РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 731 663**(13) **C2**

(51) МПК
G06F 21/35 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 1/1684 (2020.02); *G06F 21/32* (2020.02); *G06F 21/35* (2020.02); *G06F 3/0414* (2020.02); *G06F 3/044* (2020.02); *G06K 9/0002* (2020.02)

(21)(22) Заявка: **2018118364, 20.10.2016**

(24) Дата начала отсчета срока действия патента:
20.10.2016

Дата регистрации:
07.09.2020

Приоритет(ы):
(30) Конвенционный приоритет:
20.10.2015 FR 1559966

(43) Дата публикации заявки: **26.11.2019** Бюл. № **33**

(45) Опубликовано: **07.09.2020** Бюл. № **25**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **21.05.2018**

(86) Заявка PCT:
EP 2016/075235 (20.10.2016)

(87) Публикация заявки PCT:
WO 2017/068044 (27.04.2017)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, стр. 3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
МЭЗОН Тьерри (FR),
ЛЕ БАЙ Янн (FR)

(73) Патентообладатель(и):
БАЙСТЭМП (FR)

(56) Список документов, цитированных в отчете о поиске: **US 2015/0178489 A1, 25.06.2015. US 2003/0106447 A1, 12.06.2003. US 2014/0026213 A1, 23.01.2014. WO 2015/015523 A1, 05.02.2015. RU 2364516 C2, 20.08.2009.**

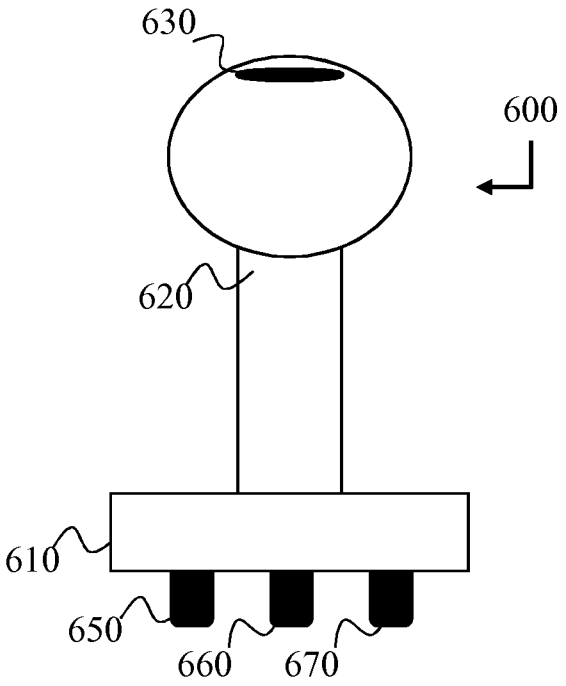
(54) УСТРОЙСТВО ТАКТИЛЬНОЙ И ЗВУКОВОЙ АУТЕНТИФИКАЦИИ

(57) Реферат:

Изобретение относится к вычислительной технике. Технический результат заключается в уменьшении неудобства существующих штемпельных подушечек с сохранением простоты их использования. Предлагается устройство аутентификации, предназначенное для использования с электронным устройством, содержащим емкостный сенсорный экран и приемник, содержащее множество штырьков, расположенных на одной и той же поверхности устройства аутентификации, причем по меньшей мере два штырька состоят из проводящего материала, а остальные штырьки состоят из изолирующего материала, все штырьки имеют одинаковый внешний вид, средство для обнаружения давления, оказываемого на по меньшей мере один штырек, и средство для излучения сигнала аутентификации, принимаемого приемником при обнаружении давления, причем сигнал аутентификации является звуковым сигналом. 5 н. и 6 з.п. ф-лы, 12 ил.

RU 2731663 C2

RU 2731663 C2



ФИГ. 6

RU 2731663 C2

RU 2731663 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 731 663**(13) **C2**

(51) Int. Cl.
G06F 21/35 (2013.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 1/1684 (2020.02); *G06F 21/32* (2020.02); *G06F 21/35* (2020.02); *G06F 3/0414* (2020.02); *G06F 3/044* (2020.02); *G06K 9/0002* (2020.02)

(21)(22) Application: **2018118364, 20.10.2016**

(24) Effective date for property rights:
20.10.2016

Registration date:
07.09.2020

Priority:
(30) Convention priority:
20.10.2015 FR 1559966

(43) Application published: **26.11.2019** Bull. № **33**

(45) Date of publication: **07.09.2020** Bull. № **25**

(85) Commencement of national phase: **21.05.2018**

(86) PCT application:
EP 2016/075235 (20.10.2016)

(87) PCT publication:
WO 2017/068044 (27.04.2017)

Mail address:
129090, Moskva, ul. B. Spasskaya, 25, str. 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):
MAISON, Thierry (FR),
LE BAIL, Yann (FR)

(73) Proprietor(s):
BYSTAMP (FR)

RU 2731663 C2

(54) TACTILE AND SOUND AUTHENTICATION DEVICE

(57) Abstract:

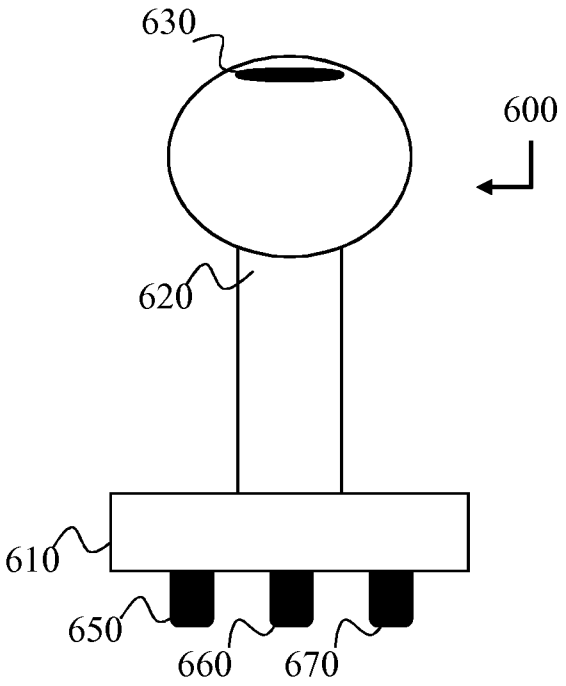
FIELD: computer equipment.

SUBSTANCE: disclosed is an authentication device for use with an electronic device comprising a capacitive touch screen and a receiver comprising a plurality of pins, located on the same surface of the authentication device, wherein at least two pins consist of a conductive material, and the remaining pins consist of an insulating material, all pins have same appearance, means for detecting pressure exerted on at least one pin, and means for emitting an authentication signal, received by receiver when pressure is detected, wherein authentication signal is audio signal.

EFFECT: technical result consists in reduction of inconvenience of existing stamp pads with preservation of ease of their use.

11 cl, 12 dwg

RU 2731663 C2



ФИГ. 6

RU 2731663 C2

Настоящее изобретение относится к области устройств аутентификации.

Штемпельная подушечка 100, представленная на фиг. 1, является основным устройством аутентификации или подписания. Штемпельная подушечка 100 состоит из ручки 120, за которую может держаться пользователь, и штемпеля 110, причем штемпель 110 имеет внешний рельефный рисунок. Такая штемпельная подушечка 100 традиционно используется для аутентификации документов. Пользователю штемпельной подушечки 100, прежде всего, необходимо прижать штемпель 110 к штемпельной подушечке таким образом, чтобы штемпель 110 покрылся слоем чернил, а затем прижать штемпель 110 к аутентифицируемому документу, чтобы отпечатать на нем штамп, соответствующий рисунку штемпеля 110. Отпечатанный штамп обеспечивает аутентификацию или подписание документа. Существуют более сложные штемпельные подушечки, так называемые подушечки с автоматическим нанесением чернил, такие как описанные в заявке на патент Франции FR 3 016 142. Однако штемпельная подушечка 100, а также подушечка с автоматическим нанесением чернил, описанная в вышеупомянутой заявке на патент, используются одинаковым образом, при этом пользователю приходится более или менее сильно прижимать штемпельную подушечку к аутентифицируемому или подписываемому документу. Классическим примером использования штемпельной подушечки 100 является подписание компаниями транспортных накладных, при этом подписание осуществляется «резиновым штампованием» транспортной накладной.

Уровень аутентификации, обеспечиваемый такими устройствами, весьма слаб, поскольку очень легко скопировать рисунок штемпеля, и, кроме того, один и тот же рисунок многократно используется без изменения. Следовательно, можно его скопировать и использовать копию мошенническим путем.

Более того, данный основной способ аутентификации до сих пор часто используется, при этом он не приспособлен к небумажным документам. Фактически, необходимо пройти первую стадию, на которой документ аутентифицируется путем использования штемпельной подушечки, а затем вторую стадию, на которой аутентифицированный документ сканируется. Этот процесс является долгим и трудоемким.

Таким образом, необходимо предложить устройство аутентификации, которое может уменьшить неудобства существующих штемпельных подушечек, сохранив простоту использования этих штемпельных подушечек.

Настоящее изобретение относится к устройству аутентификации, предназначенному для использования с электронным устройством, содержащим емкостный сенсорный экран и приемник, причем устройство аутентификации отличается тем, что оно содержит множество штырьков, расположенных на одной и той же поверхности устройства аутентификации, причем по меньшей мере два штырька состоят из проводящего материала, а остальные штырьки состоят из изолирующего материала, все штырьки имеют одинаковый внешний вид, средство для обнаружения давления, оказываемого на по меньшей мере один штырек, и средство для излучения сигнала аутентификации, принимаемого приемником при обнаружении давления, причем сигнал аутентификации является звуковым сигналом.

Предпочтительно, устройство аутентификации может заменять штемпельную подушечку для использования в процессе безбумажной аутентификации. Штырьки, состоящие из проводящего материала, обеспечивают обнаружение - с помощью емкостного сенсорного экрана электронного устройства - рисунка, связанного с расположением упомянутых проводящих штырьков. Средство для обнаружения давления позволяет обеспечивать выдачу сигнала аутентификации только при

использовании устройства аутентификации, например, благодаря размещению в контакте с сенсорным экраном электронного устройства. Использование аутентификации путем комбинирования звукового сигнала аутентификации и рисунка обеспечивает все возможности аутентификации звуковым сигналом (доступность электронных устройств, имеющих микрофон, бесконечность доступных звуковых кодов). Комбинирование аутентификации путем комбинирования звукового сигнала аутентификации и рисунка - причем последний требует физического соприкосновения - позволяет гарантировать, что только электронное устройство, к которому прижимается устройство аутентификации, может успешно осуществлять процесс аутентификации.

В соответствии с одним дополнительным вариантом осуществления изобретения, геометрическое расположение штырьков, состоящих из проводящего материала, образует рисунок, причем рисунок связан с сигналом аутентификации.

При этом устройство аутентификации обеспечивает дополнительную степень защиты во время обнаружения звукового сигнала, причем указанный звуковой сигнал связан с рисунком. При этом только электронное устройство, к которому прижимается устройство аутентификации и на котором может обнаруживаться рисунок, способно устанавливать, что звуковой сигнал и рисунок соответствуют друг другу.

В соответствии с одним дополнительным вариантом осуществления изобретения, устройство аутентификации по меньшей мере частично изготовлено из проводящего материала, причем электрическая непрерывность обеспечивается штырьками, состоящими из проводящего материала.

При этом устройство аутентификации, находящееся в руке пользователя, может использоваться на емкостном сенсорном экране электронного устройства. Электрическая непрерывность реализуется между пользователем и емкостным сенсорным экраном.

В соответствии с одним дополнительным вариантом осуществления изобретения, проводящий материал, составляющий штырьки и/или устройство аутентификации, является гибким.

При этом устройство аутентификации может использоваться без риска поцарапать или повредить экран электронного устройства.

В соответствии с одним дополнительным вариантом осуществления изобретения, устройство аутентификации содержит моноблочный и полый корпус, состоящий из гибкого материала, являющегося проводником электричества, причем корпус содержит по меньшей мере одну канавку, позволяющую вставлять опорную пластину, состоящую из электропроводящего материала, на которой держатся штырьки, причем внутренняя часть корпуса устройства аутентификации образует клетку Фарадея.

При этом устройство аутентификации является технологичным и прочным. Кроме того, электронные компоненты, помещенные внутрь устройства аутентификации, защищены от электромагнитных помех.

В соответствии с одним дополнительным вариантом осуществления изобретения, устройство аутентификации дополнительно содержит средство для считывания отпечатков пальцев при обнаружении давления на по меньшей мере одном штырьке, причем сигнал аутентификации излучается только в том случае, если считанный отпечаток пальца соответствует предварительно заданному отпечатку пальца.

При этом обеспечивается определенная степень защиты, поскольку устройство аутентификации может использоваться только предварительно заданным пользователем.

В соответствии с одним дополнительным вариантом осуществления изобретения, по большей мере четыре штырька состоят из проводящего материала, остальные

штырьки состоят из изолирующего материала.

При этом емкостный сенсорный экран электронного устройства может быстро обнаруживать рисунок, образуемый штырьками, состоящими из проводящего материала. Кроме того, гарантируется совместимость устройства аутентификации с емкостными сенсорными экранами, неспособными одновременно обнаруживать более четырех точек касания.

