Винахід відноситься до способів, пристроїв і системи для доступу до виробничого пристрою, зокрема в процесі замовлення систем замків або їх частин.

У такому процесі замовлення можуть бути надані картки безпеки, які забезпечують безпечний доступ до виробничого пристрою під час процесу замовлення. Наприклад, тільки якщо автентифікація пройшла успішно в процесі замовлення, замовлена система замків або замовлена частина системи замків надасть доступ до виготовлення виробничим пристроєм.

Способи та пристрої за незалежними пунктами формули винаходу пропонують безпечну мобільну автентифікацію доступу до виробничого пристрою.

У винаході запропонований реалізований комп'ютером спосіб ініціювання запиту на доступ до виробничого пристрою з терміналом користувача, при цьому спосіб містить у себе наступні стадії: зчитування терміналом даних для ідентифікації і з конкретного для користувача пасивного або активного передавального пристрою, на якому зберігаються ці дані, генерування часової дійсності, генерування токена терміналом користувача, причому токен містить інформацію для ідентифікації, яка базується на даних, та інформацію, яка стосується часової дійсності, відправку токена через термінал користувача та на обчислювальний пристрій.

Переважно токен містить зашифрований і/або аутентифікований набір даних, при цьому набір даних містить інформацію для ідентифікації і/або часової дійсності.

Може бути передбачено, що дані містять перший ключ із першої пари ключів, при цьому дані містять перший ключ з другої пари ключів, причому дані містять першу частину даних для ідентифікації для запиту доступу, зокрема у незашифрованому вигляді, і що дані містять зашифровану другу частину даних для ідентифікації, при цьому спосіб містить у себе зберігання першого ключа з першої пари ключів і першого ключа з другої пари ключів, зокрема у накопичувачі даних терміналу, відправку зашифрованої другої частини даних для ідентифікації, і першої частини даних для ідентифікації через термінал і на інший обчислювальний пристрій, генерування покажчика часу через термінал користувача, який знаходиться в допустимому діапазоні часу, генерування токена через термінал користувача, при цьому токен містить набір даних, який захищено операцією над набором даних за допомогою першого ключа з другої пари ключів, при цьому в наборі даних інформація про часову дійсність містить покажчик часу, а інформація для ідентифікації містить дані для ідентифікації.

Цей спосіб можна виконати як додаток для мобільного телефону. Конкретним для користувача пасивним або активним передавальним пристроєм може бути картка безпеки, наприклад, гібридна картка зі зв'язком ближнього поля та магнітними смугами. Операція може бути шифруванням згідно з криптографічним методом шифрування або згідно з методом криптографічного підпису.

Цей спосіб переважно забезпечує високий стандарт безпеки за допомогою динамічного шифрування або аутентифікації, при цьому спосіб передбачає, що операція над набором даних за допомогою першого ключа з другої пари ключів шифрує набір даних або що операція над набором даних за допомогою першого ключа з другої пари ключів підписує набір даних.

Спосіб також може містити у себе прийом даних на терміналі та від іншого обчислювального пристрою, при цьому дані захищені за допомогою операції над другою частиною даних для ідентифікації другим ключем з першої пари ключів, і перевірку і/або визначення другої частини даних для ідентифікації за допомогою операції над даними першим ключем з першої пари ключів.

Для підвищення стандарту безпеки може бути передбачено, що операція над даними за допомогою першого ключа з першої пари ключів розшифровує дані або що операція над даними за допомогою першого ключа з першої пари ключів верифікує дані.

Реалізований комп'ютером спосіб контролю доступу до виробничого пристрою містить у себе прийом токена через перший обчислювальний пристрій і від другого обчислювального пристрою, при цьому токен містить інформацію для ідентифікації і для часової дійсності, перевірку того, чи існує в базі даних набір даних, який збігається з інформацією для ідентифікації і чи знаходиться токен у межах своєї часової дійсності або ні, дозвіл, який забезпечує доступ до виробничого пристрою через другий обчислювальний пристрій, якщо у базі даних існує набір даних, який збігається з інформацією для ідентифікації і токен знаходиться в межах своєї часової дійсності, а у протилежному випадку надається відмова у доступі через другий обчислювальний пристрій.

