



**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2011141580/08, 13.10.2011

(24) Дата начала отсчета срока действия патента:
13.10.2011

Приоритет(ы):

(30) Конвенционный приоритет:
14.10.2010 JP 2010-231884

(43) Дата публикации заявки: 20.04.2013 Бюл. № 11

(45) Опубликовано: 10.02.2014 Бюл. № 4

(56) Список документов, цитированных в отчете о поиске: US 2009/0217367 A1, 27.08.2009. EP 1426847 A2, 09.06.2004. RU 85707 U1, 10.08.2009. RU 2346823 C1, 20.02.2009.

Адрес для переписки:

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

(72) Автор(ы):

ХОСОДА Ясухиро (JP)

(73) Патентообладатель(и):

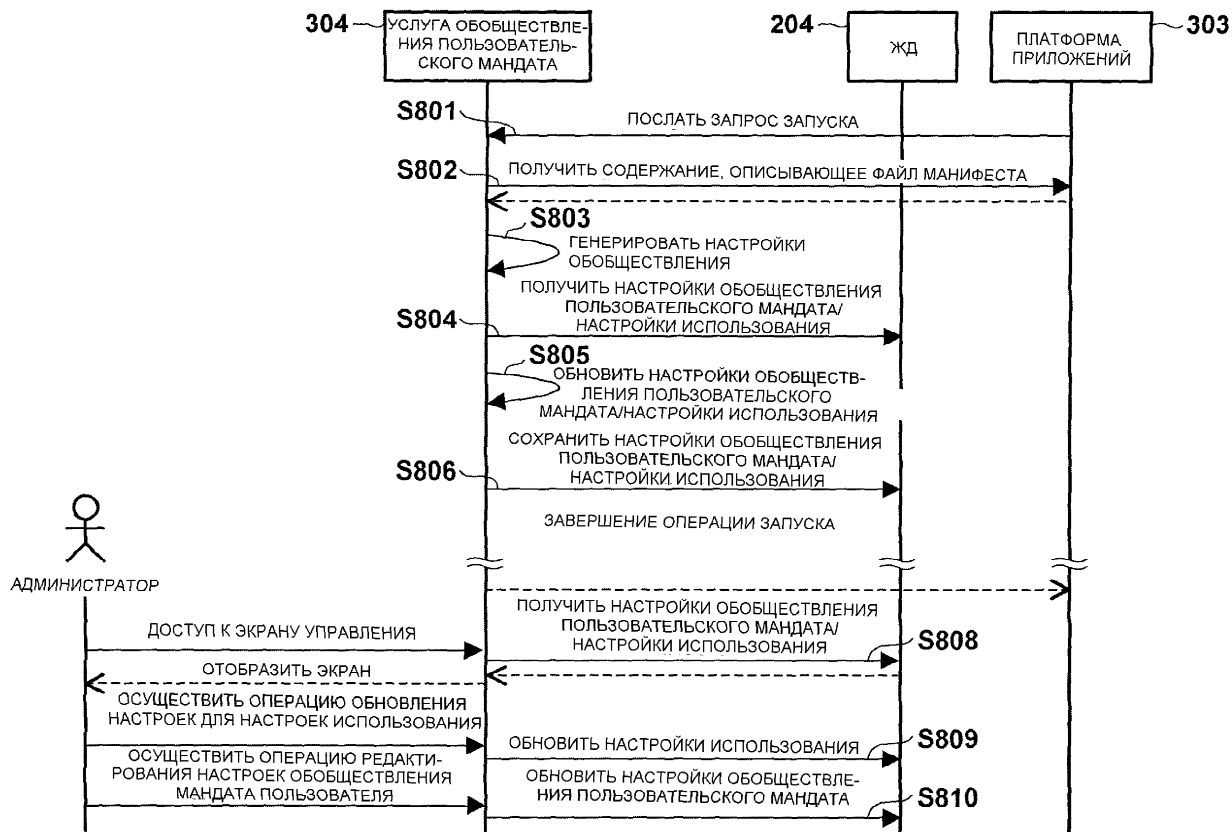
КЭНОН КАБУСИКИ КАЙСЯ (JP)

(54) УСТРОЙСТВО ОБРАБОТКИ ИНФОРМАЦИИ, СПОСОБ ЕГО УПРАВЛЕНИЯ И КОМПЬЮТЕРНО-СЧИТЫВАЕМЫЙ НОСИТЕЛЬ ИНФОРМАЦИИ

(57) Реферат:

Изобретение относится к устройству обработки информации, на которое может быть установлена совокупность приложений и которое может обобществлять мандат пользователя среди приложений, и к способу управления для устройства обработки информации. Техническим результатом является повышение защиты пользовательского мандата за счет использования условий совместного использования с другим приложением при передаче пользовательского мандата приложениями. Устройство содержит: блок получения, который получает от каждого из множества приложений, выполняющихся на устройстве обработки информации, условие

совместного использования мандата пользователя с другим приложением; блок генерации, который генерирует на основании полученного условия совместного использования настройки совместного использования, которые задают упомянутое условие совместного использования мандата пользователя среди приложений; и блок предоставления, который предоставляет по получении запроса мандата пользователя от приложения, отличного от упомянутого первого приложения из упомянутого множества, упомянутый мандат пользователя запрашивающему приложению согласно настройкам совместного использования, хранящимся в памяти. 3 н. и 7 з.п. ф-лы, 13 ил.



ФИГ. 8



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2011141580/08, 13.10.2011**

(24) Effective date for property rights:
13.10.2011

Priority:

(30) Convention priority:
14.10.2010 JP 2010-231884

(43) Application published: **20.04.2013 Bull. 11**

(45) Date of publication: **10.02.2014 Bull. 4**

Mail address:

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

(72) Inventor(s):

KhOSODA Jasukhiro (JP)

(73) Proprietor(s):

KEhNON KABUSIKI KAJJSa (JP)

(54) INFORMATION PROCESSING DEVICE, DRIVING METHOD THEREFOR AND COMPUTER-READABLE DATA MEDIUM

(57) Abstract:

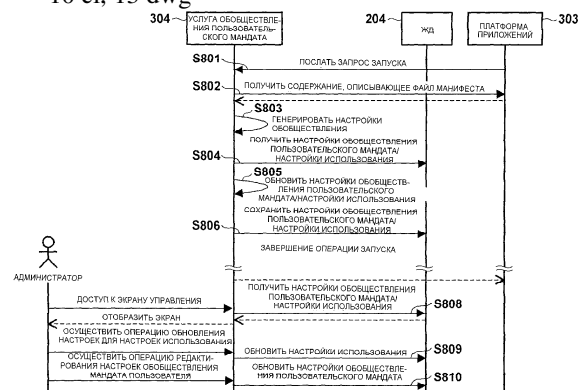
FIELD: physics, computer engineering.

SUBSTANCE: invention relates to an information processing device on which a plurality of applications can be installed and which can collectivise user mandate among applications, and a method of driving the information processing device. The device comprises: an obtaining unit which obtains, from each of the plurality of applications running on the information processing device, a condition for sharing user mandate with another application; a generation unit which generates, based on the obtained sharing condition, sharing settings which assign said user mandate sharing condition among applications; and a providing unit which provides, upon receiving a user mandate request from an application, different from said first application from said plurality, said user mandate to the requesting application in accordance with sharing

settings stored in memory.

EFFECT: high security of user mandate owing to use of conditions for sharing with another application when transferring user mandate with applications.

10 cl, 13 dwg



ФИГ. 8

Область техники

Настоящее изобретение относится к устройству обработки информации, на которое может быть установлена совокупность приложений и которое может обобществлять мандат пользователя среди приложений, к способу управления для устройства

Уровень техники

На устройство формирования изображений, например копировальный аппарат или MFP (многофункциональное периферийное устройство), имеющее возможность подключения к сети, можно дополнительно устанавливать приложение входа для аутентификации пользователя и встроенное приложение. Пример приложения, выполнимого на устройстве формирования изображений, включает в себя приложение для передачи документа, считанного сканером, на внешний сервер по сети и приложение для соединения с внешним сервером по сети для получения внешних ресурсов. Производители, помимо тех, которые обеспечивают оборудование устройства, могут создавать и продавать приложения.

Если при каждом обращении пользователя к внешним ресурсам ему приходится осуществлять операцию аутентификации на таком устройстве формирования изображений, это может быть затруднительно для пользователя. Поэтому был разработан метод однократного входа, согласно которому пользователю необходимо осуществлять операцию аутентификации только один раз. Например, в выложенном патенте Японии № 08-263417 предложен способ обобществления мандата пользователя для компьютера и мандата пользователя для доступа к внешним системам среди сетевых провайдеров во всей сетевой системе.

Однако традиционный подход страдает следующими недостатками. А именно, устройство формирования изображений в отсутствие сетевого провайдера, который позволяет обобществлять мандат пользователя, как раскрыто в выложенном патенте Японии № 08-263417, не может обобществлять мандат пользователя среди приложений. Кроме того, если обобществление мандата пользователя среди приложений разрешено без каких-либо условий, приложения, отличные от тех, которые зарегистрировали мандат пользователя, могут пропустить его наружу. Поэтому производитель, создающий приложение, хочет обобществлять мандат пользователя только среди приложений, созданных самим производителем или доверенных производителей. Однако согласно традиционному способу обобществления мандата пользователя производитель, создающий приложение, не может ограничивать круг приложений, между которыми может обобществляться мандат пользователя.