Настоящее изобретение также относится к способу аутентификации идентификатора, связанного с устройством аутентификации, причем способ исполняется электронным устройством, содержащим емкостной сенсорный экран и приемник, и включает в себя этапы приема выбранного варианта первого идентификатора, связанного с первым устройством аутентификации, извлечения первого сигнала аутентификации и первого рисунка, связанного с первым идентификатором, обнаружения на емкостном сенсорном экране по меньшей мере двух точек ввода, создаваемых наложением второго устройства аутентификации на емкостной сенсорный экран, определения второго рисунка в зависимости от обнаруженных точек ввода, приема второго сигнала аутентификации с помощью приемника, аутентификации первого идентификатора, если второй сигнал аутентификации равен первому сигналу аутентификации и если второй рисунок равен первому рисунку.

В соответствии с одним дополнительным вариантом осуществления изобретения, этап определения второго рисунка включает в себя этап вычисления по меньшей мере одного расстояния между точками ввода, обнаруженными на емкостном сенсорном экране.

Настоящее изобретение также относится к компьютерной программе, которая может храниться на носителе данных и/или загружаться из сети передачи данных с целью считывания и исполнения процессором или реализации в микроконтроллере. Такая компьютерная программа содержит инструкции для реализации вышеупомянутого способа в соответствии с одним или более из его вариантов. Изобретение также относится к средству хранения данных, содержащему такую компьютерную программу.

Вышеупомянутые характеристики изобретения, а также другие характеристики станут более понятными после прочтения нижеследующего описания иллюстративного варианта осуществления, причем данное описание приводится применительно к прилагаемым чертежам, на которых:

- фиг. 1 схематически иллюстрирует штемпельную подушечку, известную на предшествующем уровне техники;
- фиг. 2 схематически иллюстрирует пример внешнего вида устройства аутентификации в соответствии с одним вариантом осуществления настоящего изобретения;
- фиг. 3 схематически иллюстрирует систему в соответствии с одним вариантом осуществления изобретения;
- фиг. 4 схематически иллюстрирует пример архитектуры аппаратных средств устройства аутентификации в соответствии с одним вариантом осуществления изобретения;
- фиг. 5 представляет собой структурную схему способа выдачи сигнала аутентификации в соответствии с одним вариантом осуществления изобретения;
- фиг. 6 схематически иллюстрирует пример внешнего вида устройства аутентификации в соответствии с дополнительным вариантом осуществления настоящего изобретения;
- фиг. 7 представляет собой вид снизу устройства аутентификации в соответствии с дополнительным вариантом осуществления изобретения, изображенным на фиг. 6;
- фиг. 8 схематически иллюстрирует пример архитектуры аппаратных средств

устройства аутентификации в соответствии с дополнительным вариантом осуществления изобретения, изображенным на фиг. 6;

- фиг. 9 представляет собой структурную схему способа аутентификации с использованием устройства аутентификации в соответствии с дополнительным вариантом осуществления изобретения, изображенным на фиг. 6;

- фиг. 10 представляет собой вид в разрезе корпуса устройства аутентификации в соответствии с дополнительным вариантом осуществления настоящего изобретения;

- фиг. 11 является иллюстрацией части, предназначенной для встраивания в устройство аутентификации, изображенное на фиг. 10;

- фиг. 12 представляет собой вид в разрезе штырька, предназначенного для встраивания в устройство аутентификации, изображенное на фиг. 10.

Фиг. 2 схематически иллюстрирует пример внешнего вида устройства аутентификации в соответствии с одним вариантом осуществления настоящего изобретения. В соответствии с данным вариантом осуществления, внешний вид устройства 200 аутентификации очень сходен со штемпельной подушечкой 100.

При этом устройство 200 аутентификации может состоять из ручки 220 и части 210, именуемой «штемпелем», сходным по своей форме со штемпелем 110 штемпельной подушечки 100. Ручка 220 может быть частично или полностью телескопической с целью размещения в ней механического импульсного регулятора REGM 410, который описывается ниже.

В соответствии с одним вариантом осуществления изобретения, устройство 200 аутентификации содержит устройство 230 считывания отпечатков пальцев, например, расположенное наверху ручки 220, чтобы без труда применяться пользователем, который может помещать на него свои пальцы, как правило, свой большой палец.

В соответствии с одним вариантом осуществления изобретения, устройство 200 аутентификации не имеет средства открытия или разборки после сборки или изготовления.

В соответствии с одним вариантом осуществления изобретения, устройство 200 аутентификации имеет внешний интерфейс обмена данными, например, USB-порт (порт универсальной последовательной шины) или беспроводной интерфейс типа связи ближнего поля (NFC), не представленный в данном документе, позволяющий, например, конфигурировать его. В качестве альтернативы, устройство 200 аутентификации не имеет внешнего интерфейса обмена данными. В этом случае конфигурирование устройства 200 аутентификации, то есть, внутренних компонентов устройства 200 аутентификации, описываемых ниже, может осуществляться до полной сборки корпуса устройства 200 аутентификации и, например, сварки.

Фиг. 3 схематически иллюстрирует систему в соответствии с одним вариантом осуществления изобретения, причем система состоит из первого устройства 200 аутентификации, описанного выше, второго устройства TAB 310, выполненного с возможностью приема сигнала аутентификации, излучаемого упомянутым первым устройством 200 аутентификации, и сервера SRV 320, причем упомянутый сервер SRV 320 содержит базу данных BDD 330 или выполнен с возможностью доступа к ней. При этом, в соответствии с данным вариантом осуществления изобретения, устройство TAB 310, как правило, представляет собой цифровой планшет или интеллектуальный телефон (смартфон), исполняющий приложение, обеспечивающее безбумажное управление подписями или сигналами аутентификации. Предпочтительно, устройство TAB 310 может представлять собой цифровой планшет или смартфон, повсеместно имеющийся в продаже, если, например, устройство 200 аутентификации излучает звуковой сигнал

аутентификации. В действительности для регистрации такого сигнала аутентификации при этом используется микрофон устройства TAB 310.

В соответствии с одним возможным сценарием применения устройства 200 аутентификации, устройство TAB 310 используется для приема подписи, например, если это устройство используется почтальонами, которые доставляют почтовое отправление в ответ на подпись получателя, использующего устройство 200 аутентификации. Приложение на устройстве TAB 310 позволяет устройству TAB 310 услышать возможный звуковой сигнал аутентификации (звуковой сигнал, возможно, излучаемый в ультразвуковом диапазоне). Пользователь устройства 200 аутентификации выполняет жест использования классической штемпельной подушечки 100 над устройством TAB 310, причем данный жест обеспечивает, как описывается ниже, включение устройства 200 аутентификации и излучение звукового сигнала аутентификации. Этот звуковой сигнал аутентификации может иметь низкую интенсивность, поскольку устройство 200 аутентификации имеет слабые энергетические ресурсы, но также и с целью сохранения конфиденциальности излучения звукового сигнала аутентификации, который при этом сложнее зарегистрировать на большом расстоянии. Иными словами, звуковой сигнал аутентификации низкой интенсивности гарантирует более высокую конфиденциальность, но требует близости - во время излучения указанного звукового сигнала - между устройством 200 аутентификации и устройством TAB 310. Устройство TAB 310, принимающее через микрофон звуковой сигнал аутентификации, вычисляет первый бит информации, содержащий, например, идентификатор устройства 200 аутентификации, и отправляет на сервер SRV 320 запрос, содержащий этот первый бит информации. Сервер SRV 320 на основе принятого первого бита информации опрашивает базу BDD 330 данных и извлекает один или более битов идентификационной информации, связанной с первым битом информации. Сервер SRV 320 отправляет эту идентификационную информацию в устройство TAB 310, которое при этом позволяет приложению, исполняемому устройством TAB 310, расписаться в получении клиентом письма с помощью устройства 200 аутентификации.

Фиг. 4 схематически иллюстрирует пример архитектуры аппаратных средств устройства 200 аутентификации в соответствии с одним вариантом осуществления изобретения. В данном варианте осуществления устройство 200 аутентификации содержит механический импульсный регулятор REGM 410, электромеханический преобразователь TRAN 420, модуль 450 электропитания, микроконтроллер 460 и, возможно, передатчик EMET 430. На фиг. 4 стрелка 405 обозначает размещение устройства 200 аутентификации при перемещении, создаваемом, например, пользователем. Размещение устройства 200 аутентификации при перемещении может осуществляться пользователем, держащим устройство 200 аутентификации за ручку 220, как описано выше, и выполняющим жест, сходный с жестом «резинового штампования», используемым со штемпельной подушечкой 100.

Механический импульсный регулятор REGM 410 представляет собой механическое устройство, способное преобразовывать жест или размещение устройства 200 аутентификации при перемещении потенциально случайного характера в механический импульс с заданными характеристиками во время каждого применения устройства 200 аутентификации пользователем. Преобразование размещения при перемещении в механический импульс с заданными характеристиками может предполагать промежуточную стадию накопления и сохранения механической энергии, связанной с размещением при перемещении. Например, механический импульсный регулятор REGM 410 способен генерировать постоянный механический импульс, соответствующий

взведению - жестом размещения устройства 200 аутентификации при перемещении пользователем - и затем освобождению ударника, установленного, например, на пружине. При этом механическим импульсным регулятором REGM 410 генерируется постоянный механический импульс, сопровождающий размещение при перемещении одним жестом или множеством жестов пользователя устройства 200 аутентификации, например, одним или более из нажатий устройства 200 аутентификации на твердую поверхность, такую как устройство TAB 310. Размещение при перемещении может осуществляться с использованием жеста, сходного с использованием штемпельной подушечки 100, например, прижатием устройства 200 аутентификации к устройству TAB 310, причем механический импульсный регулятор REGM 410 способен преобразовывать это прижатие - потенциально различной длительности или давления - в равномерный механический импульс, то есть, в одну из общих постоянных характеристик. Иными словами, характеристики механического импульса на выходе механического импульсного регулятора REGM 410 в целом сходны во время каждого применения устройства 200 аутентификации.

В соответствии с еще одним дополнительным или альтернативным вариантом осуществления изобретения, размещение устройства 200 аутентификации при перемещении осуществляется путем прямолинейного перемещения, например, по оси ручки 220, причем данное перемещение, возможно, включает в себя перемещения вперед-назад. Механический импульсный регулятор REGM 410 может содержать качающийся грузик. Размещение устройства 200 аутентификации при перемещении обеспечивает размещение качающегося грузика при перемещении и взведение пружины, накапливающей механическую энергию. В данном варианте осуществления устройство 200 аутентификации содержит детектор (не показан), такой как переключатель, расположенный на так называемой штемпельной части 210 устройства 200 аутентификации. Детектор способен обнаруживать нажатие устройства 200 аутентификации на поверхность, такую как поверхность устройства TAB 310, и освобождать ударник, тем самыми освобождая механический импульс при прижатии устройства 200 аутентификации к устройству TAB 310. Детектор, такой как переключатель, при этом способен обеспечивать нахождение устройства 200 аутентификации на близком расстоянии от устройства TAB 310, чтобы обеспечивать обмен звуковыми сигналами. Как и в предыдущем случае, характеристики механического импульса на выходе механического импульсного регулятора REGM 410 в целом сходны во время каждого применения устройства 200 аутентификации.

Электромеханический преобразователь TRAN 420 принимает на своем входе механический импульс с выхода механического импульсного регулятора REGM 410. Электромеханический преобразователь TRAN 420 представляет собой устройство типа электрического генератора, способное преобразовывать механический импульс, принимаемый на его входе, в электрический импульс. Электромеханический преобразователь TRAN 420, например, может представлять собой электромеханический преобразователь пьезоэлектрического типа, реализующий так называемый «прямой» пьезоэлектрический эффект с целью преобразования механического импульса в электрический импульс. Электромеханический преобразователь TRAN 420 может при этом являться керамическим или пьезоэлектрическим композитом. Электромеханический преобразователь TRAN 420 может также представлять собой динамоэлектрическую машину, называемую микро-динамо, или альтернатор. Электромеханический преобразователь TRAN 420 при этом способен преобразовывать механическую энергию в электрическую энергию с целью - как объяснялось выше - подачи электрической

энергии в микроконтроллер. Выходом электромеханического преобразователя TRAN 420 при этом является электрический импульс, соответствующий механическому импульсу, принимаемому на входе.

Модуль 450 электропитания принимает электрический импульс, генерируемый электромеханическим преобразователем TRAN 420. Модуль 450 электропитания имеет функциональности преобразования электрического импульса, принимаемого на входе модуля 450 электропитания, в электропитание с возможностью питания микроконтроллера 460. Модуль 450 электропитания способен выдерживать скачки электрического тока, связанные с поступлением электрической энергии, в форме электрических импульсов, поступающих от электромеханического преобразователя TRAN 420, и накапливать эту электрическую энергию с целью передачи ее в микроконтроллер 460 с напряжением, адаптированным под микроконтроллер 460, в течение интервала времени, достаточного для исполнения микроконтроллером 460 инструкций, необходимых для процесса излучения сигнала аутентификации.

