РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 369 025** (13) **C2**

(51) МПК
H04L 9/32 (2006.01)
G06F 21/20 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2004131027/09, 22.10.2004**

(24) Дата начала отсчета срока действия патента:
22.10.2004

(30) Конвенционный приоритет:
24.10.2003 US 10/693,585

(43) Дата публикации заявки: **10.04.2006**

(45) Опубликовано: **27.09.2009** Бюл. № **27**

(56) Список документов, цитированных в отчете о поиске: **US 5774551 A, 30.06.1998. RU 2158444 C2, 27.10.2000. US 5655077 A, 05.08.1997. US 2002112155, 15.08.2002.**

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
ХАЦ Бенджамин А. (US),
ИЛАС Кристьян (US),
ПЕРЛИН Эрик К. (US),
ФЛО Эрик Р. (US),
СТЕФЕНС Джон (US),
ШУТЦ Клаус У. (US),
РИЧАРДЗ Стефан (US),
РИЗОР Стерлинг М. (US)

(73) Патентообладатель(и):
МАЙКРОСОФТ КОРПОРЕЙШН (US)

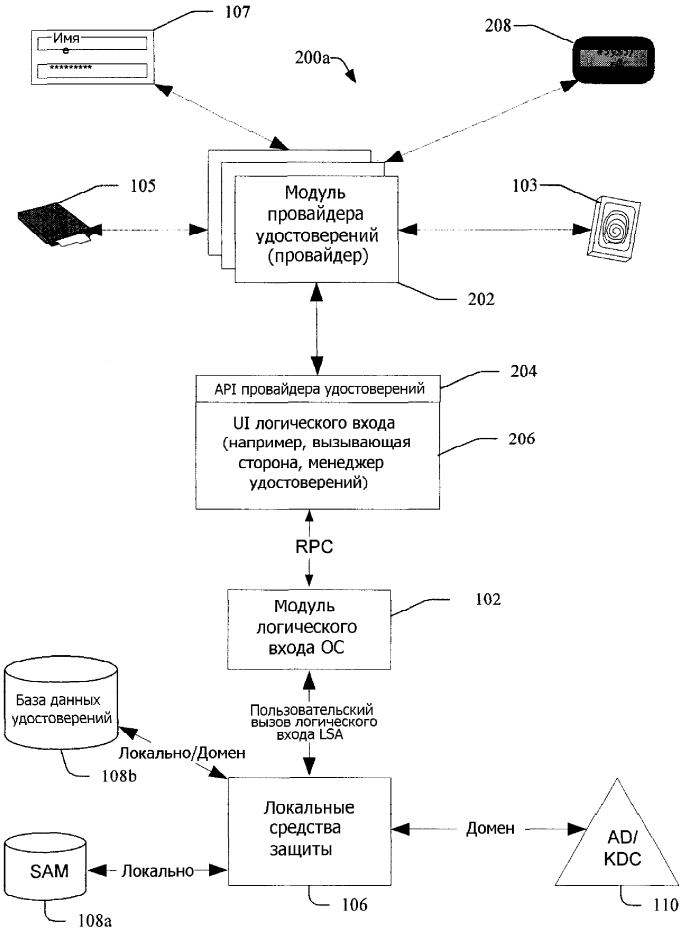
(54) ВЗАИМОДЕЙСТВУЮЩИЕ МОДУЛЬНЫЕ СРЕДСТВА СБОРА УДОСТОВЕРЕНИЙ И ДОСТУПА

(57) Реферат:

Изобретение относится к области машинного доступа, в частности к идентификации и аутентификации объекта, пользователя или принципала с удостоверением для логического входа в локальную и/или удаленную машину с операционной системой. Техническим результатом является возможность безопасного совместного использования множества взаимодействующих модулей, полностью совместимых с операционной системой локальной машины. Удостоверения преобразуют посредством одного из множества отличающихся модулей провайдеров удостоверений, каждый из которых преобразует соответствующий отличающийся тип удостоверений в общий протокол. Преобразованные удостоверения передают через интерфейс прикладного программирования (API) к модулю пользовательского интерфейса (UI) логического входа операционной системе (ОС) локальной машины, который вызывается модулем UI логического входа для аутентификации преобразованных удостоверений по базе данных удостоверений. Пользователь, идентифицированный преобразованным удостоверением, осуществляет логический вход для доступа к локальной машине в случае успешной аутентификации. 5 н. и 13 з.п. ф-лы, 14 ил.

RU 2369025 C2

RU 2369025 C2



Фиг. 2a

RU 2369025 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 369 025** (13) **C2**

(51) Int. Cl.
H04L 9/32 (2006.01)
G06F 21/20 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2004131027/09, 22.10.2004**

(24) Effective date for property rights:
22.10.2004

(30) Priority:
24.10.2003 US 10/693,585

(43) Application published: **10.04.2006**

(45) Date of publication: **27.09.2009 Bull. 27**

Mail address:
129090, Moskva, ul. B.Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
KhATs Bendzhamin A. (US),
ILAS Krist'jan (US),
PERLIN Ehrik K. (US),
FLO Ehrik R. (US),
STEFENS Dzhon (US),
ShUTTs Klaus U. (US),
RIChARDZ Stefan (US),
RIZOR Sterling M. (US)

(73) Proprietor(s):
MAJKROSOFT KORPOREJShN (US)

(54) INTERACTING MODULE FACILITIES FOR COLLECTION OF AUTHENTICATORS AND ACCESS

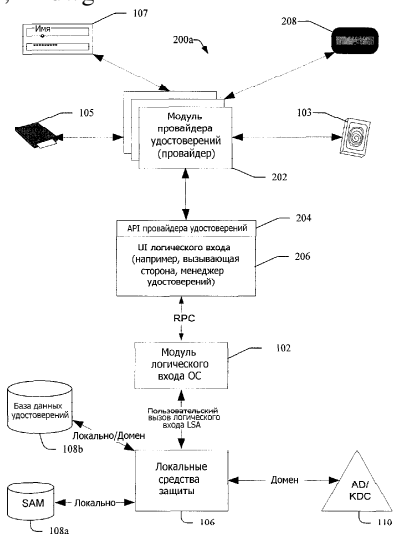
(57) Abstract:

FIELD: instrument making.

SUBSTANCE: invention is related to the field of machine access, in particular to identification and authentication of object, user or principal with authenticator for logical entry into local and/or remote machine with operating system. Authenticators are transformed by means of one of multiple different modules of authenticator provides, every of which transforms according different type of authenticators into common protocol. Transformed authenticators are sent through application programming interface (API) to user interface module (UI) of logical entry to operating system (OS) of local machine, which is called by UI module of logical entry for authentication of transformed authenticators according to database of authenticators. User identified with transformed authenticator realises a logical entry for access to local machine in case of successful authentication.

EFFECT: possibility of safe joint application of multiple interacting modules that are fully compatible with operating system of local machine.

18 cl, 22 dwg



Фиг. 2a

RU 2369025 C2

RU 2369025 C2

Область техники, к которой относится изобретение

Настоящее изобретение относится в общем к области машинного доступа, в частности к идентификации и аутентификации (установлению подлинности) объекта, пользователя или принципала (пользователя или процесса, имеющего учетную запись) с удостоверением для логического входа в локальную и/или удаленную машину, имеющую операционную систему.

Предшествующий уровень техники

На Фиг.1 показан иллюстративный традиционный процесс 100, позволяющий пользователю войти в систему инфраструктуры аутентификации операционной системы локальной машины. В данном случае термин «локальная машина» означает вычислительное устройство с операционной системой, такое как персональный компьютер, карманный компьютер, устройство «толстый» клиент, устройство «тонкий» клиент, персональное цифровое информационное устройство, экспертная система и т.д. Инфраструктура аутентификации производит аутентификацию пользователя с использованием удостоверения с целью предоставления доступа к вычислительному устройству посредством его операционной системы, такой как операционная система WINDOWS®, поставляемая корпорацией Майкрософт, Редмонд, Вирджиния, США. Аутентификация удостоверения здесь рассматривается как эквивалентная аутентификации пользователя, объекта или принципала с соответствующим удостоверением, причем эти понятия и концепции используются здесь как взаимозаменяемые.

На этапе 102 процесса 100 операционная система выполняет программу логического входа. Программа логического входа может передать управление только одному из трех (3) различных модулей аутентификации. Иными словами, локальная машина может иметь только один модуль аутентификации, с помощью которого может быть произведена аутентификация. В случае операционной системы (ОС) WINDOWS® модулем аутентификации по умолчанию является Графический модуль идентификации и аутентификации, обозначаемый здесь как 'GINA'. Модуль GINA в составе ОС WINDOWS® представляет собой динамически подключаемую библиотеку (*.dll), реализующую пользовательский интерфейс логического входа на дисплее в виде экрана с диалоговым окном логического входа, куда пользователь вводит имя пользователя и пароль. Модуль GINA осуществляет аутентификацию пользователя в операционной системе вычислительного устройства посредством использования удостоверений, предъявляемых пользователем. Удостоверения пользователя представлены набором информации, включающим в себя идентификацию и подтверждение идентификации, которые используются для получения доступа к локальным и сетевым ресурсам.

Примерами удостоверений являются имя пользователя и пароль, смарт-карты, биометрические удостоверения, цифровые сертификаты X.509 и другие виды сертификатов. Модуль GINA 104, показанный на Фиг.1, является стандартным модулем ОС WINDOWS® и требует традиционного интерактивного процесса логического входа, такого как предложение пользователю ввести имя пользователя и пароль в пользовательском интерфейсе 103. После выполнения GINA 104 управление передается модулю 106 локальных средств защиты безопасности (LSA). Модуль 106 LSA обращается к локальной базе данных менеджера (средства управления) 108a учетных записей системы безопасности (SAM), каждая из которых представляет собой локальное хранилище информации логического входа и безопасности для данного вычислительного устройства и/или релевантного окружения. База 108b данных

удостоверений, которая может быть локальной или удаленной, может хранить такие удостоверения, как отпечатки пальцев, пароли, информацию о сетчатке глаза, информацию распознавания лиц и другую биометрическую информацию, которая может быть использована для аутентификации пользователя в соответствии с конкретным GINA. Модуль 106 LSA может также установить соединение для доступа к удаленной базе данных удостоверений, к службе удостоверений с маркерным протоколом, к службе удостоверений с протоколом запроса-ответа, и/или к Активному каталогу (AD) и центру 110 распределения ключей Kerberos (KDC). Kerberos представляет собой сетевой протокол аутентификации для идентификации пользователей, пытающихся осуществить логический вход в сеть, и для шифрования выполняемого ими обмена данными посредством криптографии с секретным ключом. Модуль AD использует технологию, позволяющую приложениям находить, использовать и управлять ресурсами каталогов (например, именами пользователей и полномочиями) в распределенной вычислительной среде. С помощью таких видов доступа производится идентификация и аутентификация пользователя согласно пользовательским удостоверениям с целью определения привилегий доступа пользователя в отношении логического входа в вычислительное устройство посредством операционной системы. При успешной идентификации и аутентификации пользователю будет разрешен логический вход, и управление будет возвращено модулю 102 логического входа ОС. После этого пользователь считается осуществившим логический вход и может начать использование вычислительного устройства.

Модуль 112 GINA опосредованной аутентификации первого типа, показанный на Фиг.1, является сторонним модулем идентификации и аутентификации, который может быть написан независимым производителем программного обеспечения, не разрабатывавшим операционную систему. Модуль 112 GINA опосредованной аутентификации первого типа взаимодействует с устройством 105 чтения смарт-карт, а также с используемым по умолчанию базовым модулем 114 GINA операционной системы. Модуль 112 GINA опосредованной аутентификации первого типа принимает удостоверения, считываемые устройством 105 чтения смарт-карт со вставленной в него смарт-карты. Сертификат, считываемый со вставленной в устройство 105 чтения смарт-карт смарт-карты, а также любые другие удостоверения, полученные от пользователя, могут быть использованы для идентификации и аутентификации пользователя по базе 108b данных удостоверений. В таком случае модуль 112 GINA опосредованной аутентификации первого типа позволяет вносить ограниченные изменения в процесс идентификации и аутентификации пользователя при поддержке процедуры идентификации и аутентификации, используемой по умолчанию, согласно интерфейсу базового модуля 114 GINA операционной системы.

Модуль 116 GINA опосредованной аутентификации второго типа представляет собой полную замену стандартного модуля 104 GINA операционной системы. Модуль 116 GINA опосредованной аутентификации второго типа взаимодействует с устройством 107 чтения отпечатков пальцев. Модуль 116 GINA опосредованной аутентификации второго типа получает удостоверения, считываемые устройством 107 считывания отпечатков пальцев, из оптически сканированного изображения пальцев. Оптически сканированное изображение пальцев, вставленных в устройство 107 считывания отпечатков пальцев, а также любые другие удостоверения, полученные от пользователя, могут быть использованы для идентификации и аутентификации пользователя по базе 108b данных удостоверений. Модуль 116 GINA опосредованной

аутентификации второго типа является сторонним модулем идентификации и аутентификации, который не взаимодействует со стандартным модулем GINA ОС, а напрямую взаимодействует с LSA 106. В отличие от модуля 112 GINA опосредованной аутентификации первого типа, модуль 116 GINA опосредованной аутентификации второго типа допускает полное управление пользовательским интерфейсом, который пользователь видит при логическом входе. Типичной проблемой, как указывалось выше, является то, что только один из модулей GINA 104, модуль 112 GINA опосредованной аутентификации первого типа или модуль 116 GINA опосредованной аутентификации второго типа, может использоваться с операционной системой. Иными словами, никакой сторонний или стандартный модуль GINA не может сосуществовать с другим сторонним модулем GINA, посредством которого ОС могла бы предоставить пользователю доступ к вычислительному устройству или вычислительной среде.

В дополнение к изложенному могут возникнуть другие ограничения в использовании сторонних модулей GINA, например, применение любого нового механизма сбора удостоверений или изменение существующего (например, для биометрических данных, смарт-карт, маркеров и т.д.) для доступа к операционной системе вычислительного устройства. В этом случае сторонний модуль GINA накладывает на разработчика значительное бремя в части кодирования. Для применения нового или измененного механизма сбора удостоверений разработчик должен написать новую модель аутентификации для аутентификации пользователя, желающего получить доступ к вычислительному устройству. В случае ОС WINDOWS® разработчик должен написать полностью пересмотренный сторонний модуль GINA, включающий в себя сложные коды интерфейса и управления состояниями, чтобы сторонний модуль GINA мог взаимодействовать напрямую с системными компонентами ОС. Ненадлежащее кодирование стороннего модуля GINA может подорвать надежность ОС.

Замена стороннего или стандартного модуля GINA весьма чувствительна в том смысле, что это один из важнейших компонентов безопасности ОС. Некачественный модуль GINA может значительно ослабить надежность ОС и снизить ее функциональность. Сложность разработки заменяющего или стороннего модуля GINA может также потребовать от разработчика получения базовых исходных кодов стандартного модуля GINA ОС. Более того, инсталляция стороннего модуля GINA означает замену стандартного модуля GINA, так как два способа сбора удостоверений (например, GINA) не могут сосуществовать в одном компьютерном устройстве. Это не позволяет независимым разработчикам программного обеспечения разрабатывать решения, применяемые повсеместно и позволяющие пользователям осуществлять логический вход посредством более чем одной инфраструктуры аутентификации. В данной области техники большие преимущества предоставило бы решение способа логического входа, позволяющее пользователям осуществлять логический вход посредством различных, совместно существующих инфраструктур аутентификации, таких как выбираемый сетевой сеанс, где были бы преодолены сформулированные выше проблемы.

Сущность изобретения

В различных вариантах осуществления удостоверения транслируются посредством одного из множества различных и сосуществующих модулей провайдера (поставщика) удостоверений. Каждый модуль преобразует соответствующий отличающийся тип удостоверений в общий протокол удостоверений. Транслированные удостоверения

передаются посредством интерфейса прикладного программирования (API) провайдера удостоверений модулю пользовательского интерфейса (UI) логического входа собственной операционной системы (ОС) локальной машины. Для аутентификации пользователя согласно преобразованным удостоверениям по базе данных удостоверений вызывается стандартная процедура логического входа ОС. В случае успешной аутентификации пользователь, идентифицированный посредством преобразованных удостоверений, осуществляет логический вход и получает доступ к локальной машине.

В других вариантах осуществления модулем UI логического входа ОС осуществляется запрос через API менеджера провайдеров предварительного доступа (PLAP). Запрашивается одноуровневый список служб доступа соответствующего множества совместно существующих отличающихся модулей PLAP. Одноуровневый список служб доступа отображается модулем UI логического входа на экране. Принимаются введенное удостоверение и выбор одной из служб доступа, отображенных в одноуровневом списке на экране. При установлении соединения с сетью с использованием выбранной службы доступа удостоверения передаются в базу данных удостоверений службы доступа для первичной аутентификации. В случае успешной первичной аутентификации удостоверения передаются из API PLAP модулю UI логического входа. Модуль UI логического входа осуществляет вызов RPC (вызов удаленной процедуры) для передачи удостоверений модулю логического входа ОС. Далее удостоверения передаются с модуля логического входа ОС посредством пользовательского вызова логического входа LSA на LSA. LSA производит вторичную аутентификацию пользователя по базе данных удостоверений. В случае успешной вторичной аутентификации пользователь, идентифицированный удостоверениями, успешно осуществляет логический вход для использования локальной машины посредством ОС.

Перечень фигур чертежей

Более полное понимание вариантов осуществления может быть достигнуто с помощью последующего детального описания в сочетании с прилагаемыми фигурами чертежей, где:

Фиг.1 - блок-схема последовательности операций, поясняющая традиционный процесс, при котором пользователь осуществляет логический вход в локальную машину посредством предоставления удостоврений для идентификации и аутентификации.

