



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2014103778/08, 04.02.2014

(24) Дата начала отсчета срока действия патента:
04.02.2014

Приоритет(ы):

(30) Конвенционный приоритет:
12.02.2013 EP 13154974.3

(43) Дата публикации заявки: 10.08.2015 Бюл. № 22

(45) Опубликовано: 10.04.2016 Бюл. № 10

(56) Список документов, цитированных в отчете о поиске: US 2008/0144071 A1, 19.06.2008. US 2012/0227098 A1, 06.09.2012. US 2012/0084135 A1, 05.04.2012. US 2011/0244798 A1, 06.10.2011. US 2012/0233118 A1, 13.09.2012.

Адрес для переписки:

129090, Москва, ул. Б. Спасская, 25, строение 3,
ООО "Юридическая фирма Городиский и
Партнеры"

(72) Автор(ы):

ПАРКС Бенджамин Джон (GB)

(73) Патентообладатель(и):

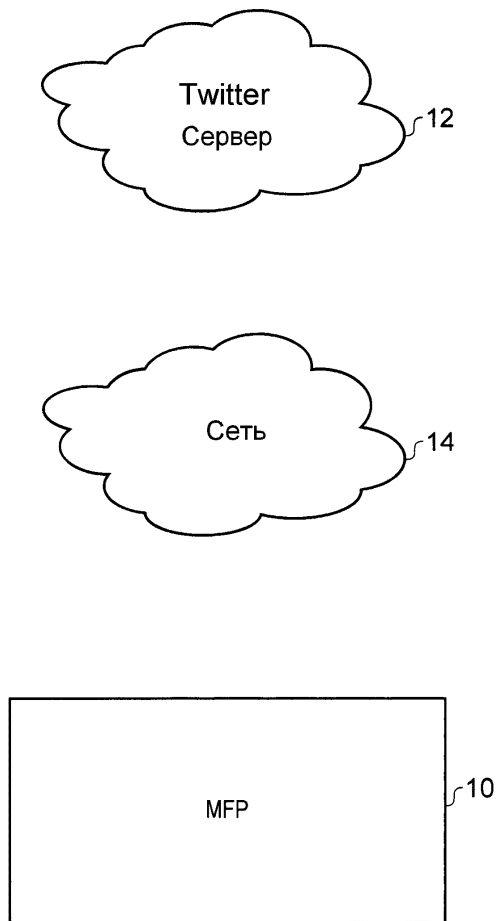
КЭНОН ЭРОПА Н.В. (NL)

(54) СПОСОБ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПЕРИФЕРИЙНОГО УСТРОЙСТВА, ПЕРИФЕРИЙНОЕ УСТРОЙСТВО И СИСТЕМА ДЛЯ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПЕРИФЕРИЙНОГО УСТРОЙСТВА

(57) Реферат:

Изобретение относится к области аутентификации пользователей. Технический результат - прощение процесса аутентификации пользователя в периферийном устройстве. Способ аутентификации пользователя в периферийном устройстве, включающий этапы, на которых принимают запрос логического входа от пользователя; отправляют службе социальных сетей запрос аутентификации учетной записи пользователя в службе социальных сетей; принимают от службы социальных сетей информацию учетной записи пользователя; определяют на основе информации учетной записи пользователя, разрешено ли пользователю

осуществлять доступ к периферийному устройству, посредством соединения с учетной записью администратора службы социальных сетей, чтобы определить, связана ли информация учетной записи пользователя в службе социальных сетей со списком в службе социальных сетей; если на основе информации учетной записи пользователя в службе социальных сетей определено, что пользователю разрешено осуществить доступ к периферийному устройству, обеспечивают пользователю доступ к периферийному устройству. 10 н. и 32 з.п. ф-лы, 24 ил.



ФИГ.1



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(51) Int. Cl.

G06F 21/41 (2013.01)*G06F 21/60* (2013.01)*H04L 29/06* (2006.01)(12) **ABSTRACT OF INVENTION**(21)(22) Application: **2014103778/08, 04.02.2014**(24) Effective date for property rights:
04.02.2014

Priority:

(30) Convention priority:
12.02.2013 EP 13154974.3(43) Application published: **10.08.2015** Bull. № 22(45) Date of publication: **10.04.2016** Bull. № 10

Mail address:

**129090, Moskva, ul. B. Spasskaja, 25, stroenie 3,
OOO "Juridicheskaja firma Gorodisskij i Partnery"**

(72) Inventor(s):

PARKS Bendzhamin Dzhon (GB)

(73) Proprietor(s):

KENON EROPA N.V. (NL)(54) **METHOD FOR AUTHENTICATION OF PERIPHERAL DEVICE USER, PERIPHERAL DEVICE AND SYSTEM FOR AUTHENTICATION OF PERIPHERAL DEVICE USER**

(57) Abstract:

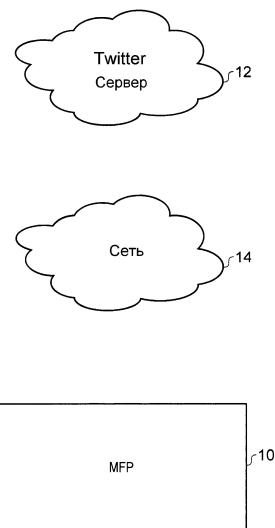
FIELD: physics, computer engineering.

SUBSTANCE: invention relates to user authentication. A method of authenticating a user in a peripheral device, which comprises steps of receiving a logic input request from the user; sending to a social network service an authentication request of the user account in the social network service; receiving user account information from the social network service; determining, based on the user account information, whether the user is allowed to access the peripheral device by connecting with the administrator account of the social network service in order to determine whether the user account information in the social network service is associated with the list in the social network service; if, based on the user account information in the social network service, it is determined that the user is allowed to access the peripheral device, the user is granted access to the peripheral device.

EFFECT: simple process of authenticating a user

in a peripheral device.

42 cl, 24 dwg



ФИГ.1

УРОВЕНЬ ТЕХНИКИ**ОБЛАСТЬ ТЕХНИКИ, К КОТОРОЙ ОТНОСИТСЯ ИЗОБРЕТЕНИЕ**

[0001] Настоящее изобретение относится к способу аутентификации, к устройству аутентификации и к системе аутентификации. В частности, настоящее изобретение
5 относится к способу аутентификации пользователя в периферийном устройстве, к периферийному устройству для аутентификации пользователя периферийного устройства и к системе аутентификации пользователя периферийного устройства.

ОПИСАНИЕ ПРЕДШЕСТВУЮЩЕГО УРОВНЯ ТЕХНИКИ

[0002] Открытый протокол OAuth является протоколом аутентификации, который
10 позволяет пользователям разрешать приложениям действовать от их имени, не сообщая приложениям свои учетные данные, например, пароль. В традиционной клиент-серверной модели аутентификации клиент использует свои учетные данные для того, чтобы получить доступ к ресурсам, размещенным на сервере. Протокол OAuth вводит третьего участника в эту модель: владельца ресурса. В модели OAuth клиент (который не является
15 владельцем ресурса, но действует от его имени), запрашивает доступ к ресурсам, которыми управляет владелец ресурса, но которые размещены на сервере.

[0003] Для того, чтобы клиент получил доступ к ресурсам, он должен сначала получить разрешение от владельца ресурса. Это разрешение выражается в форме токена и соответствует совместно используемому секрету. Цель токена заключается в том,
20 чтобы сделать для владельца ресурса ненужным сообщение его учетных данных клиенту. В отличие от учетных данных владельца ресурса, токены могут выдаваться с ограниченным контекстом и ограниченным временем жизни, а также отзываться независимо. Для дополнительной информации о протоколе OAuth можно обратиться к официальному веб-сайту <http://oauth.net/>.

[0004] Служба социальных сетей является онлайн службой, платформой или сайтом, который сосредотачивается на том, чтобы создавать и отображать социальные сети или общественные отношения среди людей, которые, например, имеют общие интересы и/или занятия, и людей с подобными или несколько схожими интересами, квалификацией и/или разного рода деятельностью, создавая свои собственные сообщества. Служба
30 социальных сетей состоит из представления каждого пользователя (зачастую профиля), его/ее социальных связей и множества дополнительных сервисов. Большинство сервисов социальных сетей являются сетевыми и предоставляют пользователям средства для взаимодействия по Интернету, такие как электронная почта и мгновенный обмен сообщениями. Сайты социальных сетей позволяют пользователям совместно
35 использовать идеи, разного рода деятельность, события и интересы в пределах их индивидуальных сетей.

[0005] Основными типами служб социальных сетей являются те, которые содержат категории (такие как годы учебы или одноклассники), служащие средством объединения с друзьями (обычно со страницами самоописания), а также систему рекомендаций,
40 соединенную с доверием. Популярные способы теперь комбинируют многие из них, например, широко используемые во всем мире социальные сети Facebook (зарегистрированный товарный знак), Google+ (зарегистрированный товарный знак) и Twitter (зарегистрированный товарный знак). Twitter является сервисом интерактивной социальной сети и сервисом микроблогинга, который позволяет его пользователям
45 отправлять и читать текстовые сообщения длиной до 140 символов, известные как "твиты". Незарегистрированные пользователи могут читать твиты, в то время как зарегистрированные пользователи могут публиковать твиты через интерфейс веб-сайта, через телефонные короткие текстовые сообщения SMS или с помощью ряда приложений

для мобильных устройств.

[0006] В больших системах MFP (многофункциональных периферийных устройств), для того, чтобы управлять логическим входом пользователей, может быть установлена служба каталога Active Directory компании Microsoft (зарегистрированный товарный знак). Однако, в меньших системах установка Active Directory является дорогой и неудобной. Желательно предложить альтернативный механизм логического входа, который бы являлся подходящим для небольших систем из групп многофункциональных периферийных устройств.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0007] Задача настоящего изобретения заключается в том, чтобы предложить периферийное устройство и способ функционирования периферийного устройства, который обеспечивает аутентификацию пользователей в периферийном устройстве без потребности в выделенных ресурсах аутентификации в периферийном устройстве. Другими словами, задача настоящего изобретения заключается в том, чтобы предложить упрощенный дешевый механизм для аутентификации пользователей в периферийном устройстве.

[0008] В соответствии с первым аспектом настоящего изобретения предлагается способ аутентификации пользователя в периферийном устройстве, включающий в себя следующие этапы, выполняемые периферийным устройством: получение запроса на логический вход (log-in) от пользователя; отправка запроса службе социальных сетей для того, чтобы аутентифицировать учетную запись пользователя в службе социальных сетей; получение от службы социальных сетей информации учетной записи пользователя в службе социальных сетей; определение на основе информации учетной записи пользователя в службе социальных сетей, разрешено ли пользователю осуществлять доступ к периферийному устройству; и, в случае, если в результате этого определения на основе информации учетной записи пользователя в службе социальных сетей определено, что пользователю разрешено осуществлять доступ к периферийному устройству, обеспечение пользователю доступа к периферийному устройству.

[0009] В некоторых вариантах осуществления это определение включает в себя соединение с учетной записью администратора службы социальных сетей для того, чтобы определить, связана ли информация об учетной записи пользователя в службе социальных сетей с представлением периферийного устройства в службе социальных сетей.

[0010] В некоторых вариантах осуществления представление периферийного устройства в службе социальных сетей связано со списком членов службы социальных сетей в службе социальных сетей, и/или представление периферийного устройства в службе социальных сетей связано с группой списков членов службы социальных сетей в службе социальных сетей.

[0011] В некоторых вариантах осуществления связывание представления периферийного устройства в службе социальных сетей со списком членов службы социальных сетей включает в себя определение уровней доступа к функциям периферийного устройства для списка членов службы социальных сетей, причем связывание представления периферийного устройства в службе социальных сетей с группой списков членов службы социальных сетей включает в себя определение уровней доступа к функциям периферийного устройства для группы списков членов службы социальных сетей.

[0012] В некоторых вариантах осуществления отправка запроса в службу социальных сетей включает в себя запрос токена доступа у службы социальных сетей. В некоторых

вариантах осуществления определение включает в себя использование токена доступа для того, чтобы получить имя пользователя в службе социальных сетей и определить, связан ли этот пользователь с представлением периферийного устройства в службе социальных сетей. В некоторых вариантах осуществления способ дополнительно
 5 включает в себя хранение токена доступа на периферийном устройстве совместно с информацией, идентифицирующей пользователя. В некоторых вариантах осуществления такое хранение включает в себя хранение токена доступа совместно с радиочастотным идентификатором (RFID) пользователя. Предпочтительно, сохраненный токен доступа служит для того, чтобы производить повторные запросы на логический вход от имени
 10 пользователя.

[0013] В некоторых вариантах осуществления запрос токена доступа у службы социальных сетей включает в себя использование процесса аутентификации в соответствии с протоколами OAuth или xAuth.

[0014] В некоторых вариантах осуществления перед отправкой запроса в службу
 15 социальных сетей производится определение мобильным устройством первой части информации, предоставленной периферийным устройством.

[0015] В некоторых вариантах осуществления первая часть информации является адресом URL (единый указатель ресурсов); причем периферийное устройство предоставляет адрес URL пользователю; и мобильное устройство определяет адрес
 20 URL посредством ввода адреса URL в мобильное устройство пользователем. В некоторых вариантах осуществления адрес URL, полученный мобильным устройством, позволяет пользователю входить в службу социальных сетей. В некоторых вариантах осуществления адрес URL, полученный мобильным устройством, позволяет пользователю входить в службу социальных сетей и авторизовать выдачу токена доступа
 25 к периферийному устройству.

[0016] В других вариантах осуществления периферийное устройство предоставляет машиночитаемый код, кодирующий первую часть информации; причем мобильное устройство определяет первую часть информации посредством чтения и декодирования машиночитаемого кода, предоставленного периферийным устройством.

[0017] В некоторых вариантах осуществления после отправки в службу социальных
 30 сетей запроса на аутентификацию пользователя производится определение мобильным устройством второй части информации, предоставленной службой социальных сетей. В некоторых вариантах осуществления вторая часть информации является кодом, и способ включает в себя получение периферийным устройством кода от пользователя
 35 через пользовательский интерфейс периферийного устройства. В некоторых вариантах осуществления код является числом.

[0018] В других вариантах осуществления машиночитаемый код является штрих-кодом или другим машиночитаемым кодом, кодирующим часть идентификационной информации; и мобильное устройство конфигурируется так, чтобы определить часть
 40 идентификационной информации посредством чтения и декодирования штрих-кода или другого машиночитаемого кода, предоставленного периферийным устройством.

[0019] В соответствии с другим аспектом настоящего изобретения предлагается периферийное устройство, сконфигурированное для: получения от пользователя запроса на логический вход; отправки в службу социальных сетей запроса на аутентификацию
 45 учетной записи пользователя в службе социальных сетей; получения от службы социальных сетей информации об учетной записи пользователя в службе социальных сетей; определения на основе информации об учетной записи пользователя в службе социальных сетей, разрешается ли пользователю осуществлять доступ к периферийному

устройству; и, в случае, если периферийное устройство на основе информации учетной записи пользователя в службе социальных сетей определило, что пользователю разрешено осуществлять доступ к периферийному устройству, обеспечения пользователю доступа к периферийному устройству.

5 [0020] В некоторых вариантах осуществления периферийное устройство включает в себя периферийное устройство, которое функционирует по меньшей мере как принтер, факс и сканер.

[0021] В соответствии с дополнительным аспектом настоящего изобретения предлагается мобильное устройство, включающее в себя функцию аутентификации
10 пользователя в периферийном устройстве, которая включает в себя: средства для чтения и декодирования машиночитаемого кода для того, чтобы определить часть идентификационной информации; а также средства для того, чтобы использовать эту определенную часть идентификационной информации, чтобы позволить пользователю войти в службу социальных сетей с тем, чтобы авторизовать выдачу токена доступа к
15 периферийному устройству.

[0022] В некоторых вариантах осуществления мобильное устройство является мобильным телефоном, персональным цифровым помощником PDA, цифровым фотоаппаратом, ноутбуком или другим мобильным устройством.

[0023] В соответствии с дополнительным аспектом настоящего изобретения предлагается система для аутентификации пользователя периферийного устройства, которая включает в себя: периферийное устройство, выполненное с возможностью получения от пользователя запроса на логический вход и отправки службе социальных сетей запроса аутентификации учетной записи пользователя в службе социальных сетей; а также службу социальных сетей, выполненную с возможностью получать запрос и
25 отправлять информацию учетной записи пользователя в службе социальных сетей периферийному устройству; при этом периферийное устройство выполнено с возможностью: получения от службы социальных сетей информации об учетной записи пользователя в службе социальных сетей; определения на основе информации об учетной записи пользователя в службе социальных сетей, разрешается ли пользователю
30 осуществлять доступ к периферийному устройству; и, в случае, если периферийное устройство на основе информации учетной записи пользователя в службе социальных сетей определило, что пользователю разрешено осуществить доступ к периферийному устройству, обеспечения пользователю доступа к периферийному устройству.

[0024] В соответствии с дополнительным аспектом настоящего изобретения, предлагается способ аутентификации пользователя в периферийном устройстве, включающий в себя следующие этапы: определение мобильным устройством первой части идентификационной информации и отправку через службу социальных сетей запроса на доступ к периферийному устройству, включающего в себя эту определенную первую часть идентификационной информации и вторую часть информации,
40 идентифицирующую учетную запись пользователя в социальной сети; получение периферийным устройством запроса на доступ через службу социальных сетей и определение на основе информации, содержащейся в запросе на доступ, разрешается ли пользователю осуществлять доступ к периферийному устройству; и в случае, если периферийное устройство на основе запроса на доступ определило, что пользователю разрешено осуществить доступ к периферийному устройству, обеспечение пользователю
45 доступа к периферийному устройству.

[0025] В некоторых вариантах осуществления перед определением периферийным устройством выполняется соединение периферийного устройства с учетной записью

администратора службы социальных сетей и регистрация первой части идентификационной информации совместно с представлением периферийного устройства в службе социальных сетей; причем определение периферийным устройством включает в себя: соединение с учетной записью администратора службы социальных сетей, доступ к запросу на доступ, и определение того, соответствует ли информация, содержащаяся в запросе на доступ, зарегистрированной детальной информации о периферийном устройстве.

[0026] В некоторых вариантах осуществления запрос доступа является прямым (конфиденциальность) сообщением, отправленным от учетной записи пользователя в службе социальных сетей учетной записи администратора службы социальных сетей.

[0027] В некоторых вариантах осуществления периферийное устройство определяет уровень доступа к периферийному устройству на основе второй части информации, идентифицирующей учетную запись пользователя в службе социальных сетей.

[0028] В некоторых вариантах осуществления первая часть идентификационной информации включает в себя код, периферийное устройство предоставляет этот код пользователю, и мобильное устройство определяет первую часть идентификационной информации путем ввода пользователем кода в мобильное устройство.