Токен переважно містить зашифрований і/або аутентифікований набір даних, причому набір даних містить інформацію для ідентифікації та/або часову дійсність.

Може бути передбачено, що набір даних захищений операцією над набором даних за допомогою першого ключа з другої пари ключів, при цьому в наборі даних інформація про часову дійсність містить покажчик часу, а інформація для ідентифікації містить дані для ідентифікації, при цьому спосіб містить у себе: перевірку і/або визначення набору даних з токена за допомогою операції над набором даних другим ключем з другої пари ключів, перевірку того, чи існує у базі даних набір даних, що збігається з набором даних у даних для ідентифікації і чи знаходиться покажчик часу в межах допустимого діапазону часу або ні, дозвіл на надання доступу до виробничого пристрою через другий обчислювальний пристрій, якщо в базі даних існує набір даних, який збігається з даними для

ідентифікації і покажчик часу знаходиться в допустимому діапазоні часу, а у протилежному випадку надається відмова у доступі через другий обчислювальний пристрій.

Для підвищення безпеки спосіб може передбачати, що операція над набором даних за допомогою першого ключа з другої пари ключів шифрує набір даних, при цьому операція над набором даних другим ключем з другої пари ключів розшифровує набір даних, або що операція над набором даних за допомогою першого ключа з другої пари ключів підписує набір даних, при цьому операція над набором даних другим ключем з другої пари ключів аутентифікує набір даних.

Спосіб може містити у себе прийом першої частини даних для ідентифікації, зокрема незашифрованої, та зашифрованої другої частини даних для ідентифікації через перший обчислювальний пристрій і від терміналу, ідентифікацію набору даних, що збігається з даними для ідентифікації на сервері шляхом порівняння першої частини даних для ідентифікації і другої частини даних для ідентифікації з наборами даних, які зберігаються у першому обчислювальному пристрої, зокрема у базі даних, генерування даних шляхом шифрування другої частини даних для ідентифікації другим ключем з другої пари ключів і відправку даних через перший обчислювальний пристрій і на термінал. Це ще більше підвищує надійність способу.

Реалізований комп'ютером спосіб доступу до виробничого пристрою містить у себе прийом токена для першого обчислювального пристрою через другий обчислювальний пристрій і від терміналу користувача, при цьому токен містить інформацію для ідентифікації і для часової дійсності, відправку токена через другий обчислювальний пристрій і на перший обчислювальний пристрій для верифікації запиту на доступ, перевірку того, чи дозволяє перший обчислювальний пристрій доступ до виробничого пристрою або ні, відправку виробничих даних на виробничий пристрій, якщо перший обчислювальний пристрій дозволяє, що через другий обчислювальний пристрій надається доступ до виробничого пристрою (109), а у протилежному випадку надається відмова у доступі, наданому через другий обчислювальний пристрій.

Переважно токен містить зашифрований і/або аутентифікований набір даних, при цьому набір даних містить інформацію для ідентифікації і/або часової дійсності.

Може бути передбачено, що набір даних захищений операцією над набором даних за допомогою першого ключа з другої пари ключів, при цьому в наборі даних інформація про часову дійсність містить покажчик часу, а інформація для ідентифікації містить дані для ідентифікації. Завдяки цьому ефективно виконується рішення про те, чи дозволений доступ або ні.

Безпека підвищується, якщо операція передбачена на додаток до зашифрованої передачі даних.

Термінал, зокрема, мобільний термінал, для користувача призначений для здійснення стадій способу ініціювання запиту на доступ до виробничого пристрою за допомогою терміналу.