Фиг.2a-2b - блок-схемы последовательности операций, поясняющие соответствующие варианты осуществления процесса идентификации и аутентификации пользователя посредством предоставленных пользователем удостоверений с целью осуществления пользователем логического входа в локальную машину для множества стандартных или сторонних альтернативных провайдеров удостоверений, где пользователь может в необязательном порядке выбрать один из нескольких модулей провайдера удостоверений, и где каждый модуль провайдера удостоверений взаимодействует с операционной системой таким образом, чтобы предоставлять удостоверения, совместимые с механизмом аутентификации данной операционной системы.

Фиг.3 - блок-схема последовательности операций, поясняющая вариант осуществления процесса идентификации и аутентификации пользователя по удостоверениям, представленным пользователем с целью логического входа в локальную машину в домене системы аутентификации нижнего уровня, для

провайдера удостоверений аутентификации нижнего уровня, где орган аутентификации нижнего уровня возвращает удостоверения логического входа провайдеру удостоверений аутентификации нижнего уровня, и где провайдер удостоверений аутентификации нижнего уровня предоставляет удостоверения, совместимые с механизмом аутентификации данной операционной системы.

Фиг.4 - блок-схема последовательности операций, поясняющая иллюстративный вариант осуществления процесса, при котором каждый из множества различных сосуществующих провайдеров удостоверений может собирать удостоверения пользователя по запросу приложения на локальной машине, и где удостоверения могут быть отправлены в домен, такой как Web-сайт Интернет, в котором пользователь может быть аутентифицирован посредством этих удостоверений и сможет использовать локальную машину для доступа к этому домену.

Фиг.5a - экранное окно, где пользователь вводит удостоверения в виде имени пользователя и пароля, по которым провайдер удостоверений произведет идентификацию и аутентификацию.

Фиг.5b - экранное окно, отображающее множество имен пользователей, связанных с общим псевдонимом или префиксом имени пользователя, причем эти имена пользователей автоматически отображаются по запросу соответствующей базы данных имен пользователей.

Фиг.5c - экран логического входа, позволяющий пользователю выбрать опцию, которая, будучи выбранной, отобразит на экране выбор типов учетных записей и выбор типов соединений для входа в систему.

Фиг.6a - экран логического входа, позволяющий пользователю выбрать тип учетной записи и тип соединения для входа в систему из списков в соответствующих ниспадающих меню.

Фиг.6b - экран логического входа, отображаемый после выбора пользователем типа учетной записи Novell, где экранная подсказка для ввода удостоверений выполнена в пользовательском интерфейсе Novell.

Фиг.7a - экран логического входа, отображающий две (2) учетные записи, которые на текущий момент осуществили логический вход в локальную машину.

Фиг.7b - экран логического входа, отображающий пользовательскую учетную запись с приглашением ввода Персонального идентификационного номера (PIN) в качестве удостоверения для идентификации и аутентификации с целью осуществления логического входа в локальную машину.

Фиг.8a - экран логического входа, отображающий две (2) учетные записи, которые на текущий момент осуществили логический вход в локальную машину, и третью учетную запись, соответствующую сертификату смарт-карты, считываемому локальной машиной, которая отображает экран логического входа.

Фиг.8b - экран логического входа, отображающий две (2) учетные записи, для первой из которых отображено приглашение на ввод PIN для проверки соответствия как удостоверения сертификату смарт-карты, считываемому локальной машиной, которая отображает экран логического входа.

Фиг.9a - экран логического входа, отображающий четыре (4) учетные записи на локальной машине, которые могут аутентифицировать пользователя с использованием удостоверений, считываемых устройством чтения биометрических параметров.

Фиг.9b - экран логического входа, отображающий четыре (4) учетные записи, подтвержденные на локальной машине, где экран логического входа чувствителен к

нажатию для считывания изображения отпечатков пальцев в качестве удостоверений, по которым локальная машина может провести аутентификацию пользователя, используя удостоверения совместно с соответствующим провайдером удостоверений, где удостоверения, включающие в себя отпечатки пальцев, преобразуются провайдером удостоверений в удостоверения, совместимые с механизмом аутентификации операционной системы данной локальной машины.

Фиг.9c - экран логического входа, отображающий одну (1) учетную запись, для которой соответствующий пользователь прошел процедуру аутентификации с целью получения доступа к локальной машине с использованием удостоверения, включающего в себя отпечатки пальцев пользователя.

Фиг.10 - экран логического входа, где пользователь может сделать выбор одного из множества типов соединения для логического входа и соответствующих служб доступа, которые будут использоваться для установления сеанса сетевого соединения с использованием удостоверений, предоставляемых посредством ввода на экране логического входа.

Фиг.11 - блок-схема последовательности операций иллюстративного варианта осуществления процесса использования экрана логического входа, на котором пользователь может сделать выбор одного из множества типов соединений для логического входа и соответствующих служб доступа, которые будут использоваться для установления сеанса сетевого соединения с использованием удостоверений, предоставляемых посредством ввода на экране логического входа в систему.

Фиг.12 - экран логического входа для получения удостоверений от пользователя, в котором пользователь может сделать выбор одного из множества типов соединений для логического входа и соответствующих служб доступа, а также выбор одного из множества провайдеров удостоверений, где любой выбор пользователя может быть использован для его идентификации и аутентификации посредством пользовательских удостоверений, чтобы пользователь мог осуществить логический вход для использования локальной машины, которая отображает экран логического входа в систему.

Фиг.13 - блок-схема последовательности операций иллюстративного варианта осуществления процесса использования экрана логического входа для получения удостоверений от пользователя, где пользователь может сделать выбор одного из множества типов предварительного доступа, а также выбор одного из множества провайдеров удостоверений, при этом любой выбор пользователя может быть использован для его идентификации и аутентификации посредством пользовательских удостоверений, чтобы пользователь мог осуществить логический вход посредством выбранной службы доступа для дальнейшего использования локальной машины, которая отображает экран логического входа в систему.

Фиг.14 - пример вычислительной среды, в которой могут быть полностью или частично реализованы описанные здесь программные приложения, способы и системы.

Для обозначения аналогичных компонентов и элементов в описании и прилагаемых фигурах чертежей используются одинаковые номера. Номера серии 100 относятся к элементам, исходно указанным на Фиг.1, номера серии 200 относятся к элементам, исходно указанным на Фиг.2, номера серии 300 относятся к элементам, исходно указанным на Фиг.3 и т.д.

Детальное описание

Различные варианты осуществления предполагают сосуществующие модули, взаимодействующие с операционной системой вычислительного устройства, причем

каждый модуль может осуществлять аутентификацию принципала, объекта или пользователя с помощью набора информации (например, удостоверений), содержащего идентификацию и подтверждение идентификации, используемые для получения доступа к локальным и сетевым ресурсам посредством операционной системы. Более того, в результате установления стабильного интерфейса между модулями и операционной системой изменения, касающиеся только одного из модулей и операционной системы, не влияют на процессы идентификации и аутентификации, производимые другими модулями.

Фиг.2а показывает блок-схему последовательности операций, демонстрирующую иллюстративный процесс 200а идентификации и аутентификации пользователей с целью логического входа и получения доступа к локальным и сетевым ресурсам через операционную систему локальной машины. Множество модулей 202 провайдеров удостоверений предоставлено различными независимыми поставщиками программного обеспечения, любой из которых может быть использован локальной машиной для идентификации и аутентификации пользователей. По существу, модули 202 провайдеров удостоверений представляют собой совместно существующие интерфейсы операционной системы, посредством которых пользователь может осуществить логический вход в локальную машину с помощью ее операционной системы.

Каждый модуль 202 провайдера удостоверений использует отдельный процесс идентификации и аутентификации. Один модуль 202 провайдера удостоверений использует пользовательский интерфейс (UI) 107, принимающий в качестве удостоверений имя пользователя и пароль. Другой модуль 202 провайдера удостоверений использует маркер 208. В качестве примера, маркер 208 может быть физическим устройством. Физическое устройство хранит номер, считываемый устройством чтения при попытке пользователя осуществить логический вход в вычислительное устройство. После каждого логического входа, либо с периодическими интервалами с помощью основывающегося на времени алгоритма, номер, хранимый в маркере 208, меняется. Новый номер может быть сохранен также в вычислительном устройстве для будущих аутентификаций. Пользователь может также получить приглашение на ввод Персонального идентификационного номера (PIN) в дополнение к считыванию маркера 208 устройством чтения. Устройство 103 чтения отпечатков пальцев и/или устройство 105 чтения смарт-карт могут использоваться другими модулями 202 провайдеров удостоверений для, соответственно, считывания в качестве удостоверений отпечатков пальцев пользователя, полученных устройством 103 считывания отпечатков пальцев, или считывания удотоверений со смарт-карты, вставленной в устройство 105 чтения смарт-карт. Конечно же, другие устройства считывания удостоверений могут использоваться для предоставления удостоверений другим модулям 202 провайдеров удостоверений, такие как модуль сканирования сетчатки глаза, модуль камеры распознавания лица, модуль камеры распознавания походки, модуль распознавания почерка, модуль распознавания голоса, модуль распознавания запаха, модуль распознавания генетического кода и другие подобные биометрические модули.

При использовании совместно существующих модулей 202 провайдеров удостоверений возможны различные альтернативные решения. В частности, локальная машина может требовать от всех или от отдельных пользователей аутентификации несколькими способами. В качестве примера таких требований на аутентификацию множеством способов от пользователя могут потребовать

аутентификации для получения доступа к локальной машине посредством двух различных смарт-карт. В качестве другого примера, пользователь может быть поставлен перед выбором, какой из множества способов использовать для логического входа в локальную машину. В частности, для логического входа в локальную машину пользователь может выбирать между вводом пароля или использованием датчика отпечатков пальцев.

Каждый модуль 202 провайдера удостоверений может принимать и преобразовывать удостоверения в общий протокол удостоверений. Протокол удостоверений обеспечивает совместимость преобразованных удостоверений с компонентом аутентификации собственной операционной системы локальной машины. Аутентификация преобразованных удостоверений осуществляется по базе данных удостоверений. В случае успешной аутентификации пользователю, идентифицированному посредством удостоверения, разрешается логический вход в собственную операционную систему для доступа к локальной машине.

Каждый модуль 202 провайдера удостоверений взаимодействует с интерфейсом 204 прикладного программирования (API) провайдера удостоверений для обработки обмена данными с системой аутентификации. API 204 провайдера удостоверений взаимодействует с вызывающей стороной, которой может служить Пользовательский интерфейс 206 (UI) логического входа. UI 206 логического входа может быть менеджером удостоверений, получающим и обслуживающим удостоверения пользователя. UI 206 логического входа использует Процедуру удаленного вызова (RPC) модуля 102 логического входа операционной системы (ОС). Модуль 102 логического входа ОС является интерфейсом к ОС вычислительного устройства. Модуль 102 логического входа ОС осуществляет пользовательский вызов логического входа локальных средств защиты (LSA) в модуль 106 локальных средств защиты (LSA). Как описывалось выше со ссылкой на Фиг.1, модуль 106 LSA осуществляет доступ к локальной базе 108a данных менеджера учетных записей системы безопасности (SAM) для типичной идентификации и аутентификации имени пользователя и пароля. Модуль 106 LSA может также осуществить доступ к локально хранимой базе данных 108b удостоверений для идентификации и аутентификации принципала, элемента или пользователя посредством удостоверений, собранных устройством чтения, аналогичным одному из устройств 103-107 и 208 чтения удостоверений.

Преобразованные удостоверения передаются через API 204 провайдера удостоверений на UI 206 логического входа и далее модулю 102 логического входа ОС для локальной аутентификации посредством модуля 106 LSA с целью осуществления пользователем логического входа в локальную машину. В альтернативном случае модуль 106 LSA может осуществить удаленный доступ за пределы локальной машины посредством соединения, устанавливаемого с доменом. В домене можно получить доступ к хранимым там Активному каталогу (AD) и центру распределения ключей Kerberos (KDC) 110. Посредством такого доступа производятся идентификация и аутентификация пользователя по преобразованным удостоверениям, и определяются привилегии доступа пользователя для логического входа в локальную машину через ОС. Успешная идентификация и аутентификация позволяют пользователю осуществить логический вход. Пользователь, осуществивший логический вход через ОС, может начать использование локальной машины.

Общий иллюстративный процесс 200b логического входа показан на Фиг.2b и будет описан со ссылками на Фиг.2a. Процесс 200b логического входа начинается с этапа

212, где операционная система (ОС) локальной машины загружает Пользовательский интерфейс (UI) 206 логического входа. На этапе 214 UI 206 логического входа загружает и инициализирует всех зарегистрированных провайдеров 202 удостоверений с использованием API 204 провайдеров удостоверений.

На этапе 216 модуль 102 логического входа ОС передает UI 206 логического входа команду отобразить экран приветствия UI, который пользователь может видеть и взаимодействовать. На этапе 218 пользователь вводит последовательность клавиш control-alt-delete (CAD). При вводе пользователем последовательности CAD, либо другой последовательности клавиш, которая также является Последовательностью обращения к системе безопасности (SAS), генерируется аппаратное событие, которое может быть перехвачено только ОС. Это действие пользователя заставляет модуль 102 логического входа ОС уведомить UI 206 логического входа на этапе 220 о готовности к приему удостоверений логического входа. На этапе 222 UI 206 логического входа демонстрирует UI для логического входа, как предписывает модуль 202 провайдера удостоверений, используемый по умолчанию. UI 206 логического входа запрашивает модули 202 провайдеров удостоверений о предоставлении одноуровневого списка всех провайдеров удостоверений для его отображения. На этапе 224 UI 206 логического входа принимает входные данные, сообщающие о выборе пользователем одного из множества отображенных провайдеров удостоверений, каждый из которых соответствует одному из модулей 202 провайдеров удостоверений. Эти входные данные инициируют взаимодействие между пользовательским вводом и одной или более внешними системами через API 204 провайдеров удостоверений. Конкретный модуль 202 провайдера удостоверений может зависеть от типа события, инициируемого пользователем для предоставления ОС удостоверений (например, посредством использования пользователем одного из устройств чтения 103-107 и 208 удостоверений). На этапе 226 UI 206 логического входа возвращает полученные удостоверения модулю 102 логического входа ОС посредством RPC. На этапе 228 модуль 102 логического входа ОС производит пользовательский вызов логического входа LSA в LSA 106 для осуществления логического входа пользователя. На этапе 230 модуль 102 логического входа ОС производит RPC в отношении UI 206 логического входа для сообщения результатов процесса 200b логического входа. На этапе 232 UI 206 логического входа вызывает конкретный модуль провайдера 202 удостоверений через API 204 провайдеров удостоверений для сообщения результатов процесса 200b логического входа. После этого управление возвращается модулю 102 логического входа ОС. На этапе 234 модуль 102 логического входа ОС завершает установление сеанса пользователя, и пользователь осуществляет логический вход в компьютерное устройство.

Процесс 300, показанный на Фиг.3 и отображенный в виде блок-схемы последовательности операций, демонстрирует этапы, посредством которых локальная машина 300a может использовать процесс аутентификации нижнего уровня в домене 300b для аутентификации пользователя по его удостоверениям. Провайдер 302 удостоверений аутентификации нижнего уровня на локальной машине 300a взаимодействует с системой 304 аутентификации нижнего уровня в домене 300b. Домен 300b, в частности, может быть сторонним сервером. Провайдер 302 удостоверений аутентификации нижнего уровня взаимодействует с API 204 провайдеров удостоверений описанным выше способом в соответствии с Фиг.2. По существу, процесс 300 аналогичен процессу 200a в части блоков 206, 102 и 106. В

процессе 300 AD/KDC 110 взаимодействуют с LSA 106. Система 304 аутентификации нижнего уровня в домене 300b использует протокол аутентификации нижнего уровня для возвращения удостоверений логического входа провайдеру 302 удостоверений аутентификации нижнего уровня.

Процесс 300 использует процесс предварительной аутентификации, при котором пользовательские удостоверения используются для аутентификации пользователя согласно стороннему способу аутентификации вместо такового на локальной машине. По окончании аутентификации сторонний способ возвращает удостоверения, совместимые с ОС, чтобы обеспечить логический вход пользователя в локальную машину 300a через ее ОС. На практике провайдер 302 удостоверений аутентификации нижнего уровня взаимодействует через API 204 провайдеров удостоверений с UI 206 логического входа, показанный на Фиг.3. Когда пользователь вводит удостоверения, эти удостоверения отправляются с локальной машины 300a на AD/KDC 110 в домене 300b, который может являться для локальной машины 300a сетевым сервером. AD/KDC 110 во взаимодействии с системой 304 аутентификации нижнего уровня в домене 300b производит аутентификацию пользователя по его удостоверениям. Система 304 аутентификации нижнего уровня возвращает удостоверения логического входа провайдеру 302 аутентификации нижнего уровня. Провайдер 302 аутентификации нижнего уровня возвращает удостоверения UI 206 логического входа через API 204 провайдеров удостоверений. После этого UI 206 логического входа может передать удостоверения модулю 102 логического входа ОС посредством RPC. Соответственно, ОС локальной машины 300a изолирована от сторонней системы 304 аутентификации нижнего уровня в домене 300b.