[0029] В других вариантах осуществления периферийное устройство предоставляет машиночитаемый код, кодирующий первую часть идентификационной информации; и мобильное устройство определяет первую часть идентификационной информации посредством чтения и декодирования машиночитаемого кода, предоставленного периферийным устройством.

[0030] В некоторых вариантах осуществления первая часть идентификационной информации включает в себя случайное число.

[0031] В некоторых вариантах осуществления первая часть идентификационной информации включает в себя часть информации, идентифицирующую учетную запись администратора службы социальных сетей (например, имя пользователя).

[0032] В некоторых вариантах осуществления периферийное устройство выполнено с возможностью генерировать первую часть идентификационной информации.

[0033] В некоторых вариантах осуществления первая часть идентификационной информации получается из положения периферийного устройства; и мобильное устройство определяет первую часть идентификационной информации путем определения положения периферийного устройства. Предпочтительно положение периферийного устройства определяется с использованием средств определения положения в мобильном устройстве. В некоторых вариантах осуществления средство определения положения представляет собой датчик глобального положения. Предпочтительно первая часть идентификационной информации является предопределенным количеством цифр координат положения периферийного устройства.

[0034] В соответствии с дополнительным аспектом настоящего изобретения предлагается система для аутентификации пользователя в периферийном устройстве, включающая в себя: мобильное устройство, выполненное с возможностью определять первую часть идентификационной информации и отправлять через службу социальных сетей запрос доступа к периферийному устройству, включающий в себя эту определенную первую часть идентификационной информации и вторую часть информации, идентифицирующую учетную запись пользователя в социальной сети; при этом периферийное устройство выполнено с возможностью получать запрос доступа и определять на основе информации, содержащейся в запросе доступа, разрешается ли пользователю осуществлять доступ к данному периферийному устройству; при этом

периферийное устройство выполнено с возможностью, в случае, если периферийное устройство на основе запроса доступа определило, что пользователю разрешено осуществить доступ к периферийному устройству, обеспечить пользователю доступ к периферийному устройству.

5 [0035] В соответствии с дополнительным аспектом настоящего изобретения предлагается мобильное устройство, включающее в себя функцию для аутентификации пользователя в периферийном устройстве, включающую в себя: средства для чтения и декодирования машиночитаемого кода для того, чтобы определить первую часть идентификационной информации; а также средства для отправки через службу
10 социальных сетей запроса на доступ к периферийному устройству, включающего в себя эту определенную первую часть идентификационной информации и вторую часть информации, идентифицирующую учетную запись пользователя в службе социальных сетей.

[0036] В соответствии с дополнительным аспектом настоящего изобретения
15 предлагается периферийное устройство, включающее в себя: средство, выполненное с возможностью предоставлять пользователю первую часть идентификационной информации в форме машиночитаемого кода; а также средство, выполненное с возможностью осуществлять доступ к учетной записи в службе социальных сетей и определять на основе первой части идентификационной информации, разрешается ли
20 пользователю осуществлять доступ к периферийному устройству.

[0037] В некоторых вариантах осуществления средство, выполненное с возможностью предоставлять пользователю первую часть идентификационной информации, выполнено с возможностью предоставлять пользователю идентификационную информацию посредством по меньшей мере одного из: отображения идентификационной информации
25 на дисплее периферийного устройства и печати идентификационной информации.

[0038] В некоторых вариантах осуществления идентификационная информация включает в себя случайное число.

[0039] В некоторых вариантах осуществления идентификационная информация включает в себя информацию, идентифицирующую учетную запись администратора
30 службы социальных сетей.

[0040] В некоторых вариантах осуществления периферийное устройство включает в себя средство для генерирования идентификационной информации.

[0041] В некоторых вариантах осуществления периферийное устройство выполнено с возможностью предоставлять идентификационную информацию в форме штрих-кода
35 или QR-кода.

[0042] В соответствии с дополнительным аспектом настоящего изобретения, предлагается способ сообщения информации относительно периферийного устройства, включающий в себя следующие этапы, выполняемые периферийным устройством: соединение с учетной записью службы социальных сетей, представляющей периферийное
40 устройство; и отправка информации относительно периферийного устройства одному или более пользователям службы социальных сетей.

[0043] В некоторых вариантах осуществления информация, отправляемая периферийным устройством, является информацией относительно одного или более из следующего: информация относительно состояния периферийного устройства,
45 информация относительно использования периферийного устройства, информация относительно расположения периферийного устройства, информация, идентифицирующая пользователей периферийного устройства, информация относительно общей или индивидуальной пользовательской деятельности на

периферийном устройстве, информация относительно действий, выполняемых пользователями с использованием периферийного устройства, информация, детализирующая затраты пользователей на использование периферийного устройства, информация, детализирующая материалы, используемые периферийным устройством для обработки пользовательских действий, а также информация относительно обслуживания периферийного устройства.

[0044] В соответствии с дополнительным аспектом настоящего изобретения, предлагается периферийное устройство для сообщения информации относительно периферийного устройства, включающее в себя: средство для соединения с учетной записью службы социальных сетей, представляющей периферийное устройство; а также средство для отправки информации относительно периферийного устройства одному или более пользователям службы социальных сетей.

[0045] В некоторых вариантах осуществления периферийное устройство включает в себя периферийное устройство, которое функционирует по меньшей мере как одно из принтера, факса или сканера.

[0046] В некоторых вариантах осуществления мобильное устройство является мобильным телефоном, персональным цифровым помощником PDA, цифровым фотоаппаратом, ноутбуком или другим мобильным устройством.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0047] Далее будут описаны варианты осуществления настоящего изобретения, посредством примеров со ссылками на сопровождающие чертежи, в которых:

[0048] Фиг. 1 показывает конфигурацию первого варианта осуществления;

[0049] Фиг. 2 показывает аппаратные средства многофункционального периферийного устройства;

[0050] Фиг. 3 показывает учетную запись администратора Twitter;

[0051] Фиг. 4 показывает список многофункциональных периферийных устройств в Twitter;

[0052] Фиг. 5 показывает создание списка многофункциональных периферийных устройств в Twitter;

[0053] Фиг. 6 показывает выбор пользователя Twitter, который будет добавлен к списку многофункциональных периферийных устройств;

[0054] Фиг. 7 показывает добавление пользователя Twitter к списку многофункциональных периферийных устройств, создаваемому на фиг.5;

[0055] Фиг. 8 показывает этапы общей процедуры логического входа на многофункциональном периферийном устройстве;

[0056] Фиг. 9 показывает дисплей многофункционального периферийного устройства;

[0057] Фиг. 10 показывает другой дисплей многофункционального периферийного устройства;

[0058] Фиг. 11 показывает этапы, выполняемые на многофункциональном периферийном устройстве в соответствии с первым вариантом осуществления;

[0059] Фиг. 12 показывает другой дисплей многофункционального периферийного устройства;

[0060] Фиг. 13 показывает другой дисплей многофункционального периферийного устройства;

[0061] Фиг. 14 показывает этапы, выполняемые на многофункциональном периферийном устройстве в соответствии со вторым вариантом осуществления;

[0062] Фиг. 15 показывает конфигурацию третьего варианта осуществления;

[0063] Фиг. 16 показывает аппаратные средства мобильного телефона;

[0064] Фиг. 17 показывает другой дисплей многофункционального периферийного устройства;

[0065] Фиг. 18 показывает дисплей мобильного телефона;

[0066] Фиг. 19 показывает этапы, выполняемые в соответствии с третьим вариантом осуществления;

[0067] Фиг. 20А показывает реестр для хранения радиочастотного идентификатора RFID пользователя совместно с токеном доступа;

[0068] Фиг. 20В показывает этапы, выполняемые на многофункциональном периферийном устройстве в соответствии с четвертым вариантом осуществления;

[0069] Фиг. 21 показывает этапы, выполняемые на многофункциональном периферийном устройстве в соответствии с пятым вариантом осуществления;

[0070] Фиг. 22 показывает этапы, выполняемые на мобильном телефоне в соответствии с пятым вариантом осуществления;

[0071] Фиг. 23 показывает этапы, выполняемые на многофункциональном периферийном устройстве в соответствии с пятым вариантом осуществления;

[0072] Фиг. 24 показывает этапы, выполняемые на многофункциональном периферийном устройстве в соответствии с шестым вариантом осуществления;

ОПИСАНИЕ ВАРИАНТОВ ОСУЩЕСТВЛЕНИЯ

Первый вариант осуществления

[0073] Фиг. 1 показывает архитектуру системы обработки изображений первого варианта осуществления. Система обработки изображений включает в себя многофункциональное периферийное устройство (MFP) 10 и сервер 12 аутентификации. Многофункциональное периферийное устройство 10 может соединяться с Интернетом через локальную сеть, такую как Wi-Fi сеть 14, для того, чтобы получить доступ к прикладному программному интерфейсу (API) системы Twitter, размещенному на сервере 12 аутентификации.

[0074] Фиг. 2 показывает аппаратную конфигурацию многофункционального периферийного устройства 10. Многофункциональное периферийное устройство включает в себя центральный процессор (CPU) 20, постоянное запоминающее устройство (ROM) 21, жесткий диск 22 и оперативную память (RAM) 23. Эти компоненты являются стандартными аппаратными компонентами для компьютеров и других устройств и выполняют их обычные функции. Многофункциональное периферийное устройство 10 дополнительно включает в себя блок 24 отображения, операционный блок 25, блок 26 управления связью, устройство 27 считывания изображения, записывающий блок 28, видеопамять 29, блок 210 обработки изображений, блок 211 аутентификации, устройство 212 считывания с карт, и блок 213 управления вводом-выводом. Блок 24 отображения является сенсорным жидкокристаллическим экраном, предусмотренным на многофункциональном периферийном устройстве 10 для того, чтобы позволить пользователю делать выбор и просматривать информацию о многофункциональном периферийном устройстве 10. Операционный блок 25 представляет собой клавиатуру и другие кнопки для того, чтобы позволить пользователю вводить учетные данные для аутентификации, настройки и другую информацию в многофункциональное периферийное устройство 10. Блок 26 управления связью предусматривается для того, чтобы позволить многофункциональному периферийному устройству 10 связываться по локальной сети с веб-сервером 12. Устройство 27 считывания изображения является сканером, который позволяет сканировать документы. Записывающий блок 28, показанный на фиг.2, представляет собой части многофункционального периферийного устройства 10, предназначенные для печати. Записывающий блок 28 печатает данные

изображения на носителе записи и выводит носитель записи для пользователя.

Видеопамять 29 является памятью, предусмотренной для хранения данных изображения во время сканирования устройством 27 считывания изображения или печати

записывающим блоком 28. Блок 210 обработки изображений представляет собой

5 различные специализированные интегральные схемы (ASIC), предусмотренные в многофункциональном периферийном устройстве 10 для того, чтобы увеличить скорость определенных операций обработки изображений, таких как преобразование отсканированных в формате R,G,B данных в данные формата C, M, Y, K во время операции копирования. Блок 211 обработки аутентификации предусматривается для

10 того, чтобы аутентифицировать пользовательскую информацию, полученную от устройства 212 считывания с карт. Данные от устройства 212 считывания с карт получают блоком 211 аутентификации через блок 213 управления вводом-выводом. Блок аутентификации вместо отдельного аппаратного компонента может быть реализован программным обеспечением, выполняемым с использованием центрального

15 процессора 20 и оперативной памяти 23. Компоненты, описанные выше, соединяются друг с другом посредством системной шины 214.

[0075] Многофункциональное периферийное устройство 10 выполняет операционную систему. В этом конкретном варианте осуществления операционная система выполняет приложение MEAP (многофункциональная встроенная прикладная платформа)

20 (приложение логического входа), которое является средой выполнения, обеспечиваемой на многофункциональных периферийных устройствах, продаваемых компанией Canon (зарегистрированный торговый знак). Операционная система позволяет запускать JAVA-приложения и может также включать в себя веб-интерфейс, как будет объяснено позже. Эти приложения могут затем управлять работой периферийного устройства и

25 могут выводить на экран информацию и получать входные инструкции от пользователя через операционный блок 25 и блок 24 сенсорного дисплея.

[0076] Далее со ссылками на фиг. 3-7 будет описана работа системы обработки изображений. Как более подробно будет описано ниже, в вариантах осуществления

30 настоящего изобретения администратор использует поставщика услуг (например, конкретную службу социальных сетей, такую как Twitter) для того, чтобы управлять доступом к периферийным устройствам, таким как многофункциональное периферийное устройство 10.

[0077] НАСТРОЙКА СПИСКА У ПОСТАВЩИКА УСЛУГ

[0078] Например, администратор использует учетную запись администратора в

35 Twitter для создания списков многофункциональных периферийных устройств в Twitter для того, чтобы управлять доступом определенных зарегистрированных пользователей Twitter к конкретным многофункциональным периферийным устройствам. Каждое многофункциональное периферийное устройство может быть представлено списком в Twitter. Например, пользователи с доступом к многофункциональному периферийному

40 устройству 10 будут включены в список Twitter, представляющий многофункциональное периферийное устройство 10. Альтернативно, для того, чтобы сделать управление доступом к соответствующим многофункциональным периферийным устройствам более гибким, администратор может создать списки пользователей в логических группах (как это делается в Active Directory (AD)), например, группы могут быть созданы в

45 Twitter. Вышеописанная схема управления доступом может быть реализована путем поддержки полномочий для групп (или списков Twitter) локально на многофункциональном периферийном устройстве 10, то есть многофункциональное периферийное устройство 10 (приложение MEAP) может конфигурироваться

администратором для проверки конкретных групп - информация о том, какие группы проверять, не обязана храниться в учетной записи администратора Twitter, но вместо этого может быть сохранена локально на многофункциональном периферийном устройстве 10. Система управления доступа (AMS) может использоваться для того, чтобы обеспечить различные виды/уровни доступа к соответствующим функциям/возможностям соответствующих многофункциональных периферийных устройств, различным группам пользователей. Например, Group1 может копировать и отправлять факс, но Group2 может только копировать.

[0079] Администратор может предоставлять/запрещать пользовательский доступ к многофункциональному периферийному устройству 10 путем добавления/удаления пользователя из списка Twitter для многофункционального периферийного устройства 10.

[0080] Как только администратор (например, имеющий в системе Twitter идентификатор пользователя @BenTesting 2) вошел в Twitter под учетной записью администратора, на экран выводится домашняя страница, показанная на фиг. 3. Для того, чтобы создать список принтера, администратор выбирает пункт 'Списки' из меню профиля (вверху слева), который выведет на экран страницу, показанную на фиг. 4. Как можно видеть на фиг. 4, один список принтера (Canon iR-ADV5030) уже был создан. Как проиллюстрировано на фиг. 5, для того, чтобы создать новый список, администратор выбирает пункт 'Создать Список' ("Create list"), вводит имя принтера (Canon iR-ADV2020) и его описание (например, "В углу возле окна"), после чего нажимает кнопку 'Сохранить Список' ("Save list"). Как проиллюстрировано на фиг. 6 и фиг. 7, новый пользователь может быть добавлен к конкретному списку принтера путем поиска пользователя в Twitter. Фиг. 6 иллюстрирует предоставление доступа к принтеру пользователю RobertTesting путем выбора пункта 'Добавить или удалить из списков' рядом с именем учетной записи пользователя. Фиг. 7 иллюстрирует выбор принтера, к которому предоставляется пользовательский доступ. В конкретном примере, показанном на фиг. 7, пользователю предоставляется доступ к принтеру Canon iR-ADV2020.

[0081] ОБЩАЯ ПРОЦЕДУРА ЛОГИЧЕСКОГО ВХОДА

[0082] Обращаясь к фиг. 8, в многофункциональном периферийном устройстве 10 пользователь вводит свои данные для логического входа через экран логического входа (этап S810 на фиг. 8). Как будет подробно описано ниже, в первом варианте осуществления веб-браузер используется для того, чтобы непосредственно осуществить доступ к серверу поставщика услуг с тем, чтобы позволить пользователю сохранять его/ее имя пользователя и пароль в тайне и не использовать их совместно с приложением MEAP или с любым другим сайтом; тогда как во втором варианте осуществления, который будет описан позже, пользователь вводит свои учетные данные непосредственно в приложение MEAP, и приложение MEAP затем передает эти учетные данные поставщику услуг. На этапе S820, изображенном на фиг. 8, приложение MEAP запрашивает токен доступа у поставщика услуг. На этапе S830, изображенном на фиг. 8, приложение MEAP получает токен доступа от поставщика услуг. На этапе S840, изображенном на фиг. 8, осуществляется доступ к списку MFP для многофункционального периферийного устройства 10, определенному у поставщика услуг (например, Twitter) администратором (как ранее описано со ссылками на фиг. 3-7), и определяется, содержится ли идентификатор пользователя у поставщика услуг (идентификатор пользователя Twitter/имя пользователя) в списке многофункционального периферийного устройства, представляющем многофункциональное периферийное

устройство 10, к которому пользователь хочет получить доступ (этап S850). Если идентификатор пользователя Twitter содержится в списке, тогда пользователю предоставляется доступ к многофункциональному периферийному устройству (этап S860 на фиг. 8). Если идентификатор пользователя в системе Twitter не содержится в списке, тогда на экран многофункционального периферийного устройства 10 может быть выведено сообщение об ошибке (этап S870 на фиг. 8).

[0083] ПОДРОБНАЯ ПРОЦЕДУРА ЛОГИЧЕСКОГО ВХОДА

[0084] Обращаясь теперь к иллюстрациям фиг. 9-11, вообразим себе сценарий, в котором пользователь приближается к многофункциональному периферийному устройству 10 и хочет осуществить доступ к многофункциональному периферийному устройству 10. Когда пользователь смотрит на блок 24 отображения многофункционального периферийного устройства 10, он или она видит дисплей, соответствующий фиг. 9. Пользователь использует сенсорный экран блока 24 отображения для того, чтобы выбрать иконку 60 'Зарегистрироваться в Twitter'. Касание иконки 60 на сенсорном экране заставляет приложение MEAP, которое является приложением логического входа, изменить состояние так, чтобы отобразить экран логического входа (см. фиг.10), этап S1101 на фиг.11.

[0085] Приложение MEAP выполнено с возможностью осуществления логического входа с использованием одной или более служб социальных сетей (например, Twitter). Для того, чтобы сделать это, приложение MEAP ранее получило от Twitter набор клиентских учетных данных (идентификатор клиента и секретную часть) для использования в прикладном программном интерфейсе (API) Twitter, поддерживающем протокол OAuth.

[0086] На этапе S1102, изображенном на фиг. 11, приложение MEAP определяет, есть ли у него сохраненный токен доступа OAuth для данного пользователя. Если такой токен доступа действительно есть, приложение MEAP переходит к выполнению этапа S1114. Если токена доступа нет, приложение MEAP переходит к выполнению этапа S1103.

