РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 636 105**(13) **C1**

(51) МПК
G06F 21/33 (2013.01)
G06F 15/16 (2006.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2016110793, 28.09.2012**

(24) Дата начала отсчета срока действия патента:
28.09.2012

Дата регистрации:
20.11.2017

Приоритет(ы):
(30) Конвенционный приоритет:
29.09.2011 US 13/248,962;
29.09.2011 US 13/248,953;
29.09.2011 US 13/248,973
Номер и дата приоритета первоначальной заявки, из которой данная заявка выделена:
2014117153 29.09.2011

(45) Опубликовано: **20.11.2017** Бюл. № **32**

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

(72) Автор(ы):
РОТ Грегори Б. (US),
БЕХМ Брэдли Джеффри (US),
КРАХЕН Эрик Д. (US),
ИЛАК Кристиан М. (US),
ФИТЧ Натан Р. (US),
БРАНДУАЙН Эрик Джейсон (US),
О`НЕЙЛЛ Кевин Росс (US)

(73) Патентообладатель(и):
АМАЗОН ТЕКНОЛОДЖИС, ИНК. (US)

(56) Список документов, цитированных в отчете о поиске: **US 5956404 A, 21.09.1999. US 6601172 B1, 29.07.2003. US 2003/0120940 A1, 26.06.2003. US 2004/0172535 A1, 02.09.2004. US 2007/0234410 A1, 04.10.2007.**

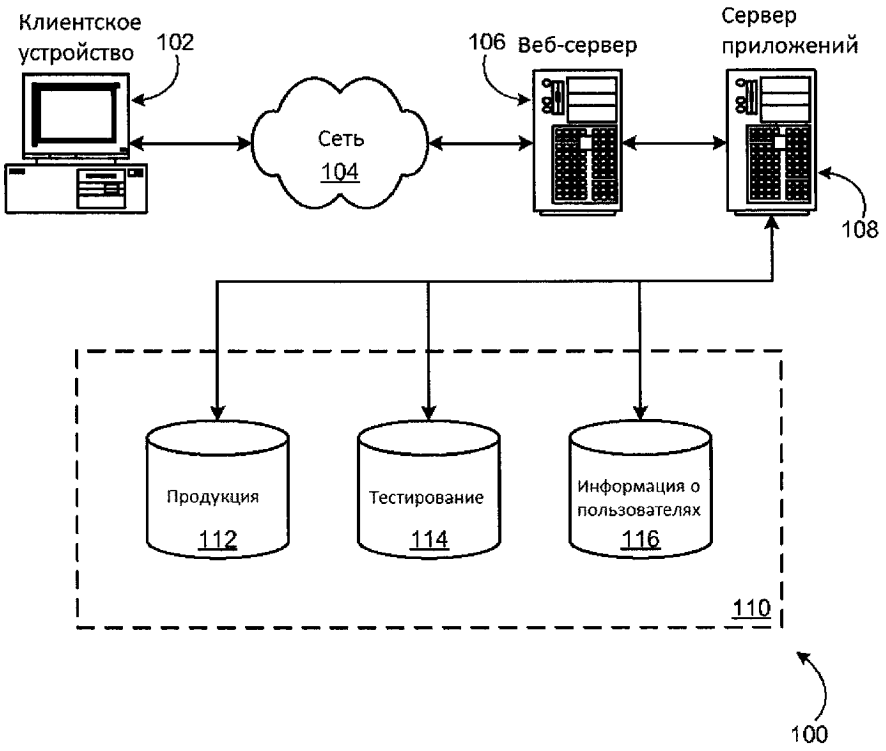
(54) ФОРМИРОВАНИЕ КЛЮЧА В ЗАВИСИМОСТИ ОТ ПАРАМЕТРА

(57) Реферат:

Изобретение относится к области аутентификации пользователей. Технический результат – эффективное управление безопасностью вычислительных ресурсов. Способ управления доступом к одному или более вычислительным ресурсам провайдера вычислительных ресурсов содержит: под управлением одной или более компьютерных систем, функционирующих на основе выполняемых команд, прием от первого объекта запроса делегирования, выполнение которого включает в себя разрешение второму объекту привилегии доступа к вычислительному ресурсу; генерирование ключа сеанса на основе, по меньшей мере частично, ограничения и секретного сертификата, совместно используемого с первым объектом; предоставление ключа сеанса первому объекту; прием от второго объекта запроса доступа на осуществление доступа к вычислительному ресурсу, причем запрос доступа включает в себя ключ сеанса, предоставленный первому объекту; подтверждение запроса доступа на основе, по меньшей мере частично, ключа сеанса, содержащегося в запросе доступа; и разрешение второму объекту доступа к вычислительному ресурсу. 3 н. и 17 з.п. ф-лы, 24 ил.

RU 2636105 C1

RU 2636105 C1



ФИГ.1

RU 2636105 C1

RU 2636105 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 636 105**(13) **C1**

(51) Int. Cl.
G06F 21/33 (2013.01)
G06F 15/16 (2006.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2016110793, 28.09.2012**

(24) Effective date for property rights:
28.09.2012

Registration date:
20.11.2017

Priority:
(30) Convention priority:
29.09.2011 US 13/248,962;
29.09.2011 US 13/248,953;
29.09.2011 US 13/248,973
Number and date of priority of the initial application, from which the given application is allocated:
2014117153 29.09.2011

(45) Date of publication: **20.11.2017** Bull. № **32**

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

(72) Inventor(s):
ROT Gregori B. (US),
BEKHM Bredli Dzheffri (US),
KRAKHEN Erik D. (US),
ILAK Kristian M. (US),
FITCH Natan R. (US),
BRANDUAJN Erik Dzhejson (US),
O`NEJLL Kevin Ross (US)

(73) Proprietor(s):
AMAZON TEKNOLODZHIS, INK. (US)

(54) KEY FORMATION DEPENDING ON PARAMETER

(57) Abstract:

FIELD: information technology.

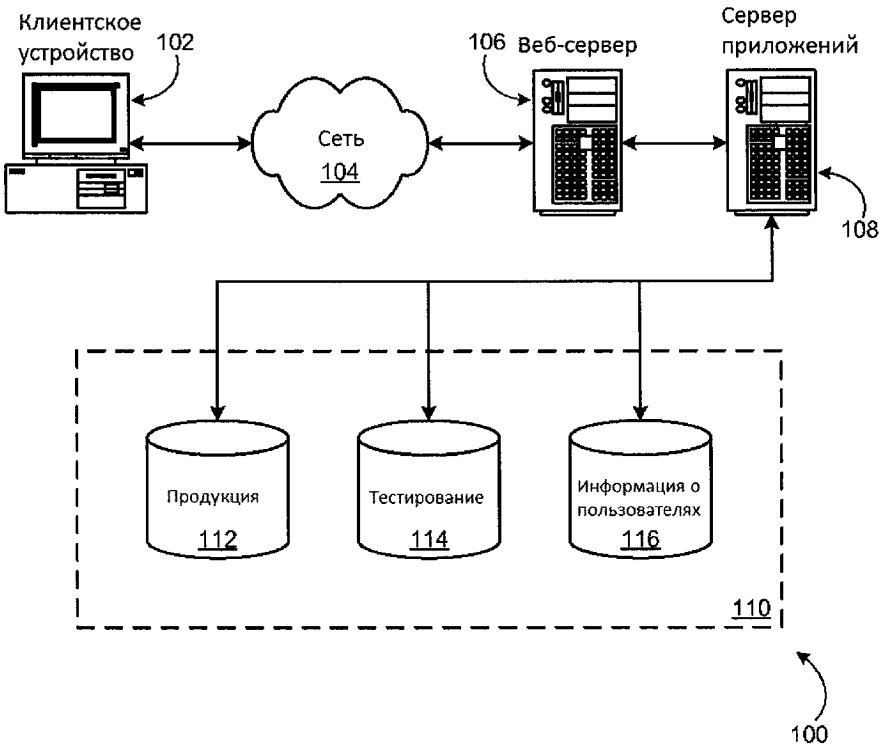
SUBSTANCE: method for controlling access to one or more computing resources of a provider of computing resources comprises: receiving, under the control of one or more computer systems operating on the basis of executable instructions, the first delegation request object, the execution of which includes permitting the second entity to gain access to the computing resource; generating a session key based, at least, in part, on the restriction and secret certificate shared with the first entity; providing the session key to the first object; receiving a request access from the second object to access the computing resource. The access request includes a session key provided to the first entity; acknowledgment of the access request based, at least, in part, on the session key contained in the access request; and allowing the second object to access the computing resource.

EFFECT: effective controlling the safety of computing resources.

20 cl, 24 dwg

RU 2636105 C1

RU 2636105 C1



ФИГ.1

RU 2636105 C1

RU 2636105 C1

ПЕРЕКРЕСТНЫЕ ССЫЛКИ НА РОДСТВЕННЫЕ ЗАЯВКИ

[0001] Данная заявка заявляет приоритет на основании заявок на патент США: № 13/248962, поданной 29 сентября 2011, озаглавленной “ФОРМИРОВАНИЕ КЛЮЧА НА ОСНОВАНИИ ПАРАМЕТРА ОБЪЕКТА” (Attorney Docket № 90204-813889 (029400PC)); № 13/248953, поданной 29 сентября 2011, озаглавленной “АЛГОРИТМЫ ДЛЯ СЕАНСОВ, СОЗДАННЫХ КЛИЕНТОМ” (Attorney Docket №. 90204-818478 (032300US)); и № 13/248973, поданной 29 сентября 2011, озаглавленной “АЛГОРИТМЫ ФОРМИРОВАНИЯ КЛЮЧА” (Attorney Docket № 90204-813890 (029500US)), полное раскрытие которых включается в данную заявку посредством ссылки.

УРОВЕНЬ ТЕХНИКИ

[0002] Существует множество разновидностей вычислительных сред. Например, часто организации для предоставления своим пользователям множества функциональных сервисов используют сети вычислительных устройств. Часто сети покрывают множество географических границ и соединяются с другими сетями. Например, для обеспечения своей работы организации могут использовать как внутренние сети вычислительных ресурсов, так и вычислительные ресурсы, управляемые сторонними организациями. Так, принадлежащие организации компьютеры могут обмениваться данными с компьютерами других организаций, осуществляя доступ и/или предоставляя данные для пользования сервисами другой организации. В большинстве случаев для настройки и обслуживания удаленных сетей организации используют аппаратные средства, управляемые другими организациями, благодаря чему снижаются затраты на инфраструктуру и достигаются другие преимущества.

[0003] Наряду с тем что различные вычислительные среды хорошо себя зарекомендовали для широкого спектра применения, использование таких сред вызывает множество сложных проблем. Например, настройка конфигурации компьютерных ресурсов для достижения целей одной организации может отрицательно сказываться на достижении целей другой организацией. К примеру, эффективное управление безопасностью вычислительных ресурсов часто достигается за счет эффективности доступа к данным и сервисам. Очень сложно достичь баланса между целями безопасности и эффективности, поскольку это требует значительных усилий и затрат ресурсов.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0004] Фиг. 1 иллюстрирует пример вычислительной среды, которая может использоваться для реализации различных аспектов настоящего изобретения, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0005] Фиг. 2 иллюстрирует пример среды, содержащей вычислительный ресурс провайдера, управляющий множеством зон отказа, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0006] Фиг. 3 иллюстрирует пример вычислительной среды внутри зоны отказа, показанной на Фиг. 2, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0007] Фиг. 4 иллюстрирует пример конфигурации вычислительного ресурса, которая может использоваться для обеспечения вычислительной среды, такой как вычислительная среда, показанная на Фиг. 3, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0008] Фиг. 5 иллюстрирует схему, поясняющую типичный способ, в котором различные элементы, задействованные в вычислительной среде, могут быть наделены разным объемом полномочий, по меньшей мере, в соответствии с одним вариантом

реализации изобретения;

[0009] Фиг. 6 иллюстрирует схему, поясняющую типовой способ, в котором информация может передаваться между сторонами аутентификации, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0010] Фиг. 7 представляет собой структурную схему, поясняющую пример процесса подписывания сообщений, в соответствии с вариантом реализации;

[0011] Фиг. 8 представляет собой структурную схему процесса проверки подписи, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0012] Фиг. 9 иллюстрирует схему типового способа распределения ключей, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0013] Фиг. 10 иллюстрирует схему использования типового способа распределения ключей в способе, который обеспечивает разные объемы полномочий, в соответствии, по меньшей мере, с одним вариантом реализации изобретения;

[0014] Фиг. 11 иллюстрирует структурную схему процесса формирования ключа, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0015] Фиг. 12 иллюстрирует схему формирования множественно-ограниченного ключа, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0016] Фиг. 13 иллюстрирует наглядный пример функциидля получения подписи, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0017] Фиг. 14 иллюстрирует пример того, как может быть реализовано и использовано получение множественного ключа, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0018] Фиг. 15 иллюстрирует схему, поясняющую типовой способ, при помощи которого могут быть получены ключи, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0019] Фиг. 16 иллюстрирует схему, поясняющую другой типовой способ, при помощи которого могут быть получены ключи, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0020] Фиг. 17 иллюстрирует схему, поясняющую еще один типовой способ, при помощи которого могут быть получены ключи, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0021] Фиг. 18 иллюстрирует структурную схему, поясняющую процесс инициализации сеанса, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0022] Фиг. 19 иллюстрирует структурную схему, поясняющую процесс генерации сеансового ключа, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0023] Фиг. 20 иллюстрирует структурную схему, поясняющую процесс получения доступа к одному или более вычислительным ресурсам во время сеанса, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0024] Фиг. 21 иллюстрирует структурную схему, поясняющую процесс принятия решения о предоставлении запрашиваемого доступа к одному или более вычислительным ресурсам, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0025] Фиг. 22 иллюстрирует структурную схему, поясняющую процесс делегирования полномочий, по меньшей мере, в соответствии с одним вариантом реализации изобретения;

[0026] Фиг. 23 иллюстрирует схему, поясняющую процесс множественного делегирования полномочий, по меньшей мере, в соответствии с одним вариантом

реализации изобретения; и

[0027] Фиг. 24 иллюстрирует схему, поясняющую способ, посредством которого могут быть получены ключи при помощи ключей с множественными полномочиями.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0028] В следующем описании будет рассмотрен ряд вариантов реализации изобретения. Особые конфигурации и подробности изложены в порядке, необходимом для предоставления всестороннего понимания реализации изобретения. При этом для специалистов в данной области будет очевидным, что изобретение может быть реализовано на практике без конкретных подробностей. Кроме того, с целью облегчения понимания описываемой реализации изобретения общеизвестные особенности могут быть опущены или упрощены.

