УДК: 519.7, 005 DOI 10.33111/mise.102.13

Мамонова Г.В., к.фіз.-мат.н., доцент
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Лисенко М.Ю., магістрант, ННІ «ІІТЕ»
Київський національний економічний університет
імені Вадима Гетьмана

Mamonova H.V., PhD of Physical and Mathematical Sciences, Associate Professor
of the Computer Mathematics and Information Security department
KNEU named after V. Hetman

Lysenko M.Y., graduate student,
Institute Information Technologies in Economics
KNEU named after V. Hetman

ІСТОРІЯ СТВОРЕННЯ ТА РОЗВИТКУ 3DS-ТЕХНОЛОГІЇ

HISTORY OF CREATION AND DEVELOPMENT OF 3DS-TECHNOLOGY

Анотація. *Питання безпеки платежів завжди було одним із найважливіших завдань будь-якої платіжної системи. Інженери та криптографи постійно працюють над створенням нових алгоритмів і систем безпеки, а хакери шукають уразливі місця в цих системах. Запровадження стандарту EMV для фізичних карток і технології 3D Secure для онлайн-платежів значно обмежило можливості шахраїв викривати та фальсифікувати дані карток і використовувати вкрадені реквізити. Стаття містить загальний огляд історії створення даної техніки, принцип її дії та шлях розвитку. Перехід платіжних програм на роботу з інтегрованим SDK (software development kit) підвищить швидкість та зручність процесу підтвердження операції. Доведено, що завдяки передачі відбитка пристрою також значно підвищиться рівень «впізнавання» емітентом свого клієнта. Частка операцій, що вимагають підтвердження, стрімко зменшуватиметься з поширенням таких додатків та їх активним використанням власниками карток для оплати товарів та послуг. Показано, що платіжна автентифікація для merchant-initiated платежів також підвищить конверсію платежів за підписками на регулярні сервіси, які стають особливо затребуваними останніми роками разом із переходом на сервісну модель споживання. Стаття має науково-методичний характер.*

Ключові слова: *стандарт EMV; 3D Secure; дані картки; оплата; система оплати; онлайн оплата.*

Abstract. *The issue of payment security has always been one of the most important tasks of any payment system. Engineers and cryptographers are*

constantly working to create new algorithms and security systems, while hackers are looking for these systems' vulnerabilities. The introduction of the EMV standard for physical cards and the 3D Secure technology for online payments had significantly limited the fraudsters' opportunities to expose and falsify card data and exploit stolen details. This article contains a general overview of the history of the creation of this technology, the principle of its operation and the path of development. The transition of payment programs to work with an integrated SDK (software development kit) will increase the speed and convenience of the transaction confirmation process. At the same time, thanks to the transfer of the device's fingerprint, the level of "recognition" by the issuer of its client will also significantly increase. The share of transactions requiring confirmation will rapidly decrease with the spread of such applications and their active use by cardholders to pay for goods and services. Payment authentication for merchant-initiated payments will also increase the conversion of payments for subscriptions to regular services, which have become especially popular in recent years with the transition to a service consumption model. The article has a scientific and methodological character.

Keywords: *EMV standard; 3D Secure; card data; payment; payment system; online payment.*

Постановка наукової проблеми та її значення. Питання безпеки під час проведення платежів було і залишається одним із найголовніших завдань будь-якої платіжної системи. Інженери та криптографи працюють над створенням нових алгоритмів та систем захисту, а зловмисники шукають у цих системах вразливі місця.

Період значного підвищення безпеки платежів припадає на 2000–2010 рр., коли впровадження стандарту EMV для фізичних карток і технології 3D Secure для інтернет-платежів суттєво обмежило можливості шахраїв у викритті та підробці карткових даних та експлуатації вкрадених реквізитів [1, 3]. Ця стаття містить загальний огляд історії створення даної технології, принцип її роботи та шлях розвитку.

З технічного боку платіжні картки виявилися захищеними настільки добре, що найслабшою ланкою при здійсненні платежів залишилась людина. В той самий час реальний досвід показав, що впровадження додаткових ступенів захисту може знизити зручність користування для кінцевого користувача і зменшити конверсію — частку платежів, що успішно завершуються. Втрата конверсії означає, наприклад, що магазин недоотримає прибуток, а власник картки не здійснить бажану покупку.

