



УКРАЇНА

(19) UA

(11) 101469

(13) C2

(51) МПК

G06Q 20/40 (2012.01)

G06F 17/30 (2006.01)

ДЕРЖАВНА СЛУЖБА  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ  
УКРАЇНИ

## (12) ОПИС ДО ПАТЕНТУ НА ВІНАХІД

(21) Номер заявки:	а 2009 01769	(72) Винахідник(и):	Вальтер Грег (AU)
(22) Дата подання заявки:	01.08.2007	(73) Власник(и):	К'ЮПЕЙ ХОЛДІНГС ЛІМІТЕД, 74 Wentworth Drive, Capalaba, QLD 4157, Australia (AU)
(24) Дата, з якої є чинними права на винахід:	10.04.2013	(74) Представник:	Петров Андрій Володимирович, реєстр. №139
(31) Номер попередньої заявки відповідно до Паризької конвенції:	2006904149, 2007900469	(56) Перелік документів, взятих до уваги експертизою:	US 2003221125 A1; 27.11.2003 EP 0745961 A2; 04.12.1996 EP 1136961 A1; 26.09.2001 WO 2005073889 A1; 11.08.2005 US 2006282395 A1; 14.12.2006 GB 2399209 A; 08.09.2004 GB 2398159 A; 11.08.2004 US 2005043964 A1; 24.02.2005 US 2004078238 A1; 22.04.2004 WO 0142883 A2; 14.06.2001 JP 02027463 A; 30.01.1990
(32) Дата подання попередньої заявки відповідно до Паризької конвенції:	01.08.2006, 01.02.2007		
(33) Код держави-учасниці Паризької конвенції, до якої подано попередню заявку:	AU, AU		
(41) Публікація відомостей про заявку:	10.07.2009, Бюл.№ 13		
(46) Публікація відомостей про видачу патенту:	10.04.2013, Бюл.№ 7		
(86) Номер та дата подання міжнародної заявки, поданої відповідно до Договору РСТ	PCT/AU2007/001076, 01.08.2007		

## (54) СИСТЕМА АВТОРИЗАЦІЇ ТРАНЗАКЦІЙ ТА СПОСІБ ЇЇ ЗАСТОСУВАННЯ

## (57) Реферат:

Система авторизації транзакцій (20), яка дозволяє клієнту (40) авторизовувати транзакції відносно як мінімум до одного рахунку клієнта (40), пов'язаного з установою (50), система (20) включає в себе засоби зберігання даних (24) для можливості доступу до ідентифікаційних даних, пов'язаних з клієнтом (40) та віддаленим комунікаційним пристроєм (RCD) (30) клієнта (40), та безпечного ідентифікатора даних, пов'язаних з рахунком клієнта (40) з ідентифікаційними даними. Система (20) також включає в себе засоби зв'язку (26) для отримання авторизаційного запиту, який посилається до безпечного ідентифікатора даних, відносно до транзакції від установи (50) і для можливості зв'язку з клієнтом (40) через RCD (30), щоб авторизувати транзакцію рахунку клієнта (40). Засоби обробки даних (22) системи (20) ідентифікують клієнта (40) та RCD (30), використовуючи ідентифікаційні дані та визначають, якщо транзакція авторизована клієнтом (40). Засоби зв'язку (26) надають вказівку, яка посилається до безпечного ідентифікатора даних, до установи (50) авторизована чи ні транзакція клієнтом (40).

UA 101469 C2

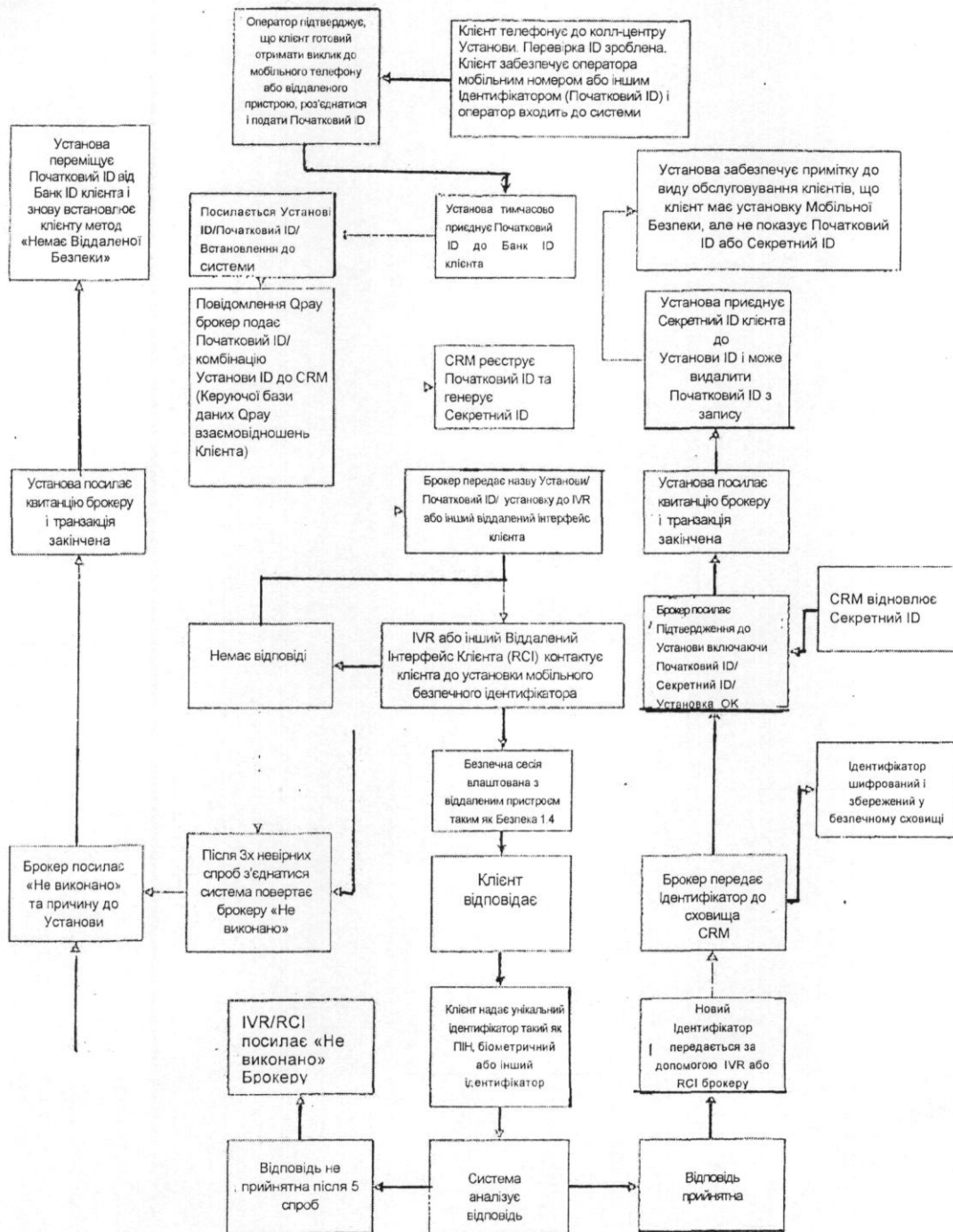


Fig. 2

Даний винахід має відношення до системи та способу авторизації транзакцій таких як покупки за допомогою кредитної картки, банківські перекази, та купівля акцій, особливо у навколишньому середовищі, де віддалені платежі за товари і послуги вже зроблені

Передумови створення винаходу

Безпека фінансових і інших типів транзакцій дуже важлива завдяки відносно недавньому зростанню загроз таких як фішинг і фармінг, які мають намір шахрайськи отримати чутливу інформацію, як наприклад паролі, пін коди та деталі кредитних карток, маскуючись як надійна особа або бізнес в електронній комунікації. Як тільки такі деталі шахрайськи отримані, вони використовуються для фінансових платежів або незаконного привласнювання грошей з фінансових рахунків. Тримач рахунку часто не знає про ці шахрайські транзакції до тих пір, поки вони вже зроблені і тоді вже надто пізно для їх відміни. Бажано, щоб дозвіл був отриманий для транзакції від клієнта перед тим як транзакція вже буде виконана фінансовою установою.

У поточних системах використання авторизації фінансових транзакцій, це важко і часто неможливо отримати гарантію фірми про те, що особа, яка ініціювала транзакцію є тримачем рахунку і уповноважена проводити транзакцію. Наприклад, коли продавець проводить кредитною картою клієнта, термінал кредитної картки з'єднується з покупцем, або процесором кредитної картки, який перевіряє дійсність рахунку клієнта і достатні фонди для покриття вартості транзакції. Проте, цей процес не забезпечує жодної форми перевірки тому що індивідуально зроблена транзакція також потребує авторизації.

Хоча продавець може порівнювати підпис на кредитній картці з підписом клієнта, проте такі методи перевірки взагалі або не шахрайської транзакції далекі від надійності. До того ж, тримач рахунку і постачальник кредитної картки залежать від продавця, що відхиляє транзакції, які йому здаються обманними чи непідтвердженими.

Цей результат особливо явний з транзакціями проведеними у навколишньому середовищі або по телефону, коли продавець не може перевірити підпис клієнта і тому визначають була чи не була транзакція обманною.

Один спосіб подолання таких проблем - вимагати, щоб покупець надав Код Важливого Підтвердження Картки (CVV), який не є частиною номера картки безпосередньо, і також відомий як CVV2, CVC2, та CID. CVV пізнавальна процедура, встановлена компаніями кредитної картки, щоб зменшити фальсифікацію для Інтернет і телефонних транзакцій. Це складається з необхідності тримача картки CVV номер під час підтвердження транзакції, коли картка є під рукою. Поки CVV код допомагає з'ясувати, що клієнт розміщує замовлення фактично володає кредитною/дебетною картою і що рахунок картки легітимний, ця пізнавальна процедура неефективна, коли карта безпосередньо була незаконно привласнена або по сценарію коли був не підтверджений доступ до фінансових записів тримача рахунку.

Так само, в поточних системах, де клієнт потребує надання паролю або пін-коду перед тим як транзакція підтверджена, не уповноважений доступ до записів тримача рахунку ймовірно, забезпечує інформацію, потрібну для шахрайської авторизації транзакцій.

Відповідно, це - предмет винаходу, щоб забезпечувати систему для авторизації транзакцій, який прагне полегшити завдання попереднього способу систем.

Це ясно розумітиметься що якщо попередній опублікований спосіб або системи направлені в цьому, то це посилення не визначає допущення, що публікація або система формує частину загальних основних знань в рівні техніки в Австралії або в будь-якій іншій країні.

Короткий виклад суті винаходу

В цілому, винахід дозволяє транзакції такі, як платежі кредитними картками, он-лайн банківські перекази фондів, або інші, щоб бути безпечно авторизованими клієнтом, переважно перед тим, як транзакція виконана уповноваженою установою. У одному випадку, така авторизація відбувається, коли клієнт, спонукає систему, наприклад, інтерактивним розпізнаванням голосу (IVR), надати один або більше унікальних ідентифікаторів підтвердження його чи її ідентичності і засвідчити транзакцію. Альтернативно, клієнт, можливо, указує, що транзакція обманна, яка у свою чергу повідомлена уповноваженій установі таким чином, що відповідні дії можливо виконані. Інформація, підтримувана системою авторизації відділяється від рахунку і записів клієнтів фінансової установи для того, щоб максимізувати безпеку в процесі авторизації і зменшити ризик обманної ідентифікації транзакцій які, можливо, виникають в результаті не уповноваженого доступу до збереженої інформації.

У одному аспекті, винахід забезпечує систему авторизації транзакції для дозволу клієнта авторизувати транзакції, що мають відношення як мінімум до одного рахунку клієнта, пов'язаного з установою, системою, що включає:

засоби зберігання даних для можливості доступу до

(а) ідентифікаційних даних, пов'язаних з клієнтом;

(b) ідентифікаційних даних, пов'язаних з віддаленим комунікаційним пристроєм (RCD) клієнта; та

(c) безпечного ідентифікатора даних, пов'язаних з як мінімум одним рахунком клієнта з будь-яким одним або обома з (a) та (b);

5 засоби першої комунікації для дозволу комунікації з клієнтом через RCD, щоб авторизувати транзакцію як мінімум одного рахунку клієнта;

структуру обробки даних, що включає обробку даних, яка має намір ідентифікувати клієнта використовуючи (a), ідентифікує RCD використовуючи (b) і визначає, чи транзакція авторизована клієнтом; і

10 засоби другої комунікації для отримання запиту авторизації відносно транзакції та забезпечення вказівок установи, чи була або не була транзакція авторизована клієнтом, там, де запит авторизації отриман і вказівка, забезпечена до установи, посиляється до даних ідентифікаторів безпеки.

У іншому аспекті, даний винахід забезпечує спосіб для дозволу клієнта авторизувати транзакції, пов'язані як мінімум з одним рахунком клієнта, що знаходиться в установі, спосіб включає наступні етапи:

a) авторизаційний сервер одержує запит авторизації від установи відносно транзакції як мінімум одного рахунку клієнта;

20 b) авторизаційний сервер зв'язується з клієнтом через віддалений комунікаційний пристрій (RCD) клієнта, щоб авторизувати транзакцію;

c) авторизаційний сервер ідентифікує клієнта використовуючи ідентифікаційні дані, пов'язані з клієнтом, до якого авторизаційний сервер має доступ;

d) авторизаційний сервер ідентифікує RCD використовуючи збережені ідентифікаційні дані, пов'язані з RCD, до якого авторизаційний сервер має доступ;

25 e) авторизаційний сервер визначає чи транзакція авторизована клієнтом;

f) авторизаційний сервер повідомляє вказівки установі, чи була або не була транзакція авторизована клієнтом;

там, де запит авторизації отриман авторизаційним сервером і вказівка, забезпечена до установи, посиляється установою та аутентифікаційний сервер до ідентифікаційних даних безпеки для з'єднання як мінімум одного рахунку клієнта з одним або обома із збережених ідентифікаційних даних, пов'язаних з клієнтом і збереженими ідентифікаційними даними, пов'язаними з RCD.