Перший обчислювальний пристрій, зокрема сервер, призначений для здійснення стадій у способі керування доступом до виробничого пристрою.

Другий обчислювальний пристрій, зокрема сервер замовлень, призначений для здійснення способу доступу до виробничого пристрою.

Система, яка містить перший обчислювальний пристрій і другий обчислювальний пристрій, дозволяє конкретно надавати або забороняти доступ до виробничого пристрою в процесі замовлення.

Доступ до процедури замовлення стає можливим для користувача або підприємства через комп'ютерну програму, яка містить у себе здатні до машинного зчитування інструкції, які при виконанні комп'ютером здійснюють стадії способу.

Інші переважні варіанти здійснення випливають з наступного опису та креслень. На кресленні показано:

на фіг. 1 схематично зображена система,

на фіг. 2 стадії способу доступу до виробничого пристрою.

У подальшому описі операції над даними виконуються за допомогою першої пари ключів SP1 та другої пари ключів SP2. В одному варіанті здійснення перша пара ключів SP1 та друга пара ключів SP2 є парами ключів криптографічного методу. Можуть бути використані різні криптографічні методи. Дані захищені операціями. У цьому контексті "захищений" означає, що несанкціоноване використання даних, захищених операцією, або несанкціонований доступ до них утруднені.

Перша пара ключів SP1 містить перший ключ S11 і другий ключ S12.

Друга пара ключів SP2 містить перший ключ S21 і другий ключ S22.

Операції можуть містити шифрування або дешифрування, з одного боку. З іншого боку, операції можуть містити підписання або автентифікацію.

Шифрування або дешифрування:

Наприклад, за допомогою першого ключа S11 з першої пари ключів SP1 можна розшифрувати дані, які були зашифровані другим ключем S12 з першої пари ключів SP1.

Наприклад, за допомогою другого ключа S22 з другої пари ключів SP2 можна розшифрувати дані, які були зашифровані за допомогою першого ключа S21 з другої пари ключів SP2.

Підпис або автентифікація:

Наприклад, за допомогою першого ключа S11 з першої пари ключів SP1 можна верифікувати дані, які були підписані другим ключем S12 з першої пари ключів SP1.

Наприклад, за допомогою другого ключа S21 з другої пари ключів SP2 можна верифікувати дані, які були підписані першим ключем S21 з другої пари ключів SP2.

На фігурі 1 схематично показано систему 101. Система 101 містить у себе перший обчислювальний пристрій 102. В одному варіанті здійснення перший обчислювальний пристрій 102 являє собою сервер.

Перший обчислювальний пристрій 102 містить базу 103 даних або підключений до неї через канал передачі даних. База 103 даних містить множину наборів даних, які містять різні дані для ідентифікації.

Перший обчислювальний пристрій 102 призначений для надання даних для ідентифікації, зокрема з бази 103 даних. Дані для ідентифікації містять першу частину I1 і другу частину I2.

В одному варіанті здійснення дані для ідентифікації містять ІД об'єкта. За допомогою ІД об'єкта однозначно ідентифікують всю систему, що складається з N ключів і N циліндрів замка.

Система 101 містить конкретний для користувача пасивний або активний передавальний пристрій 104. В одному варіанті здійснення передавальний пристрій 104 являє собою карту безпеки. В одному варіанті здійснення картку безпеки надано певному ІД об'єкта.

На передавальному пристрої 104 зберігаються дані K1, K2, K3, K4.

Дані K1 містять перший ключ S11 з першої пари ключів SP1.

Дані K2 містять зашифровану другу частину I2 даних для ідентифікації для ІД об'єкта.

Дані K3 містять перший ключ S21 з другої пари ключів SP2.

Дані K4 містять першу частину I1 даних для ідентифікації для ІД об'єкта, зокрема незашифровану.

