МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря Сікорського»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ПРРКС

“Дослідження криптографічних протоколів систем WebMoney, PayPal”

Виконали:

Студенти групи ФІ-22мн
Бондаренко Андрій
Яценко Артем

Київ – 2023

Платіжна система. Визначення

Колектив авторів однієї із найвідоміших економічних книг України – Економічної енциклопедії за редакцією С. В. Мочерного, поняттю **«платіжна система»** надають три значення:

1) об'єднання адміністрації, розрахункового банку, еквайра, процесингового центру на основі єдиних нормативних, договірних, фінансових і технічних документів, що регламентують взаємовідносини учасників системи, а також правила і порядок надання автоматизованих послуг з використанням платіжних карток;
2) платіжна організація, члени платіжної системи, учасники платіжної системи та відносин, що виникають між ними при здійсненні розрахунків за операції, що виконуються із використанням платіжних карток цієї системи;
3) сукупність нормативних, договірних, фінансових та інформаційно-технічних засобів і рішень учасників (банків, установ, компаній), які регламентують свої взаємовідносини щодо порядку використання банківської платіжної картки.

Електронна платіжна система, також відома як цифрова платіжна система або система електронних платежів, - це спосіб здійснення фінансових операцій в електронному вигляді, без необхідності використання фізичної валюти або традиційних паперових засобів, таких як чеки або готівка. Вона передбачає обмін коштами між покупцями та продавцями або між сторонами, що беруть участь у транзакції, за допомогою електронних засобів. Вона має багато форм, таких як кредитна картка, віртуальна картка, поштове замовлення, електронний гаманець, мобільний платіж, криптовалюта тощо.

Характеристики ЕПС

1. **Кредитні/дебетові картки**

Це електронні платежі, які здійснюються за допомогою кредитної чи дебетової картки споживача. Платіж обробляється через мережу карток, наприклад Visa або Mastercard, а кошти переказуються з банківського рахунку споживача на рахунок продавця.

Цими електронними платіжними системами можна користуватися у звичайних магазинах, протягнувши картку в POS, і для онлайн-покупок, додавши дані картки на платіжну сторінку.

2. **Електронні гаманці**

Це цифрові гаманці, які дозволяють споживачам зберігати дані своїх кредитних/дебетових карток, а також іншу особисту інформацію в безпечному онлайн-розташуванні. Тут оплата здійснюється шляхом додавання коштів у гаманець з банківського рахунку користувача, пов'язаного з гаманцем. Це може бути переказ з гаманця на гаманець або з гаманця в банк.

3. **Інтернет-банкінг**

Онлайн-банкінг – це онлайн-портал банківського рахунку користувача, створений відповідними банками. За допомогою цього порталу користувач може здійснювати прямі міжбанківські перекази в тому самому банку або в інші банки.

Іншою версією цього рішення є додаток мобільного банкінгу, який виконує ті ж функції, що й онлайн-портал. Дивлячись на збільшення кількості Інтернету та смартфонів, банки придумали це рішення.

4. **Платежі за допомогою QR-коду**

Платежі за допомогою QR-коду здійснюються шляхом сканування коду швидкого реагування (QR), який є типом штрих-коду, який можна сканувати камерою смартфона. QR-код містить інформацію про транзакцію, наприклад інформацію про обліковий запис продавця та суму покупки. Ці платежі можна здійснити через гаманець або банківський додаток. Це одна з найпопулярніших платіжних систем у світі.

5. **Безконтактні платежі**

Безконтактний платіж – це спосіб оплати за допомогою технології NFC та RFID. У цьому способі потрібно торкнутися платіжного пристрою або картки біля POS-терміналу. Ці безконтактні електронні платежі також відомі як одноразові платежі.

Під час користування безконтактними електронними платіжними пристроями не потрібно міняти картки або вводити будь-який PIN-код. Коли система продавця підкаже, клієнту потрібно піднести свій пристрій або картку ближче, щоб здійснити оплату. Потім інформація передається з магнітного чіпа в банк.

Багато компаній використовують цю електронну платіжну систему для зручності та пришвидшення операцій. Хоча клієнти вважають його дуже простим у використанні та зручним водночас.

6. **Платежі ACH**

Платежі ACH або платежі Automated Clearing House — це електронні платежі, які здійснюються через мережу ACH. Ця мережа використовується для обробки фінансових операцій, включаючи прямі депозити, оплату рахунків та електронні чеки. Платежі ACH дешевші, ніж платежі картками, і їх можна використовувати як для дебетових, так і для кредитних операцій.

Важливо зазначити, що платежі ACH не можна відмінити, тому споживачам важливо переконатися, що на їхніх рахунках достатньо коштів для покриття транзакції.

7. **Міжнародний переказ**

Міжнародний грошовий переказ означає переказ грошей іноземним працівником своїй родині у своїй країні. У багатьох країнах міжнародні грошові перекази становлять значну частину ВВП.

Сьогодні мобільні гаманці спростили грошові перекази за допомогою міжнародних грошових переказів. Він пропонує кілька функцій, щоб зробити перекази легкими, швидкими та безпечними. Використовуючи мобільні гаманці, ви можете встановити фіксовані курси обміну для

переказу грошей. Ви також можете дозволити своїм клієнтам заздалегідь визначити курс обміну валют.

8. **Однорангові платежі**

Однорангові платежі дозволяють здійснювати перекази між двома сторонами за допомогою кредитних карток або дебетових карток через програму платіжного електронного гаманця. Щоб налаштувати платіж P2P, вам потрібно зареєструватися за допомогою банківського рахунку, пов'язаного з кредитною або дебетовою карткою.

Після налаштування облікового запису ви можете почати переказувати гроші своїм друзям і родині. Час переказу грошей у одноранговому переказі відрізняється від одного постачальника послуг до іншого.

Крім згаданих вище основних електронних платіжних систем, існують різні інші системи, як-от переносні пристрої, біометричні платежі, оплата за допомогою ШІ, криптовалюта, віртуальні картки тощо.

Як працює оплата кредитної картки?

Власники та керівники компаній, як правило, також є кмітливими споживачами. Це зрозуміло, оскільки ви регулярно оцінюєте багато продуктів і послуг, необхідних для безперебійної роботи вашого бізнесу.

Прийом кредитних карток дає змогу отримувати гроші. Це означає, що вам потрібно вибрати компанію, яка займається обробкою кредитних карток. Оператори кредитних карток є важливими партнерами, окрім основної послуги обробки платежів, що робить це критично важливим бізнес-рішенням. Вам не потрібно ставати експертом, але ви станете кращим споживачем, якщо знаєте, як працює процес обробки кредитних карток.

Щоб зрозуміти, як працює обробка платежів, ми розглянемо акторів і їхні ролі.

Хто бере участь у транзакціях з кредитними та дебетовими картками?