Аналіз останніх досліджень і публікацій. Наприкінці 1990-х років Інтернет почав стрімко проникати у повсякденне життя людини. Канал продажів через мережу відкрив нову сторінку в історії торгівлі і викликав дуже швидке зростання дистанційних платежів банківськими картами. Так само стрімко почала збільшуватись частка шахрайства з інтернет-картами, оскільки для здійснення платежу достатньо було мати лише номер картки та термін її дії.

Платіжні системи зреагували на нову загрозу введенням нового захисного параметра — CVV коду, який друкується на звороті картки. Він має гарантувати, що платіж здійснює саме власник картки. Однак через малу довжину коду (3 символи) існує можливість підглянути його під час оплати товарів на касі або отримати шляхом крадіжки фізичної картки.

Так гостра необхідність захистити дистанційні платежі сприяла появі першого стандарту безпеки — 3D Secure. Він додає для онлайн-платежів ще один крок — аутентифікацію держателя, що дозволяє банку переконатися, що платіж ініціював саме держатель картки, аби захиститися від шахрайських операцій.

Вперше розроблена у 1999 р. для Visa Inc., технологія 3D Secure вже понад 20 років забезпечує безпеку інтернет-платежів [2, 4].

Схема роботи 3D Secure 1.0.2. Протокол описує взаємодію трьох сторін (доменів), що і відображено у назві «3D». Ухвалення рішення про можливість здійснення операції з залученням трьох незалежних доменів стало основною ідеєю технології.

Виділимо ці домени та зони їхньої відповідальності [4, 8].

- *Домен емітента* містить власника картки та банк, який випустив цю картку (банк-емітент). У зоні відповідальності цього домену лежить автентифікація власника картки, тобто підтвердження факту легітимного володіння карткою особою, яка здійснює операцію. Основним 3DS-компонентом у домені емітента є ACS (Access Control Server).
- *Домен еквайра* включає інтернет-магазин і банк, що обслуговує його рахунок та операції (банк-еквайр). Цей домен відповідає за вибудовування комерційних відносин із покупцем, а також за проведення фінансової складової операції через платіжну систему. Саме з домену еквайра ініціюється проведення платіжної операції. Основним 3DS-компонент у домені еквайра є MPI (Merchant Plugin Interface).
- *Домен взаємодії* — це платіжна система (ПС). Платіжна система забезпечує взаємодію між доменом еквайра та доменом емітента, встановлює правила цієї взаємодії, визначає вимоги до безпеки, а також надає можливість здійснення фінансової частини операції. Основним 3DS-компонент у домені ПС є DS (Directory Server).

Після визначення основних складових перейдемо до технічної реалізації. Протокол 3D Secure побудований поверх HTTPS протоколу з використанням повідомлень у форматі XML для передачі між доменами. Спрощену схему роботи подано на рис. 1.

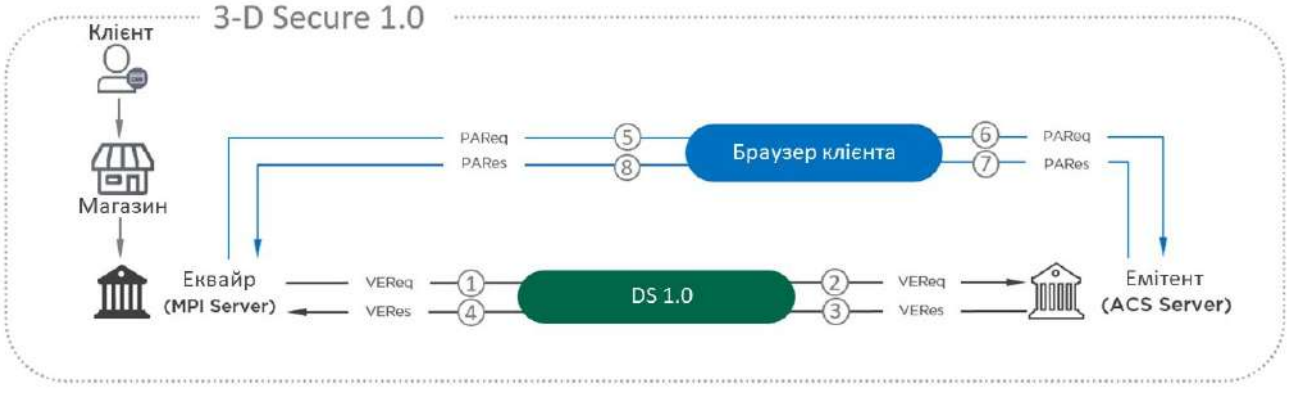

Рис. 1. Загальна схема роботи протоколу 3DS 1.0

Джерело: розроблено авторами.