Фиг.4 содержит блок-схему последовательности операций, изображающую иллюстративный процесс 400, посредством которого принципал, элемент или пользователь может быть аутентифицирован по дополнительным удостоверениям для получения доступа к домену, такому как Web-сайт, и в котором принимают участие запросчик удостоверений и аутентификатор 406 (средство аутентификации) Web-сайта. По существу, после того, как принципал, элемент или пользователь осуществил логический вход в локальную машину, принципал, элемент или пользователь проходит процедуру удаленной аутентификации посредством запросчика удостоверений и аутентификатора 406 Web-сайта, обрабатывающих дополнительные удостоверения. Пользовательский интерфейс (UI) 402 удостоверений запрашивает дополнительные удостоверения посредством приложения 404, выполняемого на локальной машине. Локальная машина содержит ОС, в которую пользователь осуществил логический вход как активный. Локальная машина находится на связи с устройством ввода (например, 103, 105, 107 или 208), посредством которого могут быть получены дополнительные удостоверения. Один из множества различных совместно существующих модулей 202 провайдеров удостоверений используется для сбора дополнительных удостоверений пользователя с устройства ввода (например, 103, 105, 107 или 208). Как только дополнительные удостоверения собраны, они передаются приложению 404 для аутентификации. Приложение 404 является локальным приложением, исполняемым на локальной машине, которое может запрашивать и получать дополнительные удостоверения. Каждый из модулей 202 провайдеров удостоверений может собирать различные типы удостоверений, таких как дополнительные удостоверения, с одного из устройств ввода (103, 105, 107, 208), и каждый модуль 202 провайдера удостоверений взаимодействует через API 204 провайдеров удостоверений с ОС локальной машины. API 204 провайдеров

удостоверений получает удостоверения, собранные одним из модулей 202 провайдеров удостоверений, причем каждый модуль 202 провайдера удостоверений может предоставлять соответствующий тип собираемых им удостоверений API 204 провайдеров удостоверений для аутентификации принципала, такого как пользователь, с целью осуществления логического входа принципала в ОС для доступа к локальной машине.

Иллюстративные изображения экрана дисплея, демонстрирующие различные варианты осуществления, которые предоставляют различные варианты логического входа, показаны на Фиг.5a-10 и 12. Один вариант осуществления использует имя пользователя и пароль для ввода в модуль провайдера удостоверений, что может быть способом по умолчанию для ввода пользователем удостоверений в экране логического входа. Другой вариант осуществления использует смарт-карту Инфраструктуры открытого ключа (PKI) для ввода удостоверений во взаимодействии с модулем провайдера удостоверений смарт-карт. Еще один вариант осуществления использует модуль провайдера удостоверений с удостоверением в виде отпечатков пальцев, при этом провайдер удостоверений проводит идентификацию и аутентификацию пользователя по его отпечаткам пальцев, полученным путем сканирования.

Обсуждаемые ниже варианты осуществления включают в себя провайдеров удостоверений, которые либо выбираются пользователем, либо управляются событиями, в зависимости от того, каким образом пользователь выбирает модуль провайдера удостоверений для использования. Выбираемый пользователем провайдер удостоверений выбирается пользователем из двух или более провайдеров удостоверений, предлагаемых пользователю пользовательским интерфейсом (UI). Фиг.5a показывает пример экрана по умолчанию, отображаемого согласно конфигурации ОС, в которой UI содержит только одного выбираемого пользователем провайдера удостоверений, в этом случае UI может предложить только ввод имени пользователя (username) и пароля (password). В случае по Фиг.5a никаких дополнительных выбираемых пользователем провайдеров удостоверений на вычислительном устройстве с данной ОС не установлено.

Как показано на Фиг.5b, псевдоним или имя пользователя может быть общим для одного или более адресов электронной почты (e-mail) или имен пользователя. По сути, провайдер удостоверений должен быть гибким в части использования Универсального имени принципала (UPN), как это показано. UPN представляет собой имя в стиле Интернет для входа пользователя в систему, основывающееся на стандарте Интернет RFC 822. По соглашению, оно должно отображаться в имя пользователя в системе электронной почты. UPN объединяет пространства адресов e-mail и имен пользователей, так что пользователь должен помнить единственное имя. По сути, UI на Фиг.5b поддерживает стиль имен UPN, где функция автозаполнения обеспечивает многие символы в UPN, которые пользователю не требуется вводить с клавиатуры. Для этого центр каталогов (DC) может получить запрос и вернуть список имен UPN в UI на Фиг.5b для отображения. Соответственно, UI логического входа использует UPN в качестве имени пользователя как части удостоверений, предоставляемых модулю провайдера удостоверений. Кроме того, UI логического входа может использоваться для отображения нумерованного списка пользователей, входящих в рабочую группу, или для отображения всех учетных записей локальной машины на экране логического входа. UI логического входа может также использоваться для отображения нумерованного списка пользователей, входящих в

домен, например, при этом UI отображает пиктограммы или изображения для каждого пользователя, уже осуществившего логический вход. UI может отображать одну (1) пиктограмму или изображение для пользователя, который еще не осуществил логический вход в домен.

При установке на локальной машине провайдера удостоверений для нового пользователя локальная машина может быть сконфигурирована для отображения ссылки 504 options (опции), показанной на Фиг.5c ниже поля ввода пароля. Пользователю, выбравшему ссылку 504 options, будет показан список провайдеров удостоверений, из которых пользователь может сделать выбор. В альтернативном варианте администратор сети или другой специалист в области информационных технологий может сконфигурировать на локальной машине политику выбора определенного провайдера удостоверений по умолчанию, так что пользователю локальной машины не нужно будет выбирать требуемого провайдера удостоверений. Как показано на Фиг.6a, отображается список 602 типов учетных записей, соответствующих различным провайдерам удостоверений UI экрана 600a. Список 602 позволяет пользователю выбрать тип учетной записи, которую пользователь хочет использовать для логического входа в ОС, тогда как поле 604 типа соединения для логического входа позволяет пользователю выбрать стандартный или специализированный тип логического входа на основе Службы удаленного доступа (RAS), например, соединение специализированной Виртуальной частной сети (VPN) или специализированную программу дозвона для соединения по телефонной линии. Посредством создания секции расширенных опций по ссылке 504 options по Фиг.5c в процесс логического входа пользователя вносится дополнительная расширенная функциональность без ущерба эстетичности и чрезмерного усложнения процедуры логического входа.

Провайдер удостоверений может обеспечивать дополнительную функциональность в процесс логического входа, что демонстрирует UI на экране 600a. Для получения экрана 600b по Фиг.6b, пользователь выбирает опцию "Novell" из списка 602 по Фиг.6a, что приводит к отображению UI кнопки 606 Advanced Novell Options (Усовершенствованные опции Novell). Когда пользователь нажимает кнопку 606 Novell Options, может быть отображен UI 608 логического входа клиента Novell, как показано на Фиг.6b. Эта функция позволяет пользователю просмотреть список серверов Novell в сети, с которой связана локальная машина пользователя, до логического входа в сеть. В этом случае провайдер удостоверений Novell может также обеспечивать поддержку добавочных скриптов (сценариев) входа в систему.

Модуль 402 провайдера удостоверений аутентификации нижнего уровня, показанный на Фиг.4, может быть настроен таким образом, что пользовательский интерфейс будет отображать только фирменную символику, логотипы, торговые или сервисные марки только одного стороннего производителя. В одном из вариантов осуществления пользователь может выбирать тип учетной записи из списка 602, что активирует модуль 402 провайдера удостоверений аутентификации нижнего уровня. Модуль 402 провайдера удостоверений аутентификации нижнего уровня может далее управлять UI для предоставления пользователю характерного для определенной торговой марки варианта логического входа, полностью совместимого с процессом логического входа для ОС. Более того, локальная машина может содержать множество модулей 402 провайдеров удостоверений аутентификации нижнего уровня, каждый из которых может предоставлять пользователю разные и различимые варианты логического входа, тем не менее полностью совместимые с процессом

логического входа для ОС локальной машины. В качестве примера, персональный компьютер может использоваться как уличный киоск для покупок через Интернет. Киоск может быть подключен к сети Интернет и отображать множество пиктограмм, каждая из которых может соответствовать модулю 402 провайдера удостоверений аутентификации нижнего уровня. Когда пользователь выбирает одну из отображаемых пиктограмм, представляющих торговую марку, соответствующий модуль 402 провайдера удостоверений аутентификации нижнего уровня предоставляет отличающийся вариант логического входа, уникальный для данной торговой марки, после чего пользователь осуществляет логический вход через ОС в локальную машину и на Web-сайт Интернет, соответствующий торговой марке.

UI на экранах 600a-600b, показанные, соответственно, на Фиг.6a-6b, предоставляют примеры, соответствующие управляемым пользователем провайдерам удостоверений. UI на экранах, показанных, соответственно, на Фиг.7a-9c, предоставляют примеры, соответствующие управляемым событиями провайдерам удостоверений. Управляемые событиями провайдеры удостоверений выбираются на основании некоторых действий пользователя. Одним из таких действий пользователя является вставка пользователем смарт-карты в устройство чтения смарт-карт. В случае биометрии таким действием пользователя считается приведение некоторой части тела пользователя в контакт с биометрическим датчиком (например, считывание изображения отпечатка пальца производится датчиком отпечатков пальцев, лицо считывается камерой для последующего анализа программным алгоритмом распознавания черт лица и т.д.).

UI на экране 700a по Фиг.7a показан в момент ввода пользователем последовательности клавиш CAD (Ctrl+Alt+Del). Экран 700a логического входа показывает, что два (2) пользователя уже осуществили логический вход в локальную машину. Пиктограмма 702 на Фиг.7a показывает пользователю, что смарт-карты могут быть использованы для логического входа в локальную машину. Далее пользователь вставляет смарт-карту в устройство чтения смарт-карт, аналогичное устройству 105, подключенное к локальной машине.

Когда завершается считывание пользовательских удостоверений со смарт-карты, список пользователей с Фиг.7a, осуществивших логический вход, исчезает, а экран 700b логического входа по Фиг.7b отображает только перечисление сертификатов, считанных со смарт-карты пользователя. Этот экран создается в результате совместной обработки, при которой используются устройство 105 чтения карт с соответствующим ему модулем 202 провайдера удостоверений, API 204 провайдеров удостоверений и UI 206 логического входа. Если на смарт-карте был только один сертификат, ОС автоматически выбирает этот сертификат и отображает поле 704 ввода PIN в качестве экранного приглашения для ввода данных пользователем. Обращаясь далее к Фиг.2, где пользователь набирает на клавиатуре PIN в поле 704 ввода PIN, UI 206 логического входа передает PIN модулю 102 логического входа ОС совместно с сертификатом, считанным со смарт-карты. Считанный устройством 105 чтения смарт-карт сертификат и введенный пользователем PIN могут далее быть использованы для идентификации и аутентификации пользователя с помощью LSA 106 совместно с управляемым событиями модулем 202 провайдера удостоверений, взаимодействующим посредством API 204 провайдеров удостоверений с ОС локальной машины. Если пользователь, вставивший смарт-карту, оставит смарт-карту в устройстве 105 чтения и нажмет кнопку отмены 706 на экране 700b по Фиг.7b, то экран логического входа

вернется к предыдущему состоянию и перечислит всех трех пользователей, как показано на экране 800a по Фиг.8a. Если, однако, смарт-карта содержит более одного сертификата, то ОС отобразит экран с перечислением всех сертификатов. Как показано на экране 800b по Фиг.8b под ссылочным номером 804, как только пользователь выделит один из сертификатов 802, ОС отобразит экран, содержащий поле 806 ввода PIN. Далее пользователь может ввести PIN в поле 806 ввода PIN.

Управляемый событиями модуль 202 провайдера удостоверений, соответствующий устройству 105 чтения смарт-карт, аналогичен управляемому биометрическими событиями модулю 202 провайдера удостоверений устройства 103 считывания отпечатков пальцев. Иллюстративный вариант логического входа пользователя для случая использования отпечатков пальцев в качестве удостоверения показан на Фиг.9a-9c. Как видно из Фиг.9a, отдельная локальная машина отображает экран, показывающий четыре (4) учетных записи (т.е., четыре пользователя имеют право доступа к локальной машине). Пиктограмма 900a на экране по Фиг.9a показывает, что на локальной машине установлен датчик отпечатков пальцев. Пользователь помещает свой палец на датчик/сканер отпечатков пальцев, аналогичный периферийному датчику/сканеру 103 отпечатков пальцев, показанному на Фиг.2. В альтернативном случае чувствительный к нажатию экран, как показано на Фиг.9b, может содержать пиктограмму датчика отпечатков пальцев 900b, являющуюся средством оптического сканирования с обратной связью. В обоих случаях датчик/сканер отпечатков пальцев активируется и считывает отпечаток пальца пользователя. Пользователь получает сообщение, что процесс считывания завершился успешной идентификацией и аутентификацией пользователя по отпечатку пальца в качестве удостоверения для логического входа пользователя в локальную машину при использовании отпечатка пальца пользователя управляемым событиями модулем 202 провайдера удостоверений, показанном на Фиг.2. Модуль 202 провайдера удостоверений сравнивает считанный отпечаток пальца пользователя с содержимым своего кэша сохраненных отпечатков пальцев в базе 108b данных удостоверений и находит соответствие отпечатка пальца пользователю 'Richard', как показано на Фиг.9c. Модуль 202 провайдера удостоверений передает удостоверения Ричарда UI 206 логического входа через API 204 провайдера удостоверений. UI 206 логического входа далее передает удостоверения Ричарда модулю 102 логического входа ОС, который регистрирует Ричарда на локальной машине, результат чего показан в виде изображения пользователя Ричарда на экране Фиг.9c под ссылочным номером 900c.

Вышеупомянутые Фиг.2-9c были описаны для моделей защищенных подключаемых модулей в архитектуре, предназначенной для процесса логического входа посредством модулей провайдеров удостоверений. В соответствии с Фиг.10-11 процесс логического входа может включать в себя один или более специализированных модулей 1102 Провайдеров предварительного доступа (PLAP), взаимодействующих с ОС локальной машины. Каждый модуль 1102 PLAP позволяет пользователю выбрать тип соединения для логического входа, как, например, использование модемного подключения к своему Провайдеру услуг Интернет (ISP), использование кабельного модема для установления сетевого соединения, использование VPN для подключения к сети, подключение к локальной сети и т.д.

В некоторых обстоятельствах локальная машина может быть сконфигурирована для осуществления логического входа при запуске сеанса Службы удаленного доступа (RAS), где для логического входа устанавливается сетевое соединение с целью аутентификации пользователей локальной машины в сети. В частности,

администратор сети может требовать от пользователей осуществления логического входа в локальную машину посредством сеанса RAS, так как это требование позволяет администратору сети осуществлять жесткий контроль над программным обеспечением, установленным на локальной машине, до того, как локальная машина сможет установить соединение с корпоративной сетью, администрируемой этим сетевым администратором. Такой жесткий контроль над локальной машиной может включать в себя обновление антивирусных программ и других приложений, а также периодическую принудительную смену паролей и т.д. В некоторых случаях от всех локальных машин корпоративной сети может требоваться установление соединения посредством конкретного сеанса RAS до логического входа в корпоративную сеть.

Как показано на Фиг.10, при активации пиктограммы 1006 ниспадающего меню пользователю предлагается список типов соединений для логического входа. Каждый пункт данного списка представляет отдельного провайдера логического входа или тип соединения, посредством которого может быть установлено соединение с сетью с использованием соответствующей службы доступа. Как показано на Фиг.10, от пользователя требуется выбрать из списка тип соединения и соответствующую службу доступа, помимо ввода имени пользователя и пароля в поля 1002 и типа учетной записи в поле 1004. Список типов соединений для логического входа и соответствующих служб доступа вызывается активацией пиктограммы 1006, при этом он демонстрирует все доступные машине внешние соединения и позволяет пользователю выбрать одно из них. Каждое соединение представляет Службу удаленного доступа (RAS), которая не обязательно предоставлена провайдером данной ОС, однако совместима с ОС. Например, RAS может быть специализированным модулем дозвона, предоставленным сторонним производителем программного обеспечения, не имеющим отношения к провайдеру данной ОС. В этом случае специализированная RAS позволяет избежать необходимости использования модуля дозвона RAS, поставляемого с ОС и используемого по умолчанию. Сеанс RAS использует удостоверения, введенные в полях 1002-1004, при попытке установления соединения с сетью, определенного пользователем из списка под ссылочным номером 1006. Если введенные пользователем удостоверения не позволят установить соединение, выбранное пользователем, то будет отображена подсказка, предлагающая пользователю предоставить дополнительные удостоверения. С использованием этих дополнительных удостоверений будет предпринята новая попытка установить соединение согласно типу соединения для логического входа, выбранному пользователем из списка под ссылочным номером 1006. Если эта попытка установления соединения с сетью будет успешной, новые удостоверения будут выданы для использования в процессе логического входа, описанном выше в соответствии с Фиг.2-9c.

Пользовательский интерфейс, показанный на экране 1000 Фиг.10, далее может быть пояснен со ссылкой на Фиг.11, демонстрирующей иллюстративный процесс 1100 установления типа соединения с заданной пользователем службой доступа. UI 206 логического входа через API 1112 менеджера провайдеров предварительного доступа (PLAP) запрашивает модули 1102 PLAP о предоставлении одноуровневого списка соответствующих типов соединения и служб доступа. Службы доступа одноуровневого списка соответствуют, например, специализированной службе 1106 доступа по телефонной лиии, специализированной службе 1108 доступа VPN или любому другому типу специализированной или стандартной службы 1104 доступа. Представление каждой службы 1104-1108 доступа отображается для пользователя UI

206 логического входа. Пользователь заполняет поля 1002-1006, включая имя пользователя, пароль, тип учетной записи, а также задаваемый пользователем тип соединения и соответствующую службу доступа из списка под ссылочным номером 1006. API 1112 менеджера PLAP пытается установить соединение с доменом, используя выбранную пользователем службу доступа. Если соединение установить не удалось, API 1112 менеджера PLAP может запросить UI 206 логического входа предложить пользователю ввести дополнительную информацию, например, дополнительные удостоверения, перед повторной попыткой установления соединения с выбранной пользователем службой доступа.

