УДК 004.7.056.5:336.717.1

О.В. Клювак[1], С.С. Королюк[2], А.А. Засядько[2]

[1]*Львівський інститут банківської справи Університету банківської справи НБУ, Львів*
[2]*Черкаський інститут банківської справи Університету банківської справи НБУ, Черкаси*

АНАЛІЗ МЕТОДІВ АУТЕНТИФІКАЦІЇ ЗА ДОПОМОГОЮ БАНКІВСЬКИХ КАРТОК В ІНТЕРНЕТ-ПЛАТІЖНИХ СИСТЕМАХ

У статті проаналізовано механізми дії технології 3D Secure, протоколу автентифікації KERBEROS та багатофакторної автентифікації в інтернет-платіжній системі. Обґрунтовано основні недоліки описаних методів та запропоновано шляхи вдосконалення схеми автентифікації під час здійснення транзакцій за допомогою банківських карток.

Ключові слова: *протокол автентифікації, інтернет-платіжна система, інтернет-транзакція, технологія 3D Secure автентифікаційний сервер, платіжний сервер, банківська платіжна картка, маркер сеансу, маркер платежу, багатофакторна автентифікація, транзакційний ідентифікаційний код (TIC), служба коротких повідомлень (SMS).*

Вступ

Постановка проблеми у загальному вигляді і її зв'язок з важливими науковими та практичними завданнями. На сьогоднішній день розроблено достатньо велику кількість протоколів автентифікації, зокрема для застосування у інтернет-платіжних системах. Проте, більшість з них не володіють усіма необхідними властивостями для проведення взаємної автентифікації як покупця, так і продавця. Також у них не враховано той факт, що Інтернет є абсолютно незахищеним середовищем, а платіжна картка є досить ризиковим платіжним засобом, і саме тому повинні ставитися досить високі вимоги до розробки схем таких протоколів. Паралельний опис технології 3D Secure, протоколу KERBEROS та багатофакторної системи автентифікації дає можливість видокремити їхні недоліки та на основі цього запропонувати комбінований механізм автентифікації під час здійснення транзакції в інтернет-платіжній системі. **Аналіз останніх досліджень, у яких започатковано вирішення проблеми.** Дослідженнями у сфері автентифікації в інтернет-платіжних системах займаються як зарубіжні вчені, так і вітчизняні. Зокрема, науковець Юнг Кім Ин детально описує механізм дії протоколу KERBEROS та можливості його вдосконалення. Серед інших зарубіжних авторів публікацій у цій галузі можна назвати наступних: Річард Е.Сміт, Майкл Дж. Венстром, К.Н. Кузовкін. Серед вітчизняних учених, котрі займаються дослідженнями у сфері криптографічних протоколів, зокрема аутентифікаційних, являються Яковина В.С., Одуха О.В. та деякі інші. Російські учені Афанасьев, Л. Т. Веденьев, А.А. Воронцов у своїх працях аналізують методи безпечного доступу до інформаційних ресурсів. Дослідженнями у сфері багатофакторної автентифікації в інтернет-платіжних системах займаються наступні науковці: Сугата Саньял, Аю Тіварі, Судіп Саньял, Тархов А. та інші.

Мета роботи полягає у аналізі методів автентифікація міжнародних платіжних систем VISA і MasterCard, протоколу автентифікації KERBEROS, який застосовується при розрахунках в інтернет-платіжних системах, та багатофакторної автентифікації. Основні завдання дослідження: проаналізувати механізми дії технології 3D Secure, протоколу KERBEROS та багатофакторної автентифікації; відокремити основні недоліки описаних методів; запропонувати шляхи вдосконалення існуючих методів автентифікація в інтернет-платіжних системах.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів

Високоефективними розробками у галузі безпеки електронних платежів є технології 3D Secure (Verified by VISA і MasterCard Secure Code), які дозволяють значно знизити ризики при мережевих розрахунках. Суть технології 3-D Secure полягає у попередній перевірці особистості власника карти. Звірку даних виконує банк-емітент платіжної картки, який володіє необхідною інформацією про клієнта. Платіжний сервер (наприклад, eCommerce Connect Gateway) з боку банку-еквайєра автоматично організує зв'язок із системою автентифікації банку-емітента, використовуючи спеціальні ресурси платіжних систем (VISA Directory Server, Master Card Directory Server). Для здійснення платежів за технологією 3-D Secure користувач картки має зареєструватися у відповідній системі автентифікації банку-емітента, яку називають ACS (Access Control Server) та отримати особистий пароль, який буде відомий тільки власнику картки та банку. Під час

здійснення транзакції у мережі Інтернет, магазин, передаючи централізованому ресурсу (платіжному серверу банку-еквайрера) основні параметри транзакції, ініціює зв'язок платіжного сервера зі спеціальною системою Visa (або MasterCard). Це робиться з метою перевірки, чи є користувач картки учасником програми Verified by Visa (або MasterCard SecureCode). У випадку позитивної відповіді від цієї системи, що називається 'Directory Server', банку-емітенту направляється запит на аутентифікацію користувача картки. Цей запит передається емітенту у вигляді рядка параметрів, приєднаного до URL (WEB-адреси) системи автентифікації банку-емітента. URL з параметрами передається до броузера покупця. У такий спосіб покупець переадресується на систему автентифікації свого банку-емітента.

Банк запитує у користувача картки його особистий пароль, виданий у процесі реєстрації у програмі Verified by Visa або MasterCard SecureCode. Після підтвердження особи користувача картки система автентифікації банку-емітента генерує спеціальне унікальне цифрове значення, що відіграє роль "підпису", що засвідчує дану операцію. Цей "підпис" передається платіжному серверу і потім стає частиною авторизаційного запиту, який магазин (платіжний сервер) направляє своєму банку-еквайреру, а той, у свою чергу, направляє авторизаційний запит банку-емітенту. Перевіривши підпис та впевнившись у платоспроможності картки, банк-емітент завершує (схвалює) транзакцію. Таким чином, банк-емітент аутентифікує користувача картки у момент здійснення платежу та повідомляє віртуальний магазин у режимі реального часу про те, чи дійсно покупець є користувачем даної картки [1]..

Іншим методом автентифікації, який, на нашу думку вартий уваги,є протокол Kerberos. Основним недоліком даного протоколу є безпосередня передача реквізитів картки від покупця до продавця. Враховуючи це, можна запропонувати удосконалену систему автентифікації на основі Kerberos. Ця система передбачає відсутність ключа між сервером продавця та покупця, а також присутні нові зв'язки між сервером продавця та PGS (TGS у Kerberos) (рис. 1).