- **Власник картки** отримує кредитну або дебетову картку від банку-емітента, використовує рахунок для оплати товарів або послуг.
- **Продавець** – це будь-який вид бізнесу, який приймає платежі карткою в обмін на товари чи послуги.
- **Торговий банк** відкриває та підтримує торгові рахунки. Торговельні банки дозволяють торговцям приймати депозити від платежів кредитними та дебетовими картками.
- **Платіжні процесори** – це компанії, які обробляють транзакції з кредитних і дебетових карток. Платіжні процесори з'єднують продавців, торговельні банки, мережі карток та інших, щоб зробити платежі картками можливими.
- **Банки-емітенти** – це банки, кредитні спілки та інші фінансові установи, які видають дебетові та кредитні картки власникам карток через карткові асоціації.
- **Карткові асоціації** включають Visa, Mastercard, Discover і American Express. Карткові асоціації встановлюють курси обміну та кваліфікаційні рекомендації, а також виконують роль арбітра між банками-емітентами та банками-еквайрами, серед інших життєво важливих функцій.

Як виглядає обробка кредитної картки в русі?

Обробка кредитної картки складається з трьох різних процесів:

1. Авторизація
2. Поселення
3. Фінансування

Спочатку розглянемо процес авторизації кредитної та дебетової картки.

1. Власник картки надає свою картку (проведіть, торкніться, вставте або іншим безпечним способом, наприклад безконтактним способом

або шляхом введення номера для онлайн-оплати кредитною карткою) продавцю в обмін на товари чи послуги. Запит може надходити з терміналу кредитної картки або системи торгових точок у звичайному магазині, шлюзу веб-сайту електронної комерції, через мобільний пристрій або прийом платежів у програмі.
2. Продавець надсилає запит на авторизацію платежу своєму платіжному процесору.
3. Платіжний процесор надсилає транзакції відповідній картковій асоціації, зрештою досягаючи банку-емітента.
4. Запити на авторизацію надсилаються до банку-емітента, включаючи такі параметри, як CVV, перевірка AVS і термін дії.
5. Банк-емітент схвалює або відхиляє транзакцію. Трансакції можуть бути відхилені через недостатню кількість коштів або доступний кредит, якщо обліковий запис власника картки закрито або термін його дії закінчився, якщо платіж прострочений або інші фактори.
6. Потім банк-емітент надсилає статус схвалення (або відмови) назад по лінії до асоціації карток, торгового банку і, нарешті, продавцю.

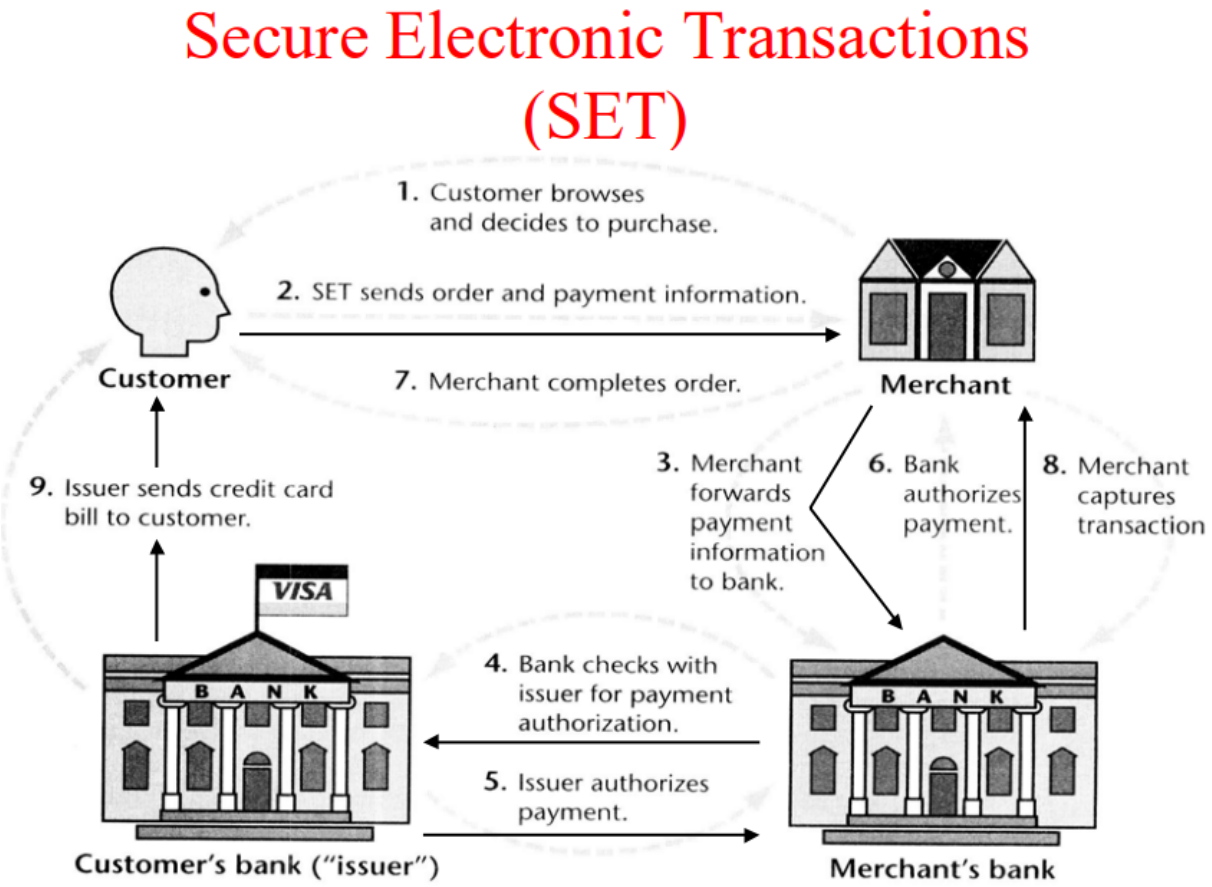
Коротко про процес авторизації кредитної картки. Процес авторизації картки займає лічені секунди.

Тепер давайте розглянемо процес розрахунків за кредитною карткою та фінансування. Ця частина, по суті, полягає в тому, як продавець отримує гроші з кредитних карток, які вони приймають.

1. Продавці надсилають пакети авторизованих транзакцій до свого платіжного процесора.
2. Платіжний процесор передає деталі транзакції асоціаціям карток, які передають відповідні дебети банкам-емітентам у своїй мережі.
3. Банк-емітент стягує з рахунку власника картки суму операцій.
4. Потім банк-емітент переказує відповідні кошти для транзакцій торговому банку за вирахуванням комісій за обмін.
5. Торговий банк перераховує кошти на рахунок торговця.
6. Процеси розрахунків і фінансування, які раніше тривали днями, тепер майже завжди виконуються за ніч, що допомагає продавцям швидко отримувати гроші.

Це спрощений процес оплати кредитною карткою.