[0029] Алгоритмы, описанные и предложенные в данной заявке, включают системы и способы для генерации ключа, соответственно различным реализациям изобретения. Ключи могут быть использованы для различных целей, таких как аутентификация и участие в схемах подписывания сообщений. В реализации изобретения вычислительные ресурсы провайдера предоставляют пользователям вычислительные сервисы, основанные, по меньшей мере, частично на электронных запросах, принятых от пользовательских устройств, использующих сервисы. Сервисом может быть любая подходящая служба, включая, но не ограничиваясь, доступ к данным, доступ к выполняющим операции вычислительным ресурсам, доступ к сервисам хранения данных и тому подобное.

[0030] Для того чтобы убедиться, что эти сервисы предоставляются с должной безопасностью, в различных реализациях настоящего раскрытия изобретения используются алгоритмы аутентификации запросов (также именуемых как «сообщения») для того, чтобы удостовериться в подлинности запросов. Согласно реализации изобретения аутентификация запросов реализована при помощи алгоритма хэш-кода аутентификации сообщения (HMAC) или другого подходящего алгоритма, как подробно описано ниже.

[0031] Согласно реализации изобретения оба стороны процесса аутентификации (например, пользователи служб или сторона, действующая в интересах пользователя) и аутентификатор (например, провайдер услуг или сторона, действующая в интересах провайдера) совместно используют секретный сертификат, который может именоваться как ключ. Аутентификатор может хранить совместно используемые секретные сертификаты для множества пользователей. Как часть транзакции, проводящая аутентификацию сторона может подписывать запросы, используя совместно используемый секретный сертификат, тем самым создавая подпись. Подпись аутентификатору может быть предоставлена с запросами. Аутентификатор может использовать собственную копию совместно используемого секретного сертификата, чтобы генерировать подпись для принятых запросов и принимать решение, были ли запросы подписаны при помощи совместно используемого секретного сертификата, сравнивая, соответствует ли генерируемая подпись принятой (например, будут ли подписи идентичны). Если принято решение, что запросы подписаны при помощи совместно используемого секретного сертификата, запросы могут считаться подлинными и, следовательно, принимается решение, что запросы должны быть удовлетворены.

[0032] Из-за того что вышеуказанное взаимодействие является симметричным (т.е. сторона аутентификации при выполнении своих ролей используют общую информацию), совместно используемые секретные сертификаты, хранящиеся в аутентификаторе, могут использоваться для того, чтобы аутентифицировать обе стороны процесса

аутентификации или действовать от их имени. Как следствие, для защиты этих сертификатов желательна высокая степень безопасности. Обеспечение высокой степени безопасности может негативно сказаться на производительности и доступности системы. Например, обеспечение высокой степени безопасности может подразумевать обслуживание централизованной системы хранения ключа. Однако такая централизованная система может привести к образованию «узкого места», так как увеличение числа пользователей и/или сервисов служит причиной большей нагрузки на централизованную систему. Если такая централизованная система выходит из строя, аутентифицировать запросы может быть трудно или невозможно. Следовательно, централизация приводит одновременно к преимуществам в отношении безопасности и к недостаткам в отношении масштабируемости и доступности сервисов.

[0033] В реализации изобретения негативные последствия таких систем (и других систем) минимизированы с помощью протокола подписи, который основывается на артефактах совместно используемого секретного сертификата, используемых для подтверждения того, что аутентифицируемая часть содержит совместно используемый секретный сертификат и, следовательно, подходит для получения авторизованного доступа, определенного в подписанных с помощью артефактов запросах. В реализации изобретения такие артефакты получены путем конфигурирования компьютерных систем аутентификации таким образом, чтобы принимать в качестве подписи величину, основанную, по меньшей мере, на части полученного совместно используемого сертификата, вместо самого совместно используемого сертификата. Формирование совместно используемого сертификата возможно при условии, чтобы на практике было невозможно определить совместно используемый сертификат, как это более подробно описано ниже.

[0034] Например, в реализации изобретения стороны процесса аутентификации могут ставить подпись, согласно:

HMAC(M, HMAC(X, сертификат)),

где M - это сообщение, а HMAC(X, сертификат) - это артефакт, полученный из общедоступного секретного сертификата. Величина X может иметь некоторое значение, известное двум сторонам процесса аутентификации и аутентификатору, и может быть совместно используемой. Например, X может быть текущей датой, кодированной заранее определенным образом, чтобы убедиться, что HMAC(X, сертификат) вычисляется соответственно стороной процесса аутентификации и аутентификатором. В качестве другого примера, X может быть идентификатором службы, с которой может использоваться артефакт. В качестве еще одного примера, X может кодироваться множеством семантических значений и представляться таким образом, что обе стороны процесса аутентификации и аутентификатор соответственно вычисляют артефакт. Семантическое значение может быть ограничением на использование ключа, включая значение, показывающее, что не нужно использовать полученную форму представления ключа. В случае комбинации предыдущих примеров настоящего абзаца X может кодироваться как «20110825/DDS», где последовательность слева от косой черты представляет дату, а последовательность справа от косой черты представляет название службы, с которой используется артефакт, вычисленный с X. В большинстве случаев X может быть любой величиной или набором величин, кодированных соответственно для двух сторон процесса аутентификации и аутентификатора. Следует заметить, что могут быть также использованы другие подходящие функции, отличные от функций HMAC, как описано ниже.

[0035] Вернемся к примеру использования функции HMAC в реализации изобретения,

величины для X выбираются так, чтобы обеспечить дополнительные преимущества. Как отмечалось, X может (но не обязательно) соответствовать одному или более семантическим значениям. В реализации изобретения используются семантические значения, такие как временные метки, названия служб, идентификаторы округов, и тому подобное, чтобы предоставить систему, в которой получены артефакты, в соответствии с алгоритмами настоящей реализации изобретения, соответствующими ограничениям на использование полученных из X ключей. Таким образом, даже несмотря на взлом генерированных ключей, который может сделать доступной аутентификацию для нежелательных сторон, ограничение с использованием кодированных ключей создает возможность минимизации отрицательных последствий, в случае когда ключи взломаны. Например, временные ограничения используются для получения ключей, чтобы обеспечить системе возможность эффективной проверки, была ли предложенная подпись сделана с ключом, который был действительным во время добавления подписи. В качестве конкретного примера, если для получения ключа используется текущая дата, и система аутентификации принимает только подписи, представленные текущей датой, система аутентификации примет решение, что подписи, генерированные при помощи ключей, полученных из дат, отличающихся от текущей, являются недействительными. Подобным образом ключ, полученный из идентификатора некоторой службы, может быть недействительным для использования с другой службой. Ниже приводятся другие примеры.

[0036] Как было отмечено, различные алгоритмы настоящего раскрытия сущности изобретения для получения ключей позволяют использовать набор параметров. В реализации изобретения ключи получаются из набора параметров посредством многократного использования функции HMAC. Например, ключ может быть вычислен следующим образом:

$K_S=HMAC(...HMAC(HMAC(HMAC(K, P_1), P_2), P_3)..., P_N)$,

где K является совместно используемым секретным сертификатом, а P_i являются параметрами. Ключ, K_S, может быть использован для генерации подписи, например:

$S=HMAC(K_S,M)$,

где M - это сообщение, которое может быть канонизированным. Таким образом, принимая во внимание частные производные ключа для доступа к различным компонентам распределенной вычислительной системы, ключ получается многоуровневым. Например, $K_{P1}=HMAC(K, P_1)$ может быть вычислен и получен доступ к одному или более компонентам распределенной вычислительной системы. Компоненты, принимающие K_{P1}, могут вычислить $K_{P2}=HMAC(K_{P1}, P_2)$, где P_2 может быть одинаковым для каждого компонента или различным для некоторых или для всех компонентов. Величины K_{P2}, вычисленные различными компонентами, могут передавать вычисления другим компонентам распределенной вычислительной системы, которые могут вычислить $K_{P3}=HMAC(K_{P2}, P_3)$. Каждый компонент может помещать в кэш-память результаты вычислений, а также возможные результаты, вычисленные другими компонентами. Таким образом, может быть обеспечена более высокая степень защиты на протяжении всего процесса хранения данных, хранящего совместно используемые секретные ключи, поскольку вычисление производных ключей может быть выполнено другими компонентами распределенной вычислительной системы.

[0037] Алгоритмы настоящего раскрытия сущности изобретения также предусматривают инициацию сеансов. Например, как уже было сказано, для получения

ключа могут быть использованы совместно используемый секретный сертификат и один или более параметров. Соответственно, параметры для сеанса могут использоваться для генерации сертификата, который может использоваться во время этого сеанса. Сертификат может использоваться пользователем, запрашивающим сертификат, или, в некоторых реализациях изобретения, пользователем, которому был передан сертификат и право доступа к одному или более вычислительным ресурсам. В таких случаях, из-за того что объект делегирования такого доступа использует ключ, полученный из совместно используемого секретного сертификата, но не сам совместно используемый секретный сертификат, поддерживается высокая степень защиты и нет необходимости менять совместно используемый секретный сертификат для предотвращения будущего его использования объектом делегирования. Как более детально описано ниже, объекты делегирования могут также становиться делегаторами, используя алгоритмы настоящего раскрытия изобретения, многие из которых более детально описаны ниже.

[0038] Фиг. 1 иллюстрирует аспекты типовой вычислительной среды 100 для реализации аспектов настоящего раскрытия сущности изобретения согласно различным вариантам реализации. Следует иметь в виду, что, хотя в целях пояснения используется вычислительная среда на основе веб-технологии, для различных вариантов реализации изобретения соответствующим образом могут использоваться другие вычислительные среды. Вычислительная среда включает электронное клиентское устройство 102, содержащее любое подходящее устройство, пригодное для отправки и получения запросов, сообщений или информации, посредством подходящей сети 104 и для отправки информации пользователю устройства. Примерами таких клиентских устройств могут быть персональные компьютеры, мобильные телефоны, портативные устройства для обмена сообщениями, переносные компьютеры, декодеры каналов кабельного телевидения, КПК, электронные книги и тому подобное. Сетью может быть любая подходящая сеть, включая интранет, интернет, сеть сотовой связи, локальная вычислительная сеть, или любая другая подобная сеть или их комбинации. Выбор используемых компонентов для таких систем может зависеть, по меньшей мере, в некоторой степени от типа сети и/или выбранной вычислительной среды. Протоколы и компоненты для передачи данных посредством такой сети являются общеизвестными и в этой заявке подробно рассматриваться не будут. Передача данных по сети может осуществляться при помощи проводных или беспроводных подключений или их комбинации. В данном примере в качестве сети используется интернет, веб-сервер 106 используется в качестве вычислительной среды для получения запросов и обслуживания ответной информации, хотя очевидно, что альтернативное устройство, служащее аналогичной цели для других сетей, может использоваться обычным для специалиста в данной области образом.

[0039] Типичная вычислительная среда содержит, по меньшей мере, один сервер приложений 108 и хранилище данных 110. Следует понимать, что может быть несколько серверов приложений, уровней или других элементов, процессов или компонентов, которые могут быть включены последовательно или скомпонованы иным образом и могут взаимодействовать друг с другом для выполнения задач, таких как получение данных из соответствующего хранилища данных. Используемый в данной заявке термин "хранилище данных" относится к любому устройству или комбинации устройств, способных хранить, организовывать доступ и извлекать данные, которые могут содержать любую комбинацию и количество серверов данных, баз данных, устройств хранения данных и носителей информации в любой стандартной, распределенной или

кластерной вычислительной среде. Сервер приложений может содержать любое соответствующее аппаратное и программное обеспечение для интеграции с хранилищем данных, насколько это необходимо для выполнения аспектов одного или более приложений клиентского устройства, обработки множества доступов к данным и бизнес-логики приложений. Сервер приложений обеспечивает доступ управляющих служб при взаимодействии с хранилищем данных и может генерировать информацию, такую как текст, графика, звук и/или видео, передаваемую пользователю при помощи веб-сервера в виде HTML, XML или другого языка, имеющего структуру, подходящую для данного примера. Обработка всех запросов и ответов, а также доставка информации между клиентским устройством 102 и сервером приложений 108, может обрабатываться веб-сервером. Следует понимать, использование веб-серверов и серверов приложений не обязательно, и они являются только типовыми компонентами, поскольку описанный в настоящей заявке структурированный код может выполняться на любом подходящем устройстве или хост-машине, как описано в данной заявке.