У іншому аспекті, даний винахід забезпечує спосіб для дозволу клієнта авторизувати транзакції, пов'язані як мінімум з одним рахунком клієнта, спосіб включає наступні етапи:

35 a) авторизаційний сервер одержує запит авторизації відносно транзакції рахунку клієнта;

b) авторизаційний сервер зв'язується з клієнтом через віддалений комунікаційний пристрій (RCD) клієнта, щоб авторизувати транзакцію;

40 c) авторизаційний сервер запитує клієнта дослівно повторити випадкове слово або фразу, створені сервером, та/або забезпечити як мінімум деяку інформацію, пов'язану з клієнтом або рахунком клієнта;

d) авторизаційний сервер надає доступ до даних, пов'язаних з клієнтом або рахунком клієнта, та голосового відбитка або голосових біометричних ідентифікаційних даних, пов'язаних з клієнтом; та

45 e) авторизаційний сервер ідентифікує клієнта, порівнюючи слово, фразу та/або інформацію, надані клієнтом з випадковим словом або фразою, створеними сервером, та/або наданий доступ до даних за допомогою сервера, та порівнюють результуючий голосовий відбиток або голосові біометричні дані клієнта з голосовим відбитком або

голосовими біометричними ідентифікаційними даними, наданими сервером,

50 де клієнту тільки дозволено авторизувати транзакцію один раз, як тільки клієнт був ідентифікований.

У іншому аспекті, даний винахід забезпечує систему авторизації транзакцій для дозволу клієнта авторизувати транзакції, пов'язані як мінімум з одним рахунком клієнта, система включає:

засоби зберігання даних для можливості доступу до

55 a) голосового відбитка або голосових біометричних ідентифікаційних даних, пов'язаних з клієнтом; та

b) ідентифікаційних даних, пов'язаних з віддаленим комунікаційним пристроєм (RCD) клієнта; та

c) даних, пов'язаних з клієнтом та/або рахунком клієнта;

засоби зв'язку для можливості зв'язку з клієнтом через RCD та запитування клієнта дослівно повторити випадкове слово або фразу, створені сервером, та/або забезпечити як мінімум деяку інформацію, пов'язану з клієнтом або рахунком клієнта; та

структуру оброблення даних, що включає засоби оброблення даних, щоб ідентифікувати RCD, використовуючи (b), ідентифікувати клієнта, порівнюючи слово, фразу та/або інформацію надані клієнтом з випадковим словом або фразою, що створені системою та/або (c), і порівняти результуючий голосовий відбиток або голосові біометричні дані клієнта з (a), та визначити, якщо транзакція авторизована клієнтом;

де клієнту тільки дозволено авторизувати транзакцію один раз, як тільки клієнт був ідентифікований.

У одній формі, винахід перебуває у віддаленій системі оплати, що дозволяє клієнтові вести оплати за товари і послуги віддалено у безпечній формі з членами системи, система включає:

i) засоби зберігання даних, що містять оновлюванні дані, що мають відношення до кожного з множинності клієнтів і кожний з множинності членів системи, там, де кожен клієнт має як мінімум один пов'язаний реєстраційний профіль із пов'язаним грошовим сховищем;

ii) структуру обробки даних, що включає засоби обробки даних і систему розрахункового центру для врегулювання заборгованості між членами і клієнтами системи,

iii) засоби зв'язку, пов'язані з структурою обробки даних для зв'язку з клієнтами через віддалений комунікаційний пристрій (RCD) кожного з клієнтів,

система організовується для одного або більше з сказаних клієнтів вести справу оплат за товари або послуги згідно із запитом оплати, зробленим один або більше з членів, запиту оплати, що запускає комунікаційну подію від засобів зв'язку до RCD важливого клієнта з метою підтвердження ідентичності клієнта і доступу до відповідного реєстраційного профілю, і система, крім того організовується, щоб підтверджувати ідентичність клієнта і як тільки таке має місце, дозволяючи клієнтові вести справу платежів забезпечує позитивний баланс залишений в грошовому сховищі.

В другій формі, винахід перебуває у віддаленому способі оплати, що дозволяє клієнтові вести справу оплат за товари і послуги віддалено в безпечній формі з членами віддаленої системи оплати, система включає в себе:

i) засоби зберігання даних для змісту оновлюваних даних, що мають відношення до кожного з множинності клієнтів, і кожний з множинності членів системи, там, де кожен клієнт має як мінімум один пов'язаний реєстраційний профіль, пов'язаним із грошовим сховищем;

ii) структуру обробки даних, що включає засоби обробки даних і систему розрахункового центру для врегулювання заборгованості між членами і клієнтами системи,

iii) засоби зв'язку, пов'язані з структурою обробки даних для зв'язку з клієнтами через віддалений комунікаційний пристрій (RCD) кожного з клієнтів,

там, де клієнт використовує систему, щоб вести справу оплат за товари або послуги згідно із запитом оплати, зробленим один або більше членами, запит оплати, що запускає комунікаційну подію як мінімум одного з засобів зв'язку до RCD важливого клієнта з метою підтвердження ідентичності клієнта і доступу до відповідного реєстраційного профілю, і як тільки ідентичність клієнта була підтверджена, клієнт дозволяє вести справу платежів, забезпечивши залишений позитивний баланс в грошовому сховищі.

Термін транзакція призначений для широкого покриття різних дій, які можуть бути виконані за рахунком, такі, як запити оплат, запити замовлень, передачі акцій, грошові перекази, запити посвідчення особи, запити виділення інформації, або комбінація цих дій. Такі дії також можуть бути ініційовані в різноманітних формах, наприклад, запит оплат може виходити від транзакції кредитною картою на фізичне зберігання, покупка на сайті електронної торгівлі (клацніть для покупки), або віддаленій системі оплат, яка використовує мобільний телефон клієнта для оплати товарів і послуг, таких, як системи текст для покупки або розмова для покупки.

Термін клієнт призначений для розуміння широко включати в себе не тільки клієнтів фінансових установ, але також і будь-яких осіб, які мають рахунок в установі, наприклад, працівників, постачальників, або громадян, пов'язаних з державною установою.

Винахід вигідно надає клієнтові можливість, бажано з використанням, принаймні одного із засобів комунікації, такої як оффлайн і, отже, менш чутливі до порушень безпеки, щоб авторизувати або сигналізувати транзакцію до того, як її затвердить банк або кредитна картка емітента, та кошти передаються продавцю.

Хоча це, як правило, бажано, щоб авторизація транзакції сталася якомога швидше до кінця процесу транзакції, то слід зазначити, що авторизація транзакції може відбуватися в будь-якому місці в ході процесу транзакції. Наприклад, у ньому передбачається, що авторизація транзакції може відбутися ще до прохання про виділення коштів продавцем. Це особливо вигідно у

навколишньому середовищі, де час обробки транзакцій, як правило, повинен підпадати під специфічні обмеження.

Крім того, передбачено, що винахід може застосовуватися в тих випадках, коли попереднє схвалення авторизації надається без першого контакту з клієнтом, що дозволяє проводити транзакцію без зволікань. Однак, якщо клієнт, один раз звертався щодо транзакції, не авторизував транзакцію або сигналізував про транзакцію як несанкціоновану, попередня авторизація негайно скасовується, і якщо кошти вже були переведені, вони також будуть повернені.

Використання безпечних ідентифікаторів, таких, як PIN, який запам'ятав клієнта або біометричні дані (наприклад, голосовий слід, відбиток пальця, сканування сітківки ока, манери т. ін.) означає, що транзакція є лише авторизованою коли ідентичність клієнта, використовуючи інформацію, яка як правило, не доступна для шахрайських осіб, перевіряється. Ще одна перевага забезпечується тим, що перевірка клієнта та контактних даних в системі ведуться в окремому сховищі даних для деталей клієнтів банку з тільки одним ідентифікатором безпеки (відомим тільки в банківській системі і системі авторизації) посилюючись на окреме сховище даних. Така установка забезпечує підвищену безпеку, коли несанкціонований доступ до будь-якої з цих сховищ даних сам по собі не забезпечує адекватну інформацію для обходу системи авторизації та проведення шахрайських транзакцій.

Система цього винаходу є особливо корисною для клієнтів, які не мають доступу до традиційних банківських послуг, або тих, хто просто хочуть мати більш зручний і безпечний спосіб, в якому можливо авторизувати платежі за товари та послуги, або інші транзакції, в безпечний спосіб. Платежі можуть стягуватися з боку системного адміністратора для транзакцій ефективно використовуючи систему, яка може бути фіксованою сумою гонорару або відсотками від суми транзакції, або їх комбінацією.

Віддалений комунікаційний пристрій (RCD), може бути будь-який пристрій, здатний для зв'язку і не обмежений односторонніми або двохсторонніми комунікаційними пристроями. Приклади бажаних форм RCDs включають в себе фіксованих клієнтів або мобільний телефон, персональний обчислювальний пристрій (будь-то мобільний або стаціонарний) або факсиміле або пейджер клієнта. Всі ці пристрої, та інші, які не зазначені у переліку, але вони включені в якості RCD, зазвичай мають програмний компонент.

Будь-який RCD(s), який клієнт бажає використовувати з системою, повинен бути зареєстрований у системі і, відповідно, інформація ідентифікації RCD (яка, як правило, унікальна для того RCD) записується для використання в процесі ідентифікації.

Клієнт може призначити який RCD або групи RCDs вони хотіли б використовувати для контакту з системою, та, якщо група призначена, наприклад, для багатофакторної аутентифікації (див. нижче), клієнт може додатково призначити RCD, який полягає в тому, щоб виступати в основі багатофакторного процесу ідентифікації.

Авторизація для конкретної транзакції буде залежати від підтвердження особи клієнта, яка, як правило, потрібна, перш ніж авторизація на транзакцію дається. Ця система визначає підтвердження особистості клієнта, як попереднє умова авторизації, і транзакція буде по можливості заблокованою до авторизації, якщо ця умова не задоволена. Іншими словами, ця транзакція буде відмінена якщо особистість клієнта не може бути встановлена системою. Повідомлення може бути відправлено системному адміністратору, повідомивши про невірність підтвердження особистості клієнта системному адміністратору, що дозволяє відмовитися від кроків або блокувати запит транзакції, який повинен бути прийнятий.

Як правило, авторизація транзакцій в цілому, що надається фінансовими установами залежить від підтвердження ідентифікаційного параметру та/або інших параметрів, до тих пір, поки сума транзакції не перевищує кредитний ліміт, і/або членство, як і раніше в силі і т.п. Система даного винаходу може застосовуватися в якості додаткової частини цього процесу авторизації. Система може бути пов'язана з даними, гонорарами, що використовуються в ході процесу авторизації та задоволення чи порушення критеріїв ідентифікації пов'язаних з системним адміністратором може бути ще параметр, який може знадобитися до проведення авторизації фінансовою установою.

У контексті транзакції загальних кредитних карток, наприклад, клієнт, який, як правило, є власником картки використовує картку, щоб зробити покупки у продавця, який приймає бізнес платежі кредитною карткою за товари чи послуги, що продаються клієнту. Продавець зазвичай збирає інформацію з картки, шляхом сканування картки через зчитувач або аналогічні пристрої, якщо він знаходиться в магазині, чи інакше через Інтернет або по телефону.

Якщо продавець бажатиме перевірити, наприклад, що картка дійсна і клієнт кредитної картки має достатньо коштів, щоб здійснити покупку, електронна перевірка проводиться,

використовуючи термінал оплати кредитної картки, систему Пункт Продажу (POS) або подібну через комунікаційні посилання до запитуємого банку продавця. Дані з картки надходять від магнітної стрічки або чіпа на картці, чіпа на пристрої клієнта, або забезпечені клієнтом в оперативній формі або словами по телефону.

5 Покупець, також фінансова установа або інша організація, яка забезпечує послуги обробки картки до продавця, контактує з емітентом картки через асоціацію картки, таку мережу як наприклад VISA або MasterCard (та інші), яка служить доступом між покупцем і емітентом для авторизації і проведення транзакцій.

10 Емітент, переважно перед авторизацією і проведенням транзакції, подає запит до системи даного винаходу для авторизації клієнта.

Це повинно цінуватися, що такі авторизаційні запити клієнтів не обмежені системами оплат, що залучають кредитні картки, але можуть бути однаково застосовані до систем фінансових транзакцій, що залучають дебетові картки, перекази коштів між рахунками, закупівлі акцій, і т. ін., або наприклад, при доступі до безпечних систем через мережу і запит з метою авторизування доступу до віддаленої системи впливає.

Повна віддалена система оплат, в якій запит авторизації клієнта отриманий і оброблений безпосередньо системою, також передбачена і описана детально нижче.

Важливо, не дивлячись на спосіб, в якому контакт для оплати використовує систему, незалежні частини ідентифікації і процесів підтверджень переважно матимуть місце, починаючи з контакту системи з зазначеним RCD клієнта і переважно використовує систему інтерактивного розпізнавання голосу (IVR) або подібну систему, щоб перевірити ідентичність клієнта. Процес ідентифікації має включати в себе один або більше чинники і способи контакту з клієнтом і ідентифікацію включаючи, але не обмежуючись, системами IVR, біометричною інформацією, що має відношення до клієнта як наприклад визнання голосу зокрема, кодовий вхід від одного або 25 більше джерел через один або більше канали зв'язку, генеровані коди, Радіочастоту ID (RFID), одноразово тільки коди або подібне.

Двохчинна ідентифікація, можливо, використовується в спробі подолати новіші форми фальсифікації, оскільки використовує два різних шляхи комунікацій. Наприклад, система може повідомляти виклик до стільникового телефону клієнта через SMS і чекати вказану відповідь. 30 Якщо передбачається, що всі клієнти банків мають стільникові телефони тоді ці результати в двухчинній ідентифікації проходять без додаткових технічних засобів. Багаточинна ідентифікація зазвичай залучає використання більш ніж одного каналу зв'язку або сесій де виклик може бути переданий по першому каналу і, відповідь клієнта або друга ідентифікаційна частина повідомляється по іншим каналам зв'язку або іншою комунікаційною сесією, ніж спочатку, вимагаючи, щоб клієнт мав доступ до обох для того, щоб виконати її, роблячи підслуховування набагато важчим. Канали зв'язку зазвичай будуть направлені специфічному RCD, який безпосередньо, як правило, матиме унікальну інформацію ідентифікації, яка також потрібна для підтвердження або кореляції інформації перевірки клієнта, що запам'ятала система перед тим, як ідентифікація надана.