Set специфікація



- **SET = Secure Electronic Transactions**
  - Стандарт від Visa та MasterCard 1996 року
  - Сьогодні майже не має значення (після спроби відродити його в 1999 році)
  - Але все ще є зразком ґрунтовного підходу до вирішення проблеми
- Сфера застосування обмежена авторизацією платежів за допомогою кредитних карток
  - Відсутність фактичного переказу коштів
- Фокус на моделі довіри та авторизації
  - Використання криптосистеми з відкритим/закритим ключем
- Складна (три томи специфікації)
  - Але захищена від усіх основних ризиків
- Спеціальна PKI: всі учасники повинні отримати сертифікати (X.509)
  - "Центр сертифікації бренду" (MasterCard/Visa)
  - Геополітичний орган (необов'язково)

    - Власник картки / Пропадавець / Платіжний центр платіжний центр

Ініціалізація SET

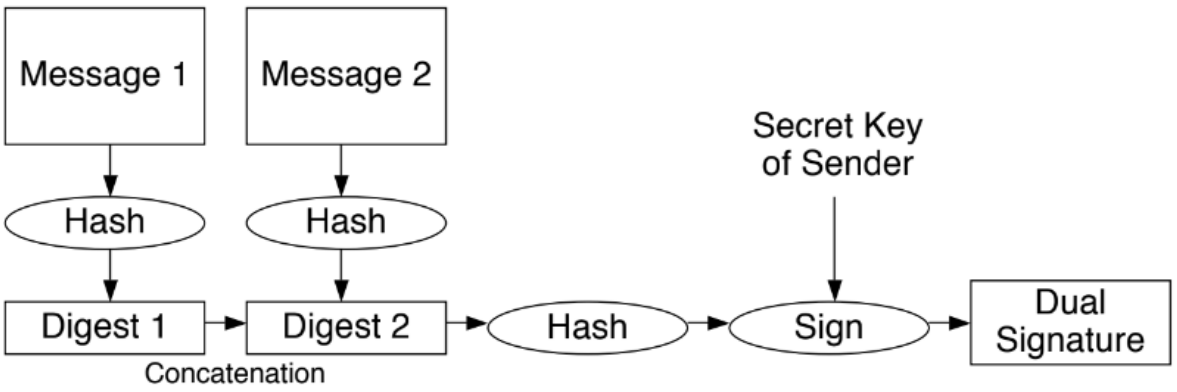
- Ініціалізація (PInitReq):
    - Від власник картки до продавця
    - Містить: Бренд картки, список сертифікатів, "challenge" (для забезпечення свіжості)
- Відповідь на ініціалізацію (PInitRes):
    - Від продавця до власника картки
    - Містить: Ідентифікатор транзакції, відповідь на виклик, сертифікати, "виклик продавця"

- Ролі:
    - Власник картки (Покупець)
    - Торговець (Продавець)
    - "Еквайр" (по суті, організація, що видає кредитні картки)
        - Управління "платіжним шлюзом"

Подвійні підписи

- Загальна концепція:
- Аліса хоче відправити Повідомлення 1 Бобу і Повідомлення 2 Керол, і вона хоче запевнити Боба і Керол, що відповідне інше повідомлення існує

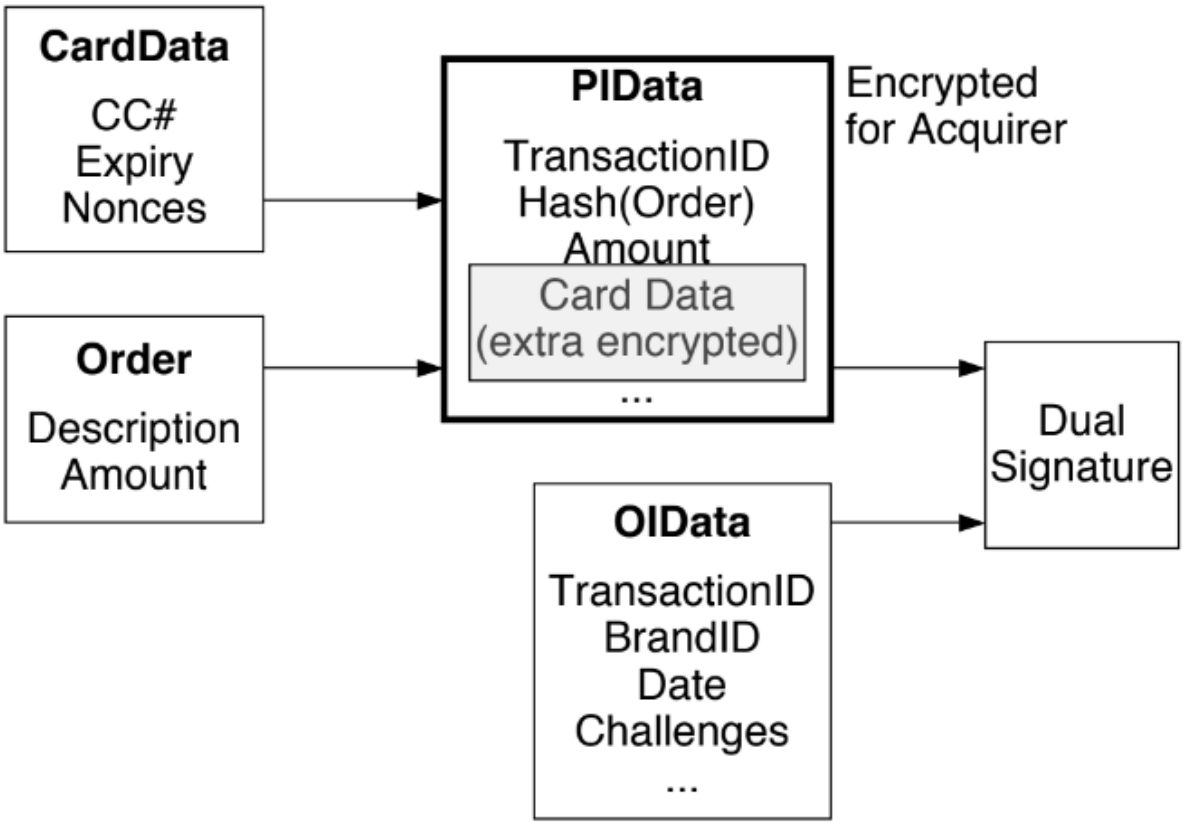
    - Бобу вона відправляє Повідомлення 1 і Дайджест 2
    - Керол вона надсилає Повідомлення 2 і Дайджест 1



SET. Купівля

- Замовлення на покупку (PReq):
  - Держатель картки продавцю
  - Інформація про замовлення (OI):
    - Ідентифікує опис замовлення у продавця
    - Містить відповідь на виклик продавця
    - Містить випадкову інформацію ("nonce") для захисту від словникових атак
  - Платіжні інструкції (PI):
    - Дані картки, сума покупки, хеш замовлення, ідентифікатор транзакції
    - Платіжні інструкції зашифровані відкритим ключем еквайра (продавець не може їх прочитати)
    - "Надстійке" шифрування з використанням RSA (а не DES, наприклад)
  - Подвійний підпис для OI, що надходить до продавця, та PI, що надходить до еквайра