Другий ключ S12 з першої пари ключів SP1 і другий ключ S22 з другої пари ключів SP2 надаються як дані автентифікації обчислювального пристрою 101.

Система 101 призначена для зв'язку з терміналом 105 користувача. В одному варіанті здійснення термінал 105 являє собою мобільний телефон. На мобільному телефоні може працювати додаток, тобто комп'ютерна програма, за допомогою якої користувач може виконати процес верифікації процедури замовлення для системи замків або частини системи замків, наприклад, ключа і/або замка. У цьому контексті процес верифікації означає, що підтверджується справжність, чи дозволено користувачеві робити замовлення або ні.

Термінал 105 містить накопичувач 106 даних. Термінал 105 призначений для виконання стадій способу, описаного нижче.

Система 101 містить другий обчислювальний пристрій 108. В одному варіанті здійснення другий обчислювальний пристрій 108 являє собою сервер замовлень, який надає послуги роздрібного продавця в процесі замовлення. Послуга дозволяє користувачеві здійснювати процес верифікації процедури замовлення через мобільний телефон. В одному варіанті здійснення послуга надає вибір системи замків або її частини. Для цього послуга дозволяє вводити дані, тобто інформацію про замовлення, через мобільний телефон і здійснювати процес верифікації процедури замовлення. В одному варіанті здійснення послуга дозволяє отримувати та обробляти дані для ідентифікації і токени для цього. Послуга містить у себе інтерфейс користувача порталу інтернет-торгівлі та інтерфейс для мобільного телефону. В одному варіанті здійснення послуга являє собою комп'ютерну програму або містить множину комп'ютерних програм.

В одному варіанті здійснення процес оплати і/або здійснення процедури замовлення між користувачем та спеціалізованим роздрібним продавцем відбувається у системі спеціалізованого роздрібного продавця. Замовлення спеціалізованого продавця відбувається через портал замовлень.

У процесі верифікації користувач підтверджує порталу замовлень і системі спеціалізованого продавця, що він має право робити замовлення.

Система 101 призначена для зв'язку з виробничим пристроєм 109. Виробничий пристрій 109 і/або термінал 105 також можуть бути частиною системи 101.

Перший обчислювальний пристрій 102 призначений для виконання стадій описаного нижче способу.

Другий обчислювальний пристрій 108 призначений для надання даних B замовлення для виробничого процесу, щоб виготовити систему замків або частину системи замків, наприклад ключа і/або замка, відповідно до даних B замовлення. В одному варіанті здійснення дані B замовлення містять у себе дані для ідентифікації з процедури замовлення.

Виробничий пристрій 109 призначений для виконання виробничого процесу залежно від даних B замовлення. В одному варіанті здійснення виробничий пристрій 109 призначений для виготовлення частини системи замків, зокрема ключа і/або замка, згідно з даними B замовлення.

Для доступу до виробничого пристрою 109 за допомогою терміналу 105 користувача в системі 101, зокрема передбачені наступні стадії:

зчитування даних через термінал 105 і з конкретного для користувача пасивного або активного передавального пристрою 104, на якому ці дані зберігаються;

генерування покажчика часу через термінал 105 користувача, який знаходиться в межах допустимого діапазону часу. В одному варіанті здійснення допустимий діапазон часу визначає дату закінчення терміну дії, після якої дані B замовлення стають недійсними;

генерування токена FS через термінал 105 користувача, при цьому токен FS містить набір даних F, де набір даних F містить покажчик часу і дані для ідентифікації I1, I2. В одному варіанті здійснення токен FS являє собою запит на доступ і призначений для першого обчислювального пристрою 102, щоб таким чином він міг перевірити, чи дозволений або заборонений доступ;

прийом токена FS для першого обчислювального пристрою 102 через другий обчислювальний пристрій 108 і від терміналу 106 користувача. В одному варіанті здійснення токен FS відправляється не безпосередньо на перший обчислювальний пристрій 102, а через другий обчислювальний пристрій 108. Для цього термінал 105 не вимагає з'єднання для першого обчислювального пристрою 101. Для цього термінал 105 потребує з'єднання для другого обчислювального пристрою 108;