Как только API 1112 менеджера PLAP установит соединение с доменом с использованием выбранной пользователем службы доступа, введенные пользователем имя пользователя и пароль передаются в качестве удостоверений для аутентификации соответствующего пользователя, элемента или принципала в домене. Успешная идентификация и аутентификация пользователя, элемента или принципала с его удостоверениями будут переданы от API 1112 менеджера PLAP на UI 206 логического входа. UI 206 логического входа выполняет RPC модуля 102 логического входа ОС, причем RPC передаст также удостоверения. Модуль 102 логического входа ОС передаст удостоверения в виде пользовательского вызова логического входа LSA на LSA 106 для локальной идентификации и аутентификации по базе данных удостоверений SAM 108a или локальной или удаленной базе 108b данных удостоверений. В альтернативном случае LSA 106 может передать удостоверения посредством соединения домена на AD/KDC 110 для идентификации и аутентификации в домене. Если удостоверения, использованные для идентификации и аутентификации пользователя посредством SAM 108a, базы 108b данных удостоверений, либо AD/KDC 110, успешно приняты, этот факт передается модулю 102 логического входа ОС для завершения процесса логического входа пользователя в локальную машину. В некоторых вариантах осуществления SAM 108a, база 108b данных удостоверений и AD/KDC 110 могут находиться в одном домене и даже быть одной и той же базой данных. В других вариантах осуществления аутентификация принципала, элемента или пользователя может осуществляться посредством службы удостоверений маркерного протокола и/или посредством службы удостоверений протокола запроса-ответа.

Модели подключаемых средств логического входа для провайдеров удостоверений, обсуждавшиеся выше, могут комбинироваться с провайдрами предварительного доступа в различных вариантах осуществления, примеры которых будут продемонстрированы в соответствии с Фиг.12-13. Фиг.12 демонстрирует пример экрана 1200, позволяющего пользователю ввести имя пользователя и пароль, а также выбрать кнопку 1202 options опций логического входа. Выбор пользователем кнопки 1202 options опций логического входа отображает одноуровневый список учетных записей, из которых пользователь может сделать выбор в рамках типа учетной записи 1208a. Выбор типа 1208a учетной записи представляет выбор пользователем модели подключаемого средства логического ввода для конкретного провайдера удостоверений. Как показано на экране 1200, пользователь выбрал тип учетной записи "Novell". Выбор типа учетной записи "Novell" позволяет пользователю выбрать далее кнопку 1208b "advanced Novell options". Выбор кнопки 1208b "advanced Novell options" вызывает UI Novell 1208c, который предлагает пользователю ввести дополнительные удостоверения. Эти дополнительные удостоверения будут использованы для идентификации и аутентификации пользователя по базе данных

доступа на сервере Novell. Пользователь может также видеть и осуществить выбор PLAP из одноуровневого списка служб доступа, выполняя щелчок мышью по пиктограмме 1210 ниспадающего меню.

Процесс 1300 демонстрирует множество модулей 1302, включающих в себя как модули PLAP, так и модули провайдеров удостоверений, каждый из которых имеет соответствующий API 1312 к UI 206 логического входа. Каждый модуль 1302 PLAP может соответствовать любому из нескольких стандартных или специализированных провайдеров предварительного доступа. Каждый модуль 1302 PLAP может быть выбран пользователем из одноуровневого списка служб доступа, отображаемого UI 206 логического входа после активации пользователем пиктограммы 1210 ниспадающего меню. Каждый модуль 1302 PLAP может установить соединение с соответствующей сетью посредством отличающегося типа соединения и соответствующих служб доступа для аутентификации пользователя с использованием его удостоверений по локальной и/или удаленной базе данных удостоверений. Одноуровневый список служб доступа запрашивается UI 206 логического входа у модулей 1302 PLAP.

UI 206 логического входа предлагает пользователю ввести удостоверения в полях, показанных на Фиг.12, таких как поля ввода имени пользователя и пароля, согласно указаниям определяемого пользователем стандартного или специализированного модуля 1302 провайдера удостоверений. Каждый модуль 1302 провайдера удостоверений может соответствовать устройствам 103-107 и 208 чтения, что обсуждалось выше. Такие введенные удостоверения обрабатываются соответствующим модулем 1302 провайдера удостоверений локально на локальной машине. Модуль 1302 провайдера удостоверений может быть сконфигурирован для преобразования вводимых удостоверений, как, например, для преобразования биометрических удостоверений, принятых устройством 103 считывания отпечатков пальцев, или сертификатов удостоверений, считанных устройством 105 чтения смарт-карт. Модуль 1302 провайдеров удостоверений преобразует удостоверения в протокол удостоверений, который должен быть совместимым с ОС локальной машины для дальнейшей идентификации и аутентификации. По сути, преобразование исходных удостоверений в преобразованные удостоверения может производиться локально на локальной машине. По завершении преобразования исходных удостоверений в преобразованные удостоверения преобразованные удостоверения передаются модулем 1302 провайдера удостоверений на UI 206 логического входа через API 1312. API 1312 к UI 206 логического входа использует выбранный пользователем модуль 1302 PLAP для установления соединения со службой доступа с использованием соответствующего типа соединения. Иными словами, модуль 1302 PLAP идентифицирует службу доступа, выбранную пользователем из одноуровневого списка служб доступа, отображаемого посредством пиктограммы 1210 ниспадающего меню на экране 1200.

Модуль 1302 PLAP получает совместимые с ОС удостоверения, как они были получены от модуля 1302 провайдера удостоверений. Далее UI 206 логического входа вызывает модуль 1302 PLAP для использования преобразованных удостоверений, полученных от модуля 1302 провайдера удостоверений, для установления сеанса защищенного сетевого соединения с соответствующей выбранной пользователем службой доступа. Модуль 1302 PLAP пытается установить посредством выбранной пользователем службы доступа сеанс сетевого соединения с доменом, где расположена база данных удостоверений. Если модулю 1302 PLAP не удается

установить сетевой сеанс с использованием выбранной пользователем службы доступа, то модуль 1302 PLAP может запросить UI 206 логического входа отобразить специализированный UI, который предлагает пользователю ввести дополнительные удостоверения, специфичные для этого специализированного UI. В частности, модуль 1302 PLAP может запросить удостоверения, характерные для аутентификации на сервере Novell. Эти дополнительные удостоверения могут потребовать дальнейшего ввода специального имени пользователя и специального пароля, необходимых для доступа к определенному Web-сайту Интернет (например, Novell.com, AOL.com, MSN.com, и т.д.), с целью получения соединения для сетевого сеанса посредством выбранной пользователем службы доступа. В этом случае отображается специализированный UI для модуля 1302 PLAP, содержащий диалоговое окно, предлагающее пользователю ввести дополнительные удостоверения (например, UI Novell 1208c).

По завершении ввода модуль 1302 PLAP подставляет заново введенные удостоверения из UI Novell 1208c вместо первичных удостоверений (имени пользователя и пароля), введенных ранее. Ранее введенные удостоверения удаляются и используются новые. Заново введенные удостоверения возвращаются UI 206 логического входа. UI 206 логического входа передает заново введенные удостоверения модулю 102 логического входа посредством вызова RPC. Далее модуль 102 логического входа ОС передает заново введенные удостоверения LSA 106. Заново введенные удостоверения проверяются в LSA 106 на предмет идентификации и аутентификации. LSA 106 проверяет их достоверность по локальной базе данных, используя SAM 108a и/или локальную или удаленную базу 108b данных удостоверений. В случае домена активного каталога проверка достоверности заново введенных удостоверений осуществляется передачей заново введенных удостоверений посредством сетевого сеанса в домен AD/KDC 110, где соединение сетевого сеанса устанавливается модулем 1302 PLAP. Соответственно, процесс идентификации и аутентификации с использованием провайдера удостоверений и модулей 1302 PLAP может быть циклической процедурой.

В качестве дальнейшего примера, пользователь может изначально ввести имя пользователя "Bill" и пароль "101" в качестве первого набора удостоверений, обрабатываемых локально на локальной машине. Модуль 1302 PLAP, соответствующий выбранной пользователем службе доступа, вызывает через API 1312 UI 206 логического входа для приглашения пользователю ввести другой пароль. Тогда пользователь вводит пароль "102". Новый пароль "102" пересылается базе данных удостоверений (например, SAM 108a, базе 108b данных удостоверений, AD/KDC 110 и т.д.) по соединению, используя выбранную пользователем службу доступа в соединении сетевого сеанса. После успешной аутентификации по базе данных удостоверений пароль "102" пересылается из UI 206 логического входа через модуль 102 логического входа ОС на LSA 106. LSA 106 передает пароль "102" в домен для идентификации и аутентификации по AD/KDC 110 или другой базе данных удостоверений. Таким образом, первая операция выполняется модулем 1302 PLAP, а вторая операция выполняется модулем 1302 провайдера удостоверений.

Каждый модуль 1302 PLAP принимает участие как в процедуре безопасной идентификации и аутентификации, так и в установлении сеанса сетевого соединения с доменом. Кроме того, выбираемая пользователем служба доступа, устанавливаемая соответствующим стандартным или специализированным модулем 1302 PLAP, может представлять собой сеанс сетевого соединения, используемый модулем 1302 провйдера

удостоверений для дальнейшей идентификации и аутентификации удостоверений.

Локальная аутентификация удостоверений может производиться в стиле, отличном от аутентификации удостоверений в домене. Этот стиль может определяться способом хранения данных учетной записи пользователя в активном каталоге домена AD/KDC 110. Активный каталог для учетной записи пользователя может содержать различные атрибуты, как, например, один атрибут, определяющий, может ли учетная запись пользователя устанавливать сеанс RAS, и другой атрибут, определяющий, разрешен ли учетной записи пользователя интерактивный вход в систему. В качестве примера, эти атрибуты могут храниться в виде двух (2) различных битов в учетной записи пользователя в активном каталоге домена, и таким образом могут быть запрошены.

Другие варианты осуществления могут комбинировать использование провайдера удостоверений и PLAP, как в случае, когда локальная машина осуществляет доступ в Интернет в процессе логического входа пользователя. В этом случае при запуске локальной машины автоматически выполняется процедура автозагрузки. Процедура автозагрузки в автоматическом режиме использует удостоверения пользователя как для логического входа в локальную машину, так и для подключения к провайдеру услуг Интернет (ISP) для автоматического получения информации с Web-сайта по умолчанию. В альтернативном случае пользователь может получить приглашение ввести два (2) набора удостоверений - один набор для локальной машины, а другой для ISP, доступ к которому осуществляется посредством определяемого пользователем PLAP.

В еще одном варианте осуществления локальная машина может быть сконфигурирована таким образом, что будет требовать идентификации и аутентификации всех пользователей на сервере Novell (или другого типа) определенного домена. В этом случае пользователь локальной машины получит приглашение ввести характерные для данного сервера удостоверения (например, удостоверения, характерные для сервера Novell). Далее пользователь выбирает кнопку 1208b advanced Novell option, показанную на Фиг.12. UI 206 логического входа, показанный на Фиг.13, собирает введенные пользователями удостоверения, удовлетворяющие требованиям модулей 1302 как для службы доступа, так и для провайдера удостоверений, относящегося к серверу Novell. В течение сбора удостоверений сетевое соединение с доменом сервера Novell еще не установлено. Пользователь может также выбрать специализированное средство дозвона PLAP из списка служб доступа, связанного с пиктограммой 1210. Далее пользователь может сигнализировать, что вся требуемая информация ввеена (например, нажать клавишу 'enter'). В этот момент, в частности, может начаться сетевой трафик от локальной машины к удаленной базе удостоверений в домене и к домену AD/KDC 110. Сетевой трафик использует сеанс сетевого подключения, установленный модулем 1302 PLAP для соответствующей службы доступа. Сетевой трафик может включать в себя удостоверения в форме метаданных, которые могли быть собраны вместе и последовательно переданы - сначала для аутентификации принципала с целью использования службы доступа, устанавливаемой с использованием модуля 1302 PLAP, а затем для аутентификации провайдером удостоверений в модуле 1302 провайдера удостоверений. По сути, служба доступа позволяет локальной машине безопасным образом осуществлять связь с активным каталогом в своем домене, который может быть сторонним сервером Интернет.

Иллюстративная компьютерная система и окружение

Фиг.14 демонстрирует иллюстративную вычислительную систему и окружение,

которые могут быть использованы для реализации описанных процессов. Компьютер 1442, который может быть локальной машиной, описанной в соответствии с Фиг.2а-13, включает в себя один или более процессоров или устройств 1444 обработки данных, системную память 1446 и шину 1448, соединяющую различные системные компоненты, включая системную память 1446, и процессоры 1444. Шина 1448 представляет собой одну или более из нескольких типов шинных структур, включая шину памяти или контроллер памяти, периферийную шину, ускоренный графический порт, и процессорную либо локальную шину, с использованием любой из множества шинных архитектур. Системная память 1446 включает в себя постоянное запоминающее устройство (ROM) 1450 и оперативное запоминающее устройство (RAM) 1452. Базовая система ввода/вывода (BIOS) 1454, содержащая базовые процедуры, способствующие обмену информацией между элементами компьютера 1442, например, в течение загрузки, хранится в ROM 1450.

Компьютер 1442 далее содержит накопитель 1456 на жестких дисках для чтения с жесткого диска (не показан) и записи на него, магнитный дисковод 1458 для чтения со съемного магнитного диска 1460 и записи на него, а также оптический дисковод 1462 для чтения со съемного оптического диска 1464, такого как CD ROM или другой оптический носитель, и записи на него. Накопитель 1456 на жестких дисках, магнитный дисковод 1458 и оптический дисковод 1462 соединены с шиной 1448 по интерфейсу SCSI 1466 или любому другому соответствующему интерфейсу. Эти дисководы и накопители и связанные с ними машиночитаемые носители обеспечивают энергонезависимое хранение машиночитаемых инструкций, структур данных, программных модулей и других данных, предназначенных для компьютера 1442. Хотя иллюстративный вариант осуществления, описываемый здесь, содержит жесткий диск, съемный магнитный диск 1460 и съемный оптический диск 1464, специалистам в данной области техники должно быть понятно, что в иллюстративной операционной среде могут быть использованы другие типы машиночитаемых носителей, которые могут обеспечить хранение требуемых компьютеру данных, как то магнитные кассеты, карты флэш-памяти, цифровые видеодиски, оперативные запоминающие устройства (RAM), постоянные запоминающие устройства (ROM) и т.п.

На жестком диске 1456, магнитном диске 1460, оптическом диске 1464, ROM 1450 и RAM 1452 может содержаться некоторое количество программных модулей, в том числе ОС 1470, один или более модулей прикладных программ 1472. В качестве примера, но не в ограничительном смысле, одним или более модулями 1472 прикладных программ могут быть модули 202 провайдеров удостоверений, провайдеры 302 удостоверений аутентификации нижнего уровня, модули 1102 PLAP и другие модули 1302. На жестком диске 1456, магнитном диске 1460, оптическом диске 1464, ROM 1450 и RAM 1452 могут содержаться и другие элементы, в том числе другие программные модули 1474 и данные 1476 программ. Пользователь может вводить команды и информацию в компьютер 1442 посредством устройств ввода, таких как клавиатура 1478 и координатно-указательное устройство 1480. Другие устройства ввода (не показанные на Фиг.14) могут включать в себя устройство считывания 103 отпечатков пальцев, устройство 208 чтения маркеров, устройство 105 чтения смарт-карт, микрофон, джойстик, игровую панель, антенну спутниковой связи, камеру или оптический сканер, устройство распознавания и анализа сетчатки и т.п. Эти и другие устройства ввода подключаются к процессору 1444 посредством интерфейса 1482, подсоединенного к шине 1448. Монитор 1484 или другой тип устройства вывода изображений также подключен к шине 1448 посредством такого

интерфейса, как видеоадаптер 1486. В дополнение к монитору персональные компьютеры, как правило, содержат и другие периферийные устройства вывода (не показаны), такие как громкоговорители и принтеры.

Компьютер 1442 в общем случае функционирует в сетевой среде, используя логические соединения с одним или более удаленных компьютеров, таких как удаленный компьютер 1488. Удаленный компьютер 1488 может быть другим персональным компьютером, сервером, маршрутизатором, сетевым ПК, одноранговым узлом сети или другим традиционным сетевым узлом, и, как правило, включает в себя многие или все элементы, описанные выше относительно компьютера 1442. Логические соединения, показанные на Фиг.14, включают в себя локальную сеть (LAN) 1490 и глобальную сеть (WAN) 1492. Такие сетевые среды характерны для офисов, компьютерных сетей масштаба предприятия, интрасетей и Интернет.

При использовании в сетевом окружении LAN компьютер 1442 подключен к локальной сети посредством сетевого интерфейса или адаптера 1494. При использовании в сетевом окружении WAN компьютер 1442, как правило, содержит модем 1496 или другие средства установления связи через глобальную сеть 1492, такую как Интернет. Модем 1496, который может быть как внутренним, так и внешним, подключен к шине 1448 посредством интерфейса 1468 последовательного порта. В сетевой среде программные модули, описанные относительно персонального компьютера 1442, или их части, могут храниться на удаленном запоминающем устройстве. Необходимо принимать во внимание, что показанные сетевые соединения являются иллюстративными и могут использоваться другие средства установления связи между компьютерами.

В общем случае процессоры 1442 данных компьютера программируются посредством инструкций, хранимых в различные моменты времени на разных запоминающих устройствах компьютера. Программы и операционные системы, как правило, распространяются, к примеру, на дискетах или компакт-дисках. Оттуда они устанавливаются или загружаются во вторичную память компьютера. При исполнении они загружаются, по меньшей мере частично, в первичную электронную память компьютера. Описываемое здесь изобретение включает в себя эти и различные другие типы машиночитаемых носителей в случае, если эти носители содержат инструкции или программы для реализации описанных ниже блоков во взаимодействии с микропроцессором или другим процессором данных. Изобретение также включает в себя собственно компьютер в случае, если он запрограммирован согласно описанным здесь способам и технологиям.