SET Дані запиту на купівлю



Авторизація SET

- Запит на авторизацію (AuthReq)
  - Від продавця до еквайра
  - Зашифрований відкритим ключем еквайра
  - Підписаний секретним ключем продавця
- Містить TransactionID, суму, Hash(Order), Hash(OIData), PIData, реквізити продавця, платіжну адресу власника картки
  - Hash(Order) міститься двічі
    - безпосередньо від продавця
    - у складі PID-даних (зашифрованих, наприклад, щойно пересланих від держателя картки)
  - Може бути використаний для перевірки того, що власник картки та продавець погодили замовлення деталі
- Відповідь на авторизацію (AuthRes)
  - Від еквайра до продавця

    - Містить TransactionID, код авторизації, суму, дані, токен захоплення (використовується для фактичного переказу коштів)

Електронна готівка та мікроплатежі

Електронна готівка

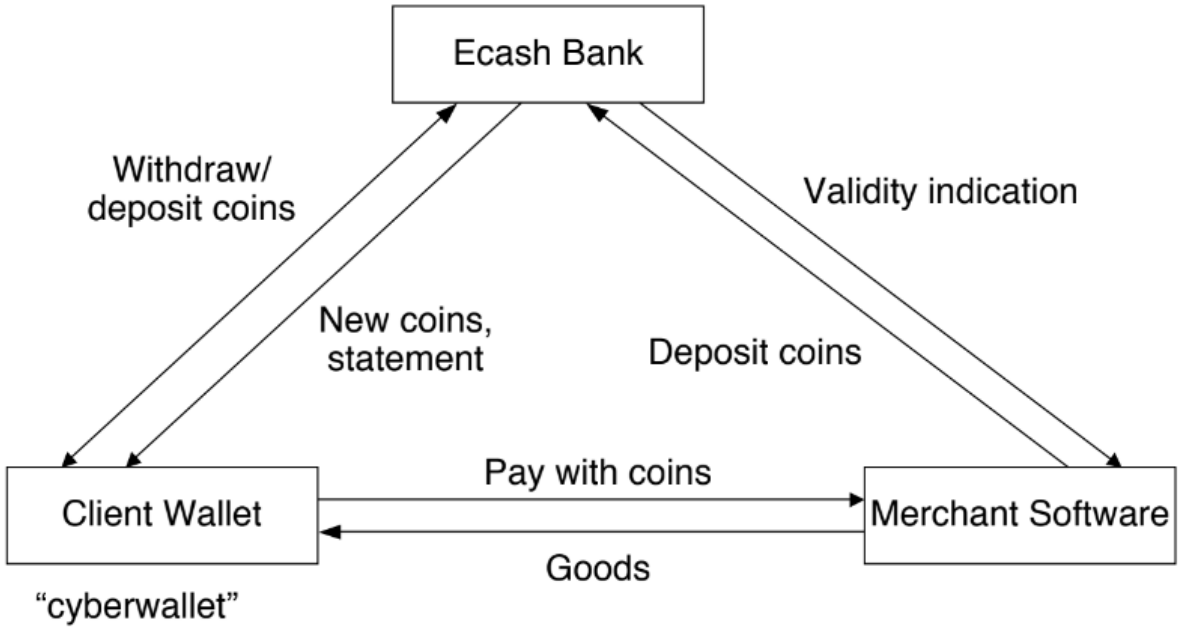
- Було зроблено багато спроб перенести переваги готівкових грошей на цифрові транзакції:
    - Прийнятність незалежно від суми транзакції
    - Гарантований платіж – відсутність ризику скасування пізніше
    - Без комісії за транзакцію
        - немає авторизації, немає відповідного трафіку зв'язку
    - Анонімність
- Не існує електронної системи, яка б фіксувала всі вищезазначені атрибути!
- Але є цікаві наближення...

DigiCash / Ecash

- DigiCash (Девід Чаум)
    - Голландська/США компанія, 1992р
- Електронна готівка
    - Електронний еквівалент готівки, розроблений DigiCash
    - Повністю анонімно з використанням криптографічних методів
- Історія:
    - 1995: Mark Twain Bank, штат Міссурі, почав випуск справжніх доларових монет Ecash.
    - 1998: банкрутство DigiCash

    - Перезапустити як «eCash Technologies»
    - 2002: InfoSpace поглинає компанію eCash Technologies
        - Головним чином для придбання цінних патентів
- Електронна готівка залишається цікавою моделлю електронної готівки

Модель Ecash



Карбування електронних монет

- Кожна монета має серійний номер
    - Серійний номер генерується програмним забезпеченням «кібергаманця» клієнта
    - Вибраний випадковим чином, достатньо великий, щоб уникнути частих дублікатів (наприклад, 100 біт)
- Монети, відповідно їх серійні номери, підписуються банком
    - Банк не знає серійний номер через «засліплення» (див. наступний слайд)
    - Банк не може відстежити, які монети якій людині передано

- Банк використовує різні ключі для різних номіналів монет
    - Наприклад Підписи в 5, 10, 50 центів
- Вміст електронної монети:
    - Серійний номер SN
    - Версія ключа (можна використовувати для отримання вартості, валюти, терміну дії)
    - Підпис: F(SN), зашифрований одним із секретних ключів банку
        - Де F обчислює хеш-код SN і додає деяку зайву інформацію – щоб уникнути підробки монет

Засліплення

- Загальна концепція:
- Аліса хоче, щоб Боб підписав повідомлення так, щоб Боб не бачив його змісту.
- Аналогія: Конверт з повідомленням і аркуш копіювального паперу
    - Підпис на зовнішній стороні конверта проходить крізь повідомлення, що міститься в ньому
- Процедура:
    - Засліплення досягається множенням на випадкову величину (коефіцієнт засліплення)
    - Аліса надсилає помножене (засліплене) повідомлення B(M) Бобу
    - Боб підписує засліплене повідомлення: SignBob(B(M))
    - Функція підпису та засліплення (множення) є комутативними:
        - SignX(B(M)) = B(SignX(M))
    - Аліса де-бліндує повідомлення (діленням із засліплюючим множником)
    - Отримане повідомлення має вигляд SignBob(M), яке неможливо відрізнити від повідомлення, підписаного безпосередньо Бобом

Уникає фальшивих монет

- Припустимо, що функція F опущена
    - Монета містить серійний номер SN у відкритому вигляді
    - Підпис просто SK$1(SN)
- Підробка монети:
    - Вибираємо велике випадкове число R
    - Зашифруйте R за допомогою відкритого ключа банку $1: S = PK$1(R)
    - Створіть монети, які містять S як серійний номер і R як підпис
    - Тепер монету можна перевірити (не відрізнити від справжньої монети):
        - SK$1(S) = SK$1(PK$1(R)) = R
    - Тому введення функції F у визначення монети