Сущность изобретения

Настоящее изобретение позволяет реализовать устройство обработки информации, которое предоставляет услугу обобществления пользовательского мандата согласно условию обобществления мандата пользователя, установленному производителем, создающим приложение, способ управления для устройства обработки информации и компьютерно-считываемый носитель информации.

Один аспект настоящего изобретения предусматривает устройство обработки информации, содержащее: блок получения, который получает от каждого из совокупности приложений, выполняющихся на устройстве обработки информации, условие обобществления мандата пользователя с другим приложением, которое было задано для каждого из совокупности элементов мандата пользователя, включающих в себя информацию для сертификации пользователя; блок генерации, который

генерирует на основании полученного условия обобществления настройки обобществления, которые задают условие обобществления для каждого элемента мандата пользователя среди приложений, и сохраняет сгенерированные настройки обобществления в памяти; блок удержания, который удерживает в памяти мандат пользователя, переданный из, по меньшей мере, одного из приложений; и блок предоставления, который предоставляет по получении запроса мандата пользователя от одного из приложений мандат пользователя запрашивающему приложению согласно настройкам обобществления, хранящимся в памяти.

Другой аспект настоящего изобретения предусматривает способ управления для устройства обработки информации, содержащий этапы, на которых: получают, от каждого из совокупности приложений, выполняющихся на устройстве обработки информации, условие обобществления мандата пользователя с другим приложением, которое было задано для каждого из совокупности элементов мандата пользователя, включающих в себя информацию для сертификации пользователя; генерируют на основании полученного условия обобществления настройки обобществления, которые задают условие обобществления для каждого элемента мандата пользователя среди приложений, и сохраняют сгенерированные настройки обобществления в памяти; удерживают в памяти мандат пользователя, переданный из, по меньшей мере, одного из приложений; и предоставляют по получении запроса мандата пользователя от одного из приложений мандат пользователя запрашивающему приложению согласно настройкам обобществления, хранящимся в памяти.

Еще один аспект настоящего изобретения предусматривает компьютерно-считываемый носитель информации для хранения компьютерной программы, предписывающей компьютеру выполнять каждый этап способа управления для устройства обработки информации.

Другие признаки настоящего изобретения явствуют из нижеследующего описания иллюстративных вариантов осуществления со ссылкой на прилагаемые чертежи.

Краткое описание чертежей

Фиг. 1 - блок-схема, демонстрирующая конфигурацию сети согласно первому варианту осуществления.

Фиг. 2 - блок-схема, демонстрирующая аппаратную конфигурацию устройства формирования изображений согласно первому варианту осуществления.

Фиг. 3 - блок-схема, демонстрирующая программную конфигурацию устройства формирования изображений согласно первому варианту осуществления.

Фиг. 4 - вид, демонстрирующий пользовательский интерфейс для управления приложениями согласно первому варианту осуществления.

Фиг. 5 - вид, демонстрирующий экраны ввода информации аутентификации пользователя согласно первому варианту осуществления.

Фиг. 6 - вид, демонстрирующий API услуги обобществления пользовательского мандата согласно первому варианту осуществления.

Фиг. 7 - вид, демонстрирующий файлы манифеста приложений согласно первому варианту осуществления.

Фиг. 8 - схема последовательности операций, демонстрирующая запуск и настройку услуги обобществления пользовательского мандата согласно первому варианту осуществления.

Фиг. 9 - вид, демонстрирующий настройки обобществления пользовательского мандата/настройки использования согласно первому варианту осуществления.

Фиг. 10 - вид, демонстрирующий пользовательский интерфейс для создания

настроек использования для настроек обобществления пользовательского мандата согласно первому варианту осуществления.

Фиг. 11 - вид, демонстрирующий пользовательский интерфейс для редактирования настроек обобществления пользовательского мандата согласно первому варианту осуществления.

Фиг. 12 - схема последовательности операций, демонстрирующая использование услуги обобществления пользовательского мандата согласно первому варианту осуществления.

Фиг. 13 - вид, демонстрирующий таблицу управления мандатными данными пользователя согласно первому варианту осуществления.

Описание вариантов осуществления

Опишем более подробно варианты осуществления настоящего изобретения со ссылкой на чертежи. Заметим, что относительное размещение компонентов, численные выражения и числовые значения, приведенные в этих вариантах осуществления, не ограничивают объем настоящего изобретения, если прямо не указано обратное.

<Первый вариант осуществления>

<Конфигурация сети>

Ниже со ссылкой на фиг. 1-13 описан первый вариант осуществления настоящего изобретения. Сначала объясним конфигурацию сети согласно этому варианту осуществления со ссылкой на фиг. 1. В этом варианте осуществления, в качестве примера устройства используется устройство формирования изображений (устройство обработки информации), например MFP, принтер, факс и копировальный аппарат.

Согласно фиг. 1, локальная сеть (LAN) 105 соединена с возможностью связи с устройством 101 формирования изображений, почтовым сервером 102, сервером 103 обобществления файлов и прокси-сервером 104. Почтовый сервер 102 включает в себя такие протоколы, как SMTP (Simple Mail Transfer Protocol) и POP3 (Post Office Protocol Version 3). Сервер 103 обобществления файлов включает в себя такие протоколы, как SMB (Server Message Block). Прокси-сервер 104 соединен с LAN 105 и интернетом (WLAN) 106 и используется в качестве прокси-терминала, когда терминал, соединенный с LAN 105, подключается к интернету 106. Каждый сервер 102, 103 или 104 имеет функцию аутентификации пользователя, согласующуюся с каждым протоколом для аутентификации пользователя, желающего использовать сервер.

<Аппаратная конфигурация устройства формирования изображений>

Теперь со ссылкой на фиг. 2 опишем аппаратную конфигурацию устройства формирования изображений. Устройство 101 формирования изображений является примером устройства обработки информации и включает в себя ЦП 201, ПЗУ 202, ОЗУ 203, ЖД 204, операционную панель 205, устройство 206 чтения смарт-карты, сетевой интерфейс 207, принтер 208 и сканер 209. ЦП 201 управляет работой устройства 101 формирования изображений в целом. ПЗУ 202 - это постоянная память для хранения программ, выполняемых на ЦП 201, данных шрифта. ОЗУ 203 - это оперативная память, используемая в качестве рабочей области ЦП 201 и приемного буфера, а также используемая для визуализации изображения. На ЖД (жестком диске) 204 записываются данные, например программные коды и информация аутентификации пользователя.

Операционная панель 205 включает в себя различные переключатели и кнопки и жидкокристаллический дисплей для отображения сообщений. Устройство 206 чтения смарт-карты используется для аутентификации пользователя. Сетевой интерфейс 207

используется для подключения устройства 101 формирования изображений к сети. Принтер 208 осуществляет печать на листах бумаги согласно данным изображения. Сканер 209 считывает отпечатанный документ и т.п. и преобразует его в электронные данные.

5 <Программная конфигурация устройства формирования изображений>

Объясним со ссылкой на фиг. 3-5 программную конфигурацию устройства 101 формирования изображений и хранящуюся информацию. Согласно фиг. 3, устройство 101 формирования изображений включает в себя группу 301 драйверов устройств, операционную систему 302, платформу 303 приложений, услугу 304 обобществления пользовательского мандата, приложение 305 входа и приложения 306-313. Группа 301 драйверов устройств включает в себя совокупность драйверов устройств для управления различными вышеописанными аппаратными компонентами. Операционная система 302 обеспечивает интерфейсы группы 301 драйверов устройств для соответствующих приложений.

Платформа 303 приложений устанавливает/удаляет встроенное приложение устройства 101 формирования изображений и управляет операцией запуска/остановки и пр. Платформа 303 приложений, например, может включать в себя платформу JAVA® или инфраструктуру OSGi. JAVA® это зарегистрированный товарный знак Sun Microsystems, Inc. Инфраструктура OSGi - это платформа услуг на основе JAVA, созданная Альянсом OSGi - (стандартизирующей организацией). Помимо приложений, фабрично установленных на устройство 101 формирования изображений, пользователь может дополнительно устанавливать приложения на платформе 303 приложений. Платформа 303 приложений, например, представляет пользователю сервер, имеющий пользовательский интерфейс, показанный на фиг. 4, для управления приложениями. Администратор устройства 101 формирования изображений может указывать файл выполнения (JAR файл) приложения для дополнительной установки приложения по сети.

30 <Типы приложений>

Опишем типы приложений. Приложения, которые могут выполняться на платформе 303 приложений, включают в себя, например, системное приложение, приложение входа и общее приложение. Когда тип приложения не имеет конкретных ограничений, используется просто слово "приложение". Системное приложение фабрично устанавливается на устройство 101 формирования изображений. Приложение входа - это особое приложение, используемое для аутентификации пользователя, который входит в устройство 101 формирования изображений. Общее приложение - это приложение, отличное от приложения входа, которое может быть установлено/удалено пользователем.