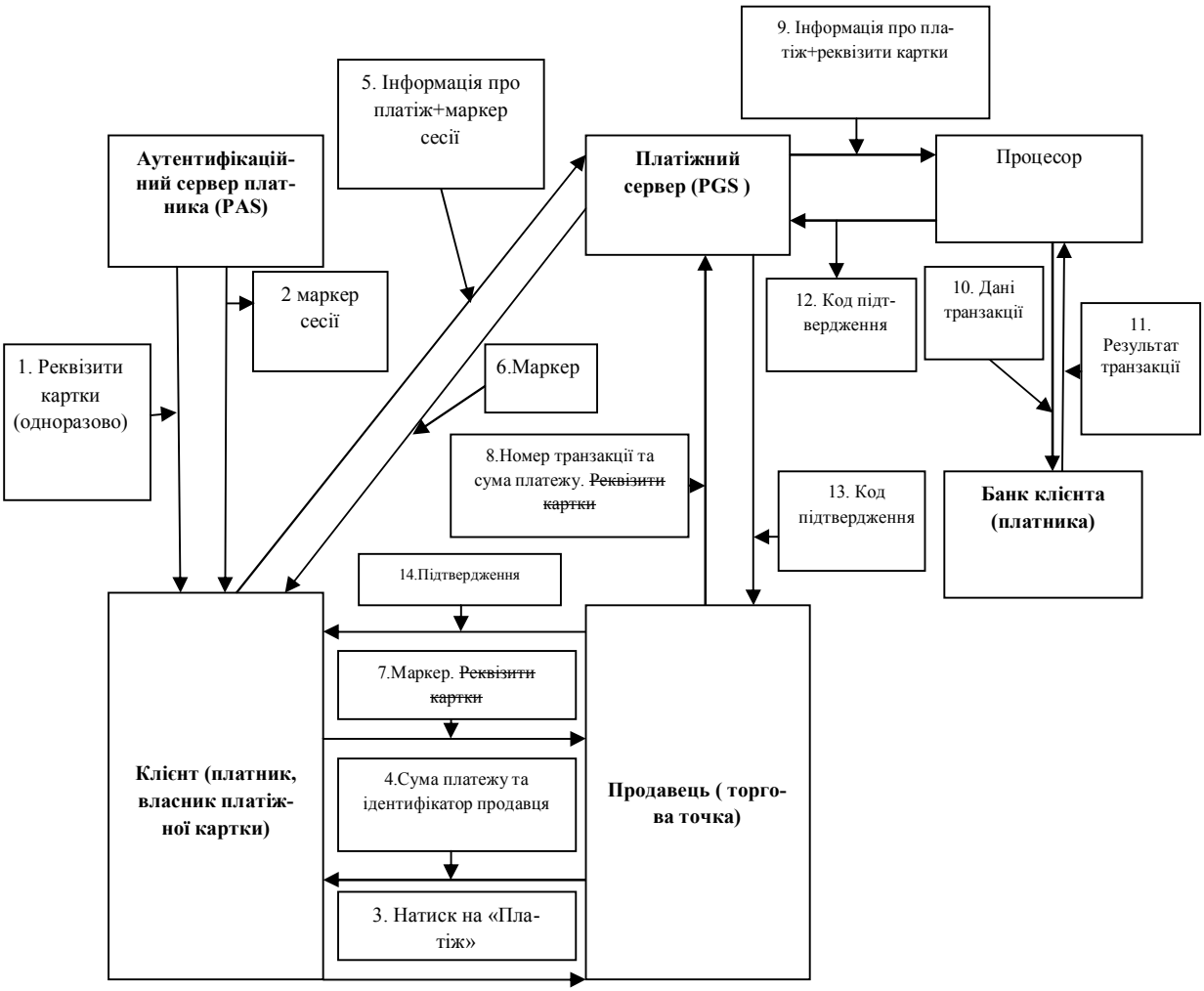

Рис. 1. Схема реалізації інтернет-транзакції
на основі удосконаленого протоколу автентифікації Kerberos

У схемі інтернет-транзакції на основі системи Kerberos клієнт зв'язується із торговою точкою, а торгова точка у свою чергу – із платіжним шлюзом. У нашому ж випадку, із схеми на рис. 1, видно, що платіжний сервер (PGS), який замінив платіжний шлюз, зв'язується, як з покупцем, так і з продавцем, на відміну від існуючої системи Kerberos. В обміні ключами також вартує дещо змінити, а саме між покупцем і продавцем (рис. 2).

Також, у вище запропонованій системі використовуються два маркери – маркер сеансу (присутній у системі Kerberos) та маркер платежу, який містить інформацію про покупця, продавця та суму платежу.