Уникнення подвійних витрат

- Електронні монети - це лише фрагменти даних, які можна скопіювати
    - Як уникнути того, що одна й та сама монета витрачається кілька разів?
- Рішення від Ecash:
    - Центральна база даних витрачених монет
    - Торговці повинні мати онлайн-зв'язок з банком Ecash
    - Перш ніж приймати монету: перевірте, чи не була вона вже витрачена
- Проблема:
    - База даних витрачених монет може стати вузьким місцем у роботі
    - Офлайн торгівля монетами неможлива

Купівля Ecash

- Клієнт має монети Ecash на своєму кібергаманці
- Торговець отримує замовлення від клієнта
- Торговець відправляє запит на оплату на гаманець клієнта
    - Сума, позначка часу, опис замовлення, ...
- Користувача запитують, чи хоче він/вона платити
- Монети на (точну) суму знімаються з гаманця
    - З Ecash нічого не змінюється
    - В іншому випадку продавець міг би записати серійні номери своїх монет, виданих клієнту, і спробувати ідентифікувати клієнта
- Монети шифруються відкритим ключем банку при відправці продавцю
    - Торговець просто пересилає їх, але не може нічого прочитати
- Для підтвердження платежу:
    - Клієнт генерує секретний ключ і додає його (хеш) до інформації про платіж.

Ідеальний злочин

Брюс Шнайер:

- Анонімний викрадач бере заручника.
- Викрадач готує велику кількість сліпих монет і надсилає їх у банк як вимогу викупу. в банк як вимогу викупу.
- Банк підписує монети, щоб врятувати заручника.
- Викрадач вимагає, щоб підписані монети були опубліковані, наприклад, в газеті або на телебаченні. Викрадення не можна відстежити. Ніхто, крім викрадача, не може розгледіти монети.
- Викрадач зберігає засліплені монети на своєму комп'ютері, роздруковує їх і має цілий статок в анонімній цифровій готівці
- Сподіваємось, викрадач відпустить заручника...

Офлайн монети

- Чаум/Педерсен 1992, Стефан Брандс 1993:

    - Монети можуть складатися з декількох частин
    - Щоб використати монету в платіжній транзакції, одна частина монети повинна бути розкрита. Платник не ідентифікується.
    - Якщо монета використовується вдруге, розкривається друга частина монети - і платник ідентифікується.
    - Таким чином, можна відстежити подвійні витрати постфактум, а також ідентифікувати походження двічі витрачених монет.

- Алгоритмічна ідея:
    - Ідентифікатор I користувача шифрується одноразовим випадковим числом P
        - є частиною монети
    - Спеціальна система "виклик-відповідь": Мерчант запитує у клієнта відповідь на випадковий виклик і зберігає результати
    - Як тільки у продавця з'являється два результати на різні виклики, він може обчислити інформацію, необхідну для розшифрування особи платника

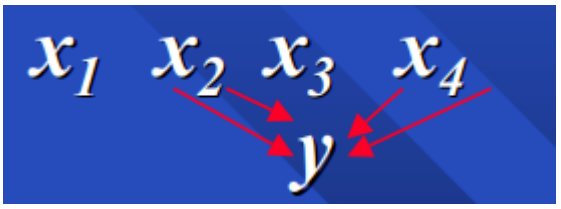
Макроплатежі та мікроплатежі

- Описані вище системи були розроблені для "макроплатежів"
    - Мінімальна деталізація 1 цент (пенні тощо)
- Ціни на послуги часто вказуються в менших кількостях
    - Наприклад, ціни на бензин...
    - Соті або тисячні частки цента
- Мікроплатіж:
    - Платіжна технологія, що підходить для дуже малих сум
- Проблема:
    - Накладні витрати макроплатіжних систем, що перевищують вартість транзакції
- Перевага:
    - Втрата електронної мікромонети не є серйозною шкодою
- Легкі, швидкі, масштабовані протоколи
- Історичний першопроходець: Проект Millicent (1995)
    - Digital Equipment Corporation (поглинута компанією Compaq, яка зараз є частиною HP)

- Ключові інновації: Брокери, що виступають посередниками між постачальниками і scrip (цифрові гроші, дійсні лише для певного постачальника)

PayWord: кредитна схема з використанням ланцюжків : кредитна схема з використанням ланцюжків хеш-значень (або хеш-значень (або платіжних слів платіжних слів)

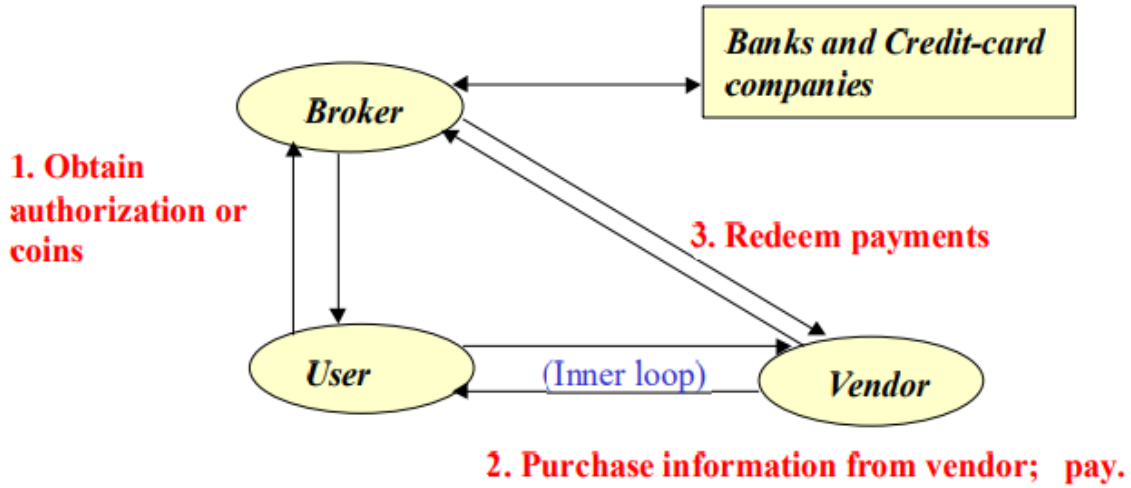
MicroMint: цифрові монети як : цифрові монети як k-way hash -way hash function collisions:



- Схема оплати для транзакцій невеликої вартості, наприклад 1 ¢ за доступ до веб-сторінки
- Занадто малий для «макроплатежів» кредитною карткою (за які може стягуватися комісія 29 ¢ + 2%)
- Криптографія з відкритим ключем відносно дорога:
  - Підписання RSA (приватний ключ) 2 / сек
  - Перевірка RSA (відкритий ключ) 200 / сек
  - Хеш-функція 20000 / сек

Деякі розширені функції, такі як анонімність, є ймовірно, занадто дорогі, щоб реалізувати їх у схемі схемою мікроплатежів.
- З полегшеними схемами потрібно бути прагматично ставитися до шахрайства та зловживань:
- Метою має бути ефективне управління ризиками, а не а не тотальне запобігання.
- "Погані яблука" можна виявити та усунути з системи.