Виконання платежу складається з таких кроків [8].

1. Утримувач картки оформляє замовлення в інтернет-магазині з оплатою онлайн, на платіжній сторінці вводить реквізити картки та натискає кнопку «Сплатити».

2. Дані з платіжної сторінки передаються до MPI.

3. MPI надсилає до DS повідомлення VEReq (Verification Request) (1) з номером картки та даними про інтернет-магазин.

4. DS перевіряє VEReq-повідомлення, визначає банк-емітент картки та відправляє повідомлення VEReq (2) до ACS.

5. ACS перевіряє VEReq-повідомлення та визначає можливість проведення автентифікації покупця за 3D Secure, після чого формує повідомлення VERes (Verification Response) (3). Якщо проведення автентифікації можливе, в VERes передається URL сторінки ACS, на яку повинен бути перенаправлений користувач. Повідомлення VERes передається до DS.

6. DS перевіряє повідомлення VERes і повертає його назад до MPI (4).

7. MPI формує повідомлення PAReq (Payment Request) (5) з інформацією про операцію та технічними даними від ACS. Повідомлення передається через браузер на URL-адресу ACS, отриману в VERes.

8. ACS у відповідь на запит браузера PAReq (6) повертає форму автентифікації власника картки. Утримувач бачить поле введення одноразового пароля.

9. Утримувач вводить отриманий за sms/push код і натискає кнопку «Підтвердити», код відправляється в ACS;

10. ACS перевіряє код та формує повідомлення PARes (Payment Response) з результатом автентифікації та даними для виконання фінансової складової операції. Повідомлення PARes (7) передається через браузер на адресу MPI.

11. MPI отримує від браузера PARes (8), перевіряє повідомлення, включаючи підпис, а у разі успішної перевірки — ініціює проведення фінансової частини операції (авторизації).

12. MPI отримує результат проведення авторизації та перенаправляє браузер назад в інтернет-магазин, власник картки бачить результат проведення платежу.

Як бачимо, у процесі 3DS-автентифікації відбувається обмін технічною інформацією між декількома залученими сторонами і при цьому процес виглядає досить просто.

Етапи розвитку 3D Secure в Україні. Технологія 3DS стала принципово новим явищем у платіжному просторі країни, тому її входження на український ринок було непростим. Як наслідок,

використання 3DS спочатку сильно підірвало транзакційний потік (конверсію).

Згадаємо, які методи використовували банки для перевірки клієнта [1, 4].

– *Статичний пароль* — найбільш простий спосіб, який було впроваджено одним із перших. При першому платежі з інтернет-магазину клієнт переадресовувався на ACS, де мав вигадати пароль і заповнити форму. Створений пароль прив'язувався до карти і під час наступних платежів з'являлася сторінка автентифікації, де потрібно було його вводити. Перевагами цього способу була відносна простота і можливість швидко змінити пароль за необхідності, тому деякий час цей спосіб автентифікації вважався безпечним та зручним. Але незабаром безпека статичних паролів почала падати і через кілька років після запуску вони перестали вважатися безпечними, тому платіжні системи не рекомендують використовувати їх для 3DS-автентифікації.

– *Скретч карта* — це карта, на якій інформація знаходиться під шаром, що стирається. Для 3D Secure випускалися подібні карти, на кожній знаходилося кілька одноразових паролів. Клієнти отримували ці картки у відділеннях банків. У разі чергового платежу на сторінці ACS потрібно було ввести один із паролів зі скретч-картки. Такий підхід забезпечував більш високий рівень безпеки, але виникали інші проблеми: одноразові коди на карті закінчувалися або, якщо карта губилася, доводилося йти у відділення банку за новою. Клієнти забували про це і стикалися з проблемою вже під час проведення платежу. У результаті падала і конверсія, і задоволеність клієнта.

– *Коди на чеку* — підхід, схожий із попереднім варіантом, але тут одноразові коди друкувалися на чеку під час операції в банкоматі, де отримувати їх було зручніше, ніж у відділеннях. Але чеки також можна було вкрасти, а в банкоматах з'явився інший спосіб: маючи дублікат карти, зловмисник міг зняти гроші, отримати коди та розплатитись в інтернеті.