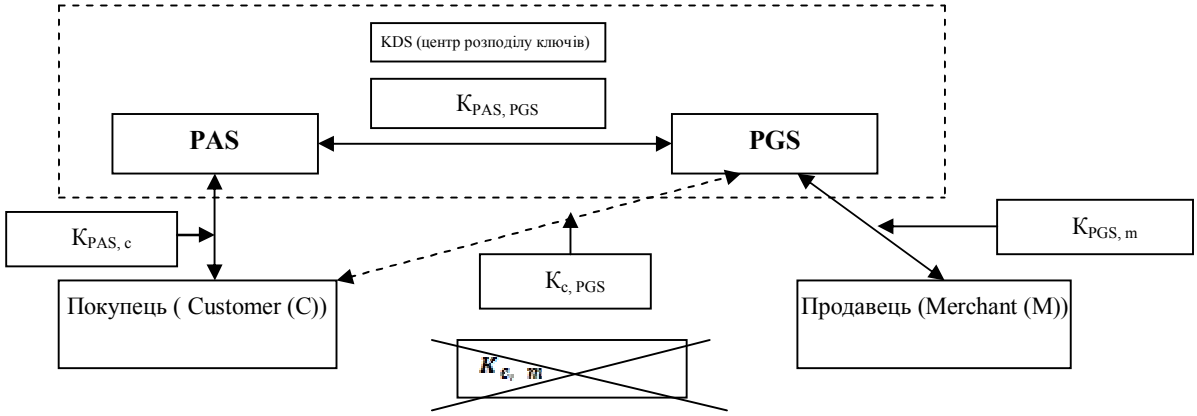

Рис. 2. Процес обміну ключами в удосконаленому протоколі автентифікації Kerberos

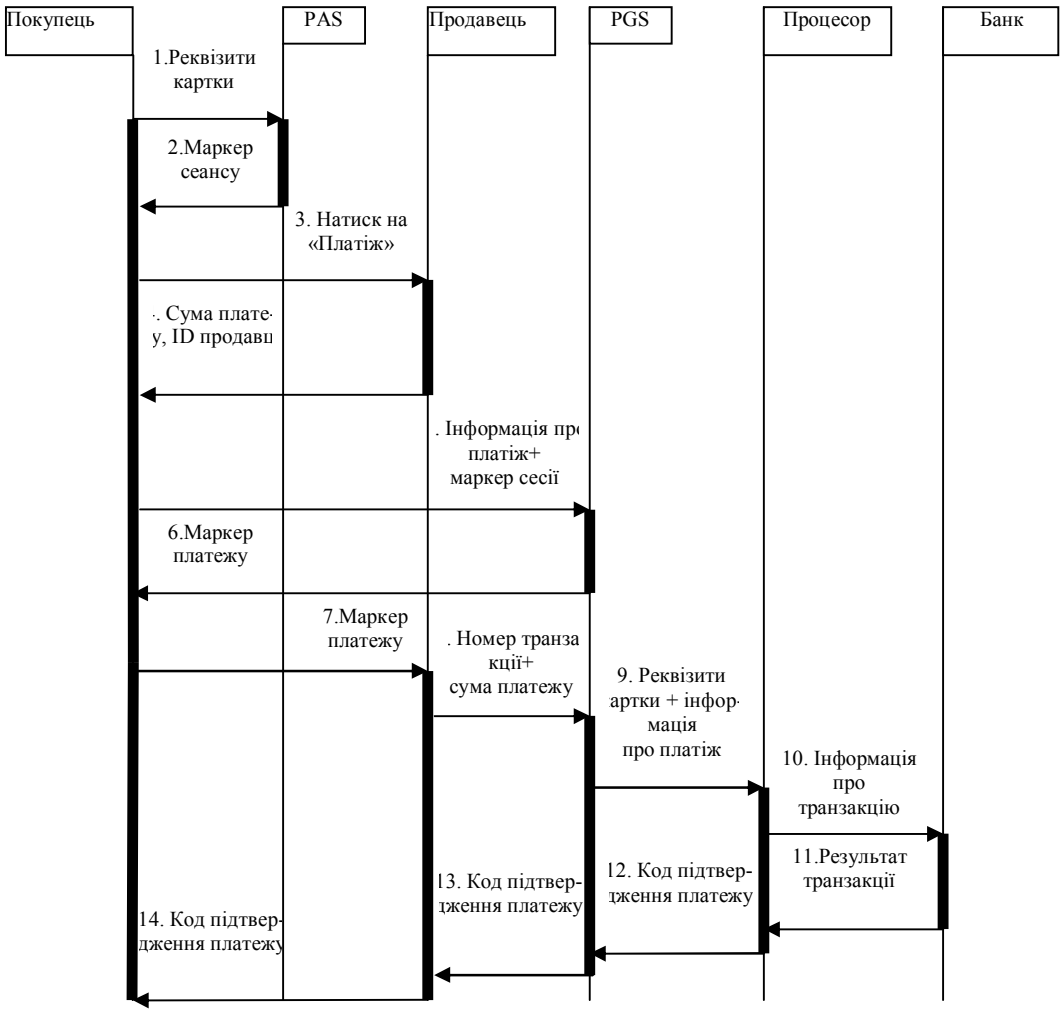

Рис. 3. Покрокова діаграма здійснення інтернет-транзакції в удосконаленому протоколі Kerberos