40 Система використовує запит ідентифікації як підставу для контакту з клієнтом через як мінімум один RCD клієнта, використовуючи швидке введення даних. Швидке введення даних, можливо, є повідомленням, що запрошує вхід специфічної приватної ідентифікації (приватний ID) інформації як наприклад код або інші дані перевірок, оригінальний вхід яких створений клієнтом або проводиться, коли рахунок клієнта спочатку пов'язують з системою і який, можливо 45 змінити при необхідності.

Інформація має відношення до одного або більше приватних IDs, і один або більше RCDs клієнта запам'ятовує система, але утримує окремо від інформації рахунку клієнта, якого підтримують системи доречної установи. Інформація, що має відношення до специфічного клієнта в системі і систем фінансової установи, використовуючи унікальний безпечний ідентифікатор (Безпека ID), який не обов'язково має відношення до ідентифікаційних характеристик клієнта або RCD клієнта, і навіть не вимагає, щоб бути наданим клієнту.

Система порівнює приватну інформацію ID, отриману від клієнта, або аспекти наданої інформації, згідно з швидким введенням даних, до приватних ідентифікаційних даних, підтримуваних системою для потреб перевірок. Переважно, відповідні приватні ідентифікаційні 55 дані від клієнта і які зберегла система забезпечуються з механізмом кодування як наприклад випадкові дані.

Форма контакту з клієнтом, якій надається перевага, для потреб ідентифікації, є система, що використовує компонент інтерактивного розпізнавання голосу (IVR), який є комп'ютеризованою системою, яка дозволяє людині, зазвичай телефонному клієнту, вибрати опцію з голосового меню і іншого інтерфейсу з комп'ютерною системою. Загалом система програє заздалегідь 60

записані підказки голосу, за якими людина натискає номер на телефонній допоміжній клавіатурі, щоб вибрати обрану опцію, або говорить прості відповіді такі як "так", "ні", або номери відповідей до підказок голосу.

Найостанніші системи використовують розпізнавання розмовної мови, щоб інтерпретувати питання, які людина хоче відповісти. Новітня тенденція Ведеться Розмовне IVR, яка об'єднує живих людських агентів в проєкті і технологічному процесі додатку, щоб допомогти розпізнаванню мови з людським контекстом. IVR розвивається, як телефонна система, але подібні системи зараз доступні, які функціонують на нетелефонних системах і на будь-якій функціонально еквівалентній системі або комбінаціях систем, можуть використовуватися.

Зазвичай, компонент IVR включає в себе, як мінімум, засоби одного зв'язку і на структурі обробки даних, одержуючи швидку ідентифікацію, компонент IVR зазвичай контактуватиме з клієнтом, використовуючи їх переважний віддалений комунікаційний пристрій (RCD). Ймовірно, RCD є мобільним телефоном або подібний і система IVR може тоді проводити клієнта через вхід їх ідентифікаційної інформації, яка використовується в процесі розпізнавання. Важливо, засіб зв'язку системи також зазвичай матиме здатність визначити ідентифікаційні характеристики специфічних віддалених засобів зв'язку, що використовувалися, як наприклад номери SIM-карт або адреси IP, або цифрові свідоцтва і подібні для того, щоб ідентифікувати клієнта згідно процесу багаточинної ідентифікації.

Якщо дані перевірок введені, підтверджені або корельовані до даних перевірок на файлі, потім вважається, що клієнт пройшов перевірку для авторизації транзакції. Якщо введені дані перевірок, не відповідають або корелюють до даних перевірок на файлі, потім вважається, що клієнт не пройшов перевірку і він викидається з системи.

Невірне введення даних перевірки може також сигналізувати завершення від адміністратора системи. Переважно, один раз невірного введення даних перевірки обумовлює ряд разів, які, можливо, як мінімум, є одного разу, але переважно не більше ніж тричі, коли клієнт, можливо, блокується системою протягом періоду часу. Блокування, можливо, активне на рахунку(ах) клієнта або, можливо, обмежено блокуванням доступу до системи від специфічних віддалених засобів зв'язку, використовуваних клієнтом, як, визначені використання ідентифікаційних характеристик специфічних віддалених використовуваних засобів зв'язку.

Як тільки ідентифікація надана або відхилена, відповідна вказівка передана до доречної фінансової установи(в) і відповідного повідомлення, що радить клієнтові результат ідентифікаційного процесу, переважно проводиться структурою обробки даних і пересилається до переважної RCD клієнта.

Короткий опис фігур

Переважні втілення даного винаходу зараз будуть описані з посиланням на супровідні фігури, в яких:

Фіг.1 є контекстною діаграмою, що забезпечує короткий огляд переважного втілення винаходу;

Фіг.2 блок-схема процесу встановлення переважного втілення винаходу;

Фіг.3 блок-схема процесу авторизації переважного втілення винаходу;

Фіг.4 блок-схема процесу зміни пристрою переважного втілення винаходу;

Фіг.5 блок-схема процесу зміни ідентифікатора клієнта переважного втілення винаходу;

Фігура 6 є контекстною діаграмою, що забезпечує короткий огляд віддаленої системи оплат, об'єднуючої переважне втілення даного винаходу;

Фігура 7 блок-схема процесу реєстрації клієнта віддаленої системи оплат, об'єднуючої переважне втілення даного винаходу;

Фігура 8 блок-схема процесу реєстрації веб-сайту віддаленої системи оплат, об'єднуючої переважне втілення даного винаходу;

Фігура 9 блок-схема процесу ідентифікації клієнта віддаленої системи оплат, об'єднуючої переважне втілення даного винаходу;

Фігура 10 блок-схема першого депозитного процесу віддаленої системи оплат, об'єднуючої переважне втілення даного винаходу;

Фігура 11 блок-схема процесу покупок віддаленої системи оплат, об'єднуючої переважне втілення даного винаходу;

Фігура 12 блок-схема процесу переказу коштів віддаленою системою оплат, об'єднуючої переважне втілення даного винаходу; та

Фігура 13 блок-схема процесу запиту балансу віддаленої системи оплат, об'єднуючої переважне втілення даного винаходу.

Детальний опис втілення винаходу

Даний винахід не особливий до будь-яких специфічних технічних засобів або виконання



програмного забезпечення, і знаходиться на концептуальному рівні вище за специфічні особливості виконання. Це повинно розумітися, що різні інші втілення і зміни винаходу можуть проводитись без відхилення від змісту або сфери втілення винаходу. Наступне забезпечене, щоб допомогти в розумінні практичного виконання специфічних втілень винаходу.

5 Авторизаційна система 20, як показано на Фіг. 1, включає засоби обробки даних, такі як сервер 22, із засобами зв'язку 26, які зв'язуються з системою установи 10 установи 50 і пристроєм клієнта 30 клієнта 40. Клієнт 40 - загалом клієнт установи 50, але, можливо, є працівником, постачальником, громадянином, що має відношення до урядової організації або подібної. При різних обставинах, отже, клієнт 40, можливо, ідентифікується системою установи 10, використовуючи будь-яку форму загальнодоступних ідентифікаційних даних (Суспільний ID), як наприклад номер рахунку, кредит/дебет або інший номер картки, номер працівника, логін, пароль або інший відповідний ідентифікатор. У декількох випадках, комбінація цих ідентифікаторів, можливо, використовується як Суспільний ID.

15 Ідентифікаційна інформація, що має відношення, наприклад, до установи 50, пристрою клієнта 30 і клієнта 40, безпечно запам'ятовується в базі даних 24 авторизаційної системи 20. База даних 24 може мати будь-яку з декількох форм, наприклад, єдина центральна база даних, розподілена база даних або ряд безпечних баз даних.

20 Цінуватиметься, що при авторизаційній системі 20 обговорюється в контексті фінансової установи, як наприклад емітент кредитної картки, установа 50 може бути будь-якою організацією, що вимагає безпечної авторизації транзакції. Приклади таких установ включають працедавця, банк, урядову організацію, фондового маклера або будь-який інший об'єкт, який шукає безпечної ідентифікації або авторизації.

25 Також цінуватимуть, що при авторизаційній системі 20 обговорюється в контексті фінансової транзакції, транзакція може приймати інші відповідні форми, як наприклад, запит для ідентифікації клієнта 40. Приклади транзакцій, що вимагають авторизації авторизаційною системою 20 включають в себе оперативну або без посередників фінансову транзакцію, запит, щоб схвалити закупівлю акцій або продаж, або запит для ідентифікації, який, можливо, потрібен для клієнта 40, щоб увійти до будівлі, відкрити рахунок, або домовитися з установою або урядовою організацією.

30 У одній формі, авторизаційна система 20 і система установи 10, можливо, розміщена в такому ж безпечному навколишньому середовищі, щоб мінімізувати можливості комунікацій між ними, будучи перехопленим неавторизованою стороною або якщо авторизаційна система 20 об'єднана з установою 50 в їх власному безпечному місці обробки.

35 Проте, де авторизаційна система 20 і система установи 10 розміщені в окремих фізичних навколишніх середовищах, комунікації між ними потрібно переважно полегшити через безпечний зв'язок як наприклад прямий зв'язок, переважно використовуючи "мережеві" (тобто не Інтернет або веб-заснована павутина) технології як наприклад блок даних або безпечний пункт, щоб вказати момент зв'язку. Коли авторизаційна система 20 і система установи 10 зв'язуються через використання "включених-мережевих" технологій, сильну ідентифікацію і способи кодувань, як наприклад VPN, що прокладає зв'язок з ідентифікацією виклику або подібною технологією як наприклад Клієнтські/Серверні свідоцтва, потрібно переважно використовувати. У таких випадках, віддається перевага, щоб дані, повідомлені через зв'язок, кодувалися з мінімальним кодуванням 128 біт. Додаткову безпеку, можливо, забезпечити, підтвердивши пакети даних, що використовують алгоритм HMAC (Ідентифікаційний Код Повідомлення мішанини), в якому система установи 10 забезпечена з секретним ключем і всією інформацією, посланою системою установи 10, відкидається проти ключа, щоб засвідчити дані. До того ж, додаткові рівні безпеки для переданих даних можуть бути також бути доданими, якщо потрібно, як наприклад технічні засоби кодувань.

45 Віддається перевага, щоб зміни до авторизаційної системи 20 автоматично зареєструвалися і підтримувалися в межах безпечного контрольного журналу, який не може бути змінений навіть в привілейованому або адміністративному рівні доступу, і повинен бути доступний у форматі повідомлення.

50 Або авторизаційна система 20 і система установи 10 безпечно разом розміщені або безпечно віддалено з'єднані, унікальний безпечний ідентифікатор, надалі Безпека ID використовується, щоб корелювати інформацію, що має відношення до клієнта 40 в обох системах таких як авторизаційна система 20 і система установи 10, як тільки процедура встановлення, як показано на Фіг. 2, буде завершена для нового клієнта. Безпека ID заперечує необхідність постійно передавати ідентифікаційну інформацію про клієнта 40 або пристрій клієнта 30 (обговорюється нижче) який, можливо, легше розпізнати третіми сторонами.

60 Таким чином інформація рахунку клієнта 40, збережена в системі установи 10, тримається

достатньо незалежно від авторизаційної системи 20.

Іншими словами, використання Безпека ID гарантує, що, якщо будь-яка авторизаційна система 20 і система установи 10 успішно атаковані і записи клієнта 40 доступні неуповноваженій стороні, це є мінімальна можливість для атакуючого отримати повний набір інформації, і особливо, ідентифікатори, потрібні для завершення транзакції, яка обговорюється в подальшому детально нижче.

Для того, щоб максимізувати безпеку комунікацій і інформації, що збережена в межах бази даних 24, віддається перевага, щоб Безпека ID не був видимий клієнту 40, або колл-центри для установи 50 або авторизаційна система 20.

Для того, щоб полегшити кореляцію переданих даних з даними, що збережені системою установи 10, Безпека ID, може корелювати в безпечній формі до існування унікального ідентифікатора, використовуючи систему установи 10, таку як наприклад, номер рахунку клієнта 40. Так само, Безпека ID, може корелювати в безпечній формі до унікального ідентифікатора в межах авторизаційної системи 20, який видимий колл-центрам і т.п.

Протягом процесу внесення даних клієнта в систему 20, Установа 50 передає Пристрій ID до системи 20. Система 20 контактує з клієнтом 40 (через пристрій 30) "мережевий". У цей момент клієнт 40 може слідувати необхідними кроками, щоб встановити як мінімум один Клієнт ID. Система 20 тоді звертається до Установи 30 Пристрій ID, і нового унікального безпечного ідентифікатора (Безпека ID). З того часу, єдиний ідентифікатор, що має відношення до клієнта 40 та/або пристрій 30, який знаходиться між Установою 50 і системою 20, є Безпека ID.

Тому, для шахрая, який прагне дістати неуповноважений доступ до повного набору даних, потрібен Суспільний ID клієнта 40, Пристрій ID і Клієнт ID. Щоб дістати всю цю інформацію, їм потрібно напасти і дістати неуповноважений доступ до системи Установи 10, слідує за транзакцією до авторизаційної системи 20 і атакувати зв'язок між системою 20 і пристроєм клієнта 30. Таким чином, в прикладі, встановленому в банківському контексті, неуповноваженому клієнтові потрібно атакувати і дістати неавторизований доступ до банку, авторизаційної системи 20 і мобільної телефонної мережі, на якій пристрій 30 з'єднаний.

У типовій фінансовій операційній ситуації, як показано на Фіг. 3, продавець або подібна організація посилає запит установі 50 для авторизації транзакції. У деяких випадках, коли таку авторизацію не запрошує продавець або коли транзакції внутрішні до установи 50, установа 50 може безпосередньо запитати авторизацію транзакції. Це - як цей пункт, що система установи 10 посилає авторизаційний запит 15 до авторизаційної системи 20, яка у свою чергу контактує з клієнтом 40 для авторизації транзакції.