[0087] На этапе S1103, изображенном на фиг. 11, приложение MEAP передает подписанный запрос на получение токена неавторизованного запроса от службы OAuth-аутентификации системы Twitter. В этой точке токен неавторизованного запроса не будет специфичным для владельца ресурса, и может использоваться приложением MEAP для получения одобрения владельца ресурса от пользователя для получения доступа к его/ее учетной записи в Twitter.

[0088] На этапе S1104, изображенном на фиг. 11, служба OAuth-аутентификации системы Twitter отвечает на запрос MEAP токеном неавторизованного запроса. На этапе S1105, изображенном на фиг. 11, когда приложение MEAP получает токен неавторизованного запроса, оно перенаправляет пользователя на адрес URL OAuth-авторизации пользователя системы Twitter (фиг. 10) с токеном неавторизованного запроса для того, чтобы пользователь вошел в систему и авторизовал токен. Адрес URL перенаправления идентифицирует токен неавторизованного запроса и адрес URL обратного вызова для того, чтобы запросить Twitter перенаправить пользователя обратно к приложению MEAP после того, как приложение MEAP получит одобрение.

[0089] На этапе S1106, изображенном на фиг. 11, браузер на многофункциональном периферийном устройстве 10 управляет перенаправлением, отправляя запрос на страницу OAuth-авторизации пользователя системы Twitter. На этапе S1107, изображенном на фиг. 11, пользователь перенаправляется на конкретный URL-адрес системы Twitter (фиг. 10) и от него требуется войти на сайт. Протокол OAuth требует, чтобы Twitter

сначала аутентифицировал владельца ресурса, а затем запросил пользователя (владельца ресурса) предоставить доступ (например, через страницу запроса доступа) к многофункциональному периферийному устройству.

[0090] Пользователь может подтвердить, что он или она теперь находится на веб-странице Twitter, глядя на URL-адрес браузера (фиг. 10), и может ввести свои имя пользователя и пароль в системе Twitter, этапы S1107 и S1108 на фиг. 11.

[0091] Использование веб-браузера для того, чтобы непосредственно осуществить доступ к серверу Twitter, позволяет пользователю сохранять свои имя пользователя и пароль в тайне и не сообщать их приложению MEAP или любому другому сайту. Учетные данные пользователя никогда не вводятся в приложение MEAP.

[0092] Во время входа в Twitter или после успешного входа в Twitter пользователя просят предоставить доступ клиенту, т.е. приложению MEAP. Twitter сообщает пользователю о том, кто запрашивает доступ (в данном случае приложение MEAP) и тип запрашиваемого доступа. Пользователь может разрешить или запретить доступ, этап S1108 на фиг. 11.

[0093] Как только пользователь одобряет запрос, и если введенные учетные данные корректны, Twitter идентифицирует (помечает) токен запроса (временные учетные данные) как «авторизованные владельцем ресурса» со стороны пользователя, этап S1108 на фиг. 11. Если пользователь предоставляет доступ, служба OAuth-аутентификации системы Twitter перенаправляет пользователя назад на адрес URL обратного вызова, который приложение MEAP включило в адрес URL на этапе S1106 (этап S1109 на фиг. 11). Пользователь мог также запретить доступ, и в этом случае служба OAuth-аутентификации системы Twitter выведет на экран страницу, которая отправляет обратно к приложению MEAP. На этапе S1110, изображенном на фиг. 11, браузер пользователя управляет перенаправлением и отправляет запрос на адрес URL обратного вызова. Адрес URL перенаправления содержит значение токена авторизованного запроса. Таким образом, браузер перенаправляется обратно к приложению MEAP вместе с временным идентификатором учетных данных (токеном авторизованного запроса).

[0094] На этапе S1111 приложение MEAP представляет подписанный запрос службе OAuth-аутентификации системы Twitter для того, чтобы обменять токен запроса на токен доступа. На этапе S1112 служба OAuth-аутентификации системы Twitter отвечает на запрос приложения MEAP токеном доступа. Токены запроса используются только для получения пользовательского одобрения, в то время как токены доступа используются для того, чтобы получить доступ к защищенным ресурсам, в данном случае к идентификатору пользователя в системе Twitter (например, к имени пользователя учетной записи Twitter). В первом запросе приложение MEAP обменивает токен запроса на токен доступа путем отправки подписанного запроса в службу аутентификации Twitter, этапы S1111, S1112. Полученный токен доступа, который связан с конкретным пользователем, может быть сохранен (этап S1113 на фиг. 11) так, чтобы в будущем приложение MEAP могло использовать тот же самый токен доступа для выполнения аутентифицированных запросов для того же самого пользователя, (например, радиочастотный идентификатор RFID пользователя может быть сохранен в многофункциональном периферийном устройстве 10 совместно с ранее полученным токеном доступа, как объясняется более подробно в четвертом варианте осуществления). На этапе S1114 приложение MEAP отправляет запрос API, используя токен доступа для аутентификации запроса. В частности, во втором подписанном запросе (могут быть многократные запросы), приложение MEAP получает идентификатор пользователя в

системе Twitter из API Twitter, этап S1115 на фиг. 11. Одновременно с этим происходит доступ к списку многофункционального периферийного устройства для многофункционального периферийного устройства 10, определенному в системе Twitter администратором (как ранее описано со ссылками на фиг. 3-7), и определяется, содержится ли идентификатор пользователя в системе Twitter в списке многофункционального периферийного устройства, представляющем многофункциональное периферийное устройство 10, к которому пользователь хочет получить доступ, см. этапы S1116 и S1117 на фиг. 11. Многофункциональное периферийное устройство 10 может непосредственно получить доступ к учетной записи администратора Twitter, поскольку приложение MEAP хранит и вводит имя пользователя и пароль администратора. Альтернативно, имя пользователя/пароль администратора не хранятся. В этом случае администратор осуществляет логический вход с использованием протокола OAuth через сервлет (веб-интерфейс пользователя) во время конфигурации. Токены доступа и обновления для этой учетной записи затем сохраняются локально. Когда срок действия токена доступа истекает (маловероятно, чтобы это случилось в Twitter), токен обновления может использоваться для повторной аутентификации. Тогда токен доступа администратора используется для того, чтобы получить доступ к учетной записи администратора Twitter и, в свою очередь, к спискам многофункциональных периферийных устройств, определенным администратором в Twitter. Если идентификатор пользователя в системе Twitter содержится в списке, тогда пользователю предоставляется доступ к многофункциональному периферийному устройству. Если идентификатор пользователя в системе Twitter не содержится в списке, тогда на экран многофункционального периферийного устройства 10 может быть выведено сообщение об ошибке.

Второй вариант осуществления

[0095] Описание “НАСТРОЙКА СПИСКА У ПОСТАВЩИКА УСЛУГ”, сделанное выше со ссылками на фиг. 3-7, и описание “ОБЩАЯ ПРОЦЕДУРА ЛОГИЧЕСКОГО ВХОДА”, сделанное выше со ссылкой на фиг. 8, также применимы к этому варианту осуществления, и поэтому эти описания не будут повторены ниже для второго варианта осуществления.

[0096] Логический вход на основе протокола xAuth

[0097] Вариант, альтернативный показанному на фиг. 9-11, будет теперь описан со ссылками на фиг. 12-14. Протокол OAuth спецификации 1.0 является протоколом, который позволяет веб-сайтам или приложениям получать доступ к защищенным веб-ресурсам посредством API, не требуя от пользователей раскрытия их учетных данных. Фиг. 12-14 иллюстрируют способ, позволяющий пользователю обеспечить его учетные данные в тех случаях, когда HTTP-перенаправление к браузеру является недоступным или неподходящим, например тогда, когда у приложения MEAP, работающего на многофункциональном периферийном устройстве 10, нет никакого механизма, чтобы вызвать веб-браузер. Этот вариант осуществления реализует версию OAuth, которая называется xAuth (из-за x_auth заголовков, которые она использует). Эта версия OAuth использует схему, отличающуюся от традиционного OAuth, который требует передачи информации к браузеру и обратно, как описано со ссылками на фиг. 9-11.

[0098] Расширение xAuth протокола OAuth позволяет клиентам (например, приложению MEAP) получать учетные данные пользователя, а затем обменивать их на токен доступа OAuth без захода в браузер. Расширение xAuth является подходящим для настольных и мобильных приложений, которые работают в доверенном контексте (в отличие от веб-приложений, которые обычно работают в ненадежном контексте).

[0099] Расширение xAuth все еще является частью протокола OAuth. Подписанные запросы точно так же необходимо отправлять конкретному поставщику услуг (например, Twitter).

[0100] Процесс xAuth дает в результате токены доступа только для чтения или для чтения-записи. Прямой доступ к чтению сообщения xAuth не предоставляет.

[0101] Расширение xAuth обеспечивает настольным и мобильным приложениям способ обменивать имя пользователя и пароль на токен доступа OAuth. Как только токен доступа получен, пароль, соответствующий пользователю, уничтожается мобильным/настольным приложением. Имя пользователя также может быть уничтожено мобильным/настольным приложением. Однако имя пользователя может быть сохранено мобильным/настольным приложением, как будет объяснено более подробно для этапа 1403, изображенного на фиг. 14.

[0102] Расширение xAuth позволяет настольным и мобильным приложениям пропускать этапы получения токена запроса и авторизации и сразу переходить к этапу получения токена доступа.

[0103] Клиентский запрос на получение токена доступа

[0104] Обращаясь теперь к иллюстрациям на фиг. 12-14, вообразим себе сценарий, в котором пользователь приближается к многофункциональному периферийному устройству 10 и хочет получить доступ к многофункциональному периферийному устройству 10. Когда пользователь смотрит на блок 24 отображения многофункционального периферийного устройства 10, он или она видит дисплей, соответствующий фиг. 12. Пользователь использует сенсорный экран блока 24 отображения для того, чтобы выбрать иконку 70 'Зарегистрироваться в Twitter'. Касание иконки 70 на сенсорном экране заставляет приложение MEAP, которое является приложением логического входа, изменить состояние так, чтобы отобразить экран логического входа, этап S1401 на фиг. 14. Приложение MEAP выполнено с возможностью поддерживать логический вход с использованием одного или более поставщиков услуг, например, служб социальных сетей, таких как Twitter, Facebook и Google+. Приложение MEAP запрашивает у пользователя ввод его учетных данных для аутентификации в приложение MEAP, используя операционный блок 25, см. фиг. 13 и этап S1402 на фиг. 14. В этом варианте осуществления, поскольку пользователь вводит свое имя пользователя непосредственно в приложение MEAP (фиг. 13), приложение MEAP, возможно, ранее сохранило вводимое имя пользователя совместно с токеном доступа для этого конкретного пользователя. На этапе S1403, изображенном на фиг. 14, приложение MEAP проверяет, был ли ранее сохранен токен доступа для конкретного пользователя. Если токен доступа был ранее сохранен, сразу происходит переход к этапу S1407 на фиг. 14. Если токен доступа не был ранее сохранен для конкретного пользователя, выполнение продолжается и происходит переход к этапу S1404 на фиг. 14. На этапе S1404, изображенном на фиг. 14, для того, чтобы запросить токен доступа для безбраузерного приложения MEAP, приложение MEAP делает SSL-запрос (протокол HTTPS) на URL-адрес токена доступа поставщика услуг (например, URL-адрес токена доступа Twitter https://api.twitter.com/oauth/access_token) с абонентским ключом приложения MEAP. В дополнение к обычным параметрам подписи oauth_*, должны быть представлены следующие параметры:

x_auth_username - учетные данные логического входа пользователя, от имени которого клиент получает токен

x_auth_password - учетные данные пароля пользователя, от имени которого клиент получает токен.

x_auth_mode - это значение должно быть "client_auth" (см. описанный здесь процесс)
[0105] ОТВЕТ

[0106] Для того, чтобы предоставить токен доступа, поставщик услуг (например, провайдер социальной сети, такой как Twitter) проверяет, что:

- 5 - подпись запроса была успешно проверена, как это определено спецификацией OAuth.
- запрос с предоставленной отметкой времени и данным временем никогда не был получен ранее.
- предоставленные имя пользователя и пароль соответствуют учетным данным
- 10 пользователя.

В случае успешных проверок поставщик услуг (например, API Twitter) генерирует токен доступа и секретную часть токена и возвращает их в теле ответа HTTP, см. этап S1405 на фиг.14. Ответ содержит следующие параметры:

- oauth_token - токен доступа.
- 15 - oauth_token_secret - секретная часть токена.
- x_auth_expires - отметка времени, в секундах от 1970-01-01T00:00, когда срок действия токена доступа истекает, или 0, если его срок действия неограничен.
- Дополнительные параметры - любые дополнительные параметры, определяемые поставщиком услуг.

20 [0107] Доступ к защищенным ресурсам

- [0108] После успешного получения токена доступа и секретной части токена приложение MEAP может получить доступ к защищенным ресурсам от имени пользователя в соответствии с разделом 7 спецификации протокола OAuth. Другими словами, токен доступа, полученный в данном случае, ничем не отличается по
- 25 возможностям от токена доступа, определенного спецификацией OAuth. Полученный токен доступа, который связан с конкретным пользователем, может быть сохранен (этап S1406 на фиг. 14) приложением MEAP так, чтобы на фиг. 14 можно было от этапа S1403 перейти сразу к этапу S1407, когда конкретный пользователь в следующий раз захочет осуществить доступ к многофункциональному периферийному устройству 10.
- 30 После аутентификации с использованием вышеупомянутого процесса приложение MEAP будет подписывать все последующие запросы на защищенные ресурсы пользователя (для конкретного идентификатора пользователя в системе Twitter), используя полученную ранее секретную часть токена (этапы S1407 и S1408 на фиг. 14), что также имеет место при использовании протокола OAuth. В частности, приложение
- 35 MEAP использует полученный токен доступа для того, чтобы запросить API поставщика услуг (например, API Twitter) для получения идентификатора пользователя в системе Twitter (имени пользователя). Как только приложение MEAP получило идентификатор пользователя в системе Twitter (этап S1408 на фиг. 14), в фоновом режиме, осуществляется доступ к списку многофункционального периферийного устройства
- 40 для многофункционального периферийного устройства 10, который определяется в Twitter администратором (как объяснено выше со ссылками на фиг. 3-7), и определяется, содержится ли идентификатор пользователя в системе Twitter в списке многофункционального периферийного устройства, представляющем многофункциональное периферийное устройство 10, к которому пользователь хочет
- 45 получить доступ, см. этапы S1409 и S1410 на фиг. 14. Если идентификатор пользователя в системе Twitter содержится в списке, тогда пользователю предоставляется доступ к многофункциональному периферийному устройству 10. Если идентификатор пользователя в системе Twitter не содержится в списке, тогда на экран

многофункционального периферийного устройства 10 выводится сообщение об ошибке.

Третий Вариант осуществления

[0109] Фиг. 15 показывает архитектуру системы обработки изображений третьего варианта осуществления. Система обработки изображений включает в себя многофункциональное периферийное устройство (MFP) 10 и сервер 12 аутентификации, аналогичные первому и второму вариантам осуществления, а также мобильное устройство, например, мобильный телефон 11. Многофункциональное периферийное устройство 10, мобильный телефон 11 и сервер 12 аутентификации могут связываться друг с другом, используя сеть, например, сеть Wi-Fi 14 и Интернет.

[0110] Фиг. 16 показывает аппаратную конфигурацию мобильного телефона 11. Мобильный телефон 11 включает в себя блок 30 управления, соединенный с блоком 31 цифровой обработки сигналов. Блок 30 управления управляет работой блока 32 отображения, операционного блока 33, блока 34 камеры, внешнего интерфейса 35, блока 36 беспроводной связи и блока 37 электропитания. Блок 32 отображения включает в себя жидкокристаллический дисплей для отображения информации пользователю телефона 11. Операционный блок 33 включает в себя клавиатуру и другие рабочие кнопки для того, чтобы позволить пользователю осуществлять ввод информации в мобильный телефон 11. Блок 34 камеры является камерой, которая интегрируется в телефон 11 для того, чтобы позволить пользователю фотографировать и собирать визуальную информацию. Внешний интерфейс 35 является портом, предусмотренным в мобильном телефоне 11 для того, чтобы позволить мобильному телефону 11 связываться с другими устройствами. В частности, внешний интерфейс 35 позволяет мобильному телефону 11 соединяться с компьютером в целях синхронизации данных (контактной информации, календарных записей и т.д.), сохраненных на мобильном телефоне 11, с данными, хранящимися на компьютере. Блок 36 беспроводной связи обеспечивает поддержку для различных услуг беспроводной связи. В частности, блок 36 беспроводной связи обеспечивает поддержку связи по стандарту Wi-Fi. Блок 36 беспроводной связи соединяется с антенной 38. Блок 37 электропитания включает в себя батарею и механизм для зарядки батареи от внешнего электропитания.

[0111] Блок 31 цифровой обработки сигналов соединяется с блоком 39 аудиовхода, блоком 40 аудиовыхода и блоком радиочастотного ввода/вывода 41. Блок 39 аудиовхода является аналого-цифровым процессором для получения и преобразования аудиосигналов от микрофона 42. Блок аудиовыхода 40 является цифро-аналоговым процессором для получения и преобразования цифровых сигналов в аналоговый вывод, который выводится на динамик 43. Блок радиочастотного ввода/вывода 41 соединяется с антенной 44 и используется для того, чтобы позволить мобильному телефону 11 связываться с локальной базовой станцией мобильного телефона. Блок 39 аудиовхода, блок 40 аудиовыхода, блок 31 цифровой обработки сигналов и блок радиочастотного ввода/вывода 41 позволяют мобильному телефону 11 работать как портативный телефон.

[0112] Мобильный телефон 11 представляет собой так называемый 'смартфон' и выполняет операционную систему Google (зарегистрированный торговый знак) Android (зарегистрированный торговый знак). В других вариантах осуществления могут использоваться другие типы телефона, включая те, которые выполняют другие операционные системы для мобильного телефона.

[0113] Описание "НАСТРОЙКА СПИСКА У ПОСТАВЩИКА УСЛУГ", сделанное выше со ссылками на фиг. 3-7, и описание "ОБЩАЯ ПРОЦЕДУРА ЛОГИЧЕСКОГО ВХОДА", сделанное выше со ссылкой на Фиг. 8, также применимы к этому варианту

осуществления, и поэтому эти описания не будут повторены ниже для третьего варианта осуществления. Следует отметить, что на фиг. 8 для третьего варианта осуществления получаемые данные для логического входа представляют собой ПИН-код.