Як видно з рис. 3, спочатку покупець надсилає до аутентифікаційного серверу реквізити своєї картки і отримує натомість маркер сесії. Після цього клієнт надає інформацію про платіж (сума платежу, назва продавця) разом із маркером сесії платіжному серверу (PGS) та отримує від нього маркер платежу. Далі покупець надсилає продавцю цей маркер платежу. Згодом торгова точка надсилає номер транзакції платіжному сервера. Отримавши номер транзакції, PGS здійснює обробку платежу.

Очевидною перевагою запропонованого удосконаленого варіанту протоколу Kerberos є відсутність безпосередньої передачі реквізитів картки від покупця до продавця під час інтернет-платежу. У такий спосіб можна зменшити кількість шахрайств, пов'язаних із перехопленням реквізитів картки. У запропонованій схемі протоколу продавцю передаються маркери платежу замість інформації по картці. І, таким чином, ні продавець, ні зловмисник, який зламує базу даних, не мають можливості нелегально отримати реквізити картки. Варто також зазначити, що маркер криптографічно безпечний і дійсний лише для конкретного продавця, тож отримання його через прослуховування каналів нічого не дає зловмиснику. Наше удосконалення може бути застосоване до існуючого протоколу шляхом модифікації потоку даних, тобто замість надсилання реквізитів картки безпосередньо продавцю , до платіжного сервера надходить маркер [2-7].

Розглянемо тепер багатофакторну автентифікаційну систему, яка базуватиметься на трансакційному ідентифікаційному коді (TIC (Transaction Identification CODE)) та на службі коротких повідомлень (SMS(Short Message Service)) для створення додаткового рівня безпеки, який відсутній при традиційній автентифікації за типом ім'я користувача / пароль. Цей код схожий на одноразовий пароль (OTP (One Time Password)), але забезпечує більш надійну автентифікації, а також використовується лише один раз. TIC засвідчує, що поточна трансакція була ініційована саме тією особою, а не зловмисником, яка є істинним власником рахунку (банківської картки). TIC-коди володіють певними властивостями, а саме: створюються банком покупця; 32 бітними або 64 бітними псевдо-випадково згенерованими кодами; можуть являти собою складну послідовність цифр або комбінацію цифрових і буквено-цифрових символів; кожна трансакція вимагає унікального коду для автентифікації, тобто кожен код використовується лише один раз.

Механізм генерації кодів є суворо конфіденційним та передбачає обмежений доступ до них та лише уповноважених на це працівників фінансової установи. Банк зберігає номер телефону клієнта, щоб згодом надіслати SMS для підтвердження транзакції. Стільникова мережа використовує окремий канал для передачі і прийому SMS. Отже, багатофакторна автентифікація використовується для перевірки покупця та транзакції відповідно до наступних кроків:

1) Базова автентифікація: Спочатку покупець здійснює вхід на веб-сервер, використовуючи призначений йому веб-ім'я та пароль для базової автентифікації;

2) TIC-автентифікація: Після успішної автентифікації покупця за допомогою його веб-імені та пароля, веб сервер зажадає ввести TIC (друга автентифікація). Далі покупець розшифровує та вводить TIC для доведення своєї справжності автентифікаційному серверу та однозначної ідентифікації транзакції;

3) SMS-підтвердження: Після успішної TIC-автентифікації, третьою автентифікацією являється SMS-підтвердження. Покупець отримує SMS із деталями транзакції, які необхідні для ідентифікації та розпізнавання ініціатора транзакції. За допомогою SMS покупець надсилає підтвердження транзакції («ТАК») або скасовує її («НІ»).