Коли авторизаційна система 20 з'єднується з рядом установ та/або систем установ, авторизаційний запит 15, може включати унікальний ідентифікатор, щоб ідентифікувати установу 50, надалі Установа ID, яка пов'язана з авторизаційною системою 20 з авторизаційним запитом 15. У ситуаціях, наприклад, де установа 50 приймає авторизаційну систему 20, Установа ID, можливо, не є необхідною. Також, цінуватимуть, що Установа ID, може знаходитися в різних формах таких як інтернет-протокол (IP) або медіа контроль доступу (MAC) адрес сервера, або комбінація ідентифікаційних номерів та/або листів.

Клієнт 40 контактує з авторизаційною системою 20 на пристрої клієнта 30. Пристрій клієнта 30, можливо, є ручним пристроєм як наприклад мобільний телефон або особистий помічник даних (PDA), або портативний комп'ютер такий як ноутбук. Визначають, що клієнт 40 контактує на портативному пристрої, що несе клієнт 40, оскільки гарантують, що транзакції можуть бути авторизовані, як вимагалось і без непотрібної затримки.

Віддається перевага, щоб комунікація з пристроєм клієнта 30 проводилася за мережевою комунікаційною системою (тобто не інтернет або веб-заснованою технологією), особливо в ситуаціях коли транзакція безпосередньо була проведена через інтернет або веб-сторінку. Таким чином, навіть якщо сесія транзакції поставлена під загрозу, авторизаційний процес залишається безпечним, оскільки здійснюється за іншою системою зв'язку і тому навряд чи також поставлений під загрозу. Також, коли комунікаційна мережа, яка є такою ж, як те над чим транзакція проводиться, використовується, авторизаційний процес може проводитися над окремою сесією до сесії транзакції, або може безпосередньо впливати більше ніж комунікаційна сесія.

Для того, щоб встановити безпечну комунікаційну сесію між авторизаційною системою 20 і пристроєм клієнта 30, відповідні заходи безпеки прийняті. Точну природу цих заходів безпеки звичайно визначить вид пристрою, спосіб зв'язку, що використовувався та тип мережі.

Наприклад, у разі мобільного телефону GSM, 128-розрядний Кі в межах мобільної SIM використовується, як унікальний ідентифікаційний пристрій до мережі. 128-розрядний випадковий виклик (RAND) забезпечений мережею з пристроєм тоді, коли забезпечує 32-

розрядну відповідь (SRES). 64-розрядний ключ (Kc) обчислення створює підставу для кодування протягом сесії. Основні алгоритми включають A3 (ідентифікація), A5 (Кодування) і A8 (Генерація Ключа), і інші рівні безпеки, які потрібні.

У разі пристрою CDMA, електронний порядковий номер і А-ключ, що програмується в телефоні, використовують, щоб унікально ідентифікувати пристрій до мережі. Випадкове бінарне число (RANDSSD) генерується мережею з пристроєм, що відповідає з необхідним 128-розрядним субключем, звернувшись до Загальних Секретних Даних (SSD). Частина SSD використовується для ідентифікації, і частина для кодування, і основні алгоритми, можуть включати стандартну CAVE, CMEA, E-CMEA, або OYX у разі даних. На додаток до вищевикладеного, CDMA2000 і WCDMA можна використовувати, щоб застосувати додаткові рівні безпеки як наприклад SHA-1, AES, Kasumi і алгоритми Rijndael і AKA протокол.

У випадку, якщо Wi-Fi (802.11 базової технології), Bluetooth® і інший Біля Поля Комунікацій технології, також як і технології комунікацій великих відстаней, використовуються, щоб зв'язатися з пристроєм клієнта 30, переважно виконуються міцні методи безпеки, доступні з такими технологіями.

Для того, щоб ідентифікувати пристрій клієнта 30 до авторизаційної системи 20, унікальний ідентифікатор пристрою, надалі Пристрій ID, пристрою клієнта 30, можливо, порівнюється з Пристроєм ID, забезпеченим пристроєм клієнта 30. Приклади таких ідентифікаторів включають телефонний номер, Міжнародну Ідентичність Мобільного Устаткування (IMEI), яка є унікальним номером до кожного GSM і UMTS мобільного телефону, IP або MAC адреса, або будь-яка інша форма або комбінація, яка унікально ідентифікує пристрій клієнта 30 до авторизаційної системи 20.

Цінуватимуть, коли в декількох випадків, наприклад, де Пристрій ID включає телефонний номер, інформація там використовуватиметься, щоб також ініціювати зв'язок з пристроєм 30. Проте, де Пристрій ID складається тільки з ідентифікаційних пристроїв таких як MAC адреса, яка сама по собі не може використовуватися, щоб ініціювати зв'язок з пристроєм 30, додаткова контактна інформація для зв'язку з пристроєм 30 може бути також збережена системою 20.

Авторизаційна система 20 забезпечує процедуру, як показано на Фіг. 4, для заміни Пристрою ID, збереженого в базі даних 24, наприклад, якщо клієнт 40 отримує новий пристрій клієнта 30.

Для того, щоб авторизувати транзакції, клієнт 40 звертається до авторизаційної системи 20, щоб забезпечити як мінімум один унікальний ідентифікатор клієнта, надалі Клієнт ID, який використовується для того, щоб гарантувати актуальному клієнту схвалення транзакції, і не інша людина, яка просто, можливо, має доступ до пристрою клієнта 30. В ідеалі, Пристрій ID і Клієнт ID окремо безпечні і, можуть піддаватися процесам кодувань як наприклад випадкові дані протягом зберігання та/або комунікації.

Клієнт ID, можливо, є особистим ідентифікаційним номером (PIN) або паролем / пароль-фразою, який відомий клієнту 40, біометричним ідентифікатором як наприклад слід голосу, секретне слово, відбиток пальця, або будь-якою іншою формою ідентифікатора, який зазвичай тільки був би відомий, або доступний, клієнту 40.

У переважній формі, система інтерактивного розпізнавання голосу (IVR), тобто система IVR 28, може використовуватися як обидва нагадування клієнта 30 для Клієнт ID, так і згодом отримують Клієнт ID. IVR - комп'ютеризована система, яка дозволяє клієнту 40 вибрати опції з голосового меню і по-іншому взаємодіяти з авторизаційною системою 20. Загалом IVR система 28 програє заздалегідь записаний голос і клієнт 40 натискає номер на телефонній допоміжній клавіатурі, щоб вибрати опцію та/або каже відповідь, як наприклад Клієнт ID, який розпізнається IVR системою 28.

Наприклад, Клієнт ID, який включає 4 (або 6) цифри PIN, не відомий або збережений авторизаційною системою 20 в цифровій придатній до використання формі. Коли IVR система 28 отримує PIN через DTMF в межах сесії, пов'язаної з викликом, це кодується в сесії, використовуючи MD5, і, це - тільки ця мішанина кодованих MD5 послідовності, яка зв'язується з PIN, це повідомляється назад до авторизаційної системи 20 для затвердження або зберігання. Ця процедура гарантує, що малоімовірна подія того, що авторизаційна система 20 є атакованою, і нападаючий може порушити кодування, яке пов'язує Клієнт ID з Пристроєм ID, вони не зможуть симулювати виклик дозволу в спробі отримати PIN в придатній до вживання формі для IVR системи, якби тільки MD5 кодування було змінено. До того ж, додаткові рівні безпеки для даних можуть бути також додані, якщо потрібно, як наприклад технічні засоби кодувань.

У змінному втіленні, яке використовує біометричний голос, Клієнт ID формує слід голосу клієнта 40. Цей слід голосу, можливо, вичислюється проханням клієнта повторювати випадково

генероване слово або фразу як наприклад "Жовтий", яке дозволяє слід голосу клієнта 40 бути захопленим. Переважно, майбутній авторизаційний запит запитає клієнта 40, щоб сказати інше слово або фразу як наприклад "Вітторок" для збільшення безпеки.

Таким чином, авторизаційна система 20 визначає біометричний слід голосу для розпізнавання і порівнювання його із збереженими даними. Як інший рівень безпеки, система 20, може також перетворювати голос до конверсії тексту слова або фрази і проводить подальше порівняння із збереженими даними, щоб підтвердити, що розмовне слово - фактично одне записане. Таким чином, щоб бути зламаним, споживач, що потребує неуповноваженого доступу, потребував би не тільки високоякісний запис голосу клієнта, але також потрібно було б використовувати запис, щоб говорити випадкове запитуване слово.

У іншому альтернативному втіленні, система 20, може питати клієнта 40 питання, на яке він або вона, ймовірно, знають відповідь. Наприклад, система 20, може спитати, "Скільки була ваша остання транзакція?" або "Як Ваше ім'я по-батькові?" Відповідь клієнта 40 порівнюється не тільки з даними збереженого сліду голосу, але і точність відповіді також визначається.

Як тільки Клієнт ID забезпечений клієнтом 40, транзакція може розглядатися авторизаційною системою 20, як авторизована. Відповідно, авторизаційна система 20 повідомляє авторизацію транзакції системі установи 10, яка у свою чергу дозволить установі 50 прийняти відповідні заходи, щоб завершити транзакцію.

Авторизаційна система 20 забезпечує процедуру, як показано на Фіг. 5, для заміни Клієнт ID, збереженого в базі даних 24, наприклад, якщо клієнт 40 потребує змінити його або її пароль, PIN і т.п.

У певних ситуаціях, клієнту 40, можливо, потрібно забезпечити відповідь до авторизаційної системи 20, або замість будь-чого, або на додаток до Клієнт ID. Ця відповідь, можливо, використовується, щоб повідомити запит, щоб відмінити транзакцію або сигналізувати транзакцію, як обману, наприклад. У таких ситуаціях, авторизаційна система 20 повідомляє факт, що транзакція, можливо, обманна до системи установи 10, яка у свою чергу дозволить установі 50 прийняти відповідні заходи для припинення транзакції і зупинить переказ грошей.

Віддається перевага, щоб Клієнт ID і Пристрій ID збережені авторизаційною системою 20 у спосіб, що відокремлює їх, наприклад використанням кодованого алгоритму. Це повинно гарантувати, що в малоімовірній події атака авторизаційної системи була успішною; нападаючий не міг корелювати Клієнт ID і Пристрій ID, і згодом імітував авторизацію обманної транзакції. У одній формі Клієнт ID збережений окремо в потрібній брендмауер підмножині в межах авторизаційної системи 20 навколишнього середовища.

Також переважно, щоб Клієнт ID не зберігався або копіювався де-небудь у іншому місці протягом процесу авторизації транзакції. Це, можливо, вимагає допомоги передачі в IVR системі 28 в протилежність зберігання і способу підтвердження.

Згідно втіленню, якому особливо віддається перевага, віддалена система оплати 100, об'єднуючи авторизаційну систему 20 забезпечена.

Функціональність і використання одного виконання системи 100 ілюструється на Фігурах 6-13. Віддалена система оплати 100 дозволяє клієнту 40 проводити оплати за товари і послуги віддалено в безпечній формі з членами 60 системи 100. Переважне виконання системи 100, згідно якому використання системи 100 ілюструється на Фігурах 6-13, включає як мінімум одне зберігання даних 70 для змісту оновлюваних даних, що мають відношення до кожного клієнта 40, і кожен член 60 системи 100, там, де кожен клієнт 40 має як мінімум один зв'язаний реєстраційний профіль 80 із пов'язаним грошовим сховищем 90. Система 100 також включає структуру обробки даних 110 маючи як мінімум одну обробку даних 120 і система розрахункового центру 125 для врегулювання заборгованості між членами 60 і клієнтами 40 системи 100, як мінімум однієї комунікації 130 пов'язаної з структурою обробки даних 110 для зв'язку з клієнтом 40, і як мінімум один віддалений комунікаційний пристрій 30, який має кожен клієнт 40 для зв'язку із засобами зв'язку 130.

Клієнт 40 використовує систему 100, щоб проводити платежі 140 для товарів або послуг згідно з запитом оплати 150, запит оплати 150 запускає комунікаційну подію 165 від, як мінімум, одного засобу зв'язку 130 до, як мінімум, одного віддаленого комунікаційного пристрою 30 з метою підтвердження ідентичності клієнта 40 і доступу до відповідного реєстраційного профілю 80, і як тільки ідентичність клієнта 40 була затверджена, дозволено клієнту 40 проводити платежі 140 забезпечивши позитивний баланс, що залишається в грошовому сховищі 90.

Зазвичай будуть як мінімум дві категорії членства системи, а саме юридичні особи 60 і фізичні особи 40. Зазвичай буде множинність членів в кожній категорії членства. Членство категорії юридичних осіб 60, можливо, управляється строго та/або обмежується адміністратором системи 160. Членство категорії фізичних осіб 40, можливо, забезпечено після

прикладного процесу, який, можливо, підлягає затвердженню адміністратором 160. Важливо, що юридичні особи 60 системи 100, можливо, є фізичними особами 40 системи 100 також.

Адміністратор системи 160 зазвичай запропонує членство юридичним особам 60 і фізичним особам. Членство, можливо, вимагає підписи. Юридичні особи 60, можливо, загалом платять річний підписний грошовий збір, який дозволяє їм доступ до системи 100. Юридичні особи 60, можливо, забезпечені унікальним ідентифікаційним номером і паролем для ідентифікаційних потреб. Юридичні особи 60 можуть отримувати регулярні бюлетені і поновлюватися системою 100, як результати аналізу даних перетворених в інформацію, пов'язану з системою 100. Ці бюлетені мають бути підготовлені адміністратором системи 160. Зазвичай, інформація як така матиме відношення до програми і його вигод, рекламуючи програму або щось подібне. Адміністратор системи 160 може компіювати базу даних 170, що містить деталі юридичних осіб 60 і будь-яку іншу інформацію або статистику, яку адміністратор системи 160 бажає.

Юридична особа 60 може зібрати та/або поновити інформацію програмою фізичних осіб 40, що використовує систему 100 для сплати за товари або послуги юридичних осіб 60. Ця інформація, можливо, повідомлена адміністраторові системи 160 і, можливо, збережена в базі даних клієнта 70.

