

**УКРАЇНА****(19) UA****(11) 115500****(13) C2****(51) МПК****G06Q 20/40 (2012.01)****G06Q 20/32 (2012.01)**

**МІНІСТЕРСТВО
ЕКОНОМІЧНОГО
РОЗВИТКУ І ТОРГІВЛІ
УКРАЇНИ**

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки:	а 2016 07123	(72) Винахідник(и):	Коллінге Мехді (BE), Сметс Патрік (BE), Кейтленд Аксель Еміль Жан Чарльз (US)
(22) Дата подання заявки:	02.12.2014	(73) Власник(и):	МАСТЕРКАРД ІНТЕРНЕТНЛ ІНКОРПОРЕЙТЕД, 2000 Purchase Street, Purchase, NY 10577, United States of America (US)
(24) Дата, з якої є чинними права на винахід:	10.11.2017	(74) Представник:	Мошинська Ніна Миколаївна, реєстр. №115
(31) Номер попередньої заявки відповідно до Паризької конвенції:	61/910,819, 61/951,842, 61/955,716, 61/979,132, 61/980,784	(56) Перелік документів, взятих до уваги експертизою:	US 2013262317 A1, 03.10.2013 US 2013282502 A1, 24.10.2013 US 2012317628 A1, 13.12.2012 US 2012143752 A1, 07.06.2012 US 2009265544 A1, 22.10.2009
(32) Дата подання попередньої заявки відповідно до Паризької конвенції:	02.12.2013, 12.03.2014, 19.03.2014, 14.04.2014, 17.04.2014		
(33) Код держави-учасниці Паризької конвенції, до якої подано попередню заявку:	US, US, US, US, US		
(41) Публікація відомостей про заявку:	12.12.2016, Бюл.№ 23		
(46) Публікація відомостей про видачу патенту:	10.11.2017, Бюл.№ 21		
(86) Номер та дата подання міжнародної заявки, поданої відповідно до Договору РСТ	PCT/US2014/067992, 02.12.2014		

(54) СПОСІБ І СИСТЕМА БЕЗПЕЧНОЇ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА І МОБІЛЬНИЙ ПРИСТРІЙ БЕЗ ЕЛЕМЕНТІВ БЕЗПЕКИ**(57) Реферат:**

Спосіб генерування платіжних облікових даних в платіжній транзакції, який включає в себе: збереження в пам'яті щонайменше разового ключа, асоційованого з транзакційним рахунком; прийом приймальним пристроєм персонального ідентифікаційного номера; ідентифікацію пристроєм обробки першого сеансового ключа; генерування пристроєм обробки другого сеансового ключа, основуючись щонайменше на збереженому разовому ключі і прийнятому персональному ідентифікаційному номері; генерування пристроєм обробки першої криптограми додатка, основуючись щонайменше на першому сеансовому ключі; генерування пристроєм обробки другої криптограми додатка, основуючись щонайменше на другому сеансовому ключі; і передачу передавальним пристроєм щонайменше першої криптограми додатка і другої криптограми додатка для використання в платіжній транзакції.

UA 115500 C2

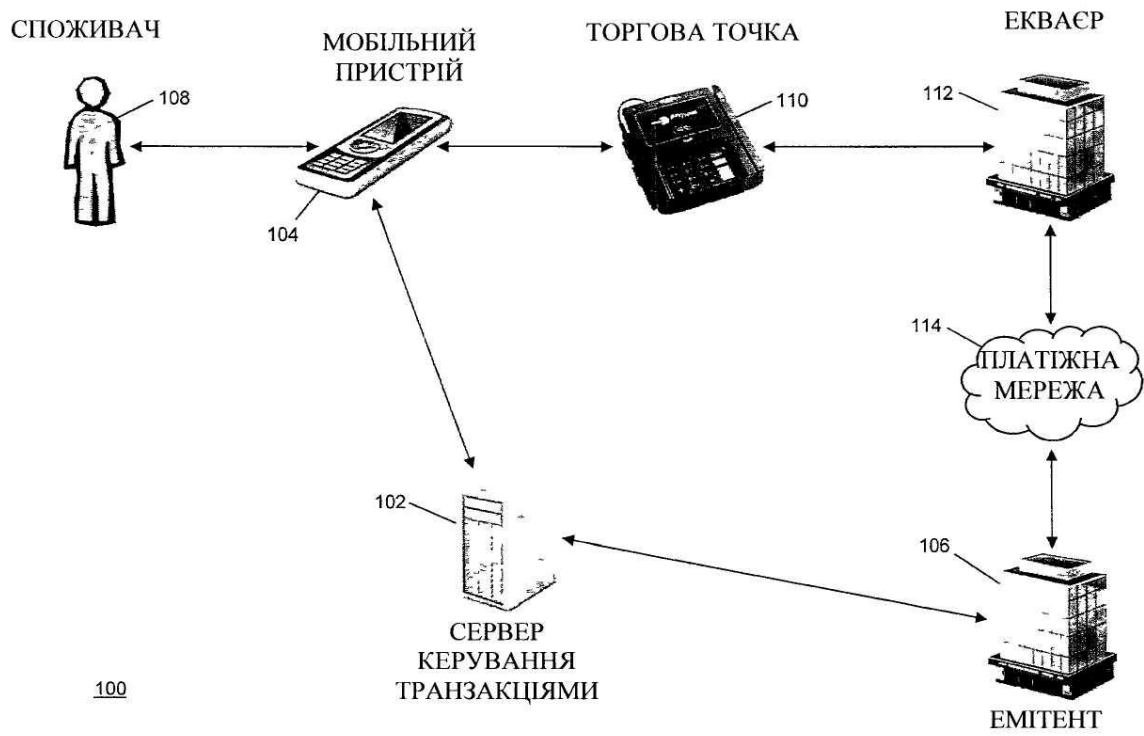


Fig. 1

СПОРИДНЕНІ ЗАЯВКИ

[0001] Дана заявка претендує на перевагу, згідно зі статтею 119(е) розділу 35 Кодексу законів США, раніше поданих попередніх заявок на патент №№ 61/979,122, поданої 14 квітня 2014 р.; 61/996,665, поданої 14 травня 2014 р.; 61/979,113, поданої 14 квітня 2014 р. і, особливо, попередніх заявок на патент №№ 61/910,819, поданої 2 грудня 2013 р.; 61/951,842, поданої 12 березня 2014 р.; 61/955,716, поданої 19 березня 2014 р.; 61/979,132, поданої 14 квітня 2014 р.; і 61/980,784, поданої 17 квітня 2014 р., при цьому кожна повністю включена в даний документ за посиланням.

ГАЛУЗЬ ТЕХНІКИ

[0002] Даний винахід стосується аутентифікації користувача і мобільного пристрою без необхідності елемента безпеки в платіжній транзакції, і, конкретніше, генерування безпечних платіжних облікових даних в мобільному пристрої, що використовується в платіжній транзакції, без використання елементів безпеки.

РІВЕНЬ ТЕХНІКИ

[0003] Досягнення в технологіях мобільного зв'язку створили величезні можливості, однією з яких є надання користувачеві мобільного обчислювального пристрою можливості ініціювати і оплачувати платіжні транзакції, використовуючи свій мобільний пристрій. Одним таким підходом, що надає можливість таких дій на мобільному пристрої, було використання технології зв'язку малого радіуса дії (NFC) для безпечної передачі реквізитів платежу з мобільного пристрою на найближчий безконтактний термінал торгової точки (POS). Щоб досягнути цього, мобільні телефони з апаратними засобами елемента безпеки, такими як кристал елемента безпеки (SE), використовуються для безпечного зберігання платіжних облікових даних. Елемент безпеки є спеціальним елементом, який може бути включений в деякі пристрої з можливістю NFC, який являє собою платформу, захищену від зловмисного втручання, яка може безпечно розміщувати додатки і їх конфіденційні дані.

[0004] Однак не всі мобільні пристрої мають елементи безпеки. Крім того, деякі фінансові установи можуть не мати доступу до елементів безпеки на мобільних пристроях, навіть якщо мобільний пристрій оснащений таким елементом. У результаті, багато які споживачі з мобільними пристроями, які мають необхідні апаратні засоби для проведення віддалених платіжних транзакцій безконтактного або інших типів, можуть бути нездатні фактично використовувати цю можливість. Через такі труднощі існує потреба в технічному рішенні, яке могло б надати можливість мобільним обчислювальним пристроям ініціювати і провести платіжні транзакції без використання елементів безпеки.

[0005] Деякі способи і системи для проведення платіжних транзакцій, використовуючи мобільні пристрої з відсутніми елементами безпеки, або без використання елементів безпеки в мобільних пристроях, оснащених ними, можна знайти в заявці на патент США № 13/827,042, під заголовком "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements" by Mehdi Collinge et al., поданої 14 березня 2013 р., яка повністю включена в даний документ за посиланням. Хоча такі способи і системи можуть бути придатні для проведення платіжних транзакцій за допомогою мобільного пристрою без використання елемента безпеки, багато які споживачі, торгово-сервісні підприємства і фінансові установи можуть застерігати від участі в таких транзакціях через бажання ще більшої безпеки.

[0006] У результаті, існує потреба в технічних рішеннях для забезпечення ще більшої безпеки прийому і зберігання платіжних облікових даних в мобільному пристрої, що не має елемента безпеки, а також забезпеченні підвищеної безпеки при передачі платіжних облікових даних на торгову точку з мобільного пристрою під час проведення фінансової транзакції. Підвищена безпека в цих процесах може приводити до підвищеного душевного спокою для всіх залучених об'єктів, що може привести до підвищення використання мобільних пристроїв для безконтактних або віддалених платіжних транзакцій, які можуть забезпечувати велику кількість переваг для споживачів в порівнянні з традиційними способами оплати.

СУТЬ ВИНАХОДУ

[0007] Даний винахід забезпечує опис систем і способів для генерування платіжних облікових даних в платіжних транзакціях.

[0008] Спосіб генерування платіжних облікових даних в платіжній транзакції включає в себе: збереження в пам'яті щонайменше разового ключа, асоційованого з транзакційним рахунком; прийом приймальним пристроєм персонального ідентифікаційного номера; ідентифікацію пристроєм обробки першого сеансового ключа; генерування пристроєм обробки другого сеансового ключа, основуючись щонайменше на збереженому разовому ключі і прийнятому персональному ідентифікаційному номері; генерування пристроєм обробки першої криптограми додатку, основуючись щонайменше на першому сеансовому ключі; генерування пристроєм

обробки другої криптограми додатку, основуючись щонайменше на другому сеансовому ключі; і передачу передавальним пристроєм щонайменше першої криптограми додатку і другої криптограми додатку для використання в платіжній транзакції.

[0009] Інший спосіб генерування платіжних облікових даних в платіжній транзакції включає в себе: збереження в пам'яті щонайменше головного ключа картки, асоційованого з транзакційним рахунком; генерування пристроєм обробки першого сеансового ключа, основуючись щонайменше на збереженому головному ключі картки; генерування пристроєм обробки другого сеансового ключа; генерування пристроєм обробки першої криптограми додатку, основуючись щонайменше на першому сеансовому ключі; генерування пристроєм обробки другої криптограми додатку, основуючись щонайменше на другому сеансовому ключі; і передачу передавальним пристроєм щонайменше першої криптограми додатку і другої криптограми додатку для використання в платіжній транзакції.

[0010] Система для генерування платіжних облікових даних в платіжній транзакції включає в себе пам'ять, приймальний пристрій, пристрій обробки і передавальний пристрій. Пам'ять виконана з можливістю зберігання щонайменше разового ключа, асоційованого з транзакційним рахунком. Приймальний пристрій виконаний з можливістю прийому персонального ідентифікаційного номера. Пристрій обробки виконаний з можливістю: ідентифікації першого сеансового ключа, генерування другого сеансового ключа, основуючись щонайменше на збереженому разовому ключі і прийнятому персональному ідентифікаційному номері; генерування першої криптограми додатку, основуючись щонайменше на першому сеансовому ключі; і генерування другої криптограми додатку, основуючись щонайменше на другому сеансовому ключі. Передавальний пристрій виконаний з можливістю передачі щонайменше першої криптограми додатку і другої криптограми додатку для використання в платіжній транзакції.

[0011] Інша система для генерування платіжних облікових даних в платіжній транзакції включає в себе пам'ять, пристрій обробки і передавальний пристрій. Пам'ять виконана з можливістю зберігання щонайменше головного ключа картки, асоційованого з транзакційним рахунком. Пристрій обробки виконаний з можливістю генерування першого сеансового ключа, основуючись щонайменше на головному ключі картки, що зберігається; генерування другого сеансового ключа; генерування першої криптограми додатку, основуючись щонайменше на першому сеансовому ключі; і генерування другої криптограми додатку, основуючись щонайменше на другому сеансовому ключі. Передавальний пристрій виконаний з можливістю передачі щонайменше першої криптограми додатку і другої криптограми додатку для використання в платіжній транзакції.

КОРОТКИЙ ОПИС КРЕСЛЕНЬ

[0012] Об'єм даного винаходу краще усього зрозумілий з подальшого докладного опису зразкових варіантів здійснення при читанні разом з прикладеними кресленнями. У креслення включені наступні фігури:

[0013] Фіг. 1 являє собою блок-схему, яка ілюструє високорівневу системну архітектуру для обробки платіжних транзакцій з підвищеною безпекою при наданні і зберіганні платіжних облікових даних згідно зі зразковими варіантами здійснення.

[0014] Фіг. 2 являє собою блок-схему, яка ілюструє мобільний пристрій за фіг. 1 для обробки платіжних транзакцій без елемента безпеки і безпечного прийому і зберігання платіжних облікових даних згідно зі зразковими варіантами здійснення.

[0015] Фіг. 3 являє собою блок-схему, яка ілюструє базу даних карток мобільного пристрою за фіг. 2 для зберігання платіжних облікових даних згідно зі зразковими варіантами здійснення.

[0016] Фіг. 4 являє собою блок-схему, яка ілюструє пам'ять мобільного пристрою за фіг. 2 для зберігання даних, що використовуються при генеруванні вдосконалених ключів зберігання і генеруванні криптограм додатку згідно зі зразковими варіантами здійснення.

[0017] Фіг. 5 являє собою блок-схему, яка ілюструє сервер керування транзакціями за фіг. 1 для обробки платіжних транзакцій з мобільним пристроєм без елемента безпеки згідно зі зразковими варіантами здійснення.

[0018] Фіг. 6 являє собою блок-схему, яка ілюструє базу даних рахунків сервера обробки за фіг. 5 для зберігання платіжних облікових даних і реквізитів рахунків згідно зі зразковими варіантами здійснення.

[0019] Фіг. 7 являє собою блок-схему послідовності операцій, що ілюструє процес передачі і перевірки достовірності подвійних криптограм додатку для обробки платіжних транзакцій, в яких бере участь мобільний пристрій, що не має елемента безпеки, згідно зі зразковими варіантами здійснення.

[0020] Фіг. 8 являє собою блок-схему послідовності операцій, що ілюструє альтернативний процес передачі і перевірки достовірності подвійних криптограм додатку для обробки платіжних транзакцій, в яких бере участь мобільний пристрій, що не має елемента безпеки, згідно зі зразковими варіантами здійснення.

5 [0021] Фіг. 9 являє собою блок-схему послідовності операцій, що ілюструє процес створення, передачі і перевірки достовірності служби віддалених сповіщень або іншого повідомлення з даними, що надається мобільному пристрою, що не має елемента безпеки, згідно зі зразковими варіантами здійснення.

10 [0022] Фіг. 10А і 10В являють собою блок-схеми послідовності операцій, що ілюструють процес створення, передачі і перевірок достовірності повідомлення, яке повертається мобільним пристроєм, що не має елемента безпеки, згідно зі зразковими варіантами здійснення.

15 [0023] Фіг. 11 являє собою блок-схему послідовності операцій, що ілюструє процес перевірки достовірності повідомлення служби віддалених сповіщень, що використовує мобільний пристрій за фіг. 2, згідно зі зразковими варіантами здійснення.

[0024] Фіг. 12 являє собою схему, яка ілюструє генерування вдосконаленого ключа зберігання, що використовує мобільний пристрій за фіг. 2, згідно зі зразковими варіантами здійснення.

20 [0025] Фіг. 13 і 14 являють собою блок-схеми послідовності операцій, що ілюструють зразкові способи генерування платіжних облікових даних в платіжній транзакції, згідно зі зразковими варіантами здійснення.

[0026] Фіг. 15 являє собою блок-схему послідовності операцій, що ілюструє зразковий спосіб прийому і обробки повідомлення служби віддалених сповіщень, згідно зі зразковими варіантами здійснення.

25 [0027] Фіг. 16 являє собою блок-схему послідовності операцій, що ілюструє зразковий спосіб формування вдосконаленого ключа зберігання, згідно зі зразковими варіантами здійснення.

[0028] Фіг. 17 являє собою блок-схему, яка ілюструє архітектуру комп'ютерної системи згідно зі зразковими варіантами здійснення.

30 [0029] Додаткові галузі застосовності даного винаходу стануть очевидні з докладного опису, представленого нижче в даному документі. Потрібно розуміти, що докладний опис зразкових варіантів здійснення призначений тільки для цілей ілюстрації і, тому, як передбачається, не обмежує обов'язково об'єм винаходу.

ДОКЛАДНИЙ ОПИС

Словник термінів

35 [0030] Платіжна мережа - система або мережа, що використовується для переказу грошей за допомогою використання заміників грошей. Платіжні мережі можуть використовувати множинну різних протоколів і процедур для обробки переказу грошей для різних типів транзакцій. Транзакції, які можуть виконуватися за допомогою платіжної мережі, можуть включати в себе покупки продукту або послуги, покупки в кредит, дебетові транзакції, безготівкові перекази грошових коштів, знімання грошей з рахунку і т. д. Платіжні мережі можуть бути виконані з

40 можливістю виконання транзакцій за допомогою заміників грошей, які можуть включати в себе платіжні картки, акредитиви, чеки, рахунки транзакції і т. д. Приклади мереж або систем, виконані з можливістю виконання як платіжні мережі включають в себе ті мережі, які управляються компаніями MasterCard®, VISA®, Discover®, American Express®, PayPal® і т. п.

45 Використання терміну "платіжна мережа" в даному документі може посилається як на платіжну мережу у вигляді об'єкта, так і на фізичну платіжну мережу, таку як обладнання, апаратні засоби і програмні засоби, що містять платіжну мережу.

[0031] Транзакційний рахунок - фінансовий рахунок, який може використовуватися для фінансування транзакції, такої як поточний рахунок, ощадний рахунок, кредитний рахунок, віртуальний платіжний рахунок і т. д. Транзакційний рахунок може асоціюватися зі споживачем, яким може бути будь-який придатний тип об'єкта, асоційований з платіжним рахунком, який може включати в себе людину, сім'ю, компанію, корпорацію, урядовий об'єкт і т. д. В деяких випадках, транзакційний рахунок може бути віртуальним, наприклад, ті рахунки, які оперуються компанією PayPal®, і т. д.

55 [0032] Платіжна картка - картка або дані, асоційовані з транзакційним рахунком, який може надаватися торгово-сервісному підприємству для фінансування фінансової транзакції за допомогою асоційованого транзакційного рахунку. Платіжні картки можуть включати в себе кредитні картки, дебетові картки, розрахункові картки, картки зі сумою, що зберігається, передплачені картки, транспортні корпоративні картки, віртуальні номери платежу, віртуальні

60 номери картки, що контролюються номери платежу і т. д. Платіжною картою може бути фізична

картка, яка може надаватися торгово-сервісному підприємству, або можуть бути дані, що представляють асоційований транзакційний рахунок (наприклад, що зберігається в пристрої зв'язку, такому як смартфон або комп'ютер). Наприклад, в деяких випадках, дані, що включають в себе номер платіжного рахунку, можуть розглядатися як платіжна картка для обробки транзакції, що фінансується за допомогою асоційованого транзакційного рахунку. У деяких випадках, чек може розглядатися як платіжна картка, де це застосовно.