– *CAP-ридер* (*Chip Authentication Program*) — пристрій, схожий на сучасні мобільні термінали, при отриманні картки видавався клієнту. У нього вставлялася карта, вводився код доступу і на екрані генерувався одноразовий пароль. Такий підхід забезпечував високий криптографічний захист, але не отримав масового поширення через високу вартість CAP-ридера та незручність використання.

– *Display Card* — банківська картка з генератором випадкових паролів. Такі карти були зручні і безпечні, оскільки генератор паролів завжди був під рукою і мав стійкий криптографічний захист. Але були й серйозні мінуси, які не дозволили подібним

картам поширитися масово. Насамперед це вартість, яка не розрахована на масового клієнта. Крім того, у карті було присутнім автономне джерело живлення, яке могло розрядитися раніше закінчення терміну дії картки, і в цілому подібні карти були більш вразливі до механічних впливів.

Сьогодні багатьма банками використовується гібридна система з push- та sms-повідомлень. Такий підхід виправданий, оскільки додаток банку може бути не встановлений, працювати некоректно або ж клієнт може не мати доступу до інтернету. У цьому випадку використовується SMS. Проте спосіб автентифікації за допомогою OTP (одноразовий пароль) перестає задовольняти сучасним вимогам зручності при здійсненні платежів, а шахраї знаходять все нові шляхи та можливості отримання OTP у клієнтів.

Виклад основного матеріалу. Понад двадцять років перша версія протоколу 3DS вирішує поставлене перед нею завдання забезпечення безпеки дистанційних платежів. Проте будь-яка технологія застаріває, і з часом виявилися деякі особливості 3DS 1.0, які зажадали таких поліпшень [4, 5]:

- *Підвищення конверсії*. Який би спосіб автентифікації не використовувався, будь-яке додаткове підтвердження платежу клієнтом створює бар'єр для завершення оплати, від чого страждає і сам клієнт, і магазин. Причини, з яких платіж не завершується, можуть бути різними:

– недовіра клієнтів до спливаючих вікон і введення в них кодів, страх бути обдуреним;

– нерозуміння що саме потрібно зробити для підтвердження оплати;

– помилки при введенні, введення іншого значення;

– погане інтернет-з'єднання, проблеми переадресації на ACS або назад із ACS до магазину;

– відсутність доступу до телефону, прив'язаного до картки;

– проблеми з відправкою SMS на стороні банку або з доставкою SMS на телефон клієнта.

- *Адаптація до мобільних пристроїв*. Платіжні системи при сертифікації емітентів за технологією 3D Secure 1.0 накладали певні вимоги щодо розміру та змісту сторінки автентифікації. Дані вимоги сильно обмежують веброзробника у верстці цих сторінок. У разі використання мобільного пристрою, частка оплат з яких зростає щороку, користувач стикається з наступною проблемою: надавана емітентом HTML-форма виглядає сторонньо в GUI мобільного додатка, її масштаб і розміщення можуть бути незручними для користувача.

- *Підвищення рівня захисту від шахрайства* із застосуванням соціальної інженерії. Жоден метод автентифікації за 3DS 1.0 не забезпечує дійсно надійного захисту платежу від методів шахрайства, відомих за загальною назвою «соціальна інженерія». Одноразовий код шахраї можуть дізнатися безпосередньо у клієнта, ввівши його в оману. Наприклад, шахрай представляється співробітником служби безпеки банку та повідомляє про здійснення підозрілої операції по картці клієнта. Для її скасування необхідно назвати код, який прийде за SMS або PUSH. У цей час за скомпрометованими реквізитами картки шахраєм здійснюється операція грошового переказу, для якої і запитується код підтвердження.
- *Поліпшення користувацького досвіду*. За останні 20 років банки привчили клієнтів, що введення OTP — це нормально. Але насправді менше як 0,05 % всіх операцій є шахрайськими. Тобто майже по всіх операціях із введенням OTP пароль насправді не потрібен, оскільки операцію проводить легітимний власник картки.

Для вирішення цих завдань була розроблена наступна версія протоколу — EMV 3DS 2.0.

Народження EMV 3D Secure. У середині 2010-х моральне та технічне старіння 3DS 1.0.2 підштовхнуло консорціум EMVCo (організація, що займається розробкою стандартів у сфері платіжних технологій) до розробки нової версії протоколу, який отримав назву EMV 3D Secure 2.0. Він схожий на попередника, але має низку істотних покращень [6, 8].