Согласно фиг. 3, услуга 304 обобществления пользовательского мандата выступает в качестве системного приложения. Приложение 305 входа осуществляет аутентификацию пользователя, отображая на операционной панели пользовательский интерфейс для ввода имени пользователя/пароля, обозначенный позицией 501 на фиг. 5. Например, приложение 305 входа может отображать сообщение "держите смарт-карту над устройством чтения смарт-карты", обозначенное позицией 502 на фиг. 5, и осуществлять аутентификацию пользователя на основании информации смарт-карты, полученной от устройства 206 чтения смарт-карты. Приложения 306-313 являются общими приложениями.

45 <Мандат пользователя>

В этом варианте осуществления, аутентификация пользователя, описанная ниже, и

информация для сертификации пользователя, создаваемая после аутентификации пользователя, совместно называются мандатом пользователя. Мандат пользователя содержит ID пользователя, пароль, доменное имя, значение хеш-функции пароля, зашифрованный пароль, билет, например Kerberos TGT и билет SAML (Security Assertion Markup Language), биометрическую информацию, например отпечатки пальцев, и информацию смарт-карты, принадлежащей пользователю.

<Услуга 304 обобществления пользовательского мандата >

Объясним услугу 304 обобществления пользовательского мандата со ссылкой на фиг. 6. Услуга 304 обобществления пользовательского мандата позволяет обобществлять мандат пользователя среди приложений. Услуга 304 обобществления пользовательского мандата включает в себя API 601-603, показанные на фиг. 6, которые позволяют приложениям пользоваться услугой 304. API 601 SetUserCredential сохраняет мандат пользователя, указанный приложением, в памяти, например в ОЗУ 203. API 602 GetUserCredential получает мандат пользователя, хранящийся в ОЗУ 203, и возвращает его приложению. Обнаружив выход пользователя или остановку устройства 101 формирования изображений, услуга 304 обобществления пользовательского мандата аннулирует мандатные данные пользователя, хранящиеся в ОЗУ 203. API 603 GetKeyforEncryptCredential возвращает приложению сгенерированную информацию ключа. Идентификатор (элемент) мандата пользователя, используемого API 601-603, показанными на фиг. 6, будем далее называть ID мандата.

<Файл манифеста>

Опишем файлы манифеста со ссылкой на фиг. 7. Файлы выполнения приложения 305 входа и общих приложений 306-313, соответственно, включают в себя файлы манифеста 701-709, показанные на фиг. 7. Производитель описывает файл манифеста при создании приложения. Это позволяет производителю, создающему приложение, задавать информацию, соответствующую условию обобществления мандата пользователя, в файле манифеста. Платформа 303 приложений считывает соответствующий файл манифеста при установке или запуске приложения. При запуске приложения или устройства 101 формирования изображений или при входе пользователя услуга 304 обобществления пользовательского мандата получает соответствующий файл манифеста от платформы 303 приложений и генерирует настройки обобществления пользовательского мандата (описанные ниже). В файлах манифеста описаны имена и значения элементов. В этом варианте осуществления, элементы, описанные в файлах манифеста, заданы следующим образом.

•ApplicationID

Указывает уникальный идентификатор приложения.

•ApplilcationType

Указывает тип приложения. Значение "Login" в файле манифеста 701 представляет приложение входа, и значение "Application" в каждом из файлов манифеста 702-709 представляет общее приложение.

•TrustApplicationID

Указывает идентификатор доверенного приложения. Когда доверенное приложение не ограничено, пишется *.

•ReferenceCredentialID

Указывает ID мандата для мандата пользователя, подлежащего обращению.

•ReadOnlySharedCredentialID

Указывает ID мандата для мандата пользователя, обращаться к которому

разрешено только доверенному приложению.

•WritableSharedCredentialID

Указывает ID мандата для мандата пользователя, к которому доверенное приложение может обращаться и который оно может сохранять/обновлять.

•WritableEncryptSharedCredentialID

Указывает ID мандата для мандата пользователя, к которому доверенное приложение может обращаться и который оно может сохранять/обновлять. Мандат пользователя зашифрован и хранится в области ОЗУ 203, управляемой услугой 304 обобществления пользовательского мандата.

•CredentialType

Указывает тип обобществленного мандата, например символьную строку, например имя пользователя, пароль и доменное имя, значение хеш-функции пароля, зашифрованный пароль, билет, например Kerberos TGT и билет SAML, биометрическую информацию, например отпечатки пальцев, информацию смарт-карты, принадлежащей пользователю, и т.п. Если ничего не описано, предполагается символьная строка.

<Приложение 305 входа>

Приложение 305 входа имеет файл манифеста 701. Приложение 305 входа получает имя пользователя и пароль, введенные через экран входа 501, и аутентифицирует пользователя, который использует устройство 101 формирования изображений. Имя пользователя и пароль пользователя, успешно прошедшего аутентификацию, записываются в ОЗУ 203 с использованием API услуги 304 обобществления пользовательского мандата. Позиция 710 указывает, что приложение 305 входа сохраняет ID мандата (LoginAccount/LoginPassword) в качестве мандата пользователя, к которому может обращаться другое приложение. Позиция 711 указывает, что приложение, которое обращается к LoginAccount/LoginPassword, не ограничено и что всем приложениям разрешено обращаться к LoginAccount/LoginPassword, поскольку значение равно * (символ замещения).

<Приложения 306 и 307>

Приложения 306 и 307 являются общими приложениями, имеющими функцию передачи/приема электронной почты путем осуществления доступа к почтовому серверу 102. Приложения 306 и 307 имеют, соответственно, файлы манифеста 702 и 703. Позиция 712 указывает, что приложение 306 обращается к LoginAccount/LoginPassword, сохраненным приложением 305 входа с использованием API услуги 304 обобществления пользовательского мандата. Приложение 306 использует LoginAccount/LoginPassword для аутентификации при осуществлении доступа к почтовому серверу 102. Аналогично, другие приложения 307 - 313 используют LoginAccount/LoginPassword в качестве информации аутентификации при осуществлении доступа к внешнему серверу. Позиция 713 указывает, что приложения 306 и 307 имеют между собой доверительные отношения. Позиция 714 указывает, что приложения 306 и 307 обобществляют посредством услуги 304 обобществления пользовательского мандата имя пользователя и пароль для доступа к почтовому серверу 102 в качестве MailAccount/MailPassword.

<Приложения 308, 309, 310 и 311>

Приложения 308, 309, 310 и 311 являются общими приложениями для доступа к серверу 103 обобществления файлов. Эти приложения имеют функцию преобразования документа, считанного сканером 209, в данные PDF и их передачи на сервер 103 обобществления файлов, и функцию печати с использованием принтера 208

документа, полученного с сервера 103 обобществления файлов. Приложения 308, 309, 310 и 311 имеют, соответственно, файлы манифеста 704, 705, 706 и 707. Позиция 715 указывает, что приложения обобществляют посредством услуги 304 обобществления пользовательского мандата имя пользователя/пароль для доступа к серверу 103

обобществления файлов в качестве FileServerAccount/FileServerMailPassword.

Позиция 716 указывает, что приложение 308 имеет доверительные отношения с приложениями 309 и 310, но между приложениями 309 и 310 нет доверительных отношений. Кроме того, указано, что приложение 311 доверяет приложению 308, но приложение 308 не доверяет приложению 311.

<Приложения 312 и 313>

Приложения 312 и 313 являются общими приложениями для получения информации путем осуществления доступа к веб-серверу в интернете (WAN 106). Поскольку приложения 312 и 313 осуществляют доступ к интернету (WAN 106) через прокси-сервер 104, им требуется пройти аутентификацию, чтобы использовать прокси-сервер 104. Приложения 312 и 313 имеют, соответственно, файлы манифеста 708 и 709. Позиция 717 указывает, что приложения 312 и 313 имеют между собой доверительные отношения. Позиция 718 указывает, что приложения 312 и 313 обобществляют в зашифрованном виде имя пользователя и пароль для доступа к прокси-серверу 104 в качестве WebProхуAccount и WebProхуPassword.

<Операция, связанная с запуском услуги 304 обобществления пользовательского мандата>

Теперь объясним, со ссылкой на фиг. 8, операцию, связанную с запуском услуги 304 обобществления пользовательского мандата согласно этому варианту осуществления. Обработка, описанная ниже, осуществляется, когда ЦП 201 считывает программу из ПЗУ 202 или ЖД 204 и выполняет ее.

На этапе S801, когда платформа 303 приложений вызывает обработку запуска, услуга 304 обобществления пользовательского мандата запускает обработку запуска. На этапе S802 услуга 304 обобществления пользовательского мандата получает через платформу 303 приложений содержимое файлов манифеста всех запущенных приложений. На этапе S803, услуга 304 обобществления пользовательского мандата анализирует все полученные файлы манифеста и генерирует надлежащие настройки 901 обобществления пользовательского мандата, которые задают условия обобществления среди приложений, показанные на фиг. 9. Настройки обобществления пользовательского мандата содержат ID мандата, тип мандата пользователя, ID управления, указывающий область хранения для мандата пользователя, выдаваемого услугой 304 обобществления пользовательского мандата, ApplicationID приложения, которое может сохранять/обновлять мандат пользователя в области хранения, указанной посредством ID управления, и ApplicationID приложения, которое может обращаться к мандату пользователя в области хранения, указанной посредством ID управления.