[0033] Платіжна транзакція - транзакція між двома об'єктами, в якій гроші або інша фінансова вигода, обмінюються від одного об'єкта до іншого. Платіжна транзакція може являти собою переказ грошових коштів, для купівлі товарів або послуг, для погашення боргу або для будь-якого іншого обміну фінансовою вигодою, що очевидно для фахівця в даній галузі техніки. У деяких випадках платіжна транзакція може посилатися на транзакції, які фінансуються за допомогою платіжної картки і/або платіжного рахунку, таких як транзакції кредитною картою. Такі платіжні транзакції можуть оброблятися емітентом, платіжною мережею і екваєром. Процес обробки такої платіжної транзакції може включати в себе щонайменше одне з авторизації, пакетування, клірингу, взаєморозрахунку і фінансування. Авторизація може включати в себе надання реквізитів платежу споживачем торгово-сервісному підприємству, представлення відомостей про транзакції (наприклад, включаючи реквізити платежу) торгово-сервісним підприємством своєму екваєру, і перевірку достовірності реквізитів платежу емітентом платіжного рахунку споживача, що використовується для фінансування транзакції. Пакетування може посилатися на збереження авторизованої транзакції в пакеті з іншими авторизованими транзакціями для розподілу екваєру. Кліринг може включати в себе посилання пакетних транзакцій від екваєра в платіжну мережу для обробки. Взаєморозрахунок може включати в себе дебетування емітента платіжною мережею для транзакцій, які займають бенефіціари емітента. У деяких випадках, емітент може сплатити екваєру за допомогою платіжної мережі. В інших випадках, емітент може сплатити екваєру безпосередньо. Фінансування може включати в себе платіж торгово-сервісному підприємству від екваєра за платіжні транзакції, за якими були виконані кліринг і взаєморозрахунок. Для фахівця в даній галузі техніки зрозуміло, що порядок і/або категоризація етапів, описані вище, виконується як частина обробки платіжної транзакції.

[0034] Торгова точка - Обчислювальний пристрій або обчислювальна система, виконана з можливістю прийому взаємодії з користувачем (наприклад, споживачем, співробітником і т. д.) для введення даних про транзакцію, платіжних даних і/або інших придатних типів даних для покупки і/або платежу за товари і/або послуги. Торгова точка може являти собою фізичний пристрій (наприклад, касовий апарат, кіоск, настільний комп'ютер, смартфон, планшетний комп'ютер і т. д.) в фізичному розташуванні, який споживач відвідує як частина транзакції, такому як фізичний магазин, або може бути віртуальною в середовищі електронної торгівлі, такий як інтернет-магазини роздрібної торгівлі, що приймають передачу даних від споживачів по мережі, такий як Інтернет. У випадках, коли торгова точка може бути віртуальною, обчислювальний пристрій, керований користувачем для ініціювання транзакції, або обчислювальна система, яка приймає дані внаслідок транзакції, може розглядатися як торгова точка при відповідних умовах.

Система для обробки платіжних транзакцій з використанням мобільного пристрою без елементів безпеки

[0035] Фіг. 1 ілюструє систему 100 для обробки платіжних транзакцій, використовуючи мобільний пристрій без вимоги використання елементів безпеки, які можуть включати в себе забезпечення безпеки платіжних облікових даних для мобільного пристрою, їх безпечне зберігання і використання при генеруванні численних криптограм додатку для використання при перевірці достовірності і обробці платіжної транзакції.

[0036] Система 100 може включати в себе сервер 102 керування транзакціями. Сервер 102 керування транзакціями, описаний детальніше нижче, може являти собою один або декілька обчислювальних пристроїв, спеціально запрограмованих для виконання функцій, описаних в даному документі, для надання платіжних облікових даних мобільному пристрою 104, використовуючи повідомлення віддаленого сповіщення, яке безпечно передається, і для перевірки достовірності платіжних облікових даних, які утворюються мобільним пристроєм 104 як частина платіжної транзакції. Хоча це зображено і описано в даному документі, що сервер 102 керування транзакціями виконує численні функції, для фахівця в даній галузі техніки зрозуміло, що сервер 102 керування транзакціями може складатися з численних обчислювальних пристроїв, серверів і/або обчислювальних мереж, виконаних з можливістю виконання функцій, описаних в даному документі. Мобільний пристрій 104, описаний детальніше нижче, може бути мобільним обчислювальним пристроєм будь-якого типу, придатний для виконання функцій, описаних в даному документі, який може включати в себе

стілниковий телефон, смартфон, розумні годинники, інший вбудований або переносний обчислювальний пристрій, планшетний комп'ютер, портативний комп'ютер і т. д. В деяких варіантах здійснення обчислювальний пристрій 104 може не мати елемента безпеки. В інших варіантах здійснення мобільний пристрій 104 може включати в собі елемент безпеки, але такий елемент може не використовуватися разом зі способами і системами, описаними в даному документі, або може використовуватися разом зі способами і системами, описаними в даному документі, наприклад, для забезпечення додаткової безпеки.

[0037] Мобільний пристрій 104 може виконувати зв'язок з сервером 104 керування транзакціями, використовуючи численні канали зв'язку, наприклад, використовуючи двоканальний зв'язок. Двоканальний зв'язок може включати в себе використання двох каналів зв'язку при передачі і прийомі даних, наприклад, для верифікації і аутентифікації, для забезпечення більшої безпеки при передачі даних. Мобільний пристрій 104 може включати в себе мобільний платіжний додаток (MPA), виконаний з можливістю виконання мобільним пристроєм 104 для виконання функцій мобільного пристрою 104, описаного в даному документі. MPA, описаний детальніше нижче, може встановлюватися на мобільному пристрої 104 і може активізуватися з використанням коду активізації, що надається сервером 102 керування транзакціями, використовуючи способи і системи, які очевидні для фахівця в даній галузі техніки, так що мобільний пристрій 104 і сервер 102 керування транзакціями можуть безпечно передавати і приймати зв'язок за одним або декількома каналами зв'язку, використовуючи спільно використовувані дані.

[0038] Система 100 також може включати в себе емітент 106. Емітент 106 може являти собою фінансову установу, таку як банк-емітент, який видає платіжну картку або платіжні облікові дані споживачеві 108, асоційованому з транзакційним рахунком. Емітент 106 може надавати реквізити платежу, асоційовані з транзакційним рахунком і/або платіжною карткою, серверу 102 керування транзакціями. Реквізити платежу можуть включати в себе, наприклад, номер транзакційного рахунку, ім'я власника рахунку, дату закінчення терміну дії, код безпеки і т. д. Сервер 102 керування транзакціями може зберігати дані в базі даних рахунків, описаний детальніше нижче. Сервер 102 керування транзакціями також може надавати платіжні облікові дані мобільному пристрою 104. Як використовується в даному документі, термін "платіжні облікові дані" може посилатися на будь-які дані, що використовуються мобільним пристроєм 104 і/або сервером 102 керування транзакціями при передачі і перевірці достовірності платіжної інформації, що використовується в платіжній транзакції, що використовує способи і системи, описані в даному документі, включаючи, але не обмежуючись ними, реквізити платежу, платіжні облікові дані, разові ключі, сеансові ключі, криптограми додатку, головні ключі картки і т. д.

[0039] У деяких варіантах здійснення платіжні облікові дані можуть надаватися мобільному пристрою 104 за допомогою повідомлення служби віддалених сповіщень. Як описано детальніше нижче, повідомлення служби віддалених сповіщень (RNS) може являти собою безпечне повідомлення, яке передається на мобільний пристрій 104, і потім проводиться перевірка його достовірності мобільним пристроєм 104, так що дані, що містяться в ньому, можуть бути захищені від інших пристроїв і користувачів. MPA мобільного пристрою 104 може верифікувати автентичність прийнятого повідомлення RNS і може розшифровувати його для отримання даних, включених в нього. Мобільний пристрій 104 потім може виконувати будь-які необхідні функції, основуючись на даних (наприклад, таких як за допомогою виконання інструкцій, включених в дані), і, якщо застосовно, може генерувати повідомлення, яке повертається, що підлягає посиланню назад на сервер 102 керування транзакціями. У деяких випадках, повідомлення, яке повертається, може перевірятися на достовірність сервером 102 керування транзакціями.

[0040] У деяких випадках перевірка достовірності повідомлень RNS в мобільному пристрої 104 або перевірка достовірності повідомлення, які повертаються, в сервері 102 керування транзакціями може використовувати щонайменше лічильники повідомлень і код аутентифікації. Використання як лічильників, так і кодів аутентифікації може гарантувати, що тільки мобільний пристрій 104, який має на увазі, може бути здатний перевірити достовірність і розшифрувати дані, включені в повідомлення RNS. Крім того, якщо правила і/або алгоритми, що використовуються при генеруванні коду аутентифікації, включені в MPA, тоді тільки мобільний пристрій 104, який також включає в себе конкретний екземпляр програми додатку, може бути здатний перевірити достовірність повідомлення RNS, приводячи до додатково підвищеної безпеки. У випадках, коли повідомлення RNS може включати в себе платіжні облікові дані, це може гарантувати, що платіжні облікові дані доступні тільки на відповідному мобільному пристрої 104, і тільки якщо MPA, що використовується для доступу до них, є належним і авторизованим додатком.

[0041] Платіжні облікові дані, надані мобільному пристрою 104, можуть бути безпечно збережені в сховищі в мобільному пристрої 104, такому як база даних карток, описана детальніше нижче. У деяких варіантах здійснення мобільний пристрій 104 може бути виконаний з можливістю генерування вдосконаленого ключа зберігання для використання при безпечному зберіганні даних, таких як платіжні облікові дані, в базі даних або пам'яті в мобільному пристрої 104. Генерування вдосконаленого ключа зберігання, як описано детальніше нижче, може використовувати унікальну інформацію про пристрій, унікальну інформацію МРА й інформацію, що випадково генерується, щоб ідентифікувати безпечний ключ зберігання, який може використовуватися для безпечного зберігання даних в мобільному пристрої 104. У результаті, платіжні облікові дані або інші вразливі дані можуть безпечно зберігатися в мобільному пристрої 104 без використання елемента безпеки, що може приводити до того, що мобільний пристрій 104 буде здатний ініціювати і провести платіжні транзакції без використання елемента безпеки, підвищуючи доступність для емітентів 106 і споживачів 108, в той же час зберігаючи високий рівень безпеки.

[0042] Якщо мобільний пристрій 104 має платіжні облікові дані для транзакційного рахунку, прийняті, перевірені на достовірність і збережені безпечно в ньому, споживач 108 може взяти мобільний пристрій 104 в торгову точку 110 в торгово-сервісному підприємстві для проведення платіжної транзакції. Споживач 108 може вибрати товари або послуги для купівлі, може ініціювати платіжну транзакцію для їх купівлі в торгово-сервісному підприємстві і може використовувати мобільний пристрій 104 для передачі платіжних облікових даних для використання при фінансуванні платіжної транзакції. Передача платіжних облікових даних торговій точці 110 може включати в себе передачу двох або більше криптограм додатку. Використання двох або більше криптограм додатку може приводити до вищого рівня безпеки для транзакцій, що обробляються з використанням способів і систем, описаних в даному документі, ніж той, який доступний при традиційних безконтактних і віддалених транзакціях, включаючи транзакції, що проводяться з використанням мобільного пристрою 104, що має елемент безпеки.

[0043] Кожна криптограма додатку може генеруватися мобільним пристроєм 104, використовуючи окремі сеансові ключі і додаткові дані, описані детальніше нижче. Криптограми додатку, що генеруються з використанням даних, які зберігаються в мобільному пристрої 104, наприклад, в сховищі, безпека якого забезпечується вдосконалим ключем зберігання і яке асоціюється з МРА, можуть гарантувати, що криптограми додатку аутентифікують мобільний пристрій 104 і конкретний екземпляр МРА. У деяких випадках одна з криптограм і/або сеансових ключів, що використовуються для генерування криптограм, може використовувати інформацію, що надається споживачем 108, таку як персональний ідентифікаційний номер (PIN). Використання PIN або іншої інформації аутентифікації споживача може зробити можливим, що криптограми аутентифікують як споживача 108, так і мобільний пристрій 104. У такому випадку криптограми, що генеруються мобільним пристроєм 104, можуть включати в себе одну, яка аутентифікує мобільний пристрій 104, і другу, яка аутентифікує як мобільний пристрій 104, так і споживача 108.

[0044] Криптограми можуть прийматися торговою точкою 110 як частина проведення платіжної транзакції, наприклад, за допомогою зв'язку малого радіуса дії. Криптограми додатку можуть супроводжувати додаткову платіжну інформацію, таку, яка може закладатися в контексті будь-якого придатного типу платіжної транзакції, такої як безконтактна транзакція, віддалена транзакція, безпечна віддалена платіжна транзакція, транзакція з використанням магнітної смуги і транзакція M/Chip стандарту EMV, і може передаватися на торгову точку 110, використовуючи будь-який придатний спосіб відповідно до описаних в даному документі, що очевидно для фахівця в даній галузі техніки. Криптограми можуть передаватися екваєру 112, яким може бути фінансова установа, така як банк-екваєр, асоційований з торгово-сервісним підприємством. Екваєр 112, наприклад, може видавати транзакційний рахунок торгово-сервісному підприємству, який використовується для прийому платежу грошовими коштами від споживача 108 для платіжної транзакції. Екваєр 112 може представити криптограми і додаткові відомості про транзакцію платіжної мережі 114, використовуючи способи і системи, які очевидні для фахівця в даній галузі техніки. Наприклад, відомості про транзакції і криптограми додатку можуть бути включені в запит авторизації, представленої платіжної мережі 114 за правилами платежу.

[0045] У деяких варіантах здійснення обидві криптограми додатку можуть бути включені в єдине повідомлення транзакції. Наприклад, мобільний пристрій 104 і/або торгова точка 110 можуть включати в себе обидві криптограми додатку в полях існуючих даних традиційного повідомлення транзакції, щоб передавати обидві криптограми додатку, використовуючи існуючі

платіжні системи і апаратні засоби. У деяких випадках сервер 102 керування транзакціями може бути виконаний з можливістю використання даних Track 2 (доріжки 2) для перевірки достовірності криптограм додатку, таких як в транзакції з використанням магнітної смуги. У таких випадках, якщо повідомлення транзакції включає в себе дані Track 1 (доріжки 1), сервер 102 керування транзакціями може бути виконаний з можливістю перетворення даних Track 1 в дані Track 2, що також можуть включати в себе перетворення модифікованих даних Track 1 або Track 2 в немодифіковані (наприклад, вихідні, відновлені і т. д.) дані Track 1 або Track 2 відповідно. За допомогою виконання цих функцій і за допомогою включення криптограм додатку в поля існуючих даних, сервер 102 керування транзакціями може бути виконаний з можливістю обробки і перевірки достовірності віддалених і безконтактних платіжних транзакцій з використанням мобільного пристрою 104 з вищим рівнем безпеки, без вимоги використання елемента безпеки на мобільному пристрої 104 і без модифікування існуючих платіжних систем.

[0046] Платіжна мережа 114 може обробляти платіжну транзакцію, використовуючи способи і системи, які очевидні для фахівця в даній галузі техніки. Як частина обробки, платіжна мережа 114 може передавати криптограми додатку емітенту 106 для верифікації. У деяких варіантах здійснення верифікація може виконуватися платіжною мережею 114. Емітент 106 або платіжна мережа 114 можуть виконувати зв'язок з сервером 102 керування транзакціями. У деяких варіантах здійснення криптограми додатку можуть передаватися серверу 102 керування транзакціями і можуть верифікуватися за допомогою генерування перевіряючих достовірність криптограм додатку, використовуючи сервер 102 керування транзакціями, які можуть генеруватися з використанням локально збережених платіжних облікових даних. В інших варіантах здійснення емітент 106 або платіжна мережа 114 можуть запитувати криптограми додатку у сервера 102 керування транзакціями, який може їх генерувати і повертати криптограми емітенту 106 або платіжній мережі 114 для перевірки достовірності в порівнянні з криптограмами, утвореними мобільним пристроєм 104.

[0047] Оскільки сервер 102 керування транзакціями має платіжні облікові дані й інші дані, що використовуються мобільним пристроєм 104 для генерування криптограм додатку, перевірка достовірності платіжних облікових даних, що утворюються мобільним пристроєм 104 для фінансування платіжної транзакції, може виконуватися за допомогою порівняння криптограм додатку, що генеруються мобільним пристроєм 104, і тих, які згенеровані сервером 102 керування транзакціями. У деяких варіантах здійснення сервер 102 керування транзакціями може бути частиною платіжної мережі 114 або емітента 106. У випадках, коли сервер 102 керування транзакціями може бути частиною платіжної мережі 114, перевірка достовірності може виконуватися перед контактуванням емітента 106 як частина традиційної обробки платіжної транзакції (наприклад, для схвалення фінансування транзакції, використовуючи транзакційний рахунок споживача 108 у емітента 106).

[0048] За допомогою використання численних криптограм додатку, може бути підвищена безпека платіжних транзакцій. Крім того, у випадках, коли кожна криптограма може аутентифікувати окремі дані, такі як випадки, коли одна криптограма аутентифікує мобільний пристрій 104, й інша аутентифікує як мобільний пристрій 104, так і споживача 108 (наприклад, за допомогою PIN споживача), вона також може надавати емітенту 106 додаткові дані і причини для використання при прийнятті рішення схвалити або відхилити транзакцію. Наприклад, якщо обидві криптограми некоректні (наприклад, криптограми, згенеровані мобільним пристроєм 104, не співпадають з тими, які були згенеровані сервером 102 керування транзакціями), транзакція може відхилятися. Якщо одна криптограма коректна, а друга некоректна, транзакція може бути відхилена з причин безпеки, або може бути схвалена, наприклад, основуючись на рішенні емітента 106. Наприклад, емітент 106 може схвалити транзакцію, де аутентифікація споживача завершується неуспішно, але проходить аутентифікація мобільного пристрою, оскільки інші доступні дані можуть вказувати, що авторизований користувач, але не споживач 108, використовує мобільний пристрій 104 для транзакції.

[0049] У результаті, використання обох криптограм може забезпечувати корисні дані, які можуть бути використані платіжними мережами 114 і емітентами 106 при обробці платіжних транзакцій. Крім того, використання двох або більше криптограм може забезпечувати підвищену безпеку, ніж в традиційних способах безконтактного або віддаленого платежу, яка може приводити до меншого шахрайства і більшого визнання для споживачів 108, емітентів 106 і торгово-сервісних підприємств. У випадках, коли використання двох або більше криптограм додатку генерується з платіжних облікових даних, які забезпечувалися безпечно з використанням способів і систем посилення повідомлень RNS, описаних в даному документі, і безпечно збережених за допомогою вдосконалених ключів зберігання, що генеруються з використанням способів і систем, описаних в даному документі, загальна безпека системи 100

може бути підвищена значною мірою в порівнянні з традиційними системами для обробки безконтактних платежів і транзакцій. У результаті, система 100 може забезпечувати підвищену безпеку в декількох аспектах передачі, зберіганні і обробці даних, ніж забезпечувалося в традиційних системах безконтактного платежу і для інших типів віддалених платіжних транзакцій і платіжних транзакцій загалом, які можуть використовувати способи і системи, описані в даному документі.