[0114] Доступ с использованием мобильного телефона

5 [0115] Вариант, альтернативный показанным на фиг. 9-11 и на фиг. 12-14, будет теперь описан со ссылками на фиг. 17-19. Фиг. 17-19 иллюстрируют способ, позволяющий пользователю обеспечить его учетные данные с использованием механизма OAuth в том случае, когда у приложения MEAP, работающего на многофункциональном периферийном устройстве 10, нет никакого механизма для вызова веб-браузера.

10 [0116] В иллюстративных целях вообразим себе сценарий, в котором пользователь с мобильным телефоном 11 приближается к многофункциональному периферийному устройству 10 и хочет произвести сканирование или печать с использованием многофункционального периферийного устройства 10. Когда пользователь смотрит на блок 24 отображения многофункционального периферийного устройства 10, он или
15 она видит дисплей, соответствующий фиг. 17. Пользователь использует сенсорный экран блока 24 отображения для того, чтобы выбрать иконку 50 'Зарегистрироваться в Twitter'. Касание иконки 50 на сенсорном экране заставляет приложение MEAP, которое является приложением логического входа, изменить состояние так, чтобы отобразить экран логического входа, этап S1901 на фиг. 19.

20 [0117] Приложение MEAP выполнено с возможностью обеспечения логического входа с использованием одной или более служб социальных сетей (например, Twitter). Для того, чтобы сделать это, приложение MEAP ранее получило от Twitter набор клиентских учетных данных (идентификатор клиента и секретную часть) для использования в прикладном программном интерфейсе (API) Twitter, поддерживающем
25 протокол OAuth.

[0118] Приложение MEAP запрашивает у системы Twitter набор временных учетных данных путем отправки подписанного запроса, включающего в себя `oauth_callback=`
ооб в качестве одного из параметров запроса, чтобы получить токен запроса от службы OAuth-аутентификации системы Twitter, этап S1902 на фиг. 19. В этой точке временные
30 учетные данные не являются специфичными для владельца ресурса, и могут использоваться приложением MEAP для получения одобрения владельца ресурса от пользователя для получения доступа к его/ее учетной записи в Twitter.

[0119] Когда приложение MEAP получает временные учетные данные (токен запроса), см. этап S1903 на фиг. 19, оно генерирует ссылку на адрес URL OAuth-авторизации
35 пользователя системы Twitter, включающую в себя параметр `oauth_token` (соответствующий токenu запроса). Приложение MEAP затем встраивает ссылку на адрес URL OAuth-авторизации пользователя системы Twitter в машиночитаемый код или в штрих-код (например, в QR-код) и отображает штрих-код на блоке 24 отображения многофункционального периферийного устройства 10, этап S1904 на фиг. 19.

40 [0120] Пользователь при помощи мобильного телефона 11 затем сканирует (этап S1905 на фиг. 19) машиночитаемый код, отображенный на многофункциональном периферийном устройстве 10, используя подходящее приложение на мобильном телефоне, в результате чего веб-браузер мобильного телефона 11 перенаправляется на
адрес URL OAuth-авторизации пользователя системы Twitter, этапы S1906 и S1907 на
45 фиг. 19, где от пользователя требуется войти в Twitter, см. фиг. 18 и этапы S1908 и S1909 на фиг. 19. Как и прежде, протокол OAuth требует, чтобы серверы сначала аутентифицировали владельца ресурса (пользователя), а затем запросили его предоставить доступ клиенту (например, приложению MEAP).

[0121] Пользователь может подтвердить, что он или она теперь находится на веб-странице Twitter, глядя на URL-адрес браузера (фиг. 18) и вводя свои имя пользователя Twitter и пароль, см. фиг.18 и этап S1909 на фиг. 19.

[0122] OAuth позволяет пользователю сохранять свои имя пользователя и пароль в тайне и не сообщать их приложению MEAP или любому другому сайту. Учетные данные пользователя никогда не вводятся в приложение MEAP.

[0123] Во время входа в Twitter или после успешного входа в Twitter пользователя просят предоставить доступ клиенту, т.е. приложению MEAP. Twitter сообщает пользователю о том, кто запрашивает доступ (в данном случае приложение MEAP) и тип запрашиваемого доступа. Пользователь может разрешить или запретить доступ (этап S1909 на фиг. 19).

[0124] Как только пользователь одобряет запрос, и если введенные учетные данные допустимы, Twitter идентифицирует (помечает) временные учетные данные как «авторизованные владельцем ресурса» со стороны пользователя. Браузер на мобильном телефоне 11 затем перенаправляется на страницу, отображающую oauth_verifier (например, ПИН-код) (этап S1910 на фиг. 19).

[0125] Пользователь вводит ПИН-код на экране приложения MEAP, используя операционный блок многофункционального периферийного устройства 10 (этап S1911 на фиг. 19), приложение MEAP может также сохранить введенный ПИН-код (этап S1912 на фиг. 19).

[0126] В то время как пользователь ожидает, приложение MEAP в фоновом режиме использует токен запроса авторизации, включающий в себя ПИН-код, введенный пользователем в качестве значения для oauth_verifier, и обменивает его на токена доступа, см. этапы S1913 и 1914 на фиг. 19. Токены запроса используются только для получения пользовательского одобрения, в то время как токены доступа используются для того, чтобы получить доступ к защищенным ресурсам, в данном случае к идентификатору пользователя в системе Twitter. В первом запросе приложение MEAP обменивает токен запроса на токен доступа путем отправки подписанного запроса в службу аутентификации Twitter, см. этапы S1913 и S1914 на фиг. 19. Полученный токен доступа, который связан с конкретным пользователем, может быть сохранен (этап S1915 на фиг. 19) так, чтобы в будущем приложение MEAP могло использовать тот же самый токен доступа для выполнения аутентифицированных запросов для того же самого пользователя. Во втором запросе (могут быть многократные запросы), приложение MEAP получает идентификатор пользователя в системе Twitter, см. этапы 1916 и 1917 на фиг. 19. Одновременно с этим в фоновом режиме происходит доступ к списку многофункционального периферийного устройства для многофункционального периферийного устройства 10, определенному в системе Twitter администратором (как ранее описано со ссылками на фиг. 3-7), и определяется, содержится ли идентификатор пользователя в системе Twitter в списке многофункционального периферийного устройства, представляющем многофункциональное периферийное устройство 10, к которому пользователь хочет получить доступ, см. этапы 1918 и 1919 на фиг. 19. Если идентификатор пользователя в системе Twitter содержится в списке, тогда пользователю предоставляется доступ к многофункциональному периферийному устройству 10. Если идентификатор пользователя в системе Twitter не содержится в списке, тогда на экран многофункционального периферийного устройства 10 может быть выведено сообщение об ошибке.

[0127] Oauth_callback является дополнительным параметром, который, обращаясь к фиг. 9-11, определяет адрес URL, на который пользователь будет перенаправлен после

предоставления приложению MEAP доступа к учетной записи Twitter пользователя. Обращаясь к фиг. 17-19, параметр `oauth_callback` устанавливается в `oauth_callback=oob`, что вызывает отображение ПИН-кода на экране многофункционального периферийного устройства 10. Однако, возможно пропустить этап отображения ПИН-кода (этап 1910 на фиг. 19), не устанавливая значение параметра `oauth_callback`. Следовательно, после того, как пользователь успешно завершит процесс логического входа (этап 1909 на фиг. 19), может быть осуществлен переход непосредственно к этапу 1913, где токен запроса обменивается на токен доступа.

Четвертый вариант осуществления

[0128] Описание “НАСТРОЙКА СПИСКА У ПОСТАВЩИКА УСЛУГ”, сделанное выше со ссылками на фиг. 3-7, и описание “ОБЩАЯ ПРОЦЕДУРА ЛОГИЧЕСКОГО ВХОДА”, сделанное выше со ссылкой на фиг. 8, также применимы к этому варианту осуществления, и поэтому эти описания не будут повторены ниже для четвертого варианта осуществления.

[0129] Обращаясь теперь к иллюстрациям на фиг. 20А и фиг. 20В, вообразим себе сценарий, в котором пользователь приближается к многофункциональному периферийному устройству 10 и хочет получить доступ к многофункциональному периферийному устройству 10. В этом варианте осуществления пользователь использует RFID-карту или RFID-метку (например, прикрепленную к мобильному телефону 11) для того, чтобы получить доступ к многофункциональному периферийному устройству 10. Когда пользователь подносит свою RFID-карту или RFID-метку к устройству 212 считывания с карт, приложение MEAP, которое является приложением логического входа, изменяет свое состояние так, чтобы отобразить экран логического входа на многофункциональном периферийном устройстве 10. Приложение MEAP поддерживает реестр пользователей, которые ранее получили доступ к многофункциональному периферийному устройству 10, и на основе полученного идентификатора RFID определяет, был ли токен доступа ранее сохранен для конкретного пользователя (см. фиг. 20А).

[0130] На этапе S2001, изображенном на фиг. 20В, приложение MEAP получает идентификатор RFID посредством устройства 212 считывания с карт. На этапе S2002, изображенном на фиг. 20В, приложение MEAP определяет, существует ли токен доступа, соответствующий полученному идентификатору RFID, в реестре, сохраняемом приложением MEAP.

[0131] Если токен доступа для полученного идентификатора RFID существует, управление на фиг. 20В передается к этапу S2003. На этапе S2003 происходит доступ к списку многофункционального периферийного устройства для многофункционального периферийного устройства 10, определенному в системе Twitter администратором (как ранее описано со ссылками на фиг. 3-7), и определяется, содержится ли идентификатор пользователя в системе Twitter в списке многофункционального периферийного устройства, представляющем многофункциональное периферийное устройство 10, к которому пользователь хочет получить доступ.

[0132] Если идентификатор пользователя в системе Twitter содержится в списке, тогда пользователю предоставляется доступ к многофункциональному периферийному устройству (этап S2004 на фиг. 20В). Если идентификатор пользователя в системе Twitter не содержится в списке, тогда на экран многофункционального периферийного устройства 10 может быть выведено сообщение об ошибке (этап S2005). Этапы S2003, S2004, S2005 соответствуют этапам 1114-1117 на фиг. 11, этапам 1407-1410 на фиг. 14 и этапам 1916-1919 на фиг. 19.

[0133] На этапе 2002, изображенном на фиг. 20В, если определено, что для полученного RFID токена доступа не существует, на фиг. 20В происходит переход к этапу S2006. На этапе 2006 токен доступа может быть получен по любой из ранее описанных блок-схем, изображенных на фиг. 8, фиг. 11, фиг. 14 и фиг. 19. Как только токен доступа получен приложением MEAP, приложение MEAP сохраняет идентификатор RFID конкретного пользователя и соответствующий ему токен доступа в реестре (см. фиг. 20А).

Пятый вариант осуществления

[0134] Архитектура устройства обработки изображений (фиг. 15) и аппаратная конфигурация мобильного телефона (фиг. 16), описанные в третьем варианте осуществления, также применимы к этому варианту осуществления, и поэтому описание этих чертежей не будет повторено в данном варианте осуществления. Описание “НАСТРОЙКА СПИСКА У ПОСТАВЩИКА УСЛУГ”, сделанное выше со ссылками на фиг. 3-7, также применимо к этому варианту осуществления, и поэтому описание этих чертежей не будет повторено в данном варианте осуществления. “Доступ с использованием мобильного телефона” в пятом варианте осуществления выполняется следующим образом.

[0135] В иллюстративных целях вообразим себе сценарий, в котором пользователь с мобильным телефоном 11 приближается к многофункциональному периферийному устройству 10 и хочет произвести сканирование или печать с использованием многофункционального периферийного устройства 10. Когда пользователь смотрит на блок 24 отображения многофункционального периферийного устройства 10, он или она видит дисплей, соответствующий фиг. 17. Пользователь использует сенсорный экран блока 24 отображения для того, чтобы выбрать иконку 50 ‘Зарегистрироваться в Twitter’. Касание иконки 50 на сенсорном экране заставляет приложение MEAP, которое является приложением логического входа, изменить состояние так, чтобы отобразить экран логического входа, этап S2101 на фиг. 21.

[0136] Приложение MEAP выполнено с возможностью обеспечения логического входа с использованием одной или более служб социальных сетей (например, Twitter). Для того, чтобы сделать это, администратор предварительно создал учетную запись в службе социальных сетей (например, учетную запись Twitter) для многофункционального периферийного устройства 10. Приложение MEAP, выполняющееся на многофункциональном периферийном устройстве 10, выполнено с возможностью генерирования случайного числа с использованием генератора случайных или псевдослучайных чисел, см. этап S2102 на фиг. 21. Приложение MEAP соединяется с учетной записью многофункционального периферийного устройства в системе Twitter (этап S2103 на фиг. 21) и регистрирует случайное число совместно с одним или более пользователями службы социальных сетей (этап S2104 на фиг. 21). Например, случайное число могло быть связано (соединено) со списками пользователей, описанными выше со ссылками на фиг. 3-7. Приложение MEAP выполнено с возможностью встраивания случайного числа и информации, идентифицирующей учетную запись многофункционального периферийного устройства в системе Twitter (имя пользователя) в машиночитаемый код или в штрих-код (например, в QR-код), см. этап S2105 на фиг. 21, и отображает машиночитаемый код или штрих-код на блоке 24 отображения многофункционального периферийного устройства 10, см. этап S2106 на фиг. 21.

[0137] Пользователь с мобильным телефоном 11 затем запускает на мобильном телефоне 11 приложение для аутентификации пользователя на периферийном устройстве

(этап S2201 на фиг. 22). Приложение на мобильном телефоне 11 используется для того, чтобы отсканировать машиночитаемый код или штрих-код, отображенный на многофункциональном периферийном устройстве 10, см. этап S2202 на фиг. 22, и приложение выполнено с возможностью автоматического входа пользователя в его учетную запись Twitter, см. этап S2203 на фиг. 22. Кроме того, приложение выполнено с возможностью генерировать сообщение, включающее в себя идентификационный код, отображаемый на периферийном устройстве, и информацию, идентифицирующую учетную запись пользователя в социальной сети, см. этап S2204 на фиг. 22. Приложение затем отправляет прямое сообщение или твит, который может быть просмотрен приложением MEAP с использованием учетной записи многофункционального периферийного устройства в системе Twitter, см. этап S2205 на фиг. 22. Сообщение может быть отправлено напрямую (прямое сообщение, то есть конфиденциально) учетной записи многофункционального периферийного устройства в системе Twitter (ящик для приема входящих сообщений), или оно может быть отправлено так, что оно будет доступно для множества пользователей Twitter. Например, твит может быть отправлен (опубликован) «поклонникам» пользователя (followers, те, кто следит за твитами данного пользователя). Конечно же, этап входа в Twitter, этап генерации сообщения и этап отправки сообщения могут быть выполнены пользователем вручную. Приложение MEAP, выполняющееся на многофункциональном периферийном устройстве 10, выполнено с возможностью получать сообщение от системы Twitter посредством логического входа с учетной записью многофункционального периферийного устройства в системе Twitter, см. этап S2301 на фиг. 23. Приложение MEAP выполнено с возможностью определять, соответствует ли детальная информация, содержащаяся в сообщении, зарегистрированной детальной информации (см. этап S2104 на фиг. 21) в учетной записи многофункционального периферийного устройства в социальной сети, см. этап S2302 на фиг. 23. Например, приложение MEAP определяет, соответствуют ли идентификатор пользователя и случайное число, содержащееся в сообщении, числу и идентификатору пользователя, зарегистрированным в учетной записи многофункционального периферийного устройства в системе Twitter. Если детальная информация соответствует, многофункциональное периферийное устройство 10 предоставляет доступ пользователю, см. этап S2303 на фиг. 23. Приложение MEAP может предоставлять различные уровни доступа различным пользователям на основе информации об учетной записи пользователя в службе социальных сетей. Например, пользователю с именем username1 может быть разрешено копировать и сканировать, а пользователю с именем username2 может быть разрешено только копировать. Конечно же, если детальная информация, полученная в сообщении, не соответствует детальной информации, зарегистрированной в учетной записи Twitter, тогда многофункциональное периферийное устройство 10 не предоставляет доступ пользователю, см. этап S2304 на фиг. 23.

[0138] В альтернативном варианте осуществления идентификационная информация генерируется на основе координат глобальной спутниковой системы позиционирования GPS для многофункционального периферийного устройства 10. Многофункциональное периферийное устройство 10 регистрирует предопределенное количество цифр из координат GPS многофункционального периферийного устройства в качестве части первой части идентификационной информации, регистрируемой в службе социальных сетей (например, Twitter). В случае, когда пользователь хочет получить доступ к многофункциональному периферийному устройству 10, пользователь помещает мобильный телефон 11 на многофункциональное периферийное устройство 10 и

открывает предопределенное приложение на мобильном телефоне 11. Предопределенное приложение получает доступ к блоку GPS на мобильном телефоне 11 и определяет координаты GPS, идентифицирующие положение мобильного телефона (альтернативно, мобильный телефон может считать координаты GPS с дисплея многофункционального периферийного устройства). Приложение на мобильном телефоне 11 выбирает предопределенное количество цифр из координат GPS и использует эти цифры в качестве идентификационной информации в сообщении, которое будет отправлено многофункциональному периферийному устройству 10. Поскольку мобильный телефон 11 и многофункциональное периферийное устройство 10 находятся в одном и том же месте (мобильный телефон 11 лежит на многофункциональном периферийном устройстве 10), первая часть идентификационной информации, зарегистрированной для многофункционального периферийного устройства 10, соответствует идентификационной информации, сгенерированной мобильным телефоном 11, и если идентификатор пользователя в системе Twitter (который также содержится в сообщении, отправленном с мобильного телефона на многофункциональное периферийное устройство 10), связан с координатами GPS для многофункционального периферийного устройства 10, зарегистрированными в системе Twitter, тогда пользователю предоставляется доступ к многофункциональному периферийному устройству 10.

Шестой вариант осуществления

[0139] В этом варианте осуществления администратор настраивает учетную запись в службе социальных сетей (например, Twitter) для многофункционального периферийного устройства 10. Приложение MEAP, выполняющееся на многофункциональном периферийном устройстве 10, выполнено с возможностью соединяться с учетной записью многофункционального периферийного устройства в службе социальных сетей, см. этап S2401 на фиг. 24, и отправлять информацию относительно работы многофункционального периферийного устройства 10 пользователям службы социальных сетей, см. этап S2402 на фиг. 24. Например, у многофункционального периферийного устройства 10 есть учетная запись в системе Twitter. Заинтересованные пользователи могут быть «поклонниками» многофункционального периферийного устройства 10 - обычно они будут пользователями типа администратор. Многофункциональное периферийное устройство 10 тогда может быть выполнено с возможностью отправлять твит с информацией о своем состоянии, например, «бумага закончилась», «замятие бумаги» и другие ошибки, или с информацией о его использовании, например, идентифицируя пользователя многофункционального периферийного устройства 10, детализируя затраты пользователя на использование многофункционального периферийного устройства 10, с информацией относительно расположения периферийного устройства, с информацией относительно общей или индивидуальной пользовательской активности периферийного устройства, с информацией, детализирующей материалы (например, тип бумаги), используемые периферийным устройством для обработки пользовательских действий, и с сервисной информацией (например, запрос на обслуживание).