С целью ясности изложения программы и другие исполняемые программные компоненты, такие как ОС, показаны здесь в виде дискретных блоков, хотя следует понимать, что такие программы и компоненты располагаются в различные моменты времени на различных компонентах хранения данных компьютера и выполняются процессором (процессорами) данных компьютера.

Заключение

Осуществление данного изобретения позволяет совместное использование множества взаимодействующих модулей, полностью совместимых с ОС локальной машины. Эти совместно существующие взаимодействующие модули могут быть моделями подключаемых средств логического входа дя провайдеров удостоверений для логического входа в локальную машину через ее ОС, причем эти модели включают в себя, но не в ограничительном смысле, цифровые сертификаты,

биометрические данные, удостоверения в виде имени пользователя и пароля и т.д. Эти совместно существующие взаимодействующие модули могут также быть провайдерами предварительного доступа, включающими в себя, но не в ограничительном смысле, приложения туннелирования Интернет, приложения беспроводной связи, приложения VPN Ethernet, приложения сетей с коммутацией каналов на витой паре, использующие оборудование проводных модемов, рассчитанных на скорость передачи данных до 56 кбит/с, и т.д.

Настоящее изобретение может быть осуществлено в других специфических формах, не отклоняясь от его сущности и существенных характеристик. Описанные варианты осуществления должны рассматриваться со всех точек зрения только как иллюстративные, но не ограничительные. Таким образом, объем изобретения определяется прилагаемой формулой изобретения, а не предшествующим описанием. Все изменения, попадающие под смысловое значение и диапазон эквивалентов в рамках средств и соответствия формулы изобретения, охватываются определяемым ими объемом.

Формула изобретения

1. Способ безопасного выполнения логического входа пользователя, включающий в себя этапы, на которых

загружают (212) пользовательский интерфейс (UI) (206) логического входа посредством процедуры (102) логического входа операционной системы (ОС), непосредственно взаимодействующей с ОС компьютерного устройства;

загружают (214) и инициализируют (214) множество зарегистрированных модулей (202) провайдеров удостоверений, представляющих собой совместно существующие интерфейсы к ОС, причем пользователь использует по меньшей мере один из этих модулей провайдеров удостоверений для осуществления логического входа на компьютерное устройство через его ОС, при этом каждый модуль провайдера удостоверений использует отличающийся от других процесс идентификации и аутентификации, соответствующий отличающемуся от других типу удостоверений;

предоставляют одноуровневый список всех провайдеров удостоверений, соответствующих упомянутому множеству зарегистрированных модулей провайдеров удостоверений, для отображения;

принимают (224) сделанный пользователем выбор одного из отображаемых провайдеров удостоверений;

принимают на устройстве ввода (103, 105, 107, 208), связанном с компьютерным устройством, удостоверение от пользователя, соответствующее выбранному провайдеру удостоверений;

преобразуют в модуле провайдера удостоверений, соответствующему выбранному провайдеру удостоверений, принятое удостоверение в общий протокол удостоверений;

передают преобразованное удостоверение через интерфейс прикладного программирования (API) (204) провайдера удостоверений в UI логического входа;

вызывают процедуру логического входа ОС с целью аутентификации преобразованного удостоверения по базе (108b) данных удостоверений; и

выполняют логический вход пользователя, идентифицированного посредством преобразованного удостоверения, для доступа к компьютерному устройству в случае успешной аутентификации.

2. Способ по п.1, в котором логический вход пользователя в компьютерное

устройство не будет выполнен до тех пор, пока множество упомянутых удостоверений не будет преобразовано соответствующим упомянутым отличающимся модулем провайдера удостоверений, передано и успешно аутентифицировано.

3. Способ по п.1, в котором логический вход пользователя в компьютерное устройство не выполняют в процессе преобразования удостоверений.

4. Способ по п.1, в котором этап предоставления одноуровневого списка дополнительно содержит этапы, на которых

запрашивают посредством UI логического входа одноуровневый список всех зарегистрированных модулей провайдеров удостоверений и

отображают одноуровневый список на экране дисплея, формируемом UI логического входа.

5. Способ по п.1, в котором вызов процедуры логического входа ОС с целью аутентификации преобразованного удостоверения по базе данных удостоверений дополнительно включает в себя этапы, на которых

передают преобразованное удостоверение локальным средствам защиты (LSA) (106) и

определяют аутентификацию посредством LSA по базе данных удостоверений, выбираемой из группы, которая содержит:

локальную базу данных менеджера учетных записей системы безопасности (SAM) (108a),

локальную базу (108b) данных, отличную от базы данных SAM,

удаленную базу данных удостоверений,

службу удостоверений маркерного протокола,

службу протокола запроса и ответа, а также

активный каталог (AD) и центр распределения ключей Kerberos (KDC) (110) в удаленном по отношению к компьютерному устройству домене.

6. Способ по п.1, в котором каждый модуль провайдера удостоверений выполнен с возможностью взаимодействия с ОС посредством API (204) провайдера удостоверений.

7. Способ по п.1, в котором каждый отличающийся тип удостоверений выбирают из группы, включающей в себя имя пользователя и пароль, удостоверение в виде аппаратного маркера, удостоверение в виде цифрового сертификата, удостоверение в виде смарт-карты, удостоверение по протоколу запроса и ответа, сетчатку глаза, человеческое лицо, походку, оразец почерка, голос, запах, отпечаток пальца и другие биометрические параметры.

8. Способ по п.1, в котором логический вход пользователя для доступа к компьютерному устройству не выполняют в процессе аутентификации преобразованных удостоверений по базе данных удостоверений посредством процедуры логического входа ОС.

9. Способ по п.1, дополнительно содержащий, после этапа логического входа пользователя для доступа к компьютерному устройству, этапы, на которых

запрашивают дополнительное удостоверение для доступа к домену с помощью приложения (404), исполняющегося в компьютерном устройстве;

используют один из упомянутых отличающихся совместно существующих модулей провайдеров удостоверений для получения от пользователя, используя устройство ввода, этого дополнительного удостоверения; и

передают полученное дополнительное удостоверение упомянутому приложению для аутентификации.

10. Машиночитаемый носитель, предназначенный для использования в

компьютерном устройстве, имеющем процессор для исполнения операционной системы (ОС), имеющей компонент аутентификации, и содержащий инструкции, которые при их исполнении процессором реализуют способ по любому из пп.1-9.

11. Способ безопасного выполнения логического входа пользователя, включающий в себя этапы, на которых

загружают (212) пользовательский интерфейс (UI) (206) логического входа посредством процедуры (102) логического входа операционной системы (ОС), непосредственно взаимодействующей с ОС компьютерного устройства;

загружают (214) и инициализируют (214) множество зарегистрированных модулей (202) провайдеров удостоверений, представляющих собой совместно существующие интерфейсы к ОС, причем пользователь использует по меньшей мере один из этих модулей провайдеров удостоверений для осуществления логического входа на компьютерное устройство, при этом каждый модуль провайдера удостоверений использует отличающийся от других процесс идентификации и аутентификации;

предоставляют одноуровневый список всех провайдеров удостоверений, соответствующих упомянутому множеству зарегистрированных модулей провайдеров удостоверений, для отображения;

предоставляют, посредством UI логического входа из состава ОС через обеспечиваемый к нему интерфейс прикладного программирования (API) (1312) менеджера провайдеров предварительного доступа (PLAP), одноуровневый список служб доступа от соответствующего множества совместно существующих отличающихся модулей (1302) PLAP для отображения;

принимают (224) от пользователя сделанный пользователем выбор одного или более из отображаемых провайдеров удостоверений и выбор одной из упомянутых служб доступа;

принимают на устройстве ввода (103, 105, 107, 208), связанном с компьютерным устройством, удостоверение от пользователя, соответствующее выбранному провайдеру удостоверений;

после установления соединения с доменом с использованием одной из упомянутых служб доступа:

передают удостоверение провайдеру аутентификации домена,

осуществляют первичную аутентификацию удостоверения посредством провайдера аутентификации домена и

в случае успешной первичной аутентификации:

передают удостоверение от API PLAP в UI логического входа,

осуществляют вызов удаленной процедуры (RPC) из UI логического входа с передачей удостоверения процедуре логического входа ОС,

передают удостоверение от процедуры логического входа ОС с помощью пользовательского вызова логического входа локальных средств защиты (LSA) средствам LSA,

осуществляют вторичную аутентификацию с помощью LSA по базе данных удостоверений, выбираемой из группы, которая содержит:

базу данных менеджера учетных записей системы безопасности (SAM),

локальную базу данных, отличную от базы данных SAM,

удаленную базу данных удостоверений,

службу удостоверений маркерного протокола,

службу протокола запроса и ответа, а также

активный каталог (AD) и центр распределения ключей Kerberos (KDC) в удаленном по отношению к компьютерному устройству домене;

в случае успеха вторичной аутентификации осуществляют логический вход пользователя, идентифицированного удостоверением, для использования компьютерного устройства, в котором исполняется ОС.

12. Способ по п.11, дополнительно включающий в себя этап, на котором при невозможности установить соединение с доменом с использованием упомянутой одной из упомянутых служб доступа:

повторно отображают одноуровневый список служб доступа на экране дисплея, формируемом UI логического входа;

приглашают ввести другие удостоверения и выбрать другую из упомянутых служб доступа;

принимают ввод других удостоверений и выбор другой из упомянутых служб доступа;

пытаются установить соединение с доменом с использованием упомянутой другой выбранной из упомянутых служб доступа.

13. Машиночитаемый носитель, предназначенный для использования в компьютерном устройстве, имеющем процессор для исполнения операционной системы (ОС), имеющей компонент аутентификации, и содержащий инструкции, которые при их исполнении процессором реализуют способ по любому из пп.11 и 12.

14. Машиночитаемый носитель по п.13, в котором компонент аутентификации из состава ОС включает в себя:

модуль (206) пользовательского интерфейса (UI) логического входа;

модуль (102) логического входа ОС для приема вызовов, соответствующих вызову удаленной процедуры (RPC), от модуля UI логического входа; а также

локальные средства защиты (LSA) для определения аутентификации по связанной с LSA базе данных удостоверений, выбираемой из группы, которая содержит:

базу данных менеджера учетных записей системы безопасности (SAM),

локальную базу данных, отличную от базы данных SAM,

удаленную базу данных удостоверений,

службу удостоверений маркерного протокола,

службу протокола запроса и ответа, а также

активный каталог (AD) и центр распределения ключей Kerberos (KDC) в удаленном по отношению к компьютерному устройству домене.

15. Машиночитаемый носитель, предназначенный для использования в компьютерном устройстве, имеющем процессор для исполнения операционной системы (ОС), включающей в себя компонент аутентификации, имеющий модуль (206) пользовательского интерфейса (UI) логического входа, модуль (102) логического входа ОС для приема вызовов удаленных процедур (RPC) от модуля UI логического входа, локальные средства защиты (LSA) для приема пользовательских вызовов логического входа LSA от модуля логического входа ОС, при этом LSA осуществляют обмен данными с одной или более базами данных удостоверений, при этом компьютерное устройство исполняет инструкции, записанные на данном машиночитаемом носителе, причем эти инструкции содержат множество отличающихся совместно существующих соответствующих модулей провайдеров предварительного доступа (PLAP) и модулей провайдеров удостоверений, представляющих собой интерфейсы к ОС, при этом пользователь использует по меньшей мере один из модулей PLAP и модулей провайдеров удостоверений для

логического входа на компьютерное устройство через его ОС, причем:

каждый из упомянутых модулей обменивается данными посредством интерфейса прикладного программирования (API) с модулем UI логического входа;

модуль UI логического входа совместим для приема от пользователя удостоверения и информации о выборе службы доступа, заданной посредством соответствующего упомянутого модуля PLAP;

API может устанавливать и поддерживать сетевой сеанс посредством соединения с доменом с использованием выбранной службы доступа, если принятое удостоверение аутентифицировано API по одной или более базам данных удостоверений в домене;

удостоверение, принятое модулем UI логического входа, преобразуется соответствующим одним из модулей провайдеров удостоверений, каждый из которых преобразует соответствующий отличающийся тип удостоверений в общий протокол удостоверений;

каждый из упомянутых модулей провайдеров удостоверений передает преобразованное удостоверение, соответствующее общему протоколу удостоверений, через API компоненту аутентификации из состава ОС для аутентификации преобразованных удостоверений по упомянутым одной ии более базам данных удостоверений;

компонент аутентификации из состава ОС осуществляет логический вход пользователя, идентифицированного преобразованным удостоверением, для доступа к компьютерному устройству в случае успешной аутентификации.

16. Машиночитаемый носитель по п.15, в котором модуль UI логического входа дополнительно содержит инструкции для:

запроса одноуровневого списка;

представлений провайдеров удостоверений, полученных от и соответствующих модулям провайдеров удостоверений, и

служб доступа, полученных от и соответствующих модулям PLAP;

отображения каждого упомянутого одноуровневого списка на дисплее; а также

приема от пользователя информации об одном или более выбранных элементов из каждого упомянутого одноуровневого списка на дисплее.

17. Машиночитаемый носитель по п.15, в котором каждый отличающийся тип удостоверений выбирается из группы, включающей в себя имя пользователя и пароль, удостоверение в виде аппаратного маркера, удостоверение в виде цифрового сертификата, удостоверение в виде смарт-карты, удостоверение протокола запроса и ответа, сетчатку глаза, человеческое лицо, походку, образец почерка, голос, запах, отпечаток пальца и другие биометрические параметры.

18. Компьютерная система, содержащая собственную операционную систему (ОС), включающую в себя интерфейс прикладного программирования (API) менеджера провайдеров предварительного доступа (PLAP) и модуль аутентификации, при этом модуль аутентификации из состава ОС включает в себя:

модуль (206) пользовательского интерфейса (UI) логического входа,

модуль (102) логического входа ОС для приема вызовов, соответствующих вызову удаленной процедуры (RPC), от модуля UI логического входа, и

локальные средства защиты (LSA) (106) для определения аутентификации по связанной с LSA базе данных удостоверений, выбираемой из группы, которая содержит:

базу данных менеджера учетных записей системы безопасности (SAM),

локальную базу данных, отличную от базы данных SAM,

удаленную базу данных удостоверений,

службу удостоверений маркерного протокола,

службу протокола запроса и ответа и

активный каталог (AD) и центр распределения ключей Kerberos (KDC) в удаленном по отношению к компьютерной системе домене;

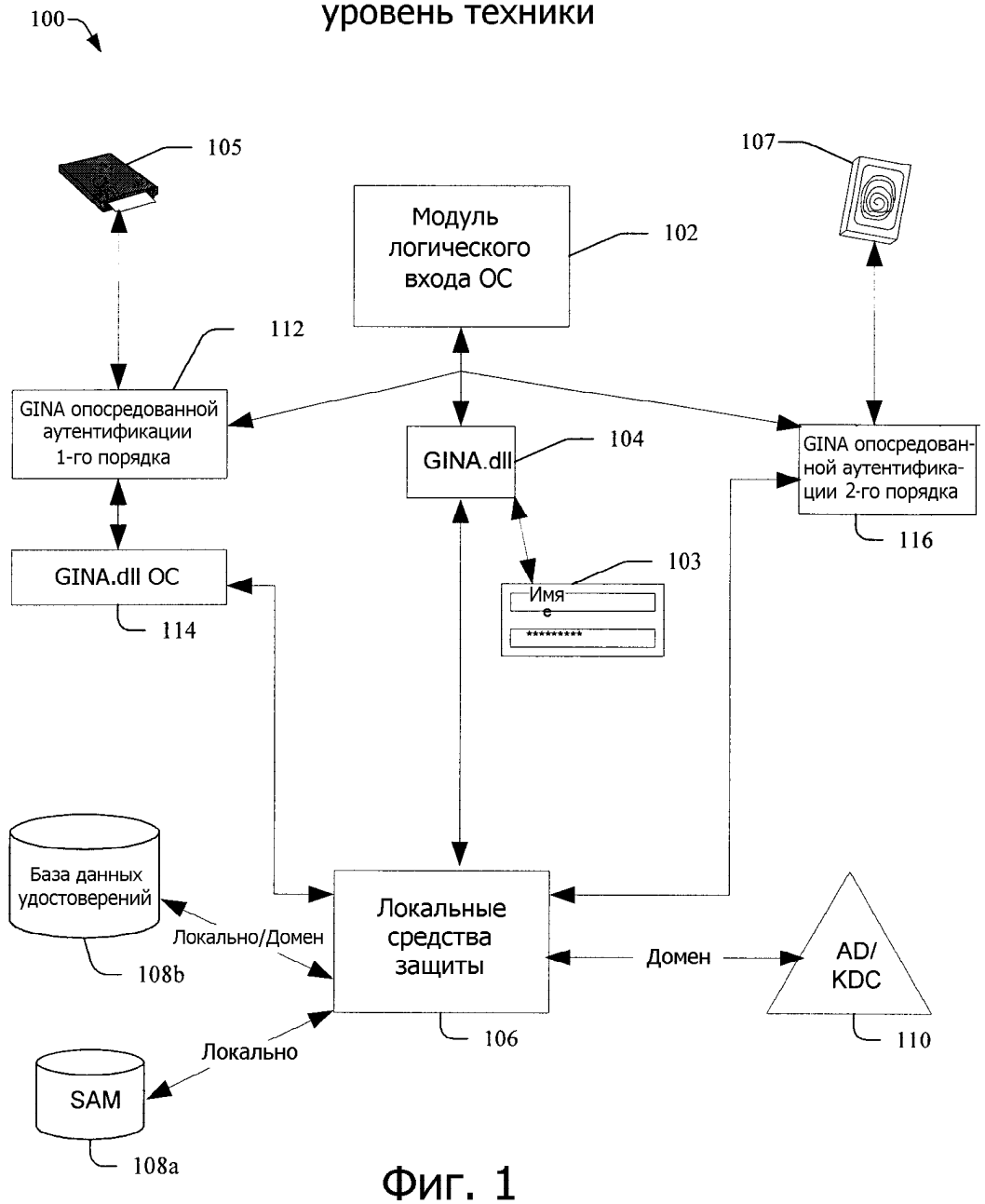
при этом каждый из множества отличающихся совместно существующих модулей PLAP может устанавливать соединение между API менеджера PLAP и службой доступа, соответствующей этому модулю PLAP, причем пользователь использует по меньшей мере один из модулей PLAP для логического входа в компьютерную систему через ее собственную ОС;