Проанализировав данные 715 и 716, например, файлов манифеста, услуга 304 обобществления пользовательского мандата генерирует три ID управления, указывающие области для хранения FileServerPassword. ID управления FileServerPassword_001 указывает область, используемую приложениями 308 и 309 для обобществления FileServerPassword. Аналогично, ID управления FileServerPassword_002 указывает область, используемую приложениями 308 и 310 для обобществления FileServerPassword. ID управления FileServerPassword_003 указывает область, используемую приложением 311

для осуществления операции сохранения/обновления. Поскольку приложение 311 доверяет приложению 308, приложение 308 может обращаться к мандату пользователя с FileServerPassword_003. Однако, поскольку приложение 308 не доверяет приложению 311, услуга 304 генерирует настройки обобществления, не позволяющие
 5 сохранять/обновлять мандат для FileServerPassword_003, к которому обращается приложение 311.

На этапе S804, если настройки 901 обобществления пользовательского мандата сгенерированы после запуска услуги 304 обобществления пользовательского мандата
 10 и настройки использования 902 записаны на ЖД 204, услуга 304 обобществления пользовательского мандата обращается к ним и получает их. Настройка использования 902 - это информация, представляющая, использует ли пользователь функцию обобществления мандата пользователя, указанную в настройках 901 обобществления пользовательского мандата. TRUE (активный) указывает, что
 15 пользователь использует функцию, и FALSE (неактивный) указывает, что пользователь не использует функцию. То есть, если настройка использования 902 указывает TRUE, согласно настройкам 901 обобществления пользовательского мандата, то услуга 304 обобществления пользовательского мандата определяет,
 20 предоставлять ли приложению соответствующий мандат пользователя. Если услуга 304 обобществления пользовательского мандата может получать предыдущие настройки обобществления пользовательского мандата с ЖД 204, она сравнивает их с вновь сгенерированными настройками обобществления пользовательского мандата и выявляет различие между ними.

При наличии дополнительной информации услуга 304 обобществления пользовательского мандата обновляет настройки обобществления пользовательского мандата на этапе S805 и сохраняет обновленную информацию на ЖД 204 на этапе S806. На этапе S805, когда услуга 304 обобществления пользовательского
 30 мандата может получать предыдущие настройки использования с ЖД 204, она вновь добавляет дополнительную информацию, если таковая имеется, таким образом, обновляя настройки использования. Если услуга 304 обобществления пользовательского мандата не может получать настройки использования с ЖД 204, она генерирует настройки использования для задания начальных значений. В этом
 35 варианте осуществления, TRUE (указывающий, что пользователь использует функцию) задается в качестве начальных значений настроек использования. Сгенерированные и обновленные настройки использования сохраняются на ЖД 204 на этапе S806.

Услуга 304 обобществления пользовательского мандата может распознавать установку или запуск нового приложения через платформу 303 приложений. В этом случае услуга 304 обобществления пользовательского мандата анализирует файл манифеста нового приложения и обновляет настройки обобществления
 40 пользовательского мандата/настройки использования, записанные на ЖД 204.

Как описано выше, услуга 304 обобществления пользовательского мандата автоматически генерирует настройки обобществления пользовательского мандата с использованием информации, описанной в файле манифеста, полученном от приложения. Это позволяет пользователю, который усматривает трудности при вводе
 45 детальных настроек для обобществления мандата пользователя, безопасно использовать услугу 304 обобществления пользовательского мандата, не беспокоясь о настройках.

<Операция, связанная с настройкой услуги 304 обобществления пользовательского

мандата>

Услуга 304 обобществления пользовательского мандата имеет функцию отображения на операционной панели 205 пользовательского интерфейса 1000, используемого для задания настроек использования настроек обобществления пользовательского мандата, показанную на фиг. 10. С пользовательским интерфейсом 1000 может работать только администратор устройства 101 формирования изображений. Позиция 1001 указывает флажки для изменения настроек использования 902 для настроек 901 обобществления пользовательского мандата, сгенерированных услугой 304 обобществления пользовательского мандата. Администратор выбирает флажки для задания значения TRUE. В этом варианте осуществления предполагается, что в начальном состоянии все флажки выбраны. Администратор может отменять выбор флажка для задания значения FALSE. Таким образом, настройки использования 902 используются для активации или деактивации условий обобществления для элементов мандата пользователя, заданных в настройках 901 обобществления пользовательского мандата.

Услуга 304 обобществления пользовательского мандата имеет функцию отображения на операционной панели 205 пользовательского интерфейса 1100 для редактирования настроек обобществления пользовательского мандата, показанную на фиг. 11. Например, когда пользователь выбирает некоторые из флажков 1101, которые соответствуют настройкам, подлежащим редактированию, и затем нажимает кнопку редактирования 1102, на операционной панели 205 отображается пользовательский интерфейс 1110, показанный на фиг. 11. Пользовательский интерфейс 1110 отображает список 1103 приложений с возможностью обновления мандата пользователя и список 1104 приложений с возможностью обращения к мандату пользователя и позволяет администратору добавлять/удалять соответствующие приложения.

Возвращаясь к фиг. 8, опишем операцию, связанную с настройкой услуги 304 обобществления пользовательского мандата. Обнаружив доступ со стороны администратора, услуга 304 обобществления пользовательского мандата получает настройки 901 обобществления пользовательского мандата и настройки использования 902 с ЖД 204 на этапе S808 и отображает пользовательские интерфейсы 1000 и 1100. Обнаружив, например, операцию смены настроек использования со стороны администратора, услуга 304 обобществления пользовательского мандата обновляет настройки использования 902 и записывает обновленные настройки использования на ЖД 204 на этапе S809. Что касается настроек обобществления пользовательского мандата, которые администратор предписал использовать, существует возможность создавать настройки использования для каждого общего пользователя, который использует устройство 101 формирования изображений. Обнаружив, что администратор отредактировал настройки обобществления пользовательского мандата с использованием пользовательских интерфейсов 1100 и 1110, услуга 304 обобществления пользовательского мандата обновляет настройки 901 обобществления пользовательского мандата и записывает обновленную информацию на ЖД 204 на этапе S810.

Некоторые пользователи, использующие приложение, могут испытывать беспокойство по поводу "утечки" мандата пользователя, и некоторые могут заострять внимание на практичности осуществления однократного входа. Согласно этому варианту осуществления, обеспечение пользовательского интерфейса, позволяющего пользователю менять настройки 901 обобществления пользовательского мандата и

настройки использования 902, дает возможность пользователю изменять настройки обобществления по своему желанию. Поскольку пользователь также может, по своему выбору, не использовать автоматически сгенерированные настройки обобществления пользовательского мандата, это позволяет предотвратить "утечку" мандата

5 пользователя. Когда пользователь изменяет автоматически сгенерированные настройки 901 обобществления пользовательского мандата, чтобы дать возможность обобществления мандата пользователя среди более широкого круга приложений, можно повысить практичность выполнения однократного входа.

10 <Операция при выполнении услуги 304 обобществления пользовательского мандата>

Объясним, со ссылкой на фиг. 12, пример операции, когда услуга 304 обобществления пользовательского мандата используется другим приложением. Заметим, что операция проиллюстрирована в случае, когда пользователь использует

15 приложение 312 сразу после входа в устройство 101 формирования изображений и затем выходит с использованием приложения 313. Обработка услуги 304 обобществления пользовательского мандата, приложения 305 входа и приложений 312 и 313, описанных ниже, осуществляется, когда ЦП 201 считывает программу из

20 ПЗУ 202 или ЖД 204 и выполняет ее.

На этапе S1200 пользователь осуществляет операцию входа, вводя свои имя пользователя и пароль через экран входа 501, отображаемый на операционной панели 205 устройства 101 формирования изображений. На этапе S1201, после

25 подтверждения, что пользователь является авторизованным пользователем, путем проверки введенных имени пользователя и пароля, приложение 305 входа извещает услугу 304 обобществления пользовательского мандата о входе пользователя. Получив извещение входа, услуга 304 обобществления пользовательского мандата на этапе S1202 обращается к настройкам 901 обобществления пользовательского

30 мандата и настройкам использования 902, хранящимся на ЖД 204.

Если настройки 901 обобществления пользовательского мандата содержат WebProxyAccount_001/WebProxyPassword_001, которые подлежат шифрованию, на этапе S1203 услуга 304 обобществления пользовательского мандата генерирует ключ шифрования, используемый для шифрования/дешифрования данных,

35 и удерживает его в ОЗУ 203. Для генерации ключа используется криптография общего ключа, например AES. Например, в ОЗУ 203 подготавливается таблица 1300 управления мандатными данными пользователя для управления данными в связи с ID управления. В этом примере, услуга 304 генерирует данные ключей шифрования 001 и 002 и сохраняет их в связи с WebProxyAccount_001 и WebProxyPassword_002,

40 соответственно.