Ознайомте брокера з проміжними та агрегованими показниками:



Цілі ефективності
- Мінімізувати використання операцій з відкритим ключем.
- Тримати брокера в режимі "офлайн" якомога більше.
- Зробити внутрішній цикл (купівля/платіж) ефективним,
- особливо для повторюваних невеликих покупок.

Payword

PayWord ланцюжки

- Користувач може легко створити ланцюжок довжиною, скажімо, n = 1000 для постачальника, використовуючи h = MD5, починаючи з wn.
- Користувач передає (підписує за допомогою RSA) продавцю "корінь" w0.
- Користувач здійснює послідовні платежі по 1¢, розкриваючи "платіжні слова" w1, w2, ... по черзі.

- Продавець викуповує зобов'язання і останнє отримане платіжне слово у Брокера.

Сертифікат PayWord

- Брокер видає Користувачеві підписаний "сертифікат" CU терміном на один місяць, що дозволяє Користувачеві створювати ланцюжки PayWord. Брокер надає кредит Користувачеві.

$$C_U = \{Broker, User, User's\ IP\ Address, PK_U, expiration\text{-}date, limits, etc.\}_{SKB}$$

where

$$PK_U = User's\ Public\ RSA\ Key.$$

- Сертифікат дає право на доставку товару тільки на вказану інтернет-адресу.

PayWord Commitment

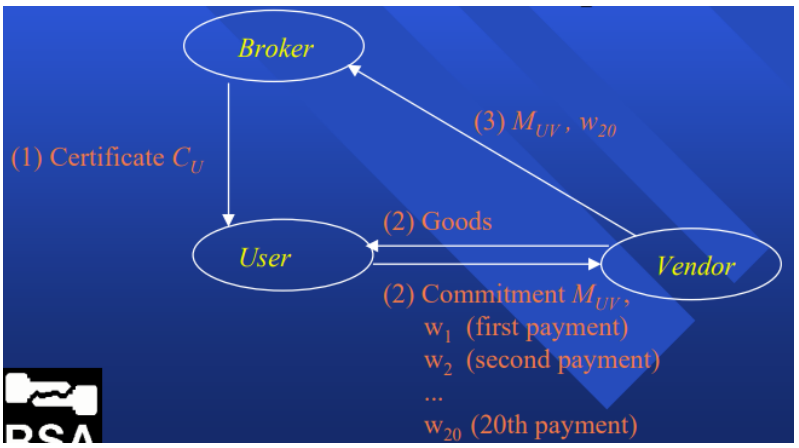
- Користувач надає Постачальнику корінь w0, підписавши повідомлення про зобов'язання MUV:

$$M_{UV} = \{User, Vendor, w_0, C_U, expiration\text{-}date\}_{SKU}$$

- Зобов'язання містить сертифікат Користувача CU.
- Користувач бере на себе зобов'язання по ланцюжку PayWord, скажімо, на один день.
- Зверніть увагу, що Брокер не бере в цьому безпосередньої участі.

Payword

- Базовий інформаційний потік PayWord. Зверніть увагу, що Брокер не працює в режимі офлайн, за винятком випуску щомісячних сертифікатів та остаточного погашення.



Витрати PayWord

- Один підпис Брокера/користувача/місяць (CU).
- Один підпис Користувача/продавця/день (MUV).
- Дві верифікації з боку продавця/користувача/день (для CU та MUV).
- Одна перевірка Брокером/користувачем/продавцем/день (для MUV).
- По одному обчисленню хеш-функції від Користувача, Продавця та Брокера для кожного платежу в 1¢.

Розширення для PayWord

- Можна заплатити за товар вартістю 5 центів, розкривши w10 після w5 (наприклад, розкривши п'ять платіжних слів одночасно).
- Може мати кілька ланцюжків платіжних слів на одне зобов'язання, з різною вартістю кожного платіжного слова в кожному ланцюжку: наприклад, ланцюжок платіжних слів по 1¢, ланцюжок платіжних слів по 25¢ і ланцюжок платіжних слів по 1$.

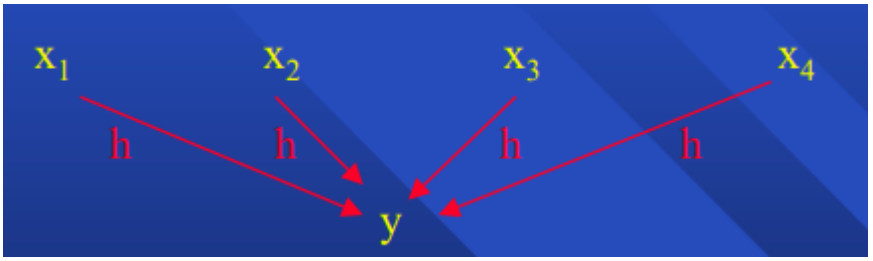
MicroMint

- Цифрова монета має бути такою:
  - Важко виготовити [за винятком брокера]
  - Легкою для перевірки [будь-ким]
- Цифрові підписи "працюють", але є відносно дорогими.
- MicroMint використовує лише хеш-функції (без криптографії з відкритим ключем).

- Брокер використовує економію від масштабу, щоб виробляти монети MicroMint дешево (як на звичайному монетному дворі).

Монети MicroMint

- Нехай геш-функція $h : \{0,1\}^{48} \rightarrow \{0,1\}^{36}$ відображає m-розрядні рядки (де m = 48) до бітових рядків та n-розрядні рядки (де n = 36)
- k-стороння колізія - це k-кортеж (x1, x2, ..., xk) значень, для яких h(x1) = h(x2) = ... = h(xk).



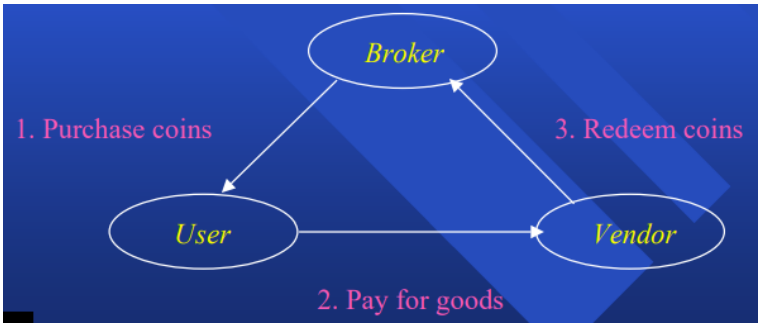
- Монета MicroMint - це 4-way колізія. Перевірити монету легко.