Механізм багатофактрної автентифікації передбачає наступні кроки :

Клієнт отримує логін та пароль у своєму банку при відкритті рахунку або маючи рахунок у цьому банку; 2. Далі покупець входить на веб-сервер свого банку через GPRS-з'єднання, використовуючи свій логін та пароль. Ця перша автентифікації призначена для ідентифікації покупця веб-сервером; 3. Після успішної першої автентифікації покупець отримає опцію, щоб розпочати транзакцію із вхідним повідомленням та ідентифікатором сесії; 4. Покупець обирає спосіб оплати (кредитна картка, дебетна картка, електронний переказ). У випадку розрахунку карткою протокол вимагає дійсні реквізити платіжного засобу; 5. Покупець вводить деталі платежу; 6. Клієнт не може здійснити транзакцію без TIC. Треба мати на увазі, що TICи захищені паролем на мобільному телефоні, і цей пароль перед використанням в трансакції буде дешифрований з допомогою одного із TIC шифрів. 7. Уся сукупність трансакційних записів разом з TIC буде далі зашифрована та передана серверу для обробки. 8. Автентифікаційний сервер банку розшифровує отриману інформацію про транзакцію та витягує звідти TIC. Сервер перевіряє отриманий від покупця код, порівнюючи його із кодом, збереженим разом із інформацією про рахунок клієнта, а також який був обраний із списку кодів бази даних сервера. Якщо обидва коди співпали, використаний код автоматично знищується із бази даних. Якщо ж коди не співпали, тоді автентифікаційний сервер скасовує будь-які подальші транзакції клієнта та надсилає повідомлення про помилку. 9. Якщо TIC автентифікація є успішною, тоді авторизаційний сервер генерує текст повідом-

лення (SMS) та надсилає його до SMS шлюзу/ адаптера для передачі через стільникову мережу. Стільникова мережа використовує SMSC як основний пристрій мережі для передачі SMS на стільниковий телефон користувача. 10. Покупець підтверджує ініційовану трансакцію за допомогою SMS із текстом «ТАК» або скасовує обираючи текст повідомлення «НІ» (рис. 4).