Мобільний пристрій

[0050] Фіг. 2 ілюструє варіант здійснення мобільного пристрою 104 системи 100. Для фахівця в даній галузі техніки очевидно, що варіант здійснення мобільного пристрою 104, зображеного на фіг. 2, надається тільки як ілюстрація і не може бути вичерпним для всіх можливих конфігурацій мобільного пристрою 104, придатних для виконання функцій, як описано в даному документі. Наприклад, комп'ютерна система 1700, зображена на фіг. 17 і описана детальніше нижче, може бути придатною конфігурацією мобільного пристрою 104.

[0051] Мобільний пристрій 104 може включати в себе приймальний блок 202. Приймальний блок 202 може бути виконаний з можливістю прийому даних по одній або декількох мережах за допомогою одного або декількох мережевих протоколів. Приймальний блок 202 може приймати, наприклад, програмні дані для однієї або декількох програм додатків, що підлягають встановленню на мобільному пристрої 104 і виконанню на ньому, таких як мобільний платіжний додаток (MPA), описаний детальніше нижче. Приймальний блок 202 також може приймати повідомлення служби віддалених сповіщень (RNS), таких як повідомлення, які передаються сервером 102 керування транзакціями, що включають в себе повідомлення RNS, які включають в себе платіжні облікові дані. Приймальний блок 202 також може приймати додаткові дані, придатні для виконання традиційних функцій мобільного пристрою 104, таких як телефонний зв'язок, стільниковий зв'язок і т. д. В деяких випадках мобільний пристрій 104 може включати в себе множину приймальних блоків 202, таких як окремі приймальні блоки 202, причому кожен виконаний з можливістю виконання зв'язку з однією або декількома окремими мережами за допомогою придатних протоколів. Наприклад, мобільний пристрій 104 може включати в себе перший приймальний блок 202 для прийому даних для транзакцій NFC, і другий приймальний блок 202 для прийому зв'язку по мережі мобільного зв'язку.

[0052] Мобільний пристрій 104 також може включати в себе блок 214 введення. Блок 214 введення може бути виконаний з можливістю виконання зв'язку з одним або декількома пристроями введення, які внутрішньо або зовнішньо підключені до мобільного пристрою 104 для прийому введення від споживача 108, такі як клавіатура, мишка, коліщатко керування, коліщатко прокрутки, сенсорний екран, мікрофон, камера, приймач і т. д. Блок 214 введення може приймати введення від споживача 108, який може бути оброблений блоком 204 обробки.

[0053] Блок 204 обробки може бути виконаний з можливістю виконання функцій мобільного пристрою 104, описаного в даному документі. Блок 214 обробки може виконувати програмний код, що зберігається в мобільному пристрої, такий як для MPA, і може бути виконаний з можливістю виконання множини функцій, асоційованих з кожною програмою додатку, в доповнення до інших функцій мобільного пристрою 104. Блок 204 обробки може приймати введення від споживача 108 за допомогою блока 214 введення і виконувати функції відповідним чином, наприклад, за допомогою виконання програм додатку, виконання функцій в програмах, прийом даних, передачу даних, відображення даних і т. д., що зрозуміло для фахівця в даній галузі техніки. Наприклад, блок 204 обробки може бути виконаний з можливістю перевірки достовірності повідомлень RNS, генерування вдосконалених ключів зберігання і генерування криптограм додатку, як описано детальніше нижче.

[0054] Мобільний пристрій 104 також може включати в себе блок 210 відображення. Блок 210 відображення може бути виконаний з можливістю виконання зв'язку з одним або декількома пристроями відображення, які внутрішньо або зовнішньо підключені до мобільного пристрою 104 для відображення даних, таких як дані, що передаються на блок 210 відображення для відображення блоком 204 обробки. Пристрої відображення можуть включати в себе рідкокристалічні дисплеї, дисплеї на світловипромінювальних діодах, дисплеї на тонкоплівкових транзисторах, дисплеї з сенсорним екраном і т. д.

[0055] Мобільний пристрій 104 також може включати в себе передавальний блок 206. Передавальний блок 206 може бути виконаний з можливістю передачі даних по одній або декільком мережах за допомогою одного або декількох мережевих протоколів. Передавальний блок 206 може передавати повідомлення у відповідь RNS на сервер 102 керування транзакціями. Передавальний блок 206 також може бути виконаний з можливістю передачі криптограм додатку і/або платіжних облікових даних, наприклад, торговій точці 110, для використання в платіжній транзакції. Передавальний блок 206 додатково може бути виконаний з

можливістю виконання додаткових функцій мобільного пристрою 104, що очевидно для фахівця в даній галузі техніки, таких як традиційні функції пристрою мобільного зв'язку для передачі стільникового зв'язку і т. д. В деяких випадках мобільний пристрій 104 може включати в себе множину передавальних блоків 206, які можуть бути окремо виконані з можливістю виконання зв'язку з однією або декількома окремими мережами, таких як передавальний блок 206, виконаний з можливістю передачі платіжних облікових даних і криптограм додатку за допомогою NFC, й інший передавальний блок 206, виконаний з можливістю передачі даних по мережі мобільного зв'язку.

[0056] Мобільний пристрій 104 також може включати в себе базу 208 даних карток. База 208 даних карток, описана детальніше нижче, може являти собою сховище даних на мобільному пристрої 104, яке виконане з можливістю зберігання даних, асоційованих з одним або декількома транзакційними рахунками і/або платіжними картками. База 208 даних карток може зберігати платіжні облікові дані, асоційовані з транзакційним рахунком, такі як надані мобільному пристрою 104 сервером 102 керування транзакціями в безпечному повідомленні RNS, і додаткові дані, які можуть використовуватися при генеруванні криптограм додатку, як описано детальніше нижче. У деяких випадках база 208 даних карток може зберігатися як частина мобільного платіжного додатку.

[0057] Мобільний пристрій 104 додатково може включати в себе пам'ять 212. Пам'ять 212, описана детальніше нижче, може бути виконана з можливістю зберігання даних для мобільного пристрою 104, придатних для виконання функцій мобільного пристрою 104, описаного в даному документі. Наприклад, пам'ять 212 може зберігати дані, придатні для генерування вдосконалених ключів зберігання для шифрування додаткових даних в мобільному пристрої 104, таких як база 208 даних карток, як описано детальніше нижче. Пам'ять 212 також може бути виконана з можливістю зберігання програмного коду для програм додатку, що виконуються блоком 204 обробки, таких як операційна система, програмний код для прийому даних за допомогою блока 214 введення і відображення даних за допомогою блока 210 відображення, правила і/або алгоритми для виконання функцій, описаних в даному документі, і т. д. Пам'ять 212 також може зберігати дані, придатні для виконання традиційних функцій мобільного пристрою 104, таких як правила і/або алгоритми для передачі і прийому стільникового зв'язку за допомогою мережі мобільного зв'язку. Додаткові дані, що зберігаються в пам'яті 212, очевидні для фахівця в даній галузі техніки.

База даних карток мобільного пристрою

[0058] Фіг. 3 ілюструє варіант здійснення бази 208 даних карток мобільного пристрою 104 для зберігання платіжних облікових даних й інших даних, асоційованих з транзакційними рахунками для використання при фінансуванні платіжних транзакцій, що проводяться за допомогою мобільного пристрою 108.

[0059] База 208 даних карток може включати в себе один або декілька платіжних профілів 302, зображених на фіг. 3, як платіжні профілі 302a, 302b і 302c. Кожний платіжний профіль 302 може асоціюватися з транзакційним рахунком, який може використовуватися для фінансування платіжної транзакції і може включати в себе щонайменше платіжні облікові дані 304, один або декілька разових ключів 306, перший сеансовий ключ 308, другий сеансовий ключ 310 і лічильник 312 транзакцій додатку.

[0060] Платіжні облікові дані 304 можуть включати в себе дані, асоційовані з відповідним транзакційним рахунком, який використовується для ідентифікації і перевірки достовірності платіжною мережею 114 і/або емітентом 106 при обробці платіжної транзакції, що використовує відповідний транзакційний рахунок. Платіжні облікові дані 304 можуть включати в себе, наприклад, номер рахунку платежу, код безпеки, дату закінчення терміну дії, ім'я держателя картки, ім'я авторизованного користувача, дані відстеження, дані опису компонування картки, числа цифр, бітові карти і т. д.

[0061] Разові ключі 306 можуть являти собою платіжні токени, дійсні для однієї платіжної транзакції, які можуть використовуватися блоком 204 обробки мобільного пристрою 104 для генерування однієї або декількох криптограм додатку, що використовується в платіжній транзакції. У деяких варіантах здійснення разовий ключ 306 може включати в себе один або декілька інших елементів даних, включених в платіжний профіль 302. Наприклад, кожний разовий ключ 306 може включати в себе окремий лічильник 312 транзакцій додатку, який може бути не включений окремо в платіжний профіль 302. Різні конфігурації даних, що зберігаються в платіжному профілі 302 для використання при виконанні функцій, описаних в даному документі, очевидні для фахівця в даній галузі техніки. У деяких випадках разовий ключ 306 може включати в себе, або може складатися з, ключа, що використовується для генерування однієї або декількох криптограм додатку. У деяких варіантах здійснення перший сеансовий ключ 308 і

другий сеансовий ключ 310 можуть бути включені в разовий ключ 306, що надається мобільному пристрою 104 і/або, що генерується з використанням даних, включених в разовий ключ 306.

[0062] Перший сеансовий ключ 308 і другий сеансовий ключ 310 можуть являти собою додаткові ключі, які використовуються блоком 204 обробки при генеруванні криптограм додатку, що передаються на торгову точку 110 як частину проведення платіжної транзакції, що використовує мобільний пристрій 104. У деяких варіантах здійснення перший сеансовий ключ 308 може використовуватися при генеруванні першої криптограми додатку блоком 204 обробки, наприклад, використовуючи програмний код, правила або алгоритми, які зберігаються в пам'яті 212 мобільного пристрою 104. Другий сеансовий ключ 310 може використовуватися при генеруванні другої криптограми додатку.

[0063] У деяких варіантах здійснення другий сеансовий ключ 310 може генеруватися блоком 204 обробки. У такому варіанті здійснення другий сеансовий ключ 310 може генеруватися з використанням разового ключа 306 і даних аутентифікації користувача, таких як PIN 108, що надається споживачем (наприклад, за допомогою блока 214 введення). У такому варіанті здійснення другий сеансовий ключ 310 може не зберігатися в платіжному профілі 302 і, замість цього, може генеруватися, використовуватися і відкидатися як частина процесу платіжної транзакції. Друга криптограма додатку, тому, може, при генеруванні з другого сеансового ключа 310, який генерується з використанням разового ключа 306 і PIN споживача, служити для аутентифікації як мобільного пристрою 104, так і споживача 108.

[0064] Персональний ідентифікаційний номер (PIN) може являти собою номер, що надається споживачем 108 (наприклад, під час реєстрації МРА на мобільному пристрої 104 або реєстрації транзакційного рахунку у емітента 106 і/або сервера 102 керування транзакціями), який може використовуватися для аутентифікації споживача 108. При проведенні платіжної транзакції споживач 108 або інший користувач мобільного пристрою 104 може надавати PIN за допомогою блока 214 введення. У деяких варіантах здійснення, якщо PIN, що надається є некоректним (наприклад, не співпадає з PIN, наданим споживачем 108 під час реєстрації), тоді блок 204 обробки може продовжувати генерування другого сеансового ключа 310 і потім генерування другої криптограми додатку. Якщо PIN, що надається є некоректним, тоді друга криптограма додатку, таким чином, буде некоректною, що приведе до неуспішної перевірки достовірності другої криптограми додатку сервером 102 керування транзакціями, емітентом 106 і/або платіжною мережею 114, що може надати емітенту 106 можливість відхилити транзакцію відповідним чином або все ж схвалити транзакцію.

Пам'ять мобільного пристрою

[0065] Фіг. 4 ілюструє варіант здійснення пам'яті 212 мобільного пристрою 104 для зберігання програм додатку й інших даних, що підлягають використанню в безпечному сховищі даних на мобільному пристрої 104 і для проведення платіжних транзакцій, що використовують мобільний пристрій 104. У зразковому варіанті здійснення пам'ять 212 не може бути елементом безпеки.

[0066] Пам'ять 212 може включати в себе інформацію 402 про пристрій. Інформація 402 про пристрій може включати в себе одну або декілька порцій даних, асоційованих з мобільним пристроєм 104, які, в деяких випадках, можуть бути унікальними для мобільного пристрою 104. Наприклад, інформація 402 про пристрій може включати в себе адресу керування доступом до середовища передачі, еталонний номер, серійний номер, ідентифікаційний номер і т. д. Додаткова інформація, яка може розглядатися як інформація 402 про пристрій мобільного пристрою 104, очевидна для фахівця в даній галузі техніки.

[0067] Пам'ять 212 також може включати в себе мобільний платіжний додаток (МРА) 404. МРА 404 може являти собою програму додатку, виконану з можливістю виконання функцій мобільного пристрою 104, описаних в даному документі, таких як прийом і зберігання платіжних облікових даних, перевірка достовірності повідомлень RNS і генерування криптограм додатку для використання при проведенні платіжних транзакцій. Додаткові ознаки МРА 404 можуть включати в себе традиційні ознаки цифрового гаманця або іншої подібної програми додатку, що очевидно для фахівця в даній галузі техніки.

[0068] МРА 404 може включати в себе програмний код 406. Програмний код 406 може являти собою код, що виконується блоком 204 обробки мобільного пристрою 104, який спричиняє виконання блоком 204 обробки й іншими компонентами мобільного пристрою 104 функцій МРА 404, як описано в даному документі. Наприклад, програмний код 406 може включати в себе код, придатний для генерування криптограм додатку, перевірки достовірності повідомлень RNS і т. д. Програмний код 406 також може включати в себе програмний код, придатний для генерування випадкового значення, яке може використовуватися при

генеруванні вдосконаленого ключа зберігання. Випадкове значення може являти собою випадкове або псевдовипадкове число, яке може генеруватися з використанням способів і систем, які очевидні для фахівця в даній галузі техніки.

[0069] МРА 404 також може включати в себе ідентифікатор 408 екземпляра. Ідентифікатор 408 екземпляра може являти собою значення, унікальне для конкретного МРА 404, яке може використовуватися при генеруванні вдосконаленого ключа зберігання, що використовується для забезпечення безпеки даних в мобільному пристрої 104, таких як база 208 даних карток. Маючи ідентифікатор 408 екземпляра унікальним для МРА 404, численні МРА 404 можуть бути встановлені на мобільному пристрої 104, причому будь-яке одне МРА 404 не може виконати доступ до даних, які безпечно збережені будь-яким іншим МРА 404, що, таким чином, може гарантувати, що платіжні профілі 302 для конкретних транзакційних рахунків не є доступними для інших програм. Ідентифікатором 408 екземпляра може бути число, буквено-цифрове значення, шістнадцяткове значення або будь-яке придатне значення, яке може бути унікальним для МРА 404.

[0070] Як описано детальніше нижче, блок 204 обробки мобільного пристрою 104 може бути виконаний з можливістю генерування значення диверсифікатора, використовуючи інформацію 402 про пристрій, випадкове значення, що генерується з використанням програмного коду 406 МРА 404, і ідентифікатора 408 екземпляра, що зберігається в МРА 404. Значення диверсифікатора може використовуватися криптографічним додатком 410, що також зберігається в пам'яті 212. Криптографічний додаток 410 може являти собою програму додатку, виконану з можливістю виконання криптографії типу "білий ящик" і/або будь-якої іншої придатної криптографічної функції, яка очевидна для фахівця в даній галузі техніки.

[0071] Криптографічний додаток 410 може включати в себе програмний код 412. Програмний код 412 може виконуватися блоком 204 обробки мобільного пристрою 104, роблячи можливим виконання блоком 204 обробки і іншими компонентами мобільного пристрою 104 криптографічних функцій криптографічного додатку 410, описаних в даному документі. Функції можуть включати в себе генерування вдосконаленого ключа зберігання. Вдосконалений ключ зберігання може генеруватися з використанням значення диверсифікатора, що генерується мобільним платіжним додатком 404 і ключем 414 шифрування, включеним в криптографічний додаток 410. У деяких варіантах здійснення ключ диверсифікатора може розшифровуватися з використанням ключа 414 шифрування для отримання вдосконаленого ключа зберігання.

[0072] Криптографічний додаток 410 також може бути виконаний з можливістю шифрування сховища в мобільному пристрої 104, використовуючи вдосконалений ключ зберігання. У деяких варіантах здійснення шифрування може виконуватися з використанням одного або декількох методів криптографії типу "білий ящик". Зашифрованим сховищем може бути база 208 даних карток і/або будь-яке інше придатне сховище в мобільному пристрої 104, таке як дані, що зберігаються в МРА 404. У деяких варіантах здійснення криптографічний додаток 410 може бути включений як частина МРА 404. Вдосконалений ключ зберігання може зберігатися в криптографічному додатку 410 або МРА 404, або, в деяких випадках, може повторно генеруватися за допомогою МРА 404 і криптографічним додатком 410, коли це необхідне.

[0073] Пам'ять 212 також може включати в себе будь-які додаткові дані, що зберігаються в мобільному пристрої 104, придатні для виконання функцій, описаних в даному документі, а також будь-яких додаткових функцій мобільних пристроїв. Наприклад, пам'ять 212 може включати в себе програмний код для операційної системи, код, правила або алгоритми для прийому і передачі мобільного зв'язку, такого як телефонні виклики і т. д.

[0074] У деяких варіантах здійснення мобільний пристрій 104 також може бути виконаний з можливістю прийому даних, вже зашифрованих з використанням вдосконаленого ключа зберігання, які можуть зберігатися в зашифрованому локальному сховищі в мобільному пристрої 104, наприклад, в пам'яті 212, базі 208 даних карток або в іншому придатному сховищі. У такому варіанті здійснення мобільний пристрій 104 може бути виконаний з можливістю передачі випадкового значення, що генерується серверу 102 керування транзакціями або іншому довіреному об'єкту, який може генерувати вдосконалений ключ зберігання, використовуючи ці ж способи і системи, що використовують згенероване випадкове значення, і може шифрувати дані, які надаються мобільному пристрою 104. Мобільний пристрій 104, таким чином, може приймати дані, вже зашифровані з використанням вдосконаленого ключа зберігання, для локального сховища в мобільному пристрої 104.

Сервер керування транзакціями

[0075] Фіг. 5 ілюструє варіант здійснення сервера 102 керування транзакціями системи 100. Для фахівця в даній галузі техніки очевидно, що варіант здійснення сервера 102 керування транзакціями, зображеного на фіг. 5, надається як тільки ілюстрація і не може бути вичерпним

для всіх можливих конфігурацій сервера 102 керування транзакціями, придатних для виконання функцій, як описано в даному документі. Наприклад, комп'ютерна система 1700, зображена на фіг. 17 і описана детальніше нижче, може являти собою придатну конфігурацію сервера 102 керування транзакціями.

5 [0076] Сервер 102 керування транзакціями може включати в себе приймальний блок 502. Приймальний блок 502 може бути виконаний з можливістю прийому даних по одній або декількох мережах за допомогою одного або декількох мережевих протоколів. Приймальний блок 502 може приймати дані від мобільного пристрою 104, наприклад, прийом повідомлення, які повертаються, повідомлень підтвердження, сповіщень транзакції і т. д., платіжної мережі 10 114, емітента 106 або іншого придатного об'єкта. Приймальний блок 502 може приймати сповіщення транзакції або запити криптограми, наприклад, щоб ініціювати генерування криптограм додатку для використання при перевірці достовірності платіжних облікових даних в платіжній транзакції. Приймальний блок 502 також може приймати дані транзакційного рахунку, наприклад, від емітента 106, для використання при генеруванні платіжних облікових даних для 15 надання мобільному пристрою 104.