Седьмой вариант осуществления

[0140] Этот вариант осуществления является вариацией шестого варианта осуществления. В этом варианте осуществления многофункциональное периферийное устройство 10 выполнено с возможностью использовать его учетную запись в службе социальных сетей для того, чтобы отправлять дружественным пользователям службы социальных сетей информацию об активности пользователя. Например, предполагая, что у многофункционального периферийного устройства 10 есть учетная запись в

системе Twitter, приложение MEAP может быть выполнено с возможностью отправлять твит об активности пользователя, возможно, в качестве маркетингового инструмента для рекламного вещания, например, '@JoeBloggs только что скопировал 15 страниц в великолепном цвете Canon! Выбирайте Canon!'. В этом случае приложение MEAP в
 5 многофункциональном периферийном устройстве 10 будет отправлять твиты, используя учетную запись пользователя в системе Twitter, и пользователь должен предоставить ему доступ для таких действий. Это может произойти во время ранее обсужденного процесса логического входа по протоколу OAuth/xAuth. Альтернативно многофункциональное периферийное устройство 10 отправляет твиты, используя свою
 10 собственную учетную запись, и упоминает в твитах учетную запись пользователя.

[0141] Варианты осуществления настоящего изобретения были описаны выше. Дополнительные варианты осуществления настоящего изобретения также могут быть реализованы системами, которые считывают и выполняют программы, записанные на запоминающем устройстве, с тем, чтобы выполнить функции вышеописанного варианта
 15 (вариантов) осуществления, а также способом, этапы которого выполняются путем, например, считывания и выполнения программы, записанной на запоминающем устройстве, с тем, чтобы выполнить функции вышеописанного варианта (вариантов) осуществления. С этой целью, программа (программы) может быть обеспечена для периферийного устройства, мобильного устройства и системы обработки изображений,
 20 например посредством сети или на носителе записи различных типов, служащем в качестве запоминающего устройства (например, машиночитаемый носитель).

Формула изобретения

1. Способ аутентификации пользователя в периферийном устройстве (10),
 25 включающий в себя следующие выполняемые периферийным устройством (10) этапы, на которых:

принимают (S810) запрос логического входа от пользователя;

отправляют (S820) службе социальных сетей запрос аутентификации учетной записи пользователя в службе социальных сетей;

30 принимают (S830) от службы социальных сетей информацию учетной записи пользователя в службе социальных сетей;

определяют (S840) на основе информации учетной записи пользователя в службе социальных сетей, разрешено ли пользователю осуществлять доступ к периферийному устройству, посредством соединения с учетной записью администратора службы
 35 социальных сетей, чтобы определить, связана ли информация учетной записи пользователя в службе социальных сетей со списком в службе социальных сетей (S1116, S1117, S1409, S1410); и

в случае, если в результате этого определения на основе информации учетной записи пользователя в службе социальных сетей определено, что пользователю разрешено
 40 осуществить доступ к периферийному устройству, обеспечивают (S850, S860) пользователю доступ к периферийному устройству (10).

2. Способ по п. 1, в котором периферийное устройство (10) представлено в службе социальных сетей путем связывания с одним или более списками членов службы социальных сетей в службе социальных сетей.

45 3. Способ по п. 2, в котором связывание представления периферийного устройства (10) в службе социальных сетей с одним или более списками членов службы социальных сетей включает в себя определение уровней доступа к функциям периферийного устройства (10) для одного или более списков членов службы социальных сетей.

4. Способ по п. 1, в котором при упомянутой отправке запроса в службу социальных сетей запрашивают токен доступа у службы социальных сетей (S1111, S1112, S1407, S1408).

5. Способ по п. 4, в котором при упомянутом определении используют токен доступа для получения имени пользователя в службе социальных сетей и определяют, связано ли имя пользователя с представлением периферийного устройства в службе социальных сетей (S1114-S1117, S1407-S1410).

6. Способ по п. 4, дополнительно включающий в себя этап, на котором сохраняют токен доступа на периферийном устройстве (10) в привязке к информации, идентифицирующей пользователя (S1113, S1406).

7. Способ по п. 6, в котором при упомянутом сохранении сохраняют токен доступа в привязке к RFID пользователя (S2002).

8. Способ по п. 6, в котором сохраненный токен доступа предназначен для выполнения повторных запросов логического входа от имени пользователя.

9. Способ по п. 4, в котором при упомянутом запрашивании токена доступа у службы социальных сетей используют процесс аутентификации в соответствии с протоколами OAuth или xAuth.

10. Способ по п. 1, в котором периферийное устройство (10) включает в себя периферийное оборудование, которое функционирует

как по меньшей мере одно из принтера, факса и сканера.

11. Способ по п. 1, в котором перед упомянутой отправкой запроса в службу социальных сетей производится определение мобильным устройством (11) (S1905) первой части информации, предоставленной периферийным устройством (10).

12. Способ по п. 11, в котором первая часть информации является адресом URL; при этом периферийное устройство (10) предоставляет адрес URL пользователю; и при этом мобильное устройство (11) определяет адрес URL посредством ввода адреса URL в мобильное устройство (11) пользователем.

13. Способ по п. 12, в котором URL, принятый мобильным устройством (11), позволяет пользователю входить в службу социальных сетей.

14. Способ по п. 12, в котором URL, принятый мобильным устройством (11), позволяет пользователю входить в службу социальных сетей (S1909) и авторизовать выдачу токена доступа к периферийному устройству (10).

15. Способ по п. 11, в котором периферийное устройство (10) предоставляет машиночитаемый код, кодирующий первую часть информации; и

при этом мобильное устройство (11) определяет (S1905) первую часть информации посредством чтения и декодирования машиночитаемого кода, предоставленного периферийным устройством (10).

16. Способ по п. 11, в котором после упомянутой отправки в службу социальных сетей запроса аутентификации пользователя производится определение (S1910) мобильным устройством (11) второй части информации, предоставленной службой социальных сетей.

17. Способ по п. 16, в котором вторая часть информации является кодом, и способ включает в себя (S1911) прием периферийным устройством (10) кода от пользователя через пользовательский интерфейс (25) периферийного устройства (10).

18. Способ по п. 15, в котором машиночитаемый код является штрихкодом или QR-кодом.

19. Носитель информации, на котором сохранена программа, которая при ее исполнении на периферийном устройстве (10) предписывает периферийному устройству

(10) выполнять способ по любому из пп. 1-18.

20. Носитель информации, на котором сохранена программа, которая при ее исполнении на мобильном устройстве (11) предписывает мобильному устройству (11) выполнять способ по любому из пп. 11-18.

- 5 21. Периферийное устройство (10), выполненное с возможностью принимать от пользователя запрос логического входа; отправлять в службу социальных сетей запрос аутентификации учетной записи пользователя в службе социальных сетей; принимать от службы социальных сетей информацию учетной записи пользователя в службе социальных сетей; 10 определять на основе информации учетной записи пользователя в службе социальных сетей, разрешено ли пользователю осуществлять доступ к периферийному устройству (10), посредством соединения с учетной записью администратора службы социальных сетей, чтобы определить, связана ли информация учетной записи пользователя в службе социальных сетей со списком в службе социальных сетей (S1116, S1117, S1409, S1410); и 15 в случае, если периферийное устройство (10) на основе информации учетной записи пользователя в службе социальных сетей определило, что пользователю разрешено осуществить доступ к периферийному устройству (10), обеспечивать пользователю доступ к периферийному устройству (10). 20

22. Система для аутентификации пользователя периферийного устройства (10), которая включает в себя:

- периферийное устройство (10), выполненное с возможностью принимать от пользователя запрос логического входа и отправлять в службу социальных сетей запрос аутентификации учетной записи пользователя в службе социальных сетей; и 25 службу социальных сетей, выполненную с возможностью принимать данный запрос и отправлять информацию учетной записи пользователя в службе социальных сетей периферийному устройству (10); при этом периферийное устройство (10) выполнено с возможностью 30 принимать от службы социальных сетей информацию учетной записи пользователя в службе социальных сетей; определять на основе информации учетной записи пользователя в службе социальных сетей, разрешено ли пользователю осуществлять доступ к периферийному устройству (10), посредством 35 соединения с учетной записью администратора службы социальных сетей, чтобы определить, связана ли информация учетной записи пользователя в службе социальных сетей со списком в службе социальных сетей (S1116, S1117, S1409, S1410); и в случае если периферийное устройство (10) на основе информации учетной записи пользователя в службе социальных сетей определило, что пользователю разрешено 40 осуществить доступ к периферийному устройству (10), обеспечивать пользователю доступ к периферийному устройству (10).

23. Способ аутентификации пользователя в периферийном устройстве (10), включающий в себя следующие этапы, на которых:

- посредством мобильного устройства (11) определяют (S2202) первую часть 45 идентификационной информации и отправляют (S2205) через службу социальных сетей в периферийное устройство (10) запрос доступа, включающий в себя эту определенную первую часть идентификационной информации и вторую часть информации, идентифицирующую учетную запись пользователя в социальной сети;

посредством периферийного устройства (10) принимают запрос доступа через службу социальных сетей и определяют (S2302) на основе информации, содержащейся в запросе доступа, разрешено ли пользователю осуществлять доступ к периферийному устройству (10), посредством соединения с учетной записью администратора службы социальных сетей, чтобы определить, связана ли информация учетной записи пользователя в службе социальных сетей со списком в службе социальных сетей (S1116, S1117, S1409, S1410);
и

в случае если периферийное устройство (10) на основе запроса доступа определило, что пользователю разрешено

осуществить доступ к периферийному устройству (10), посредством периферийного устройства (10) обеспечивают (S2303) пользователю доступ к периферийному устройству (10).

24. Способ по п. 23, в котором перед упомянутым определением периферийным устройством (10) выполняется соединение периферийного устройства (10) (S2103) с учетной записью администратора службы социальных сетей и регистрация (S2104) первой части идентификационной информации в привязке к представлению периферийного устройства (10) в службе социальных сетей;

при этом при упомянутом определении (S2302) посредством периферийного устройства (10) соединяются с учетной записью администратора службы социальных сетей, осуществляют доступ к запросу доступа и определяют, соответствует ли информация, содержащаяся в запросе доступа, зарегистрированной детальной информации о периферийном устройстве (10).

25. Способ по п. 24, в котором запрос доступа является прямым сообщением, отправленным с учетной записи пользователя в службе социальных сетей на учетную запись администратора службы социальных сетей.

26. Способ по п. 23, в котором периферийное устройство (10) определяет уровень доступа к периферийному устройству на основе второй части информации, идентифицирующей учетную запись пользователя в службе социальных сетей.

27. Способ по п. 23, в котором:

первая часть идентификационной информации включает в себя код, периферийное устройство (10) предоставляет этот код пользователю, и мобильное устройство (11) определяет (S2202) первую часть идентификационной информации путем ввода пользователем кода в мобильное устройство (11).

28. Способ по п. 23, в котором:

периферийное устройство (10) предоставляет машиночитаемый код, кодирующий первую часть идентификационной информации; и

мобильное устройство (11) определяет (S2202) первую часть идентификационной информации посредством чтения и декодирования машиночитаемого кода, предоставленного периферийным устройством (10).

29. Способ по п. 23, в котором первая часть идентификационной информации включает в себя случайное число.

30. Способ по п. 23, в котором первая часть идентификационной информации включает в себя часть информации, идентифицирующую учетную запись администратора службы социальных сетей.

31. Способ по п. 23, в котором периферийное устройство (10) выполнено с возможностью генерировать первую часть идентификационной информации.

32. Способ по п. 23, в котором:

первая часть идентификационной информации получается из положения

периферийного устройства; и

мобильное устройство (11) определяет (S2202) первую часть идентификационной информации путем определения положения периферийного устройства (10).

33. Носитель информации, на котором сохранена программа,

5 которая при ее исполнении на периферийном устройстве (10) предписывает периферийному устройству (10) выполнять способ по любому из пп. 23-32.

34. Носитель информации, на котором сохранена программа, которая при ее исполнении на мобильном устройстве (11) предписывает мобильному устройству (11) выполнять способ по любому из пп. 23-32.

10 35. Система для аутентификации пользователя в периферийном устройстве (10), включающая в себя:

мобильное устройство (11), выполненное с возможностью определять первую часть идентификационной информации и отправлять через службу социальных сетей в периферийное устройство запрос доступа, включающий в себя эту определенную первую
15 часть идентификационной информации и вторую часть информации, идентифицирующую учетную запись пользователя в социальной сети;

при этом периферийное устройство (10) выполнено с возможностью принимать запрос доступа и определять на основе информации, содержащейся в запросе доступа, разрешено ли пользователю осуществлять доступ к периферийному устройству (10),
20 посредством соединения с учетной записью администратора службы социальных сетей, чтобы определить, связана ли информация учетной записи пользователя в службе социальных сетей со списком в службе социальных сетей (S1116, S1117, S1409, S1410);
и

при этом периферийное устройство (10) выполнено с возможностью, в случае, если
25 периферийное устройство (10) на основе запроса доступа определило, что пользователю разрешено

осуществить доступ к периферийному устройству (10), обеспечивать пользователю доступ к периферийному устройству (10).

36. Периферийное устройство (10), включающее в себя:

30 средство, выполненное с возможностью предоставлять пользователю первую часть идентификационной информации в форме машиночитаемого кода; и

средство, выполненное с возможностью осуществлять доступ к учетной записи в службе социальных сетей и определять на основе первой части идентификационной информации, разрешено ли пользователю осуществлять доступ к периферийному
35 устройству (10), посредством соединения с учетной записью администратора службы социальных сетей, чтобы определить, связана ли информация учетной записи пользователя в службе социальных сетей со списком в службе социальных сетей (S1116, S1117, S1409, S1410).

37. Периферийное устройство (10) по п. 36, в котором средство, выполненное с
40 возможностью предоставлять пользователю первую часть идентификационной информации, выполнено с возможностью предоставлять пользователю идентификационную информацию посредством по меньшей мере одного из отображения идентификационной информации на дисплее периферийного устройства (10) и печати идентификационной информации.

45 38. Периферийное устройство по п. 36, в котором идентификационная информация включает в себя случайное число.

39. Периферийное устройство по п. 36, в котором идентификационная информация включает в себя информацию, идентифицирующую учетную запись администратора

службы социальных сетей.

40. Периферийное устройство по п. 36, дополнительно включающее в себя средство для генерирования идентификационной информации.

5 41. Периферийное устройство по п. 40, при этом периферийное устройство (10) выполнено с возможностью предоставлять идентификационную информацию в форме штрихкода или QR-кода.

42. Периферийное устройство по п. 36, дополнительно включающее в себя периферийное оборудование, которое функционирует как по меньшей мере одно из принтера, факса и сканера.