На этапе S1204, услуга 304 обобществления пользовательского мандата распространяет сгенерированный ключ шифрования на приложения 312 и 313, использующие WebProxyAccount_001 и WebProxyPassword_002. Услуга 304

45 обобществления пользовательского мандата может иметь API 603, с помощью которого каждое приложение может получать ключ шифрования в произвольное время. На этапе S1205, приложение 305 входа использует API 601 SetUserCredential, чтобы запрашивать услугу 304 обобществления пользовательского мандата

50 сохранить имя пользователя и пароль, полученные на этапе S1200. Обращаясь к настройкам 901 обобществления пользовательского мандата и настройкам использования 902, услуга 304 обобществления пользовательского мандата проверяет, может ли приложение 305 входа обновить LoginAccount_001/LoginPassword_001.

Услуга 304 обобществления пользовательского мандата сохраняет имя пользователя/пароль (Alice/AliceLogin) в таблице 1300 управления мандатными данными пользователя в связи с LoginAccount_001/LoginPassword_001. Записываются также ApplicationID последнего приложения, произведшего обновление, и дата/время обновления.

На этапе S1206, приложение 312 выявляет пользовательскую операцию, которая требует доступа в интернет. На этапе S1207, приложение 312 использует API 602 GetUserCredential, чтобы запрашивать услугу 304 обобществления пользовательского мандата, чтобы получить WebProxyAccount/WebProxyPassword. Хотя услуга 304 обобществления пользовательского мандата обращается к таблице 1300 управления мандатными данными пользователя, таблица 1300 не сохраняет WebProxyAccount_001/WebProxyPassword_001 сразу после входа, возвращая, таким образом, NULL.

Если приложение 312 не может получить WebProxyAccount/WebProxyPassword, оно запрашивает услугу 304 обобществления пользовательского мандата, чтобы получить LoginAccount/LoginPassword на этапе S1208. Услуга 304 обобществления пользовательского мандата возвращает LoginAccount (Alice)/LoginPassword (AliceLogin).

После этого, на этапе S1209, приложение 312 осуществляет доступ к прокси-серверу 104 и пытается пройти аутентификацию с использованием имени пользователя и пароля, полученных на этапе S1208. Если имя пользователя (Alice) и пароль (AliceLogin) зарегистрированы на прокси-сервере 104, аутентификация завершается успешно. В этом случае пользователь может осуществлять доступ в интернет, не проходя специально аутентификацию на прокси-сервере 104. Альтернативно, если имя пользователя (Alice) и пароль (AliceLogin) не зарегистрированы на прокси-сервере 104, возвращается ошибка аутентификации.

Объясним последующую обработку в случае, когда возвращается ошибка аутентификации. В случае неудачной аутентификации на прокси-сервере 104, на этапе S1210 приложение 312 отображает экран 503 аутентификации на прокси-сервере, предлагающий пользователю ввести свои имя пользователя/пароль для аутентификации на прокси-сервере. После этого, обнаружив операцию ввода пользователем имени пользователя/пароля для аутентификации на прокси-сервере на этапе S1211, приложение 312 повторно осуществляет доступ к прокси-серверу 104 для осуществления обработки аутентификации с использованием введенных имени пользователя/пароля на этапе S1212. В случае успешной обработки аутентификации на прокси-сервере, на этапе S1213 приложение 312 использует ключ шифрования, полученный на этапе S1204, для шифрования имени пользователя/пароля, для которых аутентификация на прокси-сервере прошла успешно. После этого, на этапе S1214, приложение 312 использует API 601 SetUserCredential для сохранения зашифрованных имени пользователя/пароля в услуге обобществления пользовательского мандата.

На этапе S1215, приложение 313 выявляет пользовательскую операцию, которая требует доступа в интернет. На этапе S1216, приложение 313 использует API 602 GetUserCredential, чтобы запрашивать услугу 304 обобществления пользовательского мандата для получения WebProxyAccount/WebProxyPassword. Обращаясь к настройкам 901 обобществления пользовательского мандата и настройкам использования 902, услуга 304 обобществления пользовательского мандата проверяет, может ли приложение 313 обращаться к WebProxyAccount_001/WebProxyPassword_001. Если да, то услуга 304 обобществления пользовательского мандата обращается к

таблице 1300 управления мандатными данными пользователя и затем возвращает зашифрованные имя пользователя/пароль, хранящиеся в WebProxyAccount_001/WebProxyPassword_001. Если возможно обращение к совокупности имен пользователя/паролей, связанных с ID управления для одного ID мандата, то услуга 304 возвращает совокупность имен пользователя/паролей. В этом случае услуга 304 может возвращать имена пользователя/пароли, сортируя их в порядке приоритета с учетом приложения, произведшего операцию сохранения, даты/времени обновления и пр.

Когда приложению 313 удастся получить зашифрованные имя пользователя/пароль, на этапе S1217 оно дешифрует зашифрованные данные с использованием ключа шифрования, полученного на этапе S1204, получая, таким образом, имя пользователя/пароль. На этапе S1218, приложение 313 осуществляет доступ к прокси-серверу 104 для осуществления обработки аутентификации с использованием полученных имени пользователя/пароля.

Обнаружив операцию выхода пользователя на этапе S1219, приложение 305 входа передает извещение выхода услуге 304 обобществления пользовательского мандата на этапе S1220. Получив извещение выхода, на этапе S1221 услуга 304 обобществления пользовательского мандата аннулирует все данные, записанные в таблице 1300 управления мандатными данными пользователя.

<Дополнительное объяснение API SetUserCredential>

При наличии совокупности обновляемых ID управления, связанных с CredentialID, указанным в качестве аргумента, API 601 SetUserCredential сохраняет мандат пользователя во всех областях, указанных посредством ID управления. Например, опишем операцию, когда приложение 308 вызывает API 601 SetUserCredential, указывая FileServerPassword в качестве CredentialID. Обращаясь к настройкам 901 обобществления пользовательского мандата и настройкам использования 902, услуга 304 обобществления пользовательского мандата подтверждает, что приложение 308 может обновить FileServerPassword_001/FileServerPassword_002. Затем услуга 304 сохраняет мандатные данные пользователя, указанные в качестве аргументов, в связи с FileServerPassword_001/FileServerPassword_002 таблицы 1300 управления мандатными данными пользователя, соответственно.

<Другие варианты осуществления>

Согласно вышеописанному варианту осуществления, был описан случай, когда имя пользователя/пароль обобществляется с использованием услуги 304 обобществления пользовательского мандата. Однако настоящее изобретение этим не ограничивается. Можно также обобществлять с использованием услуги 304 обобществления пользовательского мандата значение хеш-функции пароля, билет, например Kerberos TGT и билет SAML, биометрическую информацию, например отпечатки пальцев, информацию смарт-карты, принадлежащей пользователю, и пр. в качестве другого мандата пользователя.

Согласно вышеописанному варианту осуществления, ID приложения, выступающий в качестве информации, указывающей приложение, являющееся целью обобществления, описан как TrustApplicationID в файле манифеста. Однако можно описывать другую информацию при условии, что информация связана с приложением. Например, информацию о производителе, создавшем приложение, можно описывать в файле манифеста, и все приложения, созданные производителем, можно указывать как цели обобществления. Кроме того, информацию группы приложений можно описывать в файле манифеста, и все приложения, принадлежащие группе приложений,

можно указывать как цели обобществления.

Аспекты настоящего изобретения также можно реализовать посредством компьютера системы или устройства (или устройств, например, ЦП или МРU), которое считывает и выполняет программу, записанную в запоминающем устройстве для осуществления функций вышеописанного(ых) варианта(ов) осуществления, и посредством способа, этапы которого осуществляются посредством компьютера системы или устройства, например, считывающего и выполняющего программу, записанную в запоминающем устройстве для осуществления функций вышеописанного(ых) варианта(ов) осуществления. С этой целью программа передается на компьютер, например, по сети или в виде носителя записи того или иного типа, служащего запоминающим устройством (например, компьютерно-считываемого носителя).

Хотя настоящее изобретение описано со ссылкой на иллюстративные варианты осуществления, следует понимать, что изобретение не ограничивается раскрытыми иллюстративными вариантами осуществления. Объем нижеследующей формулы изобретения должен соответствовать широчайшей интерпретации, чтобы охватывать все подобные модификации и эквивалентные структуры и функции.

Формула изобретения

1. Устройство обработки информации, содержащее

блок получения, который получает от каждого из множества приложений, выполняющихся на устройстве обработки информации, условие совместного использования мандата пользователя с другим приложением, причем мандат пользователя включает в себя информацию для сертификации пользователя,

блок генерации, который генерирует на основании полученного условия совместного использования настройки совместного использования, которые задают упомянутое условие совместного использования мандата пользователя среди приложений, и сохраняет сгенерированные настройки совместного использования в памяти,

блок удержания, который удерживает в памяти мандат пользователя, переданный из первого приложения из упомянутого множества приложений, и

блок предоставления, который предоставляет по получении запроса мандата пользователя от приложения, отличного от упомянутого первого приложения из упомянутого множества, упомянутый мандат пользователя запрашивающему приложению согласно настройкам совместного использования, хранящимся в памяти.

2. Устройство по п.1, в котором блок генерации генерирует настройки совместного использования при запуске устройства, при запуске приложения или при входе в систему пользователя, сравнивает сгенерированные настройки совместного использования с настройками совместного использования, уже хранящимися в памяти, и обновляет содержимое памяти сгенерированными настройками совместного использования, если имеется различие в результате сравнения.