Можливо, переважно є дві частини або сектори системи. Дві частини системи, можливо, переважно відомі, як клієнтська частина системи і сервер баз даних. Клієнтська частина системи, можливо, переважно охоплює інтерфейс користувача. Інтерфейс користувача дозволяє передплатникові або адміністраторові бази даних мати доступ або з'єднатися із сервером баз даних системи 100. Клієнтська частина системи або інтерфейс користувача може переважно бути розміщений або доступний, використовуючи Інтернет браузер або мобільний телефон, PDA або інший персональний пристрій з можливістю зв'язку. Альтернативно інтерфейс користувача, можливо, розміщується на комп'ютері або сервері або мережі комп'ютерів або серверів. Це, можливо, є будь-який відповідний тип або конфігурація.

Сервер баз даних системи 100 може переважно включати як мінімум одне сховище даних, що означає зазвичай множинність баз даних. Як мінімум одна з баз даних може, переважно, бути клієнтською базою даних 70, містячи інформацію про фізичних осіб 40 і пов'язаний з ними грошовий реєстр 90, і друга база даних може, переважно, бути базою даних юридичних осіб 170, містячи інформацію про юридичних осіб 60 і їх рахунки 180. Доступ до кожної з баз даних через інтерфейс користувача може, переважно, диференціюватися залежно від доступу або деталей логінів. Наприклад доступ фізичним особам 40 може дозволяти тільки часткові або обмежені функції для виконання, які, можливо, обмежуються до деякої міри до доступу, наданого фізичним особам 40, але з такою же або різною функціональністю, тоді як доступ адміністратором системи 160 може надати статус "суперкористувача" і дозволити доступ до всіх частин системи 100 і всіх функцій системи 100.

Зазвичай, потенційний член може контактувати з адміністратором системи 160 для того, щоб підписатися на систему 100. Адміністратор системи може відповідно забезпечити члена унікальним ім'ям користувача і паролем, щоб дозволити доступ до системи. Член може, переважно, платити адміністратору системи 160 передплатний грошовий збір для того, щоб отримати доступ до системи 100 протягом зазначеного періоду часу. Ім'я користувача і пароль можуть включати Особистий Ідентифікаційний Номер, номер рахунку, або ім'я користувача може бути пов'язане з ідентифікаційними характеристиками віддалених засобів зв'язків, що використовуються з ідентифікаційними характеристиками специфічних віддалених засобів зв'язків, які використовуються фізичними особами 40, може відрізнятися згідно виду пристрою 30, який використовується. Наприклад, комп'ютери, що використовують негнучкі інтернет-з'єднання, можуть використовувати засоби ID як, наприклад, технологія Ідентифікації Абонентської Лінії (CLI), послуги мобільної телефонії, які можуть дозволити ідентифікаційні характеристики SIM-картки використовувати і прямий інтернет-доступ до інтерфейсу мережеву адресу або адресу Інтернет-протоколу, що переважно підтверджується через постачальника послуг, як ім'я користувача.

Згадане вище обговорення засноване навколо мобільної телефонії або обчислювального пристрою. Система 100 може також використовуватися через Інтернет наприклад. На відкритті обумовленої веб-сторінки, клієнт 40 може, відповідно, швидко ввести його ім'я користувача і пароль для того, щоб отримати доступ до системи 100. Правильний вхід клієнта 40 імені користувача і супровідний пароль можуть переважно дозволити доступ до системи 100 як клієнту 40.

Використання системи 100 юридичними особами 60, можливо, злегка відмінне від того, що використовують фізичні особи 40. Юридичні особи 60 переважно використовуватимуть систему 100, щоб повідомити фізичних осіб 40 про розгляд запитів оплат 150 і, щоб контролювати

баланс їх власного рахунку 180. Система 100 може також дозволяти юридичним особам 60 проводити бухгалтерський облік статистичних записів з інформації системи 100.

Використання системи 100 адміністратором системи 160 може також, переважно, надати доступ через інтерфейс користувача клієнтської частини системи. До деякої міри подібно введенням клієнтом 40 їх імені користувача і пароля, адміністратор 160 може також мати ім'я користувача і пароль, введення яких може, відповідно, дозволяти широкий необмежений доступ до системи 100, ніж це дозволено клієнтові 40.

Правильне введення адміністратором 160 імені користувача і супровідного паролю може, переважно, дозволити доступ до системи 100, як адміністратору бази даних. Адміністратор 160 переважно матиме здатність підтримувати систему 100, включаючи виправлення реєстраційних профілів клієнта 80 і віртуальні гаманці 90, щоб виправити помилки, а також генерувати звіти від системи 100.

Клієнти 40 можуть мати опцію для відновлення їх ідентифікаційних деталей або контактних деталей через, наприклад, веб-інтерфейс. На етапі вибору опції, щоб змінити деталі клієнта 40, доступна для редагування форма переважно показана, дозволяючи клієнту 40 редагувати їх деталі рахунків. Це може дозволити модифікацію деталей таких як ім'я користувача, пароль, контактне ім'я і деталі адреси, включаючи телекомунікаційні номери, електронну пошту і адресу веб-сайту клієнта. Зміна ідентифікаційної інформації в цій формі зазвичай запустить підтверджувальний процес, який здійснюватиметься знову.

Специфічні переважні особливості системи 100 більш легко описані з відношенням до системи 100 фізичною особою 40 або юридичною особою 60, або адміністратором 160.

Перший крок в системі 100 загалом має бути встановити реєстраційний профіль 80 нового клієнта 40. Події, які можуть ініціювати Нову Реєстрацію Клієнта разом з процесом, якому віддається перевага, для роботи з подіями, ідентифікуються на Фігурі 7. Клієнтську частину системи можна, переважно, досягнути, використовуючи інтернет-браузер, щоб відвідати обумовлену адресу веб-сайту. Це, можливо, виконується або клієнтом 40 безпосередньо, використовуючи інтернет-інтерфейс, або контактуючи з офіцером обслуговування клієнтів (CSO) системи 100 іншими засобами і CSO використовує інтернет-інтерфейс, щоб увійти до деталей клієнта 40, які потрібні для початкового підтвердження клієнта 40. Виконання фактичного процесу Нової Реєстрації Клієнта ілюструється на Фігурі 8.

На виборі опції, щоб увійти до деталей клієнта 40, доступна для редагування форма переважно показана, дозволяючи клієнту 40 (або CSO) увійти (або редагувати) їх підписні деталі або деталі рахунків. Це може дозволити модифікацію деталей таких як ім'я користувача, пароль, контактне ім'я і деталі адрес, включаючи телекомунікаційні номери, електронну пошту і адресу веб-сайту клієнта 40. Це може також включати інші другорядні дані такі як дата народження, посилання і банківські деталі. Якщо будь-яка введена ідентифікаційна інформація вже у використанні або частина інформації відсутня, підказка, можливо, запущена, щоб запитати інформацію або виправлення інформації.

Як тільки ідентифікаційна інформація клієнта 40 підтверджена первинною процедурою підтвердження, якій віддавалася перевага, введена інформація, можливо, використовується, щоб створити реєстраційний профіль 80 клієнту 40 і грошове сховище або "віртуальний гаманець" 90. Гроші для використання в системі 100 справжнього винаходу зазвичай переказуються в віртуальний гаманець 90 клієнта 40. Переказ грошей, можливо, є з дебетового рахунку 210 з постачальником встановлених фінансових послуг 190 таких як банк, соціальне підприємство або інший або від кредиту, запропонованого постачальником 190. Переважно, в цій стадії, джерело, якому віддається перевага, для переказу, можливо, пропонується клієнтом 40, але не обробляється.

Це, можливо, слідує друга процедура ідентифікації зазвичай, слідує за вторинною процедурою перевірки адміністратором системи 160 також як і більш довершена перевірка інформації, що забезпечена, яка, можливо, вимагає підтвердження від незалежних частин адміністратора системи 160.

Одного разу клієнт 40 радить системі 100 джерела, якому віддається перевага, для переказу, клієнта 40 можуть попросити слідувати за ідентифікаційною процедурою, щоб засвідчити їх ідентичність, підтвердження доступу до системи 100 і до джерела рахунку 210 для переказу або подібну. Виконання ідентифікаційного процесу, якому віддається перевага, ілюстроване на Фігурі 9.

Ідентифікаційна процедура може включати структуру обробки даних 110, створюючи швидку ідентифікацію і повідомляючи ідентифікацію як мінімум одному засобу зв'язку 130, який пов'язаний з структурою обробки даних 110.

Підтвердження і авторизація для оплати 200 виконується, використовуючи ідентифікаційну

систему 20 описану раніше. Знову, як тільки ідентифікація надана або відхилена, відповідне повідомлення, що радить клієнтові 40 з результату ідентифікаційного процесу переважно генерувати структуру обробки даних 110, і пересилається віддаленому комунікаційному пристрою 30, якому надає перевагу клієнт 40, через, як мінімум, один засіб зв'язку 130, пов'язаний з структурою обробки даних 110.

Якщо ідентифікаційний процес успішний, оплату 200 записує система 100 і віртуальний гаманець 90 клієнта 40 відновлюється, щоб дати звіт про оплату 200 і, щоб точно відобразити фонди, доступні клієнту 40 через систему 100.

Виконанні грошові перекази додаються до їх віртуального гаманця 90 або запит балансу або інші типи транзакцій також зазвичай будуть можливі. Кожна транзакція зазвичай підлягатиме ідентифікаційному процесу, що включає контакт клієнта 40 з системою 100 і запит для підтвердження інформації.

Як тільки ідентичність клієнта 40 була підтверджена, клієнт 40 зазвичай буде вимушений переказати стартові фонди в їх віртуальний гаманець 90 для використання під системою 110. В даному випадку, клієнт 40 зазвичай слідуватиме за першою процедурою депозиту, виконання якої, переважно, ілюструється на Фігурі 10. Переказ грошей може по-різному залежати від того, чи клієнт 40 використовує дебет або кредит. Якщо кредит використовується, система 100, можливо, функціонує в реальному часі на підставі, зчитуючи інформацію кредитної картки і обробляючи оплату кредитної картки за запитом, тоді як, якщо дебет використовується, клієнт 40, можливо, переказує гроші в їх віртуальний гаманець 90 для негайного використання або пізніше.

Слідуючи підказці, щоб переказати стартові фонди, система 100 все ще використовує IVR компонент 28 і загалом на тому ж контакті, як ідентифікаційний контакт, просить, щоб клієнт 40 вказав кількість грошей, які треба переказати. Система може потім обробити цей запит з назначеною фінансовою установою 190 клієнта 40 і рахунок і видати успішне/невдале повідомлення клієнтові 40. Контакт клієнта 40 з IVR компонентом 28, можливо, закінчується в цій стадії або система 100 може запитати, чи повинна будь-яка подальша діяльність бути виконана клієнтом 40. Якщо переказ успішний, оплата 200 записується системою 100 і віртуальний гаманець 90 клієнта 40 відновлюється, щоб дати звіт про оплату 200 і, щоб точно відобразити фонди, доступні клієнтові 40 через систему 100.

Зазвичай, для балансування оброблювального завантаження на системі 100, транзакції клієнта 40 і відновлення до відповідних віртуальних гаманців 90, можливо, проводиться в реальному часі, але оновлення переказу грошей до юридичних осіб 60 системи 100 може відбуватися за періоди тимчасового затишшя в системі 100. Оновлення переказів грошей до юридичних осіб 60 може відбуватися в об'ємі "струмені" в якому єдину кількість, можливо, переказують до юридичних осіб 60 з відповідною інформацією, щоб ідентифікувати платників клієнтів 40. Вибір часу періодів тимчасового затишшя може відбуватися в специфічний час кожен період, зазвичай кожен день, або система 100, можливо, сама контролює процес переказів до юридичних осіб 60, коли іде обробка переказів клієнта 40.

В залежності від результату першої процедури депозиту, реєстраційний профіль 80 і особливіше, віртуальний гаманець 90 клієнта 40, можливо, "завантажується" з входом, вказуючи значення фондів, переказаних з початкового рахунку 210 в віртуальний гаманець 90 клієнта 40, який може тоді використовуватися клієнтом 40, щоб проводити оплати 140 юридичних осіб 60 системи 100 у будь-який час.

Виконання процесу оплати, якому віддається перевага, ілюструється на Фігурі 11. Для того, щоб проводити оплату 140, використовуючи систему, запит оплати 150 зазвичай проводитиметься через інтерфейс системи 100 юридичним особам 60 (дія "тяги"), фізичним особам 40 (дія "поштовху") або іншими засобами і запит оплати 150 переважно буде позначений і пов'язаний із специфічним реєстраційним профілем 80 клієнта 40. Фізична особа 40 також буде повідомлена про попередній запит оплати 150 або юридичною особою 60 безпосередньо, або самою системою 100.

Як тільки запит оплати 150 був проведений, клієнт 40 указує, що оплата 140 використовуючи систему 100 повинна виконуватися, нормально контактуючи із засобами зв'язку 130, які пов'язані з структурою обробки даних 120. Структура обробки даних 120 тоді зазвичай перевіряє деталі запиту оплати 150 і може, також перевірити ідентичність клієнта 40 і доступність фондів у віртуальному гаманці 90 клієнта, а потім слідує підказка до засобів зв'язку 130, щоб контактувати з клієнтом 40 для підтвердження або авторизації для оплати 140.

Знову, підтвердження і авторизація для оплати 140 виконується, використовуючи блок-схему авторизаційної системи 20 раніше. Як тільки ідентифікація надана або відхилена, відповідне повідомлення радить клієнтові 40 результат ідентифікаційного процесу переважно

проводити структурою обробки даних 120, і передати до віддаленого комунікаційного пристрою 30, якому надає перевагу клієнт, через, як мінімум, один засіб зв'язку 130, який пов'язаний з структурою обробки даних 120.

5 Якщо ідентифікаційний процес успішний, оплата 140 записується системою 100 і віртуальний гаманець 90 клієнта 40 відновлюється, щоб дати звіт про оплату 140 і, щоб точно відобразити фонди, доступні клієнтові 40 через систему 100.