В соответствии с одним конкретным вариантом осуществления изобретения, модуль электропитания содержит контроллер CONT 451 электрического сигнала, выпрямитель RECT 452 электрических импульсов, накопитель ACCU 453 электрической энергии, формирователь COND 454 потока электрической энергии и регулятор REGE 455 потока электрической энергии. Контроллер CONT 451 электрического сигнала принимает на своем входе электрический импульс, обеспечиваемый электромеханическим преобразователем TRAN 420, и передает его в выпрямитель RECT 452 электрических импульсов. Выпрямитель RECT 452 электрических импульсов способен преобразовывать электрический сигнал, соответствующий принимаемому электрическому импульсу, который является переменным сигналом, в положительный или выпрямленный сигнал. Выпрямитель RECT 452 электрических импульсов может содержать электрический выпрямитель или преобразователь переменного тока в постоянный. Накопитель ACCU 453 электрической энергии принимает электрический сигнал, выпрямленный выпрямителем RECT 452 электрических импульсов, и обеспечивает сохранение электрической энергии, соответствующей принимаемому электрическому сигналу. Накопитель ACCU 453 электрической энергии может, например, содержать конденсатор или заряжаемую батарею. Электрическая энергия при этом сохраняется временно или постоянно в зависимости от технологии, используемой накопителем ACCU 453 электрической энергии. Формирователь COND 454 потока электрической энергии способен управлять электрической энергией, хранящейся в накопителе ACCU 453 электрической энергии, то есть, освобождать эту накопленную энергию при выполнении одного или более из заданных условий. Например, формирователь COND 454 потока электрической энергии может содержать детектор электрического напряжения на выводах накопителя ACCU 453 электрической энергии и формировать освобождение хранящейся электрической энергии по достижении определенного электрического напряжения. При этом регулятор REGE 455 потока электрической энергии принимает электрическую энергию, хранящуюся в накопителе ACCU 453 электрической энергии, только в том случае, если, например, эта энергия сохранена в достаточно большом количестве. Представление об энергии, сохраненной накопителем ACCU 453 электрической энергии, может быть получено, например, путем измерения напряжения на выводах накопителя ACCU 453 электрической энергии. При этом, в соответствии с одним вариантом осуществления изобретения, регулятор REGE 455 потока электрической энергии принимает электрическую энергию, хранящуюся в накопителе ACCU 453 электрической энергии, только в том случае, если напряжение на выводах

накопителя ACCU 453 электрической энергии больше заданной величины. Регулятор REGE 455 потока электрической энергии имеет функцию формирования электрической энергии, принимаемой до своего микроконтроллера 460, с целью снабжения последнего электрической энергией. Формирование может предполагать, например, согласование напряжения электропитания микроконтроллера 460. Фактически, с целью надлежащего функционирования может потребоваться снабжение микроконтроллера 460 при некотором напряжении. При этом устройства 453, 455 и 456 позволяют обеспечивать сохранение достаточного количества энергии в накопителе ACCU 453 электрической энергии для снабжения микроконтроллера 460, причем эта электрическая энергия формируется перед снабжением микроконтроллера 460 регулятором REGE 455 потока электрической энергии. Модуль питания при этом позволяет снабжать микроконтроллер 460 в течение некоторого периода времени и при заданных характеристиках (таких как входное напряжение микроконтроллера 460).

Микроконтроллер 460 представляет собой электронное устройство, содержащее программируемый блок обработки данных (центральный процессор) CPU 461, оперативное запоминающее устройство RAM 462, энергонезависимую память или модуль хранения ROM 463 и один или более интерфейсов ввода-вывода E/S 464. Интерфейсы E/S 464 могут содержать аналого-цифровые (CAN) или цифро-аналоговые (CNA) преобразователи сигналов, которые могут содержать модуль широтно-импульсной модуляции (PWM). При электрическом включении модулем 450 питания микроконтроллер 460 выполнен с возможностью генерирования излучения первого электрического сигнала на выходе интерфейса E/S 464, причем первый электрический сигнал соответствует излучаемому сигналу аутентификации.

В соответствии с альтернативными вариантами осуществления, функциональности микроконтроллера 460 реализуются программируемой логической схемой (программируемыми пользователем вентильными матрицами - FPGA), цифровым сигнальным процессором (DSP), специализированной интегральной схемой (ASIC) или любым иным эквивалентным устройством.

В соответствии с одним конкретным вариантом осуществления, упомянутый интерфейс E/S 464 соединен с передатчиком EMET 430, который при этом излучает сигнал аутентификации. В зависимости от характера передатчика EMET 430 это может быть сигнал звукового типа (например, передатчик EMET 430 типа громкоговорителя), визуального типа (например, передатчик EMET 430 типа светодиода) или любого иного типа.

В соответствии с одним вариантом осуществления изобретения, передатчик EMET 430 представляет собой передатчик, совместимый с технологиями радиосвязи, такими как Bluetooth, связь ближнего поля (NFC) или радиочастотная идентификация (RFID). В соответствии с одним дополнительным вариантом осуществления, передатчик EMET 430 представляет собой приемопередатчик, то есть, он может также принимать сигнал и обеспечивает возможность двусторонней связи.

При этом сигнал аутентификации предназначен для приема устройством TAB 310, которое содержит средство приема, адаптированное к принимаемому сигналу, например, микрофон в случае звукового сигнала аутентификации. Использование сигнала аутентификации звукового типа при этом обеспечивает широкую совместимость применений устройства 200 аутентификации с устройствами TAB 310, которые весьма часто содержат микрофон.

В соответствии с одним дополнительным вариантом осуществления, заданный бит информации записывается в энергонезависимой памяти ROM 463 микроконтроллера

460. Эта информация может записываться в памяти в ходе изготовления устройства 200 аутентификации или на более поздней стадии конфигурирования устройства 200 аутентификации, например, с помощью не показанного интерфейса программирования. Заданная информация может содержать несколько бит информации, например, идентификатор устройства 200 аутентификации или ключ шифрования.

В соответствии с одним вариантом осуществления, энергонезависимая память ROM 463 - неперезаписываемого типа, и, следовательно, невозможно изменить или стереть заданную информацию после ее записи.

Необходимо отметить, что в соответствии с одним вариантом осуществления в указанную энергонезависимую и неперезаписываемую память ROM 463 записывается программа, содержащая рабочие инструкции микроконтроллера. Это позволяет защищаться от любого изменения режима работы устройства 200 аутентификации. При этом, когда микроконтроллер 460 включается модулем 450 питания, микроконтроллер 460 может быть выполнен с возможностью извлечения заданной информации, записанной в модуле памяти или хранения ROM 463, и генерирования по этой заданной информации излучения первого электрического сигнала, соответствующего излучаемому сигналу аутентификации.

В соответствии с одним вариантом осуществления, микроконтроллер 460 при каждом использовании увеличивает на один содержимое первого счетчика, значение которого может сохраняться в памяти ROM 463. Электрический сигнал может генерироваться по значению этого первого счетчика, увеличиваться на один во время каждого использования и по идентификатору и ключу шифрования включаться в заданную информацию. При этом первый электрический сигнал во время каждого использования является различным, а, следовательно, и излучаемый сигнал аутентификации, что уменьшает возможности атаки типа атаки повторением в системе, состоящей из устройства 200 аутентификации, устройства TAB 310 и сервера SRV 320. С этой целью устройство TAB 310 может сохранять в памяти последнее значение, принимаемое от первого счетчика, и после приема нового сигнала аутентификации устанавливать, что новое значение, принимаемое от первого счетчика, в действительности отличается от предыдущего значения, хранящегося в памяти, или превышает его. В случае первого счетчика, значение которого увеличивается на один после каждого излучения сигнала аутентификации устройством 200 аутентификации, если принимаемое значение первого счетчика принимаемого сигнала аутентификации меньше или равно значению, ранее сохраненному в памяти устройством TAB 310, это означает, что упомянутый принимаемый сигнал аутентификации является сигналом аутентификации повторения; устройство TAB 310 в этом случае должно запретить аутентификацию.

В соответствии с одним конкретным вариантом осуществления настоящего изобретения, электромеханический преобразователь TRAN 420 представляет собой электромеханический преобразователь пьезоэлектрического типа. Указанный электромеханический преобразователь TRAN 420 при этом также часто используется в качестве передатчика EMET 430 для выдачи сигнала аутентификации, причем сигнал аутентификации - звукового типа. В соответствии с данным вариантом осуществления, модуль 450 питания соединен с электромеханическим преобразователем TRAN 420 и с микроконтроллером 460.

В данном варианте осуществления модуль 450 питания способен принимать электрический импульс, поступающий от электромеханического преобразователя TRAN 420 пьезоэлектрического типа, с целью генерирования электропитания микроконтроллера 460, одновременно защищая этот микроконтроллер от скачка

напряжения, и передавать первый электрический сигнал, излучаемый микроконтроллером, в электромеханический преобразователь TRAN 420 пьезоэлектрического типа, используемый в качестве передатчика EMET 430, с целью генерирования сигнала аутентификации звукового типа. В соответствии с более конкретным вариантом осуществления данного изобретения, именно контроллер электрического сигнала CONT 451 модуля 450 питания выполнен с возможностью приема электрического импульса, поступающего от электромеханического преобразователя TRAN 420, с целью генерирования электропитания, одновременно защищая микроконтроллер 460, и передачи первого электрического сигнала, поступающего от микроконтроллера 460, в электромеханический преобразователь TRAN 420, используемый в качестве передатчика EMET 430, с целью генерирования сигнала аутентификации звукового типа. Указанные последние варианты осуществления используют возможности пьезоэлектрического преобразователя, используемого в качестве альтернативы в так называемом «прямом» режиме (генерирование электрического напряжения под действием механической силы) или в так называемом «обратном» режиме (деформация пьезоэлектрического преобразователя при подаче на него электрического напряжения). Деформации электромеханического преобразователя TRAN 420 пьезоэлектрического типа при этом используются для генерирования звукового сигнала. Использование одного и того же элемента для двух различных функций (электромеханического преобразователя TRAN 420 и передатчика EMET 430) позволяет сократить расходы на изготовление и площадь устройства 200 аутентификации.

В соответствии с одним дополнительным вариантом осуществления изобретения, электромеханический преобразователь TRAN 420 пьезоэлектрического типа выполнен с возможностью регистрации звукового сигнала, соответствующего сообщению, и передачи в модуль 450 питания второго электрического сигнала, соответствующего звуковому сигналу, зарегистрированному электромеханическим преобразователем TRAN 420 пьезоэлектрического типа, причем модуль 450 питания выполнен с возможностью передачи в микроконтроллер 460 данного второго электрического сигнала, причем микроконтроллер 460 выполнен с возможностью обработки указанного второго электрического сигнала, соответствующего сообщению. Например, микроконтроллер 460 может генерировать третий электрический сигнал, соответствующий звуковому сигналу, для излучения или записи в память RAM 462 или ROM 463 бита информации, извлеченного из второго электрического сигнала или сообщения. Одно применение данной функциональности приема сообщения, связанного со вторым электрическим сигналом, описывается ниже для записи идентификационной информации пользователя в энергонезависимой памяти ROM 463.

В соответствии с одним дополнительным вариантом осуществления, устройство 200 аутентификации содержит устройство 230 считывания отпечатков пальцев. Данное устройство 230 считывания отпечатков пальцев обеспечивает возможность выдачи звукового сигнала аутентификации только при условии обнаружения одного или более из заданных отпечатков пальцев. Это позволяет обеспечивать дополнительную степень защиты, гарантируя, что пользователь имеет разрешение на его использование. При этом информация, соответствующая отпечаткам пальцев пользователей, имеющих разрешение на использование устройства 200 аутентификации, может быть записана ранее в энергонезависимой памяти ROM 463 на стадии изготовления или на более поздней стадии конфигурирования. Если во время использования устройства 200 аутентификации микроконтроллером 460 не извлечен ни один отпечаток,

соответствующий отпечатку, зарегистрированному в энергонезависимой памяти ROM 463, то процесс выдачи сигнала аутентификации останавливается без выдачи сигнала аутентификации. В соответствии с одним дополнительным вариантом осуществления изобретения, после этого вместо сигнала аутентификации выдается заданный сигнал, соответствующий коду ошибки. В соответствии с альтернативным вариантом осуществления изобретения, вместо сигнала аутентификации выдается случайный сигнал.

В соответствии с одним дополнительным вариантом осуществления изобретения, данные, соответствующие отпечатку пальца, считанному устройством 230 считывания отпечатков пальцев, содержатся в сигнале аутентификации, излучаемом устройством 200 аутентификации. Функциональность установления отпечатка пальца на основе данных, соответствующих считанному отпечатку пальца, может при этом быть перенесена в устройство TAB 310 или в сервер SRV 320.

В соответствии с одним вариантом осуществления изобретения, устройство 200 аутентификации содержит первый индикатор, который загорается, когда электрическая энергия, накопленная модулем 450 питания, достаточна для питания микроконтроллера 460. Первый индикатор при этом обеспечивает информацию, указывающую, является ли энергия, накопленная модулем 450 питания, достаточной. При этом, когда при следовании одного или более перемещений устройства 200 аутентификации светодиод не загорается, пользователь устройства 200 аутентификации знает, что устройство 200 аутентификации неспособно излучать сигнал аутентификации, что побуждает его повторить свое перемещение.