Перша чорнова версія специфікації EMV 3DS мала номер 2.0.1. Перша робоча версія має номер 2.1.0. Перерахуємо її основні можливості та особливості:

- *Frictionless-автентифікація*. За допомогою ризикового аналізу протокол дозволяє (Risk-based analysis, або RBA) виконати Frictionless-аутентифікацію, тобто підтвердження належності картки платнику відбувається без його безпосередньої участі. Це одне з найважливіших нововведень, яке і спричиняє основні переваги нового протоколу: зручність для клієнта та підвищення рівня конверсії для торгівельно-сервісних підприємств (ТСП).
- *Підтримка кількох каналів проведення автентифікації*:

– браузерний (browser-based, або BRW) — звичний канал оплати з інтернет-магазину через браузер на десктопі, мобільному пристрої тощо;

– з програми (application-based, або APP) — 3DS-автентифікація виконується безпосередньо з мобільного додатку, при цьому за реалізацію функцій EMV 3DS відповідає спеціальна

інтегрована у програму бібліотека. Це дозволяє поліпшити користувацький досвід, оскільки автентифікація проходить у нативному оточенні платіжного додатку. При цьому збираються додаткові дані про пристрій, що важливо для впізнавання ризиковою машиною клієнта і підвищує безпеку операції, що проводиться;

– ініційований ТСП (3DS requestor initiated (3RI)) — ініціюється магазином самостійно без запиту власника. Цей канал може бути використаний для передплат, регулярних платежів тощо.

- *Підтримка двох категорій автентифікації*:

– платіжна (Payment, або PA) — власник автентифікується для того, щоб провести оплату товару чи послуги, здійснити грошовий переказ;

– неплатіжна (Non-Payment, або NPA) — власник автентифікується під час здійснення операції, яка не передбачає подальшого руху коштів. Це може бути прив'язка карти до сервісу, перевірка при токенізації картки тощо.

- *Захищеність інформаційних потоків*. На відміну від першої версії 3DS 1.0.2, в якій прикладні дані передаються через браузер, усі значущі дані в EMV 3DS передаються через захищене середовище безпосередньо між компонентами платіжної 3DS-інфраструктури. Пристрій користувача використовується лише для виконання технічних запитів при взаємодії з ACS емітента;
- *Підтримка гнучкої системи ризикового аналізу*, яка, крім виконання Frictionless, може також реагувати на загрози. Якщо система фіксує нетиповий для даного клієнта грошовий переказ, наприклад, з незнайомого пристрою або з іншої країни, то така операція може бути заблокована або вимагати посилених методів автентифікації. Для підтвердження може знадобитися не тільки введення одноразового пароля, але й відповіді на додаткові питання контролю або введення біометричних даних. Очевидно, стовідсоткового захисту від соціальної інженерії не існує, але дана технологія знижує можливість успішного шахрайства порівняно з першою версією 3DS [7].

Як бачимо, наявні проблеми 3DS 1.0.2 значною мірою вирішуються EMV 3DS 2.0. Крім того, протокол активно розвивається, платіжні системи та банки займаються впровадженням його наступної версії — 2.2.0.

Схема роботи EMV 3D Secure 2.0. Протокол 3D Secure 2.0 побудований поверх HTTPS протоколу з використанням повідомлень у форматі JSON. Склад доменної моделі не змінився порівняно з 3DS 1.0. Основні зміни стосуються саме схеми роботи, спрощена модель якої представлена на рис. 2.