відправка токена FS через другий обчислювальний пристрій 108 і на перший обчислювальний пристрій 102 для верифікації запиту на доступ;

перевірка того, чи надає або не надає перший обчислювальний пристрій 102 доступ до виробничого пристрою 109;

відправка виробничих даних на виробничий пристрій 109, якщо перший обчислювальний пристрій 102 дає дозвіл, що через другий обчислювальний пристрій 108 надається доступ до виробничого пристрою 109, а у протилежному випадку відхиляє доступ, що надається через другий обчислювальний пристрій 108. Це означає, в одному варіанті здійснення, що другий обчислювальний пристрій 108 надає або забороняє терміналу доступ до виробничого пристрою 109. Це означає, в одному з варіантів здійснення, що другий обчислювальний пристрій 108 управляється через перший обчислювальний пристрій 101.

Зразковий спосіб показано на фіг. 2 і описано на прикладі сервера, карти безпеки, мобільного телефону, сервера замовлень та виробничого пристрою. В одному варіанті здійснення спосіб починається зі стадії 201.

На стадії 201 виконується зчитування мобільним телефоном 105 даних K1, K2, K3, K4 з карти безпеки. В одному варіанті здійснення для зчитування використовують зв'язок ближнього поля, NFC. Для NFC призначені як мобільний телефон, так і карта безпеки. Також може бути використана радіочастотна ідентифікація, RFID, або інший зокрема бездротовий спосіб передачі.

Після цього виконується стадія 202.

На стадії 202 здійснюється зберігання даних K1 і K3. Це означає, що зберігаються перший ключ S11 з першої пари ключів SP1 і перший ключ S21 з другої пари ключів SP2. Дані зберігаються у накопичувачі 106 даних терміналу 105, в одному з варіантів здійснення у мобільному телефоні 105.

Після цього виконується стадія 203.

На стадії 203 здійснюється відправка даних K2 і K4 мобільним телефоном 105 на сервер 102.

Після цього виконується стадія 204.

В одному варіанті здійснення дані K2 містять у себе першу частину I1 даних для ідентифікації, незашифровану. Дані K2 містять у себе другу частину I2 даних для ідентифікації та вже у зашифрованому вигляді зберігаються на карті 104 безпеки.

На стадії 204 здійснюється визначення другої частини I2 даних для ідентифікації, наприклад, шляхом розшифровки даних K2 сервером. В одному варіанті здійснення на сервері 102 передбачена третя пара ключів SP3 для шифрування другої частини I2 даних для ідентифікації при виготовленні карти 104 безпеки і для розшифровки другої частини I2 даних для ідентифікації у процедурі замовлення з картою безпеки.

Після цього виконується стадія 205.

На стадії 205 на сервері 102 здійснюється ідентифікація набору даних I1 і I2, який збігається з даними для ідентифікації I1 і I2. Для цього може бути передбачено порівняння одержаної в даних K4 першої частини I1 даних для ідентифікації і одержаної в даних K2 другої частини I2 даних для ідентифікації з набором даних, що зберігається на сервері 102 у базі даних.

Після цього виконується стадія 206. Може бути передбачено, що процедура замовлення скасовується, якщо не може бути знайдений набір даних, який збігається з даними для ідентифікації I1 і I2.

На стадії 206 на сервері 102 здійснюється генерування даних A3 шляхом шифрування другої частини I2 даних для ідентифікації I2 другим ключем S12 з першої пари ключів SP1.

Після цього виконується стадія 207.

На стадії 207 здійснюється передача даних A3 з сервера 102 на мобільний телефон 105.

Після цього виконується стадія 208.