10 Виконанні грошові перекази додаються до їх віртуального гаманця 90 (виконання цього процесу, якому віддається перевага, ілюструється на Фігурі 12) або запит балансу (виконання цього процесу, якому віддається перевага, ілюструється на Фігурі 13) або інші типи транзакцій також зазвичай будуть можливі. Кожна транзакція зазвичай підлягатиме ідентифікаційному процесу, використовуючи авторизаційну систему 20, включаючи контакт клієнта з системою 100 і запит для підтвердження інформації.

15 У даному описі і формулі винаходу (якщо є), слово "охоплюючий" і його похідні слова включаючи "охоплює" і "охоплюють" включають кожне із встановлених цілих чисел, але не виключає включення одного або більше подальших цілих чисел.

20 Посилання всюди в цьому описі до "одного втілення" або "втілення" означає, що специфічна особливість, структура, або характеристика, описана у зв'язку з втіленням, яке входить, як мінімум, в одне втілення справжнього винаходу. Тому, поява фраз "в одному втіленні" або "у втіленні" в різних місцях всюди в цьому описі необов'язково є всіма посиланнями на таке ж втілення. До того ж, специфічні особливості, структури, або характеристики, можливо, комбінуються в будь-якій відповідній формі в одній або більше комбінаціях.

25 Вищевикладене обговорення розглядається, як ілюстрація тільки принципів винаходу. До того ж, з тих пір, як численні модифікації і зміни з готовністю відбуватимуться до тих навичок в галузі техніки, не бажано обмежувати винахід точною побудовою і дією, показаною і описаною, і відповідно, всі відповідні модифікації і еквіваленти, можливо, пересорттовані, випадаючи в межах контексту винаходу.

#### ФОРМУЛА ВИНАХОДУ

30 1. Система авторизації транзакції, яка дозволяє клієнту авторизувати транзакції відносно як мінімум одного рахунку клієнта, пов'язаного з установою, де рахунок включає ідентифікаційні дані рахунку, які зберігаються в установі, причому система включає в себе:

засоби зберігання даних для можливості доступу до

35 (а) ідентифікаційних даних, пов'язаних з клієнтом,

(b) ідентифікаційних даних, пов'язаних з віддаленим комунікаційним пристроєм (RCD) клієнта, та

40 (с) даних ідентифікатора безпеки, які відомі тільки системі установи та системі авторизації, та відрізняються від ідентифікаційних даних рахунку, які зберігаються в установі, де дані ідентифікатора безпеки, пов'язані з як мінімум одним рахунком клієнта з будь-яким одним або обома з (а) та (b),

засоби першої комунікації для можливості зв'язатися з клієнтом через RCD, щоб авторизувати транзакцію як мінімум одного рахунку клієнта, де RCD ідентифікується через ідентифікаційні дані, що зберігаються в засобах зберігання даних,

45 структуру обробки даних, яка включає засоби обробки даних для того, щоб ідентифікувати клієнта, використовуючи ідентифікаційні дані (а), що зберігаються в засобах зберігання даних, ідентифікувати RCD, використовуючи ідентифікаційні дані (b), що зберігаються в засобах зберігання даних, та визначити, якщо транзакція авторизована клієнтом, та

50 засоби другої комунікації в комунікації з структурою обробки даних, для отримання авторизаційного запиту відносно до транзакції та надавання вказівки установі авторизована чи ні транзакція клієнтом,

там, де авторизаційний запит отриманий і вказівка надана установі, ідентифікуються між собою з використанням даних ідентифікатора безпеки.

2. Система авторизації транзакції за п. 1, де дані ідентифікатора безпеки не повідомлені клієнту.

55 3. Система авторизації транзакції за п. 2, де дані ідентифікатора безпеки не такі як, також не одержані з характеристик особистої інформації, пов'язаної з клієнтом.

4. Система авторизації транзакції за п. 1, де засоби першої комунікації дають можливість зв'язатися з клієнтом через RCD, використовуючи засіб зв'язку, який відмінний від засобів зв'язку, які супроводжують транзакцію.

60 5. Система авторизації транзакції за п. 1, де засоби першої комунікації дають можливість зв'язатися з клієнтом через RCD, використовуючи дві або більше комунікаційних сесій.



6. Система авторизації транзакції за п. 1, де (а) включає один або більше ПІНів, паролів, фраз-паролів або біометричних даних.

7. Система авторизації транзакції за п. 1, де клієнт ідентифікується за допомогою порівнювання (а) з голосовим відбитком або голосовими біометричними даними, одержаними від дослівної відповіді клієнта з випадковим словом, фразою та/або запитом для інформації, наданої системою, та порівнювання дослівної відповіді клієнта з випадково створеним словом або фразою та/або інформацією, доступною для системи.

8. Система авторизації транзакції за п. 1, де (b) включає один або більше телефонних номерів, Міжнародних Мобільних Ідентифікаторів Обладнання (IMEI), адрес Інтернет Протоколів (IP), або адрес Контролю Медіа Доступу (MAC).

9. Система авторизації транзакції за п. 1, де засоби першої комунікації дозволяють клієнтові вказати, якщо транзакція як мінімум одного рахунку клієнта не вірна, засоби оброблення даних визначають, якщо вказана транзакція була надана невірно клієнтом, та засоби другої комунікації забезпечують вказівку установі чи транзакція була вказана невірно клієнтом.

10. Система авторизації транзакції за п. 1, де засоби першої комунікації включають в себе систему інтерактивного розпізнавання голосу (IVR).

11. Система авторизації транзакції за п. 10, де IVR система забезпечує клієнта як мінімум опціями авторизації транзакцій, відміни транзакції або вказування на те, що транзакція невірна.

12. Система авторизації транзакції за п. 1, де засоби зберігання даних далі можуть надати доступ до контактної інформації RCD для використання засобів першої комунікації для можливості зв'язатися з клієнтом через RCD.

13. Спосіб, який дозволяє клієнту авторизувати транзакції відносно як мінімум одного рахунку клієнта, який тримається в установі, де рахунок включає ідентифікаційні дані рахунку, які зберігаються в установі, причому спосіб включає етапи:

a) авторизаційний сервер отримує авторизаційний запит від установи відносно транзакції як мінімум одного рахунку клієнта,

b) авторизаційний сервер зв'язується з клієнтом через віддалений комунікаційний пристрій (RCD) клієнта для авторизації транзакції,

c) авторизаційний сервер ідентифікує клієнта, використовуючи ідентифікаційні дані, які пов'язані з клієнтом, до яких авторизаційний сервер має доступ,

d) авторизаційний сервер ідентифікує RCD, використовуючи збережені ідентифікаційні дані, які пов'язані з RCD, до яких авторизаційний сервер має доступ,

e) авторизаційний сервер визначає чи авторизована транзакція клієнтом,

f) авторизаційний сервер передає вказівку установі авторизована чи ні транзакція клієнтом, де авторизаційний запит отриманий авторизаційним сервером та вказівка надана установі ідентифікується установою та ідентифікаційним сервером з використанням даних ідентифікатора безпеки для зв'язку як мінімум одного рахунку клієнта з одним або обома збереженими ідентифікаційними даними, пов'язаними з клієнтом і збереженими ідентифікаційними даними, які пов'язані з RCD, де дані ідентифікатора безпеки відомі тільки авторизаційному серверу та установі, та де дані ідентифікатора безпеки відрізняються від ідентифікаційних даних рахунку.

14. Спосіб авторизації транзакції за п. 13, де дані ідентифікатора безпеки не повідомлені клієнту.

15. Спосіб авторизації транзакції за п. 13, де дані ідентифікатора безпеки не такі як, також не одержані з характеристик особистої інформації, пов'язаної з клієнтом.

16. Спосіб авторизації транзакції за п. 13, де зв'язок з клієнтом через RCD використовує засіб комунікації, який відмінний від засобу комунікацій, що використовується для того, щоб проводити транзакцію.

17. Спосіб авторизації транзакції за п. 13, де зв'язок з клієнтом через RCD використовує дві або більше комунікаційних сесій.

18. Спосіб авторизації транзакції за п. 13, де збережені ідентифікаційні дані, які пов'язані з клієнтом, включають один або більше ПІНів, паролів, фраз-паролів або біометричних даних.

19. Спосіб авторизації транзакції за п. 13, де крок (с) включає стадії

i) авторизаційний сервер порівнює ідентифікаційні дані, пов'язані з клієнтом, з голосовим відбитком або голосовими біометричними даними, одержаними від дослівної відповіді клієнта з випадковим словом, фразою та/або запитом для інформації, наданої авторизаційним сервером, та

ii) авторизаційний сервер порівнює дослівну відповідь клієнта з випадково створеним словом або фразою та/або інформацією, доступною для авторизаційного сервера.

20. Спосіб авторизації транзакції за п. 13, де збережені ідентифікаційні дані, які пов'язані з RCD, включають один або більше телефонних номерів, Міжнародних Мобільних Ідентифікаторів Обладнання (IMEI), адрес Інтернет Протоколів (IP), або адрес Контролю Медіа Доступу (MAC).

21. Спосіб авторизації транзакції за п. 13, де авторизаційний сервер визначає, якщо транзакція як мінімум одного рахунку клієнта була вказана невірно клієнтом, та передає вказівку установі чи транзакція була вказана невірно клієнтом.

22. Спосіб авторизації транзакції за п. 13, де зв'язок з клієнтом через RCD включає використання системи інтерактивного розпізнавання голосу (IVR).

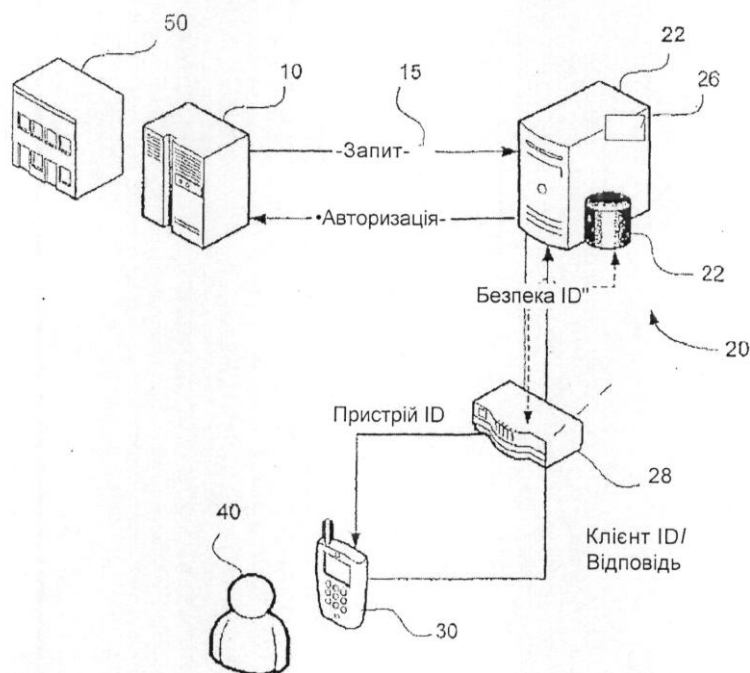
23. Спосіб авторизації транзакції за п. 22, де IVR система забезпечує клієнта як мінімум опціями авторизації транзакцій, відміни транзакції або вказування на те, що транзакція не вірна.

24. Спосіб авторизації транзакції за п. 13, де зв'язок з клієнтом через RCD можливий використовуючи збережену контактну інформацію RCD.

25. Система віддалених оплат, яка дозволяє клієнту проводити платежі за товари і послуги віддалено у безпечній формі з членами системи, включає в себе систему авторизації транзакції або спосіб відповідно до будь-якого з пп. 1-24.

26. Система авторизації транзакцій відповідно до будь-якого з пп. 1-12 для використання в контексті підтвердження транзакцій кредитних карток.

27. Спосіб авторизації транзакції відповідно до будь-якого з пп. 13-24 для використання в контексті підтвердження транзакцій кредитних карток.