Карбування монет

- Виробництво монет схоже на кидання кульок у 2n урн; k кульок в урні утворюють одну монету.
- Перше 2-стороннє зіткнення потребує часу 2^n/2; це і є "парадокс дня народження".
- Перше k-стороннє зіткнення потребує часу N_k = 2^(n(k-1)/k) (наприклад, 2^27 для k=4, n=36). Важко підробити навіть одну монету.
- За час cN_k можна виготовити ck монет; як тільки поріг N_k перевищено, монети починають вироблятись швидко. Монетний двір має ефект масштабу.

Потік монет MicroMint

1. Брокер карбує монети і продає їх Користувачеві.
2. Користувач витрачає монети у Вендора.
3. Продавець повертає монети назад Брокеру.



Web money

WebMoney Transfer - це глобальна система розрахунків і середовище для ведення бізнесу в Інтернеті, створена в 1998 році. З того часу до системи приєдналося понад 45 мільйонів людей з усього світу.

WebMoney пропонує сервіси, які дозволять вам відстежувати свої кошти, залучати фінансування, вирішувати спірні питання та здійснювати безпечні транзакції.

Технологія WebMoney базується на наборі стандартизованих інтерфейсів, які учасники системи можуть використовувати для управління своїми цінними правами власності, що знаходяться в безпеці у спеціалізованих компаній, відомих як Гаранти. Користувач системи може зареєструвати будь-яку кількість гаманців у будь-якого Гаранта. Всі гаманці, що належать одному користувачеві, зручно зберігаються в "Сховищі", яке присвоюється реєстраційному номеру WMID користувача. Цінності в системі вимірюються в одиницях WebMoney (WM). Для внутрішньої взаємодії всі учасники системи зобов'язані надати персональну інформацію, перевірену службою сертифікації.

Кожному учаснику системи автоматично присвоюється внутрішній параметр системи, доступний для публічного перегляду, так званий Бізнес-рівень, який базується на кількості транзакцій, якими він обмінюється з іншими користувачами системи.

Системна комісія

Комісія за забезпечення інформаційно-технологічної взаємодії між кореспондентами в системі WebMoney Transfer стягується за кожну

операцію і становить 0,8% (не менше 0,01WM*) від суми платежу і не більше максимальних комісій, зазначених нижче:

WMZ	50
WME	50
WMB	100
WMG	2
WMX	5
WMF	50
WMT	50
WMH	30
WMK	9 000
WML	150
WMS	500 000

Комісія не стягується за наступні операції
- між однотипними гаманцями одного WM-ідентифікатора;
- між однотипними гаманцями одного і того ж WebMoney-паспорта (для користувачів, що мають WM-паспорт не нижче Початкового).

Додаткова комісія може стягуватися при проведенні операцій з підтвердженням за номером телефону, вказаним при реєстрації

За проведення кредитних операцій з власників гаманців типу D система стягує комісію в розмірі 0,1% від суми кожного наданого ними кредиту, але не менше 0,01 WMZ.

Безпека та конфіденційність

Технологія WebMoney Transfer розроблена з урахуванням сучасних вимог безпеки до систем управління інформацією в Інтернеті.

Перевірка інформації є ключовим моментом забезпечення безпеки будь-яких даних, що проходять через Систему.

WebMoney Transfer надає 3 основних методи аутентифікації. Це:

- Логін і пароль. В якості логіна можна використовувати свій WMID, номер телефону або e-mail, вказаний при реєстрації. Зазвичай цей спосіб супроводжується додатковим підтвердженням.
- Файли з секретними ключами. Для запуску WM Keeper Classic вам знадобляться: унікальний 12-символьний WM-ідентифікатор, пароль (встановлюється користувачем), файли з секретним ключем і гаманці, що зберігаються в пам'яті комп'ютера. УВАГА! Ви повинні зберігати резервні копії файлів ключів і гаманців на портативному носії та надійно зберігати! Це істотно полегшить відновлення доступу до вашого гаманця у випадку втрати або знищення файлів на вашому ПК
- Персональні цифрові сертифікати.

Існує два способи додаткового підтвердження транзакцій:

- Надсилання коду підтвердження на телефон.
- Використання E-Num, сервісу для генерації одноразових паролів.

Архітектура системи забезпечує безпечний доступ до WM-гаманців користувачів і не дозволяє проводити розрахунки за допомогою WM-гаманців без коштів.

Стійкість до збоїв підключення забезпечується на системному рівні. При здійсненні транзакції кошти завжди знаходяться або на WM-гаманці відправника, або на WM-гаманці одержувача. Проміжного стану в системі немає. Таким чином, втратити WM-кошти концептуально неможливо.

Крім вбудованих технологій, система підтримує додаткові сервіси, які налаштовуються користувачем.

Детальніше про методи захисту можна дізнатися на сайті, присвяченому безпеці системи Webmoney Transfer.

Ідентифікація

Під час реєстрації учаснику WebMoney Transfer присвоюється унікальний номер — 12-символьний WM-ідентифікатор (WMID), необхідний для роботи в системі.

Перевірка особи власника WM-ідентифікатора в системі здійснюється за допомогою WM-верифікації.

Користувачі системи можуть використовувати автоматизовані засоби ідентифікації та аутентифікації учасників при створенні власних програм (див. розділ «Для розробників і веб-майстрів»).

Конфіденційність

За допомогою WM Keeper ви можете налаштувати відображення особистої інформації (ім'я, прізвище, e-mail, поштова адреса тощо), яка буде показуватися іншим учасникам WebMoney Transfer. У цьому випадку під час транзакцій друга сторона отримає доступ лише до вибраної вами інформації.

Якщо ваш торговий партнер попросить вас розкрити деякі з перерахованих вище особистих даних, і ви погодитеся з цією вимогою, тоді налаштування безпеки персональної системи дозволять розкрити цю інформацію.

За вашим WM-ідентифікатором неможливо дізнатися номери використовуваних вами WM-гаманців. При бажанні ви можете встановити на свій комп'ютер необмежену кількість версій WebMoney Keeper і входити в систему за різними WM-ідентифікаторами.

Paypal

#1 Шифрування

Компанія дбає про те, щоб ваша особиста та фінансова інформація була зашифрована та недоступна для сторонніх очей. PayPal використовує шифрування SSL, щоб забезпечити безпеку даних між вашим браузером і

їхніми серверами. Вони також шифрують дані під час передачі та ваші дані, що зберігаються на їхніх серверах.

#2 Автентифікація електронної пошти

Ім’я PayPal часто використовується для маскування фішингових атак. На щастя, компанія співпрацює з великими постачальниками послуг електронної пошти, такими як Gmail і Yahoo, для перевірки автентичності своїх вихідних електронних листів. Що це означає для вас?