[0040] Хранилище данных 110 может содержать несколько отдельных таблиц данных, базы данных или другие механизмы хранения данных, также носитель информации для хранения данных, применительно к тем или иным аспектам изобретения. Например, описанное хранилище данных содержит механизмы для хранения производственных данных 112 и пользовательской информации 116, которая может использоваться для обработки информации о производственной деятельности. Также показано, что хранилище данных содержит механизм для хранения данных журнала событий 114, который может использоваться для отчета, анализа или для других подобных целей. Нужно понимать, что могут иметь место многие другие аспекты, которые, возможно, понадобится хранить в хранилище данных, например, страницу графической информации, и предоставлять информацию о правах доступа, которая может храниться при необходимости в любом из описанных выше механизмов или в дополнительных механизмах в хранилище данных 110. Хранилище данных 110 может использоваться при помощи логической связи с ним для получения команд из сервера приложений 108, а также получения, обновления или обработки других данных в ответ на его запрос. В одном примере пользователь может принять поисковый запрос для элемента определенного вида. В этом случае хранилище данных может предоставлять доступ к пользовательской информации, проверяя подлинность пользователя, и может предоставить доступ к каталогу детальной информации для получения информации об элементах данного типа. Затем информация может быть возвращена пользователю, например, результаты листинга на веб-странице, которые пользователь может просматривать при помощи браузера на пользовательском устройстве 102. Интересующая пользователя информация может быть просмотрена на отдельной странице или в окне браузера.

[0041] Обычно каждый сервер содержит операционную систему, обеспечивающую выполнение программных команд для общего администрирования и работы такого сервера, и, как правило, содержит машиночитаемый носитель информации (например, накопитель на жестком диске, оперативное запоминающее устройство, постоянное запоминающее устройство и т.д.), в котором хранятся команды, которые при выполнении процессором сервера позволяют серверу выполнять его функции. Соответствующие реализации операционной системы и общей функциональности серверов известны или доступны для приобретения и быстро реализуются специалистами в данной области, особенно в свете раскрытия настоящей заявки.

[0042] Вычислительная среда в одном из вариантов реализации изобретения является

распределенной вычислительной средой, использующей несколько компьютерных систем и компонентов, которые взаимосвязаны через линии связи, используя одну или более компьютерную сеть или прямые подключения. Однако специалистам в данной области ясно, что такая система могла бы работать с тем же успехом в системе, имеющей меньшее или большее количество компонентов, изображенных на Фиг. 1. Следовательно, изображение системы 100 на Фиг. 1 следует принимать, как являющееся по своему характеру иллюстративным и не ограничивающимся рамками раскрытия сущности изобретения.

[0043] Фиг. 2 иллюстрирует наглядный пример вычислительной среды 200, включающей вычислительный ресурс провайдера 202, который управляет множеством зон отказа 204, в соответствии, по меньшей мере, с одним вариантом реализации изобретения. В реализации изобретения вычислительный ресурс провайдера является организацией, которая управляет компьютерными аппаратными средствами в интересах одного или более пользователей 206. Вычислительный ресурс провайдера может предоставлять вычислительные ресурсы различным образом. Например, в реализации изобретения вычислительный ресурс провайдера 202 управляет аппаратным средством, которое конфигурировано для использования пользователями 206. Вычислительный ресурс провайдера 202 предоставляет интерфейс, позволяющий пользователям 206 программным путем конфигурировать вычислительные ресурсы используемых аппаратных средств. Например, вычислительный ресурс провайдера может администрировать аппаратные средства серверов, которые управляют виртуальными компьютерными системами, программно управляемыми пользователем. В другом примере вычислительный ресурс провайдера 202 может управлять различными хранилищами данных, чтобы обеспечить удаленные решения для хранения данных, такие как высоконадежное хранилище данных и хранилище данных на уровне блоков.

[0044] В варианте реализации изобретения зона отказа - это совокупность вычислительных ресурсов, которые отделены одной или более границами отказа, так что каждая зона отказа является устойчивой к отказу другой зоны отказа. Как пример, каждая зона отказа 204 может быть отдельным дата-центром. Следовательно, если один дата-центр перестает работать, предположительно из-за отключения электропитания или другого деструктивного явления, то другой дата-центр может продолжать работу. Зоны отказа могут быть расположены в различных географических местоположениях, и некоторые или все из зон отказа могут быть отделены государственными границами. Например, две или более зон отказа могут располагаться в разных странах. Следует отметить, что в целях пояснения настоящее раскрытие изобретения снабжено многочисленными примерами, где зоны отказа являются дата-центрами. Однако зоны отказа могут быть определены множеством других способов. Например, отдельные комнаты в одном и том же дата-центре могут рассматриваться как отдельные зоны отказа, в согласии с различными вариантами реализации изобретения. В качестве другого примера, вычислительные ресурсы находятся в одном и том же месте, но получают электропитание от разных генераторов резервного электропитания и/или поддерживаются разными сетевыми ресурсами, таким образом они могут рассматриваться как разные зоны отказа. В качестве еще одного примера, дата-центры могут быть кластерными, так что каждый кластер дата-центра может рассматриваться как зона отказа. К тому же может быть много причин, по которым зона отказа может выйти из строя, включая причины, связанные с работой электросети, работой сети общего пользования, политическими событиями и другими причинами.

[0045] В данном варианте реализации изобретения пользователи 206 связываются с

вычислительными ресурсами провайдера 202 посредством сети 208, такой как интернет. Пользователи 206 могут иметь ресурсы, скомпонованные в одной или более зонах отказа 204, и могут связываться с ресурсами путем отправки электронных сообщений, таких как сообщения активации веб-сервиса интерфейса программирования приложений (API) вычислительного ресурса провайдера для того, чтобы конфигурировать ресурсы и управлять ими. Пользователи могут использовать ресурсы во многих зонах отказа для того, чтобы уменьшить влияние потенциальных неполадок, которые оказывают влияние на ресурсы пользователя. Пользователь, который использует вычислительные ресурсы провайдера 202 для работы с веб-сайтом с открытым доступом, например, может администрировать веб-сервер и другие серверы в отдельных зонах отказа, в таком случае если серверы в одной зоне отказа выходят из строя, пользователи будут получать доступ к веб-сайту благодаря доступу к серверам в другой зоне отказа.

[0046] Фиг. 3 иллюстрирует в качестве наглядного примера среду 300 внутри зоны отказа 302, которая может быть зоной отказа вычислительного ресурса провайдера, как показано на Фиг. 2. В данном варианте реализации изобретения зона отказа 302 содержит вычислительные ресурсы, используемые для предоставления различных сервисов в интересах пользователей. Например, как показано на Фиг. 3, зона отказа 302 содержит вычислительные ресурсы, используемые для предоставления службе долговременного хранения данных, которая может хранить довольно большие массивы данных с низкими эксплуатационными расходами и возможностью резервирования. Такой сервис может находить применение, когда необходимо хранение больших массивов данных и/или высокая безопасность хранения данных. Зона отказа 306 может также содержать службу хранения данных на уровне блоков 306, предоставляющую пользователям возможность пользоваться устройствами хранения данных на уровне блоков, физических устройств и/или виртуальных устройств. Например, пользователи могут подключать устройства хранения данных на уровне блоков к используемым ими компьютерным системам. Также показана служба виртуальной компьютерной системы 308, которая может предоставлять пользователям вычислительные сервисы. В данном варианте реализации изобретения служба виртуальной компьютерной системы 308 предоставляет пользователям сервисы путем реализации виртуальных компьютерных систем на физических серверах, администрируемых вычислительными ресурсами провайдера, хотя и возможны варианты, такие как местоположение физической компьютерной системы, выделенной для использования пользователям. В варианте реализации изобретения связанном с виртуальными компьютерными системами, пользователи, в зависимости от их потребностей, могут программно управлять виртуальными компьютерными системами. Например, как показано на Фиг. 3, пользователи могут конфигурировать виртуальные компьютерные системы службы виртуальной компьютерной системы 308 для обслуживания пользователей службы виртуальных вычислений провайдера. Виртуальные компьютерные системы, к примеру, могут быть сконфигурированы для работы с общедоступным веб-сайтом. Как пользователи виртуального вычислительного ресурса провайдера, так и пользователи этих пользователей в различных вариантах реализации изобретения могут иметь доступ к различным службам, выполняемым в зоне отказа 302 путем установления связи со службами, посредством сети 310, в качестве которой может быть сеть 208, описанная выше в связи с Фиг. 2.

[0047] Следует отметить, что различные варианты реализации изобретения, иллюстрированные на Фиг. 3, как и в случае всех вариантов, изображенных на фигурах и описанных в настоящей заявке, по своему характеру являются схематическими и

рассматриваются в рамках данного раскрытия сущности изобретения. Например, другие службы, отличные от показанных, могут быть представлены в зоне отказа 302 как дополнение или вместо показанных служб. Например, как показано многоточием на Фиг. 3, в зоне отказа 302 могут выполняться дополнительные службы. К тому же, некоторые службы могут использовать также и другие службы. Например, многие службы (такие как служба хранения данных на уровне блоков 306 и служба виртуальной компьютерной системы 308) могут использоваться совместно для обеспечения работы других служб, таких как служба реляционной базы данных, служба электронной почты и, как правило, вычислительной службы любого типа, которая обеспечивается за счет средств вычислительного ресурса провайдера.

[0048] Как показано на Фиг. 3, вычислительный ресурс провайдера может содержать отдельный верификатор 312 для каждой из служб. Верификатором может быть вычислительное устройство, совокупность вычислительных устройств, модуль приложения или другой ресурс, который проверяет различные удостоверения, сделанные пользователями и, возможно, другими компьютерными системами. В варианте реализации изобретения каждый верификатор 312 проверяет подписи сообщений, которые создаются согласно различным вариантам реализации настоящей заявки и затем предоставляются пользователями вместе с запросами на доступ к вычислительным ресурсам, как более подробно описано ниже. Ключи и другая важная информация может поступать к верификаторам из главного источника ключей, что позволяет верификаторам проверять информацию. Следует отметить, что каждая служба, имеющая верификатор, является наглядным примером конкретной реализации изобретения, так что другие конфигурации находятся в рамках настоящего раскрытия изобретения. Например, один верификатор может поддерживать множество служб или все службы и даже множество зон отказа.

[0049] Фиг. 4 иллюстрирует наглядный пример конфигурации вычислительного ресурса, которая может использоваться для обеспечения вычислительной среды, такой как вычислительная среда, показанная на Фиг. 3, по меньшей мере, в соответствии с одним вариантом реализации изобретения. Фиг. 4 иллюстрирует конкретный пример, в котором зоной отказа на Фиг. 3 является дата-центр. Таким образом, возвращаясь к Фиг. 4, дата-центр 402 может содержать множество серверных стоек 404-406. Дата-центр 402 является примером одного или более дата-центров, которые могут использоваться в различных реализациях настоящего раскрытия изобретения, как например, дата-центры, показанные на Фиг. 4. Многоточие между серверными стойками 404 и 406 показывает, что дата-центр 402 может включать любое необходимое количество серверных стоек, несмотря на то что для наглядности на Фиг. 4 показано только две. Каждая серверная стойка 404-406 может принимать участие в администрировании служб, таких как служба электропитания и служба передачи данных, для множества серверных компьютеров 408-414 и 416-422. Кроме того, многоточие показывает, что серверные стойки 404-406 могут содержать любое необходимое количество серверных компьютеров. Например, серверные компьютеры 408-422 могут включать один или более серверов виртуальных компьютерных систем (VCS) и/или один или более серверов хранения данных. Каждый из серверов 408-422 может соответствовать блоку выделенных ресурсов.

[0050] На Фиг. 4, каждая серверная стойка 404-406 изображена содержащей полку коммутаторов 424-426. Полка коммутаторов 424 и 426 может отвечать за коммутацию пакетов цифровых данных, поступающих и передаваемых в соответствующие комплексы серверных компьютеров 408-414 и 416-422. Полка коммутаторов 424-426 может быть

подключена к коммутационной матрице дата-центра 428 и затем к выбранным граничным маршрутизаторам 430, которые соединяют дата-центр 402 с одной или более компьютерными сетями, включая интернет. Коммутационная матрица может содержать любой необходимый комплект сетевых компонентов, включая взаимосвязанные коммутаторы 432-438 (для наглядности на Фиг. 4 показано только четыре) одного или более типов коммутации, упорядоченных в один или более уровней коммутации, наряду с маршрутизаторами, шлюзами, мостами, концентраторами, повторителями, межсетевыми экранами, компьютерами и их необходимыми соответствующими комбинациями. По меньшей мере, в одном варианте реализации изобретения полка коммутаторов 424-426 и граничный маршрутизатор 430 рассматриваются как часть коммутационной матрицы 428. Полка коммутаторов 424-426, граничный маршрутизатор 430 и компоненты коммутационной матрицы 428 являются примером сетевых аппаратных средств 224, показанных на Фиг. 2.

[0051] Как было отмечено, различные варианты реализации настоящего раскрытия изобретения создают возможность назначения различных уровней полномочий, установленных по разным причинам. Фиг. 5 иллюстрирует схему, поясняющую типовой способ, в котором различным элементам, задействованным в вычислительной среде, могут назначаться разные уровни полномочий, по меньшей мере, в соответствии с одним вариантом реализации изобретения. На Фиг. 5 показан вычислительный ресурс провайдера 502. Как проиллюстрировано Фиг. 5, в варианте реализации изобретения вычислительный ресурс провайдера 502 имеет полномочия выше, чем у принадлежащих ему ресурсов, и может распределять эти полномочия между различными пользователями ресурсов. Следует отметить, что в целях пояснения, согласующегося с другими чертежами и описаниями к ним, Фиг. 5 иллюстрирует вычислительные ресурсы провайдера 502, имеющие полномочия выше доменных. Однако вариант реализации данного раскрытия изобретения применим также к другим владельцам полномочий доменов. Например, владельцем полномочий может быть правительство или правительственная организация, ее подразделение или другая организация или, как правило, любой субъект с полномочиями над некоторым доменом.