Фіг. 1

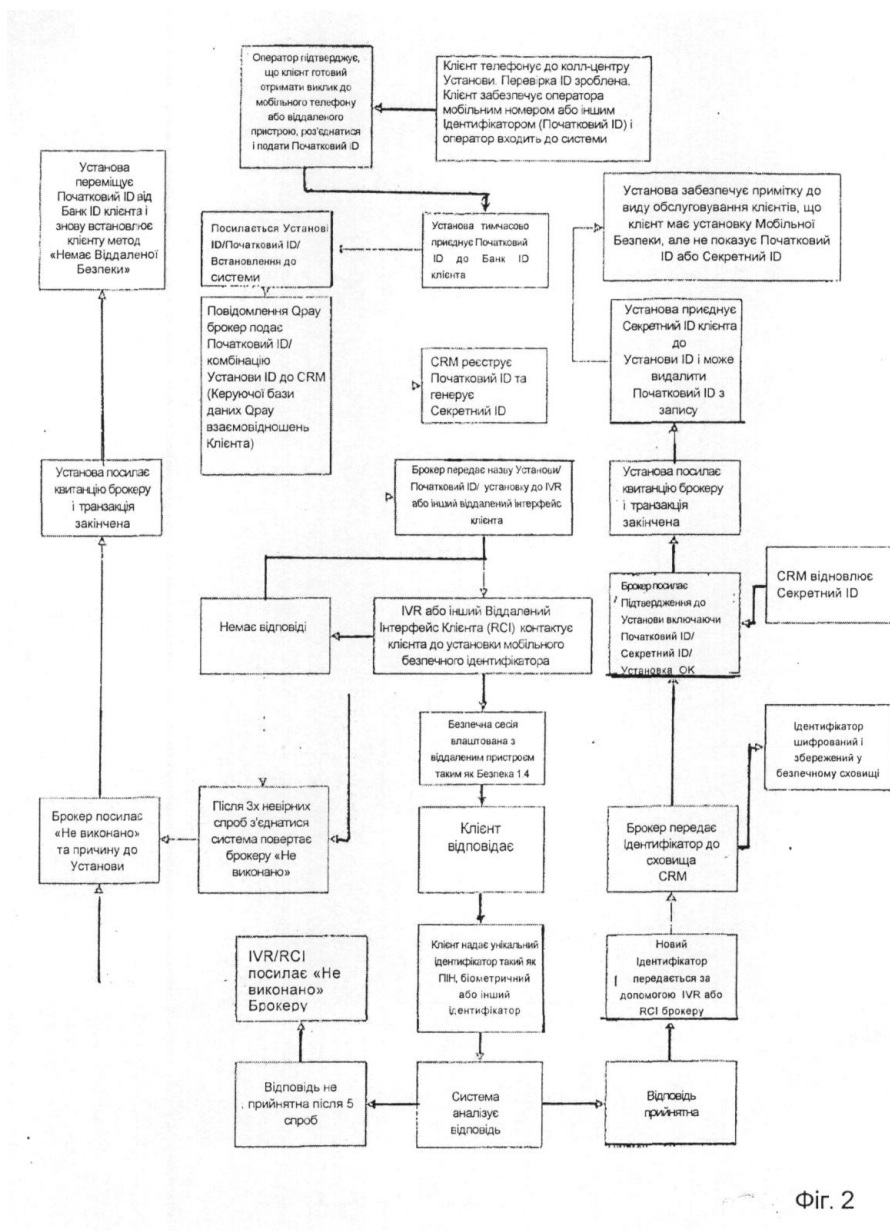


Fig. 2

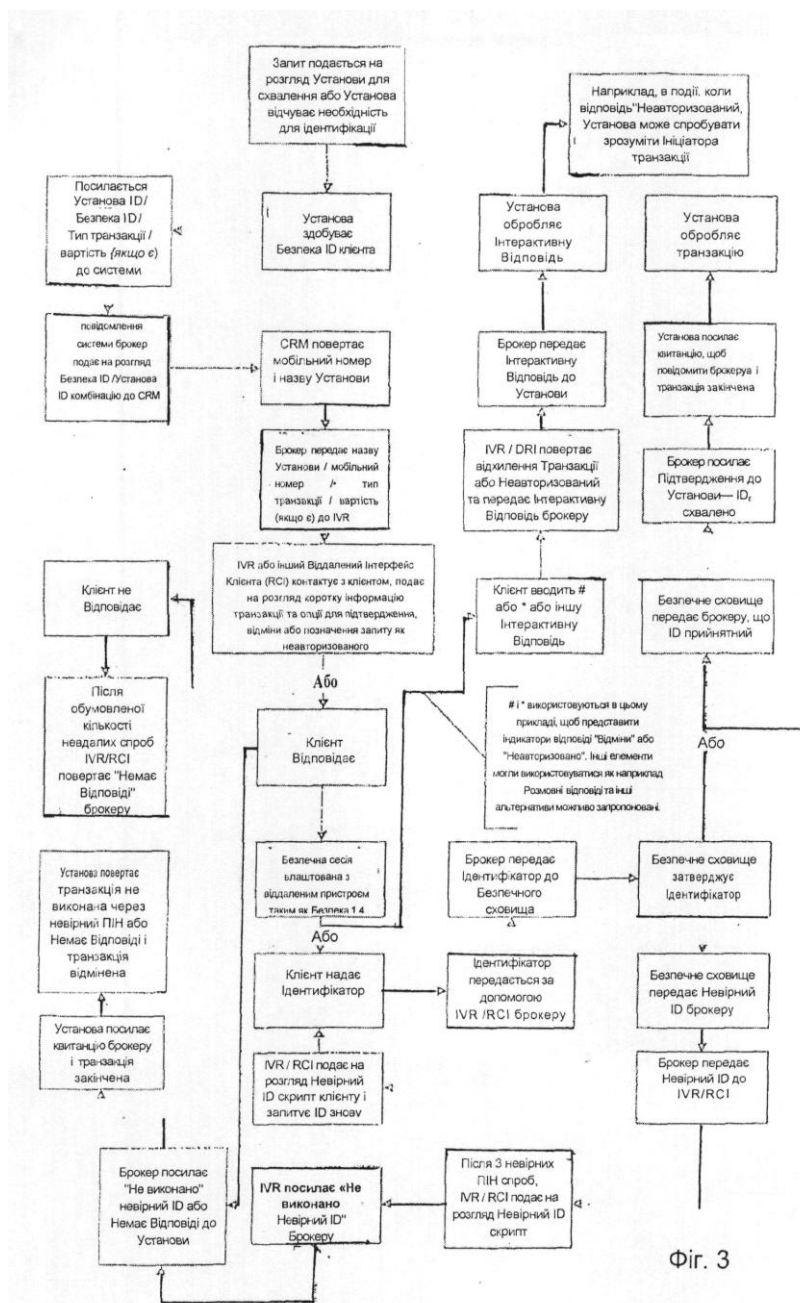
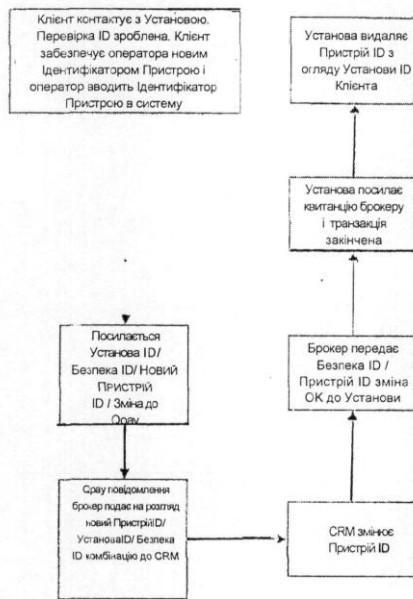


Fig. 3



Фіг. 4

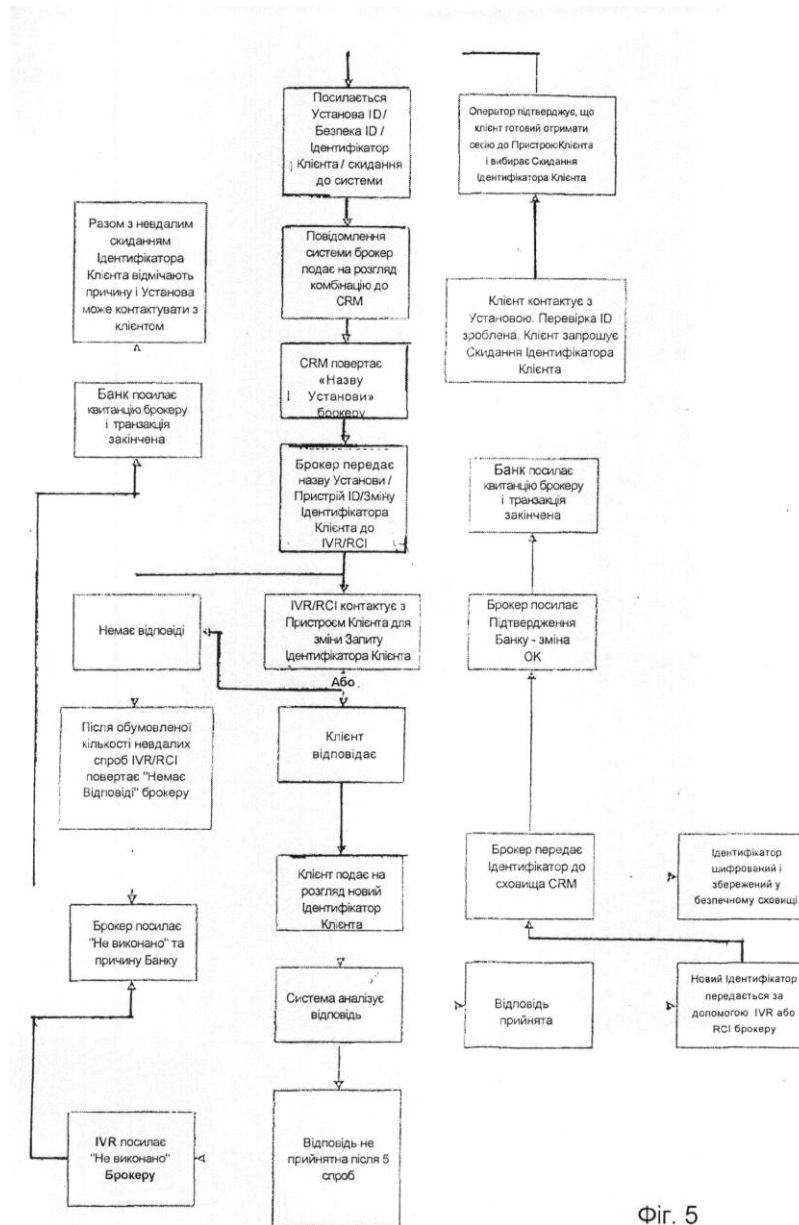


Fig. 5

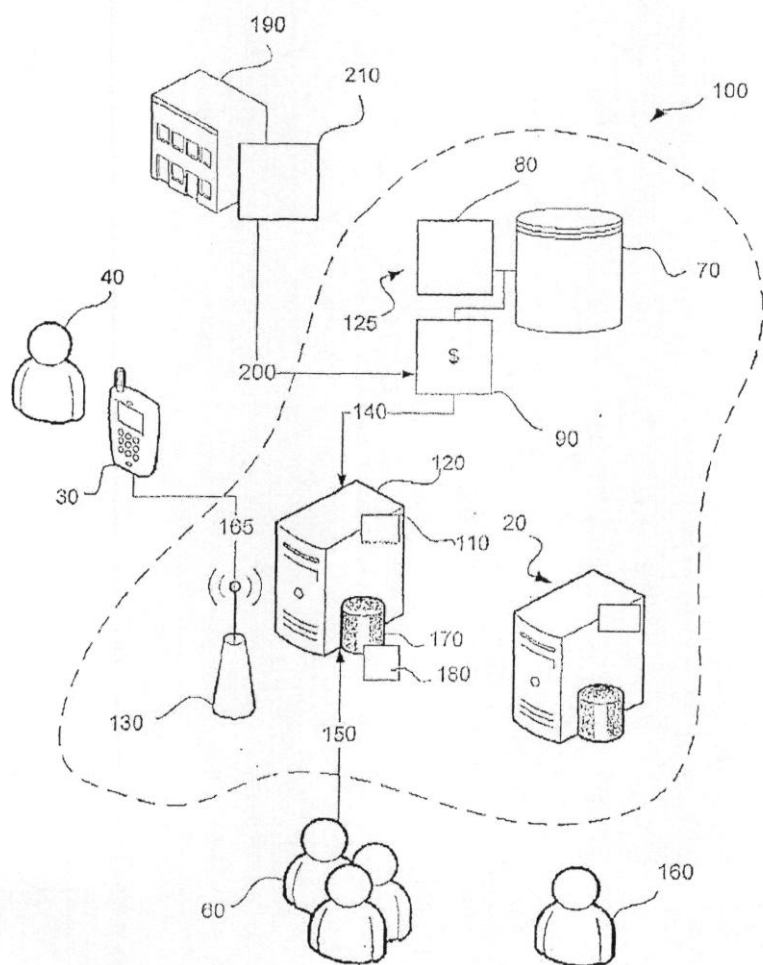
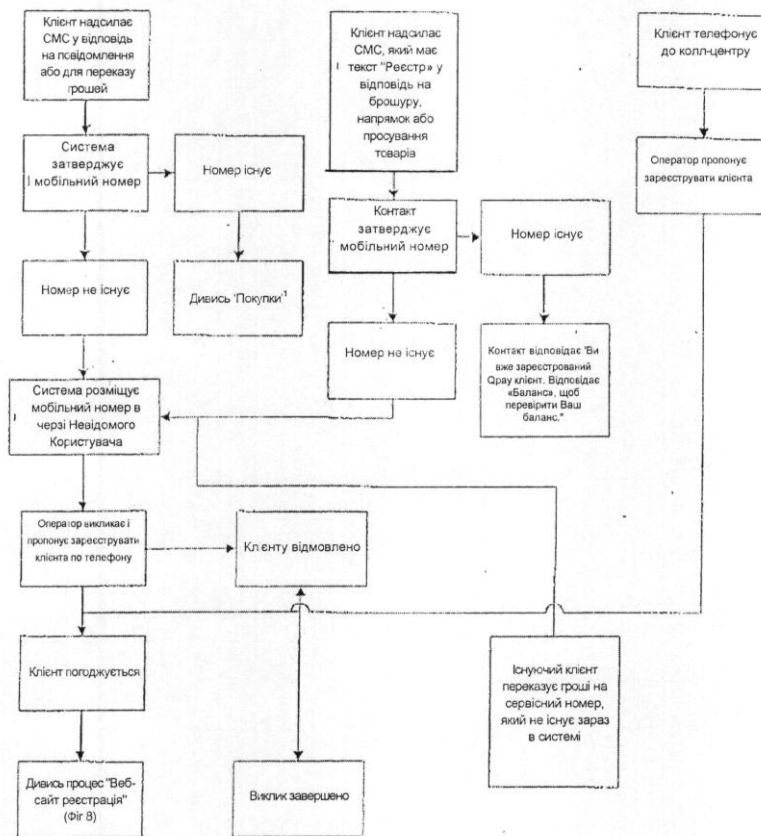