На стадії 208 у мобільному телефоні 105 здійснюється верифікація даних A3 і розшифровка другої частини I2 даних для ідентифікації I2 за допомогою першого ключа S11 з першої пари ключів SP1.

Після цього виконується стадія 209.

На стадії 209 здійснюється генерування дати закінчення терміну та інформації про замовлення комп'ютерною програмою, яка працює на мобільному телефоні 105.

На стадії 209 відбувається створення набору даних F для дозволу мобільним телефоном 105 і з використанням дати закінчення терміну та інформації про замовлення.

Набір даних F містить покажчик часу і дані для ідентифікації I1 і I2. Покажчик часу може вказувати дату закінчення терміну, наприклад у вигляді покажчика абсолютного часу. Покажчик часу може також вказувати час початку визначення дати закінчення терміну.

Після цього виконується стадія 210.

На стадії 210 у мобільному телефоні 105 здійснюється шифрування набору даних F за допомогою першого ключа S21 з другої пари ключів SP2 через мобільний телефон для формування токена FS.

Після цього виконується стадія 211.

На стадії 211 здійснюється передача токена FS і даних для ідентифікації I1 і I2 з мобільного телефону 105 на сервер 108 замовлень.

Це означає, що мобільний телефон 105 ініціює запит доступу до виробничого пристрою 109.

Після цього виконується стадія 212.

На стадії 212 здійснюється відправка запиту на верифікацію токена FS через сервер 108 замовлень на сервер 102.

Після цього виконується стадія 213.

Сервер 102 управляє доступом до виробничого пристрою 109. Управління бачить перевірку набору даних F з токену FS.

Наприклад, на стадії 213 відбувається розшифровка токена FS сервером 102 за допомогою другого ключа S22 з другої пари ключів SP2.

Після цього на сервері 102 виконується стадія 214.

На стадії 214 виконується перевірка того, чи існує у базі даних 103 набір даних, який у даних для ідентифікації I1 і I2 збігається з набором даних F і чи покажчик часу знаходиться в межах допустимого часового діапазону або ні.

На стадії 214 відбувається визначення даних B замовлення згідно з даними для ідентифікації I1 і I2 та інформації замовлення з токену FS.

Може бути передбачена можливість скасування процедури замовлення, тобто відмови у наданні доступу другим обчислювальним пристроєм 108, якщо розшифрування набору даних F не вдалося або не існує відповідного набору даних у базі даних 103.

Після цього виконується стадія 215.

На стадії 215 здійснюється дозвіл на доступ до виробничого пристрою 109 другим обчислювальним пристроєм 108, якщо у базі даних 103 існує набір даних, що збігається з даними для ідентифікації I1 і I2, і покажчик часу знаходиться в межах допустимого часового діапазону. В іншому випадку відбувається відмова у доступі другим обчислювальним пристроєм 108.

Якщо доступ дозволено, в одному варіанті здійснення виконується передача назад даних замовлення B із сервера 102 на сервер 108 замовлень.

Після цього виконується стадія 216.

На стадії 216 здійснюється співвідношення токена FS до даних замовлення B сервером 108 замовлень.

Після цього виконується стадія 217.

На стадії 217 здійснюється випуск замовлення і передача даних B замовлення сервером 108 замовлень на виробничий пристрій 109.

В одному варіанті здійснення токен FS являє собою програмний токен. Токен FS також можна реалізувати в інший спосіб, наприклад, як набір даних випуску.

В одному варіанті здійснення зв'язок між першим обчислювальним пристроєм 101, другим обчислювальним пристроєм 108 і терміналом 105 відбувається з використанням щонайменше одного протоколу шифрування.

У цьому контексті протоколи шифрування являють собою мережні протоколи, які гарантують зашифровану передачу даних через комп'ютерну мережу. Наприклад, мережний протокол використовують відповідно до одного з наступних стандартів: Transport Layer Security, TLS, Wi-Fi Protected Access 3, WPA3, Wi-Fi Protected Access 2, WPA2, Secure Shell, SSH або Internet Protocol Security, IPsec.