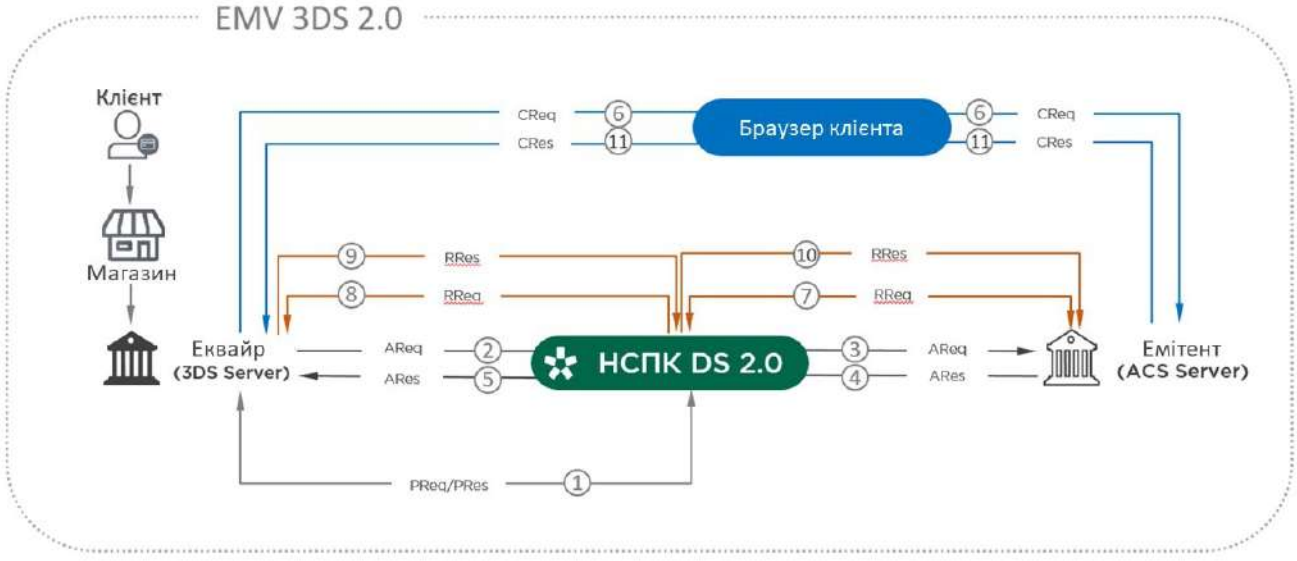

Рис. 2. Загальна схема роботи протоколу 3DS 2.0

Джерело: розроблено автором.

У EMV 3DS доданий новий інформаційний потік між 3DS Server (MPI у минулій версії) та DS. У ньому 3DS Server періодично отримує з DS запитом PReq (1) інформацію про підписані на протокол карткові діапазони емітентів та їх параметри. У повідомленні PRes компонент DS для кожного карткового діапазону повертає підтримувану версію протоколу, додаткові опції, а також адресу 3DS Method URL. 3DS Method URL — це URL-адреса компонента ACS, яка має викликатися 3DS Server-ом у браузері перед автентифікацією користувача. Завдяки цьому виклику ACS може виконати ідентифікацію пристрою, зібрати його параметри та при отриманні запиту на автентифікацію зв'язати його з цими даними.

Нові можливості в EMV 3DS 2.2.0. Випущена наприкінці грудня 2018 року версія специфікації 2.2.0 містить важливі нововведення та покращення [4][8]:

Платіжна автентифікація у 3RI каналі. У 2.1.0 версії для 3RI була можлива лише неплатіжна автентифікація (NPA), доречна при прив'язці карти до особистого кабінету, електронного гаманця тощо, що не є затребуваним для операцій, які ініціюються ТСП без участі власника. У 2.2.0 стала можлива реалізація платіжної автентифікації (PA) у рамках 3RI. Причому сценарій автентифікації можливий як Frictionless, і Challenge. В останньому випадку використовується новий підхід до автентифікації — Decoupled Authentication.

Decoupled Authentication або відкладена автентифікація — це підхід, при якому перевірка власника картки може бути відкладена у часі. Метод автентифікації, який використовуватиметься при цьому, залишається на розсуд емітента. Наприклад, це може бути дзвінок з банку у зручний для клієнта час, запит підтвердження електронною поштою або через мобільний додаток. Ключовим аспектом відкладеної автентифікації є те, що підтвердження необов'язково потрібне в конкретний момент проведення операції, а може бути виконано протягом тривалого часу (до 7 днів).