Fig. 6



Фіг. 7



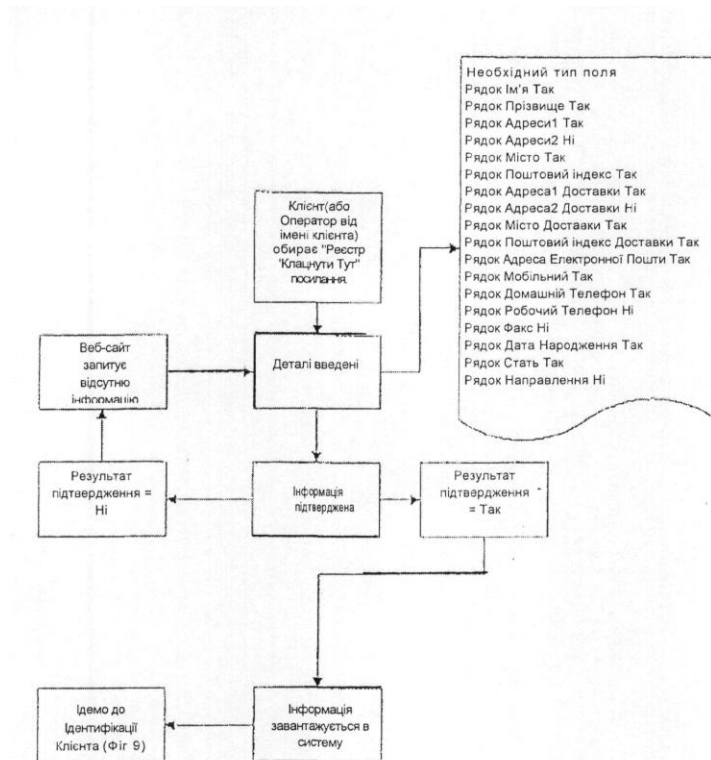
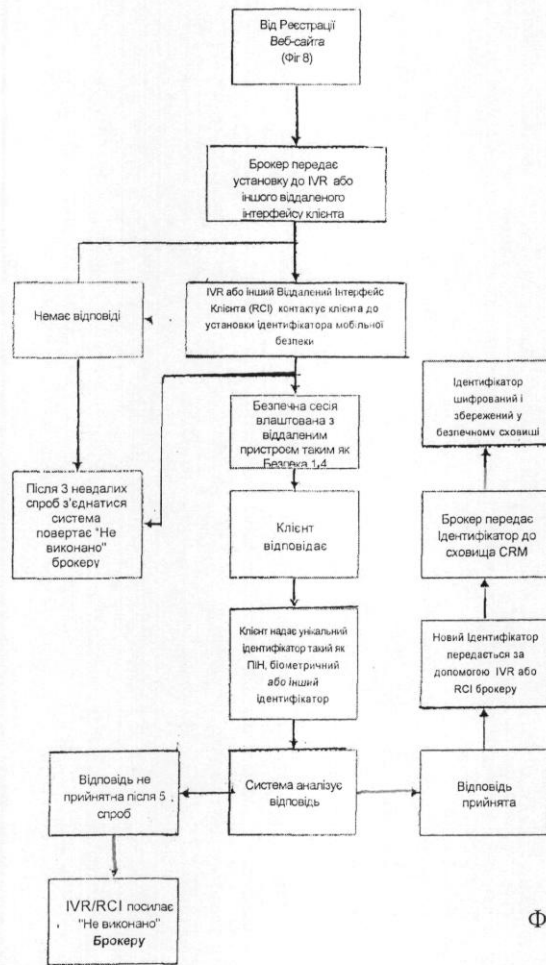


Fig. 8



Фіг. 9

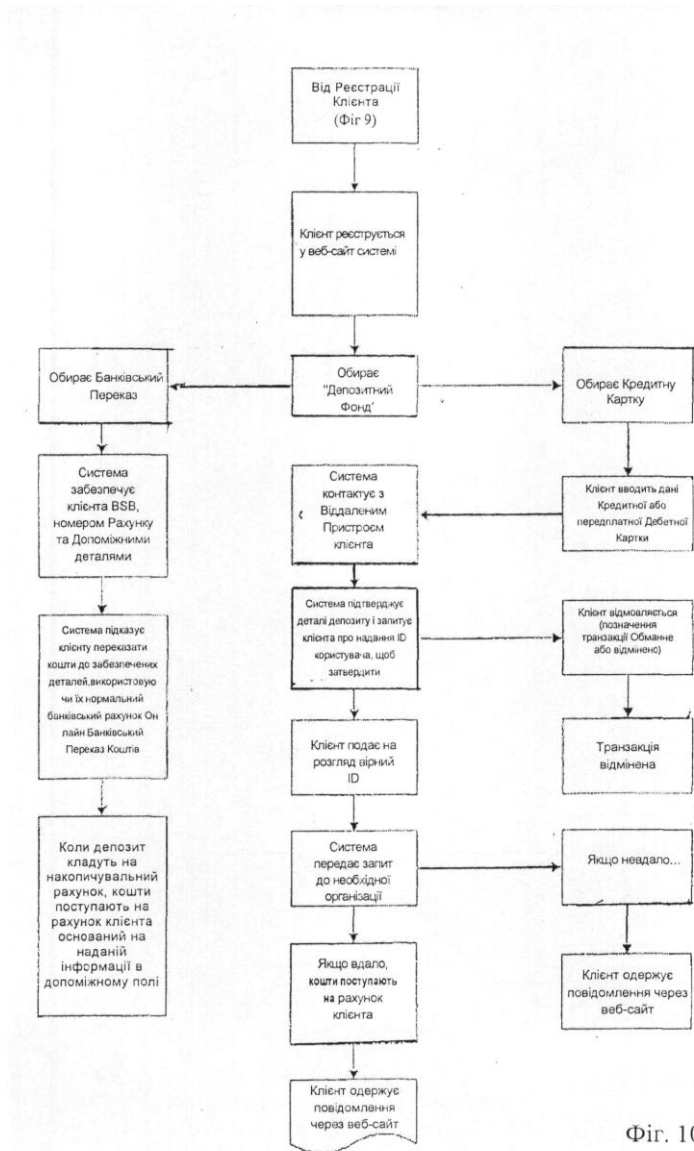
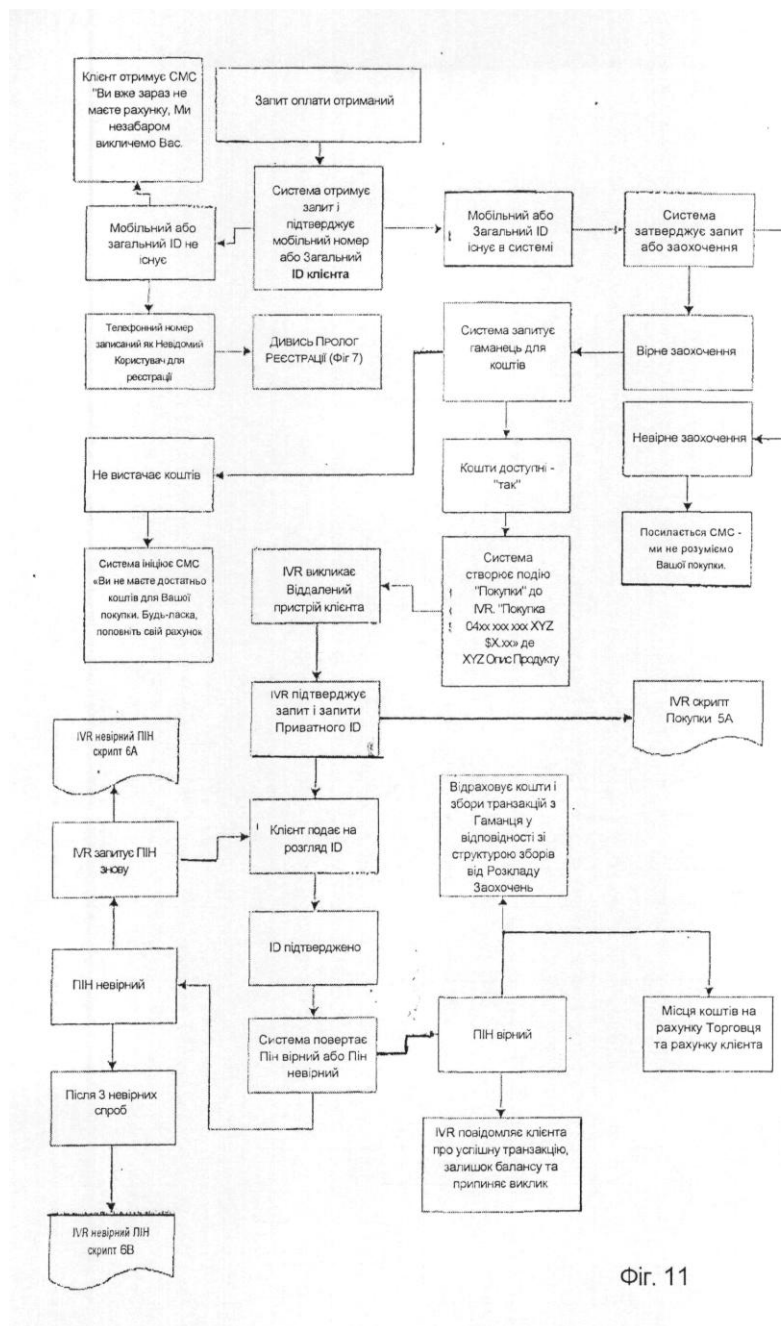
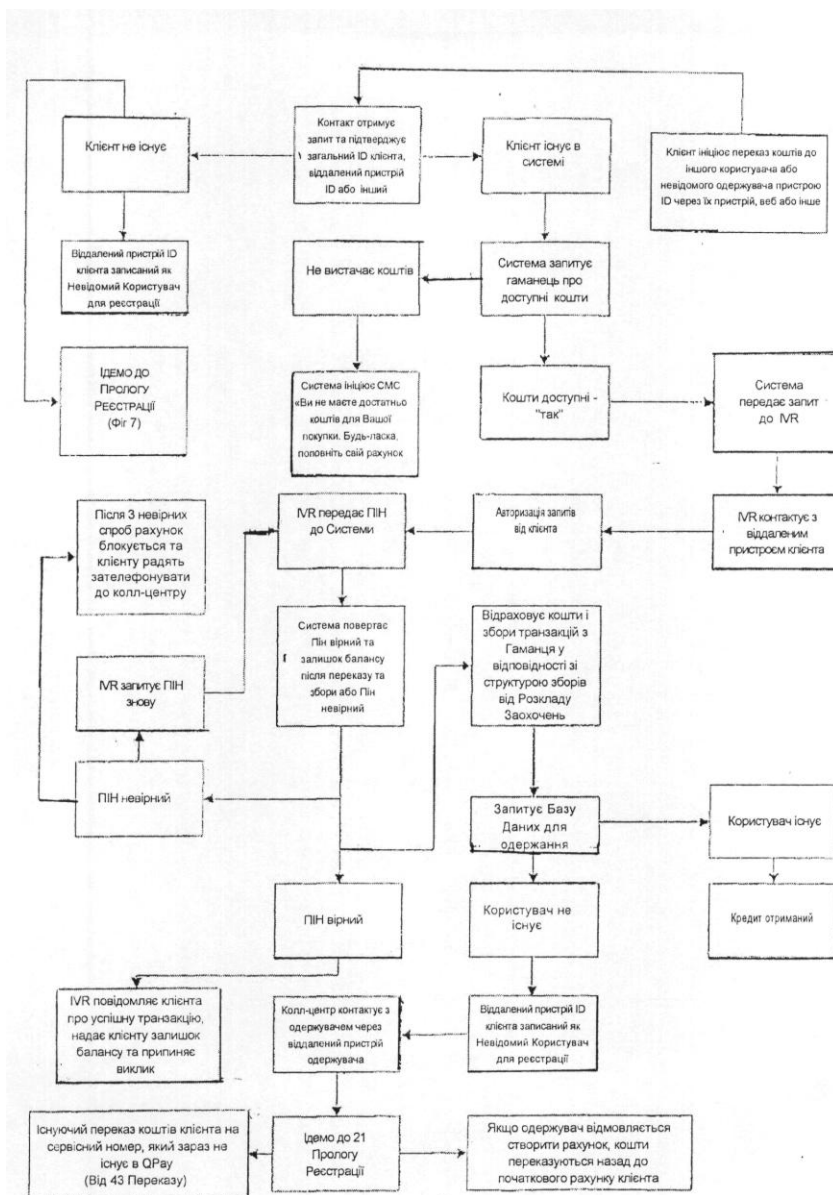


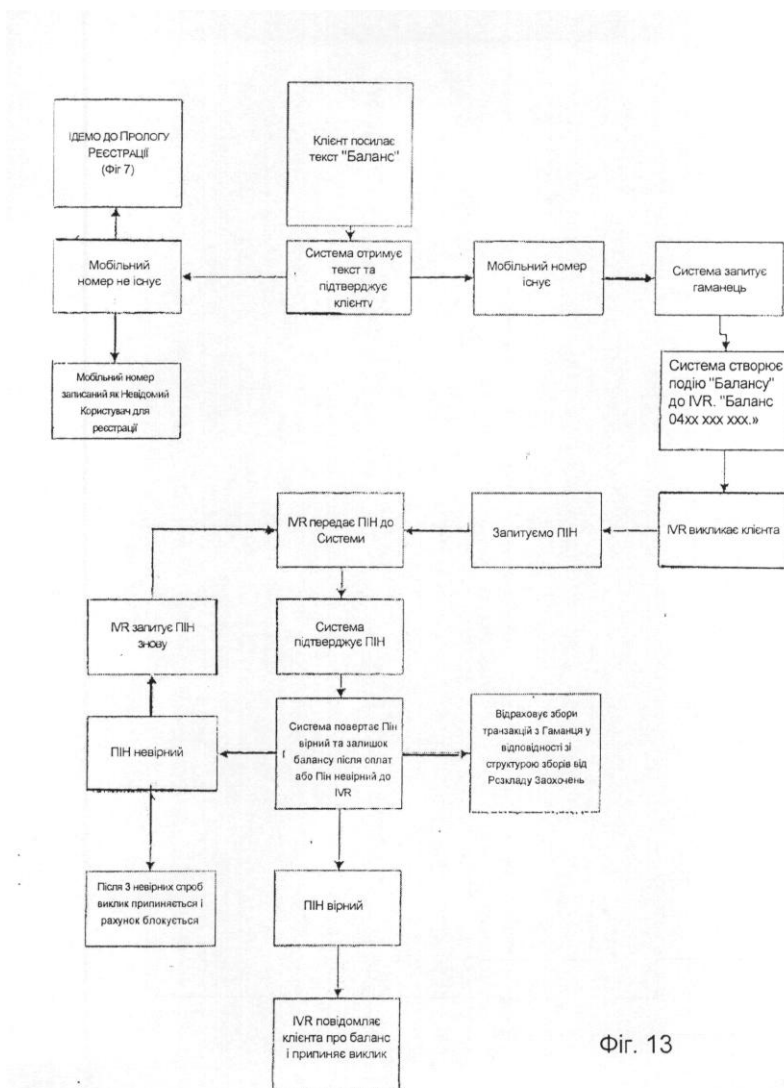
Fig. 10



Фіг. 11



Фіг. 12



Фіг. 13