[0052] Возвратимся к наглядному примеру, иллюстрируемому Фиг. 5, где вычислительные ресурсы провайдера 502 управляют его полномочиями, позволяя различным подразделениям субъектов иметь полномочия над различными поддоменами. Например, как проиллюстрировано фигурой, каждая из зон отказа 504 вычислительного ресурса провайдера представлена соответствующим поддоменом вычислительного ресурса домена провайдера 502. Следовательно, каждая зона отказа может иметь полномочия над своими собственными ресурсами, но не ресурсами другой зоны отказа (хотя в некоторых вариантах реализации полномочия над некоторыми поддоменами могут использоваться совместно). Следовательно, соответственно варианту реализации изобретения зона отказа может предоставить пользователю доступ к вычислительным ресурсам в зоне отказа, но не доступ к вычислительным ресурсам другой зоны отказа.

[0053] Как отмечалось выше, каждая зона отказа может содержать одну или более служб 506. Соответственно, как иллюстрирует Фиг. 5, каждая служба может отвечать за поддомен домена соответствующей зоны отказа 506. Следовательно, в варианте реализации изобретения служба может предоставлять доступ к ресурсам, доступным службе, но не к другим службам. Каждая служба может обслуживать одного или более пользователей 508, и, таким образом, каждый пользователь может отвечать за поддомен полномочий соответствующей службы 506. Следовательно, в реализации изобретения пользователь может предоставлять доступ к своим ресурсам, связанным с

соответствующей службой, но не к службе другого пользователя. В качестве конкретного наглядного примера рассмотрим случай, в котором служба является службой виртуального вычислительного ресурса, пользователь может предоставить доступ (например, общий доступ) к своим виртуальным компьютерным системам, но не к виртуальным компьютерным системам других пользователей без их разрешения.

[0054] Как отмечалось, частичная локализация полномочий, показанная на Фиг. 5, приведена для наглядности, и в рамках настоящего раскрытия сущности изобретения рассматриваются многочисленные варианты. Как отмечалось выше, варианты реализации настоящего раскрытия изобретения, применимые к доменам полномочий вне доменов, управляемых вычислительными ресурсами провайдера и поддоменами, и могут определяться в согласии с особыми потребностями и обстоятельствами. Также Фиг. 5 изображает пользователей виртуального ресурса провайдера, имеющих наименьший поддомен полномочий. При этом алгоритмы настоящего раскрытия изобретения могут позволить пользователю разделить домены на один или более поддоменов.

[0055] Ряд осуществлений настоящего раскрытия изобретения относится к подписям сообщений. На Фиг. 6 изображена схема 600, иллюстрирующая типовой способ, в котором информация между участниками может передаваться в процессе проверки подписи сообщения, по меньшей мере, в соответствии с одним вариантом реализации изобретения. В варианте реализации изобретения источник ключей 602 предоставляет ключ как отправителю сообщения 604, так и верификатору подписи 606. Источником ключей может быть компьютерная система, конфигурированная для предоставления ключей, по меньшей мере, отправителю сообщения 604 и верификатору подписи 606. Источник ключей также может генерировать ключи, используя различные алгоритмы, включая ряд описанных в настоящей заявке вариантов реализации, или получать ключ из другого источника. Отправителем сообщения 604 может быть компьютерная система, конфигурированная для отправки сообщения и подписи верификатору подписи 606 или другому компоненту, работающему вместе с верификатором подписи 606. Компьютерной системой отправителя сообщений 604 может быть, например, компьютерная система пользователя вычислительного ресурса провайдера. Верификатором подписи 606 может быть компьютерная система, конфигурированная для получения сообщений и подписей, а также анализа подписи, чтобы проверить, какое сообщение является достоверным, как описано ниже. Верификатор подписи 606 может анализировать полученную подпись и сообщение для принятия решения была ли подпись генерирована при помощи достоверного ключа K. Следует заметить, что в то время, как Фиг. 6 иллюстрирует источник ключей 602 отдельно от отправителя сообщения 604 и верификатора подписи 606, источником ключей может быть также отправитель сообщения или верификатор подписи. Например, пользователи компьютерного ресурса провайдера могут предоставлять свои собственные ключи. Ключи пользователя затем могут предоставляться верификатору подписи для проверки подписей. К тому же, получатель сообщения 604 и верификатор подписи 606 могут получать разные ключи от источника ключей 602. Например, и получатель сообщения 604, и верификатор подписи 606 могут получить ключ, извлеченный из ключа присланного отправителю сообщения 604, при помощи различных вариантов реализации настоящего раскрытия сущности изобретения.

[0056] Как показано на Фиг. 6, верификатор подписи 606 получает сообщения и соответствующие подписи от отправителя сообщения 604. Сообщениями могут быть, например, электронные запросы доступа к вычислительной службе 608. Сообщения

могут, например, кодировать API вызовы к веб-службе. Если анализ подписи и сообщения показывает, что сообщение достоверно, тогда верификатор подписи уведомляет службу (или компонент, управляющий доступом к службе), что отправитель сообщения может получить запрашиваемый доступ. Например, верификатор подписи может пропустить полученное сообщение к службе, чтобы позволить ей выполнить запрос. Соответственно, службой может быть компьютерная система, действующая для выполнения запросов, как ряд описанных ниже служб. Следует заметить, что в то время как различные компоненты Фиг. 6 и другие, насколько это возможно, описываются как предназначенные для определенных действий компьютерные системы, они также могут содержать множество вычислительных устройств, таких как сети вычислительных устройств, конфигурированные для выполнения совместных действий.

[0057] Фиг. 7 иллюстрирует структурную схему, поясняющую пример процесса 700 подписывания сообщений, соответственно варианту реализации изобретения. Некоторые или все процессы 700 (или любые другие процессы, описанные в настоящей заявке, или различные варианты и/или их комбинации) могут выполняться под управлением одной или более компьютерных систем, сконфигурированных при помощи выполнимых команд, и могут быть реализованы в виде кода (например, выполнимых команд, одной или более компьютерной программы, или одного или более приложений), выполняемые совместно на одном или более процессорах аппаратными средствами или их комбинациями. Код может храниться на машиночитаемом носителе информации, например, в виде компьютерной программы, включающей совокупность команд, выполняемых одним или более процессорами. Машиночитаемый носитель информации может быть носителем для постоянного хранения информации.

[0058] В варианте реализации изобретения процесс 700 включает получение 701 ключа K. Ключ может быть произведен любым подходящим способом. Например, ключ может быть генерирован компьютерной системой, выполняющей процесс 700. Ключ может быть получен в электронном виде компьютерной системой, выполняющей процесс 700. Как правило, полученный ключ может быть произведен любым подходящим способом. Ключом может быть любой ключ, соответствующий требованиям для использования в конкретном алгоритме подписи. Например, если используется схема хэш-кода аутентификации сообщения (HMAC) с алгоритмом безопасного хэширования (SHA)-256 функции криптографического хэширования информации, ключом может быть последовательность байтов, например, последовательность 64 или меньше байтов. Также могут использоваться различные функции криптографического хэширования, например, SHA-224, SHA-384 и SHA-512.

[0059] В варианте реализации изобретения процесс также подразумевает канонизацию сообщения M к форме канонизированного сообщения M_c. Канонизация сообщения может включать упорядочивание информации в сообщении в формат, позволяющий верификатору проверять, является ли подпись сообщения действительной. Как правило, многие протоколы передачи информации преобразуют биты, содержащие сообщение, в то же время оставляя сообщения семантически идентичными. В результате два семантически идентичных сообщения могут содержать разные наборы битов и, следовательно, в результате могут содержать разные подписи. Соответственно, канонизация дает возможность проверять подпись путем простой проверки. Однако следует заметить, что некоторые варианты реализации настоящего раскрытия изобретения не требуют канонизации сообщений. Например, если ряд используемых протоколов не приводит к образованию семантически идентичных сообщений, содержащих разные наборы битов, канонизация не является необходимой и может

быть пропущена. Как правило, канонизацией можно пренебречь в любом случае, когда подпись можно успешно проверить без обработки подписывающего сообщения.

[0060] В реализации изобретения подпись генерируется путем вычисления HMAC(K, M_c), где HMAC() является хэш-функцией кода аутентификации сообщений, как описано выше. HMAC функции имеют несколько параметров, делающих их весьма целесообразными для различных вариантов реализации данного раскрытия изобретения. Например, HMAC функции могут быть успешно вычислены компьютерной системой, тем самым предоставляя вычислительные ресурсы для других задач. К тому же, HMAC функции являются стойкими к восстановлению прообраза (неинвертируемыми). К примеру, дана подпись S=HMAC(K, M) с ключом K и сообщением M, и практически отсутствует информация о ключе K. Например, из S путем вычислений невозможно или, по крайней мере, нецелесообразно практическим путем получить K из S. HMAC функции являются также стойкими к восстановлению второго прообраза. Другими словами, при данной S=HMAC(K, M) и M невозможно или, по крайней мере, нецелесообразно путем вычислений найти сообщение M', отличающееся от M так, что S=HMAC(K,M'). К тому же HMAC функции устойчивы к подделке подписи. Например, дан прогноз для S=HMAC(K, M), прогноз запрашивается N раз (N - положительное число), допускается получение максимум N пар подпись-сообщение. Другими словами, если дан набор пар подпись-сообщение, невозможно или нецелесообразно путем вычислений определить ключ или функцию, которая бы произвела корректную подпись для сообщения не из совокупности.

[0061] В то время как используются HMAC функции, в частности, для различных осуществлений изобретения, могут использоваться и другие функции. К примеру, может использоваться любая функция с вышеупомянутыми свойствами HMAC функций. К тому же, другие функции, которые не обязательно имеют все (или любые) из вышеупомянутых свойств, могут использоваться, например, в обстоятельствах, когда безопасность не является первоочередной задачей и/или когда безопасность важна, но поддерживается за счет использования других механизмов. Следует заметить, что разнообразные пояснения различных вариантов реализации изобретения отображают характерные величины, подставленные в функции HMAC, но такие варианты являются возможными. Например, величины, подставленные в функции HMAC (или другую функцию) могут быть различными. Как описано выше, в частном случае, одной из исходных величин является ключ. При этом исходная величина может быть получена из ключа или иным образом, основываясь, по меньшей мере, на части ключа. В качестве наглядного примера исходная величина может содержать ключ с информацией, такой как идентификатор схемы подписи (скажем, идентификатор версии), который добавляется к ключу как префикс и суффикс. В качестве другого примера исходной величиной может быть информация, полученная при помощи сопоставления ключа с информацией, которой может быть другой ключ. Исходная величина, представленная в виде сообщения, также может быть получена из сообщения. Как другой типовой вариант, рассматриваемый в рамках данного раскрытия сущности изобретения, подпись может быть не результатом HMAC функции, а одним или более значений, полученных из выходной величины HMAC функции (или другой подходящей функции). В некоторых вариантах реализации изобретения ключ и сообщение могут переходить в функцию в обратном порядке.

[0062] Возвращаясь к описанию Фиг. 7, как только подпись была генерирована путем вычисления HMAC(K, Mc), подпись и сообщение M предоставляются приемнику 708, которым может быть вычислительное устройство, проверяющее подписи, или другое

вычислительное устройство, участвующее в процессе проверки подписи, например вычислительное устройство, предоставляющее интерфейс для передачи сообщений и подписей. Как и все варианты реализации изобретения, подробно описанные в настоящей заявке, различные варианты реализации рассматриваются в рамках настоящего раскрытия сущности изобретения. Например, канонизированное сообщение M_C может быть предоставлено приемнику вместо или дополнительно к сообщению M. К тому же, предоставление сообщения M и подписи приемнику может также включать другую информацию, например идентификатор ключа, который может использоваться для идентификации в хранилище данных, сопоставляя ключ с идентификатором. Также другая информация, например параметры кодирования методики, как описано ниже, могут предоставляться с сообщением M и подписью.

[0063] Фиг. 8 иллюстрирует структурную схему, поясняющую пример процесса 800 проверки подписи, по меньшей мере, в соответствии с одним вариантом реализации изобретения. Показанный на Фиг. 8 процесс 800 может выполняться верификатором, как показано на Фиг. 2. К тому же, процесс 800 может выполняться в ответ на получение подписи сообщения, например в ответ другой компьютерной системе, которая должна выполнить процесс 700 Фиг. 7. В варианте реализации изобретения процесс 800 включает получение 802 ключа K, как описано выше. Получение ключа K также может включать другие действия в различных вариантах реализации изобретения. Например, процесс 800 используется компьютерной системой, которая проверяет подпись, генерированную из набора ключей (например, от множества пользователей вычислительных ресурсов провайдера), а получение ключа K может содержать выбор ключа из набора ключей в хранилище данных. Хранилище данных может сопоставлять различные ключи с ключами, отправляемыми для проверки подписи. К примеру, каждый пользователь вычислительного ресурса провайдера может иметь идентификатор ключа (или несколько идентификаторов ключа), используемых для того, чтобы ссылаться на хранилище данных и проводить идентификацию соответствующего ключа. Идентификатор ключа может быть получен вместе с получением сообщения и его подписи или может быть определен иным образом, например, в результате получения регистрационных сертификатов. Получатель идентификатора ключа (например, верификатор сообщения) может обратиться к хранилищу данных для принятия решения, соответствует ли ключ идентификатору ключа в хранилище данных и, если нет, может затем сам генерировать ключ, например, используя описанные в настоящей заявке алгоритмы для прямого или косвенного получения ключа из совместно используемого секретного сертификата. Чтобы осуществить это, получатель должен иметь доступ к пути получения ключа, являющемуся в варианте реализации изобретения данными, в которых закодирована информация, необходимая для получения ключа из данных, уже имеющихся у получателя (например, ключа, полученного из совместно используемого секретного сертификата). Эти данные могут быть предоставлены получателю отправителем сообщения вместе с подписью, или могут стать доступными получателю иным образом. Так, получатель может запрограммировать автоматическую генерацию ключей, используя назначенный ему округ и код для текущей даты. Как правило, может применяться способ получения ключа, используемый для генерирования подписи (или другого ключа, который может использоваться для проверки подписи в некоторых вариантах реализации изобретения). Приемник также может вводить в действие политику допустимых и недопустимых путей получения ключа по отношению к рассматриваемому запросу или к какой-нибудь другой известной приемнику характеристике.