каждый упомянутый модуль PLAP задает удостоверение и соответствующий отличающийся тп соединения для соответствующей службы доступа;

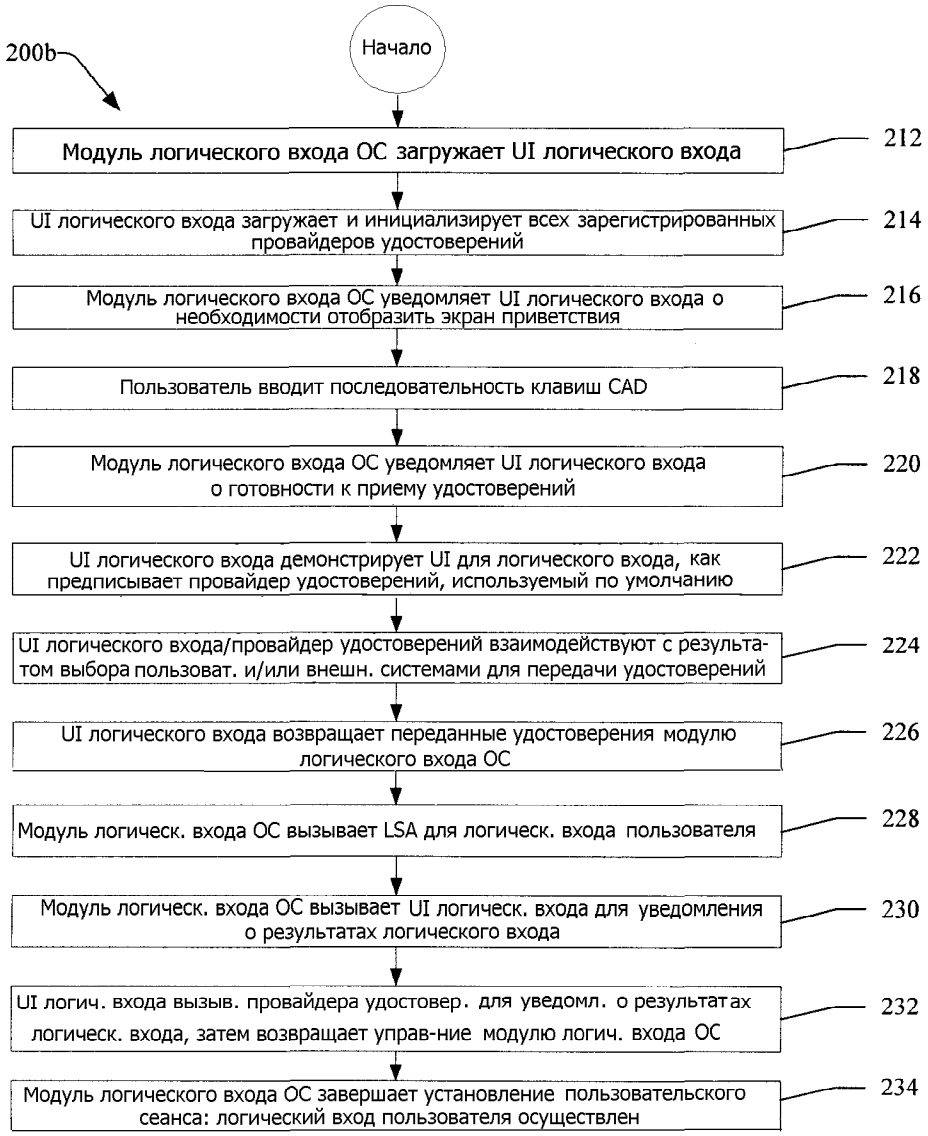
модуль аутентификации осуществляет аутентификацию принципала, используя удостоверение, заданное одним из упомянутых модулей PLAP для доступа к компьютерной системе посредством ее собственной ОС;

в случае успешной аутентификации принципала, принципал использует компьютерную систему для обмена данными между API менеджера PLAP и службой доступа, соответствующей упомянутому модулю PLAP.

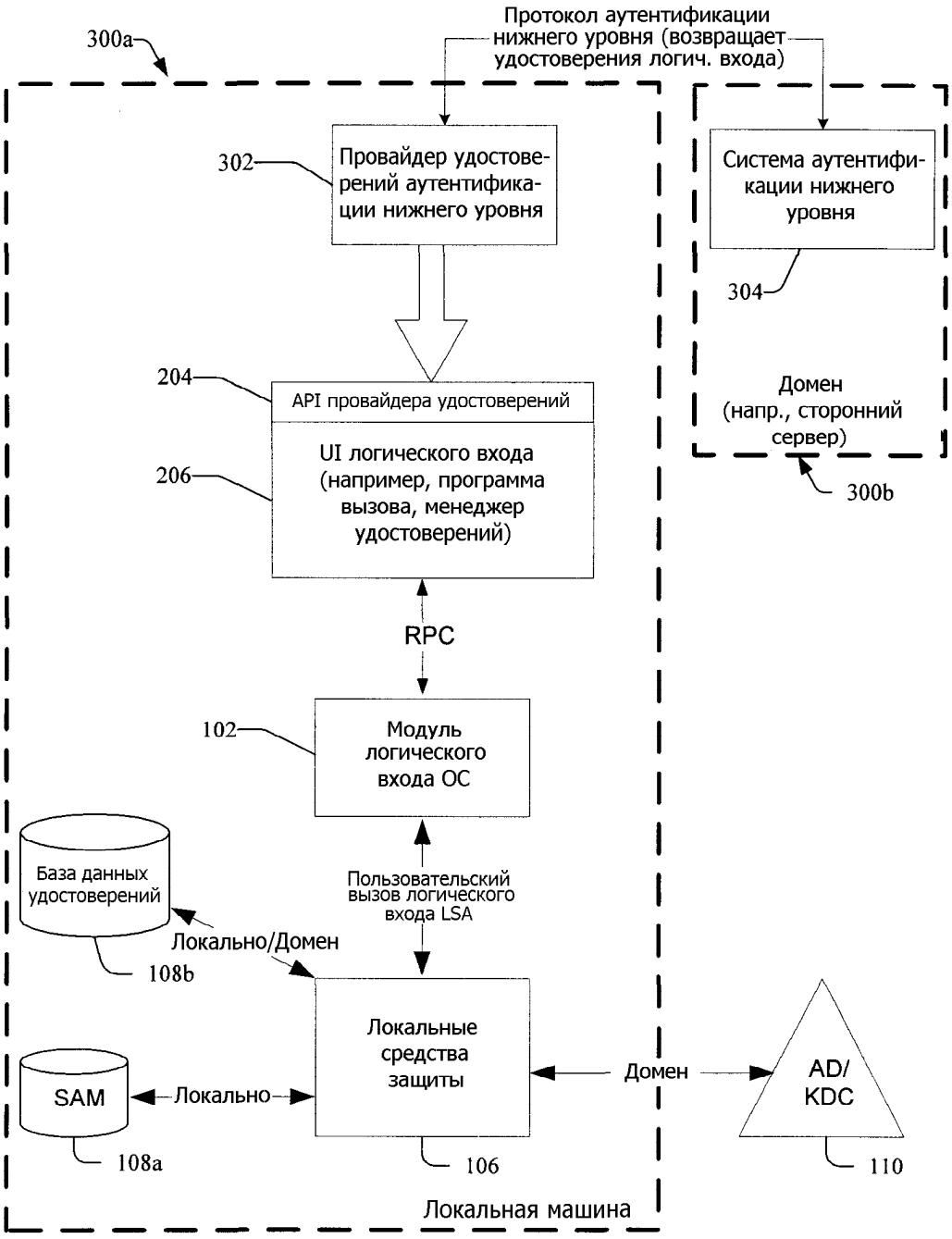
Предшествующий уровень техники



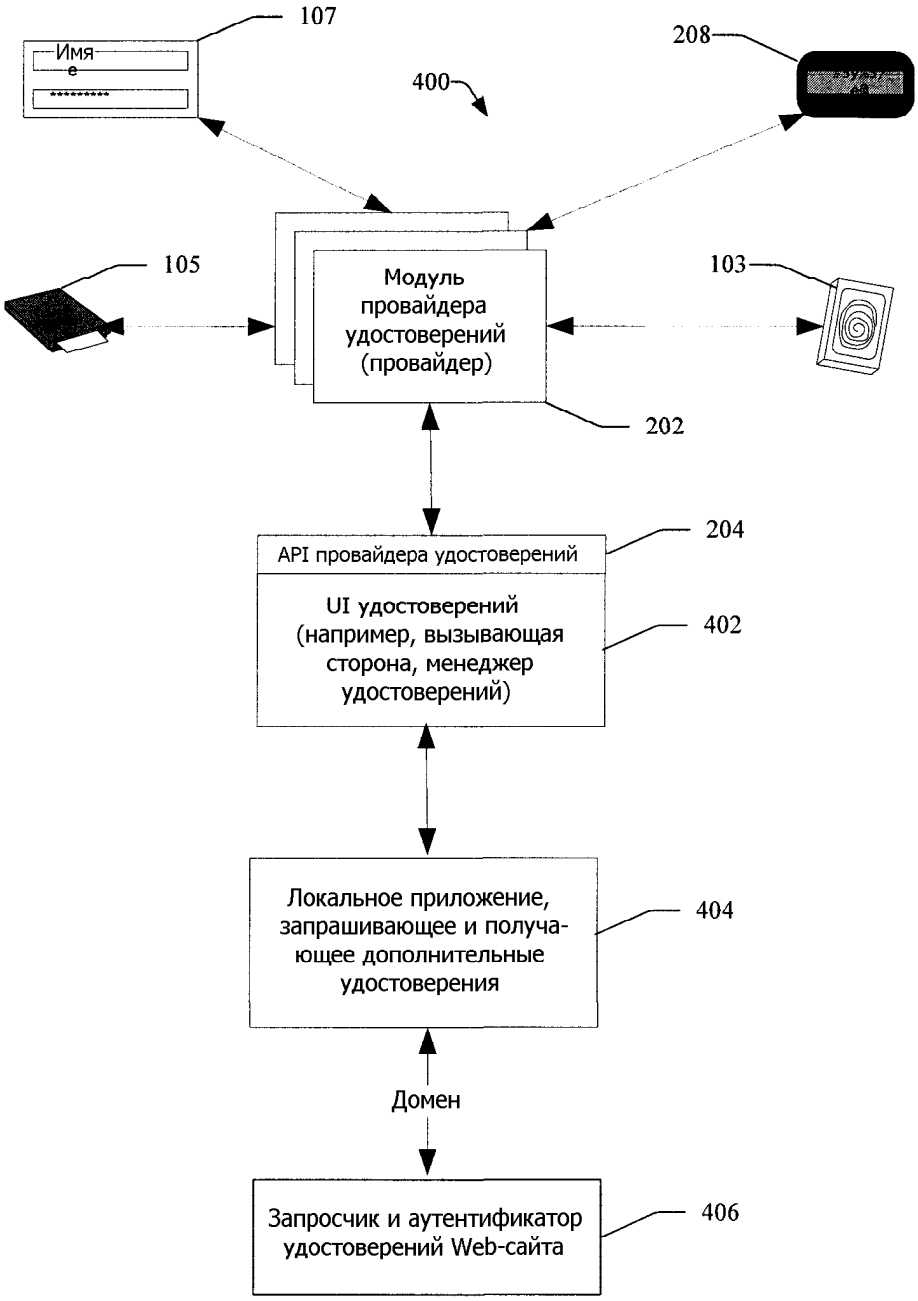
Фиг. 1


200b
Начало
Модуль логического входа ОС загружает UI логического входа
212
UI логического входа загружает и инициализирует всех зарегистрированных провайдеров удостоверений
214
Модуль логического входа ОС уведомляет UI логического входа о необходимости отобразить экран приветствия
216
Пользователь вводит последовательность клавиш CAD
218
Модуль логического входа ОС уведомляет UI логического входа о готовности к приему удостоверений
220
UI логического входа демонстрирует UI для логического входа, как предписывает провайдер удостоверений, используемый по умолчанию
222
UI логического входа/провайдер удостоверений взаимодействуют с результатом выбора пользоват. и/или внешн. системами для передачи удостоверений
224
UI логического входа возвращает переданные удостоверения модулю логического входа ОС
226
Модуль логическ. входа ОС вызывает LSA для логическ. входа пользователя
228
Модуль логическ. входа ОС вызывает UI логическ. входа для уведомления о результатах логического входа
230
UI логич. входа вызыв. провайдера удостовер. для уведомл. о результатах логическ. входа, затем возвращает управ-ние модулю логич. входа ОС
232
Модуль логического входа ОС завершает установление пользовательского сеанса: логический вход пользователя осуществлен
234

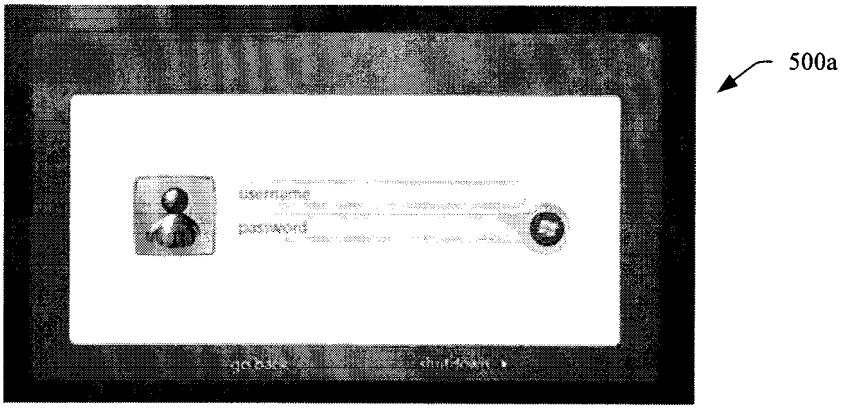
Фиг. 2b


300a
Протокол аутентификации нижнего уровня (возвращает удостоверения логич. входа)
302
Провайдер удостоверений аутентификации нижнего уровня
Система аутентификации нижнего уровня
304
Домен (напр., сторонний сервер)
300b
204
API провайдера удостоверений
206
UI логического входа (например, программа вызова, менеджер удостоверений)
RPC
102
Модуль логического входа ОС
База данных удостоверений
Пользовательский вызов логического входа LSA
Локально/Домен
108b
Локальные средства защиты
SAM
Локально
Домен
AD/ KDC
108a
106
110
Локальная машина

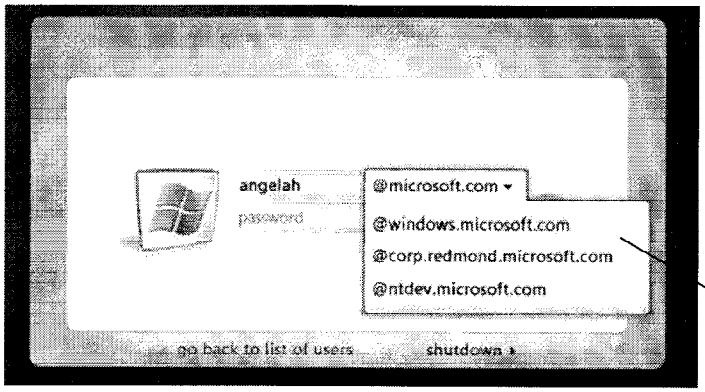
Фиг. 3


107
Имя
208
400
105
Модуль провайдера удостоверений (провайдер)
103
202
API провайдера удостоверений
204
UI удостоверений (например, вызывающая сторона, менеджер удостоверений)
402
Локальное приложение, запрашивающее и получающее дополнительные удостоверения
404
Домен
Запросчик и аутентификатор удостоверений Web-сайта
406