Фиг. 5 представляет собой структурную схему способа выдачи сигнала аутентификации в соответствии с одним вариантом осуществления изобретения. Данный способ может осуществляться устройством, таким как устройство 200 аутентификации, описываемое в настоящем документе.

Первый этап INI 510 соответствует стадии инициализации устройства 200 аутентификации. Этот первый этап может выполняться во время изготовления устройства 200 аутентификации, и он предполагает запись в энергонезависимую память ROM 463 микроконтроллера 460 микропрограммы или компьютерной программы, содержащей инструкции для исполнения процесса излучения сигнала аутентификации. Этот первый этап может также включать в себя запись в энергонезависимую память ROM 463 заданного бита информации. Эта заданная информация может содержать уникальный идентификатор, связанный с устройством 200 аутентификации, и ключ шифрования. Заданная информация может также содержать любую информацию, обеспечивающую идентификацию пользователя устройства 200 аутентификации, например, наименование компании или пользователя. Если эта информация недоступна на стадии изготовления или инициализации устройства 200 аутентификации, можно записывать информацию на более поздней стадии с помощью процедуры, описываемой ниже.

Второй этап MOU 520 соответствует размещению устройства 200 аутентификации при перемещении пользователем. Это размещение при перемещении может удовлетворять некоторым ограничениям в зависимости от варианта осуществления настоящего изобретения. В одном предпочтительном варианте осуществления размещение при перемещении осуществляется с помощью жеста, сходного с жестом при использовании штемпельной подушечки 100.

Следующий этап IMPM 530 соответствует преобразованию перемещения или перемещений, применяемых к устройству 200 аутентификации во время предыдущего

этапа MOU 520, в механический импульс с заданными характеристиками. Это преобразование может осуществляться с помощью механического импульсного регулятора REGM 410, описанного выше.

Следующий этап IMPE 540 соответствует преобразованию упомянутого механического импульса в электрический импульс. Это преобразование может осуществляться с помощью электромеханического преобразователя TRAN 420, описанного выше.

На следующем этапе SIGE 550 по упомянутому электрическому импульсу генерируется электропитание с заданными характеристиками и с возможностью активации средств генерирования первого электрического сигнала, соответствующего излучаемому сигналу аутентификации. Ранее описанный модуль 450 питания может выполнять этот этап SIGE 550.

На этапе SIGA 560 устройство 200 аутентификации излучает сигнал аутентификации на основе первого электрического сигнала, генерируемого во время предыдущего этапа. В соответствии с одним вариантом осуществления изобретения, передатчик EMET 430 излучает сигнал. В соответствии с еще одним вариантом осуществления изобретения, электромеханический преобразователь TRAN 420 является пьезоэлектрическим преобразователем и также используется для излучения звукового сигнала аутентификации.

В соответствии с одним вариантом осуществления изобретения, в тех случаях, когда необходимо утвердить конфигурацию устройства 200 аутентификации после стадии изготовления, например, выдать часть заданной информации, записанной в энергонезависимой памяти ROM 463, которая содержит идентификационную информацию пользователя, можно использовать возможности приема звукового сигнала электромеханическим преобразователем TRAN 420 пьезоэлектрического типа. При этом в ответ на излучение устройством 200 аутентификации сигнала аутентификации устройство TAB 310 излучает звуковой сигнал, соответствующий сообщению, содержащему бит идентификационной информации, который регистрируется электромеханическим преобразователем TRAN 420 пьезоэлектрического типа. Сообщение, соответствующее этому звуковому сигналу, принимается в форме электрического сигнала и обрабатывается микроконтроллером 460. Микроконтроллер 460 извлекает из сообщения идентификационную информацию пользователя и записывает эту информацию вместе с заданной информацией в энергонезависимой памяти ROM 463. В соответствии с одним вариантом осуществления изобретения, вся энергонезависимая память ROM 463 или ее часть является неперезаписываемой, то есть, информацию, записанную в энергонезависимую память ROM 463, невозможно впоследствии изменить или стереть.

В соответствии с одним дополнительным вариантом осуществления изобретения, устройство TAB 310 излучает звуковой сигнал, соответствующий сообщению, содержащему бит идентификационной информации, причем сообщение также содержит значение, соответствующее второму счетчику. Микроконтроллер 460 извлекает из сообщения это значение для второго счетчика и записывает его в перезаписываемую часть энергонезависимой памяти ROM 463. Значение этого второго счетчика соответствует ограничению числа применений устройства 200 аутентификации для генерирования сигнала аутентификации. При этом во время каждого генерирования сигнала аутентификации устройство 200 аутентификации уменьшает на единицу значение второго счетчика, записанное в энергонезависимой памяти ROM 463. Когда значение второго счетчика достигает заданного значения, например, нуля, устройство 200

аутентификации блокируется, предотвращая любое дальнейшее генерирование сигнала аутентификации. Иными словами, во время этапа генерирования сигнала аутентификации микроконтроллер 460 извлекает значение второго счетчика и сравнивает его с заданным значением. Если значение второго счетчика меньше заданного значения или, возможно, равно ему, то микроконтроллер отменяет генерирование сигнала аутентификации, возможно, генерируя вместо него заданный сигнал ошибки или случайный сигнал. При этом необходимо заново начинать процедуру инициализации значения второго счетчика устройством TAB 310 для повторной активации устройства 200 аутентификации, причем повторная активация пригодна для ряда применений, то есть, генерирований сигнала аутентификации в зависимости от нового значения второго счетчика. Иными словами, устройство 200 аутентификации записывает в энергонезависимую память ROM 463 значение, соответствующее второму счетчику, и уменьшает на единицу это значение при каждом применении устройства 200 аутентификации для генерирования сигнала аутентификации. Устройство 200 аутентификации блокирует генерирование сигнала аутентификации, когда значение второго счетчика достигает заданного значения.

В соответствии с дополнительным вариантом осуществления, устройство 200 аутентификации содержит модуль типа тактовой синхронизации (не представлен), соединенный с микроконтроллером 460 или встроенный в него. Этот модуль тактовой синхронизации может содержать батарею или элемент, обеспечивающий ему энергонезависимость. Например, литиевая батарея может обеспечивать эксплуатационный ресурс модуля тактовой синхронизации порядка от десяти до двадцати лет. Модуль тактовой синхронизации снабжает микроконтроллер 460 временной информацией, такой как время или дата. Микроконтроллер 460 может использовать эту временную информацию, поступающую от модуля тактовой синхронизации, для генерирования первого электрического сигнала, соответствующего сигналу аутентификации. Кроме того, информация типа времени или даты может записываться в энергонезависимую память ROM 463. Эта информация может записываться в части энергонезависимой памяти ROM 463, которая является перезаписываемой, или, наоборот, в части энергонезависимой памяти ROM 463, которая является неперезаписываемой. В первом случае микроконтроллер 460 может обновлять эту информацию на основе принимаемого сообщения. Эта информация позволяет контролировать функционирование устройства 200 аутентификации. При этом микроконтроллер 460 может вводить этап установления даты или текущего времени с целью генерирования выдачи сигнала аутентификации. Если дата или текущее время, соответствующее временной информации, поступающей от модуля тактовой синхронизации, не соответствует заданным критериям, зависящим от информации о времени и дате, записанной в энергонезависимой памяти ROM 463, микроконтроллер 460 отменяет или блокирует выдачу сигнала аутентификации. В соответствии с одним сценарием использования, устройство 200 аутентификации при этом содержит дату, записанную в энергонезависимой памяти ROM 463, за пределами которой микроконтроллер 460 будет блокировать выдачу сигнала аутентификации. Данный сценарий при этом позволяет проверять срок службы устройства 200 аутентификации, отключая его после определенной даты. В соответствии с еще одним дополнительным сценарием, выдача сигнала аутентификации разрешается только в определенные дни, например, с понедельника по пятницу или в определенные интервалы времени, например, в рабочее время. В соответствии с еще одним дополнительным сценарием использования, устройство 200 аутентификации генерирует различный сигнал аутентификации в зависимости от временной информации, поступающей от модуля тактовой

синхронизации. При этом первый сигнал аутентификации может выдаваться в течение первого временного интервала, соответствующего, например, первому идентификатору, а второй сигнал аутентификации - за пределами этого первого временного интервала, соответствующего второму идентификатору. Кроме того, временная информация, поступающая от модуля тактовой синхронизации, может шифроваться с использованием ключа шифрования устройства 200 аутентификации и встраиваться в выдаваемый сигнал аутентификации. В соответствии с одним вариантом осуществления изобретения, сервер SRV 320 может проверять достоверность сигнала аутентификации, передаваемого путем использования передаваемой зашифрованной временной информации. Например, сервер SRV 320 может проверять достоверность сигнала аутентификации, если рассогласование между локальным временем сервера SRV 320 и принимаемой зашифрованной временной информацией меньше заданной величины.

В соответствии с альтернативным вариантом осуществления изобретения, устройство 200 аутентификации содержит приемник (не представлен). Данный приемник может быть, например, типа фотоэлектрического элемента, и, следовательно, он может регистрировать или принимать световой сигнал. Такой фотоэлектрический элемент может представлять собой, например, диодный приемник, фотодиод или фототранзистор. Этот приемник соединен с микроконтроллером 460 и позволяет передавать на него электрический сигнал, соответствующий принимаемому световому сигналу. Этот приемник может использоваться в качестве альтернативы электромеханическому преобразователю TRAN 420 пьезоэлектрического типа для единственной функции приема сигнала в вариантах осуществления, в которых устройство TAB 310 излучает сигнал светового типа, а не звуковой сигнал.

В соответствии с одним дополнительным вариантом осуществления изобретения, приемник является передатчиком EMET 430, то есть, передатчик EMET 430 является приемопередатчиком.

В соответствии с одним дополнительным вариантом осуществления настоящего изобретения, микроконтроллер 460 генерирует первый электрический сигнал на основе информации, содержащейся в ранее принятом сообщении. Как правило, это может быть информация типа «отдельного жетона». В соответствии с данным вариантом осуществления изобретения, сообщение может приниматься посредством звукового сигнала, регистрируемого электромеханическим преобразователем TRAN 420 пьезоэлектрического типа, или посредством светового сигнала, принимаемого приемником, способным регистрировать световые сигналы. Информация, содержащаяся в сообщении, может извлекаться микроконтроллером и шифроваться путем использования ключа шифрования, записанного в энергонезависимой памяти ROM 463, с целью генерирования сигнала аутентификации. При этом устройство TAB 310, принимающее сигнал аутентификации, или сервер SRV 320, на который должен передаваться сигнал аутентификации, может проверять аутентичность устройства 200 аутентификации путем установления того, что ключ шифрования, используемый устройством 200 аутентификации, действительно является ключом шифрования, связанным с устройством 200 аутентификации. В данном варианте осуществления информация, содержащаяся в сообщении, представляет собой информацию типа «отдельного жетона», при этом процесс аутентификации устройства 200 аутентификации предполагает, например, этапы:

- предварительного сопоставления сервером SRV 320 идентификатора устройства 200 аутентификации с ключом шифрования, причем идентификатор и ключ шифрования записываются в базу данных BDD 330 и записываются в энергонезависимую память

ROM 463 на стадии изготовления и инициализации устройства 200 аутентификации,

- отправки устройством 200 аутентификации первого сигнала в устройство TAB 310, причем указанный первый сигнал может являться сигналом аутентификации, генерируемым без шифрования какого-либо отдельного жетона, или любым иным заданным сигналом, информирующим устройство TAB 310, что отдельный жетон должен быть отправлен в устройство 200 аутентификации для генерирования сигнала аутентификации,
- приема устройством TAB 310 первого сигнала,
- отправки устройством TAB 310 в сервер SRV 320 запроса на отдельный жетон,
- отправки отдельного жетона сервером SRV 320 в устройство TAB 310,
- приема устройством TAB 310 отдельного жетона,
- передачи устройством TAB 310 светового или звукового сообщения в зависимости от варианта осуществления изобретения в устройство 200 аутентификации, причем сообщение содержит отдельный жетон,
- приема устройством 200 аутентификации сообщения и генерирования в ответ сигнала аутентификации, содержащего идентификатор устройства 200 аутентификации и отдельный жетон, шифруемый с использованием ключа шифрования, извлеченного из энергонезависимой памяти ROM 463,
- приема устройством TAB 310 сигнала аутентификации и извлечения идентификатора и зашифрованного отдельного жетона, а затем передачи идентификатора и указанного зашифрованного отдельного жетона на сервер SRV 320,
- приема сервером SRV 320 зашифрованного отдельного жетона с помощью устройства 200 аутентификации и установления того, что принятый зашифрованный отдельный жетон соответствует отдельному жетону, извлеченному из базы данных BDD 330 и зашифрованному ключом шифрования, связанным с принятым идентификатором; если два шифрования отдельного жетона соответствуют друг другу, то сервер SRV 320 отправляет в устройство TAB 310 сообщение проверки достоверности, информирующее его, что аутентификация устройства 200 аутентификации прошла успешно; в противном случае сервер SRV 320 отправляет в устройство TAB 310 сообщение, информирующее его, что устройство 200 аутентификации не было аутентифицировано.