[0077] Сервер 102 керування транзакціями також може включати в себе блок 504 обробки. Блок 504 обробки може бути виконаний з можливістю виконання функцій сервера 102 керування транзакціями, описаних в даному документі, що очевидно для фахівця в даній галузі техніки. Блок 504 обробки, таким чином, може бути виконаний з можливістю генерування і шифрування 20 повідомлень RNS і даних, включеного в них, перевірки достовірності повідомлення, які повертаються від мобільного пристрою 104, генерування платіжних облікових даних, генерування криптограм додатку, перевірки достовірності криптограм додатку і т. д., як описано детальніше нижче.

[0078] Сервер 102 керування транзакціями додатково може включати в себе передавальний 25 блок 506. Передавальний блок 506 може бути виконаний з можливістю передачі даних по одній або декільком мережам за допомогою одного або декількох мережевих протоколів. Передавальний блок 506 може передавати повідомлення RNS, платіжні облікові дані, криптограми додатку, сповіщення перевірки достовірності й інші дані, які очевидні для фахівця в даній галузі техніки. Передавальний блок 506 може бути виконаний з можливістю передачі 30 даних на мобільний пристрій 104, наприклад, за допомогою мережі мобільного зв'язку або Інтернету, платіжної мережі 114, емітенту 106 і будь-якому іншому придатному об'єкту.

[0079] Сервер 102 керування транзакціями також може включати в себе базу 508 даних рахунків. База 508 даних рахунків, описана детальніше нижче, може бути виконана з 35 можливістю зберігання інформації про рахунок для множини транзакційних рахунків. Інформація про рахунок може включати в себе дані й ключі, що використовуються для генерування криптограм додатку, що використовуються при перевірці достовірності платіжних облікових даних, що приймаються під час платіжних транзакцій, що проводяться з використанням мобільного пристрою 104. База 508 даних рахунків також може бути виконана з можливістю 40 зберігання даних про транзакцію для платіжних транзакцій, що проводяться з участю мобільного пристрою 104, й інших даних, таких як дані, асоційовані зі споживачем 108 або іншими авторизованими користувачами відповідного транзакційного рахунку.

[0080] Сервер 102 керування транзакціями також може включати в себе пам'ять 510. Пам'ять 510 може бути виконана з можливістю зберігання додаткових даних для використання сервером 102 керування транзакціями при виконанні функцій, описаних в даному документі. 45 Наприклад, пам'ять 510 може зберігати правила або алгоритми для перевірки достовірності криптограм додатку, правила або алгоритми для генерування сповіщень перевірки достовірності, алгоритми для генерування сеансових ключів і криптограм додатку, ключів шифрування для шифрування і розшифрування даних і повідомлень RNS і т. д. Додаткові дані, які можуть зберігатися в пам'яті 510, очевидні для фахівця в даній галузі техніки.

50 База даних рахунків сервера керування транзакціями

[0081] Фіг. 6 ілюструє варіант здійснення бази 508 даних рахунків сервера 102 керування транзакціями для зберігання даних, що стосуються транзакційних рахунків для використання при перевірці достовірності платіжних облікових даних й інших даних про транзакцію, платіжних 55 транзакцій, що забезпечуються при проведенні, що включають використання мобільного пристрою 104.

[0082] База 508 даних рахунків може включати в себе множину профілів 602 рахунку, зображених на фіг. 6, як профілі 602a, 602b і 602c рахунку. Кожний профіль 602 рахунку може включати в себе один або декілька разових ключів 604, перший сеансовий ключ 606, другий 60 сеансовий ключ 608, лічильник 610 транзакцій додатку і перший головний ключ 612 картки. У

деяких варіантах здійснення профіль 602 рахунку додатково може включати в себе другий головний ключ 612 картки.

[0083] Кожний профіль 602 рахунку може відповідати платіжному профілю 302, що надається мобільному пристрою 104. По суті, разові ключі 604, що зберігаються в профілі 602 рахунку, можуть відповідати разовим ключам 306, що зберігаються у відповідному платіжному профілі 302, що стосується цього ж транзакційного рахунку. Дані можуть бути подібними, так що, коли криптограма додатку генерується сервером 102 керування транзакціями або мобільним пристроєм 104, криптограми додатку повинні співпадати, якщо дані вірні і не були підроблені, що може робити можливою перевірку достовірності платіжних облікових даних, представлених мобільним пристроєм 104.

[0084] У деяких варіантах здійснення профіль 602 рахунку може включати в себе персональний ідентифікаційний номер (PIN), який відповідає PIN 314, що зберігається у відповідному платіжному профілі 302. У такому варіанті здійснення PIN 314 може надаватися приймальному блоку 202 сервера 102 керування транзакціями в безпечному повідомленні, такому як повідомлення отримання, що надається мобільним пристроєм 104, описане детальніше нижче. В інших варіантах здійснення головний ключ картки може використовуватися замість PIN, такий як перший головний ключ 612 картки. У такому варіанті здійснення блок 504 обробки сервера 102 керування транзакціями може бути виконаний з можливістю генерування другого сеансового ключа 608, засновуючись на другому головному ключі 614 картки, який відповідає другому сеансовому ключу 310, що генерується мобільним пристроєм 104, використовуючи разовий ключ 306 і PIN 314. У деяких випадках другий сеансовий ключ 608 також може засновуватися на відповідному разовому ключі 604. У таких варіантах здійснення алгоритми для генерування сеансових ключів і/або криптограм додатку можуть гарантувати, що криптограми, які генеруються мобільним пристроєм 104 і сервером 102 керування транзакціями, відповідають на основі даних, що використовуються в них.

[0085] Перший сеансовий ключ 606 може використовуватися блоком 504 обробки сервера 102 керування транзакціями для генерування першої криптограми додатку, і другий сеансовий ключ 608 може використовуватися для генерування другої криптограми додатку. У деяких варіантах здійснення лічильник 610 транзакцій додатку може використовуватися при генеруванні одного або декількох сеансових ключів і/або криптограм додатку. Лічильник 610 транзакцій додатку може являти собою значення, відповідне платіжній транзакції, що проводиться, яке збільшується або іншим чином модифікується під час кожної транзакції. Лічильник 610 транзакцій додатку може відповідати лічильнику 312 транзакцій додатку, що зберігається у відповідному платіжному профілі 302 в мобільному пристрої 104, так що його використання може гарантувати, що тільки достовірне МРА 404 може мати коректний лічильник 312 транзакцій додатку для генерування достовірних сеансових ключів і/або криптограм додатку. Можуть використовуватися додаткові методи для додаткового підвищення безпеки генерування сеансового ключа і/або криптограми додатку, такі як непередбачувані числа й інші методи, які очевидні для фахівця в даній галузі техніки.

Обробка платіжних транзакцій, використовуючи мобільний пристрій

[0086] Фіг. 7 ілюструє процес обробки платіжних транзакцій, що проводяться з використанням мобільного пристрою 104 без елемента безпеки і з використанням генерування і перевірки достовірності двох або більше криптограм додатку.

[0087] На етапі 702 сервер 102 керування транзакціями може надавати (наприклад, за допомогою передавального блоку 506) платіжні облікові дані 304 і інші дані рахунку мобільному пристрою 104, наприклад, за допомогою повідомлення RNS, описаного детальніше нижче. На етапі 704 приймальний блок 202 мобільного пристрою 104 може приймати платіжні облікові дані 304 і інші дані рахунку. На етапі 706 блок 204 обробки мобільного пристрою 104 може зберігати дані в платіжному профілі 302 в базі 208 даних карток. Дані рахунку можуть включати в себе платіжні облікові дані 304, один або декілька разових ключів 308 і будь-які інші придатні дані, такі як один або декілька сеансових ключів 308 і 310.

[0088] На етапі 708 блок 204 обробки може генерувати дві криптограми додатку для використання при проведенні платіжної транзакції. У деяких варіантах здійснення етап 708 може ініціюватися споживачем 108, наприклад, вказівкою за допомогою блоку 214 введення, за допомогою розміщення мобільного пристрою 104 біля торгової точки 110 для ініціювання транзакції за допомогою зв'язку малого радіуса дії або іншим придатним способом. Генерування криптограм додатку може включати в себе генерування першої криптограми додатку, використовуючи перший сеансовий ключ 308, що зберігається в платіжному профілі 302. Друга криптограма додатку може генеруватися з використанням другого сеансового ключа 310, який може генеруватися з використанням разового ключа 306 і PIN 314. У деяких випадках споживач

108 може водити PIN в мобільному пристрої 104 (наприклад, за допомогою блока 214 введення) перед етапом 708 або під час ініціювання етапу 708. У деяких варіантах здійснення одна або обидві криптограми додатку також можуть генеруватися з використанням лічильника 312 транзакцій додатку.

5 [0089] Якщо криптограми додатку були згенеровані, вони, разом з платіжними обліковими даними 304, можуть передаватися емітенту 106 за допомогою торгової точки 110, екваєра і платіжної мережі 114. Платіжні облікові дані 304 і криптограми додатку можуть прийматися емітентом 106 на етапі 710. На етапі 712 передавальний блок 206 мобільного пристрою 104 може передавати сповіщення про транзакцію серверу 102 керування транзакціями. На етапі 714
10 приймальний блок 502 сервера 102 керування транзакціями може приймати сповіщення про транзакцію. Сповіщення про транзакцію може сповіщувати сервер 102 керування транзакціями, що мобільний пристрій 104 ініціював платіжну транзакцію, використовуючи платіжний профіль 302. У деяких випадках сповіщення про транзакцію може включати в себе ідентифікаційну інформацію.

15 [0090] На етапі 716 блок 504 обробки сервера 102 керування транзакціями може ідентифікувати профіль 602 рахунку, відповідний платіжному профілю 302, і може генерувати дві криптограми додатку, використовуючи дані, що містяться в них. Перша криптограма додатку може генеруватися з використанням першого сеансового ключа 606, який може генеруватися з використанням першого головного ключа 612 картки. Друга криптограма додатку може
20 генеруватися з використанням другого сеансового ключа 608. У деяких варіантах здійснення одна або обидві криптограми додатку і/або сеансові ключі можуть додатково засновуватися на разових ключах 604, лічильнику 610 транзакцій додатку або будь-яких інших придатних даних.

[0091] На етапі 718 передавальний блок 506 сервера 102 керування транзакціями може передавати згенеровані криптограми додатку емітенту 106, який може приймати криптограми на
25 етапі 718. На етапі 720 емітент 106 може перевіряти достовірність криптограм додатку, що надаються мобільним пристроєм 104, що супроводжує платіжні облікові дані 304. Перевірка достовірності криптограм додатку може включати в себе порівняння представлених мобільним пристроєм 104 криптограм з криптограмами додатку, згенерованими і представленими сервером 102 керування транзакціями. Якщо перевірка достовірності виконана, потім, на етапі
30 722, емітент 106 може обробляти транзакцію відповідним чином. Обробка транзакції може включати в себе схвалення платіжної транзакції, наприклад, якщо одна або обидві криптограми перевірені на достовірність, або відхилення платіжної транзакції, наприклад, якщо визначено, що одна або обидві криптограми є недостовірними.

[0092] На етапі 724 сповіщення про транзакцію може передаватися емітентом 106, або
35 іншим об'єктом (наприклад, платіжною мережею 114, екваєром 112 і т. д.) як частина обробки платіжної транзакції. Сповіщення про транзакцію може передаватися серверу 102 керування транзакціями і може прийматися приймальним блоком 502 на етапі 726. Сповіщення про транзакцію також може прийматися приймальним блоком 202 мобільного пристрою 104 на етапі 728. Сповіщення про транзакцію може являти собою вказівку схвалення або відхилення платіжної транзакції. Кожний з блоків 204 і 504 обробки мобільного пристрою 104 і сервера 102
40 керування транзакціями відповідно може виконувати одну або декілька функцій внаслідок прийнятого сповіщення про транзакцію. Наприклад, якщо транзакція була схвалена й успішно оброблена, лічильники 310 і 610 транзакцій додатку у відповідних профілях можуть оновлюватися відповідним чином.

45 [0093] Фіг. 8 ілюструє альтернативний процес обробки платіжної транзакції з використанням мобільного пристрою 104.

[0094] На етапі 802 платіжні облікові дані 304 й інші дані рахунки можуть передаватися мобільному пристрою 104 передавальним блоком 506 сервера 102 керування транзакціями. На
50 етапі 804 приймальний блок 202 мобільного пристрою 104 може приймати платіжні облікові дані 304 й інші дані рахунки, які можуть зберігатися в платіжному профілі 302 на етапі 806. На етапі 808 блок 204 обробки мобільного пристрою 104 може генерувати дві криптограми додатку, як описано вище, і може передавати криптограми, платіжні облікові дані 304 й інші придатні дані емітенту 106 (наприклад, за допомогою торгової точки 110).

[0095] На етапі 810 емітент 106 може приймати криптограми додатку і будь-які інші придатні
55 дані, які можуть використовуватися емітентом 106 для перевірки достовірності даних об транзакції і/або обробки схвалення або відхилення транзакції. На етапі 812 емітент 106 може представити запит на перевірку достовірності криптограм серверу 102 керування транзакціями. У деяких варіантах здійснення запит може включати в себе платіжні облікові дані 304 або інші дані, придатні для використання сервером 102 керування транзакціями при ідентифікації
60 профілю 602 рахунку, що підлягають використанню для генерування криптограм перевірки

достовірності. В одному варіанті здійснення запит може додатково включати в себе дві криптограми додатку, згенеровані мобільним пристроєм 104 для перевірки достовірності.

[0096] На етапі 814 приймальний блок 502 сервера 102 керування транзакціями може приймати запит криптограм. На етапі 816 блок 504 обробки сервера 102 керування транзакціями може генерувати дві криптограми додатку, що підлягають використанню для перевірки достовірності, як описано вище. У варіантах здійснення, де запит криптограм також включає в себе дві криптограми додатку, згенеровані мобільним пристроєм 104, етап 816 також може включати в себе перевірку достовірності двох криптограм блоком 504 обробки, використовуючи дві знову згенеровані криптограми додатку. Криптограми перевірки достовірності, або результат перевірки достовірності в застосовних варіантах здійснення, можуть передаватися передавальним блоком 506 емітенту 106. На етапі 818 емітент 106 може приймати криптограми перевірки достовірності і/або результат перевірки достовірності.

[0097] На етапі 820 емітент 106 може перевіряти достовірність криптограм додатку, наданих мобільним пристроєм 104, використовуючи криптограми додатку, згенеровані сервером 102 керування транзакціями. У варіантах здійснення, де сервер 102 керування транзакціями надає результат перевірки достовірності емітенту 106, етап 820 може включати в себе ідентифікацію результату перевірки достовірності кожної з двох криптограм додатку. На етапі 822 емітент 106 може обробляти платіжну транзакцію відповідним чином, основуючись на результаті перевірки достовірності. На етапі 824 сповіщення про транзакцію можуть передаватися серверу 102 керування транзакціями і мобільному пристрою 104, що приймаються відповідними приймальними блоками 502 і 202 на етапах 826 і 828 відповідно.

Служба віддалених сповіщень і передача повідомлень з даними

[0098] Фіг. 9 ілюструє процес передачі і перевірки достовірності повідомлень служби віддалених сповіщень (RNS) й інших повідомлень з даними, що передається з сервера 102 керування транзакціями на мобільний пристрій 104. Повідомлення RNS можуть передаватися за допомогою служби віддалених сповіщень, такої як служба, яка використовує мережу мобільного зв'язку, асоційовану з мобільним пристроєм 104. Повідомлення RNS можуть використовуватися для надання платіжних облікових даних 304 й інших даних рахунку мобільному пристрою 104, таких як дані рахунки, що використовуються при обробці платіжних транзакцій, як описано вище, й іншу інформацію, яка може використовуватися при встановленні безпечного з'єднання між мобільним пристроєм 104 і сервером 102 керування транзакціями.

[0099] На етапі 902 блок 504 обробки сервера 102 керування транзакціями може генерувати повідомлення. У випадках, коли взаємна аутентифікація встановлюється з мобільним пристроєм 104, повідомлення може включати в себе інформацію, придатну для встановлення взаємної аутентифікації, такої як ідентифікатор сеансу. В інших випадках, таких як, коли взаємна аутентифікація була встановлена між сервером 102 керування транзакціями і мобільним пристроєм 104, використовуючи процес, зображений на фіг. 9 і описаний в даному документі, згенероване повідомлення може включати в себе платіжні облікові дані 304 і дані рахунки, може включати в себе одну або декілька команд для виконання за допомогою МРА 404 мобільного пристрою 104 (наприклад, віддалення разових ключів 306 або платіжних облікових даних 304 і т. д.), може являти собою сповіщення для представлення споживачеві 108 (наприклад, залишок на рахунку, сповіщення платежу і т. д.), або може включати в себе інші придатні дані.

[0100] На етапі 904 блок 504 обробки може шифрувати згенероване повідомлення. Повідомлення може шифруватися з використанням секретного ключа з пари з секретного/відкривального ключа, де мобільний пристрій 104 може мати відповідний відкритий ключ. У деяких випадках повідомлення може шифруватися з використанням ключа шифрування, асоційованого з мобільним пристроєм 104 або МРА 404, таким як ключ 414 шифрування. На етапі 906 блок 504 обробки може генерувати код аутентифікації повідомлень. Код аутентифікації повідомлень може генеруватися з використанням зашифрованого повідомлення і може являти собою ключ, який генерується з використанням одного або декількох спеціально сконфігурованих правил і/або алгоритмів. Наприклад, код аутентифікації повідомлень може генеруватися з використанням одного або декількох способів шифрування і заплутування, таких як заповнення незначущою інформацією. У деяких варіантах здійснення код аутентифікації повідомлень може генеруватися з використанням ключа шифрування.

[0101] На етапі 908 передавальний блок 506 сервера 102 керування транзакціями може передавати повідомлення з об'єднаними даними на мобільний пристрій 104. У варіантах здійснення, де може виконуватися взаємна аутентифікація, повідомлення з об'єднаними даними може являти собою повідомлення служби віддалених сповіщень, що передається на мобільний пристрій 104 за допомогою служби віддалених сповіщень. Повідомлення з об'єднаними даними

може прийматися приймальним блоком 202 мобільного пристрою 104 на етапі 910 і може включати в себе код аутентифікації повідомлень і зашифроване повідомлення. У деяких випадках повідомлення з об'єднаними даними також може включати в себе додатковий ідентифікатор, такий як ідентифікатор, згенерований з використанням способів, відомих для МРА 404 для перевірки його достовірності. У деяких випадках, таких як коли взаємна аутентифікація вже була виконана, повідомлення з об'єднаними даними також може включати в себе лічильник повідомлень.

[0102] На етапі 912 блок 204 обробки може генерувати еталонний код аутентифікації. Еталонний код аутентифікації може генеруватися з використанням прийнятого зашифрованого повідомлення і може генеруватися з використанням таких же правил і алгоритмів, які сервер 102 керування транзакціями використовував для генерування коду аутентифікації повідомлень, так що згенерований еталонний код аутентифікації буде відповідати коду аутентифікації повідомлень, якщо код аутентифікації повідомлень генерується достовірним джерелом (наприклад, сервером 102 керування транзакціями). У варіантах здійснення, де код аутентифікації повідомлень може генеруватися з використанням ключа шифрування, блок 204 обробки може генерувати еталонний код аутентифікації, використовуючи ключ 414 шифрування, що зберігається в пам'яті 212, або інший придатний ключ шифрування.