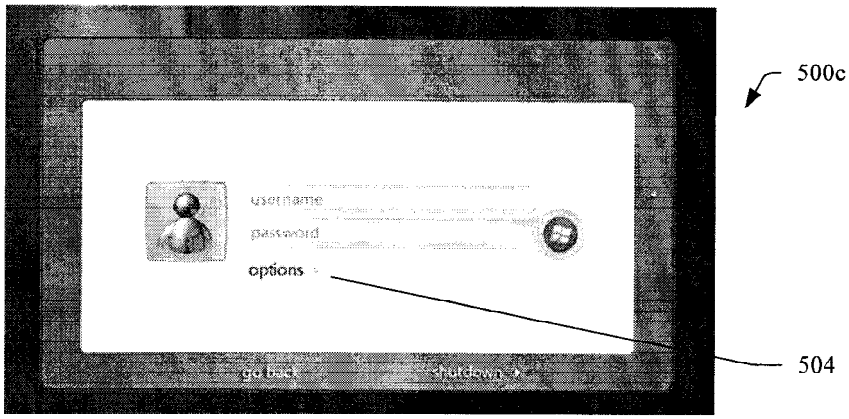
Фиг. 4


500a

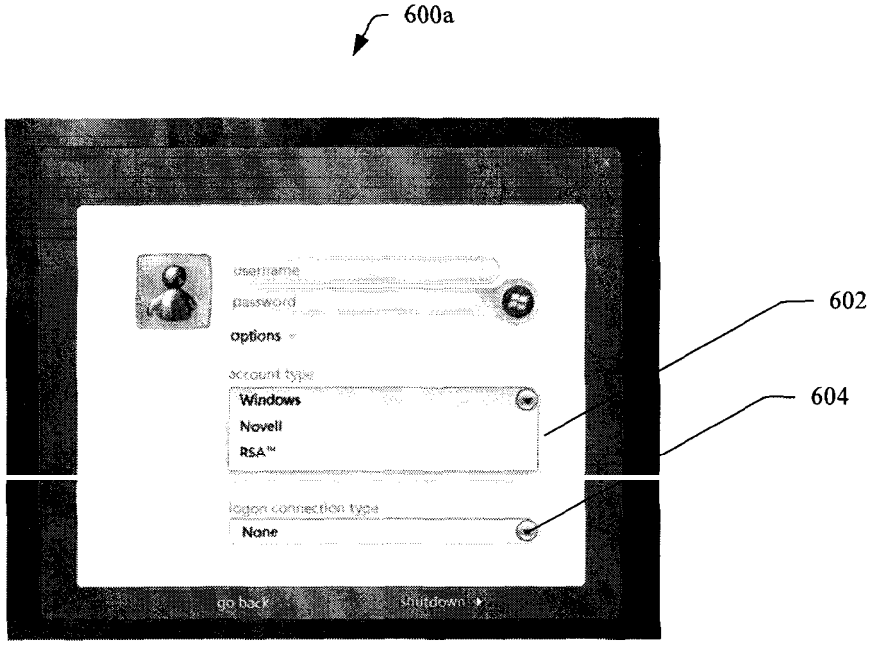
Фиг. 5а



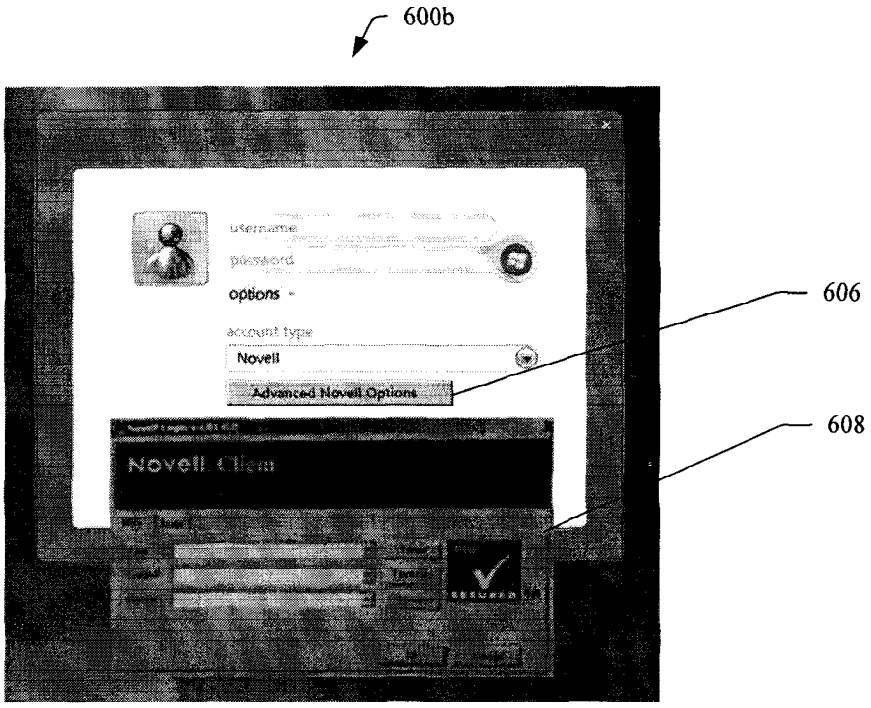
Фиг. 5b



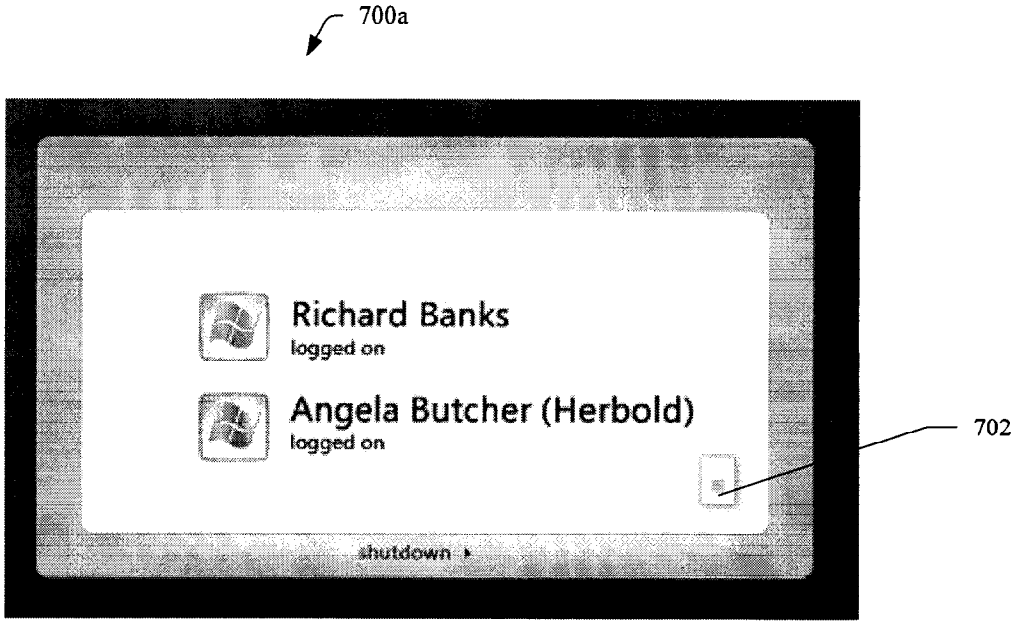
Фиг. 5c



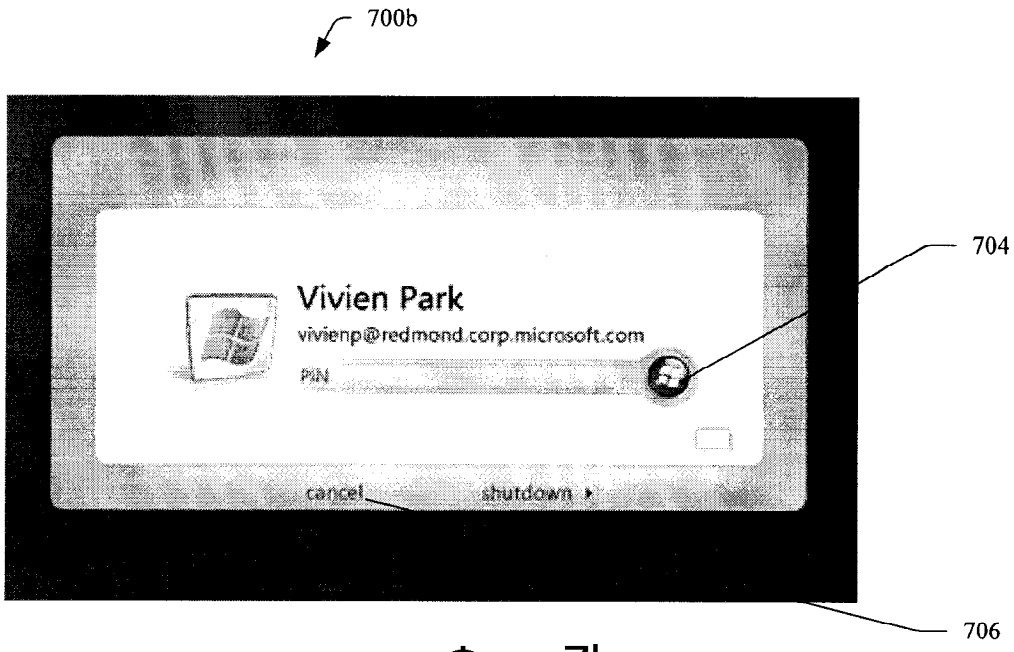
Фиг. 6a


600b
606
608
username
password
options
account type
Novell
Advanced Novell Options
Novell Client

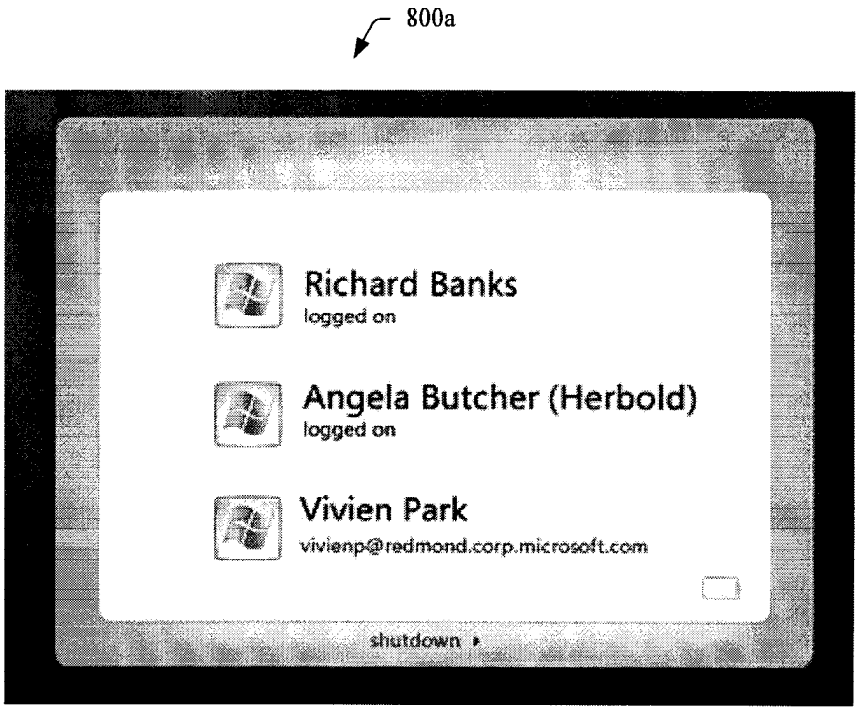
Фиг. 6b


700a
Richard Banks
logged on
Angela Butcher (Herbold)
logged on
shutdown
702

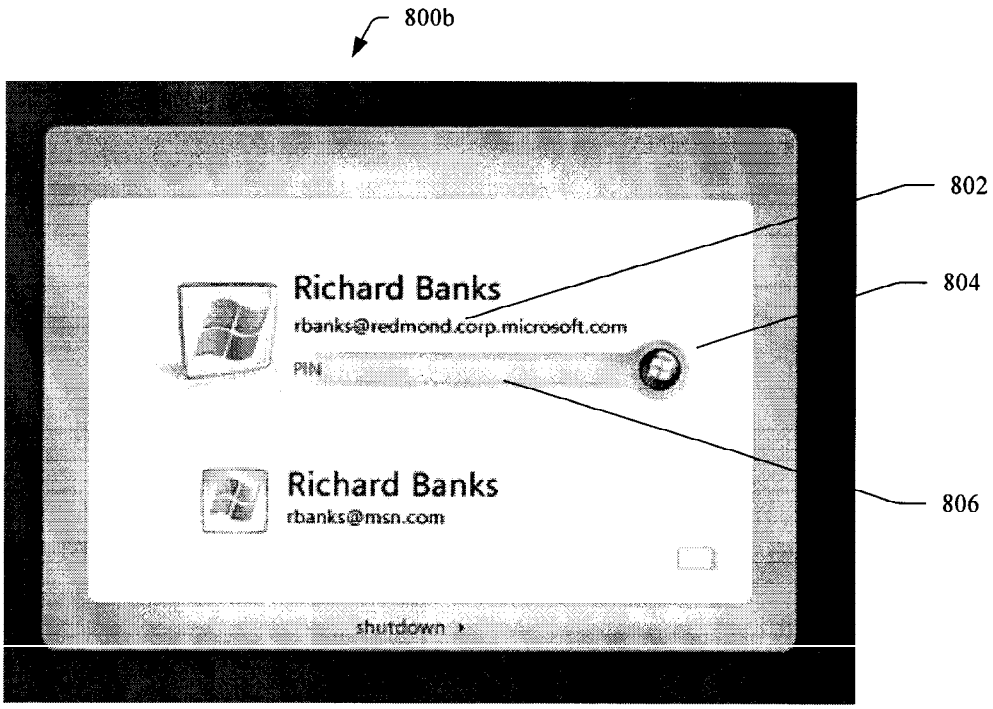
Фиг. 7a


700b
Vivien Park
vivienp@redmond.corp.microsoft.com
PIN
cancel
shutdown
704
706

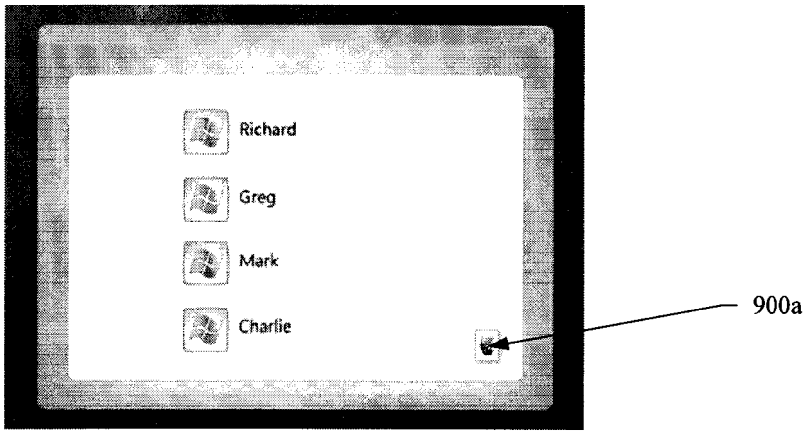
Фиг. 7b


800a
Richard Banks
logged on
Angela Butcher (Herbold)
logged on
Vivien Park
vivienp@redmond.corp.microsoft.com
shutdown