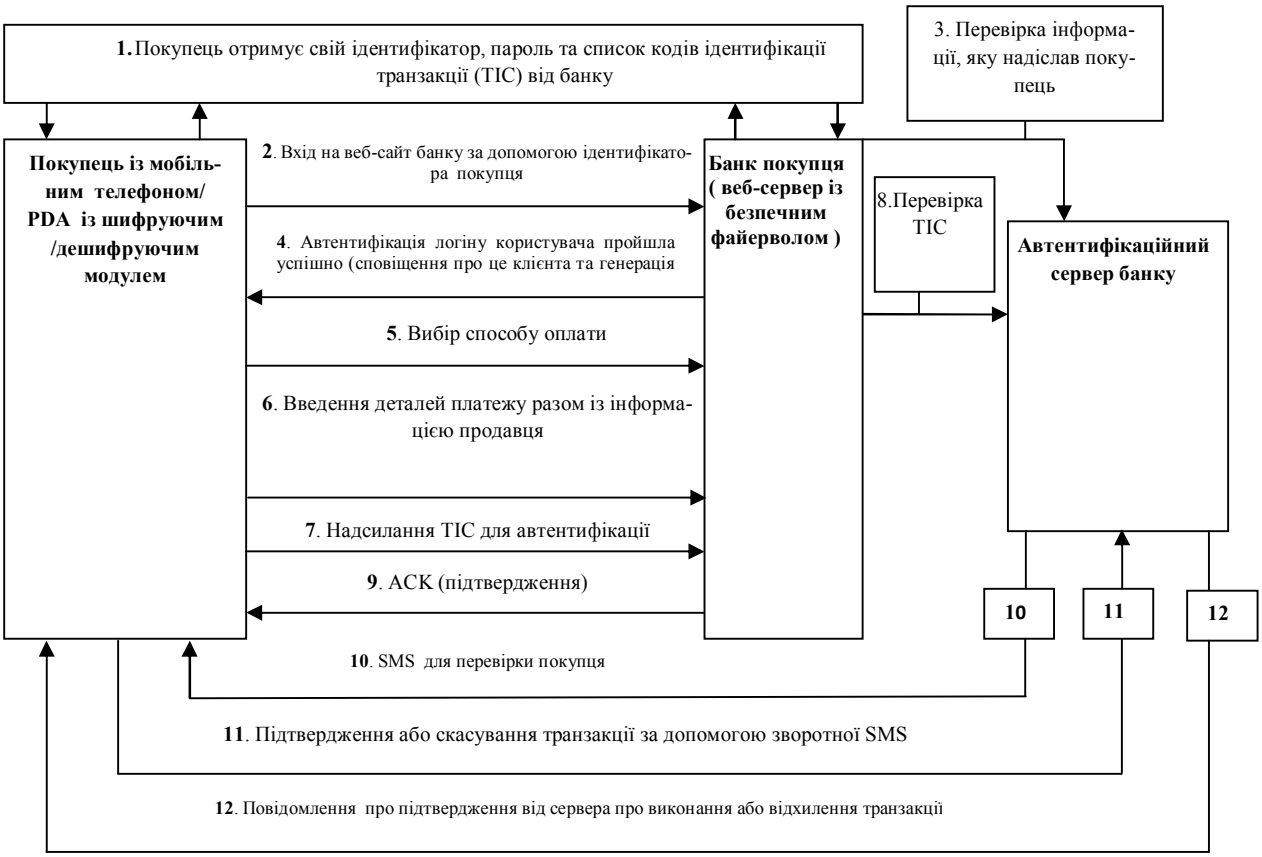

Рис. 4. Потік даних у протоколі багатофакторної автентифікації в інтернет-платіжних системах

У вищеописаному протоколі ТІС коди є найбільш уразливими даними, які зберігаються на стільниковому телефоні /КПК. Саме тому вони перебувають у цих пристроях покупця у зашифрованому форматі, а також захищені паролем, як це зображено на рис. 5.

Покупець вводить локальний пароль для відкриття списку ТІС кодів і обирає будь-який код з цього списку, щоб розпочати трансакцію. Цей вибір коду автоматично розшифровує його та автоматично виводить на екран користувача. Це також призводить до переміщення обраного коду із списку у середовище клієнта. Локальний пароль є ключем розшифрування ТІС коду та є відомий лише клієнту. Навіть серверу фінансової установи є невідомий цей пароль.

Код може бути змінений у будь-який момент за бажанням користувача [8 – 10].

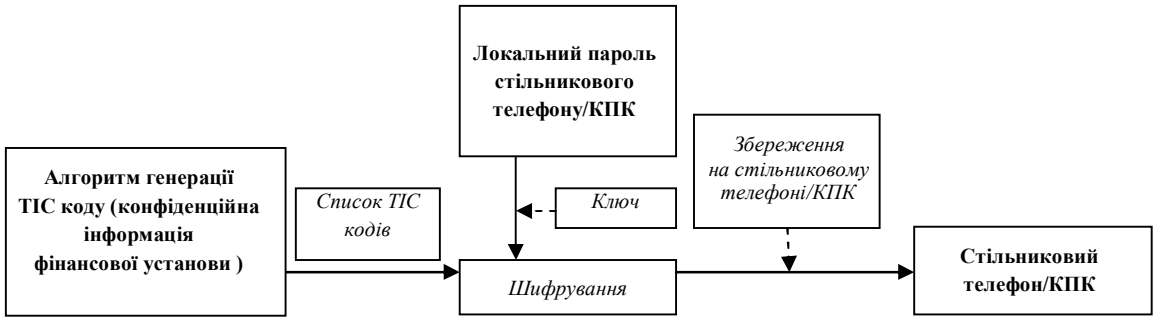

Рис. 5. Захист ТІС коду у середовищі покупця

Висновки

Таким чином, на нашу думку, найефективніший механізм автентифікації в інтернет-платіжних системах передбачає:

1) використання спеціального коду, який генерує банк покупця, що дає можливість не передавати реквізитів картки через Інтернет безпосередньо продавцеві;

2) цей код можна змінювати щоразу для нової трансакції, що передбачає значні затрати для банківської установи та створення окремого підрозділу для постійного супроводження та генерування кодів, необхідність для клієнта щоразу звертатися до свого банку за новим кодом. Проте цей код можна не змінювати щоразу для кожної нової трансакції шляхом його хешування у процесі передачі. При цьому, додатковим заходом безпеки може бути смс-підтвердження.