[0103] На етапі 914 блок 204 обробки може перевіряти достовірність коду аутентифікації повідомлень, включеного в прийняте повідомлення з об'єднаними даними, за допомогою порівняння його зі згенерованим еталонним кодом аутентифікації. Якщо перевірена достовірність як лічильник повідомлень, так і коду аутентифікації повідомлень, тоді може визначатися, що повідомлення з об'єднаними даними є достовірним (наприклад, справжнім), як що надходить з сервера 102 керування транзакціями. У випадках, коли повідомлення з об'єднаними даними може включати в себе ідентифікатор повідомлення, блок 204 обробки також може перевіряти достовірність ідентифікатора повідомлення за допомогою генерування ідентифікатора повідомлення, використовуючи процес, відомий для МРА 404 для генерування і порівняння його. У варіантах здійснення, де повідомлення з об'єднаними даними може включати в себе лічильник повідомлень, блок 204 обробки може перевіряти достовірність лічильника повідомлень, включеного в прийняте повідомлення з об'єднаними даними, з еталонним лічильником, що зберігається в мобільному пристрої 104, наприклад, в МРА 404 або в платіжному профілі 502.

[0104] На етапі 916 блок 204 обробки може розшифровувати зашифроване повідомлення, включене в прийняте повідомлення з об'єднаними даними. Зашифроване повідомлення може розшифровуватися з використанням ключа, такого як ключ, що зберігається в пам'яті 212 (наприклад, в криптографічному додатку 410 або МРА 404) або що зберігається в локальній зашифрованій базі даних (наприклад, зашифрованої з використанням вдосконаленого ключа зберігання) або іншого придатного способу розшифрування. На етапі 918 блок 204 обробки може виконувати одну або декілька відповідних дій, оснований на даних, розшифрованих із зашифрованого повідомлення. У прикладі, зображеному на фіг. 9, мобільний пристрій 104 може виконувати взаємну аутентифікацію з сервером 102 керування транзакціями, наприклад, використовуючи ідентифікатор сеансу, включений в зашифроване повідомлення і розшифрований блоком 204 обробки. На етапі 920 сервер 102 керування транзакціями може приймати ідентифікатор сеансу і виконувати будь-які додаткові дії, необхідні для взаємної аутентифікації з мобільним пристроєм 104. У випадках, коли взаємна аутентифікація вже була виконана, повідомлення може включати в себе іншу інформацію, придатну для виконання функцій, описаних в даному документі, таку як платіжні облікові дані 404, разові ключі 406, програмні інструкції для МРА 404 і т. д.

[0105] У деяких варіантах здійснення мобільний пристрій 104 може бути виконаний (наприклад, за допомогою МРА 404) з можливістю генерування і представлення повідомлення серверу 100 керування транзакціями, яке повертається. У деяких випадках повідомлення, яке повертається, може включати в себе дані, що генеруються у відповідь на дії, які виконуються так, як інструктовано в розшифрованому повідомленні, як описано вище. Наприклад, повідомлення, яке повертається може вказувати достовірне отримання і збереження платіжних облікових даних 304 або разових ключів 306. В інших випадках повідомлення, яке повертається, може являти собою сповіщення про отримання і перевірку достовірності повідомлення з об'єднаними даними. У випадках, коли взаємна аутентифікація виконується уперше, повідомлення, яке повертається, може включати в себе ідентифікатор сеансу, що використовується для виконання взаємної аутентифікації.

[0106] Фіг. 10А і 10В зображують процес генерування і передачі повідомлення, яке повертається мобільним пристроєм 104 і перевірки його достовірності сервером 102 керування транзакціями.

[0107] На етапі 1002 блок 204 обробки мобільного пристрою 104 може генерувати повідомлення отримання. Повідомлення отримання може генеруватися на основі програмного коду 406, що зберігається в МРА 404, і може додатково засновуватися на діях, що виконуються так, як указано в розшифрованому повідомленні з об'єднаними даними, що приймається від сервера 102 керування транзакціями. Наприклад, повідомлення отримання може включати в себе сповіщення про успішне отримання і збереження платіжних облікових даних 304. На етапі 1004 блок 204 обробки може збільшити лічильник отримання. Лічильник отримання може являти собою лічильник, який указує кількість повідомлень отримання, переданих на сервер 102 керування транзакціями. Лічильник отримання може зберігатися в пам'яті 212, наприклад, в МРА 404, або в базі даних, зашифрований з використанням вдосконаленого ключа зберігання. Для фахівця в даній галузі техніки очевидно, що етап 1004 може бути необов'язковим етапом і може використовуватися тільки у випадках, коли лічильник використовується для перевірки достовірності повідомлення з даними.

[0108] На етапі 1006 блок 204 обробки може шифрувати повідомлення отримання. Повідомлення отримання може шифруватися з використанням ключа 414 шифрування, що зберігається в криптографічному додатку 410, або може іншим чином зберігатися в МРА 404 або локально зашифрованій базі даних. Ключ шифрування, що використовується для шифрування повідомлення отримання, може являти собою секретний ключ як частину пари ключів, причому сервер 102 керування транзакціями має відповідний відкритий ключ. На етапі 1008 блок 204 обробки може генерувати код аутентифікації отримання, оснований на зашифрованому повідомленні отримання. У деяких варіантах здійснення код аутентифікації отримання може генеруватися з використанням цих же правил, алгоритмів і/або процесів, які використовувалися для генерування еталонного коду аутентифікації, зображеного на етапі 912 на фіг. 9, описаної вище.

[0109] На етапі 1010 передавальний блок 206 мобільного пристрою 104 може передавати повідомлення сповіщення про отримання серверу 102 керування транзакціями. Повідомлення сповіщення про отримання може прийматися приймальним блоком 502 сервера 102 керування транзакціями і може включати в себе щонайменше код аутентифікації отримання, зашифроване повідомлення отримання і лічильник отримання. У деяких варіантах здійснення повідомлення сповіщення про отримання може передаватися серверу 102 керування транзакціями, використовуючи мережу мобільного зв'язку, таку як стільникова мережа, асоційована з мобільним пристроєм 104.

[0110] На етапі 1014 блок 504 обробки сервера 102 керування транзакціями може збільшувати лічильник підтверджень. Лічильник підтверджень може вказувати кількість повідомлень, прийнятих від мобільного пристрою 104, що використовується для перевірки достовірності повідомлень, що приймаються від мобільного пристрою 104. Лічильник підтверджень може зберігатися в пам'яті 510 сервера 102 керування транзакціями або в іншому придатному сховищі даних. Наприклад, в деяких варіантах здійснення лічильник підтверджень може зберігатися в профілі 602 рахунку, асоційованому з мобільним пристроєм 104. В одному прикладі кожний профіль 602 рахунку може включати в себе лічильник підтверджень (наприклад, і/або лічильник повідомлень), що підлягає використанню для повідомлень, що передаються на/від сервера 102 керування транзакціями і мобільного пристрою 104, що стосується відповідного транзакційного рахунку. Для фахівця в даній галузі техніки очевидно, що етап 1014 може бути необов'язковим етапом і може не виконуватися у випадках, коли лічильник може не використовуватися для перевірки достовірності повідомлення, які повертаються.

[0111] На етапі 1016 блок 504 обробки може генерувати код аутентифікації підтвердження. Код аутентифікації підтвердження може генеруватися на основі зашифрованого повідомлення отримання, включеного в повідомлення сповіщення про отримання, і може генеруватися з використанням цих же правил, алгоритмів і/або процесів, що використовуються для генерування коду аутентифікації повідомлень. На етапі 1018 блок 504 обробки може перевіряти достовірність лічильника отримання, включеного в повідомлення сповіщення про отримання за допомогою порівняння його з лічильником підтверджень. На етапі 1020 блок 504 обробки може перевіряти достовірність коду аутентифікації отримання за допомогою порівняння його з кодом аутентифікації повідомлень, щоб гарантувати, що повідомлення відбувається від авторизованого мобільного пристрою 104.

[0112] Якщо перевірена достовірність лічильника (наприклад, якщо застосовно) і коду аутентифікації, тоді на етапі 1022 блок 504 обробки може розшифровувати зашифроване повідомлення, включене в прийняте повідомлення сповіщення про отримання. Зашифроване повідомлення може розшифровуватися з використанням ключа шифрування, що зберігається або іншого придатного способу розшифровування. Зашифроване повідомлення може розшифровуватися для отримання повідомлення отримання, що генерується мобільним пристроєм 104. На етапі 1024 блок 504 обробки може виконувати будь-які відповідні дії по мірі необхідності, засновуючись на даних, включених в повідомлення отримання. Наприклад, якщо повідомлення отримання включає в себе вказівку на успішне отримання і збереження разових ключів 306, блок 204 обробки може активізувати відповідні разові ключі 604 у відповідному профілі 602 рахунку.

Перевірка достовірності повідомлень з даними

[0113] Фіг. 11 ілюструє процес 1100 перевірки достовірності повідомлень з даними, що приймаються мобільним пристроєм 104 від сервера 102 керування транзакціями.

[0114] На етапі 1102 блок 204 обробки мобільного пристрою 104 може зберігати ключі шифрування, ключі генерування аутентифікації і правила і/або алгоритми для їх використання і застосування в локальному сховищі, такому як пам'ять 212 або локально зашифроване сховище, зашифроване з використанням вдосконаленого ключа зберігання. На етапі 1104 приймальний блок 202 мобільного пристрою 104 може приймати повідомлення з даними від сервера 102 керування транзакціями. У деяких варіантах здійснення повідомлення з даними може прийматися від сервера 102 керування транзакціями після встановлення взаємної аутентифікації між двома пристроями, наприклад, використовуючи процес, зображений на фіг. 9 і описаний вище. Повідомлення з даними може включати в себе щонайменше лічильник повідомлень, код аутентифікації повідомлень і зашифроване повідомлення.

[0115] На етапі 1106 блок 204 обробки може збільшувати еталонний лічильник. Еталонний лічильник може зберігатися в пам'яті 212 або іншому локальному сховищі і може використовуватися для вказівки кількості повідомлень, прийнятих від сервера 102 керування транзакціями. У деяких випадках еталонний лічильник може збільшуватися з використанням алгоритму, так що еталонний лічильник може не збільшуватися, використовуючи послідовні числа, але за допомогою алгоритму, відомого для мобільного пристрою 104 (наприклад, за допомогою МРА 404) і сервера 102 керування транзакціями.

[0116] На етапі 1108 блок 204 обробки може перевіряти достовірність лічильника повідомлень, включеного в прийняте повідомлення з даними. Перевірка достовірності лічильника повідомлень може включати в себе порівняння лічильника повідомлень зі значенням еталонного лічильника після збільшення. Неуспішна перевірка достовірності може вказувати, що джерелом повідомлення з даними не є сервер 102 керування транзакціями, або, інакше, він не є достовірним. Якщо перевірка достовірності неуспішна, тоді на етапі 1110 блок 204 обробки може виконувати одне або декілька відповідних дій, асоційованих з неуспішним отриманням і/або перевіркою достовірності повідомлення з даними. Наприклад, блок 204 обробки може відкидати повідомлення з даними, може повідомляти сервер 102 керування транзакціями, може блокувати асоційований платіжний профіль 302 або виконувати іншу дію, яка є очевидною для фахівця в даній галузі техніки.

[0117] Якщо проходить перевірка достовірності лічильника повідомлень, тоді процес 1100 може перейти на етап 1112, де зашифроване повідомлення може заповнюватися незначущою інформацією. Заповнення незначущою інформацією зашифрованого повідомлення може включати в себе додавання значень в зашифроване повідомлення або дані, асоційованим з ним. Заповнення незначущою інформацією може використовуватися для підвищення безпеки процесу перевірки достовірності повідомлення, оскільки може бути інша функція, яка повинна виконуватися мобільним пристроєм 104 і сервером 102 керування транзакціями, відома один одному, яка повинна дублюватися неавторизованим об'єктом, щоб передавати або приймати повідомлення з даними успішно без авторизації. Для фахівця в даній галузі техніки очевидно, що етап 1112 може бути необов'язковим етапом. У деяких варіантах здійснення етап 1112 може застосовуватися в деяких екземплярах процесу 1110. Наприклад, зашифроване повідомлення може заповнюватися незначущою інформацією при деяких збільшеннях еталонного лічильника.

[0118] На етапі 1114 блок 204 обробки може генерувати еталонний код аутентифікації. Еталонний код аутентифікації може генеруватися на основі зашифрованого повідомлення (наприклад, заповненого незначущою інформацією, якщо це застосовне), використовуючи одне або декілька правил або алгоритмів, таких як такі, що зберігаються на етапі 1102. У деяких варіантах здійснення еталонний код аутентифікації може являти собою ключ або може являти собою значення, що генерується застосуванням ключа до зашифрованого повідомлення. На

етапі 1116 блок 204 обробки може перевіряти достовірність коду аутентифікації повідомлень, що приймається в повідомленні RNS. Перевірка достовірності коду аутентифікації повідомлень може включати в себе порівняння коду з генерованим еталонним кодом аутентифікації, як інший спосіб ідентифікації, якщо прийняте повідомлення з даними сталося від авторизованого джерела (наприклад, сервера 102 керування транзакціями).

[0119] Якщо є неуспішною перевірка достовірності коду аутентифікації повідомлень, процес 1100 може перейти на етап 1110, де виконується обробка неуспішного завершення. Якщо проходить перевірка достовірності коду аутентифікації повідомлень, тоді на етапі 1118 зашифроване повідомлення, включене в прийняте повідомлення з даними, може розшифровуватися блоком 204 обробки. Повідомлення може розшифровуватися з використанням одного або декількох ключів шифрування/розшифрування, правил і/або алгоритмів, таких як ті, які збережені в мобільному пристрої 104 на етапі 1102. Наприклад, ключ 414 шифрування, що зберігається в криптографічному додатку 410 пам'яті 212, може використовуватися для розшифровування зашифрованого повідомлення. На етапі 1120 блок 204 обробки може виконувати одну або декілька дій при необхідності, засновуючись на вмісті розшифрованого повідомлення. Наприклад, якщо розшифроване повідомлення включає в себе разові ключі 306, разові ключі 306 можуть зберігатися у відповідному платіжному профілі 302 бази 208 даних карток, які, таким чином, можуть шифруватися, використовуючи вдосконалений ключ зберігання.

Вдосконалений ключ зберігання

[0120] Фіг. 12 ілюструє генерування і використання вдосконаленого ключа зберігання мобільним пристроєм 104 для безпечного зберігання даних в мобільному пристрої 104, таких як платіжні профілі 302 й інші дані, які можуть безпечно зберігатися і до яких можна безпечно звертатися в мобільному пристрої 104 без використання елементів безпеки.

[0121] Інформація 402 про пристрій, що зберігається в пам'яті 212 мобільного пристрою 104, може включати в себе три або більше порції інформації 1202 про пристрій, зображеної на фіг. 12 як інформації 1202a, 1202b і 1202c про пристрій. Кожна порція інформації 1202 про пристрій може асоціюватися з мобільним пристроєм 104. У деяких випадках кожна порція інформації 1202 про пристрій може бути унікальною для мобільного пристрою 104. В інших випадках одна або декілька порцій інформації 1202 про пристрій може не бути унікальною для мобільного пристрою 104 (наприклад, номер моделі), але три порції інформації 1202 про пристрій, взяті разом, можуть бути унікальними для мобільного пристрою 104 (наприклад, унікальна комбінація). Порції інформації 1202 про пристрій можуть являти собою дані, які не змінюються протягом терміну служби мобільного пристрою 104.

[0122] Блок 204 обробки мобільного пристрою 104 може генерувати характерну ознаку 1204 мобільного пристрою, основуючись на трьох порціях інформації 1202a, 1202b і 1202c про пристрій. Характерна ознака 1204 мобільного пристрою може являти собою значення, унікальне для мобільного пристрою 104, і може генеруватися з використанням одного або декількох правил або алгоритмів, що зберігаються в пам'яті 212, наприклад, включених в програмний код 406 МРА 404. Характерна ознака 1204 мобільного пристрою може являти собою, наприклад, числове значення, шістнадцяткове значення, символічний рядок і т. д.

[0123] Блок 204 обробки також може бути виконаний з можливістю генерування значення 1208 диверсифікатора, використовуючи характерну ознаку 1204 мобільного пристрою. Значення диверсифікатора може генеруватися за допомогою об'єднання характерної ознаки 1204 мобільного пристрою з ідентифікатором 408 екземпляра МРА 404, а також випадкового значення 1206. Випадкове значення 1206 може являти собою випадкове або псевдовипадкове число, що генерується блоком 204 обробки. У деяких випадках випадкове значення 1206 може генеруватися відповідно до одного або декількох правил або алгоритмів, що зберігаються в пам'яті 212. Комбінація характерної ознаки 1204 мобільного пристрою, ідентифікатора 408 екземпляра і випадкового значення 1206 також може виконуватися з використанням одного або декількох правил або алгоритмів, таких як ті, які зберігаються в програмному коді 406 МРА 404. Використання ідентифікатора 408 екземпляра для генерування значення диверсифікатора може приводити до можливості безпечного зберігання даних, асоційованих з екземпляром МРА 404, так що численні установки МРА 404 не можуть бути здатні виконувати звернення до даних, що зберігаються іншими екземплярами МРА 404.

[0124] Блок 204 обробки потім може генерувати вдосконалений ключ 1210 зберігання за допомогою застосування ключа 414 шифрування, що зберігається в криптографічному додатку 410, до значення 1208 диверсифікатора. У деяких випадках вдосконалений ключ 1210 зберігання може генеруватися за допомогою розшифрування значення 1208 диверсифікатора, використовуючи ключ 414 шифрування. В інших випадках вдосконалений ключ 1210 зберігання

може являти собою значення внаслідок шифрування значення 1208 диверсифікатора з використанням ключа 414 шифрування. У деяких варіантах здійснення вдосконалений ключ 1210 зберігання може генеруватися внаслідок виконання криптографії типу "білий ящик", використовуючи ключ 414 шифрування і значення 1208 диверсифікатора.

5 [0125] Якщо вдосконалений ключ 1210 зберігання був згенерований, блок 204 обробки може використовувати вдосконалений ключ 1210 зберігання для шифрування локальної бази 1210 даних. Локальна база 1210 даних може складатися, наприклад, з бази 208 даних карток, одного або декількох платіжних профілів 302, частини пам'яті 212 або іншого придатного джерела даних. У деяких випадках локальна база 1210 даних може являти собою частину іншої бази
10 даних в мобільному пристрої 104, такої як база 208 даних карток. Наприклад, база 208 даних карток може включати в себе множину локальних баз 1212 даних, такий як окрема локальна база 1212 даних для кожного екземпляра МРА 404 для зберігання платіжних профілів 302, асоційованих з ним. Результуюча зашифрована локальна база 1214 даних, таким чином, може безпечно зберігати дані, які є недоступними для будь-якої іншої програми додатку, внутрішньої
15 або зовнішньої для мобільного пристрою 104, за винятком конкретного екземпляра МРА 404, який включає в себе ідентифікатор 408 екземпляра. Отже, зашифрована локальна база 1214 даних може бути ідеальною для зберігання платіжних облікових даних 304, разових ключів 306 й інших даних рахунку і може забезпечувати безпечне зберігання вразливої інформації про рахунок без використання елементів безпеки.

20 [0127] У деяких варіантах здійснення ключ зберігання також може використовуватися сервером 102 керування транзакціями для надання зашифрованих даних мобільному пристрою 104 для зберігання в зашифрованій локальній базі 1214 даних. Наприклад, передавальний блок 206 мобільного пристрою 104 може передавати згенероване випадкове значення 1206 серверу 102 керування транзакціями. У деяких випадках ідентифікатор 408 екземпляра також може
25 передаватися серверу 102 керування транзакціями, або сервер 102 керування транзакціями може мати його завчасно, наприклад, під час реєстрації МРА 404. Сервер 102 керування транзакціями тоді може генерувати сам вдосконалений ключ 1210 зберігання, шифрувати дані, що підлягають наданню мобільному пристрою 104, такі як платіжні облікові дані 304, разові ключі 306 і т. д., використовуючи вдосконалений ключ 1210 зберігання, і потім передавати
30 зашифровані дані на мобільний пристрій 104. Мобільний пристрій 104 потім може зберігати вже зашифровані дані в зашифрованій локальній базі 1214 даних.