10

15

20

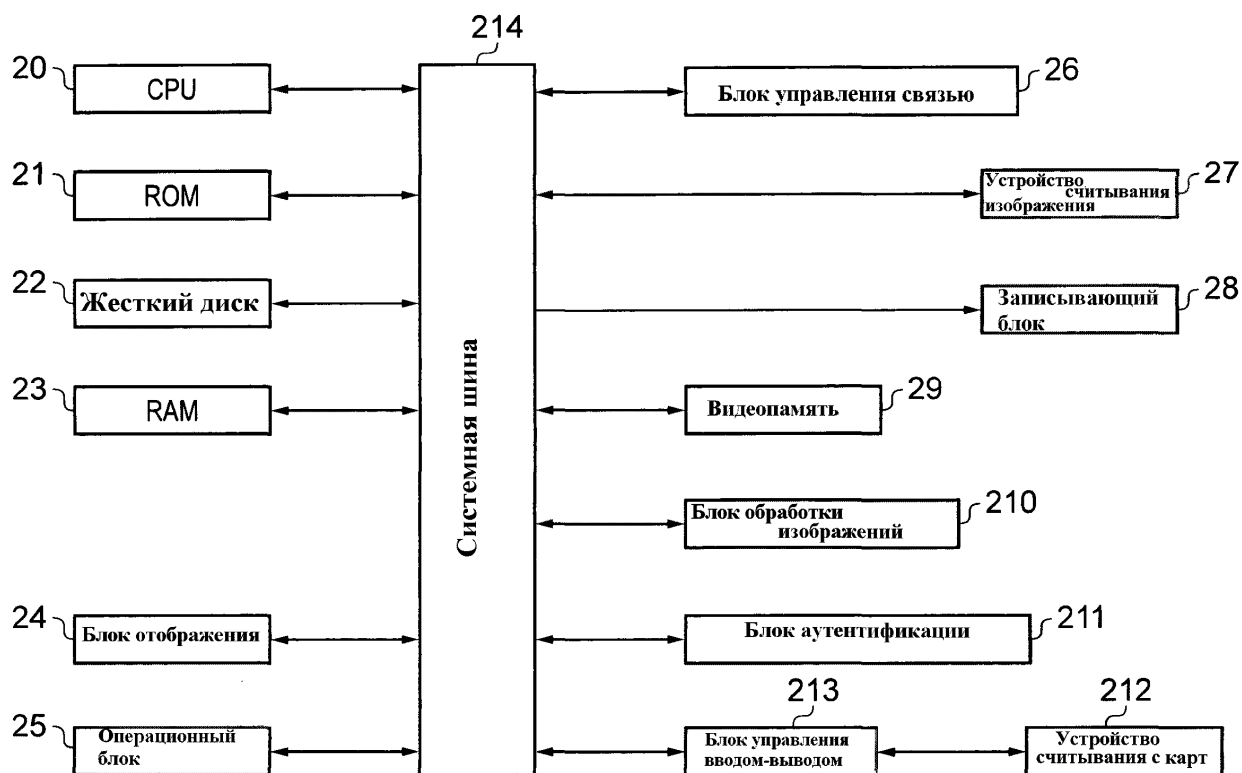
25

30

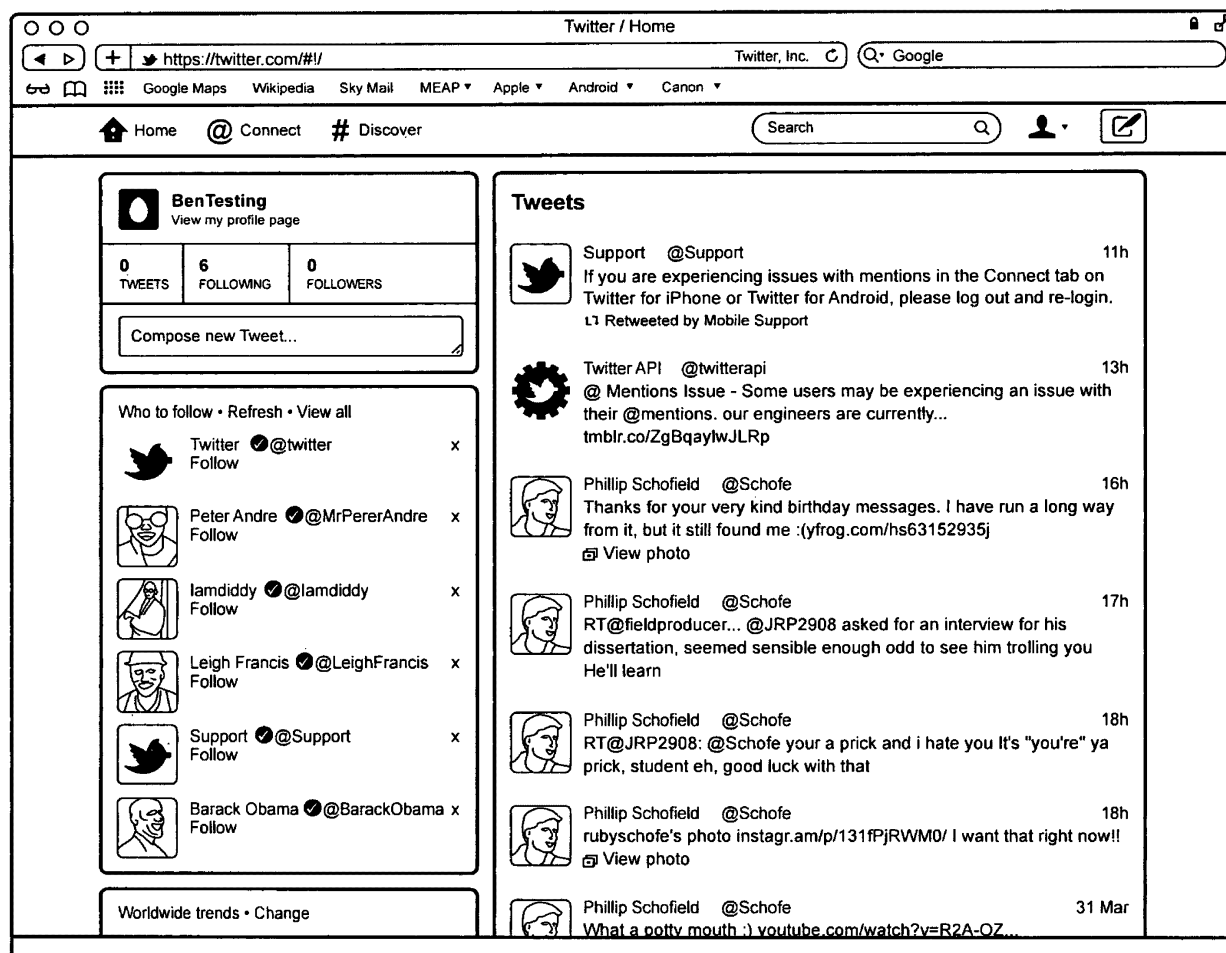
35

40

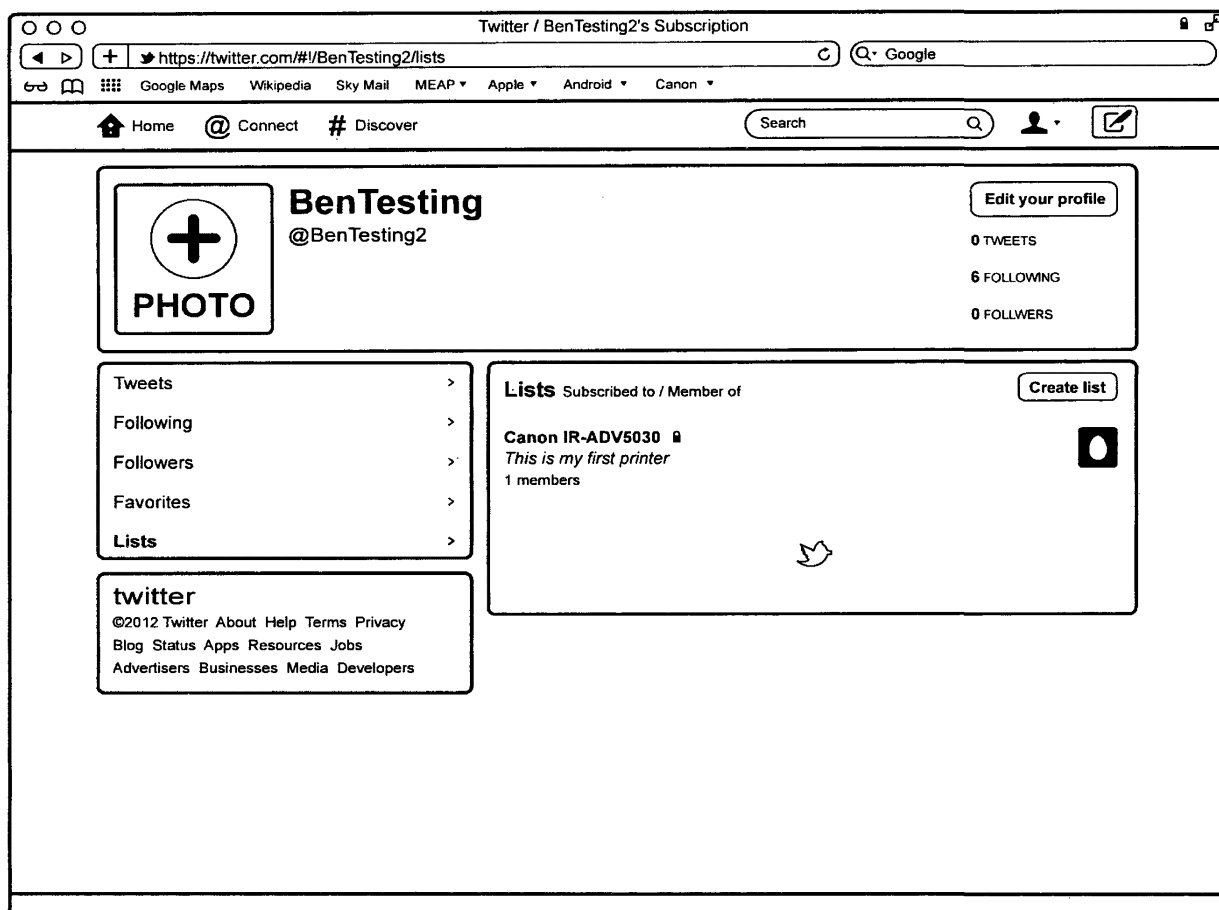
45



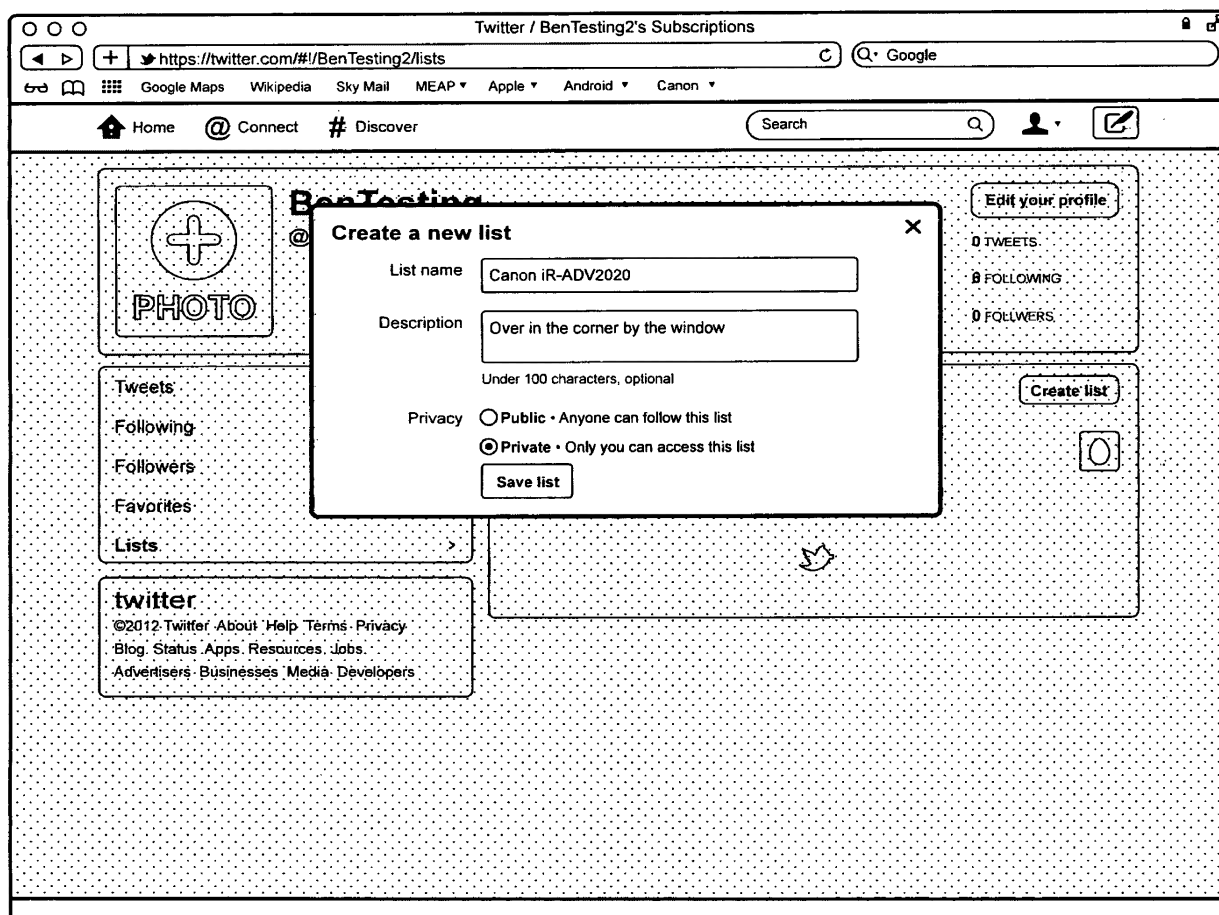
ФИГ.2



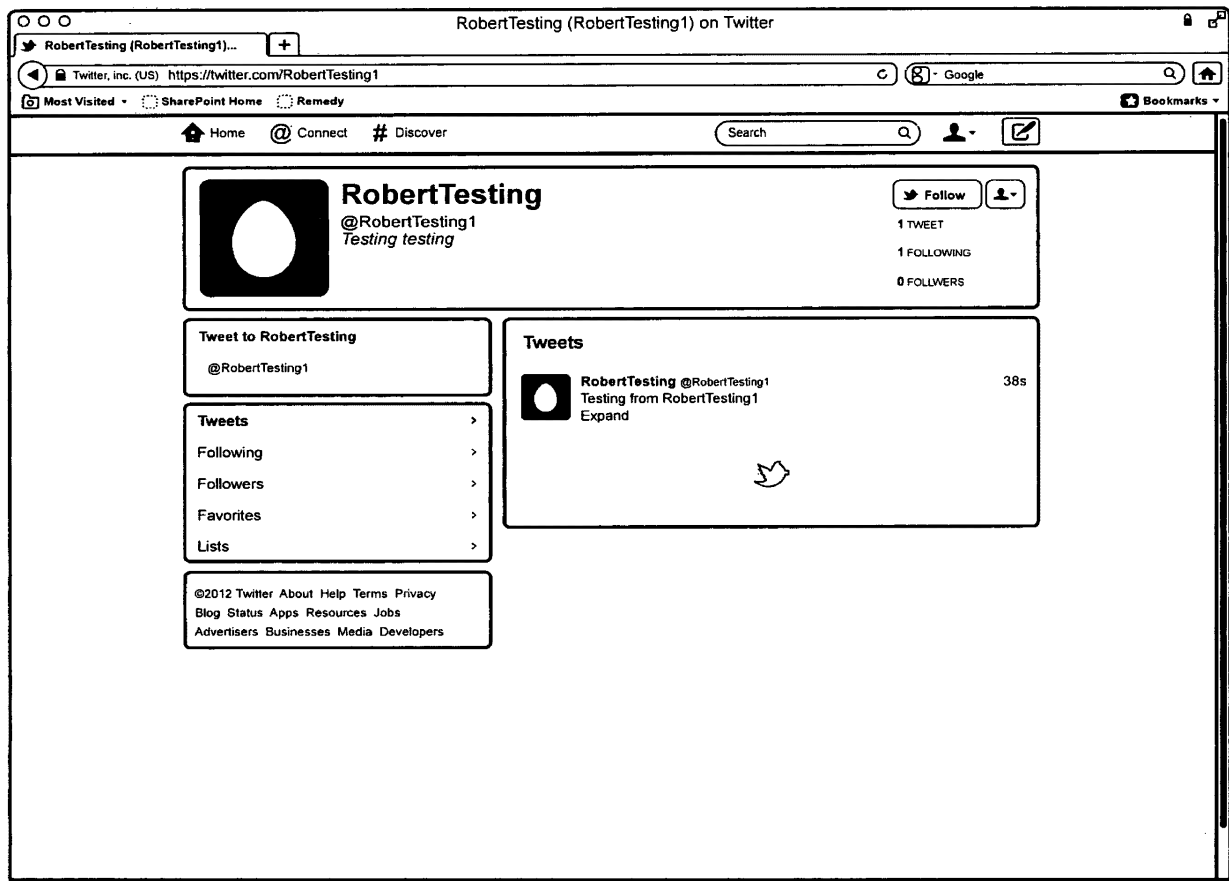
ФИГ.3



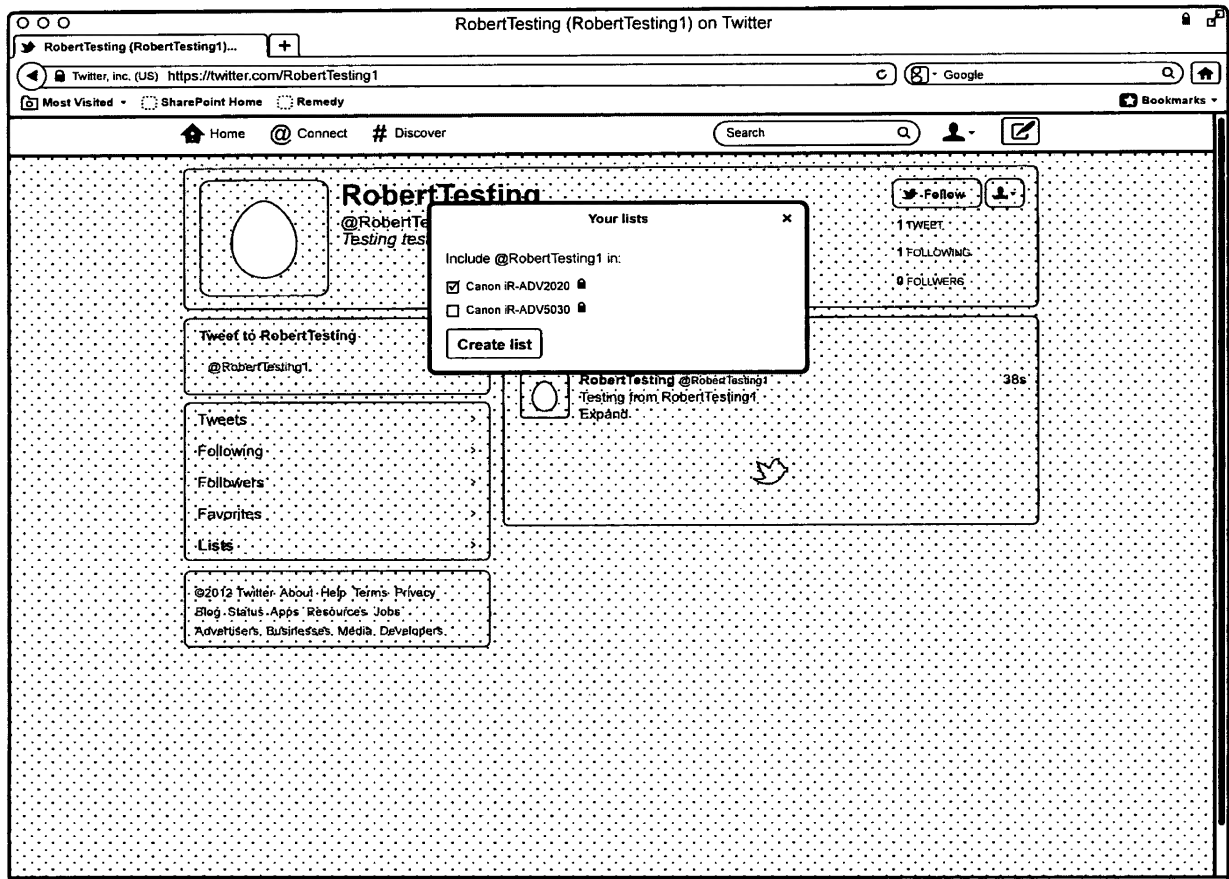
ФИГ.4



ФИГ.5

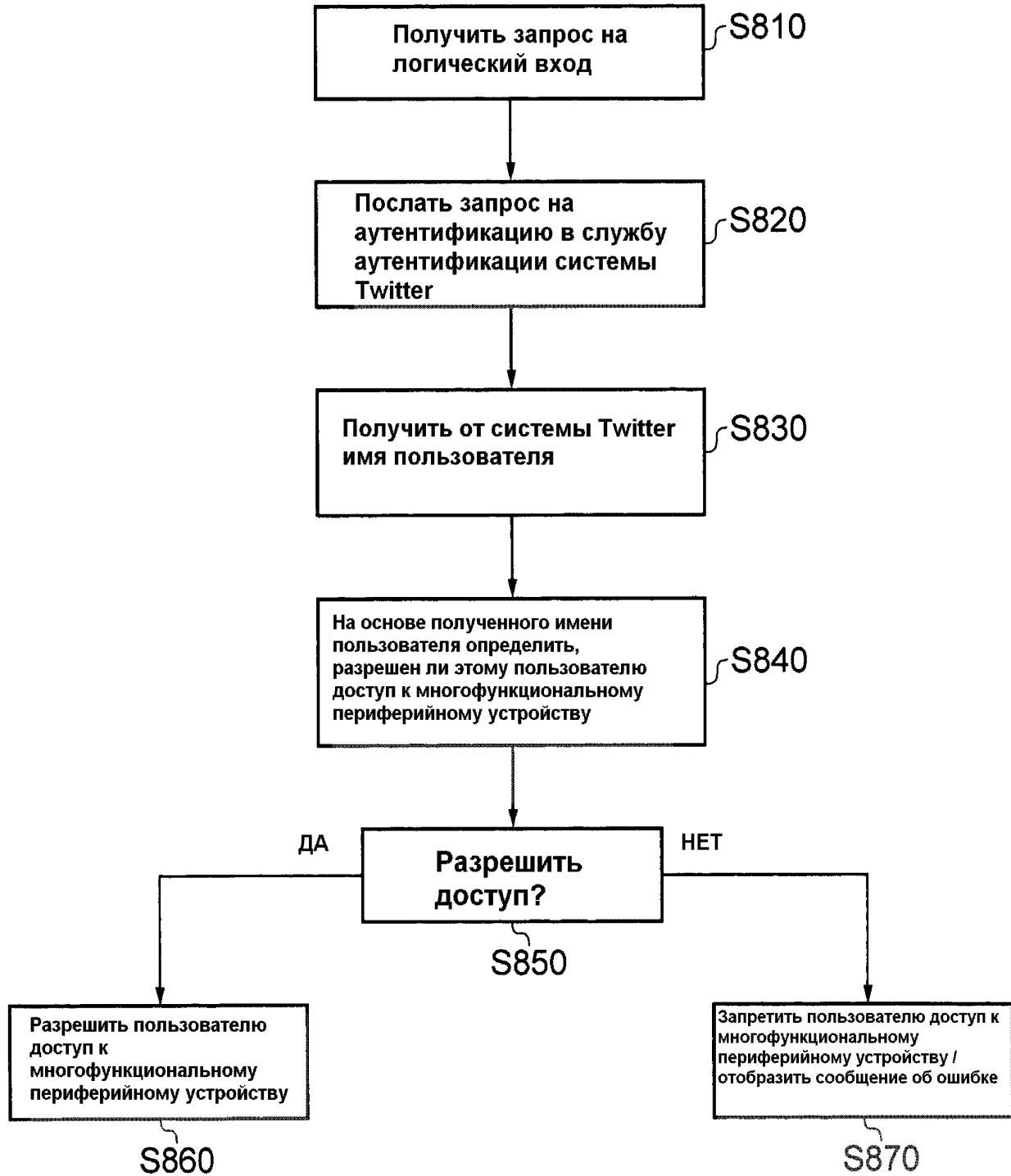


ФИГ.6



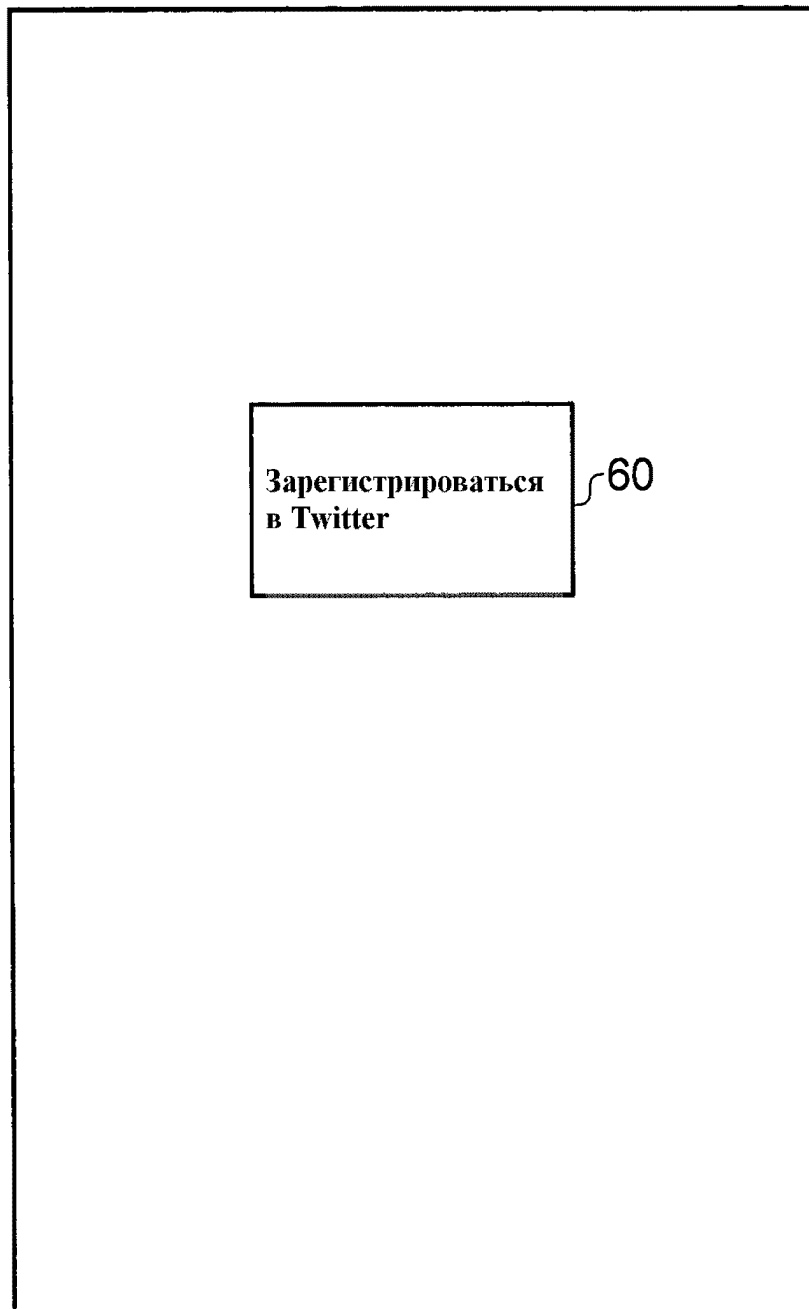
ФИГ.7

@MFP10



ФИГ.8

MFP10



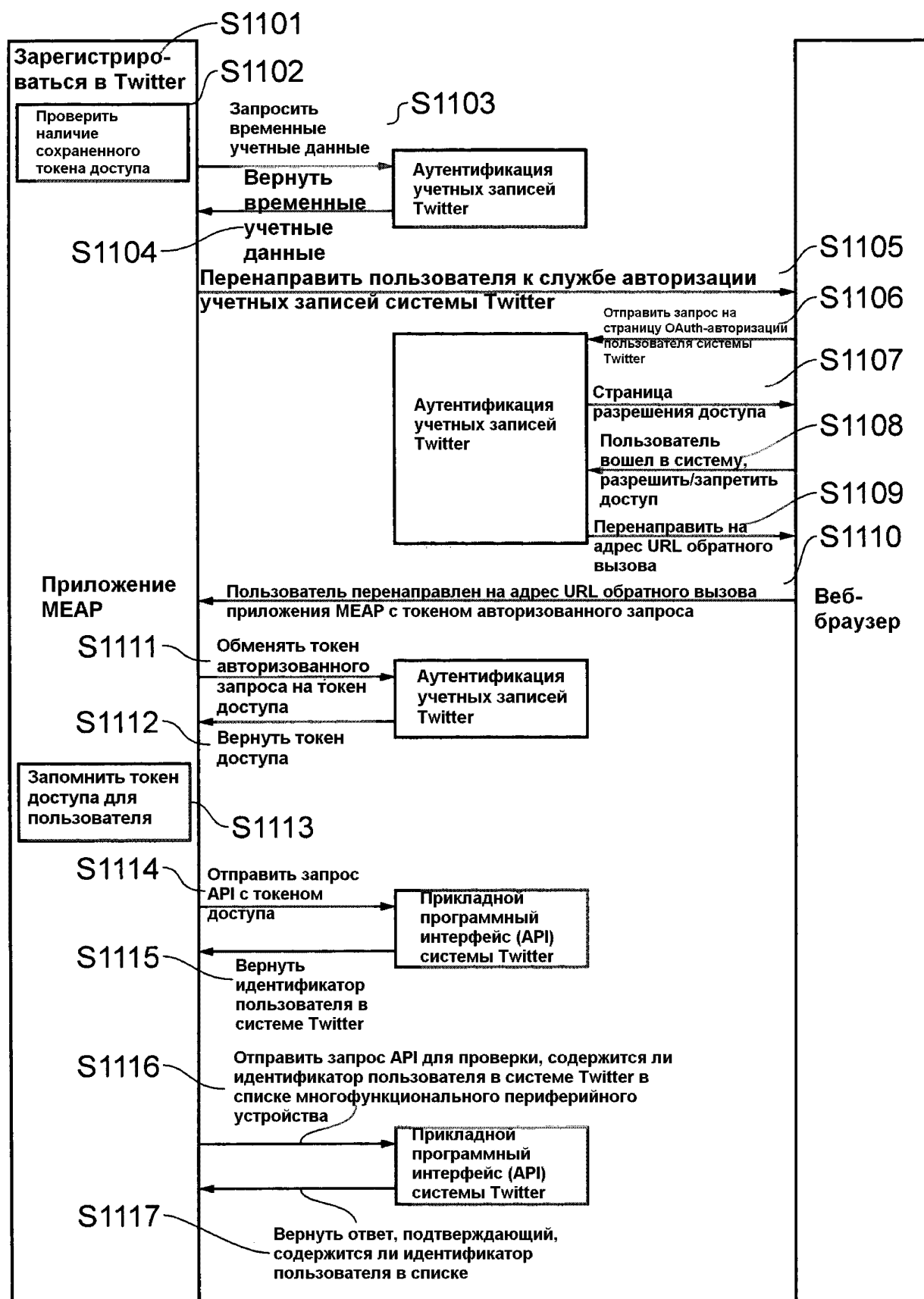
ФИГ.9

Браузер

Имя пользователя
Twitter