[0064] В варианте реализации изобретения подпись S и сообщение M принимаются

804. Подпись S и сообщение M могут быть получены в электронном виде от отправителя, например вычислительного устройства, выполняющего процесс 700 Фиг. 7. Сообщение M затем канонизируется 806 для определения M_c соответственно варианту реализации изобретения. При помощи канонизации сообщения M в различных вариантах реализации изобретения осуществляется контроль за возможностью проверки подписи S. Соответственно, в варианте реализации изобретения процесс 800 включает генерацию 808 подписи S' путем вычисления HMAC(K, M_c). В варианте реализации изобретения S' эквивалентна HMAC(K, M_c), несмотря на то что в различных вариантах изобретения S' может быть получена из HMAC(K, Mc). С целью наглядности, остальная часть процесса 800 будет описана с учетом того, что S'=HMAC(K, M_c), но в рамках данного раскрытия изобретения допустимы многочисленные варианты.

[0065] Соответственно, в варианте реализации изобретения принимается решение 810, является ли S' эквивалентной полученной подписи S. Другими словами, принимается решение, является ли полученная подпись адекватной, например, из-за того что она была генерирована при помощи ключа K. Следовательно, в варианте реализации изобретения, если 810 принимает решение, что S' и S не эквивалентны, в таком случае подпись является непроверенной 812. Однако если S' эквивалентна S, значит, подпись является проверенной 814. В зависимости от того, проверена ли подпись, могут производиться соответствующие действия. Например, сообщением был запрошен доступ к вычислительным ресурсам, запрашиваемый доступ может быть отклонен (по крайней мере, временно). Таким же образом, если сообщением был запрошен доступ к вычислительным ресурсам и подпись была проверена, запрашиваемый доступ может быть разрешен. Однако следует заметить, что выполнение соответствующих действий может в значительной степени зависеть от различных вариантов реализации изобретения в зависимости от причин(ы), которыми были получены и проверены подписи.

[0066] Как отмечалось выше, различные варианты реализации данного раскрытия изобретения применимы для множества вычислительных сред. Во многих вычислительных средах целесообразно иметь централизованное управление для различных аспектов администрирования безопасности. Например, на Фиг. 9 изображена схема 900, иллюстрирующая типовой способ распределения ключей, в соответствии с, по меньшей мере, одним вариантом реализации изобретения. На Фиг. 9 главный источник ключей обслуживает одно или более хранилищ данных (совместно именуемых как «хранилище данных»), содержащие используемые организациями различные ключи. Ключи могут соответствовать, например, пользователям вычислительных ресурсов организаций. Каждому пользователю из группы пользователей может, например, быть назначен один или более ключей. В варианте реализации изобретения, по меньшей мере, несколько ключей соответствуют пользователям (и/или пользователям пользователей) организаций. Например, в варианте реализации изобретения организация является провайдером вычислительного ресурса и каждый пользователь вычислительного ресурса провайдера соответствует одному или более ключам, которые позволяют пользователям пользователей получать доступ к вычислительным ресурсам, администрируемым вычислительным ресурсом провайдера. Другой вариант процесса 800 Фиг. 8 согласно с вариантами, описанными выше в связи с Фиг. 7, также находится в рамках раскрытия сущности изобретения.

[0067] Как показано на Фиг. 9, источник ключей 902 раздает ключи множеству зон ключей 904. Зоной ключа может быть домен организации, в которой принятый ключ является действительным. Например, ссылаясь на Фиг. 2, каждая зона ключа 904 может

соответствовать зоне отказа, такой как дата-центр. Зоны ключа могут быть, но не обязательно, ограничены географически. Например, каждая зона ключа может соответствовать стране, округу или другой географически локализованной области. Зоны ключа также могут быть определены иным образом. Например, каждая зона ключа может соответствовать службе, предоставляемой вычислительным ресурсом провайдера, пользователю организации, и тому подобное. Хотя это не было показано на примере, зоны ключа могут иметь подзоны. Например, зона ключа может соответствовать стране. Внутри страны может быть множество округов, которые соответствуют подзонам зоны ключа. Ключи в таких вариантах реализации изобретения могут передаваться подзонам.

[0068] Как показано на Фиг. 9, зона ключа 904 может передавать ключи одному или более верификатору 906 для зоны ключа. Например, если зона ключа соответствует дата-центру, вычислительное устройство дата-центра может распространять ключи верификаторам для каждой из множества служб, обеспечиваемых вычислительными ресурсами дата-центра. Таким образом, верификаторы могут использоваться для проверки подписей, полученных вместе с различными запросами. Этим источник ключей освобождает свои вычислительные ресурсы от проверки подписи, а также снижаются требования ко времени ожидания и полосе пропускания, особенно в случаях, когда источник ключей 902 географически удален от служб, запросы к которым он осуществляет.

[0069] Распространение ключа может осуществляться различными путями. В данном варианте реализации изобретения ключи распространяются получателям посредством безопасных информационных каналов. В некоторых вариантах реализации изобретения источник ключей распространяет одни и те же ключи каждой зоне ключа. Также некоторые ключи могут использоваться в нескольких зонах ключа. Источник ключей 902 может распространять ключи, приемлемые в нескольких зонах ключа, нескольким зонам ключа, в то же время не допуская рассылки этих ключей зонам ключа, в которых эти ключи нельзя использовать. Поэтому в примере вычислительных ресурсов провайдера источник ключей 902 может распространять ключ для пользователя только тем зонам ключа, в которых пользователь способен использовать ключ, например дата-центры, используемые для администрирования вычислительных ресурсов пользователя.

[0070] Различные варианты реализации настоящего раскрытия изобретения также обеспечивают распространение ключа способами, дающими множество преимуществ. Фиг. 10 иллюстрирует схему 1000, поясняющую типовой способ распределения ключей в способе, который обеспечивает разные уровни полномочий, в соответствии, по меньшей мере, с одним вариантом реализации изобретения. Согласно Фиг. 10, схема 1000 содержит источник ключей 1002 с ключом К, распространяющий ключи, прямо или косвенно, различным зонам ключа 1004 и верификаторам 1006 таким же образом, как описано выше в связи с Фиг. 9. Несмотря на то что для наглядности схема 1000 описывается с использованием одного ключа К и ключей, полученных из К, варианты реализации изобретения, описанные в настоящей заявке, применимы и в случае, когда источник ключей также действует для набора ключей.

[0071] Как показано на Фиг. 10, ключ К используется как базовый для других ключей, полученных из К. Например, из К, ключ $К_1$ получен и передается в первую зону ключа (Зона Ключа$_1$). По сути, ключ $К_1$ (или полученные из $К_1$ ключи) являются приемлемыми в первой зоне ключа, но не в другой зоне ключа, которая не имеет $К_1$ (или ключа,

полученного из ключа $К_1$). Подобным образом каждая зона ключа из числа других принимает соответствующие различные ключи, полученные из ключа К. Следует заметить, что возможны варианты, в то время как Фиг. 10 иллюстрирует ключи, полученные из ключа К, переданного из источника ключей 1002 соответствующей зоне ключа. Например, ключ К может передаваться зонам ключа, и каждая зона ключа, которая принимает ключ К, может использовать ключ К для получения одного или более соответствующих ключей. Например, зона ключа 1004, помеченная «Зона $Ключа_1$» может принимать ключ К и получать из него $К_1$. Как правило, различные задачи, вовлеченные в получение ключа и его передачу, могут выполняться иначе, чем поясняется в различных вариантах реализации изобретения.

[0072] Как показано в пояснительном примере Фиг. 10, ключи, принятые зонами ключа 1004, используются для получения ключей, которые затем передаются. Например, что касается зоны ключа 1004, помеченной «Зона $Ключа_2$», ключ $К_2$, полученный из ключа К, используется для получения дополнительных ключей $К_2$’ и $К_2$”. Ключи $К_2$’ и $К_2$” передаются соответствующим верификаторам 1006 для использования верификаторами 1006 при проверке подписей. Поэтому в варианте реализации изобретения верификатор, принимающий $К_2$’, способен проверить подпись, генерированную при помощи $К_2$’, принимая во внимание, что верификатор, который не принял $К_2$’, может быть не способен проверить подпись. Могут быть получены преимущества при передаче ключа способом, поясненным при помощи Фиг. 9 и 10 (или соответствующих вариантов). Например, благодаря передаче ключа нескольким верификаторам в нескольких местоположениях вместо одного или более централизованных верификаторов достигается более низкое время ожидания. К тому же, ссылаясь на Фиг. 10, благодаря передаче полученных ключей другим устройствам, которые по очереди получают дополнительные ключи, имеется возможность распределить вычисления между несколькими устройствами в нескольких местах; тем самым достигается более быстрое получение ключа и повышение отказоустойчивости.

[0073] Получение ключей может выполняться множеством способов. На Фиг. 11 изображена структурная схема, иллюстрирующая пример процесса 1100 получения ключа, по меньшей мере, в соответствии с одним вариантом реализации изобретения. В реализации изобретения процесс 100 включает получение 1002 ключа $К_i$, как описано выше. Ключом $К_i$ может быть любой подходящий ключ, такой как описано выше. К тому же, ключ $К_i$ может быть, но не обязательно, получен из другого ключа, такого как полученный в результате процесса 1100 или другого процесса. После получения ключа $К_i$ из $К_i$ производится новый ключ. В наглядном примере к Фиг. 11 новый ключ К $К_{i+1}$вычисляется как (или основывается, по меньшей мере, на части) $HMAC(К_i, R_{i+1})$, где R_{i+1} является информацией, идентифицирующей одно или более ограничений ключа $К_{i+1}$. R_{i+1} может быть, к примеру, последовательностью битов, кодирующей информацию, отображающую, где используется ключ $К_{i+1}$. Например, R_{i+1} может кодировать зону ключа, где может использоваться ключ $К_{i+1}$. Ограничения могут основываться, по меньшей мере частично, на географическом положении, времени, идентичности пользователя, службе и тому подобном. Пример ограничений предоставляется в примере, описанном ниже.

[0074] К тому же, как описывается более подробно ниже, для получения ключа

процесс 1100 может быть использован многократно. Например, ключ, генерируемый при помощи процесса 1100 (или соответствующих вариантов), может быть использован для генерации другого ключа при помощи того же или другого ограничения. Используя терминологию, приведенную на фигуре, R_{i+1} может быть, к примеру, последовательностью битов, которые кодируют информацию, отображающую, где может использоваться ключ K_{i+1}. K_{i+1} может стать ключом K_i для следующего цикла процесса. Например, если процесс 1100 использовался для генерации ключа, основанного на географическом ограничении, генерированный ключ может использоваться для генерации ключа с ограничением, основанным на дате. Такой процесс может использоваться многократно, используя множество ограничений получения ключа. Как более полно описано ниже, используя множество ограничений для получения ключа, один или более верификаторов могут установить политику одновременной проверки подписи. В качестве краткого наглядного примера, как часть процесса проверки подписи, верификатор может определить ожидаемую подпись, используя ограничение, например кодирование текущей даты. Если подпись была предоставлена таким образом, что генерирована в разные даты, то проверка подписи не будет пройдена, соответственно варианту реализации изобретения. Как правило, если использование подписи не соответствует требованиям ограничений, используемых для получения ключа, проверка подписи не может быть пройдена, согласно с различными вариантами реализации изобретения.

[0075] На Фиг. 12 изображена структурная схема 1200, иллюстрирующая наглядный пример получения ключа при помощи многократного ограничения, по меньшей мере, в соответствии с одним вариантом реализации изобретения. На Фиг. 12 иллюстрируется получение ключа при помощи многократных ограничений. В этом примере ключ и ограничение по дате используются для получения ключа даты ($К_{даты}$, на фигуре). На фигуре показано, что дата кодируется как 20110715, соответствующая 15 июля 2011, хотя даты могут кодироваться по-разному, и обычно информация может быть кодирована способом, отличным от изображенного на фигуре. Ключ даты используется с ограничением по округу для получения ключа округа, $К_{округа}$. В этом примере округ кодируется при помощи идентификатора округа «USA-зона-1», который может соответствовать одному или нескольким округам Соединенных Штатов. Ключ $К_{округа}$ используется с ограничением по службе для получения ключа, $К_{службы}$. В этом примере служба является службой виртуальной компьютерной системы, кодируемой ее аббревиатурой VCS. Ключ $К_{службы}$ используется с идентификатором запроса для получения подписывающего ключа, то есть ключа, используемого для подписи запросов к службе. В этом примере «vcs_запрос», что может соответствовать конкретному типу запроса, который может быть получен службой VCS. Например, «vcs_запрос» может соответствовать запросу на конфигурацию, остановку, или иным образом видоизменять виртуальную компьютерную систему. Подписывающий ключ используется для генерации подписи, которая может быть отправлена с запросами. Подпись может быть генерирована любым подходящим способом, подобным описанному выше.