В соответствии с одним вариантом осуществления изобретения, предполагается, что звуковой сигнал, излучаемый устройством TAB 310, имеет также малую дальность. При этом обмен звуковыми сигналами малой дальности между устройством 200 аутентификации и устройством TAB 310 позволяет определять, находится ли устройство 200 аутентификации на надлежащем расстоянии от устройства TAB 310, чтобы устройство TAB 310 могло принимать сигнал аутентификации. Если устройство 200 аутентификации не принимает звуковой сигнал, излучаемый устройством TAB 310, устройство аутентификации определяет, что оно находится слишком далеко от устройства TAB 310. У пользователя может при этом быть запрошено повторение перемещения. В одном варианте осуществления устройство аутентификации содержит второе индикаторное устройство, например, светодиод, который загорается, когда после выдачи сигнала аутентификации устройство 200 аутентификации не принимает в ответ звуковой сигнал, излучаемый устройством TAB 310, что при этом означает, например, что оно находится слишком далеко от устройства TAB 310.

В соответствии с одним дополнительным вариантом осуществления настоящего изобретения, электромеханический преобразователь TRAN 420 - типа электроактивного полимера. Применение электромеханического преобразователя TRAN 420 типа

электроактивного полимера обеспечивает более высокий энергетический коэффициент полезного действия по сравнению с другими технологиями типа керамического или пьезоэлектрического композита, а также уменьшенные вес и площадь, обеспечивая изготовление более компактного и легковесного устройства 200 аутентификации. Кроме того, электромеханический преобразователь TRAN 420 типа электроактивного полимера, как правило, прочнее, чем электромеханический преобразователь из керамики, и позволяет создавать более сложные формы преобразователей, что предусматривает лучшую интеграцию в устройство 200 аутентификации и более широкий спектр форм для корпуса устройства 200 аутентификации. В действительности, ввиду пластичности электроактивных полимеров их можно формовать и печатать в любой требуемой форме.

В более общем смысле, применение электромеханического преобразователя типа электроактивного полимера обеспечивает упрощенную конструкцию устройства 200 аутентификации, в частности, благодаря интеграции некоторых или всех из механического импульсного регулятора REGM 410, электромеханического преобразователя TRAN 420 и передатчика EMET 430 и, следовательно, снижение расходов на изготовление устройства 200 аутентификации. Вследствие этого применение электроактивного полимера для изготовления пружин или упругих элементов, содержащихся в механическом импульсном регуляторе REGM 410, позволяет интегрировать функциональности электромеханического преобразователя TRAN 420 в механический импульсный регулятор REGM 410. Электромеханический преобразователь TRAN 420 и механический импульсный регулятор REGM 410 при этом образуют единый модуль. Аналогичным образом, функциональности передатчика EMET 430 также могут быть интегрированы в тот же модуль, вследствие этого обеспечивая механическое упрощение устройства 200 аутентификации. Это упрощение обеспечивает в конечном итоге снижение расходов на изготовление устройства 200 аутентификации.

Фиг. 6 схематически иллюстрирует пример внешнего вида устройства 600 аутентификации в соответствии с дополнительным вариантом осуществления настоящего изобретения. В соответствии с данным дополнительным вариантом осуществления изобретения, устройство 600 аутентификации содержит батарею вместо электромеханического механизма питания, состоящего из ранее описанных элементов 410, 420 и 450. Это позволяет упростить архитектуру устройства 200 аутентификации ценой потери энергоавтономности. Поскольку батарея нуждается в зарядке или замене, устройство 600 аутентификации может содержать люк для обеспечения доступа к батарее или порт для зарядки. В одном альтернативном варианте осуществления батарея не является доступной или заряжаемой, и, следовательно, устройство 600 аутентификации непригодно к использованию, когда батарея разрядилась. Последнее, в частности, позволяет контролировать использование устройства 600 аутентификации, обеспечивая уверенность в его продолжительности работы. При этом можно использовать емкость батареи, чтобы обеспечивать более длительный или более короткий период эксплуатации.

Устройство 600 аутентификации может быть визуально сходным с устройством 200 аутентификации, то есть, напоминать панель. Устройство 600 аутентификации содержит ручку 620, сходную с ручкой 220, и штемпель 610, сходный со штемпелем 210. Устройство 600 аутентификации отличается от устройства 200 аутентификации дополнительным наличием множества штырьков или столбиков, расположенных на одной поверхности устройства 600 аутентификации. Эти штырьки расположены на фиг. 6 под устройством 600 аутентификации, то есть, под штемпелем 610. Фиг. 6 представляет собой вид в

профиль устройства 600 аутентификации - представлены только три штырька 650, 660 и 670. Штырьки расположены таким образом, что они продолжаются за пределами штемпеля 610 под устройством 600 аутентификации, и таким образом, что концы штырьков лежат в одной и той же плоскости, параллельной основанию устройства 600 аутентификации. Иными словами, когда устройство 600 аутентификации размещается вертикально, как представлено на фиг. 6, плоскость, образуемая концами штырьков, горизонтальна. В соответствии с вариантом осуществления, изображенным на фиг. 6, штырьки состоят из гибкого материала. Например, штырьки изготовлены из резины, твердость которой составляет между 25 по Шору А и 75 по Шору А, например, 50 по Шору А (Шор А относится к шкале твердости по Шору для мягких материалов). Эта гибкость обеспечивает контакт штырьков с поверхностью экрана электронного устройства типа смартфона или планшета без риска повреждения экрана. По меньшей мере два штырька из множества штырьков состоят из электропроводящего материала (в дальнейшем в этом документе - «проводника»), остальные штырьки состоят из электроизолирующего материала. В соответствии с одним вариантом осуществления изобретения, указанные два материала имеют одинаковый внешний вид, чтобы предотвратить различение проводящих изолирующих штырьков пользователем визуально или на ощупь. При этом проводящий материал может представлять собой резину с углеродным наполнением, а изолирующий материал может представлять собой резину без углеродного наполнения, причем указанные два материала выбираются с одинаковой твердостью между 25 по Шору А и 75 по Шору А, например, 50 по Шору А.

В соответствии с одним вариантом осуществления изобретения, корпус устройства 600 аутентификации, то есть, ручка 620 и/или штемпель 610 покрыт или образован, по меньшей мере частично, электропроводящим материалом. Предпочтительно, ручка 620, являющаяся частью устройства 600 аутентификации, которую держит рукой пользователь, покрыта проводящим материалом. Электрическая непрерывность обеспечивается между частью устройства 600 аутентификации, покрытой проводящим материалом, и всеми штырьками, состоящими из проводящего материала. При этом, когда пользователь держит рукой устройство 600 аутентификации, штырьки, состоящие из проводящего материала, могут использоваться для взаимодействия с сенсорным экраном с помощью так называемой емкостной сенсорной технологии (в дальнейшем в этом документе - «емкостным сенсорным экраном»). Упомянутый материал, покрывающий устройство 600 аутентификации, может также быть гибким, чтобы избежать царапания экрана электронного устройства во время обращения с устройством 600 аутентификации. Материал, по меньшей мере частично покрывающий устройство 600 аутентификации, может представлять собой резину с твердостью между 40 по Шору А и 90 по Шору А, например, 65 по Шору А. В соответствии с одним вариантом осуществления изобретения, устройство 600 аутентификации полностью покрыто гибким материалом.

Устройство 600 аутентификации содержит по меньшей мере одно средство обнаружения давления, оказываемого на по меньшей мере один штырек. Например, штырек содержит на своей внутренней стороне переключатель, который активируется, когда указанный штырек нажимает на поверхность, такую как экран электронного устройства. Штырьки могут быть установлены на подвижной опоре внутри устройства 600 аутентификации с возвратной пружиной. Давление на штырьки может при этом запускать переключатель, соединенный с подвижной опорой.

Фиг. 7 представляет собой вид снизу устройства 600 аутентификации в соответствии

с дополнительным вариантом осуществления изобретения, изображенным на фиг. 6. Штырьки 650, 660 и 670 видны в профиль на фиг. 6. В соответствии с вариантом осуществления, изображенным на фиг. 7, устройство 600 аутентификации содержит девять штырьков 650, 660, 670, 751, 761, 771, 752, 762 и 772, расположенных «3 на 3». Число штырьков может быть различным, так же, как и их расположение. По меньшей мере два из этих штырьков состоят из электропроводящего материала. Остальные штырьки состоят из электроизолирующего материала. Штырьки, состоящие из проводящего материала, определяют геометрическую форму в горизонтальной плоскости. При этом можно определять периметр упомянутой геометрической формы, соответствующий расстоянию между штырьками, состоящими из проводящего материала. Может также быть определена площадь геометрической формы. Геометрическая форма может определяться углами, образуемыми линиями, соединяющими различные точки геометрической формы. Параметр, в дальнейшем в этом документе называемый «рисунком», может при этом определяться в зависимости от размещения штырьков, состоящих из проводящего материала. Рисунок может соответствовать периметру геометрической формы отдельно или в комбинации с другими атрибутами геометрической формы. Одна и та же геометрическая форма может быть образована различными штырьками. При этом, например, наличие только штырьков 752, 751, 650 и 660, состоящих из проводящего материала, в конечном итоге приводит к той же Г-образной геометрической форме, что и наличие штырьков 751, 761,771 и 772, выполненных таким образом, наряду с другими возможностями. Эти два выбора группы штырьков, состоящих из проводящего материала, в конечном итоге определяют один и тот же рисунок.

В соответствии с одним вариантом осуществления изобретения, штырьки, состоящие из проводящего материала, и штырьки, состоящие из изолирующего материала, визуально и тактильно одинаковы. При этом пользователь устройства 600 аутентификации не может различить, какие штырьки состоят из проводящего материала, просто взглянув на штырьки. Например, все штырьки состоят из резины с твердостью между 25 по Шору А и 75 по Шору А, например, 50 по Шору А. Резина, составляющая проводящие штырьки, кроме того, заполнена углеродом, чтобы сделать ее проводником электричества. При этом невозможно отличить проводящий штырек от изолирующего штырька по виду или на ощупь. При этом пользователь устройства 600 аутентификации не может узнать рисунок, соответствующий расположению штырьков, состоящих из проводящего материала, просто взглянув на штырьки. В более общем смысле, совокупность штырьков независимо от того, являются ли они проводящими или нет, вносит вклад в устойчивость устройства 600 аутентификации, когда оно установлено вертикально. Совокупность штырьков, состоящих из гибкого материала, также вносит вклад в амортизацию, когда устройство 600 аутентификации нажимает на сенсорный экран электронного устройства, что уменьшает риски царапания или повреждения упомянутого экрана.

Фиг. 8 схематически иллюстрирует пример архитектуры аппаратных средств устройства 600 аутентификации в соответствии с дополнительным вариантом осуществления изобретения, изображенным на фиг. 6. В данном варианте осуществления изобретения устройство 600 аутентификации содержит микроконтроллер 840, возможно, сходный с микроконтроллером 460. Устройство 600 аутентификации содержит батарею BATT 820, обеспечивающую электропитание для микроконтроллера 840. Устройство 600 аутентификации содержит передатчик EMET 830, причем передатчик EMET 830 обеспечивает излучение сигнала аутентификации.

В данном варианте осуществления изобретения устройство 200 аутентификации содержит детектор PRESS 810, такой как переключатель, расположенный на так называемой штемпельной части 610 устройства 200 аутентификации. Детектор PRESS 810, возможно, встроен внутри ранее описанных гибких штырьков. Детектор PRESS 810 позволяет обнаруживать нажатие устройства 200 аутентификации на поверхность, такую как емкостный сенсорный экран электронного устройства, такого как устройство TAB 310. Детектор PRESS 810, например, переключатель или нажимная кнопка, при этом позволяет обеспечивать нажатие устройства 600 аутентификации на устройство TAB 310. Обнаружение нажатия детектором PRESS 810 инициирует излучение устройством 600 аутентификации сигнала аутентификации. Это излучение может осуществляться только при условии одновременного обнаружения заданного отпечатка пальца устройством считывания отпечатков пальцев LECT 850.

Микроконтроллер 840 представляет собой электронное устройство, содержащее программируемый блок обработки данных (центральный процессор) CPU 841, оперативное запоминающее устройство RAM 842, энергонезависимую память или модуль хранения ROM 843 и один или более интерфейсов ввода-вывода E/S 844. Интерфейсы E/S 844 могут содержать аналого-цифровые (CAN) или цифро-аналоговые (CNA) преобразователи сигналов, которые могут содержать модуль широтно-импульсной модуляции (PWM). При электрическом включении батареей BATT 820 микроконтроллер 840 выполнен с возможностью генерирования излучения первого электрического сигнала на выходе интерфейса E/S 844, причем первый электрический сигнал соответствует сигналу аутентификации, излучаемому передатчиком EMET 830.