Whitelisting. Ще одне нововведення специфікації 2.2.0 — можливість для клієнта додати ТСП (інтернет-магазин чи іншу компанію, на адресу якої здійснюється оплата) до списку довірених (whitelist) на стороні емітента. На сторінці автентифікації власник має можливість підтвердити додавання до білого списку даного ТСП. Обов'язковою умовою додавання до білого списку є успішно проведена автентифікація за challenge-сценарієм. При цьому ACS додатково може проінформувати 3DS Server про успішне

додавання цього магазину до білого списку. За підсумками емітент може проводити наступні операції з цього ТСП по тій самій карті без додаткового звернення до власника картки, тобто по frictionless-сценарію, оскільки клієнт дав на це усвідомлену згоду. Крім того, банк-еквайр при наступних сплатах також може вимагати проведення операції за frictionless-сценарієм на підставі того, що ТСП знаходиться в білому списку. Утримувач картки отримує контроль над тим, у яких магазинах він дозволяє оплату без додаткового підтвердження, що у результаті покращує користувацький досвід. Магазинотримує збільшення конверсії, оскільки прибирається зайвий бар'єр у вигляді обов'язкового підтвердження операції. За змістом whitelisting є простим і дешевим способом реалізувати переваги EMV 3DS 2.0 без створення складної RBA-машини.

Висновки. Подальше проникнення EMV 3DS 2.0 у платіжну інфраструктуру призведе до ширшого використання RBA та зниження частки операцій, які потребують підтвердження від клієнта. Робота з поліпшення якості даних і збагачення їх опціональними реквізитами платежу ще більше посилять цю тенденцію [1, 9].

Сьогодні відсутність підтвердження операції одноразовим кодом усе ще викликає стурбованість пересічного користувача. Однак протягом кількох років ситуація зміниться, і питання викликатиме вже запит банком додаткового підтвердження під час здійснення типового платежу. Найбільш технологічні та сучасні гравці ринку вже сьогодні перестають вимагати додаткове підтвердження операцій, які відповідають типовому купівельному профілю власника картки.

Впровадження нових можливостей, таких як відкладена автентифікація та білі списки, ще більше ускладнить 3DS-інфраструктуру, але при цьому запропонує кінцевому користувачеві банківської картки гнучкість та можливість змінювати платіжні налаштування під себе, що ще більше покращить зручність карткових платежів.

Перехід платіжних програм на роботу з інтегрованим SDK (software development kit) підвищить швидкість та зручність процесу підтвердження операції. При цьому завдяки передачі відбитка пристрою також значно підвищиться рівень «впізнавання» емітентом свого клієнта. Частка операцій, що вимагають підтвердження, стрімко зменшуватиметься з поширенням таких додатків та їх активним використанням власниками карток для оплати товарів та послуг.

Платіжна автентифікація для merchant-initiated платежів також підвищить конверсію платежів за підписками на регулярні сервіси, які стають особливо затребуваними останніми роками разом із переходом на сервісну модель споживання.

Отже, у найближчі кілька років ми припускаємо вирішення більшої частини проблем, пов'язаних зі спадщиною технології 20-річної давності, 3D Secure 1.0.2, і зміну на краще користувацького досвіду при здійсненні інтернет-платежів банківськими картками.

Бібліографічні посилання

1. Конверсія вища, ризики нижчі: як технологія 3ds 2.1 підніме дохід інтернет-магазину. *Finance.ua.* URL: https://web.archive.org/web/20200929063156/https://news.finance.ua/ua/news/-/479051/konversiya-vyshha-ryzyky-nyzhchi-yak-tehnologiya-3ds-21-pidnime-dohid-internet-magazynu
2. Технологія 3D Secure — безпечні розрахунки картками в інтернеті / ОТП Банк Україна. URL: https://www.otpbank.com.ua/privateclients/pay-cards/3dsecure/
3. 3D Secure. *Вікіпедія — вільна енциклопедія*. URL: https://uk.wikipedia.org/wiki/3-D_Secure
4. 3D Secure. *Wikipedia*. URL: https://en.wikipedia.org/wiki/3-D_Secure
5. Card authentication and 3D Secure. URL: https://stripe.com/docs/payments/3d-secure
6. Burdett, D. FRC 2801: Internet Open Trading Protocol — IOTP. Version 1.0E. April 2000, 290 p.
7. Murdoch, Steven J.; Anderson, Ross, Sion, R. (ed.). Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication (PDF). URL: https://www.cl.cam.ac.uk/~rja14/Papers/fc10vbvsecurecode.pdf
8. Verified by Visa Implementation Guide (PDF). URL: https://usa.visa.com/dam/VCOM/download/merchants/verified-by-visa-acquirer-merchant-implementation-guide.pdf
9. What is 3D Secure? And Its Advantages for E-commerce. MONEI. URL: https://monei.com/blog/what-is-3d-secure-and-its-advantages-for-e-commerce/

Статтю подано до редакції 22.11.2022