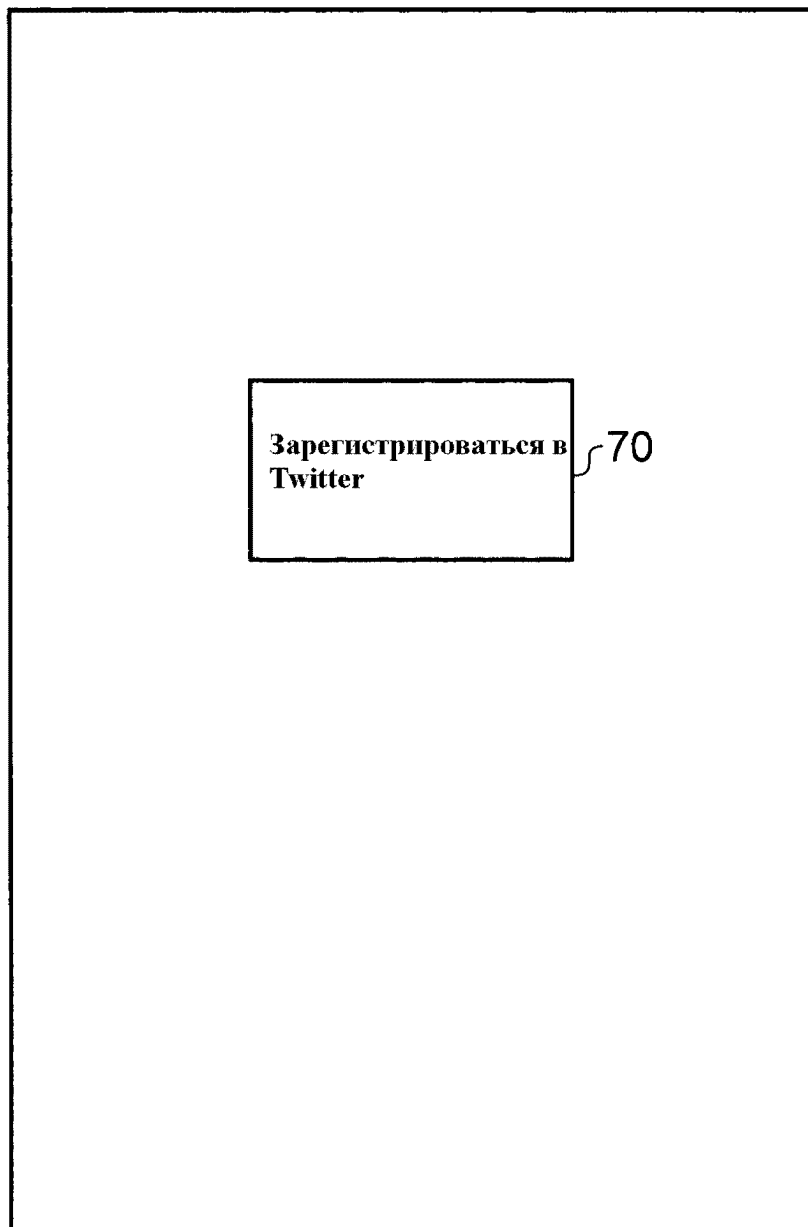
Пароль

ФИГ.10



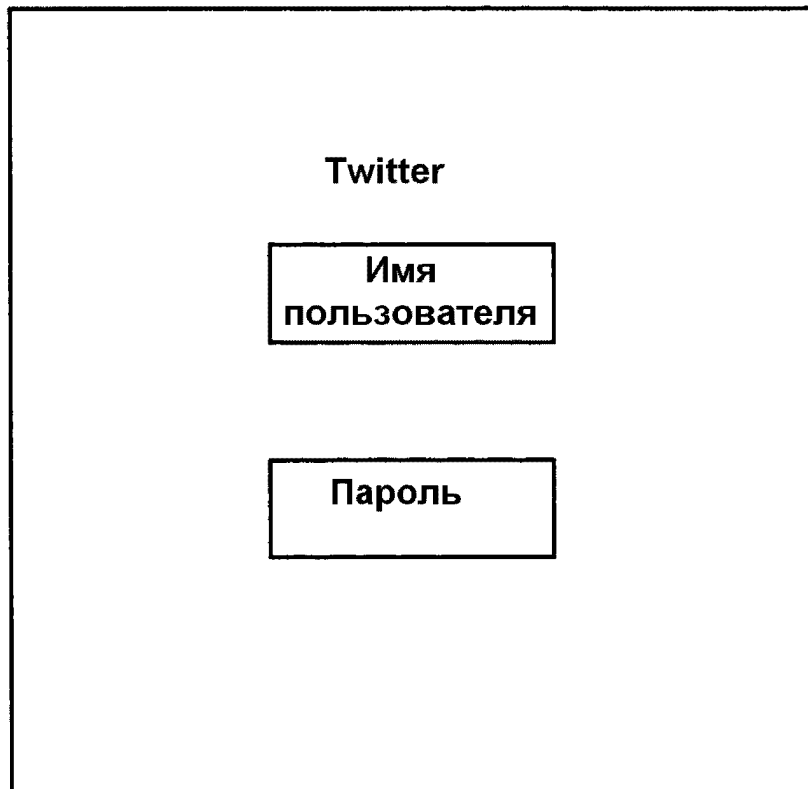
ФИГ.11

MFP10



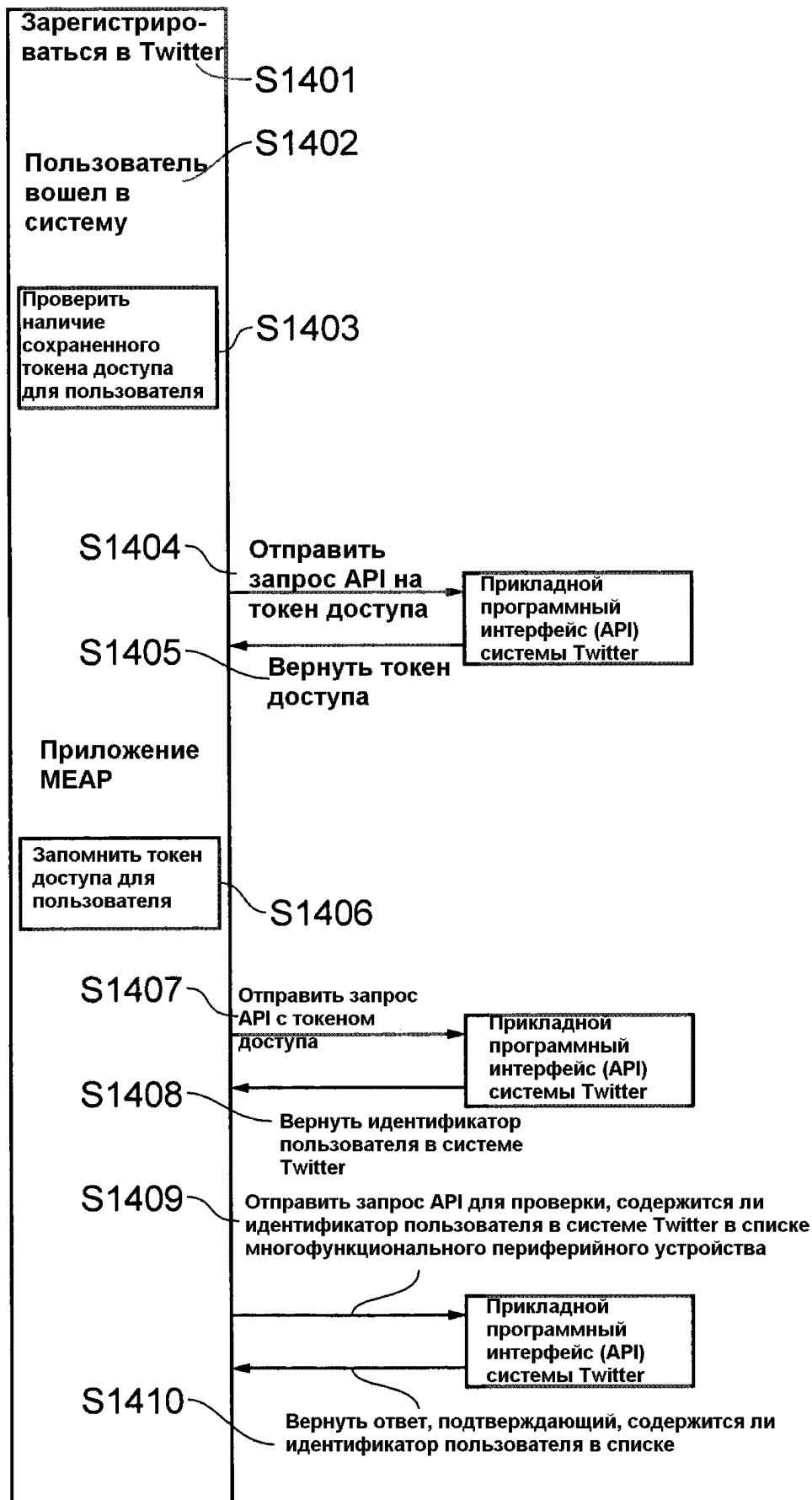
ФИГ.12

Приложение МЕАР

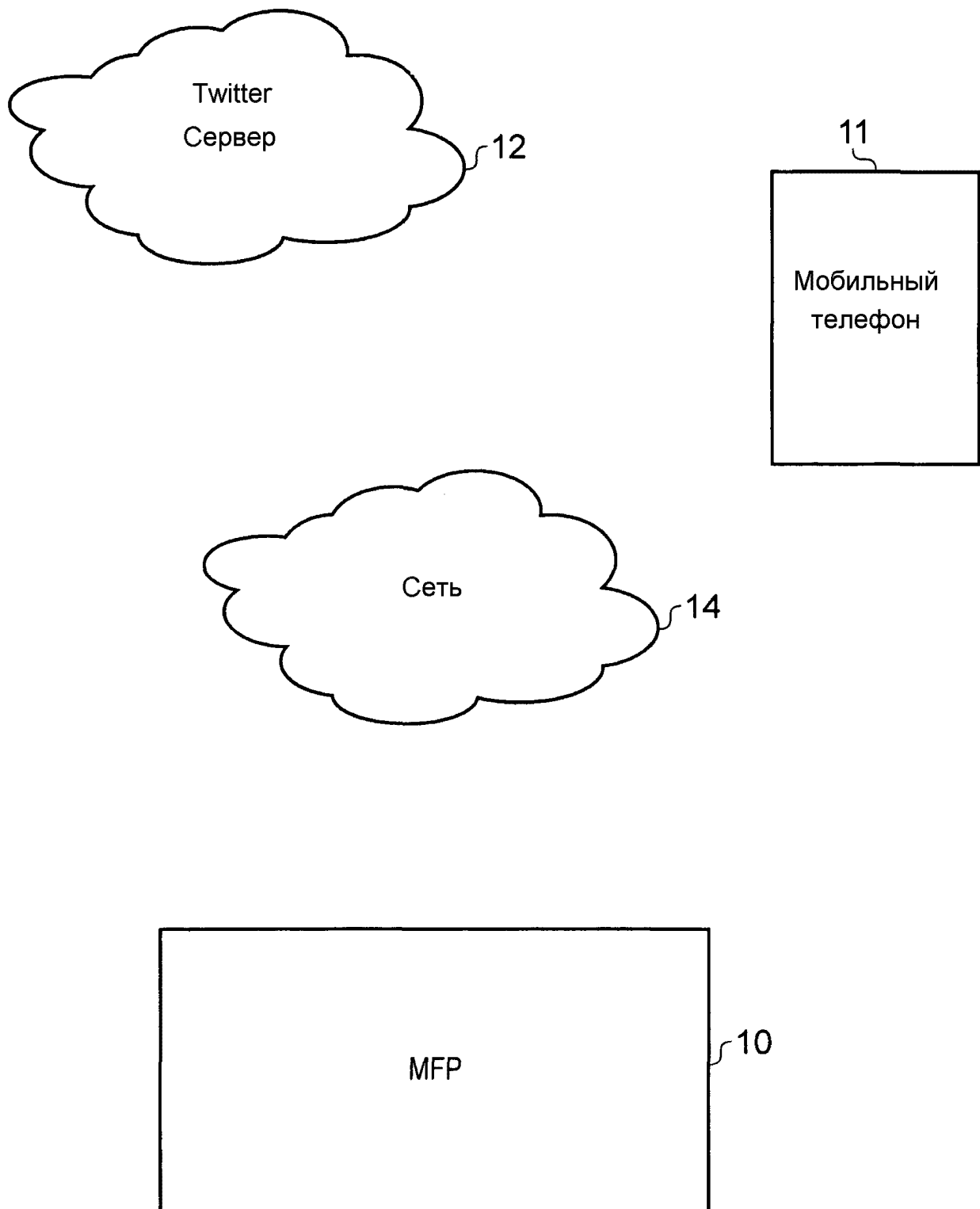


The image shows a login interface for Twitter. At the top, the word "Twitter" is displayed. Below it, there are two input fields. The first field is labeled "Имя пользователя" (Username) and the second field is labeled "Пароль" (Password). Both fields are empty and have a light gray border. The entire login area is enclosed in a larger rectangular frame.