Перший зразковий спосіб генерування платіжних облікових даних в платіжній транзакції

[0127] Фіг. 13 ілюструє спосіб 1300 генерування платіжних облікових даних в платіжній транзакції, що включає використання двох криптограм додатку для безпечного використання
35 платіжних облікових даних в мобільному пристрої 104 без елемента безпеки.

[0128] На етапі 1302 щонайменше разовий ключ (наприклад, разовий ключ 306) може зберігатися в пам'яті (наприклад, платіжному профілі 302), асоційований з транзакційним рахунком. У деяких варіантах здійснення пам'ять 302 може являти собою пам'ять без елемента безпеки в пристрої мобільного зв'язку (наприклад, мобільному пристрої 104). На етапі 1304
40 персональний ідентифікаційний номер (PIN) може прийматися приймальним пристроєм (наприклад, приймальним блоком 202 і/або блоком 214 введення).

[0129] На етапі 1306 перший сеансовий ключ (наприклад, перший сеансовий ключ 308) може ідентифікуватися пристроєм обробки (наприклад, блоком 204 обробки). На етапі 1308 другий сеансовий ключ (наприклад, другий сеансовий ключ 310) може генеруватися пристроєм 204
45 обробки, основуючись щонайменше на збереженому разовому ключі 306 і прийнятому PIN.

[0130] На етапі 1310 перша криптограма додатку може генеруватися пристроєм 204 обробки, основуючись щонайменше на першому сеансовому ключі 308. На етапі 1312 друга криптограма додатку може генеруватися пристроєм 204 обробки, основуючись щонайменше на
50 другому сеансовому ключі 310.

[0131] На етапі 1314 щонайменше перша криптограма додатку і друга криптограма додатку можуть передаватися передавальним пристроєм (наприклад, передавальним блоком 206) для використання в платіжній транзакції. У деяких варіантах здійснення перша криптограма додатку і друга криптограма додатку можуть передаватися на пристрій торгової точки (наприклад, торгову точку 110). В одному варіанті здійснення спосіб 1300 може додатково включати в себе
55 збереження в пам'яті 302 головного ключа картки, асоційованого з транзакційним рахунком, причому ідентифікація першого сеансового ключа 308 включає в себе генерування пристроєм 204 обробки першого сеансового ключа 308, основуючись щонайменше на збереженому головному ключі картки.

[0132] У деяких варіантах здійснення спосіб 1300 також може включати в себе збереження в пам'яті 302 лічильника транзакцій додатку (наприклад, лічильника 312 транзакцій додатку),
60

причому ідентифікація першого сеансового ключа 308 включає в себе генерування пристроєм 204 обробки першого сеансового ключа 308, основуючись щонайменше на збереженому лічильнику 312 транзакцій додатку. В одному варіанті здійснення способу 1300 додатково може включати в себе перевірку достовірності пристроєм 204 обробки прийнятого PIN перед генеруванням другого сеансового ключа 310. В іншому варіанті здійснення пристрій 204 обробки може бути виконаний з можливістю генерування недостовірною другого сеансового ключа 310, якщо завершується неуспішно перевірка достовірності прийнятого PIN.

Другий зразковий спосіб генерування платіжних облікових даних в платіжній транзакції

[0133] Фіг. 14 ілюструє спосіб 1400 генерування платіжних облікових даних в платіжній транзакції, що включає в себе використання перевірки достовірності двох криптограм додатку платіжних облікових даних, згенерованих мобільним пристроєм 104 без використання елемента безпеки.

[0134] На етапі 1402 щонайменше головний ключ картки (наприклад, перший головний ключ 612 картки) може зберігатися в пам'яті (наприклад, профілі 602 рахунку), асоційований з транзакційним рахунком. На етапі 1404 перший сеансовий ключ (наприклад, перший сеансовий ключ 606) може генеруватися пристроєм обробки (наприклад, пристроєм 504 обробки), основуючись щонайменше на збереженому головному ключі 612 картки. На етапі 1406 другий сеансовий ключ (наприклад, другий сеансовий ключ 608) може генеруватися пристроєм 504 обробки.

[0135] На етапі 1408 перша криптограма додатку може генеруватися пристроєм 504 обробки, основуючись щонайменше на першому сеансовому ключі 606. На етапі 1410 друга криптограма додатку може генеруватися пристроєм 504 обробки, основуючись щонайменше на другому сеансовому ключі 608. На етапі 1412 щонайменше перша криптограма додатку і друга криптограма додатку можуть передаватися передавальним пристроєм (наприклад, передавальним блоком 506) для використання в платіжній транзакції.

[0136] В одному варіанті здійснення способу 1400 може додатково включати в себе збереження в пам'яті 602 порядкового номера транзакційного рахунку, асоційованого з транзакційним рахунком, причому перший сеансовий ключ додатково базується на збереженому порядковому номері транзакційного рахунку. У деяких варіантах здійснення способу 1400 також може включати в себе збереження в пам'яті 602 другого головного ключа картки (наприклад, другого головного ключа 614 картки), асоційованого з транзакційним рахунком, причому другий сеансовий ключ 608 базується щонайменше на збереженому другому головному ключі 614 картки.

[0137] В одному варіанті здійснення способу 1400 може додатково включати в себе: прийом приймальним пристроєм (наприклад, приймальним блоком 502) першої відповідної криптограми додатку і другої відповідної криптограми додатку; перевірку достовірності пристроєм обробки (i) прийнятої першої відповідної криптограми додатку, основуючись на згенерованій першій криптограмі додатку, і (ii) прийнятої другої відповідної криптограми додатку, основуючись на згенерованій другій криптограмі додатку; і передачу передавальним пристроєм 506 результату перевірки достовірності для використання в платіжній транзакції. В іншому варіанті здійснення перша відповідна криптограма додатку і друга відповідна криптограма додатку можуть прийматися від пристрою торгової точки (наприклад, торгової точки 110). У ще іншому варіанті здійснення результат перевірки достовірності може передаватися фінансовій установі (наприклад, емітенту 106), асоційованій з транзакційним рахунком.

Зразковий спосіб обробки повідомлення з даними

[0138] Фіг. 15 ілюструє спосіб 1500 обробки повідомлення з даними, такого як повідомлення віддаленого сповіщення, що приймається за допомогою служби віддалених сповіщень, що включає в себе отримання і перевірку достовірності його мобільним пристроєм 104 без використання елемента безпеки.

[0139] На етапі 1502 щонайменше ключ шифрування може зберігатися в пам'яті (наприклад, в пам'яті 212). У деяких варіантах здійснення пам'ять 212 може являти собою пам'ять без елемента безпеки в пристрої мобільного зв'язку (наприклад, мобільному пристрої 104). На етапі 1504 повідомлення з даними може прийматися приймальним пристроєм (наприклад, приймальним блоком 202), в якому повідомлення з даними може включати в себе щонайменше зашифроване повідомлення і код аутентифікації повідомлень, де код аутентифікації повідомлень генерується з використанням щонайменше частини зашифрованого повідомлення. У деяких варіантах здійснення повідомлення з даними може являти собою повідомлення служби віддалених сповіщень, що приймається за допомогою служби віддалених сповіщень.

[0140] На етапі 1506 еталонний код аутентифікації може генеруватися пристроєм обробки (наприклад, блоком 204 обробки), використовуючи щонайменше частину зашифрованого

повідомлення, включеного в прийняте повідомлення з даними. В одному варіанті здійснення пам'ять 212 може додатково включати в себе одне або декілька правил генерування коду аутентифікації, і еталонний код аутентифікації може генеруватися на основі застосування збереженого одного або декількох правил генерування коду аутентифікації до частини зашифрованого повідомлення, включеного в прийняте повідомлення з даними. На етапі 1508 прийняте повідомлення з даними може перевірятися на достовірність пристроєм 204 обробки, основуючись на звіренні коду аутентифікації повідомлень, включеного в прийняте повідомлення з даними, зі згенерованим еталонним кодом аутентифікації. У деяких варіантах здійснення пам'ять може додатково включати в себе еталонний лічильник, прийняте повідомлення з даними може додатково включати в себе лічильник повідомлень, і прийняте повідомлення з даними може додатково перевірятися на достовірність пристроєм 204 обробки, основуючись на звіренні лічильника повідомлень, включеного в прийняте повідомлення з даними, із збереженим еталонним лічильником.

[0141] На етапі 1510 зашифроване повідомлення, включене в повідомлення з даними, може розшифровуватися пристроєм 204 обробки, використовуючи збережений ключ шифрування, для отримання розшифрованого повідомлення. В одному варіанті здійснення розшифроване повідомлення може включати в себе щонайменше одне з: оцифрованого профілю картки (наприклад, платіжні облікові дані 304) і разового ключа (наприклад, разового ключа 306) для використання в платіжній транзакції. У деяких варіантах здійснення спосіб 1500 також може включати в себе звірення пристроєм 204 обробки формату даних розшифрованого повідомлення, основуючись на одному або декількох правилах форматування даних.

[0142] В одному варіанті здійснення спосіб 1500 може додатково включати в себе передачу передавальним пристроєм (наприклад, передавальним блоком 206) сповіщення про отримання у відповідь на прийняте повідомлення з даними. В іншому варіанті здійснення спосіб 1500 може ще додатково включати в себе: виконання пристроєм 204 обробки одного або декількох дій, основуючись на розшифрованому повідомленні; генерування пристроєм 204 обробки повідомлення, яке повертається внаслідок виконаної однієї або декількох дій або на їх основі; шифрування пристроєм 204 обробки згенерованого повідомлення, яке повертається, використовуючи збережений ключ шифрування, для отримання зашифрованого повідомлення, яке повертається; і генерування пристроєм 204 обробки коду аутентифікації, що повертається, використовуючи щонайменше частину зашифрованого повідомлення, яке повертається, в якому повідомлення, що передається, про отримання включає в себе зашифроване повідомлення, яке повертається, і код аутентифікації, що повертається. У ще іншому варіанті здійснення пам'ять 212 може додатково включати в себе лічильник, що повертається, і сповіщення, що передається, про отримання може додатково включати в себе лічильник, що повертається.

[0143] У деяких варіантах здійснення спосіб 1500 також може включати в себе заповнення незначущою інформацією пристроєм 204 обробки зашифрованого повідомлення, включеного в прийняте повідомлення з даними, використовуючи ключ заповнення незначущою інформацією, в якому частина зашифрованого повідомлення, що використовується для генерування еталонного коду аутентифікації, являє собою зашифроване повідомлення із заповненням незначущою інформацією. В іншому варіанті здійснення ключ заповнення незначущою інформацією може являти собою ключ шифрування. У ще іншому варіанті здійснення пам'ять 212 може додатково включати в себе алгоритм заповнення незначущою інформацією коду аутентифікації, і заповнення незначущою інформацією зашифрованого повідомлення, використовуючи ключ заповнення незначущою інформацією, може включати в себе заповнення незначущою інформацією зашифрованого повідомлення, основуючись на застосуванні ключа заповнення незначущою інформацією до алгоритму заповнення незначущою інформацією коду аутентифікації.

Зразковий спосіб формування вдосконаленого ключа зберігання

[0144] Фіг. 16 ілюструє спосіб 600 формування вдосконаленого ключа зберігання для безпечного шифрування і зберігання локальних даних в мобільному пристрої 104 без використання елемента безпеки.

[0145] На етапі 1602 щонайменше інформація про пристрій (наприклад, інформація 402 про пристрій), асоційована з пристроєм мобільного зв'язку (наприклад, мобільним пристроєм 104), програмний код (наприклад, програмний код 406), асоційований з першою програмою додатку (наприклад, мобільним платіжним додатком 404), і програмний код (наприклад, програмний код 412), асоційований з другою програмою додатку (наприклад, криптографічним додатком 410), може зберігатися в пам'яті (наприклад, пам'яті 212) пристрою 104 мобільного зв'язку, в якому програмний код 406, асоційований з першою програмою 404 додатку, включає в себе щонайменше ідентифікатор екземпляра (наприклад, ідентифікатор 408 екземпляра) і

програмний код 412, асоційований з другою програмою 410 додатку, включає в себе щонайменше перший ключ (наприклад, ключ 414 шифрування).

[0146] У деяких варіантах здійснення інформація 402 про пристрій може включати в себе один або декілька унікальних ідентифікаторів, асоційованих з пристроєм 104 мобільного зв'язку. В одному варіанті здійснення ідентифікатор 408 екземпляра може бути унікальним для екземпляра першої програми 404 додатку. У деяких варіантах здійснення друга програма 410 додатку може бути виконана з можливістю виконання криптографії типу "білий ящик", використовуючи перший ключ. В одному варіанті здійснення першим ключем може бути динамічний ключ. У деяких варіантах здійснення програмний код 412, асоційований з другою програмою 410 додатку, може бути включений в програмний код 406, асоційований з першою програмою 404 додатку. В інших варіантах здійснення друга програма 410 додатку може являти собою функцію першої програми 404 додатку, що виконується.

[0147] На етапі 1604 характерна ознака пристрою (наприклад, характерна ознака 1204 мобільного пристрою), асоційована з пристроєм 104 мобільного зв'язку, може генеруватися пристроєм обробки (наприклад, блоком 204 обробки), основуючись на збереженій інформації 402 про пристрій, за допомогою виконання програмного коду 406, асоційованого з першою програмою 404 додатку. На етапі 1606 випадкове значення (наприклад, випадкове значення 1206) може генеруватися пристроєм 204 обробки за допомогою виконання програмного коду 406, асоційованого з першою програмою 404 додатку. У деяких варіантах здійснення випадкове значення 1206 може являти собою випадкове або псевдовипадкове число.

[0148] На етапі 1608 значення диверсифікатора (наприклад, значення 1208 диверсифікатора) може формуватися пристроєм 204 обробки, основуючись щонайменше на згенерованій характерній ознаці 1204 пристрою, згенерованому випадковому значенні 1206 й ідентифікаторі 408 екземпляра, включеним в програмний код 406, асоційований з першою програмою 404 додатку. На етапі 1610 сформоване значення 1208 диверсифікатора може розшифровуватися пристроєм 204 обробки, використовуючи перший ключ, що зберігається в програмному коді 412, асоційованим з другою програмою 410 додатку, за допомогою виконання програмного коду 412, асоційованого з другою програмою 410 додатку, для отримання ключа зберігання (наприклад, вдосконаленого ключа 1210 зберігання).

[0149] У деяких варіантах здійснення спосіб 1600 може додатково включати в себе: збереження в локальній базі даних (наприклад, локальній базі 1212 даних) пристрою 104 мобільного зв'язку, захищених даних; і шифрування пристроєм 204 обробки захищених даних, що зберігаються в локальній базі 1212 даних, використовуючи ключ 1210 зберігання. В одному варіанті здійснення спосіб 1600 також може включати в себе: збереження в пам'яті 212 програмних даних, асоційованих з першою програмою 404 додатку; і збереження в програмних даних, асоційованих з першою програмою 404 додатку, згенерованого випадкового значення 1206.

[0150] В одному варіанті здійснення спосіб 1600 також може включати в себе: передачу передавальним пристроєм (наприклад, передавальним блоком 206) щонайменше випадкового значення 1206; прийом приймальним пристроєм (наприклад, приймальним блоком 202) одного або декількох зашифрованих параметрів, в якому кожний з одного або декількох зашифрованих параметрів шифрується з використанням ключа 1210 зберігання; і збереження в локальній базі 1212 даних пристрою 104 мобільного зв'язку, прийнятих одного або декількох зашифрованих параметрів. В іншому варіанті здійснення ключ 1210 зберігання може передаватися третій стороні (наприклад, серверу 102 керування транзакціями), і один або декілька зашифрованих параметрів можуть прийматися від третьої сторони 102. У ще інших варіантах здійснення ідентифікатор 408 екземпляра також може передаватися передавальним пристроєм 206.

Архітектура комп'ютерної системи

[0151] Фіг. 17 ілюструє комп'ютерну систему 1700, в якій варіанти здійснення даного винаходу, або його частини, можуть бути реалізовані у вигляді зчитуваного комп'ютером коду. Наприклад, сервер 102 керування транзакціями і мобільний пристрій 104 за фіг. 1 можуть бути реалізовані в комп'ютерній системі 1700, що використовує апаратні засоби, програмні засоби, програмно-апаратні засоби, довготривалі зчитувані комп'ютером середовища, що мають інструкції, які зберігаються на них, або їх комбінації, і можуть бути реалізовані в одній або декількох комп'ютерних системах або інших системах обробки. Апаратні засоби, програмні засоби або будь-яка їх комбінація може містити модулі і компоненти, що використовуються для реалізації способів за фіг. 7, 8, 9A, 10A, 10B, 11 і 13-16.

[0152] Якщо використовується програмована логіка, така логіка може виконуватися на платформі обробки, що серійно випускається, або на пристрої спеціального призначення. Фахівець в даній галузі техніки може брати до уваги, що варіанти здійснення розкритого об'єкта

винаходу можуть бути здійснені на практиці з різними конфігураціями комп'ютерної системи, включаючи багатоядерні багатопроцесорні системи, мінікомп'ютери, великі електронно-обчислювальні машини, комп'ютери, зв'язані або згруповані в кластери з розподіленими функціями, а також широко поширені або мініатюрні комп'ютери, які можуть бути вбудовані практично в будь-який пристрій. Наприклад, щонайменше один процесорний пристрій і пам'ять можуть використовуватися для реалізації вищеописаних варіантів здійснення.

[0153] Процесорний блок або пристрій, як описано в даному документі, може бути одним процесором, множиною процесорів або їх комбінацією. Процесорні пристрої можуть мати один або декілька "ядер" процесора. Терміни "середовище комп'ютерної програми", "довготривале зчитуване комп'ютером середовище" і "використовуване комп'ютером середовище", як описано в даному документі, використовуються для загального посилання на матеріальні середовища, такі як знімний запам'ятовувальний блок 1718, знімний запам'ятовувальний блок 1722 і жорсткий диск, встановлений в накопичувачі 1712 на жорсткому диску.

[0154] Різні варіанти здійснення даного винаходу описані на основі даної зразкової комп'ютерної системи 1700. Після прочитання цього опису для фахівця в даній галузі техніки стане очевидним, як реалізувати даний винахід, використовуючи інші комп'ютерні системи і/або комп'ютерну архітектуру. Хоча операції можуть описуватися у вигляді послідовного процесу, деякі операції, фактично, можуть виконуватися паралельно, одночасно і/або в розподіленому оточенні і з програмним кодом, що зберігається локально або віддалено для доступу однопроцесорними або багатопроцесорними машинами. Крім того, в деяких варіантах здійснення порядок операцій може бути переупорядкований без відступу від суті розкритого об'єкта винаходу.

[0155] Процесорний пристрій 1704 може являти собою процесорний пристрій спеціального призначення або загального призначення. Процесорний пристрій 1704 може бути з'єднаний з інфраструктурою 1706 зв'язку, такою як шина, черга повідомлень, мережа, багатоядерна схема передачі повідомлень і т. д. Мережа може являти собою будь-яку мережу, придатну для виконання функцій, описаних в даному документі, і може включати в себе локальну мережу (LAN), глобальну мережу (WAN), бездротову мережу (наприклад, WiFi), мережу мобільного зв'язку, супутникову мережу, Інтернет, волоконно-оптичну лінію зв'язку, коаксіальний кабель, інфрачервону частоту, радіочастоту (RF) або будь-яку їх комбінацію. Інші придатні типи мереж і конфігурації очевидні для фахівця в даній галузі техніки. Комп'ютерна система 1700 також може включати в себе основну пам'ять 1708 (наприклад, оперативний запам'ятовуючий пристрій, постійний запам'ятовуючий пристрій і т. д.) і також може включати в себе вторинну пам'ять 1710. Вторинна пам'ять 1710 може включати в себе накопичувач 1712 на жорсткому диску і знімний накопичувач 1714, такий як накопичувач на дискетах, накопичувач на магнітній стрічці, накопичувач на оптичних дисках, флеш-пам'ять і т. д.