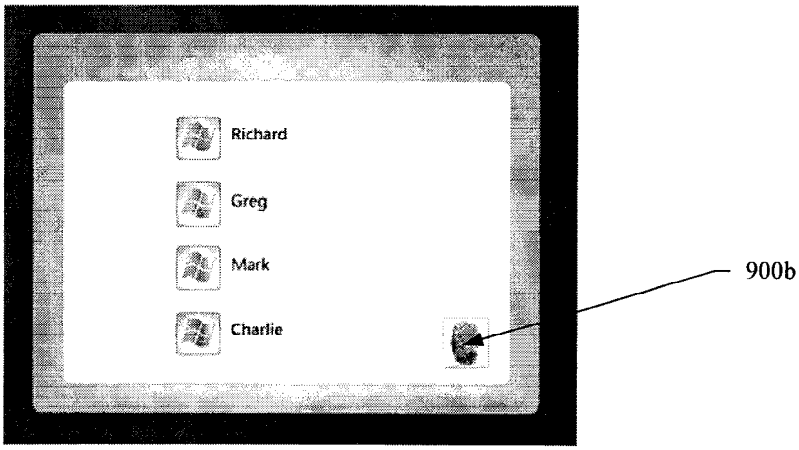
Фиг. 8a



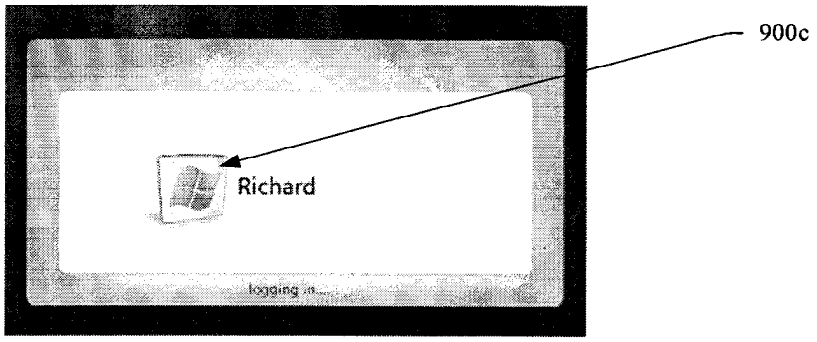
Фиг. 8b



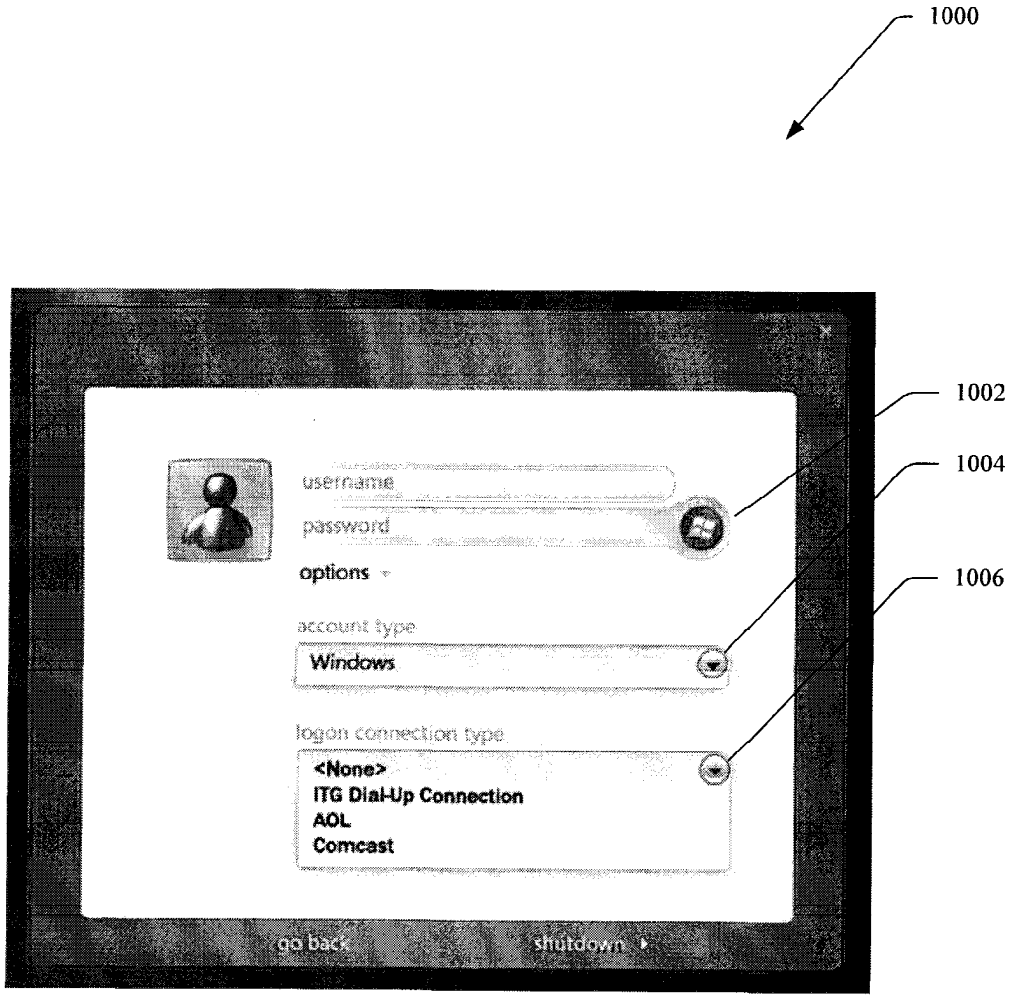
Фиг. 9a



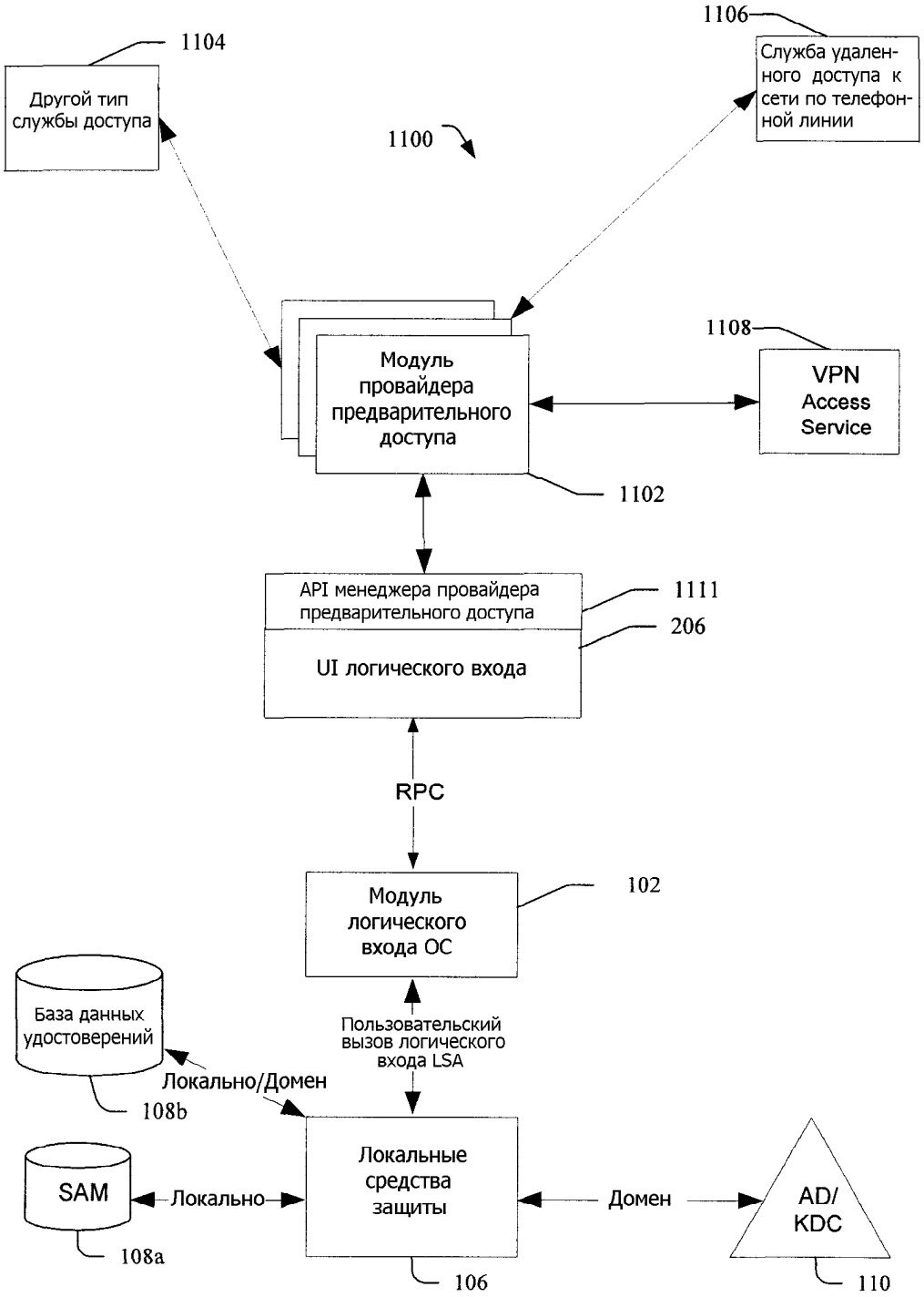
Фиг. 9b


900c
Richard
logging in...

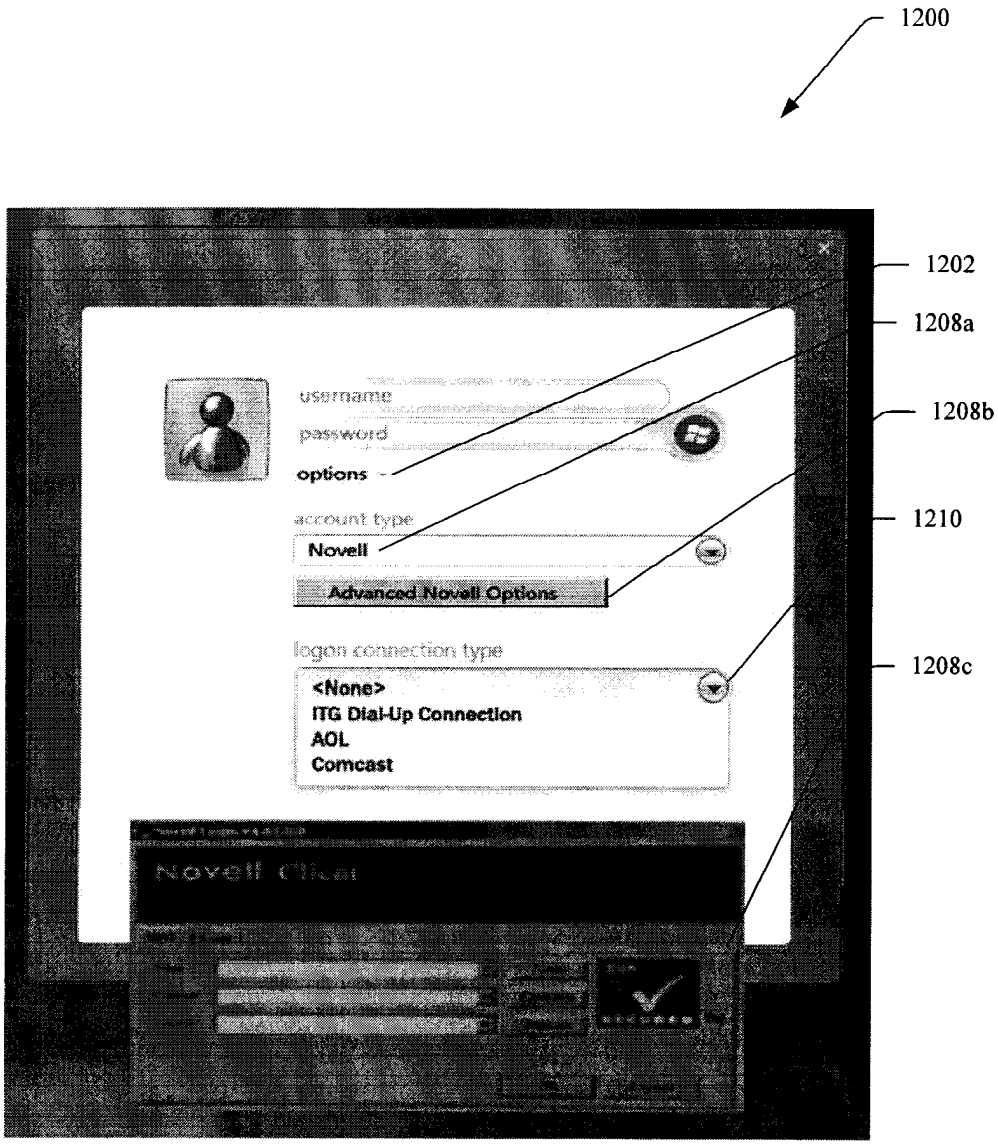
Фиг.9с


1000
1002
1004
1006
username
password
options
account type
Windows
logon connection type
<None>
ITG Dial-Up Connection
AOL
Comcast
go back
shutdown

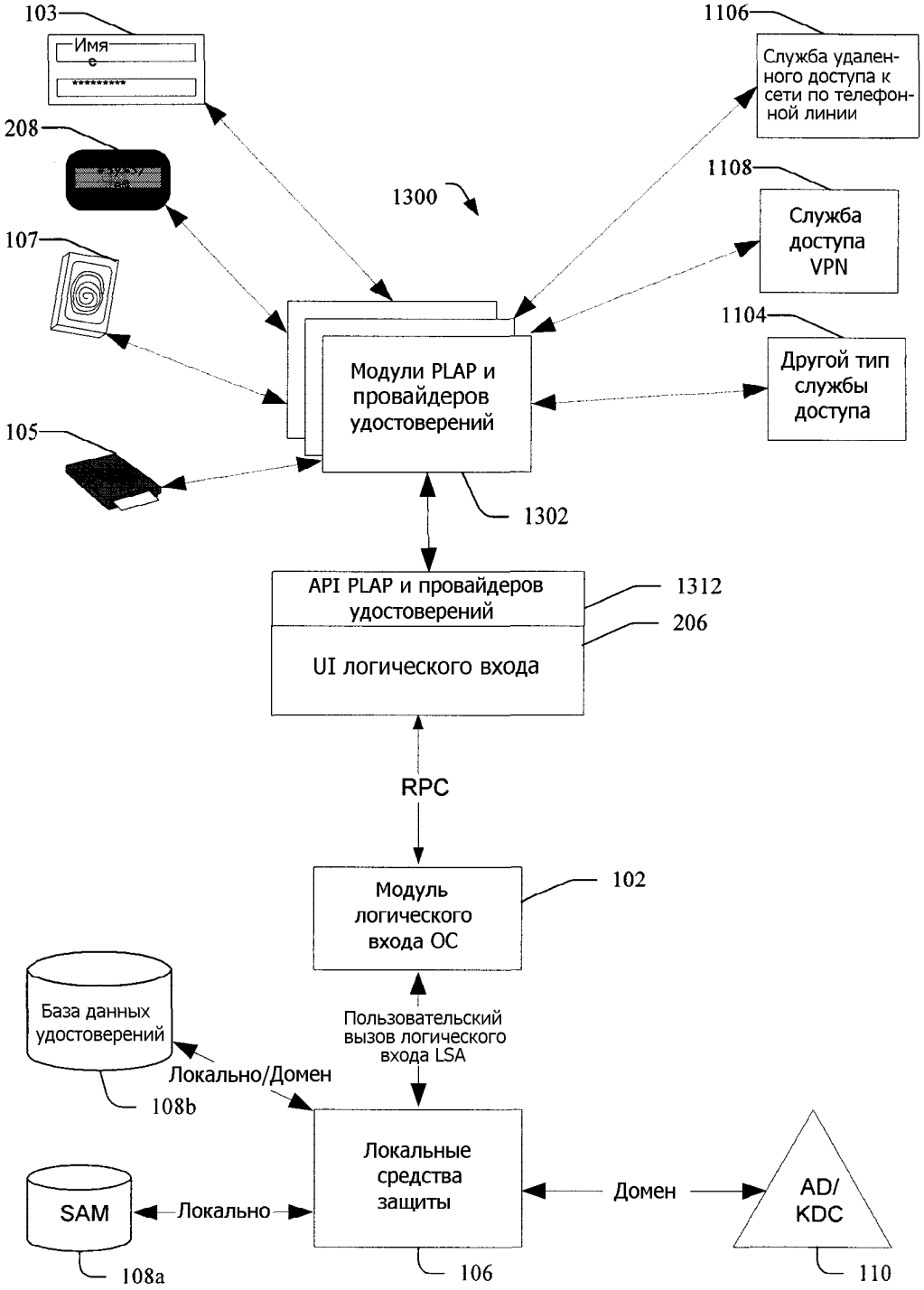
Фиг. 10


1106
Служба удаленного доступа к сети по телефонной линии
1104
Другой тип службы доступа
1100
Модуль провайдера предварительного доступа
1108
VPN Access Service
1102
API менеджера провайдера предварительного доступа
1111
206
UI логического входа
RPC
Модуль логического входа ОС
102
База данных удостоверений
Пользовательский вызов логического входа LSA
Локально/Домен
108b
SAM
Локально
Локальные средства защиты
Домен
AD/ KDC
108a
106
110

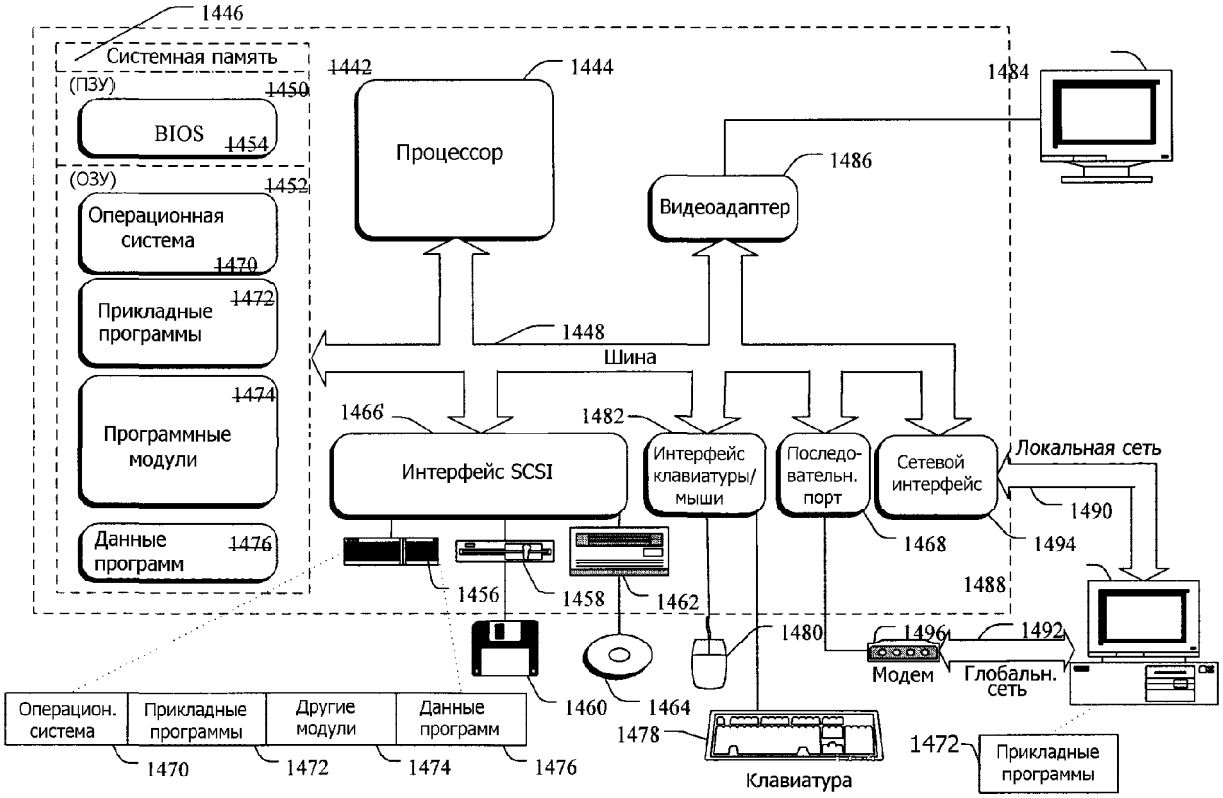
Фиг. 11


1200
1202
1208a
1208b
1210
1208c
username
password
options
account type
Novell
Advanced Novell Options
logon connection type
<None>
ITG Dial-Up Connection
AOL
Comcast
Novell Client

Фиг. 12


103
Имя
****
208
107
105
1300
1106
Служба удаленного доступа к сети по телефонной линии
1108
Служба доступа VPN
1104
Другой тип службы доступа
Модули PLAP и провайдеров удостоверений
1302
API PLAP и провайдеров удостоверений
1312
206
UI логического входа
RPC
Модуль логического входа ОС
102
База данных удостоверений
Пользовательский вызов логического входа LSA
Локально/Домен
108b
Локальные средства защиты
Домен
AD/ KDC
SAM
Локально
108a
106
110

Фиг. 13


1446
Системная память
(ПЗУ)
1450
BIOS
1454
(ОЗУ)
1452
Операционная система
1470
Прикладные программы
1472
Программные модули
1474
Данные программ
1476
1442
1444
Процессор
1484
1486
Видеоадаптер
1448
Шина
1466
1482
Интерфейс SCSI
Интерфейс клавиатуры/ мыши
Последо-вательн. порт
Сетевой интерфейс
Локальная сеть
1490
1468
1494
1488
1456
1458
1462
1480
1496
1492
Модем
Глобальн. сеть
Операцион. система
Прикладные программы
Другие модули
Данные программ
1460
1464
1478
1470
1472
1474
1476
Клавиатура
1472
Прикладные программы

Фиг. 14