3. Устройство по п.1, в котором блок удержания дополнительно удерживает в памяти настройку использования, чтобы сделать достоверным или недостоверным условие совместного использования каждого элемента мандата пользователя, заданного в настройках совместного использования, и

когда настройка использования указывает достоверное состояние, блок предоставления определяет на основании настроек совместного использования, предоставлять ли мандат пользователя запрашивающему приложению.

4. Устройство по п.3, дополнительно содержащее пользовательский интерфейс для изменения настроек совместного использования и настройки использования, удерживаемых в памяти.

5. Устройство по п.1, в котором блок предоставления не предоставляет мандат пользователя, если приложение, запросившее мандат пользователя, не задано в настройках совместного использования для совместного использования мандата пользователя, и

предоставляет мандат пользователя, если приложение, запросившее мандат пользователя, задано в настройках совместного использования для совместного использования мандата пользователя.

6. Устройство по п.1, в котором блок предоставления включает в себя блок шифрования, который шифрует мандат пользователя, удерживаемый блоком удержания, и

блок распространения, который распространяет на каждое приложение ключ шифрования, используемый для шифрования мандата пользователя.

7. Устройство по п.1, в котором множество приложений включает в себя приложение входа в систему для выдачи мандата пользователя аутентифицированного пользователя, и

блок удержания удерживает в памяти мандат пользователя, выданный приложением входа в систему, для пользователя, аутентификацию которого выполнило приложение входа в систему, и удаляет мандат пользователя из памяти при выходе пользователя.

8. Устройство по п.1, в котором для каждого элемента мандата пользователя настройки совместного использования содержат информацию о приложении, способном обращаться к информации пользовательского мандата, и информацию о приложении, способном обновлять информацию пользовательского мандата.

9. Способ управления для устройства обработки информации, содержащий этапы, на которых

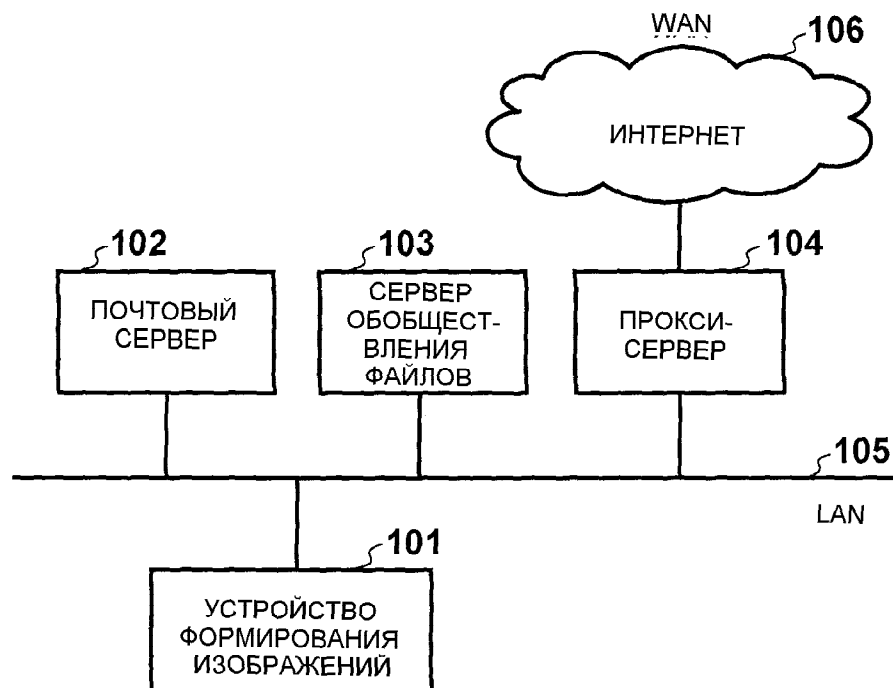
получают от каждого из множества приложений, выполняющихся на устройстве обработки информации, условие совместного использования мандата пользователя с другим приложением, причем мандат пользователя включает в себя информацию для сертификации пользователя,

генерируют на основании полученного условия совместного использования настройки совместного использования, которые задают условие совместного использования мандата пользователя среди приложений, и сохраняют сгенерированные настройки совместного использования в памяти,

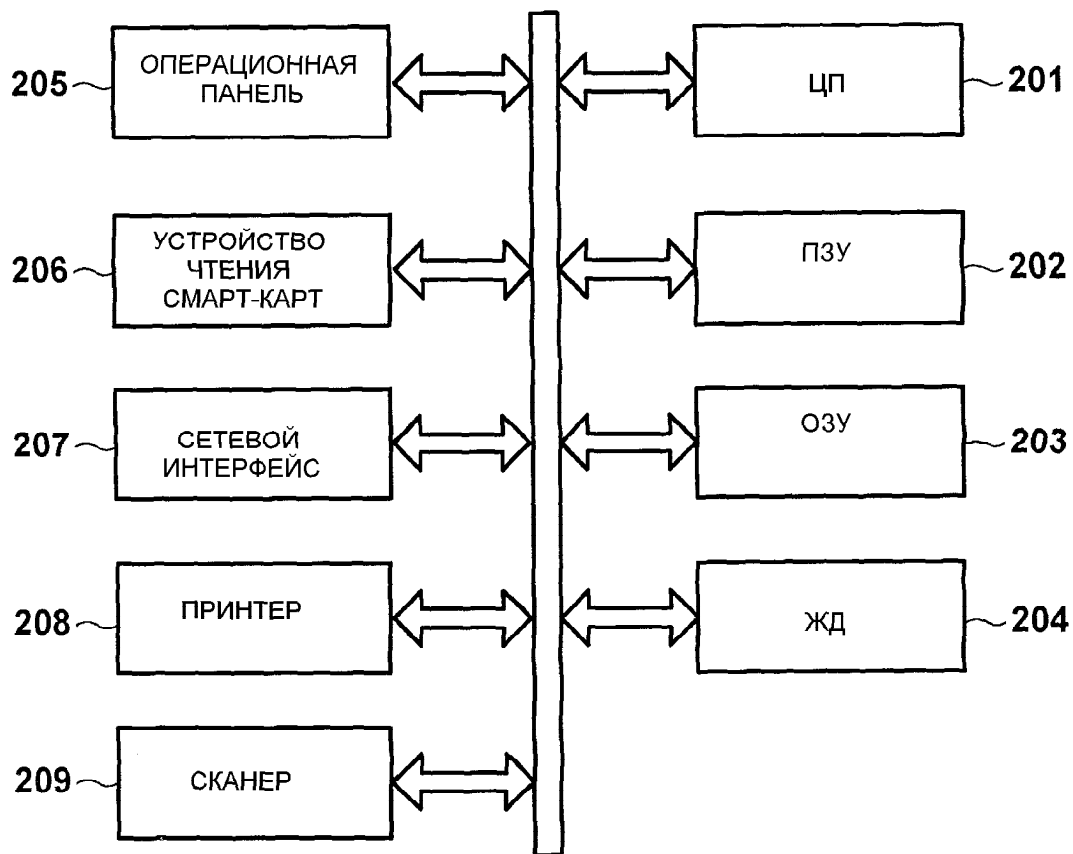
удерживают в памяти мандат пользователя, переданный из первого приложения из множества приложений, и

предоставляют после приема запроса мандата пользователя от приложения, отличного от первого приложения из упомянутого множества приложений, мандат пользователя запрашивающему приложению согласно настройкам совместного использования, хранящимся в памяти.

10. Считываемый компьютером носитель информации для хранения компьютерной программы, предписывающей компьютеру выполнять каждый этап способа управления для устройства обработки информации по п.9.



ФИГ. 1



ФИГ. 2



ФИГ. 3

ДОПОЛНИТЕЛЬНАЯ УСТАНОВКА ПРИЛОЖЕНИЯ

ВВЕДИТЕ ПУТЬ К ФАЙЛУ

УСТАНОВИТЬ

УПРАВЛЕНИЕ УСТАНОВЛЕННЫМИ ПРИЛОЖЕНИЯМИ

УДАЛИТЬ

ЗАПУСТИТЬ

ОСТАНОВИТЬ

ВХОД В ПРИЛОЖЕНИЕ	СОСТОЯНИЕ
☐ ПРИЛОЖЕНИЕ ВХОДА С ПОМОЩЬЮ СМАРТ-КАРТЫ СТОРОННЕГО ПРОИЗВОДИТЕЛЯ	НЕАКТИВНО
☒ ПРИЛОЖЕНИЕ ВХОДА 305	АКТИВНО

УДАЛИТЬ

ЗАПУСТИТЬ

ОСТАНОВИТЬ

ПРИЛОЖЕНИЕ	СОСТОЯНИЕ
☐ ПРИЛОЖЕНИЕ 306	АКТИВНО
☐ ПРИЛОЖЕНИЕ 307	АКТИВНО
☐ ПРИЛОЖЕНИЕ 308	АКТИВНО

ФИГ. 4

The figure shows three sequential user interface screens for smart card authentication, labeled 501, 502, and 503.

Screen 501: A login screen with two input fields. The first field is labeled "ID ПОЛЬЗОВАТЕЛЯ" (User ID) and the second is labeled "ПАРОЛЬ" (Password). A button labeled "ВОЙТИ" (Login) is positioned to the right of the password field.