Список літератури

1. MasterCard представляет новое решение MasterCard TM Secure CodeTM, способствующее укреплению безопасности электронной коммерции [електронний ресурс]. – Режим доступу: http://www.finances.kiev.ua/news/Ynternet_bankyn1/07-05-2008/MasterCard_pred.html

2. A secure on-line credit card transaction method based on Kerberos Authentication protocol [Електронний ресурс] / Jung Eun Kim. − Режим доступу: http://digitalcommons.library.unlv.edu/cgi/viewcontent.cgi?article=1005&context=thesesdissertations&sei-redir=1#search=%22new+methods+of+authentication+in+internet+payment+system%22.

3. Протокол аутентификации Kerberos [Електронний ресурс]. - Режим доступу: http://cheaterrr.by.ru/5.htm

4. Кузовкин К. Удаленный доступ к информационным ресурсам. Аутентификация [Електронний ресурс]/ Кузовкин К.// Директор информационной службы – 2003. - №9 . — Режим доступу до журн. : http://www.i-teco.ru/article33.html.

5. Рассел Кей Kerberos [Електронний ресурс]. — Режим доступу: http://www.infocity.kiev.ua/inet/content/inet054.phtml.

6. The Role of Kerberos in Modern Information Systems [Електронний ресурс]. — Режим доступу: http://www.kerberos.org/software/rolekerberos.pdf

7. Why is Kerberos a credible security solution? [Електронний ресурс]. – Режим доступу: http://www.kerberos.org/software/whykerberos.pdf

8. Sugata Sanyal, Ayu Tiwari and Sudip Sanyal A Multifactor Secure Authentication System For Wireless Payment [Електронний ресурс]. – Режим доступу: http://www.tifr.res.in/~sanyal/papers/Multifactor%20Secure%20Authentication.pdf

9. Тархов Андрей Entrust IdentityGuard. Система многофакторной аутентификации [Електронний ресурс]. – Режим доступу: http://www.rnbo.ru/press-center/news228.php.

10. Аутентификация. Теория и практика обезпечения безопастного доступа к информационным ресурсам. Учебное пособие для вузов/ А. А. Афанасьев, Л. Т. Веденьев, А.А. Воронцов и др.; Под. Ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – М.: Горячая линия –Телеком, 2009.- 552 с.

Надійшла до редколегії 27.03.2012

Рецензент: д-р техн. наук, проф. В.Б. Дудикевич, Національний університет «Львівська політхніка», Львів.

АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ С ПОМОЩЬЮ БАНКОВСКИХ КАРТ В ИНТЕРНЕТ-ПЛАТЕЖНЫХ СИСТЕМАХ

О. В. Клювак, С.С. Королюк, А.А. Засядько

В статье проанализированы механизмы действия технологии 3D Secure, протокола аутентификации KERBEROS и многофакторной аутентификации в интернет-платежных системах. Обоснованы основные недостатки описанных методов и предложены пути совершенствования схемы аутентификации при осуществлении транзакций с помощью банковских карт.

***Ключевые слова**: протокол аутентификации, интернет-платежная система, интернет-транзакция, технология 3D Secure, аутентификационный сервер, платежный сервер, банковская платежная карточка, маркер сеанса, маркер платежа, многофакторная аутентификация, транзакционный идентификационный код (TIC), служба коротких сообщений (SMS).*

ANALYSIS OF AUTHENTICATION METHODS DURING VIA BANKING CARDS IN INTERNET PAYMENT SYSTEMS

O.V. Klyuvak, S.S. Korolyuk, A.A. Zasjad'ko

The mechanism of KERBEROS authentication protocol in internet-payment system is analyzed in the article The main disadvantages of the described protocol are devoted and it is suggested ways of improvement the authentication scheme during the realization of internet transaction, where a banking card is a mode of payment.

***Keywords**: authentication protocol, internet-payment system, internet transaction, technology 3D Secure, authentication server, payment server, banking payment card, session token, payment token, multifactor authentication , transaction identification code, short message service*