сервера. TSA тело Поште за формирање електронског потписа временског жига користи RSA алгоритам применом стандарда PKCS#1, уз дужину RSA кључа од 2048 бита. Жиг садржи TSA електронски сертификат којим се проверава електронски потпис временског жига.

Временски жиг садржи UTC време упоредиво са UTC тачним временом, уз максимално дозвољено одступање у односу на UTC тачно време од ±1 секунди. Очекивано време важења временског жига одређено је роком важења TSA електронског сертификата, којим се проверава електронски потпис временског жига.

7. ПОВЕРЕЊЕ У ЕЛЕКТРОНСКЕ СЕРТИФИКАТЕ

За израду мастер рада спроведена је анкета о поверењу грађана у електронске сертификате. Резулатати добијени анкетирањем анонимних испитаника дефинишу постојеће стање о корисницима електронских сертификата и могу да скрену пажњу на одређене проблеме при коришћењу.

Већина учесника у анкети не користи електронске сертификате, а као главни разлог томе наводе недовољну едукованост, затим злоупотребу података док је мањи део испитаника навео страх од преваре.

Ако се погледа сам циљ постојања електронског потписа, а то је олакшано потписивање докумената на даљину уз пар клика на рачунару или паметном телефону, онда свакако процедура прибављања електронског потписа пред државним органима у Србији је установљена супротно том циљу јер захтева присуство подносиоца захтева.

Већина испитаника није имала проблема при коришћењу електронских сертификата, док они који су имали, навели су да су то мањи технички проблеми које успевају да реше помоћу упутства, реинсталацијом или помоћу техничке помоћи издавача електронског сертификата. Неки наводе да сваког месеца имају проблем са е-Управом као и да тај проблем самостално решавају.

Као предлог за унапређење услуге издавања и коришћења електронског сертификата корисници сертификата који су учествовали у анкети предложили су да се уведе електронски сертификат у што више сфера и да то не буде опционо, већ да се заиста користи како би смањили коришћење папирне форме, самим тим архивирање исте из еколошких разлога, да буду што једноставнији и бржи и да се ради на едукацији становништва као потенцијалним корисницима електронског сертификата.

8. ЗАКЉУЧАК

Електронском разменом информација појавила се потреба за заштитом поверљивих података од разних крађа и злоупотреба, што је условило појаву новог правца у области безбедности података.

Криптографија је веома динамична наука коју одликује уска повезаност између теорије и праксе. Представља веома широку област и у пракси се базира на употреби криптосистема који се састоје од алгоритама за криптовање, једног или више кључева, система за управљање кључевима, података у виду стандардног и криптованог текста. За реализацију криптографских алгоритама који су данас у употреби, користе се сложени математички изрази као и знања из електронике и програмирања.

Свака озбиљнија апликацију има имплементиран неки сигурносни алгоритам, почев од банкарских апликација, интернет трговине, па све до оперативних система.

Циљ овог рада је да укаже на нужност заштите података, упознавањем и применом електронских сертификата и електронског временског жига. Популаризација електронског пословања је сложен процес који захтева пре свега едукацију грађана са циљем да се привуку нови корисници.

Електронско пословање се стално развија, упоредо са њим развијају се и методе за превару и крађу података што захтева унапређење заштите података и идентитета корисника дигиталне комуникације.

За квалитетну и сигурну мрежу потребно поседовати информатичку инфратруктуру високог квалитета, знања стручњака из различитих области и вршити константна улагања и унапрепређења система. Пошта је једно од регистрованих сертификованих тела које све то поседује и у које корисници имају поверење.

9. ЛИТЕРАТУРА

[1] J. Kurose, Ross K., Computer Networking, Chapter 8. Security in Computer Networks, 671-691, 6ed, Pearson Education, USA, 2013

[2] J. Kurose, Ross K., Computer Networking, Chapter 8. Security in Computer Networks, 671-691, 6ed, Pearson Education, USA, 2013

[3] https://hr.wikipedia.org/wiki/Kriptografija#Povijest

[4] Kovačević Vladimir, Zaštita podataka primenom kriptografskih metoda, Univerzitet u Nišu, Elektronski fakultet, 2014.

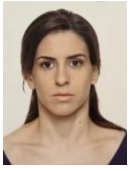
[5] Prakticna pravila Posta CA CPS QC v1.1-pdf

[6] Politika sertifikacije Posta CA CP QC v1.1-pdf

[7] https://www.ca.posta.rs/vremenskizigovi.htm

[8] Politika izdavanja vremenskog ziga Posta TSA 2015

Кратка биографија:



Ружица Петровић рођена је у Ужицу 1992. године. Мастер рад на Факултету техничких наука, из области поштанског саобраћаај и телекомуникација, одбранила је 2021. године.