В соответствии с альтернативными вариантами осуществления, функциональности микроконтроллера 840 реализуются программируемой логической схемой (программируемыми пользователем вентильными матрицами - FPGA), цифровым сигнальным процессором (DSP), специализированной интегральной схемой (ASIC) или любым иным эквивалентным устройством.

В соответствии с одним конкретным вариантом осуществления, упомянутый интерфейс E/S 844 соединен с передатчиком EMET 830, который при этом излучает сигнал аутентификации. В зависимости от характера передатчика EMET 830 это может быть сигнал звукового типа (например, передатчик EMET 830 типа громкоговорителя), визуального типа (например, передатчик EMET 830 типа светодиода) или любого иного типа. Детектор PRESS 810 и/или устройство для чтения печатного текста LECT 850, возможно, соединены с микроконтроллером 840 посредством интерфейса E/S 844.

В соответствии с одним вариантом осуществления изобретения, передатчик EMET 830 представляет собой передатчик, совместимый с технологиями радиосвязи, такими как Bluetooth, связь ближнего поля (NFC), радиочастотная идентификация (RFID) или WiFi («Беспроводная достоверность»). В соответствии с одним дополнительным вариантом осуществления, передатчик EMET 830 представляет собой приемопередатчик, то есть, он может также принимать сигнал и обеспечивает возможность двусторонней связи.

При этом сигнал аутентификации предназначен для приема устройством, таким как устройство TAB 310, изображенное на фиг. 3, которое содержит средство приема, адаптированное к излучаемому сигналу, например, микрофон в случае звукового сигнала аутентификации. Использование сигнала аутентификации звукового типа при этом обеспечивает широкую совместимость применений устройства 600 аутентификации с электронными устройствами типа смартфона или планшета, которые почти всегда содержат микрофон.

Устройство 600 аутентификации содержит штырьки, описанные выше и не представленные на фиг. 8. Применение устройства аутентификации звукового типа в комбинации с рисунком, состоящим из проводящих штырьков, обеспечивает возможность совместного действия нескольких факторов. Действительно, с одной стороны, применение звукового сигнала аутентификации обеспечивает практическую бесконечность различных звуковых сигналов аутентификации, но оно имеет недостаток, состоящий в возможности захвата находящимися поблизости электронными устройствами. При этом, как правило, звуковой сигнал аутентификации, излучаемый устройством 600 аутентификации, может приниматься электронным устройством, расположенным в нескольких сантиметрах или нескольких метрах, в зависимости от чувствительности микрофона электронного устройства. С другой стороны, рисунки, состоящие из нескольких проводящих штырьков, имеют конечное число, тем не менее, чтобы быть обнаруженными электронным устройством, они требуют физического контакта между этим электронным устройством и устройством 600 аутентификации. Детектор PRESS 810, такой как переключатель или нажимная кнопка, при этом гарантирует, что сигнал аутентификации излучается только в том случае, когда устройство 600 аутентификации нажимает на сенсорный экран электронного устройства.

Иными словами, электронное устройство, которое ожидает аутентификации одним звуковым сигналом, может потенциально принять звуковой сигнал, предназначенный для другого электронного устройства. Комбинация аутентификации звуковым сигналом и штырьками при этом позволяет, например, запускать окно прослушивания (отверстие микрофона) только в том случае, когда рисунок обнаруживается электронным устройством, что снижает риск приема звукового сигнала, предназначенного для другого электронного устройства.

В соответствии с одним дополнительным вариантом осуществления, заданный бит информации записывается в энергонезависимой памяти ROM 843 микроконтроллера 840. Эта информация может записываться в памяти в ходе изготовления устройства 600 аутентификации или на более поздней стадии конфигурирования устройства 600 аутентификации, например, с помощью не показанного интерфейса программирования. Заданная информация может содержать несколько бит информации, например, идентификатор устройства 600 аутентификации или ключ шифрования.

В соответствии с одним вариантом осуществления, энергонезависимая память ROM 843 - неперезаписываемого типа, и, следовательно, невозможно изменить или стереть заданную информацию после ее записи.

Необходимо отметить, что в соответствии с одним вариантом осуществления в указанную энергонезависимую и неперезаписываемую память ROM 843 записывается программа, содержащая рабочие инструкции микроконтроллера. Это позволяет защищаться от любого изменения режима работы устройства 600 аутентификации. При этом, когда микроконтроллер 840 включается батареей BATT 820, микроконтроллер 840 может быть выполнен с возможностью извлечения заданной информации, записанной в модуле памяти или хранения ROM 843, и генерирования по этой заданной информации излучения первого электрического сигнала, соответствующего сигналу аутентификации, излучаемому передатчиком EMET 830.

В соответствии с одним дополнительным вариантом осуществления изобретения, устройство 600 аутентификации содержит устройство считывания отпечатков пальцев LECT 850. Указанное устройство считывания отпечатков пальцев LECT 850 позволяет выдавать звуковой сигнал аутентификации только при условии обнаружения одного или более из заданных отпечатков пальцев. Это позволяет обеспечивать дополнительную

степень защиты путем гарантирования того, что пользователь устройства 600 аутентификации имеет разрешение на его применение. При этом информация, соответствующая отпечаткам пальцев пользователей, имеющих разрешение на применение устройства 600 аутентификации, может быть предварительно записана в энергонезависимой памяти ROM 843 на стадии изготовления или на более поздней стадии конфигурирования. Если во время использования устройства 600 аутентификации микроконтроллером 840 не извлечен ни один отпечаток, соответствующий отпечатку, зарегистрированному в энергонезависимой памяти ROM 843, то процесс выдачи сигнала аутентификации останавливается без выдачи сигнала аутентификации. В соответствии с одним дополнительным вариантом осуществления изобретения, после этого вместо сигнала аутентификации выдается заданный сигнал, соответствующий коду ошибки. В соответствии с альтернативным вариантом осуществления изобретения, вместо сигнала аутентификации выдается случайный сигнал.

В соответствии с одним дополнительным вариантом осуществления изобретения, данные, соответствующие отпечатку пальца, считанному устройством считывания отпечатков пальцев LECT 850, содержатся в сигнале аутентификации, излучаемом устройством 600 аутентификации. Функциональность установления отпечатка пальца на основе данных, соответствующих считанному отпечатку пальца, может при этом быть перенесена в электронное устройство, такое как устройство TAB 310, или в сервер SRV 320, как показано на фиг. 3.

В соответствии с одним не описанным вариантом осуществления изобретения, можно создать устройство аутентификации, содержащее электромеханический механизм питания, как изложено в описании устройства 200 аутентификации. Такое устройство аутентификации может при этом обходиться без батареи BATT 820. Как отмечалось выше, устройство 200 аутентификации может содержать детектор. Детектор позволяет обнаруживать нажатие устройства 200 аутентификации на поверхность, такую как поверхность устройства TAB 310, и освобождать ударник, тем самым высвобождая механический импульс при нажатии устройства 200 аутентификации на устройство TAB 310. Детектор при этом представляет собой детектор PRESS 810, описанный выше. Предпочтительно детектор PRESS 810 при этом размещается в гибком штырьке и способен выполнять функцию освобождения ударника, в конечном итоге приводя к излучению сигнала аутентификации передатчиком EMET 830. Таким же образом, как и описано ранее, передатчик EMET 830 может быть пьезоэлектрического типа.

Фиг. 9 представляет собой структурную схему способа аутентификации с использованием устройства аутентификации в соответствии с дополнительным вариантом осуществления изобретения, изображенным на фиг. 6.

Устройство 600 аутентификации может применяться в системе, описанной на фиг. 3, таким же образом, как и устройство 200 аутентификации. Устройство TAB 310 исполняет специализированное приложение. Устройство TAB 310 содержит емкостный сенсорный экран и приемник. В соответствии с одним вариантом осуществления изобретения, приемник представляет собой микрофон. Упомянутое приложение обеспечивает возможность выбора идентификатора устройства 600 аутентификации из множества возможных идентификаторов. При этом каждый идентификатор соответствует однозначно определяемому устройству 600 аутентификации, причем каждое устройство 600 аутентификации соответствует, например, компании или пользователю, такому как торговая компания. Данный способ позволяет аутентифицировать идентификатор, выбираемый устройством 600 аутентификации, соответствующим данному идентификатору. В одном сценарии применения приложение

представляет собой приложение для управления доставкой почты, причем одно устройство 600 аутентификации связано с каждым получателем почты. Лицо, доставляющее эту почту, использует электронное устройство, такое как устройство TAB 310, чтобы пользователь и получатель почты проверили достоверность получения этой почты с помощью данного соответствующего устройства аутентификации. Устройство TAB 310 исполняет специализированное приложение.

Перед этапом 901 пользователь устройства TAB 310 исполняет приложение, обеспечивающее возможность аутентификации с помощью устройства 600 аутентификации. Пользователь выбирает, возможно, посредством графического интерфейса, представленного на экране устройства TAB 310, идентификатор, связанный с устройством 600 аутентификации. Идентификатор и устройство 600 аутентификации связаны с пользователем, личность которого, возможно, ранее была установлена. В соответствии с одним вариантом осуществления изобретения, выбор идентификатора осуществляется автоматически, например, путем взятия - в качестве идентификатора - идентификатора, соответствующего получателю почты, в момент передачи получателю. Устройство TAB 310 после этого извлекает в базе данных данные аутентификации, соответствующие аутентифицируемому идентификатору. Эти данные содержат сигнал аутентификации и рисунок, связанный с устройством 600 аутентификации. В соответствии с одним вариантом осуществления изобретения, данные аутентификации не содержат сам сигнал аутентификации, а содержат его отпечаток («хеш-сумму»).

Как только выбран идентификатор, приложение дожидается обнаружения вводимых данных на его емкостном сенсорном экране.

На этапе 901 по меньшей мере одни вводимые данные обнаруживаются на емкостном сенсорном экране устройства TAB 310. Это соответствует контактированию со всеми штырьками устройства 600 аутентификации на емкостном сенсорном экране устройства TAB 310. При этом обнаруживаются только штырьки, состоящие из проводящего материала. Электрическая непрерывность между штырьками, состоящими из проводящего материала, и корпусом устройства 600 аутентификации, состоящим из проводящего материала, обеспечивает возможность надлежащей работы емкостного сенсорного экрана, если корпус устройства 600 аутентификации находится в руке пользователя. Устройство 600 аутентификации, обнаруживающее контакт, создаваемый с емкостным сенсорным экраном устройства TAB 310, с помощью детектора PRESS 810, запускает сигнал аутентификации с помощью передатчика EMET 830. В соответствии с одним вариантом осуществления изобретения, передатчик EMET 830 представляет собой громкоговоритель, излучающий звуковой или ультразвуковой сигнал. Излучение может также быть возможным только при условии наличия заданного отпечатка пальца на устройстве считывания отпечатков пальцев LECT 850.

На этапе 920 устройство TAB 310 принимает сигнал аутентификации. С этой целью либо устройство TAB 310 постоянно находится в режиме прослушивания, либо обнаружение вводимых данных во время этапа 901 запускает стадию прослушивания на заданное время.

Как только принят сигнал аутентификации, на этапе 921 устройство TAB 310 декодирует сигнал аутентификации. Этот этап может быть необязательным, либо он может предполагать установление кода исправления ошибок. Этот этап может соответствовать вычислению «хеш-суммы» на основе сигнала аутентификации.

На этапе 910 устройство TAB 310 определяет рисунок в зависимости от геометрической формы, образуемой вводимыми данными, обнаруживаемыми на емкостном сенсорном экране. Рисунок может определяться расстоянием, вычисляемым

между различными вводимыми данными. Каждые вводимые данные на емкостном сенсорном экране соответствуют положению штырька, состоящего из проводящего материала.

Может выполняться необязательный этап 911 установления определенного рисунка.

На этапе 930 устройство TAB 310 устанавливает, что сигнал аутентификации, принимаемый во время этапа 920, фактически равен сигналу аутентификации определенного рисунка. С этой целью устройство TAB 310 сравнивает два сигнала аутентификации или, скорее, их «хеш-суммы».

В то же время устройство TAB 310 устанавливает, что рисунок, определяемый во время этапа 910, в действительности соответствует рисунку, связанному с идентификатором.

Если сигналы аутентификации (или их хеш-суммы) одинаковы, а рисунки соответствуют друг другу, то проверяется достоверность аутентификации (этап 940). В противном случае аутентификация объявляется недействительной (этап 950).

Вышеописанный способ может соответствовать сценарию управления картой лояльности торговой компанией. Карта постоянного покупателя после этого становится виртуальной и интегрированной в приложение. В этом сценарии каждый пользователь или покупатель имеет электронное устройство, такое как устройство TAB 310, исполняющее приложение для управления картой лояльности. Это приложение может предназначаться для торговой компании. С другой стороны, это приложение может обеспечивать возможность управления множеством программ лояльности множества торговых компаний. Покупатель, желающий проверить достоверность своей виртуальной карты лояльности, открывает приложение и при необходимости выбирает соответствующую торговую компанию. Указанная торговая компания после этого ставит штемпель на экране электронного устройства пользователя с помощью устройства 600 аутентификации. Обнаружение рисунка и прием звукового сигнала - причем оба они комбинируются и соответствуют торговой компании - обеспечивает возможность проверки достоверности «резинового штампования» приложением. После этого виртуальная карта лояльности может быть пополнена.