[0076] Как иллюстрирует Фиг. 12, запрос может быть канонизирован в форме сообщения M_c, которое является исходной величиной HMAC функции для генерирования подписи. Разумеется, могут использоваться различные варианты, включая варианты, для которых канонизация не является обязательным требованием, и при использовании функций, отличных от HMAC, в соответствии с различными

реализациями изобретения. К тому же, Фиг. 12 иллюстрирует частный пример получения подписи, в соответствии с вариантом реализации изобретения. Однако для получения подписи может использоваться большее или меньшее количество ограничений, и ограничения могут использоваться в порядке, отличающемся от указанного. К тому же, несмотря на то что Фиг. 12 иллюстрирует получение подписи, могут применяться алгоритмы для получения других объектов, которые могут не рассматриваться как подписи во всех применениях. Например, показанные на Фиг. 12 (и в других местах) алгоритмы, как правило, могут использоваться для получения ключа.

[0077] Фиг. 13 является наглядным примером функции 1300 для получения подписи, в соответствии с, по меньшей мере, одной реализацией изобретения. Как иллюстрирует Фиг. 13, подпись вычисляется как:

HMAC(HMAC(HMAC(HMAC(HMAC(K, дата), округ), служба), протокол), Mc).

В этом примере K является ключом, «дата» является кодированной датой, «округ» является кодированным идентификатором округа, «служба» является кодированным идентификатором службы, «протокол» соответствует конкретному сообщению кодированного протокола, и M_c является канонизированным сообщением.

Следовательно, как иллюстрирует Фиг. 13, подпись вычисляется при помощи многократного вычисления одной и той же HMAC функции, каждый раз с разным ограничением входной величины для HMAC функции.

Подписывающим ключом в этом примере является:

HMAC(HMAC(HMAC(HMAC(K, дата), округ), служба), протокол), которая получается путем многократного использования HMAC функции, каждый раз с разным ограничением.

[0078] В примере на Фиг. 13 различные ограничения могут определять домен и область пересечения обозначенных доменов, что определяет способ, с помощью которого генерируется подпись с подписывающим ключом, которая была бы пригодной. В этом конкретном примере подпись генерирована с подписывающим ключом, описанным при помощи Фиг. 13, которая бы была пригодной для определенной даты, в определенном округе и для определенной службы, использующей определенный протокол. Следовательно, если запрос подписан при помощи подписывающего ключа, но с датой, отличной от даты определенного исходной величиной подписывающего ключа, подпись к запросу может рассматриваться как непроверенная, даже если запрос был сделан для определенной службы и в определенном округе.

[0079] Как другие варианты реализации изобретения, описанные в настоящей заявке, рассматриваются различные варианты реализации в рамках данного раскрытия сущности изобретения. Например, Фиг. 13 иллюстрирует многократное использование HMAC функции. Может использоваться множество функций для определения подписи, и в некоторых реализациях изобретения HMAC функции не используются на каждом этапе получения подписи. Также, как отмечалось, в различных вариантах реализации изобретения могут использоваться различные ограничения и различное число ограничений.

[0080] Получение ключа может выполняться различными способами в соответствии с различными вариантами реализации изобретения. Например, отдельное вычислительное устройство может вычислить подписывающий ключ в соответствии с вариантом реализации изобретения. В соответствии с другими вариантами несколько вычислительных устройств могут совместно вычислять подписывающий ключ. В качестве конкретного наглядного примера, соответствующего Фиг. 13, один компьютер может вычислить

$К_{округа}$=HMAC(HMAC(K, дата), округ),

а другой компьютер может вычислить

Подписывающий Ключ=HMAC($К_{округа}$, служба).

[0081] В качестве другого примера отдельная компьютерная система может выполнять различные уровни вычисления подписывающего ключа. Обращаясь к примеру в предыдущем абзаце, вместо одного компьютера, вычисляющего $К_{округа}$, один компьютер может вычислить

$К_{даты}$=HMAC(K, дата),

а другой компьютер может вычислить

$К_{округа}$=HMAC($К_{даты}$, округ).

Фиг. 14 иллюстрирует пример того, как может выполняться многократное получение ключа, и используется в соответствии с, по меньшей мере, одним вариантом реализации изобретения. В частности, Фиг. 14 иллюстрирует пример схемы 1500, отображающей элементы совокупности распределенных компьютерных систем, совместно вычисляющих подписывающий ключ (или другой ключ, в различных других вариантах реализации изобретения). Как показано на Фиг. 14, каждый элемент группы является компьютерной системой ключа провайдера 1402, которая генерирует ключ и предоставляет генерированный ключ другим компьютерным системам. Например, ключ провайдера, помеченный как $КлючПровайдера_1$, получает ключ К (из другого источника, или сам генерирует ключ) и использует ключ и ограничение, помеченное как R_1, для генерации ключа K_1. $КлючПровайдера_1$ передает ключ K_1 $КлючуПровайдера_2$, который использует K_2 и другое ограничение, R_2, для генерации другого ключа K_2. Ключ $Провайдера_2$ передает ключ K_2Ключ $Провайдера_3$, который использует K_3 и другое ограничение, R_3, для генерации другого ключа K_3. В зависимости от того, сколько имеется в конкретном варианте реализации изобретения провайдеров ключа, эти процессы могут продолжаться до тех пор, пока $КлючПровайдера_{N-1}$ передает ключ K_{N-1} Ключу $Провайдера_N$, который использует K_{N-1} и другое ограничение, R_N, для генерации другого подписывающего ключа, K_N. Ключ K_N затем передается компьютерной системе верификации 1404. Ключ К или любой ключ(и), полученные из К (в основном, именуемые как K_i на фигуре), могут также быть переданы подписывающей компьютерной системе 1406, например в виде алгоритма обмена ключами.

[0082] Подписывающая компьютерная система 1406 может также в различных вариантах реализации изобретения генерировать K_N сама, если, например, ограничения R_1-R_N предоставлены подписывающей системе и/или сделаны общедоступными. К тому же, подписывающая компьютерная система 1406 сама может выполнять только часть процесса получения K_N в различных реализациях изобретения. Например, подписывающая система может получить (возможно, из соответствующей компьютерной системы ключа провайдера) K_i, для некоторых целых чисел i является меньшим, чем N и ограничения от R_{i+1} до R_N. Подписывающая система затем использует K_i и ограничения от R_{i+1} до R_N для генерации подписывающего ключа, K_N. Также рассматриваются и другие варианты, находящиеся в рамках настоящего раскрытия сущности изобретения.

[0083] Подписывающая компьютерная система 1406 может использовать ключ K_N для подписи сообщений, проверяемых верификатором 1404. Например, как пояснялось,

подписывающая система 1406 вычисляет подпись $S=HMAC(K_N, M_C)$, где M_C является канонизированной версией сообщения M, которая также отправляется верификатором. Из-за того что верификатор имеет K_N, верификатор может самостоятельно канонизировать сообщение M и вычислять $HMAC(K_N, M_C)$ для принятия решения, соответствует ли результат вычисления принятой подписи S.

[0084] Следует отметить, что различные варианты процессов, показанных на Фиг. 14, и другие процессы, описанные в настоящей заявке, несмотря на то что показаны участвующими в многократном использовании HMAC функций, могут использовать для получения ключа многие другие функции. Например, в разное время могут использоваться различные типы функций кода аутентификации сообщений (MAC) для получения ключа. Например, значение MAC функции одного типа может использоваться как базовое для MAC функции другого типа. Как правило, в процессе получения ключа могут быть использованы другие типы функций вместо и/или как дополнение к функциям HMAC и в различных вариантах реализации изобретения нет необходимости использовать те же самые функции многократно для получения ключа, но каждый раз, когда необходима функция, могут быть использованы различные функции.

[0085] На Фиг. 15 изображена схема 1500, иллюстрирующая типовой способ, в котором ключи могут быть получены при помощи многократных ограничений, в соответствии, по меньшей мере, с одним вариантом реализации изобретения. Пример, проиллюстрированный Фиг. 15, ссылается на пользователей, например пользователей вычислительных ресурсов провайдера. Однако, как отмечалось, описанные в настоящей заявке алгоритмы, включая алгоритмы, описанные в связи с Фиг. 15, могут быть использованы в множестве других ситуаций.

[0086] Как показано, ключ пользователя, $К_{польз}$, является частью множества долгосрочных ключей пользователя, каждый из которых может быть ключом, используемым пользователем на протяжении определенного периода времени, например, пока пользователь не обновит ключ назначенным новым ключом или иным образом поменяет ключ. Ключи могут также использоваться одним или более пользователями в течение неопределенного периода времени. Ключ пользователя, $К_{польз}$, используется для получения одного или более ключей округа описанным выше способом. Например, как иллюстрирует Фиг. 15, два ключа округа могут быть генерированы, например, вычислением $HMAC(K_{польз}, USA\text{-}E\text{-}1)$ и $HMAC(K_{польз}, USA\text{-}N\text{-}1)$, где USA-E-1 и USA-N-1 являются идентификаторами соответствующих округов. Подобным образом ключи округов могут использоваться для получения ключей даты, истинность которых может быть ограничена датой, используемой для кодирования ключей даты. Каждый из ключей даты может использоваться для получения ключей службы, например, описанным выше способом.

[0087] Таким образом, в различных реализациях изобретения ключи даты могут использоваться с соответствующими службами только в день и в округе, используемом для кодирования ключей. Новые ключи даты могут генерироваться для каждого дня, принимая во внимание, что ключи округа и долгосрочные ключи пользователя могут генерироваться реже. Получение ключа при помощи многократного ограничения, например проиллюстрированное на Фиг. 15 и в других местах в настоящем раскрытии сущности изобретения, дает многочисленные преимущества. Например, получение ключа при помощи способа, описанного в связи с Фиг. 15, если подписывающий ключ взломан (например, злонамеренно получен третьей стороной), уязвимость защиты ограничится конкретным округом, конкретной датой и с использованием конкретной

службы. Другие службы по-прежнему будут оставаться незатронутыми. Подобные преимущества являются действительными для других способов, при помощи которых могут быть получены ключи.

[0088] Фиг. 16, к примеру, является схемой 1006, иллюстрирующей другой типовой способ, при помощи которого могут быть получены ключи в соответствии с, по меньшей мере, одним вариантом реализации изобретения. Фиг. 16 иллюстрирует концепцию, в некотором смысле похожую на ту, что изображена на Фиг. 16. При этом на Фиг. 16 долгосрочные ключи пользователя используются для получения ключей даты. Ключи даты используются для получения ключей округа. Ключи округа используются для получения ключей службы. Получение ключей может выполняться в соответствии с различными реализациями, описанными в заявке.

[0089] На Фиг. 17 изображена схема 1700, иллюстрирующая еще один типовой способ, при помощи которого могут быть получены ключи, в соответствии, по меньшей мере, с одним вариантом реализации изобретения. На Фиг. 17 долгосрочные ключи пользователя используются для получения ключей месяца. Ключи месяца используются для получения ключей округа. Ключи округа используются для получения ключей даты. Ключи даты используются для получения ключей службы. Получение различных ключей может быть выполнено при помощи способа, согласующегося с описанным выше.

[0090] Как описывалось выше, различные алгоритмы настоящего раскрытия сущности изобретения предусматривают новый способ генерации сеансов. Сеансом может быть период времени, для которого предусмотрена совокупность одного или более действий, где окончание (или другое завершение) сеанса является основанием для запрета совокупности одного или более действий. Фиг. 18 является структурной схемой, иллюстрирующей пример процесса 1800 инициализации сеанса, в соответствии с, по меньшей мере, одним вариантом реализации изобретения. Процесс 1800 может выполняться любым подходящим вычислительным устройством или совместно любой совокупностью подходящих вычислительных устройств. Например, процесс 1800 может выполняться клиентским устройством пользователя вычислительных ресурсов провайдера. В качестве другого примера в другом варианте реализации изобретения, относящегося к Фиг. 3, одна из служб зоны отказа может быть сеансовой службой и одно или более вычислительных устройств, принимающее участие в предоставлении службы, может выполнять процесс 1800.

[0091] Возвращаясь к Фиг. 18, в варианте реализации изобретения процесс 1800 включает получение 1802 ключа, К. Ключом К может быть любой подходящий ключ, например, ключ, полученный при использовании других ключей, например, описанным выше способом. Например, ключ К может быть передан вычислительному устройству, участвующему в выполнении процесса 1800. В определенный момент времени (например, сразу после получения ключа К, как показано на фигуре) в варианте реализации изобретения запрос инициирования сеанса может быть принят 1804. Запросом может быть электронный запрос, такой, как описано выше. К тому же в варианте реализации изобретения запрос подписывается и проверяется при помощи алгоритмов данного раскрытия сущности изобретения. Также запросом может быть уникальный запрос, зависящий от конкретной вычислительной среды, используемой для реализации процесса 1800. Например, если процесс 1800 выполняется клиентским устройством (например, пользовательским устройством пользователя вычислительных ресурсов провайдера) для генерации сеанса, запрос инициирования сеанса может быть принят модулем клиентского устройства.