Screen 502: An instruction screen displaying the text: "ДЕРЖИТЕ ВАШУ СМАРТ-КАРТУ НАД УСТРОЙСТВОМ ЧТЕНИЯ СМАРТ-КАРТ" (Hold your smart card over the smart card reader device).

Screen 503: A screen for entering information for authentication on a proxy server. The title is "ВВОД ИНФОРМАЦИИ ДЛЯ АУТЕНТИФИКАЦИИ НА ПРОКСИ-СЕРВЕРЕ" (Input information for authentication on the proxy server). It contains two input fields. The first field is labeled "ИМЯ ПОЛЬЗОВАТЕЛЯ" (User name). The second field is unlabeled. At the bottom, there are two buttons: "ОК" (OK) and "отмена" (Cancel).

ФИГ. 5

601

Void SetUserCredential (String ApplicationID, int CredentialID, int Type, Object value);

АРГУМЕНТ

ApplicationID ИДЕНТИФИКАТОР ПРИЛОЖЕНИЯ

CredentialID ИДЕНТИФИКАТОР МАНДАТА ПОЛЬЗОВАТЕЛЯ

ТИП

ТИП МАНДАТА ПОЛЬЗОВАТЕЛЯ
УКАЗЫВАЕТ ТИП, НАПРИМЕР, СИМВОЛЬНУЮ СТРОКУ, НАПРИМЕР, ИМЯ ПОЛЬЗОВАТЕЛЯ, ПАРОЛЬ И ДОМЕННОЕ ИМЯ, ЗНАЧЕНИЕ ХЕШ-ФУНКЦИИ ПАРОЛЯ, ЗАШИФРОВАННЫЙ ПАРОЛЬ, БИЛЕТ, НАПРИМЕР, KERBEROS TGT И БИЛЕТ SAML, БИОМЕТРИЧЕСКУЮ ИНФОРМАЦИЮ, НАПРИМЕР, ОТПЕЧАТКИ ПАЛЬЦЕВ, ИНФОРМАЦИЮ СМАРТ-КАРТЫ, ПРИНАДЛЕЖАЩЕЙ ПОЛЬЗОВАТЕЛЮ, И Т.П.

ЗНАЧЕНИЕ ДАННЫЕ МАНДАТА ПОЛЬЗОВАТЕЛЯ

602

ListObject GetUserCredential (String ApplicationID, int CredentialID, Object value);

АРГУМЕНТ

ApplicationID ИДЕНТИФИКАТОР ПРИЛОЖЕНИЯ

CredentialID ИДЕНТИФИКАТОР МАНДАТА ПОЛЬЗОВАТЕЛЯ

ВОЗВРАЩАЕМОЕ ЗНАЧЕНИЕ

- ВОЗВРАТИТЬ ДАННЫЕ МАНДАТА ПОЛЬЗОВАТЕЛЯ, К КОТОРОМУ МОЖНО ОБРАЩАТЬСЯ, СВЯЗАННЫЕ С *CREDENTIALID*, В ВИДЕ СПИСКА
- ВОЗВРАТИТЬ NULL В ОТСУТСТВИЕ СОХРАНЕННОГО МАНДАТА ПОЛЬЗОВАТЕЛЯ ИЛИ НАСТРОЕК ОБЩЕСТВЛЕНИЯ

603

KeyInformation GetKeyforEncryptCredential (String ApplicationID, intCredentialID);

АРГУМЕНТ

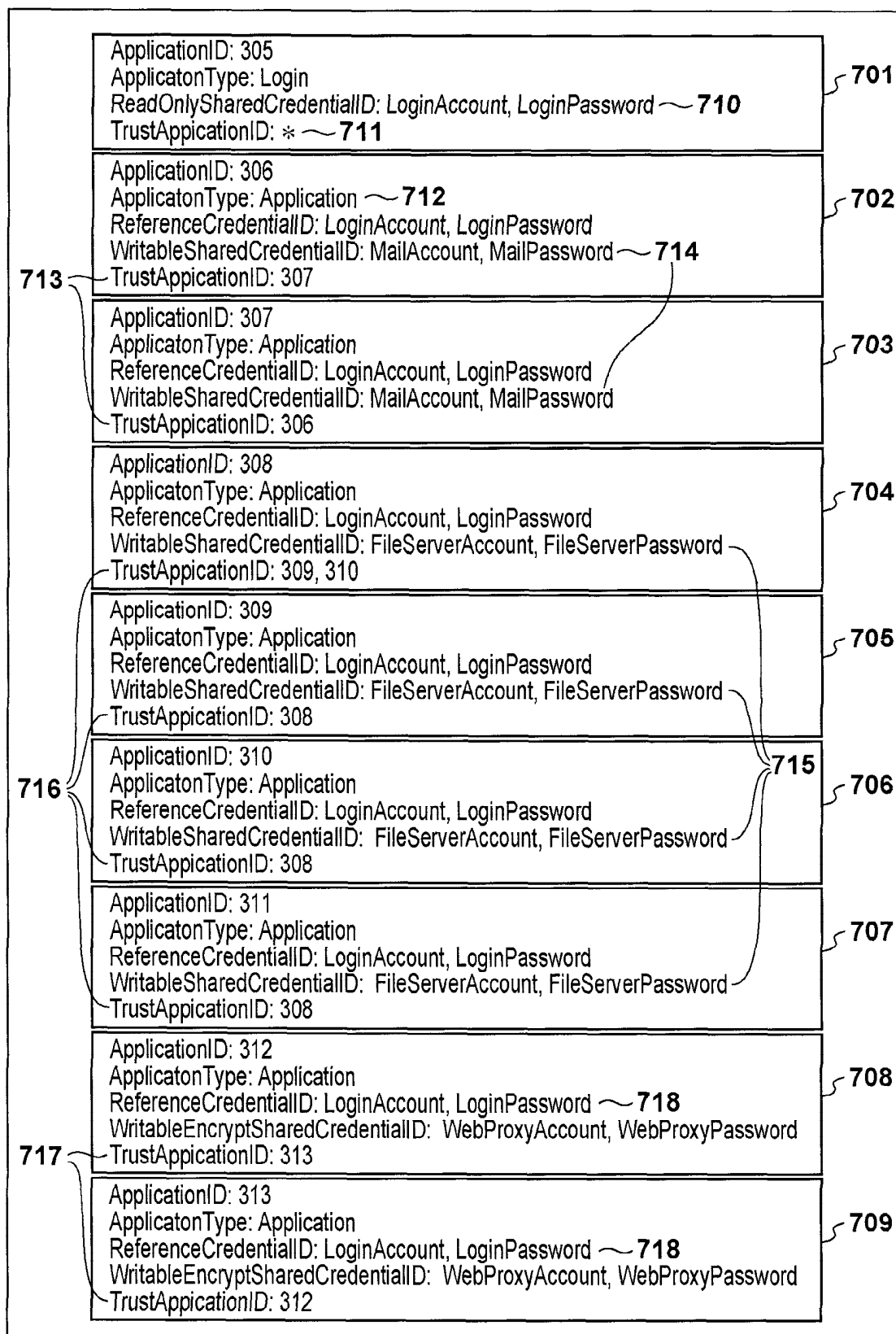
ApplicationID ИДЕНТИФИКАТОР ПРИЛОЖЕНИЯ

CredentialID ИДЕНТИФИКАТОР МАНДАТА ПОЛЬЗОВАТЕЛЯ

ВОЗВРАЩАЕМОЕ ЗНАЧЕНИЕ

ВОЗВРАТИТЬ ИНФОРМАЦИЮ КЛЮЧА (СИЛУ КЛЮЧА, АЛГОРИТМ, ДАННЫЕ КЛЮЧА И ПР.) ДЛЯ ШИФРОВАНИЯ/ДЕШИФРОВАНИЯ МАНДАТА ПОЛЬЗОВАТЕЛЯ, УКАЗАННОГО ПОСРЕДСТВОМ CREDENTIALID

ФИГ. 6



ФИГ. 7

901					902	
ID МАНДАТА	ТИП	ID УПРАВЛЕНИЯ	ПРИЛОЖЕНИЕ С ВОЗМОЖ- НОСТЬЮ ОБНОВЛЕНИЯ МАНДАТА ПОЛЬ- ЗОВАТЕЛЯ	ПРИЛОЖЕНИЕ С ВОЗМОЖ- НОСТЬЮ ОБРА- ЩЕНИЯ К МАН- ДАТУ ПОЛЬЗО- ВАТЕЛЯ	ID УПРАВЛЕНИЯ	НАСТРОЙКА ИСПОЛЬ- ЗОВАНИЯ
LoginAccount	СИМВОЛЬНАЯ СТРОКА	LoginAccount_001	305	*	LoginAccount_001	TRUE
LoginPassword	СИМВОЛЬНАЯ СТРОКА	LoginPassword_001	305	*	LoginPassword_001	TRUE
MailAccount	СИМВОЛЬНАЯ СТРОКА	MailAccount_001	306,307	306,307	MailAccount_001	TRUE
MailPassword	СИМВОЛЬНАЯ СТРОКА	MailPassword_001	306,307	306,307	MailPassword_001	TRUE
FileServerAccount	СИМВОЛЬНАЯ СТРОКА	FileServerAccount_001	308,309	308,309	FileServerAccount_001	TRUE
		FileServerAccount_002	308,310	308,310	FileServerAccount_002	TRUE
		FileServerAccount_003	311	308,311	FileServerAccount_003	FALSE
FileServerPassword	СИМВОЛЬНАЯ СТРОКА	FileServerPassword_001	308,309	308,309	FileServerPassword_001	TRUE
		FileServerPassword_002	308,310	308,310	FileServerPassword_002	TRUE
		FileServerPassword_003	311	308,311	FileServerPassword_003	FALSE
WebProxyAccount	СИМВОЛЬНАЯ СТРОКА	WebProxyAccount_001	312,313	312,313	WebProxyAccount_001	TRUE
WebProxyPassword	СИМВОЛЬНАЯ СТРОКА	WebProxyPassword_002	312,313	312,313	WebProxyPassword_002	TRUE