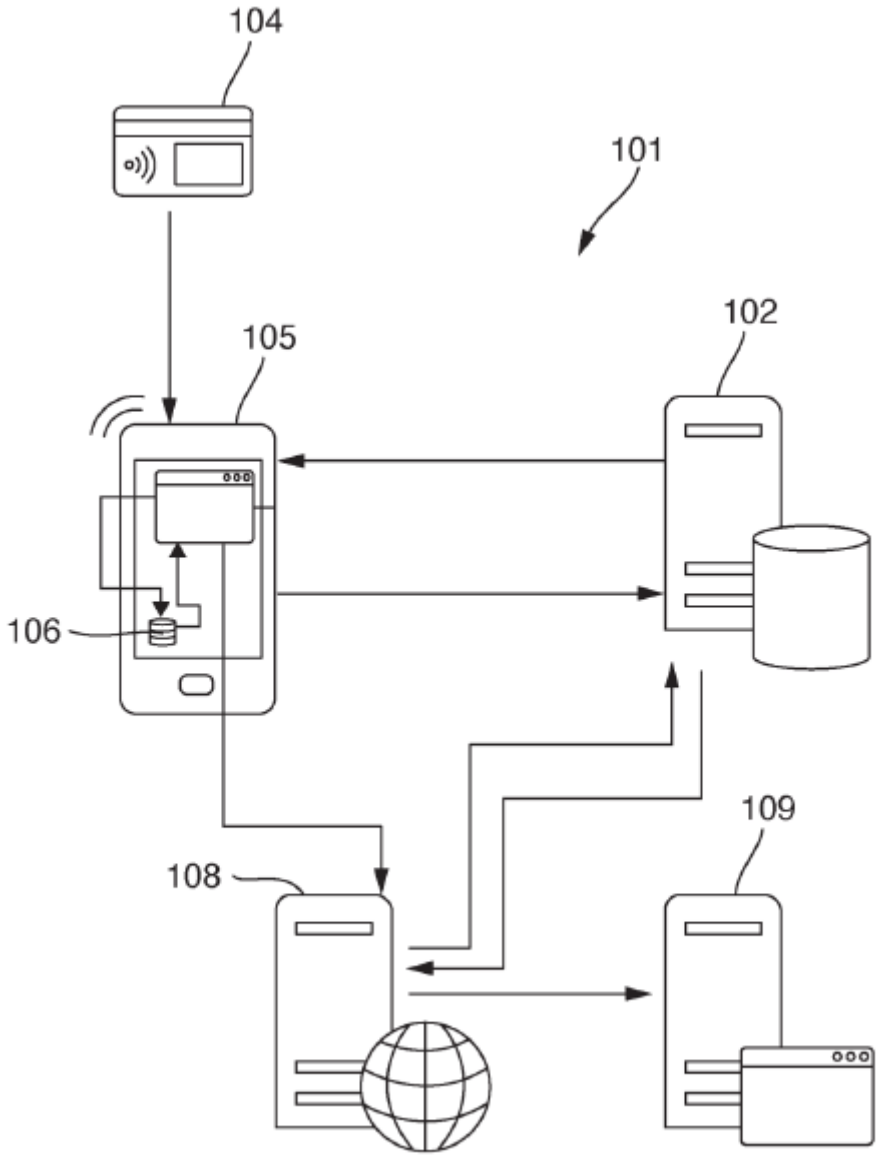
В одному варіанті здійснення описані пари ключів використовують на додачу до такого протоколу шифрування. Додаткове шифрування, що досягається таким чином, відрізняється від цих протоколів шифрування, а також від інших типів зашифрованої передачі даних, наприклад, використанням зашифрованої віртуальної приватної мережі.