В соответствии с еще одним не представленным сценарием применения, устройство 600 аутентификации может обеспечивать возможность идентификации пользователя устройства 600 аутентификации, причем пользователь ранее был связан с устройством 600 аутентификации. При этом база данных может содержать списки, обеспечивающие возможность соотнесения пользователя (имя, фамилия и т.д.) и устройства 600 аутентификации (серийный номер).

Фиг. 10 представляет собой вид в разрезе корпуса 10 устройства 600 аутентификации в соответствии с дополнительным вариантом осуществления настоящего изобретения. В соответствии с данным дополнительным вариантом осуществления, устройство 600 аутентификации состоит из моноблочного корпуса 10, получаемого, например, формованием. Ручка 620 и штемпель 610 в этом случае представляют собой единую деталь. Корпус 10 состоит из гибкого материала, такого как резина, с твердостью между 40 по Шору А и 90 по Шору А с целью предотвращения царапания экрана при каком-либо контакте устройства 600 аутентификации с экраном электронного устройства. Корпус 10, например, состоит из резины с твердостью 65 по Шору А. Корпус 10 состоит из электропроводящего материала, такого как резина с твердостью 65 по Шору А, заполненного углеродом. Корпус 10 может иметь ось симметрии вокруг вертикальной оси, при этом устройство 600 аутентификации имеет «скругленную форму». Корпус 10 может иметь две плоскости симметрии в соответствии с двумя ортогональными

вертикальными плоскостями, имеющими на своем пересечении вертикальную ось корпуса 10, при этом устройство 600 аутентификации имеет «квадратную форму». Возможны и другие формы. Корпус 10 может быть полым, в частности, иметь две незаполненные зоны 16 и 17. В соответствии с одним вариантом осуществления, зона 16 предназначена для размещения микроконтроллера, такого как микроконтроллер 840. Микроконтроллер может быть выполнен в виде печатной схемы, которая имеет размер, адаптированный под прессовую посадку в канавку 15, предусмотренную в корпусе 10, чтобы зафиксировать ее в определенном месте. Печатная схема может содержать на своей нижней поверхности, то есть, поверхности, противоположной зоне 16, нажимную кнопку, такую как детектор PRESS 810. Передатчик, такой как передатчик 830, может быть прикреплен к печатной схеме или непосредственно интегрирован в печатную схему. Передатчик может представлять собой громкоговоритель размера, адаптированного под вставку внутрь корпуса 10. Аналогичным образом, пластина или опорная пластина может быть вставлена в канавку 12. Так называемая удерживающая пластина может быть вставлена в канавку 11. Такая так называемая удерживающая пластина изображена на фиг. 11 для случая «круглого» устройства 600 аутентификации. В случае устройства 600 аутентификации «квадратной» формы удерживающая пластина должна иметь внешний вид 610. Опорная пластина, возможно, изготовлена из электропроводящего материала. Опорная пластина, как правило, является металлической. В этом случае корпус 10 также изготавливается из электропроводящего материала, создается защита типа клетки Фарадея, позволяющая защищать печатную схему, а в более общем смысле любой микроконтроллер, расположенный внутри устройства 600 аутентификации, например, в зоне 16 или 17. Микроконтроллер при этом защищен от любых электромагнитных помех, что сохраняет его срок службы. Пластина или элемент, позволяющий закрывать клетку Фарадея, вставлен в канавку 20, чтобы закрывать клетку Фарадея в верхней части устройства 600 аутентификации. Этим элементом может являться устройство 630 считывания отпечатков пальцев, которое при этом идеально расположено на верхней части устройства 600 аутентификации. В качестве альтернативы, верхняя зона корпуса 10, в которой представлена канавка 20, является сплошной, то есть, отверстие в верхней части корпуса 10 отсутствует.

Зона 17 внутри корпуса 10 может содержать батарею, такую как батарея 820. Рассматриваемая зона 17 может в качестве альтернативы содержать электромеханическое средство генерирования электропитания, как описано выше на фиг. 4, то есть, элементы 410, 420 и 450.

В соответствии с одним альтернативным вариантом осуществления изобретения, корпус 10 состоит из нескольких частей. Эти части могут быть собраны неразъемно, например, путем сварки или склеивания. Эти части могут быть собраны неокончательно, например, путем зажимания, обжимания или соединения болтами.

Фиг. 11 является иллюстрацией части 20, предназначенной для встраивания в устройство аутентификации, изображенное на фиг. 10, то есть, так называемой удерживающей пластины 20. Форма пластины 20 адаптирована под ее вставление с усилием в канавку 11 корпуса 10. В удерживающей пластине 20 предусмотрены отверстия, чтобы обеспечивать прохождение через них штырьков, таких как штырьки 750, 760, 770, 751, 761, 771, 752, 762, 772. Один такой штырек изображен на фиг. 12. На рассматриваемой удерживающей пластине 20 или в качестве альтернативы на корпусе 10 устройства 600 аутентификации может быть написан серийный номер. На стадии конфигурирования устройство 600 аутентификации может быть активировано с целью

обнаружения рисунка устройства 600 аутентификации, а также излучаемого сигнала аутентификации. При этом можно связывать упомянутый рисунок и сигнал аутентификации с серийным номером, обеспечивая возможность последующей идентификации устройства 600 аутентификации с помощью уникального идентификатора, соответствующего серийному номеру. В качестве альтернативы или дополнительно серийный номер может быть вписан на печатной схеме, возможно, применительно к сигналу аутентификации.

Фиг. 12 представляет собой вид в разрезе штырька 30, предназначенного для встраивания в устройство аутентификации, изображенное на фиг. 10. Штырек 30 в данном случае представлен в вертикальном положении. Верхняя часть штырька 30 соответствует основанию, предназначенному для нахождения в контакте с опорной пластиной. Нижняя часть соответствует части, предназначенной для расположения в контакте с сенсорным экраном электронного устройства. Штырек 30 может при этом состоять из гибкого материала, такого как резина с твердостью между 25 по Шору А и 75 по Шору А, например, 50 по Шору А. Некоторые штырьки 30 состоят из резины, заполненной углеродом, чтобы сделать их проводниками электричества. Основание каждого штырька 30 шире, чем отверстия, предусмотренные в удерживающей пластине 20, причем при удерживании штырьков их основания, возможно, сжимаются между удерживающей пластиной 20 и опорной пластиной. Придавливание устройства 600 аутентификации к сенсорному экрану электронного устройства поднимает штырьки, гарантируя контакт оснований каждого штырька, в особенности, штырьков, состоящих из проводящего материала, с опорной пластиной, состоящей из проводящего материала.

В соответствии с одним дополнительным вариантом осуществления изобретения, в центре опорной пластины просверлено отверстие напротив отверстия, соответствующего центральному штырьку (штырьку 761). При этом в штырек 761 может быть вставлен жесткий стержень таким образом, чтобы давление на этот штырек 761 могло активировать нажимную кнопку, такую как детектор PRESS 810, расположенный на нижней поверхности печатной схемы, вставленной в канавку 15. Жесткий стержень далее проходит сквозь отверстие, предусмотренное в опорной пластине.

В соответствии с одним дополнительным вариантом осуществления изобретения, некоторые штырьки содержат жесткие стержни, упирающиеся в опорную пластину, с целью регулирования глубины погружения штырьков при нажатии устройства 600 аутентификации на поверхность, такую как экран электронного устройства.

В соответствии с одним дополнительным вариантом осуществления изобретения, число штырьков, состоящих из проводящего материала, меньше или равно четырем. В действительности наличие двух, трех или четырех штырьков, изготовленных из электропроводящего материала, обеспечивает хороший компромисс между - с одной стороны - наличием достаточного числа различных рисунков и - с другой стороны - обеспечением быстрого обнаружения упомянутого рисунка сенсорным экраном электронного устройства. В действительности, когда штырьков, состоящих из проводящего материала, слишком много, как правило, более пяти, обнаружение рисунка тем или иным электронным устройством может быть случайным или медленным. Кроме того, некоторые сенсорные экраны не позволяют одновременно обнаруживать более пяти точек контакта, причем эти экраны, как правило, предназначены для использования с пятью пальцами руки.

(57) Формула изобретения

1. Устройство (600) аутентификации, предназначенное для использования с

электронным устройством (310), содержащим емкостный сенсорный экран и приемник, причем устройство аутентификации отличается тем, что оно содержит:

- множество штырьков (750, 760, 770, 751, 761, 771, 752, 762, 772), расположенных на одной и той же поверхности устройства аутентификации, причем по меньшей мере два штырька состоят из проводящего материала, а остальные штырьки состоят из изолирующего материала, все штырьки имеют одинаковый внешний вид,

- средство (810) для обнаружения давления, оказываемого на по меньшей мере один штырек, и

- средство (830) для излучения сигнала аутентификации, принимаемого приемником при обнаружении давления, причем сигнал аутентификации является звуковым сигналом.

2. Устройство аутентификации по предыдущему пункту, причем геометрическое расположение штырьков, состоящих из проводящего материала, образует рисунок, причем рисунок связан с сигналом аутентификации.

3. Устройство аутентификации по одному из предыдущих пунктов, причем устройство аутентификации по меньшей мере частично изготовлено из проводящего материала, причем электрическая непрерывность обеспечивается штырьками, состоящими из проводящего материала.

4. Устройство аутентификации по предыдущему пункту, причем проводящий материал, составляющий штырьки и/или покрывающий устройство аутентификации, является гибким.

5. Устройство аутентификации по одному из предыдущих пунктов, причем устройство аутентификации содержит моноблочный и полый корпус (10), состоящий из гибкого материала, являющегося проводником электричества, причем корпус содержит по меньшей мере одну канавку (15), позволяющую вставлять опорную пластину, состоящую из электропроводящего материала, на которой держатся штырьки, причем внутренняя часть корпуса устройства аутентификации образует клетку Фарадея.

6. Устройство аутентификации по одному из предыдущих пунктов, причем устройство аутентификации дополнительно содержит средство (850) для считывания отпечатков пальцев при обнаружении давления на по меньшей мере одном штырьке, причем сигнал аутентификации излучается только в том случае, если считанный отпечаток пальца соответствует предварительно заданному отпечатку пальца.

7. Устройство аутентификации по одному из предыдущих пунктов, причем по большей мере четыре штырька состоят из проводящего материала, остальные штырьки состоят из изолирующего материала.

8. Способ аутентификации идентификатора, связанного с устройством аутентификации, исполняемый электронным устройством, содержащим емкостный сенсорный экран и приемник, и включающий в себя этапы:

- приема выбранного варианта первого идентификатора, связанного с первым устройством аутентификации,

- извлечения первого сигнала аутентификации и первого рисунка, связанного с первым идентификатором,

- обнаружения (901) по меньшей мере двух точек ввода на емкостном сенсорном экране, создаваемых наложением второго устройства аутентификации на емкостный сенсорный экран,

- определения (910) второго рисунка в зависимости от обнаруженных точек ввода,

- приема (920) второго сигнала аутентификации с помощью приемника,

- аутентификации (930) первого идентификатора, если второй сигнал аутентификации равен первому сигналу аутентификации и если второй рисунок равен первому рисунку.

9. Способ аутентификации идентификатора, связанного с устройством аутентификации, по предыдущему пункту, причем этап определения второго рисунка включает в себя этап вычисления по меньшей мере одного расстояния между точками ввода, обнаруженными на емкостном сенсорном экране.

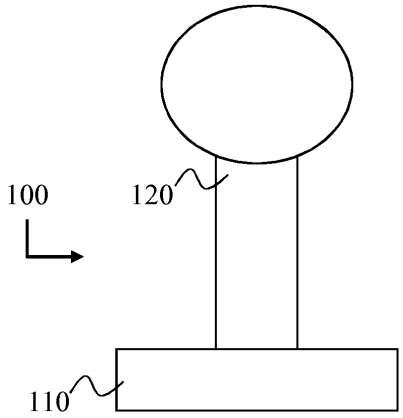
10. Система для аутентификации идентификатора, связанного с устройством аутентификации по любому из пп. 1-7, содержащая:

- устройство аутентификации по любому из пп. 1-7,

- электронное устройство, содержащее емкостный сенсорный экран и приемник, причем электронное устройство выполнено с возможностью осуществления способа аутентификации по любому из пп. 8 или 9.

11. Носитель записи, содержащий компьютерную программу, содержащую инструкции для осуществления процессором электронного устройства (310) способа, обеспечивающего аутентификацию идентификатора, связанного с устройством (600) аутентификации по любому из пп. 8 или 9, при исполнении компьютерной программы процессором.