[0156] Знімний накопичувач 1714 може зчитуватися зі знімного запам'ятовуючого блока 1718 і/або записувати на нього загальноновідомим чином. Знімний запам'ятовуючий блок 1718 може включати в себе знімні запам'ятовуючі середовища, які можуть зчитуватися і записуватися знімним накопичувачем 1714. Наприклад, якщо знімний накопичувач 1714 являє собою накопичувач на дискетах або порт універсальної послідовної шини, знімний запам'ятовуючий блок 1718 може являти собою дискету або портативний флеш-накопичувач відповідно. В одному варіанті здійснення знімний запам'ятовуючий блок 1718 може являти собою довготривалі зчитувані комп'ютером середовища запису.

[0157] У деяких варіантах здійснення повторна пам'ять 1710 може включати в себе альтернативний засіб, що дозволяє комп'ютерним програмам або іншим інструкціям завантажуватися в комп'ютерну систему 1700, наприклад, знімний запам'ятовуючий блок 1722 і інтерфейс 1720. Приклади такого засобу можуть включати в себе програмний картридж й інтерфейс картриджа (наприклад, які зустрічаються у відеоігрових системах), знімний кристал пам'яті (наприклад, електрично стираєний програмований постійний запам'ятовуючий пристрій (EEPROM), програмований постійний запам'ятовуючий пристрій (PROM) і т. д.) і зв'язане з ним гніздо, й інші знімні запам'ятовуючі блоки 1722 і інтерфейси 1720, що очевидно для фахівця в даній галузі техніки.

[0158] Дані, які зберігаються в комп'ютерній системі 1700 (наприклад, в основній пам'яті 1708 і/або вторинній пам'яті 1710) можуть зберігатися на придатних зчитуваних комп'ютером середовищах будь-якого типу, таких як оптичний запам'ятовуючий пристрій (наприклад, компакт-диск, цифровий багатофункціональний диск, диск Blu-ray і т. д.) або запам'ятовуючий пристрій на магнітній стрічці (наприклад, накопичувач на жорсткому диску). Дані можуть бути сконфігуровані в будь-якому типі придатної конфігурації бази даних, такої як реляційна база даних, база даних SQL-типу (типу мови структурованих запитів), розподілена база даних,

об'єктно-орієнтована база даних і т. д. Придатні конфігурації і типи запам'ятовуючих пристроїв очевидні для фахівця в даній галузі техніки.

[0159] Комп'ютерна система 1700 також може включати в себе інтерфейс 1724 зв'язку. Інтерфейс 1724 зв'язку може бути виконаний з можливістю перенесення програмних засобів і даних між комп'ютерною системою 1700 і зовнішніми пристроями. Зразкові інтерфейси 1724 зв'язку можуть включати в себе модем, мережевий інтерфейс (наприклад, карта Езернета), порт зв'язку, гніздо і карта PCMCIA (Міжнародна асоціація виробників карт пам'яті для персональних комп'ютерів) і т. д. Програмні засоби і дані, які переносяться за допомогою інтерфейсу 1724 зв'язку, можуть бути у вигляді сигналів, які можуть бути електронними, електромагнітними, оптичними або іншими сигналами, що очевидно для фахівця в даній галузі техніки. Сигнали можуть передаватися по тракту 1726 зв'язку, який може бути виконаний з можливістю перенесення сигналів і може бути реалізований з використанням проводу, кабеля, волоконної оптики, телефонної лінії, лінії зв'язку стільникового телефону, радіочастотної лінії зв'язку і т. д.

[0160] Комп'ютерна система 1700 додатково може включати в себе інтерфейс 1702 дисплея. Інтерфейс 1702 дисплея може бути виконаний з можливістю передачі даних між комп'ютерною системою 1700 і зовнішнім дисплеєм 1730. Зразкові інтерфейси 1702 дисплея можуть включати в себе мультимедійний інтерфейс високого розрізнення (HDMI), цифрового відеоінтерфейсу (DVI), відеографічну матрицю (VGA) і т. д. Дисплей 1730 може являти собою дисплей будь-якого придатного типу для відображення даних, що передаються за допомогою інтерфейсу 1702 дисплея комп'ютерної системи 1700, включаючи дисплей на електронно-променевої трубі (CRT), рідкокристалічний дисплей (LCD), дисплей на світловипромінювальних діодах (LED), сенсорний дисплей емнісного типу, дисплей з активною матрицею на тонкоплівкових транзисторах (TFT) і т. д.

[0161] Середовище з комп'ютерною програмою і використовуване комп'ютером середовище можуть посилатися на пам'ять, таку як основна пам'ять 1708 і вторинна пам'ять 1710, якими може бути напівпровідникова пам'ять (наприклад, динамічний оперативний запам'ятовуючий пристрій (DRAM) і т. д.). Ці продукти комп'ютерної програми можуть являти собою засіб для надання програмних засобів комп'ютерній системі 1700. Комп'ютерні програми (наприклад, логіка керування комп'ютером) можуть зберігатися в основній пам'яті 1708 і/або вторинній пам'яті 1710. Комп'ютерні програми також можуть прийматися за допомогою інтерфейсу 1724 зв'язку. Такі комп'ютерні програми при їх виконанні можуть надавати можливість комп'ютерній системі 1700 реалізовувати дані способи, описані в даному документі. Зокрема, комп'ютерні програми при їх виконанні можуть надавати можливість процесорному пристрою 1704 реалізовувати способи, зображені на фіг. 7, 8, 9A, 9B, 10A, 10B, 11 і 13-16, як описано в даному документі. Отже, такі комп'ютерні програми можуть представляти контролери комп'ютерної системи 1700. Там, де даний винахід реалізовується з використанням програмних засобів, програмні засоби можуть зберігатися в продукті комп'ютерної програми і можуть завантажуватися в комп'ютерну систему 1700, використовуючи знімний накопичувач 1714, інтерфейс 1720 і накопичувач 1712 на жорсткому диску, або інтерфейс 1724 зв'язку.

[0162] Методи, сумісні з даним винаходом, забезпечують, серед інших ознак, системи і способи обробки платіжних транзакцій з використанням мобільного пристрою без використання елемента безпеки, включаючи передачу і перевірку достовірності повідомлень служби віддалених сповіщень і безпечне зберігання даних, використовуючи вдосконалений ключ зберігання. Хоча вище були описані різні зразкові варіанти здійснення розкритої системи і способу, потрібно розуміти, що вони були представлені тільки з метою прикладу, і не обмежень. Вони не є вичерпними і не обмежують винахід розкритою точною формою. Можливі модифікації і варіанти в світлі вищезазначених ідей, або вони можуть бути отримані при практичному використанні винаходу без відступу від широти або об'єму.

ФОРМУЛА ВИНАХОДУ

1. Спосіб генерування платіжних облікових даних в платіжній транзакції, який включає:
збереження в пам'яті щонайменше разового ключа, асоційованого з транзакційним рахунком;
прийом приймальним пристроєм персонального ідентифікаційного номера;
ідентифікацію пристроєм обробки першого сеансового ключа;
генерування пристроєм обробки другого сеансового ключа, основуючись щонайменше на збереженому разовому ключі і прийнятому персональному ідентифікаційному номері;
генерування пристроєм обробки першої криптограми додатка, основуючись щонайменше на першому сеансовому ключі;

генерування пристроєм обробки другої криптограми додатка, основуючись щонайменше на другому сеансовому ключі; і передачу передавальним пристроєм щонайменше першої криптограми додатка і другої криптограми додатка для використання в платіжній транзакції.

5 2. Спосіб за п. 1, який додатково включає:

збереження, в пам'яті, головного ключа картки, асоційованого з транзакційним рахунком, причому

ідентифікація першого сеансового ключа включає в себе генерування пристроєм обробки першого сеансового ключа, основуючись щонайменше на збереженому головному ключі картки.

10 3. Спосіб за п. 1, який додатково включає:

збереження, в пам'яті, лічильника транзакцій додатка, причому

ідентифікація першого сеансового ключа включає в себе генерування пристроєм обробки першого сеансового ключа, основуючись щонайменше на збереженому лічильнику транзакцій додатка.

15 4. Спосіб за п. 1, який додатково включає:

перевірку достовірності, пристроєм обробки, прийнятого персонального ідентифікаційного номера перед генеруванням другого сеансового ключа.

5. Спосіб за п. 4, в якому пристрій обробки виконаний з можливістю генерування недостовірного другого сеансового ключа, якщо є неуспішною перевірка достовірності прийнятого персонального ідентифікаційного номера.

20 6. Спосіб за п. 1, в якому перша криптограма додатка і друга криптограма додатка передаються

на пристрій торгової точки.

7. Спосіб за п. 1, в якому пам'яттю є пам'ять без елемента безпеки в пристрої мобільного зв'язку.

25 8. Спосіб генерування платіжних облікових даних в платіжній транзакції, який включає:

збереження в пам'яті щонайменше головного ключа картки, асоційованого з транзакційним рахунком;

генерування пристроєм обробки першого сеансового ключа, основуючись щонайменше на збереженому головному ключі картки;

30 генерування пристроєм обробки другого сеансового ключа;

генерування пристроєм обробки першої криптограми додатка, основуючись щонайменше на першому сеансовому ключі;

генерування пристроєм обробки другої криптограми додатка, основуючись щонайменше на другому сеансовому ключі; і

35 передачу передавальним пристроєм щонайменше першої криптограми додатка і другої криптограми додатка для використання в платіжній транзакції.

9. Спосіб за п. 8, який додатково включає:

збереження, в пам'яті, порядкового номера транзакційного рахунку, асоційованого з транзакційним рахунком, причому

40 перший сеансовий ключ додатково базується на збереженому порядковому номері транзакційного рахунку.

10. Спосіб за п. 8, який додатково включає:

збереження, в пам'яті, другого головного ключа картки, асоційованого з транзакційним рахунком, причому

45 другий сеансовий ключ базується щонайменше на збереженому другому головному ключі картки.

11. Спосіб за п. 8, який додатково включає:

прийом приймальним пристроєм першої відповідної криптограми додатка і другої відповідної криптограми додатка;

50 перевірку достовірності, пристроєм обробки, (i) прийнятої першої відповідної криптограми додатка, основуючись на згенерованій першій криптограмі додатка, і (ii) прийнятої другої відповідної криптограми додатка, основуючись на згенерованій другій криптограмі додатка; і

передачу передавальним пристроєм результату перевірки достовірності для використання в платіжній транзакції.

55 12. Спосіб за п. 11, в якому перша відповідна криптограма додатка і друга відповідна криптограма додатка приймаються від пристрою торгової точки.

13. Спосіб за п. 11, в якому результат перевірки достовірності передається фінансовій установі, асоційованій з транзакційним рахунком.

14. Система для генерування платіжних облікових даних в платіжній транзакції, яка містить:

пам'ять, виконану з можливістю зберігання щонайменше разового ключа, асоційованого з транзакційним рахунком;
 приймальний пристрій, виконаний з можливістю прийому персонального ідентифікаційного номера;

5 пристрій обробки, виконаний з можливістю:
 ідентифікації першого сеансового ключа,
 генерування другого сеансового ключа, основуючись щонайменше на збереженому разовому
 ключі і прийнятому персональному ідентифікаційному номері,
 генерування першої криптограми додатка, основуючись щонайменше на першому сеансовому
 10 ключі, і
 генерування другої криптограми додатка, основуючись щонайменше на другому сеансовому
 ключі; і
 передавальний пристрій, виконаний з можливістю передачі щонайменше першої криптограми
 додатка і другої криптограми додатка для використання в платіжній транзакції.

15 15. Система за п. 14, в якій

пам'ять додатково виконана з можливістю зберігання головного ключа картки, асоційованого з
 транзакційним рахунком, і
 ідентифікація першого сеансового ключа включає в себе генерування пристроєм обробки
 першого сеансового ключа, основуючись щонайменше на збереженому головному ключі картки.

20 16. Система за п. 14, в якій

пам'ять додатково виконана з можливістю зберігання лічильника транзакцій додатка, і
 ідентифікація першого сеансового ключа включає в себе генерування пристроєм обробки
 першого сеансового ключа, основуючись щонайменше на збереженому лічильнику транзакцій
 додатка.

25 17. Система за п. 14, в якій пристрій обробки додатково виконаний з можливістю перевірки
 достовірності прийнятого персонального ідентифікаційного номера перед генеруванням другого
 сеансового ключа.

18. Система за п. 17, в якій пристрій обробки виконаний з можливістю генерування
 недостовірною другого сеансового ключа, якщо є неуспішною перевірка достовірності
 30 прийнятого персонального ідентифікаційного номера.

19. Система за п. 14, в якій перша криптограма додатка і друга криптограма додатка
 передаються на пристрій торгової точки.

20. Система за п. 14, в якій пам'яттю є пам'ять без елемента безпеки в пристрої мобільного
 зв'язку.

35 21. Система для генерування платіжних облікових даних в платіжній транзакції, яка містить:

пам'ять, виконану з можливістю зберігання щонайменше головного ключа картки, асоційованого
 з транзакційним рахунком;

пристрій обробки, виконаний з можливістю
 генерування першого сеансового ключа, основуючись щонайменше на головному ключі картки,
 40 що зберігається,

генерування другого сеансового ключа,
 генерування першої криптограми додатка, основуючись щонайменше на першому сеансовому
 ключі, і

45 генерування другої криптограми додатка, основуючись щонайменше на другому сеансовому
 ключі; і

передавальний пристрій, виконаний з можливістю передачі щонайменше першої криптограми
 додатка і другої криптограми додатка для використання в платіжній транзакції.

22. Система за п. 21, в якій

пам'ять додатково виконана з можливістю зберігання порядкового номера транзакційного
 50 рахунку, асоційованого з транзакційним рахунком, і
 перший сеансовий ключ додатково базується на збереженому порядковому номері
 транзакційного рахунку.

23. Система за п. 21, в якій

пам'ять додатково виконана з можливістю зберігання другого головного ключа картки,
 асоційованого з транзакційним рахунком, і
 55 другий сеансовий ключ базується щонайменше на збереженому другому головному ключі
 картки.

24. Система за п. 21, яка додатково містить:

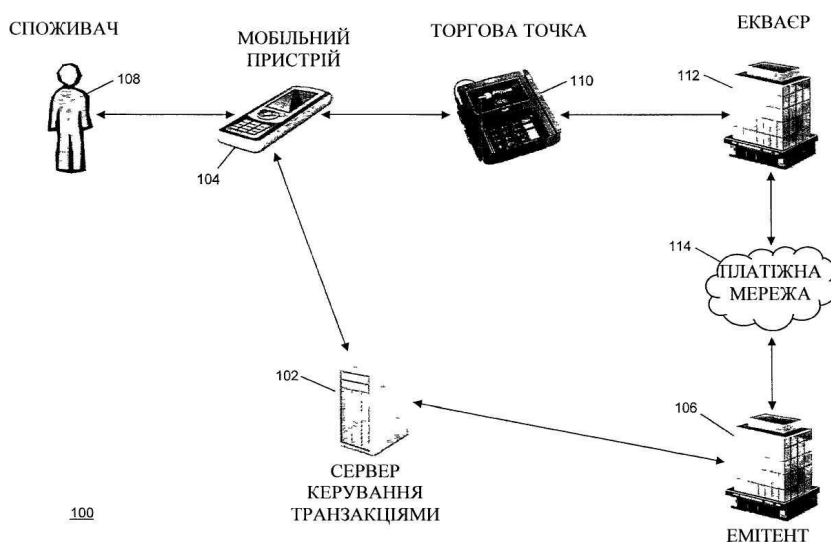
60 приймальний пристрій, виконаний з можливістю прийому першої відповідної криптограми
 додатка і другої відповідної криптограми додатка, причому

пристрій обробки додатково виконаний з можливістю перевірки достовірності (i) прийнятої першої відповідної криптограми додатка, основуючись на згенерованій першій криптограмі додатка, і (ii) прийнятої другої відповідної криптограми додатка, основуючись на згенерованій другій криптограмі додатка, і

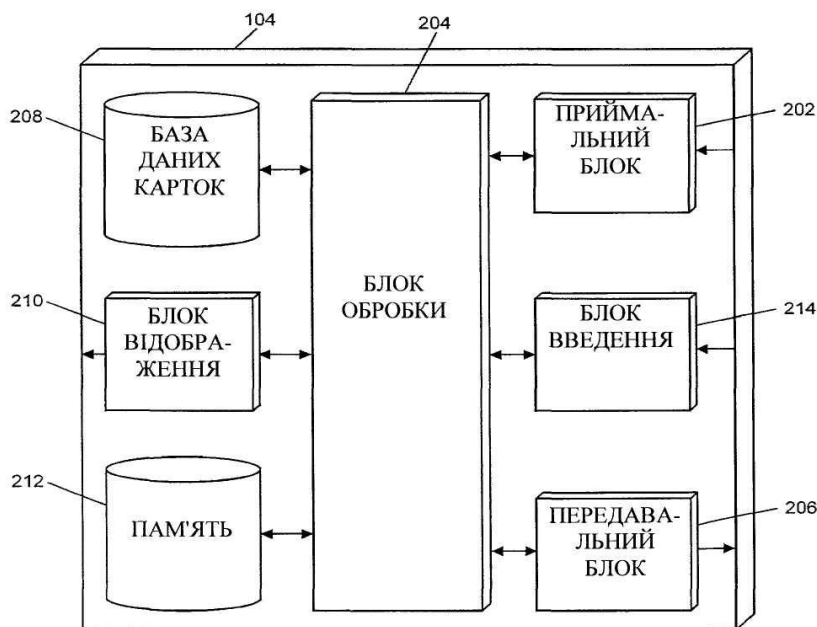
5 передавальний пристрій додатково виконаний з можливістю передачі результату перевірки достовірності для використання в платіжній транзакції.

25. Система за п. 24, в якій перша відповідна криптограма додатка і друга відповідна криптограма додатка приймаються від пристрою торгової точки.

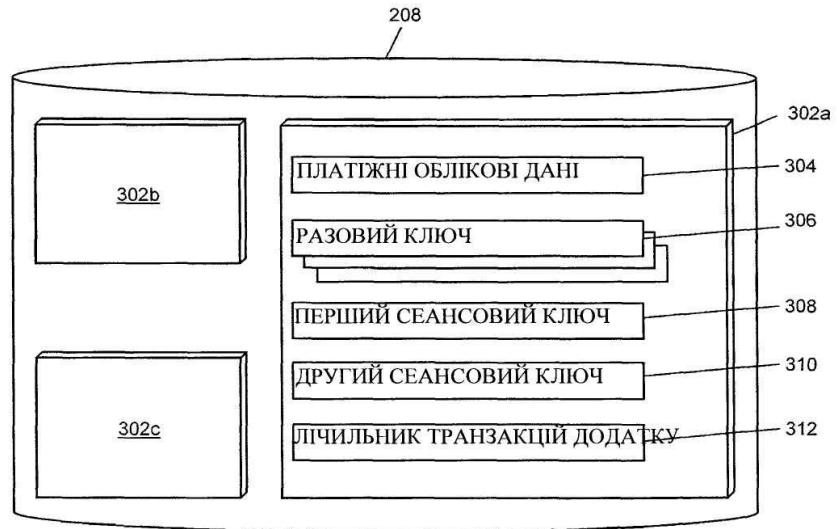
10 26. Система за п. 24, в якій результат перевірки достовірності передається фінансовій установі, асоційованій з транзакційним рахунком.