[0092] В реализации изобретения параметры сеанса определяются 1806. Параметрами сеанса может быть информация, которая отображает одно или более генерируемых ограничений сеанса. Типичные параметры содержат, но не ограничиваются ими, длительность сеанса, идентификаторы допустимых пользователей генерируемого ключа сеанса, одну или более служб, с которыми генерируется приемлемый ключ сеанса, ограничения на действия, выполняемые с использованием ключа сеанса, любые из описанных выше ограничений, и другие. Параметры могут быть кодированы в электронном виде, в соответствии с заранее заданными требованиями форматирования, чтобы следить за согласованным производством вычислений, участвующих в получении ключа сеанса. Например, даты могут запрашиваться для кодирования в формате ГГГГММДД. Другие параметры могут иметь свои собственные требования форматирования. К тому же, определение параметров сеанса может производиться различными способами. Например, параметры могут быть параметрами по умолчанию для сеанса, например, ключ сеанса является пригодным только для диапазона действий, предопределенных для инициатора запросов инициализации сеанса и для предопределенного периода времени (например, двадцатичетырехчасового периода). В качестве другого примера параметры могут предоставляться как часть принятого запроса или иным образом вместе с ним. Например, параметры могут генерироваться в соответствии с исходными данными пользователя из инициатора запросов и кодироваться соответственно предопределенной схеме.

[0093] В варианте реализации изобретения, после того как параметры определены, их используют для вычисления 1808 ключа сеанса, K_S. Вычисление ключа сеанса K_S может производиться множеством способов. Например, в одном варианте ключ сеанса K_S может быть вычислен как (или иным образом, основанным, по меньшей мере, на части)

HMAC(K, Параметры_Сеанса)

где Параметры_Сеанса являются кодированными параметрами, которые были определены 1806. Параметры_Сеанса могут быть кодированы предопределенным образом, который проверяет согласованность вычисленных данных. Ключ сеанса K_S также может быть вычислен другими способами, например описанным ниже способом на Фиг. 19.

[0094] После того как ключ сеанса K_S вычислен 1808, в варианте реализации изобретения ключ сеанса K_S предоставляется для использования. Предоставление ключа сеанса может производиться различными способами в различных реализациях изобретения. Например, ключ сеанса может предоставляться модулю инициатора запросов для предоставления инициатору запросов возможности подписывать сообщения ключом сеанса. Ключ сеанса может также предоставляться посредством сети другому устройству, чтобы предоставить другому устройству возможность подписывать сообщения ключом сеанса. Например, ключ сеанса может также предоставляться объекту делегирования, для которого инициируется сеанс. Например, инициатор запросов может иметь определенный объект делегирования в своем составе или иным образом вместе с запросом инициировать сеанс. Ключ сеанса также может обеспечиваться в электронном виде в соответствии с информацией, предоставленной инициатору запросов (то есть делегатору), например, при помощи электронной почты или другого электронного адреса.

[0095] Как отмечалось выше, Фиг. 19 отображает наглядный пример процесса 1900, который может использоваться для генерации подписи, соответственно варианту

реализации изобретения. Процесс 1900 может выполняться одним или более вычислительным устройством, например, одним или более вычислительным устройством, выполняющим процесс 1800, описанный выше в связи с Фиг. 18. Процесс 1900, как показано на Фиг. 19, включает прием параметров сеанса, например, описанных выше. С параметрами сеанса, имеющими полученный в варианте реализации изобретения промежуточный ключ, K_{i+1} вычисляется 1904 как:

$$K_{i+1} = HMAC(K_i, P_i),$$

где K_i может быть ключом К в описании Фиг. 18 для первого вычисления K_{i+1}, а P_i является i^{-M} параметром параметров сеанса. Параметры сеанса могут быть упорядочены в соответствии с предопределенной расстановкой для проверки вычислительной согласованности подписи ключа.

[0096] В варианте реализации изобретения принимается решение 1906, используются ли дополнительные параметры для генерации ключа сеанса. Если имеются дополнительные параметры, в варианте реализации изобретения индекс i увеличивается 1908 на один и $К_{+1}$ снова вычисляется 1904. Если при этом принимается решение, что нет дополнительных параметров, тогда K_S выбирается 1910 до величины $К_{+1}$.

[0097] На Фиг. 20 изображена структурная схема, иллюстрирующая пример процесса 2000 получения доступа к одному или более вычислительным ресурсам в течение сеанса, в соответствии с, по меньшей мере, одним вариантом реализации изобретения. Следует отметить, что в то время, как Фиг. 20 иллюстрирует процесс 2000 получения доступа к одному или более вычислительным ресурсам, как и в случае других описанных в настоящей заявке процессов, процесс 2000 может быть модифицирован для любой ситуации, в которой используются процессы подписи. Процесс 2000 может быть выполнен компьютерной системой пользователя, запрашивающей доступ к одному или более вычислительному ресурсу, например, клиентской компьютерной системой, иллюстрированной Фиг. 1, и/или пользовательской компьютерной системой, описанной в других местах настоящей заявки. В варианте реализации изобретения процесс 2000 включает получение ключа сеанса K_S. Ключ сеанса может быть получен любым подходящим способом, например в электронном сообщении. Ключ сеанса может быть получен из компьютерной системы делегирующего объекта доступа к одному или более вычислительным ресурсам или другой компьютерной системе, например, компьютерной системе, действующей вместе с одной или более компьютерной системой, выполняющей процесс для генерации K_S.

[0098] В варианте реализации изобретения запрос R генерируется 2004. Запрос R может быть сообщением, например, как описано выше. Запрос R затем канонизируется 2006 в варианте реализации изобретения, и подпись вычисляется 2008 из канонизированного сообщения, например, вычислением подписи как (или иным образом, по меньшей мере, на части) $HMAC(K_S, R_C)$. Сразу после генерации подписи, подпись S и запрос R предоставляются 2010. Например, как описано выше, подпись S и запрос R могут предоставляться в электронном виде интерфейсу компьютерной системы, участвующей в управлении запросами и проверке подписей. Подпись S и запрос R, как и в случае с подписями и сообщениями в общем, могут быть предоставлены вместе в одном канале связи, в отдельных каналах связи, или совместно при помощи нескольких каналов связи. Вместе с подписью S и запросом R может также предоставляться другая информация. Например, может предоставляться идентификационная информация, чтобы дать верификатору возможность выбрать корректный ключ для генерации

подписи, с которой будет проверяться принятая подпись. Идентификация может быть осуществлена, например, идентификатором ключа, который должен использоваться при генерации подписи для сопоставления. Может также предоставляться и использоваться другая информация, необходимая в различных реализациях изобретения.

[0099] На Фиг. 21 изображена структурная схема, иллюстрирующая пример процесса 2100 принятия решения, предоставить ли запрашиваемый доступ к одному или более вычислительным ресурсам, в соответствии с, по меньшей мере, одним вариантом реализации изобретения. Как иллюстрирует Фиг. 12, процесс 2100 включает подписывание 2102 ключа K_S. Как и в другом изложении настоящей заявки о получении подписывающего ключа, подписывающий ключ может быть получен различными способами, например, получением подписывающего ключа из другого источника, извлечением подписывающего ключа из памяти, вычислением подписывающего ключа из имеющейся в наличии информации, и тому подобным.

[0100] В реализации изобретения принятый запрос R канонизируется к виду R_C, например, описанным выше способом. Следует отметить, что возможны варианты, как и в случае с другими процессами, описанными в настоящей заявке. Например, вычислительная система, выполняющая вариант процесса 2100 (или другого процесса) может только принимать канонизированное сообщение, и канонизация может выполняться другим вычислительным устройством. Возвращаясь к описанию Фиг. 21, подпись S' вычисляется как (или иным образом, по меньшей мере, на части) $HMAC(K_S, R_C)$. Вычисленный подписывающий ключ S' сравнивается 2110 с принятой подписью S для определения, являются ли две подписи эквивалентными. Если определено, что две подписи не эквивалентны, сеанс определяется 2112 как неподтвержденный и могут быть предприняты соответствующие действия, например, отказ на запрос. Если две подписи определяются как эквивалентные, сеанс является подтвержденным 2114, и могут быть предприняты соответствующие действия, например, предоставление доступа к одному или более вычислительным ресурсам.

[0101] Алгоритмы настоящего раскрытия сущности изобретения могут быть использованы, чтобы предоставить делегацию полномочий. Фиг. 22 является структурной схемой, показывающая наглядный пример процесса 2200 для делегирования полномочий, по меньшей мере, в соответствии с одним вариантом реализации изобретения. Процесс 2200 может выполняться вычислительным устройством, например, вычислительным устройством пользователя, предпринимающего попытку делегировать доступ к одному или более вычислительным ресурсам, или вычислительным устройством вычислительного ресурса провайдера, или любым подходящим устройством. Как иллюстрирует Фиг. 22, процесс 2200 включает получение 2202 ключа сеанса K_{si}. Ключ сеанса K_{si} может быть получен любым подходящим способом, например, способом, в котором описанные выше ключи описываются как полученные. К тому же, ключ сеанса может быть ключом, генерируемым как часть процесса делегирования доступа к одному или более вычислительному ресурсу. Например, ключ сеанса может быть генерирован путем выполнения процесса 2200 или его соответствующим вариантом.

[0102] В реализации изобретения параметры сеанса определяются 2004. Параметры сеанса могут быть определены любым подходящим способом, например, описанным выше в связи с Фиг. 18. С параметрами сеанса, определенными 2004, может быть генерирован новый ключ сеанса $K_{S(i+1)}$, например, как описано выше, содержащий, как описано выше в связи с Фиг. 19. Генерированный один раз, новый сеанс может предоставляться для делегирования. Например, ключ сеанса может быть отправлен в

электронном сообщении объекту делегирования. Ключ сеанса может прямо или косвенно предоставляться объекту делегирования. Например, ключ сеанса может быть дан делегатору и делегатор может отвечать за предоставление ключа сеанса одному или более объектам делегирования. Объекту делегирования может быть также предоставлена и другая информация. Например, объекту делегирования могут быть предоставлены параметры сеанса, чтобы позволить объекту делегирования предоставить параметры сеанса с подписями, таким образом позволяя получателю (например, верификатору) параметров сеанса генерировать ожидаемые подписи для проверки, являются ли предоставленные подписи действительными. Например, получатель может использовать параметры для генерации ключа сеанса из секретного сертификата или полученного посредством этого ключа, и использовать такой ключ сеанса для генерации подписи для канонизированной версии соответствующего подписывающего сообщения. Как правило, параметры могут стать доступными получателю подписи любым подходящим способом, чтобы позволить получателю проверять подписи сообщения, и объекту делегирования не обязательно необходим доступ к параметрам, независимым от объекта делегирования.

[0103] Фиг. 23, например, отображает структурную схему 2300, иллюстрирующую, как могут быть многократно делегированы привилегии. Делегатор 2302 может пожелать разрешить одну или более привилегию доступа к объекту делегирования 2304. Объект делегирования 2304, однако, в этом примере может пожелать предоставить одну или более привилегий другому объекту делегирования 2306. Следовательно, в этом примере объект делегирования 2304 может становиться делегатором. Подобным образом объект делегирования 2306 может пожелать предоставить доступ к другому объекту делегирования, и этот объект делегирования может пожелать разрешить доступ к другому объекту делегирования, и так далее до тех пор, пока в конечном итоге одна или более привилегий разрешаются еще одному объекту делегирования 2308.

[0104] Следовательно, в этом примере изначальный делегатор 2302 отправляет запрос делегирования сеансоориентированной службе аутентификации 2310, которая может быть службой зоны отказа, как описано выше. В ответ в варианте реализации изобретения сеансоориентированная служба аутентификации генерирует и предоставляет ключ сеанса делегатору 2302, например, описанному выше в связи с Фиг. 22. Делегатор 2302 затем в варианте реализации изобретения предоставляет ключ сеанса, принятый им от сеансоориентированной службы аутентификации 2310 делегатору 2304. Объект делегирования 2304 может предоставлять ключ сеанса другому объекту делегирования 2306. Таким же способом объект делегирования 2306 мог бы получить сферу привилегий, полученных объектом делегирования 2304, которые могли бы быть такими же, что и уровень привилегий, предоставленный объекту делегирования 2306.

[0105] При этом, как показано на Фиг. 23, объект делегирования 2304 может отправлять запрос делегирования сеансоориентированной службе аутентификации 2310 и принимать другой ключ сеанса, который был генерирован сеансоориентированной службой аутентификации 2310 в ответ на запрос делегирования. Объект делегирования 2304 может предоставлять ключ сеанса следующему объекту делегирования 2306. Следующий объект делегирования 2306 может предоставлять ключ сеанса еще одному объекту делегирования, или как описано выше, может также отправлять запрос делегирования сеансоориентированной службе аутентификации 2310, которая могла бы затем генерировать ключ сеанса и предоставлять ключ сеанса объекту делегирования 2306, отправившему запрос делегирования. Как иллюстрируется на Фиг. 23, это может продолжаться далее и один или более объектов делегирования

могут предпринять попытку использовать ключ, который они приняли.

[0106] В этом конкретном примере объект делегирования 2308 предоставляет ключ сеанса вычислительному ресурсу 2312 вместе с запросом. Как указано выше, запрос может содержать ключ сеанса, хотя ключ сеанса может быть предоставлен отдельно от запроса. Вычислительный ресурс 2312 может быть любым из описанных выше вычислительных ресурсов или каким угодно вычислительным ресурсом. Служба управления политикой 2314 может включать верификатор, например, описанный выше, и в результате запроса вычислительного ресурса может проверять запросы на достоверность. Вычислительный ресурс 2312 и служба управления политикой 2314 могут также быть одним компонентом, несмотря на то что показаны на Фиг. 23 отдельно. Также несмотря на то что Фиг. 23 иллюстрирует одну сеансоориентированную службу аутентификации 2310, используемую для генерации ключей сеанса, различные реализации изобретения могут использовать различные сеансоориентированные службы аутентификации.