ФИГ. 9

1001		1000		
НАСТ- РОЙКА ИСПОЛЬ- ЗОВАНИЯ	ID МАНДАТА	ID УПРАВЛЕНИЯ	ПРИЛОЖЕНИЕ С ВОЗМОЖ- НОСТЬЮ ОБ- НОВЛЕНИЯ МАНДАТА ПОЛЬ- ЗОВАТЕЛЯ	ПРИЛОЖЕНИЕ С ВОЗМОЖ- НОСТЬЮ ОБ- РАЩЕНИЯ К МАНДАТУ ПОЛЬ- ЗОВАТЕЛЯ
☒	LoginAccount	LoginAccount_001	305	*
☒	LoginPassword	LoginPassword_001	305	*
☒	MailAccount	MailAccount_001	306,307	306,307
☒	MailPassword	MailPassword_001	306,307	306,307
☒	FileServerAccount	FileServerAccount_001	308,309	308,309
☒	FileServerAccount	FileServerAccount_002	308,310	308,310
☐	FileServerAccount	FileServerAccount_003	311	308,311
☒	FileServerPassword	FileServerPassword_001	308,309	308,309
☒	FileServerPassword	FileServerPassword_002	308,310	308,310
☐	FileServerPassword	FileServerPassword_003	311	308,311
☒	WebProxyAccount	WebProxyAccount_001	312,313	312,313
☒	WebProxyPassword	WebProxyPassword_002	312,313	312,313

ФИГ. 10

РЕДАКТИРОВАТЬ
НАСТРОЙКИ

1102

1100

ВЫБОР	ID МАНДАТА	ID УПРАВЛЕНИЯ	ПРИЛОЖЕНИЕ С ВОЗМОЖ- НОСТЬЮ ОБ- НОВЛЕНИЯ МАНДАТА ПОЛЬ- ЗОВАТЕЛЯ	ПРИЛОЖЕНИЕ С ВОЗМОЖ- НОСТЬЮ ОБРА- ЩЕНИЯ К МАН- ДАТУ ПОЛЬЗО- ВАТЕЛЯ
☐	LoginAccount	LoginAccount_001	305	*
☐	LoginPassword	LoginPassword_001	305	*
☐	MailAccount	MailAccount_001	306,307	306,307
☐	MailPassword	MailPassword_001	306,307	306,307
☒	FileServerAccount	FileServerAccount_001	308,309	308,309
☐	FileServerAccount	FileServerAccount_002	308,310	308,310
☐	FileServerAccount	FileServerAccount_003	311	308,311
☐	FileServerPassword	FileServerPassword_001	308,309	308,309
☐	FileServerPassword	FileServerPassword_002	308,310	308,310
☐	FileServerPassword	FileServerPassword_003	311	308,311
☐	WebProxyAccount	WebProxyAccount_001	312,313	312,313
☐	WebProxyPassword	WebProxyPassword_002	312,313	312,313

1101

1110

ID МАНДАТА : FileServerAccount

ID УПРАВЛЕНИЯ : WebProxyAccount_001

ПРИЛОЖЕНИЕ С ВОЗМОЖНОСТЬЮ
ОБНОВЛЕНИЯ МАНДАТА ПОЛЬЗОВАТЕЛЯ

1103

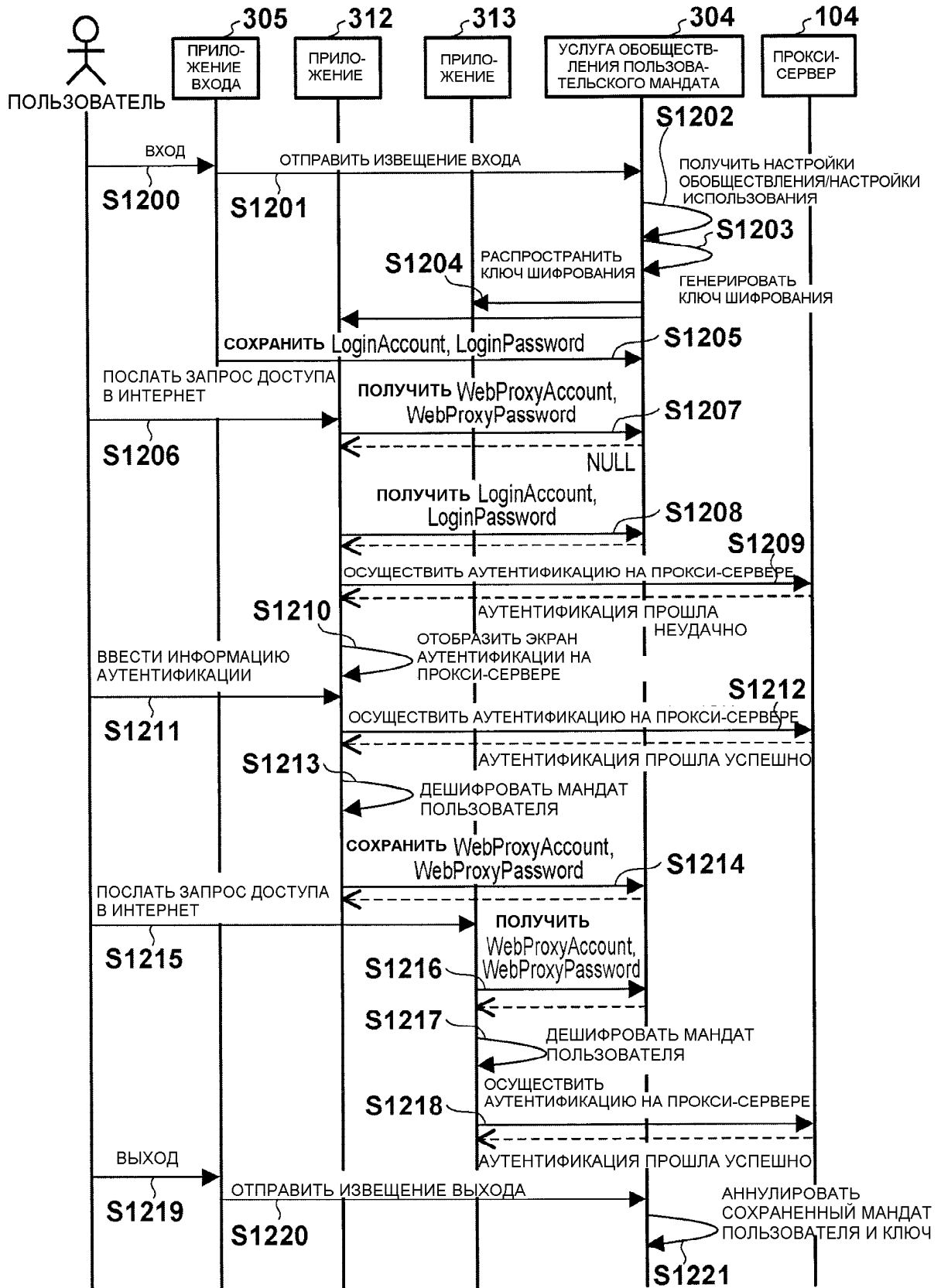
308	△	▶	310	△
309	▽	◀	311	▽

ПРИЛОЖЕНИЕ С ВОЗМОЖНОСТЬЮ ОБРАЩЕНИЯ
К МАНДАТУ ПОЛЬЗОВАТЕЛЯ

1104

308	△	▶	310	△
309	▽	◀	311	▽

ФИГ. 11



ФИГ. 12

ID УПРАВЛЕНИЯ	КЛЮЧ ШИФРОВАНИЯ	ЗНАЧЕНИЕ	ПРИЛОЖЕНИЕ ПОСЛЕДНЕГО ОБНОВЛЕНИЯ	ДАТА/ВРЕМЯ ОБНОВЛЕНИЯ
LoginAccount_001		Alice	305	2010/5/6 10:07
LoginPassword_001		Alicelogin	305	2010/5/6 10:07
WebProxyAccount_001	ENCRYPTION KEY001	ЗАШИФРОВАННЫЕ ДАННЫЕ	312	2010/5/6 10:09
WebProxyPassword_002	ENCRYPTION KEY002	ЗАШИФРОВАННЫЕ ДАННЫЕ	312	2010/5/6 10:09

ФИГ. 13