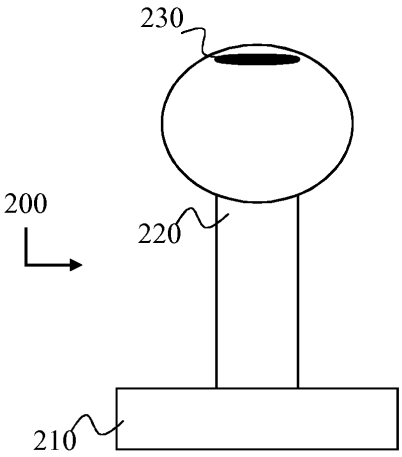
1



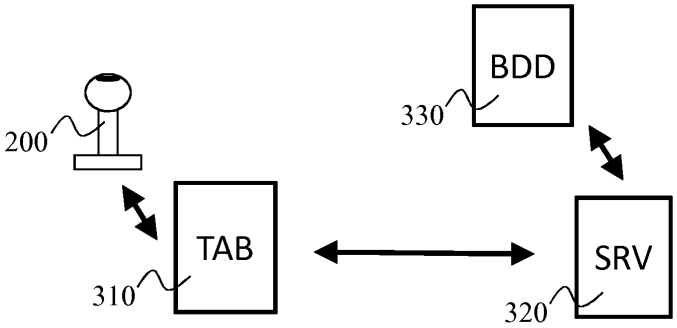
ФИГ. 1

(ПРЕДШЕСТВУЮЩИЙ УРОВЕНЬ ТЕХНИКИ)

2

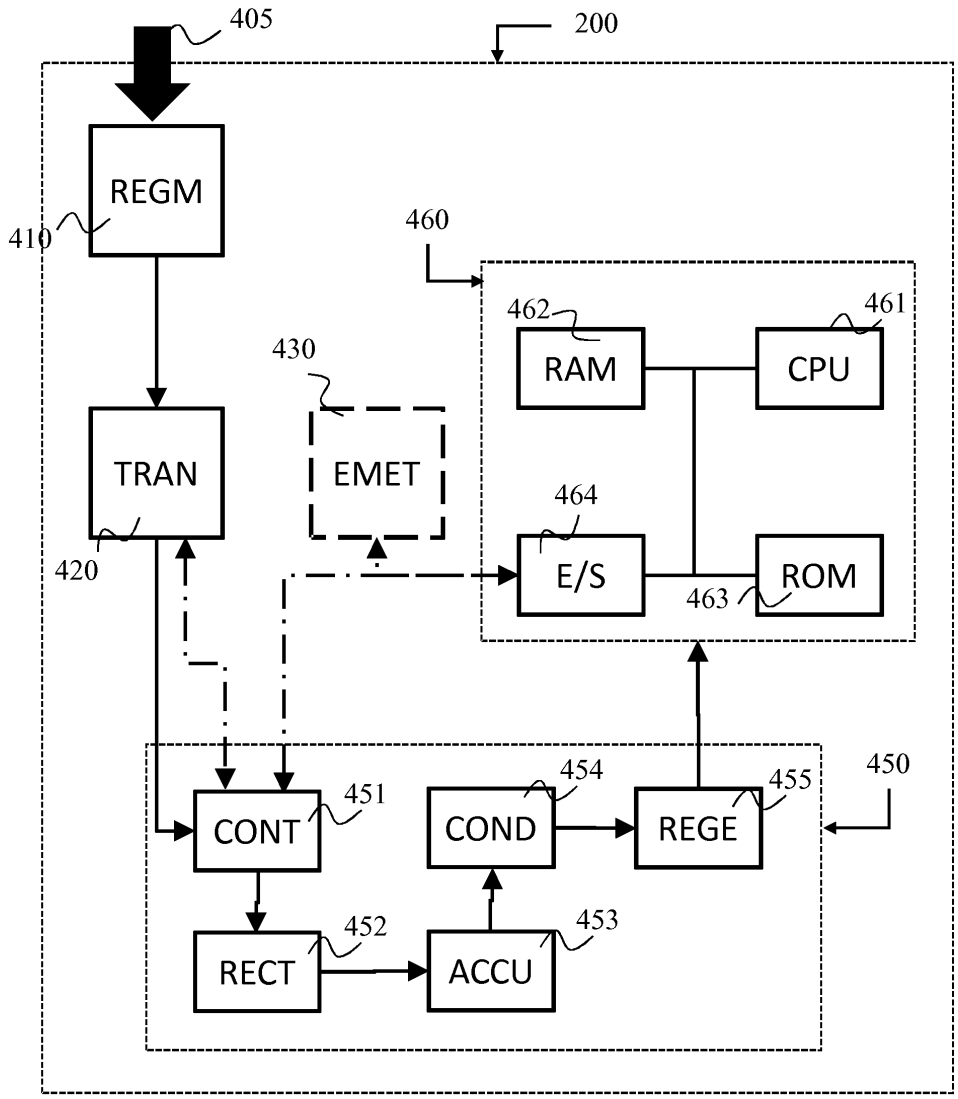


ФИГ. 2



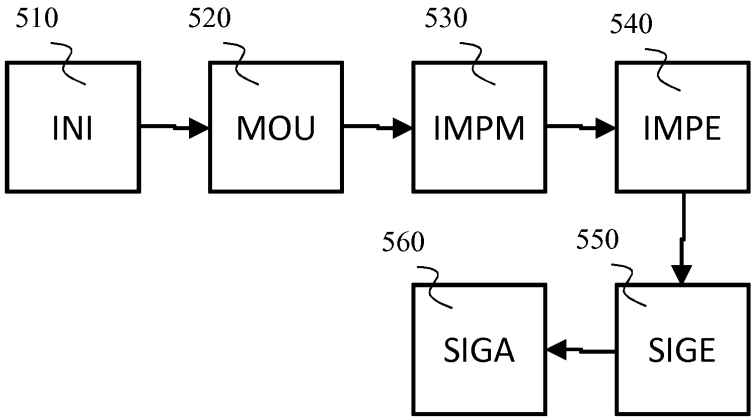
ФИГ. 3

3


405
200
REGM
410
460
462
461
RAM
CPU
430
TRAN
EMET
464
420
E/S
ROM
463
450
454
455
451
CONT
COND
REGE
452
453
RECT
ACCU

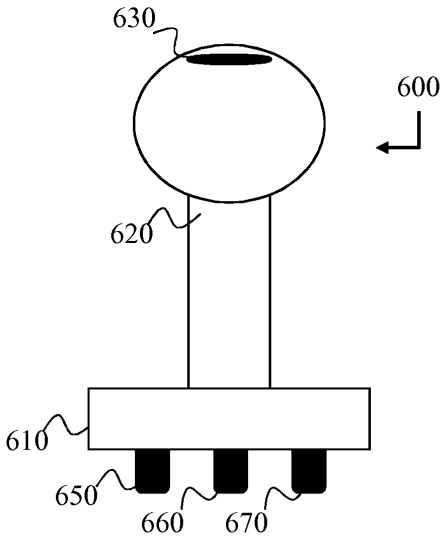
ФИГ. 4

4

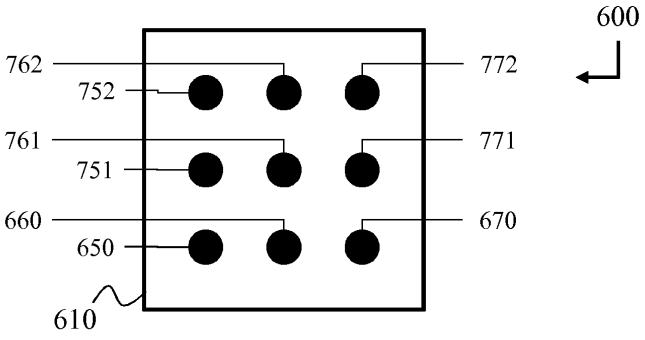


ФИГ. 5

5

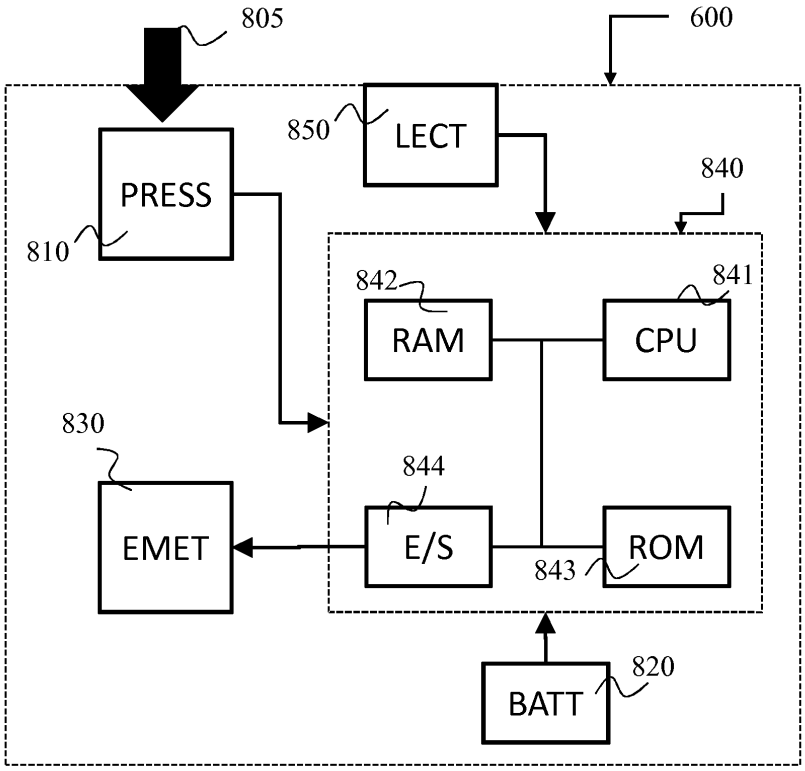

630
600
620
610
650
660
670

ФИГ. 6

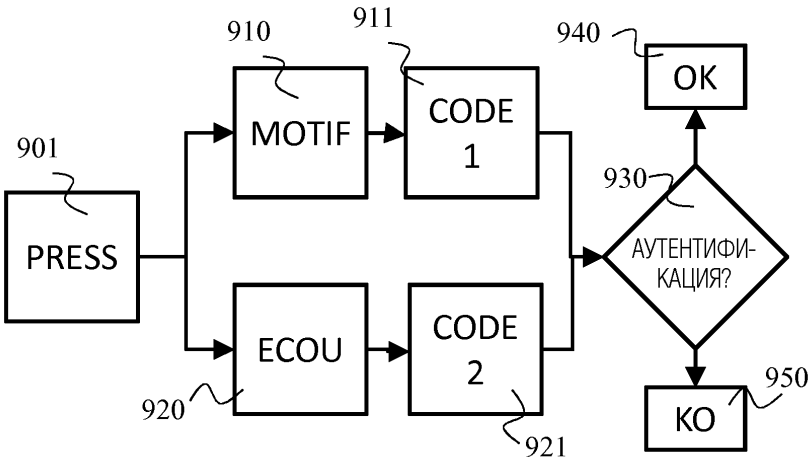

600
762
752
772
761
751
771
660
650
670
610

ФИГ. 7

6

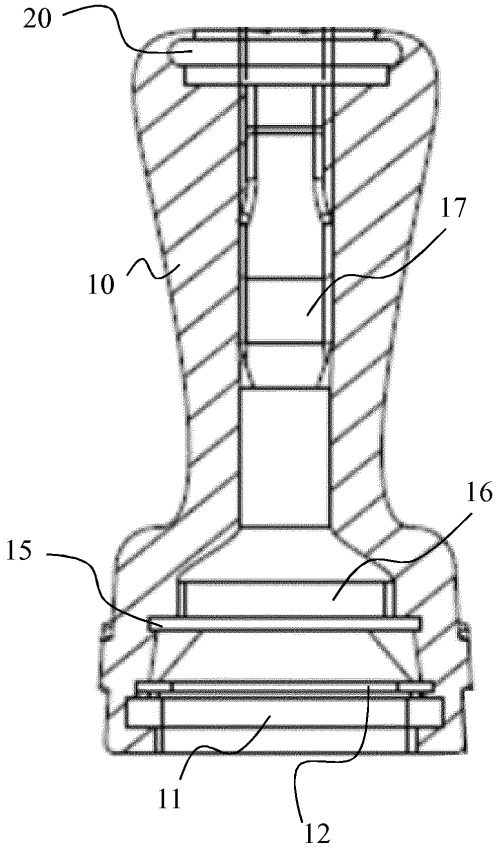

805
600
850
LECT
PRESS
810
840
842
RAM
841
CPU
830
844
EMET
E/S
ROM
843
820
BATT

ФИГ. 8

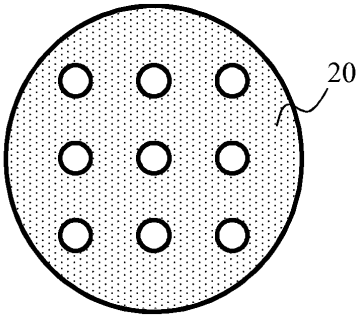

910
911
940
OK
MOTIF
CODE 1
901
930
PRESS
АУТЕНТИФИ-КАЦИЯ?
ECOU
CODE 2
950
920
921
KO

ФИГ. 9

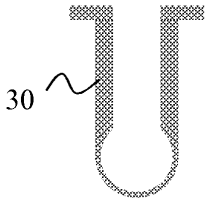
7



ФИГ. 10



ФИГ. 11



ФИГ. 12