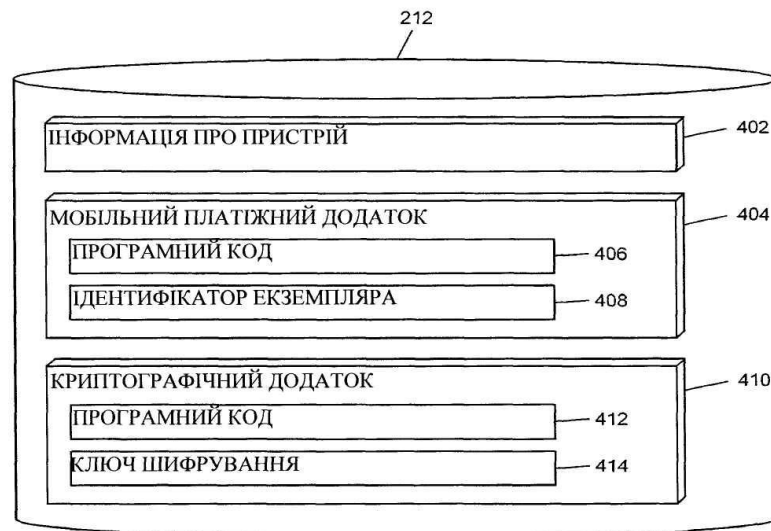
Фіг. 1



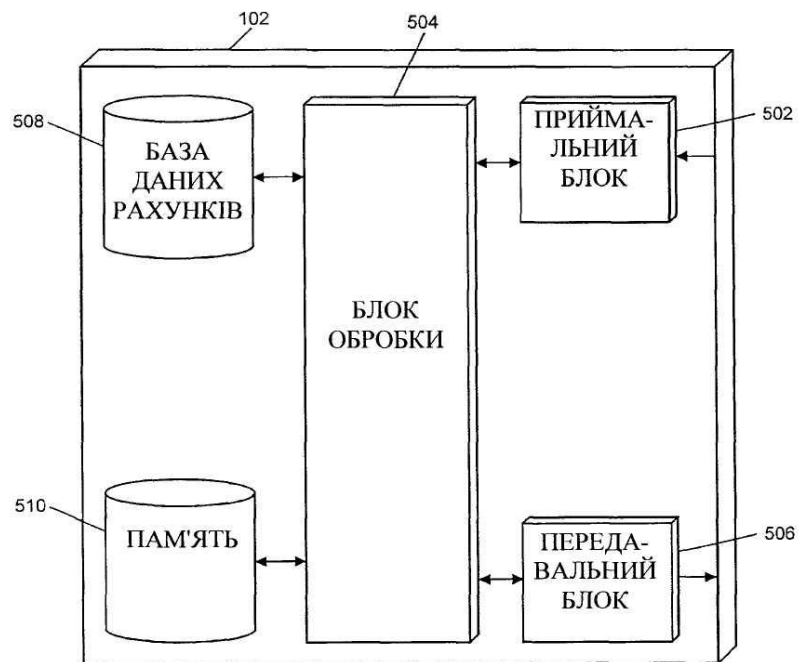
Фіг. 2



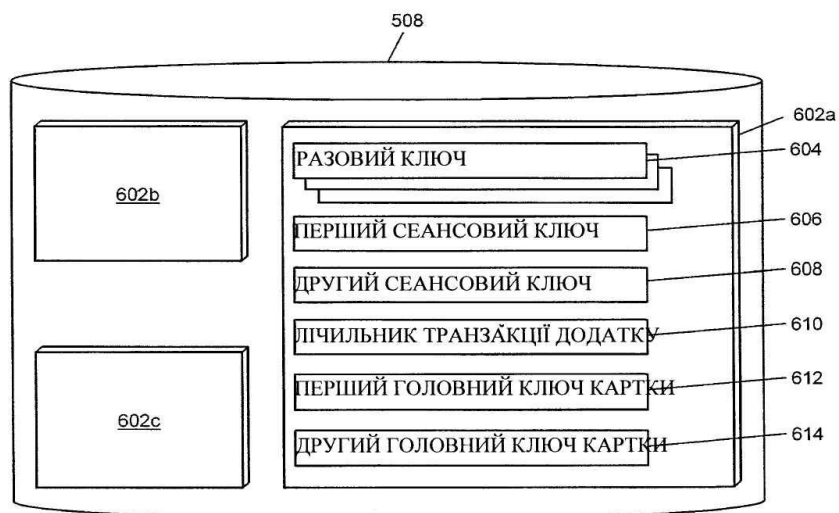
Фіг. 3



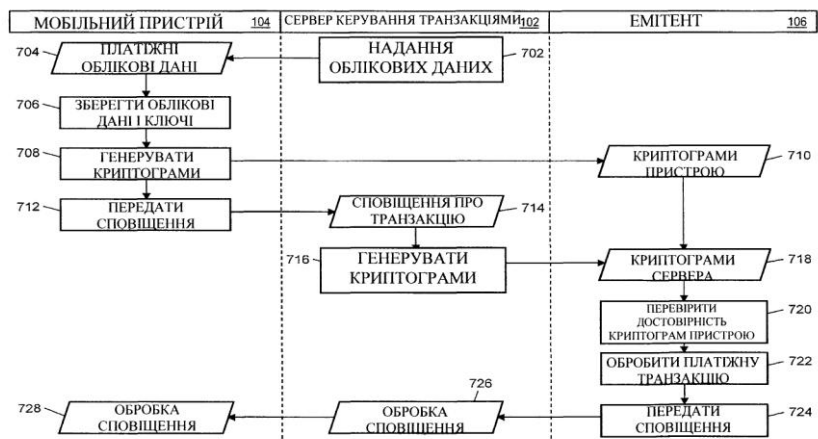
Фіг. 4



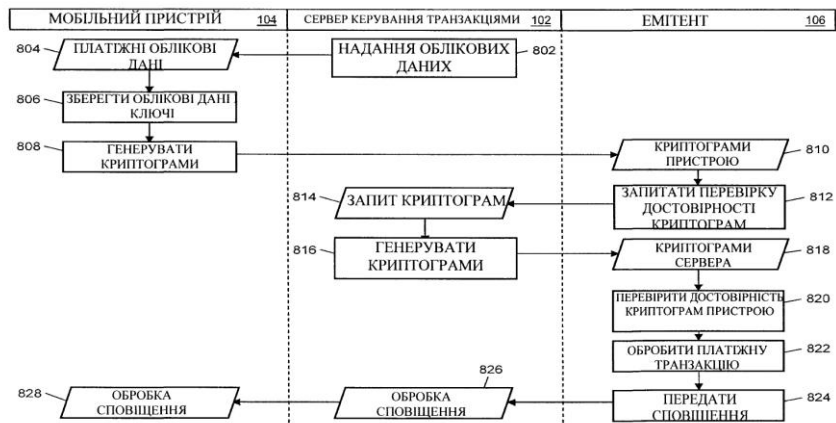
Фіг. 5



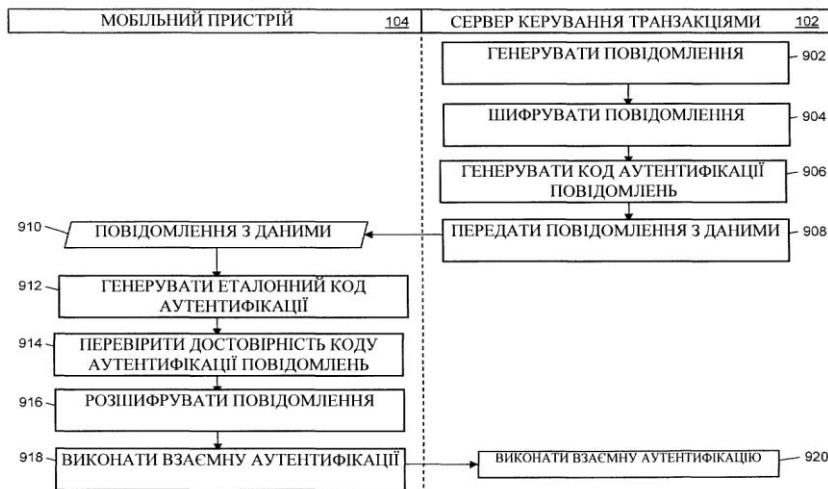
Фіг. 6



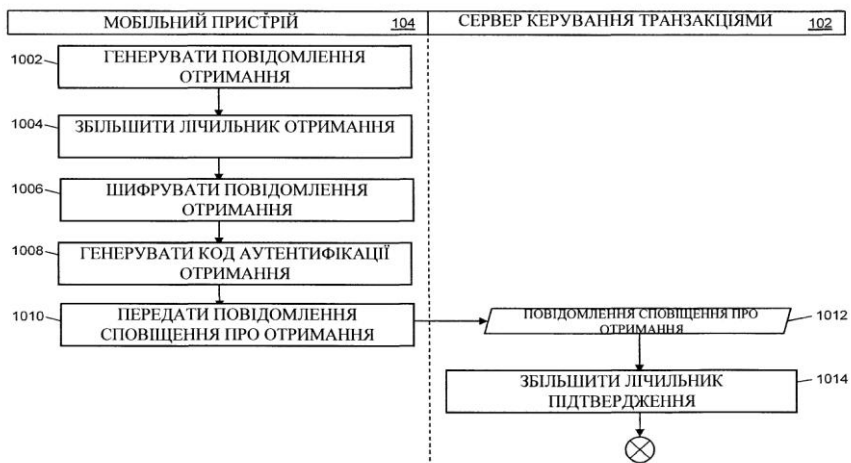
Фіг. 7



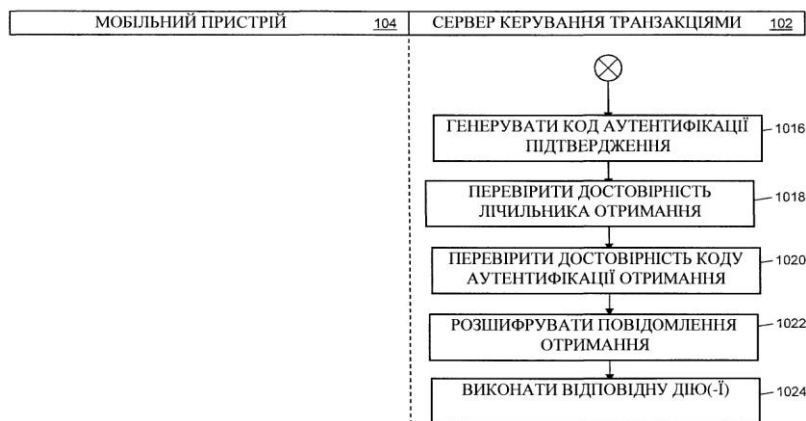
Фіг. 8



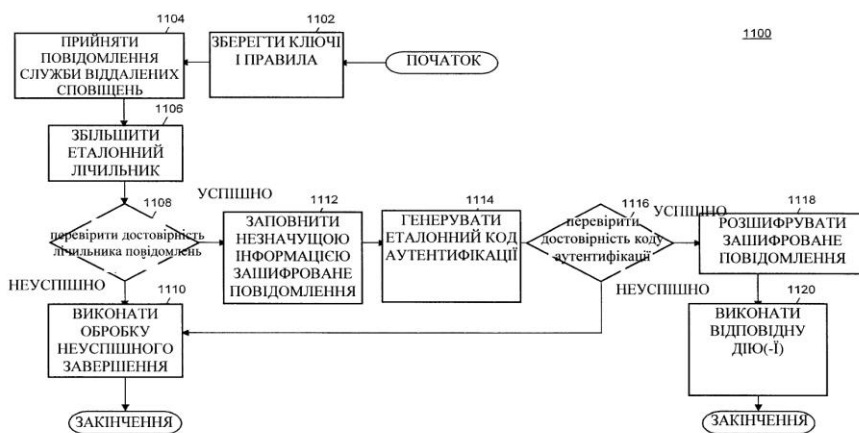
Фіг. 9



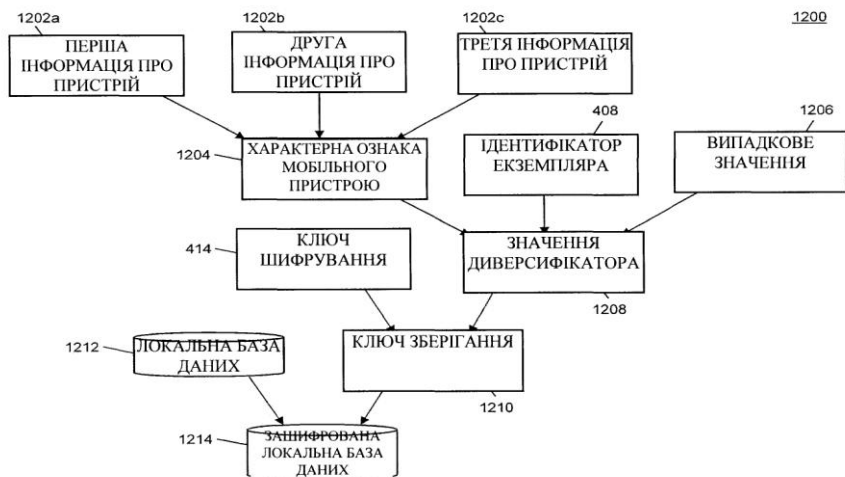
Фіг. 10А



Фіг. 10В



Фіг. 11



Фіг. 12

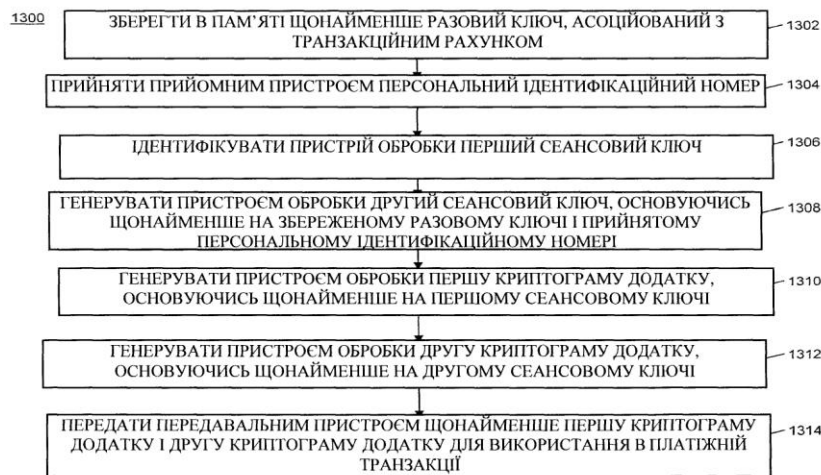


Fig. 13

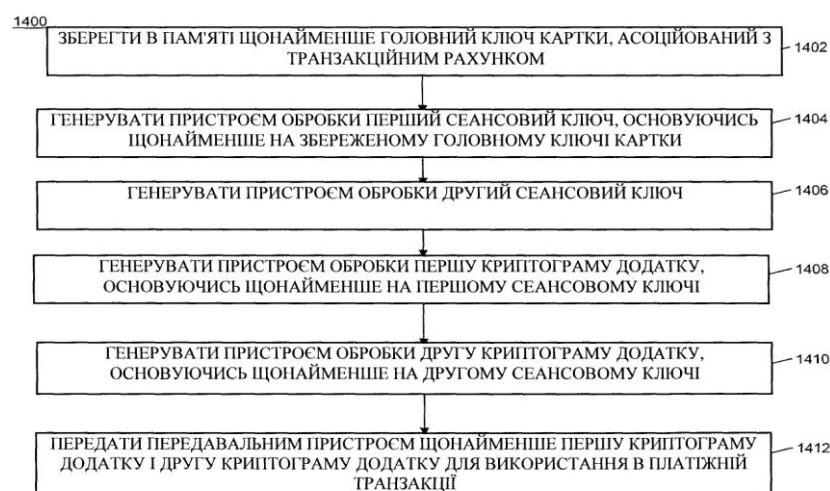


Fig. 14

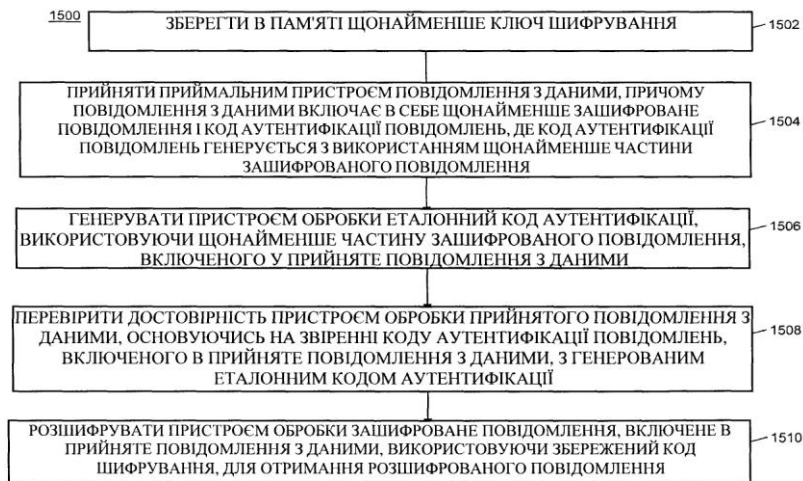


Fig. 15

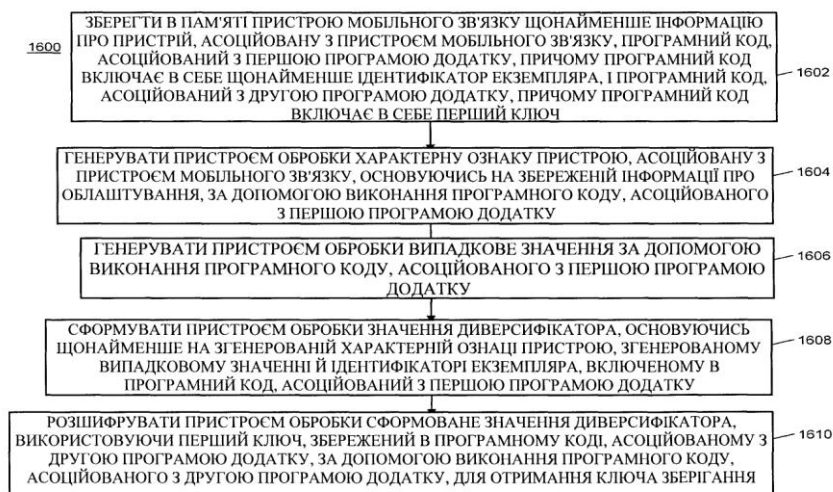


Fig. 16

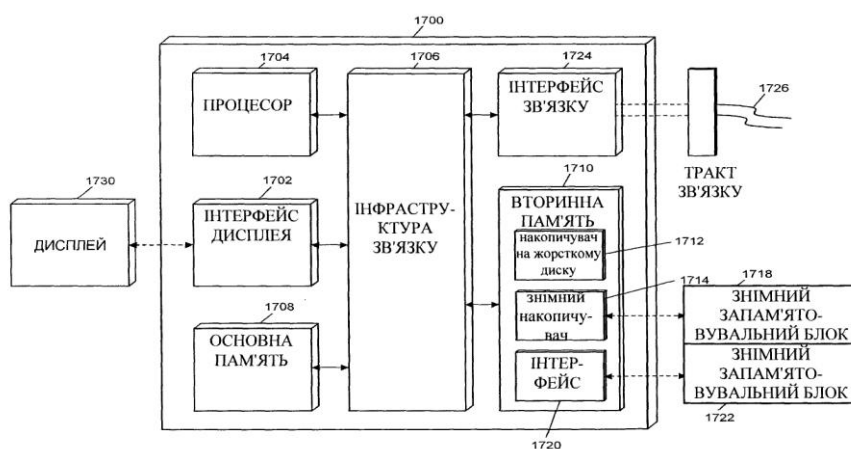


Fig. 17

Комп'ютерна верстка В. Мацело

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601