ФИГ.13



ФИГ.14

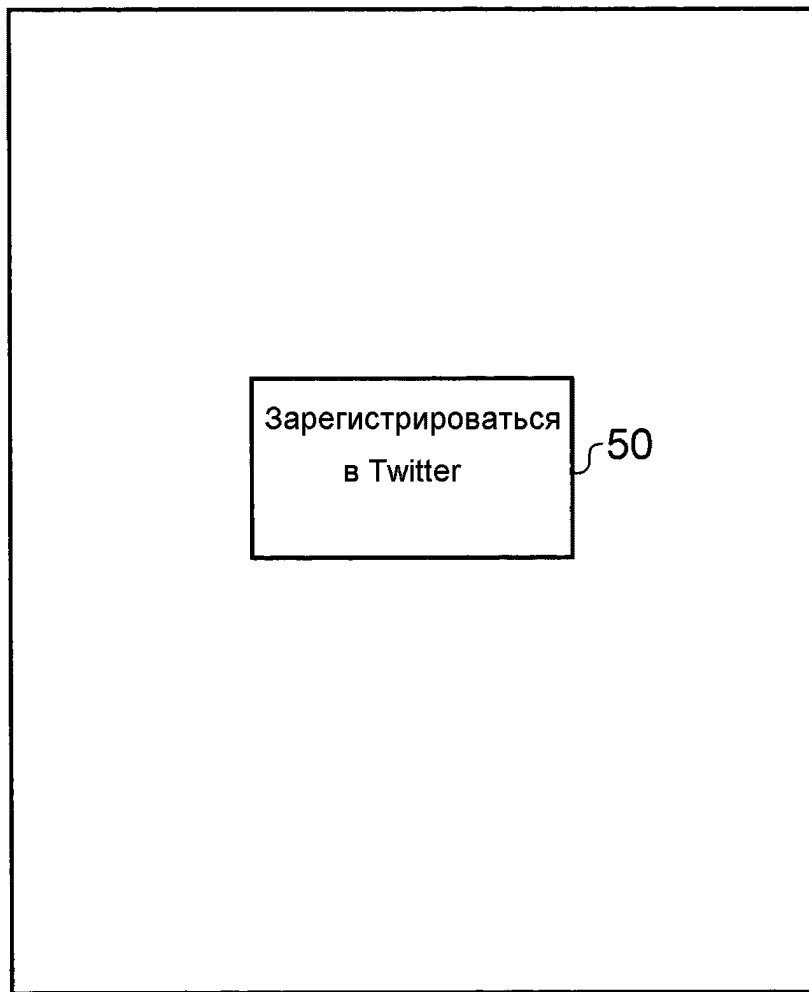


ФИГ.15



ФИГ.16

MFP10



ФИГ.17

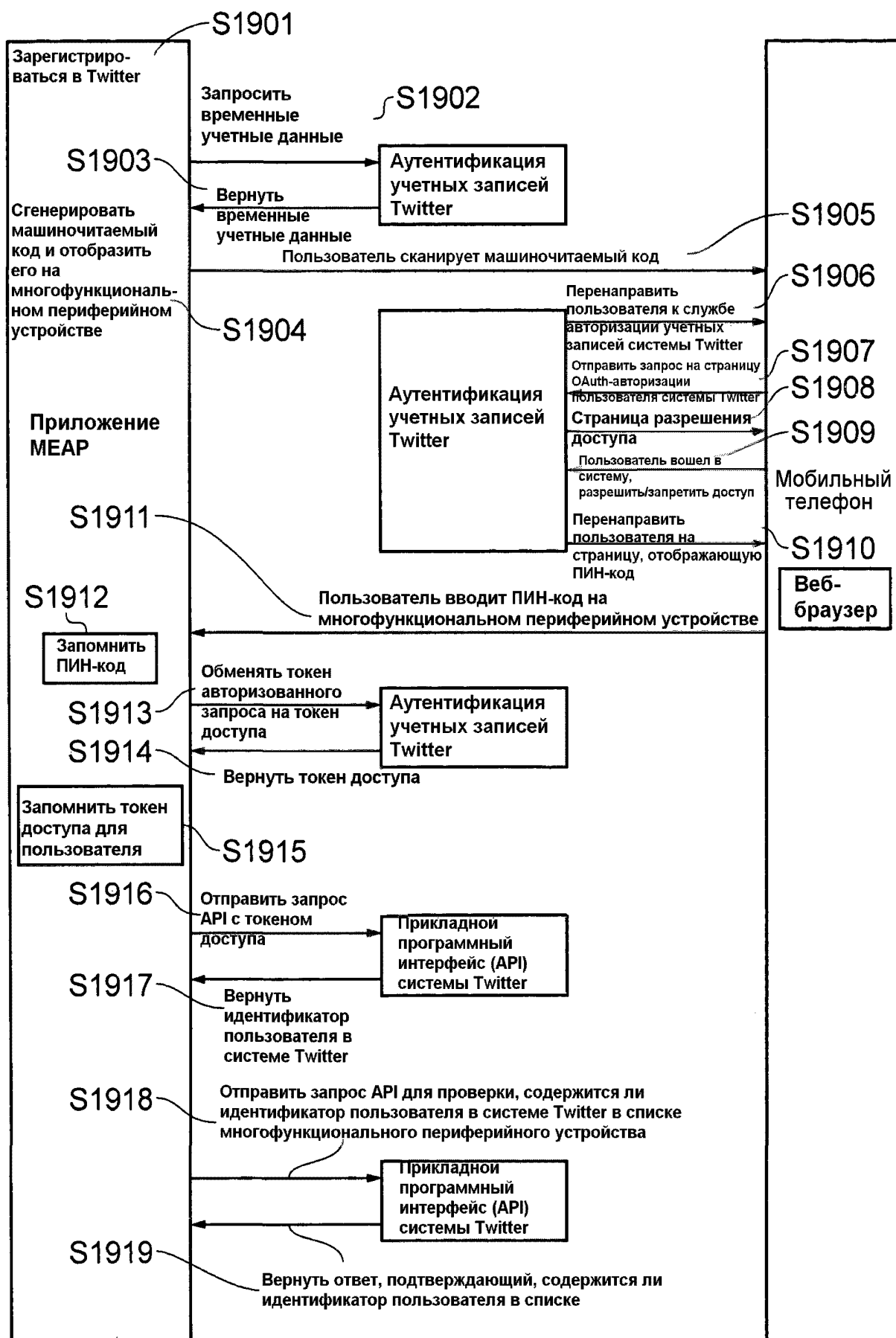
Мобильный телефон 11

Браузер

**Имя
пользователя**

Пароль

ФИГ.18

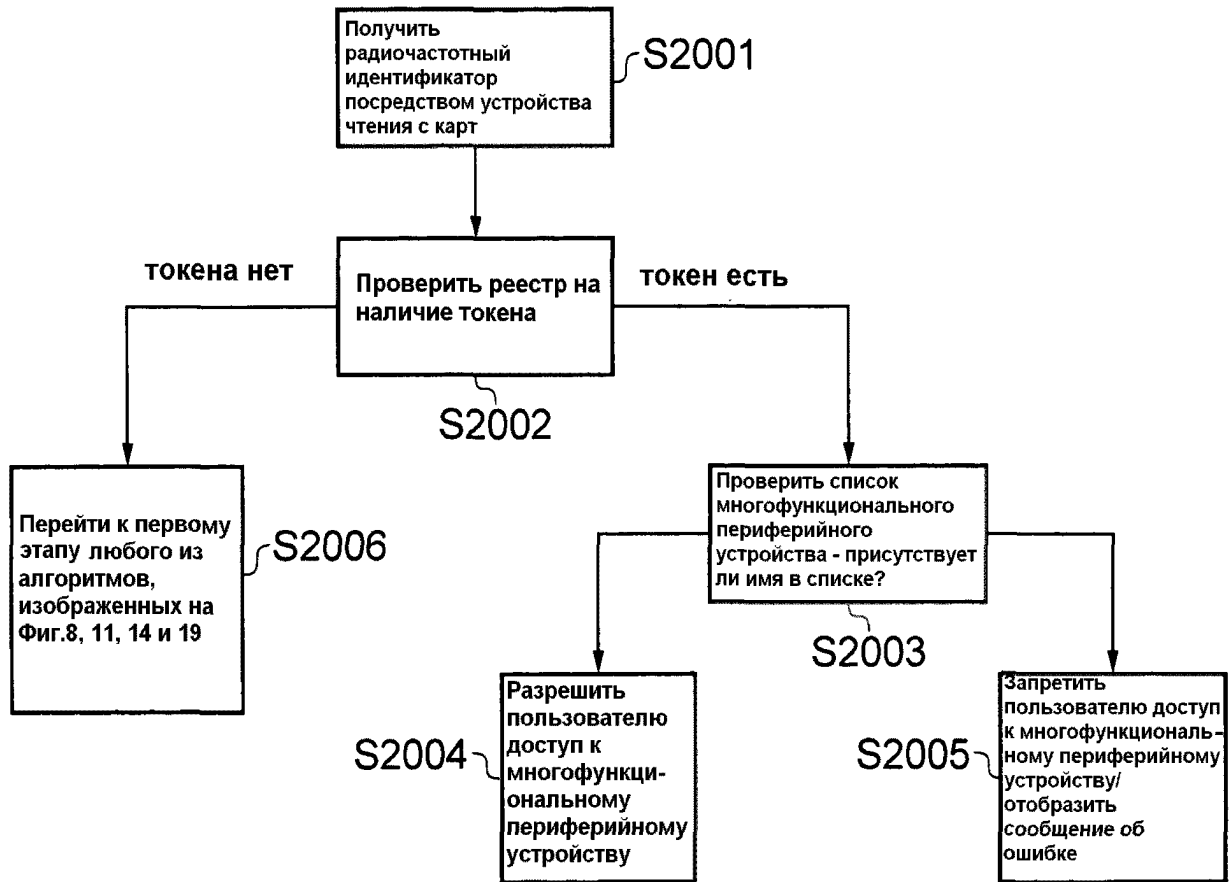


ФИГ.19

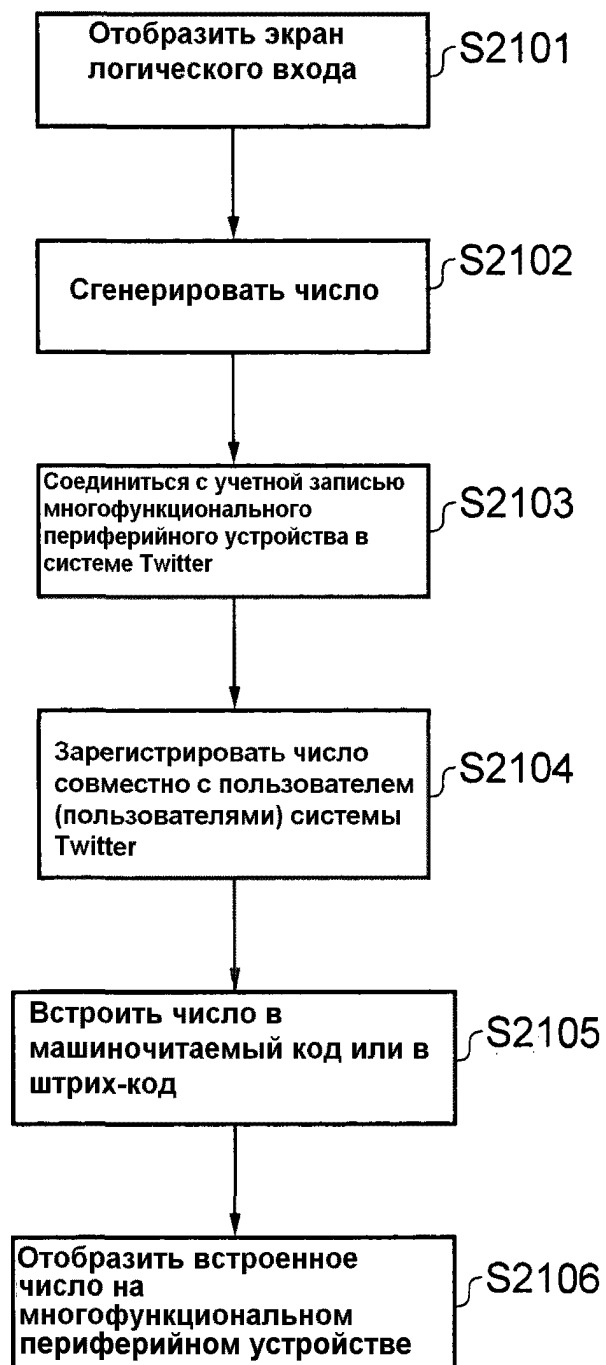
Реестр приложения MEAP

Радиочастотный идентификатор	Токен
Пользователь А	Токен А
Пользователь В	Токен В
•	•
•	•
•	•

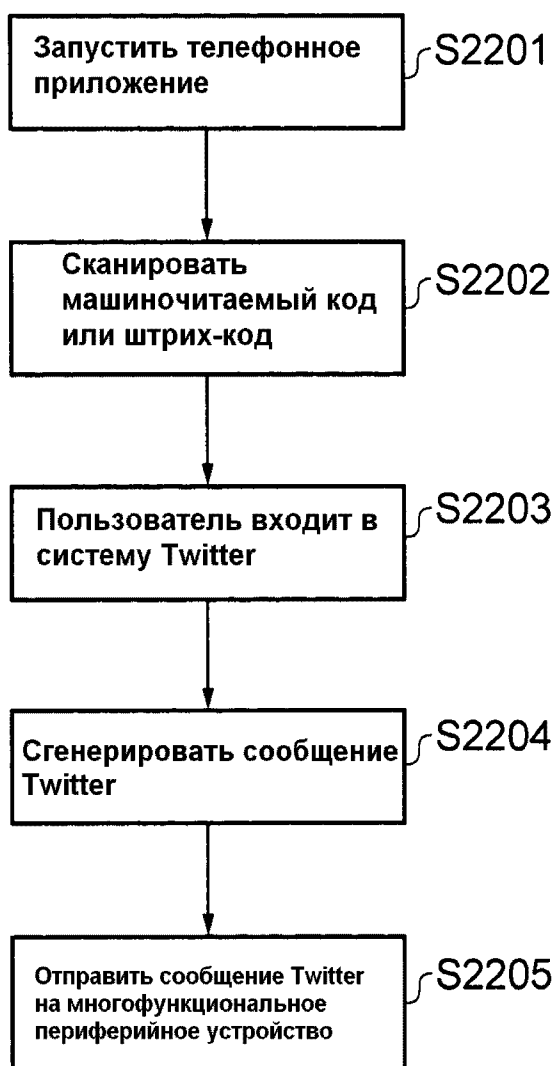
ФИГ.20А



ФИГ.20В



ФИГ.21



ФИГ.22