Ваш постачальник послуг електронної пошти розпізнає електронні листи, що надходять із справжнього домену PayPal, як законні та надсилатиме їх прямо до вашої папки "Вхідні". Фішингові листи з підроблених доменів позначатимуться як спам. З найпопулярнішими постачальниками послуг електронної пошти вам не потрібно буде навіть пальцем поворухнути.

Однак це не означає, що ви не повинні бути пильними. Завжди переконайтеся, що в адресі відправника листа, який ви читаєте, немає орфографічних помилок. Навчіться розпізнавати навіть найреалістичніші фішингові листи.

#3 Передплачена картка

Маючи обліковий запис PayPal, ви також можете замовити передплачену картку Mastercard. Це чудовий інструмент для будь-якого онлайн-покупця, оскільки він мінімізує ризики онлайн-шахрайства та крадіжки особистих даних. Крім того, деякі веб-сайти можуть не мати PayPal як варіант оплати, тому це буде безпечною альтернативою.

Якщо ви потрапите на підроблений веб-сайт і введете дані своєї передплаченої картки, ці дані все одно потраплять до хакера. Однак, якщо ви заплатили за допомогою передплаченої картки, хакер зможе отримати доступ лише до коштів, які є на вашому рахунку, і не зможе вичерпати ваші заощадження. Передплачені картки також містять набагато менше особистої інформації, тому хакери не зможуть використати її для викрадення вашої особи.

#4 Двофакторна автентифікація

PayPal також пропонує двофакторну автентифікацію (2FA). Це означає, що вам потрібно пройти додатковий етап підтвердження, але це також ускладнює злам вашого облікового запису.

Щоб увійти за допомогою 2FA, ви почнете з введення пароля свого облікового запису. Потім на ваш мобільний пристрій буде надіслано код підтвердження. Код буде надіслано одночасно з введенням пароля. Це робить майже неможливим доступ до вашого облікового запису за допомогою лише вашого пароля – їм також знадобиться доступ до вашого телефону.

На жаль, 2FA не ввімкнено за замовчуванням. Дотримуйтеся покрокових інструкцій PayPal, щоб увімкнути його.

#5 Використовує 3D пароль

Покупці, які використовують PayPal, також натраплять на тривимірний пароль, який є додатковим кроком безпеки, який онлайн-магазини просять виконати. Тип автентифікації залежатиме від вашого банку та емітента картки, але в більшості випадків вам знадобиться ввести додатковий пароль або інший код підтвердження, який ви налаштували у своєму банку. Можливо, ви раніше бачили ці сторінки з позначками «MasterCard SecureCode», «Verified by Visa» або «Safekey» для власників карток American Express.

Додаткові кроки, які вам слід зробити

Незалежно від того, скільки інструментів безпеки має PayPal, багато людей все одно попадаються на шахрайство та втрачають свої гроші. Не будьте одним із них. Вживайте таких запобіжних заходів, щоб захистити свій обліковий запис:

- Оновлюйте програмне забезпечення та антивірус на своїх пристроях. Ваш обліковий запис настільки безпечний, наскільки безпечний ваш пристрій.

- Прив’яжіть до свого облікового запису PayPal кредитну, а не дебетову картку. У більшості випадків емітент вашої кредитної картки захистить вас від шахрайства та може повернути вам гроші.
- Створіть надійний пароль, який нелегко вгадати.
- Навчіться розпізнавати фішингові електронні листи та підроблені веб-сайти.
- Не використовуйте публічний Wi-Fi для фінансових операцій.
- Використовуйте VPN, щоб захистити себе від будь-яких шпигунів, які намагаються отримати вашу інформацію для входу.
- Видаліть свій обліковий запис PayPal, якщо ви ним не користуєтеся. Чим менше особистої інформації ви надаєте в Інтернеті, тим менший ризик бути зламаним.

Висновок

Як зробити ваші електронні платіжні системи більш безпечними? Безпека платежів є першочерговим пріоритетом для кожного бізнесу. Але це стає першорядним при використанні електронної системи обробки платежів у вашому бізнесі. Крім того, існує багато заходів безпеки та протоколів для захисту ваших платіжних систем.

Ось кілька способів захисту вашої електронної платіжної системи:

Отримайте інформацію про систему безпечних електронних транзакцій По-перше, вам потрібно отримати поглиблену інформацію про систему безпечних електронних транзакцій (SET). SET — це стандарт безпечних транзакцій електронної комерції, розроблений Visa та Mastercard, щоб забезпечити споживачам безпечний спосіб здійснення покупок через Інтернет. SET використовує комбінацію шифрування та цифрових сертифікатів для забезпечення безпеки онлайн-транзакцій.

SET використовує інфраструктуру відкритих ключів (PKI) для забезпечення автентифікації та шифрування онлайн-транзакцій. Коли споживач робить покупку, його браузер шифрує інформацію про кредитну картку та цифровий сертифікат, який надсилається продавцю. Потім продавець використовує свій цифровий сертифікат, щоб розшифрувати інформацію та підтвердити транзакцію.

Переконайтеся, що ваша система сумісна з PCI
Коли ви обираєте систему електронних платежів для свого бізнесу, ви повинні переконатися, що вона сумісна з PCI. Стандарт безпеки даних платіжних карток (PCI DSS) — це список стандартів платіжних систем для безпечного прийому, зберігання та обробки платежів, а також захисту від шахрайства з кредитними картками.

Налаштування цифрових підписів
Цифрові підписи пов’язують власника картки з онлайн-платежем. Ці підписи є відкритим ключем для забезпечення транзакції. Тому для посилення безпеки вашої платіжної системи необхідно налаштувати цифрові підписи.

Використовуйте шифрування SSL і TLS
Рівень захищених сокетів або SSL — це протокол безпеки, який відповідає багатьом протоколам безпеки, таким як автентифікація, наскрізне шифрування та цілісність. Шифрування SSL гарантує безпеку транзакцій, здійснених на вашому веб-сайті.

Безпека транспортного рівня (TLS) — це протокол безпеки, який використовується для шифрування та захисту зв’язку через Інтернет. Це не що інше, як оновлена версія протоколу SSL.

Впровадити двофакторну аутентифікацію
Двофакторна автентифікація (2FA) — це процес безпеки, який додає додатковий рівень захисту, вимагаючи від клієнта надати дві форми ідентифікації для доступу до системи. Перша форма - це пароль або PIN-код. Другий генерується пристроєм або службою, до якої користувач має фізичний доступ, наприклад, одноразовим паролем (OTP) або відбитком пальця.

Крім того, існує кілька інших заходів безпеки, таких як регулярне оновлення програмного забезпечення, моніторинг підозрілих дій, використання біометричних систем, токенізація, 3D-захист, служби перевірки адреси (AVS) та багато іншого. Запровадивши всі ці заходи

безпеки, ви можете зробити свій цифровий платіжний сервіс ще безпечнішим і складнішим для зламу.