В одному варіанті здійснення використовують дані для ідентифікації та автентифікації, при цьому дані K1 містять перший ключ S11 з першої пари ключів SP1, при цьому дані K3 містять перший ключ S21 з другої пари ключів SP2, при цьому дані K4 містять першу частину I1 даних для ідентифікації для запиту доступу, зокрема у незашифрованому вигляді, і при цьому дані K2 містять зашифровану другу

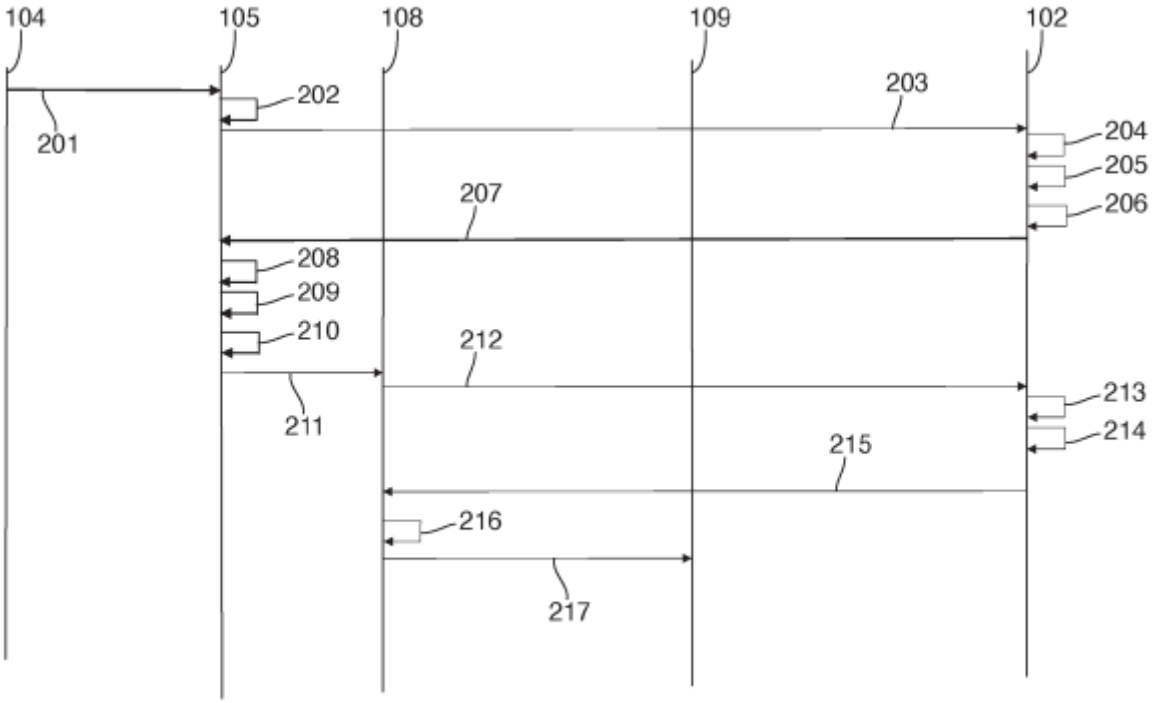
частину I2 даних для ідентифікації. Для ідентифікації або автентифікації також можуть бути використані інші дані.

В одному варіанті здійснення через термінал 105 користувача визначається часова дійсність, яка містить покажчик часу, що знаходиться в межах допустимого діапазону часу.

В одному варіанті здійснення використовується токен, який містить інформацію для ідентифікації та для часової дійсності, при цьому токен містить набір F даних, який захищений операцією над набором F даних за допомогою першого ключа S21 з другої пари ключів SP2, при цьому набір F даних містить покажчик часу і дані для ідентифікації I1, I2. Також можна використовувати інший токен, який містить у себе інформацію для аутентифікації, для ідентифікації і для часової дійсності.



Фіг. 1


104
105
108
109
102
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217

Фіг. 2