[0107] Как отмечалось выше, дополнительно к наглядным примерам, предоставленным в настоящей заявке, рассматриваются многочисленные варианты, находящиеся в рамках данного раскрытия сущности изобретения. На Фиг. 24 изображена схема 2400, представляющая наглядный пример способа, посредством которого ключи могут быть получены при помощи ключей из множества источников, соответственно варианту реализации изобретения. На Фиг. 23 ключ пользователя $К_{польз}$ является ключом из набора ключей пользователя, администрируемого вычислительным ресурсом провайдера. Как и в случае с описанными выше вариантами реализации изобретения, хотя Фиг. 23 рассматривается в качестве наглядного примера, в связи с вычислительным ресурсом провайдера рассматриваются и другие варианты, находящиеся в рамках данного раскрытия сущности изобретения.

[0108] На Фиг. 24 администрируется совокупность источников ключей, где разным источникам ключей соответствуют разные домены полномочий. Каждый ключ авторизации, полученный из ключа пользователя $К_{польз}$, может быть, например, передан разным зонам отказа, как описано выше. Зоны отказа могут быть, к примеру, дата-центрами под различной политической юрисдикцией. Следует при этом заметить, что возможны варианты, в то время как Фиг. 24 иллюстрирует каждый распределенный ключ авторизации, полученный из одного ключа пользователя $К_{польз}$. Например, распределенные ключи авторизации могут быть получены независимо друг от друга. В качестве другого примера, один или более распределенных ключей авторизации могут быть получены из общего ключа, один или более остальных ключей могут быть получены из другого общего ключа, и так далее.

[0109] В варианте реализации изобретения есть возможность объединить множество полномочий в полномочие для получения доступа к одному или более вычислительным ресурсам. Например, как показано на Фиг. 24, для получения других ключей могут быть использованы поднаборы распределенных ключей авторизации. Например, как показано на Фиг. 23, для получения совмещенного ключа авторизации используются два ключа авторизации, помеченные Авт1 и Авт2. Для получения совмещенного ключа авторизации в варианте реализации изобретения вычисляется величина HMAC(f(Авт1 , Авт2), R), где R является одним из ограничений, например, описанным выше. Например, f является функцией распределенных ключей авторизации и может иметь более двух измерений. Например, используются три распределенных ключа авторизации, Авт1 , Авт2, и Авт3, как показано на Фиг. 23, аргумент функции f(Авт1, Авт2, Авт3) для

вычисления совмещенного ключа авторизации, как (или иным образом, основываясь, по меньшей мере, частично) HMAC(f(Авт1, Авт2, Авт3), R).

[0110] Многочисленные варианты построения ключей из разных источников рассматриваются в рамках настоящего раскрытия сущности изобретения. Например, источник может генерировать (или уже сгенерировал) ключ (K_{spec}), используя различные варианты реализации настоящего раскрытия сущности изобретения. Каждый источник K_{spec} может соответствовать частной производной ключа, которая может быть общедоступным кодированием (или декодированием иным образом, доступным отправителю сообщения и верификатору подписи) ограничений, используемых для генерации его K_{spec}. Например, частной производной ключа может быть

(K1/20110810/usa-east-1/DDS, K2/20110810/org_name/jp1/DDS), где каждая последовательность между наклонными чертами является ограничением. Такое кодирование информации может называться «путь ключа». В качестве более общего примера, частная производная ключа может быть $X_1/.../X_n$, где каждому значению X_i (для i между 1 и n) соответствует параметр, например, параметр, описанный выше. Частная производная ключа из пригодных источников может быть закодирована как n-строка, рассматриваемая как производная ключа. Для примера, непосредственно над n-строкой может быть ($spec_1$, $spec_2$,...,$spec_n$), где каждая запись является путем ключа для соответствующего K_{spec}. Следует отметить, что производная ключа (и/или путь ключа) кодирует точный ключ, используя (полное ограничение между всеми авторизованными ключами) так, что владелец ключа авторизуется путем генерации подписи/ключа. К тому же, с частными производными ключа отбирается доступное как хозяевам сообщения, так и верификаторам подписи, произвольное распределение используемых для генерации ключей и подписей параметров, возможное с тех пор как, например, отправитель сообщения получает информацию, определяющую порядок параметров, которые были использованы для генерации подписывающего ключа и могут, таким образом, генерировать подпись ключа и сообщение соответственно.

[0111] Величина для функции HMAC(Kspec, ключ-производная) затем может быть получена или вычислена для каждого из пригодных источников, то есть, должны быть генерированы источники для каждого ключа. Эта величина может быть вычислена клиентом, получившим подписывающий ключ для подписи сообщений, или может быть вычислена другим устройством и впоследствии предоставлена клиенту, в различных вариантах реализации изобретения. Каждая из этих величин может рассматриваться как частный ключ, с целью последующего обсуждения. Семантика каждого из этих частных ключей в варианте реализации изобретения такова, что они действительны только тогда, когда объединены с нижеупомянутой структурой (и некоторыми вариантами нижеупомянутой структуры) и, когда объединяются, образуют область пересечения спецификаций, кодированных в производных ключа.

[0112] Для того чтобы генерировать подписывающий ключ для подписи сообщения, величина для

K_S = HMAC(частн_ключ$_1$+...+частн_ключ$_n$, ключ-производная),

где «+» может относиться к какой-нибудь ассоциативной операции с частными ключами, которые окружают символ в формуле. Символ «+» может быть, например, операцией, исключающей ИЛИ (XOR) над битами, содержащими частный ключ. Символ «+» может также ссылаться на какие-нибудь подходящие операции или функции.

[0113] Чтобы проверить подпись, используемую для подписывания сообщения, верификатор может получать каждый частный ключ, комбинировать частные ключи,

как описано выше, формировать подписывающий ключ, подписывать принятое сообщение и сравнивать результат с ожидаемым результатом для проверки подписи, например, описанной выше.

[0114] Типичные варианты реализации раскрытия сущности изобретения могут быть описаны в виде следующих пунктов:

Пункт 1. Компьютерно-реализуемый способ предоставления услуг, содержащий:

под управлением одной или более компьютерных систем, функционирующих на основе выполняемых команд,

прием от стороны аутентификации электронной кодированной информации, содержащей сообщение, подпись сообщения и набор из одного или более ограничений относительно ключей, полученных на основе совместно используемого со стороной аутентификации секретного сертификата, причем подпись может быть определена путем применения хэш-функции кода аутентификации сообщений к сообщению, секретному сертификату и набору из одного или более ограничений, а также может быть неопределяемой при наличии только хэш-функции кода аутентификации сообщений без набора из одного или более ограничений;

получение ключа, сгенерированного, по меньшей мере, частично, при помощи, по меньшей мере, поднабора из набора из одного или более ограничений;

вычисление при помощи одной или более компьютерных систем значения хэш-функции кода аутентификации сообщений посредством, по меньшей мере, ввода в хэш-функцию кода аутентификации сообщений:

первого входного значения, основанного, по меньшей мере, частично на полученном ключе, и

второго входного значения, основанного, по меньшей мере, частично на наборе из одного или более ограничений;

определение того, действительна ли подпись, посредством одной или более компьютерных систем и, по меньшей мере, частично, на основе вычисленного значения; и

предоставление доступа к одному или более вычислительным ресурсам в случае определения, что подпись является действительной.

Пункт 2. Компьютерно-реализуемый способ по п.1, в котором:

сообщение содержит запрос на доступ к одному или более вычислительным ресурсам;

при этом способ дополнительно содержит определение того, указывает ли набор из одного или более ограничений на то, что запрос должен быть удовлетворен; и

предоставление доступа к одному или более вычислительным ресурсам является возможным при определении, что ограничения указывают на то, что запрос должен быть удовлетворен.

Пункт 3. Компьютерно-реализуемый способ по п. 2, в котором кодированную информацию, содержащую набор из одного или более ограничений, кодируют с использованием определенного документа, при этом этап определения того, указывает ли набор ограничений на то, что запрос должен быть удовлетворен, включает в себя анализ документа, исходя из контекста, в котором был принят запрос.

Пункт 4. Компьютерно-реализуемый способ по п. 1, в котором:

сообщение содержит запрос на доступ к вычислительному ресурсу из упомянутых одного или более вычислительных ресурсов;

кодированная информация, содержащая набор из одного или более ограничений, включает в себя информацию, указывающую вычислительный ресурс; и

предоставление доступа к одному или более вычислительным ресурсам, включает

в себя предоставление доступа к вычислительному ресурсу, если вычислительный ресурс совпадает с указанным вычислительным ресурсом.

Пункт 5. Компьютерно-реализуемый способ по п. 1, в котором:

кодированная информация, содержащая набор из одного или более ограничений, соответствует периоду времени, в течение которого сообщение является действительным; и

определение того, действительна ли подпись, основано, по меньшей мере, частично на том, было ли сообщение предоставлено в течение соответствующего периода времени.

Пункт 6. Компьютерно-реализуемый способ по п. 1, в котором:

кодированная информация, содержащая набор из одного или более ограничений, соответствует ограничению, основанному, по меньшей мере, частично на местоположении; и

определение того, действительна ли подпись, основано, по меньшей мере, частично на том, совпадает ли местоположение по меньшей мере одной из одной или более компьютерных систем с соответствующим местоположением.

Пункт 7. Компьютерно-реализуемый способ предоставления услуг, содержащий:

под управлением одной или более компьютерных систем, функционирующих на основе выполняемых команд,

получение электронной кодированной информации, содержащей (i) сообщение, (ii) первую подпись сообщения и (iii) набор из одного или более параметров, причем первая подпись сгенерирована, по меньшей мере, частично на основе (i) сообщения, (ii) секретного сертификата и (iii) набора из одного или более параметров, и к тому же первая подпись является неопределимой при наличии только сообщения и секретного сертификата, но без набора из одного или более параметров;

получение второго сертификата, по меньшей мере, частично на основе секретного сертификата и, по меньшей мере, поднабора из набора из одного или более параметров;

генерирование второй подписи, по меньшей мере, частично на основе полученного второго сертификата;

определение того, совпадает ли первая подпись со второй подписью; и

предоставление доступа к одному или более компьютерным ресурсам, когда сгенерированная вторая подпись совпадает с первой подписью.

Пункт 8. Компьютерно-реализуемый способ по п. 7, в котором получение второго сертификата включает в себя ввод в функцию секретного сертификата и, по меньшей мере, поднабора из набора из одного или более параметров.

Пункт 9. Компьютерно-реализуемый способ по п. 8, в котором функция является симметричной функцией аутентификации сообщений.

Пункт 10. Компьютерно-реализуемый способ п. 9, в котором симметричной функцией аутентификации сообщений является хэш-функция.

Пункт 11. Компьютерно-реализуемый способ по п. 9, в котором ввод в функцию секретного сертификата и, по меньшей мере, поднабора из одного или более параметров выполняют как часть операции формирования хэш-кода аутентификации сообщений (HMAC).

Пункт 12. Компьютерно-реализуемый способ по п. 8, в котором генерирование второй подписи включает в себя ввод в функцию выходного значения функции и параметра из набора из одного или более параметров.

Пункт 13. Компьютерно-реализуемый способ по п. 7, в котором кодированная информация, содержащая один или более параметров, содержит электронный кодированный документ, содержащий набор из одного или более параметров.

Пункт 14. Компьютерно-реализуемый способ по п. 8, в котором:

генерирование второй подписи основано, по меньшей мере, частично на ключе;

набор из одного или более параметров включает в себя одно или более ограничений на использование ключа и

предоставление доступа к одному или более вычислительным ресурсам выполняют в соответствии с одним или более ограничениями.

Пункт 15. Компьютерно-реализуемый способ по п. 14, в котором ключ основан, по меньшей мере, частично на результате ввода секретного сертификата в функцию.

Пункт 16. Постоянный машиночитаемый носитель информации, на котором хранятся команды, которые при выполнении компьютерной системой обеспечивают осуществление компьютерной системой, по меньшей мере:

получения промежуточного ключа на основе, по меньшей мере, секретного сертификата и одного или более параметров, определяющих использование промежуточного ключа;

применения, по меньшей мере, частично на основе полученного промежуточного ключа, по меньшей мере, части процесса генерации подписи, который обеспечивает получение подписи сообщения, причем процесс генерации подписи сконфигурирован так, что подпись не определяется при помощи процесса генерации подписи вычислительным устройством, имеющим сообщение, секретный сертификат и подпись, но не содержащим одно или более ограничений; и

предоставления сообщения, подписи и одного или более параметров другой компьютерной системе, сконфигурированной для анализа подписи, по меньшей мере, частично на основе одного или более параметров и сообщения, чтобы определить, действительна ли подпись.

Пункт 17. Постоянный машиночитаемый носитель информации по п. 16, в котором в одном или более параметрах закодировано одно или более ограничений на использование промежуточного ключа, которые приводятся в исполнение, по меньшей мере, частично вышеупомянутой другой компьютерной системой.

Пункт 18. Постоянный машиночитаемый носитель информации по п. 16, в котором одно или более ограничений соответствуют, по меньшей мере, периоду времени, в течение которого может использоваться промежуточный ключ, местоположению, в котором может использоваться промежуточный ключ, или одной или более службам, для получения доступа к которым может использоваться промежуточный ключ.

Пункт 19. Постоянный машиночитаемый носитель информации по п. 16, в котором команды при выполнении компьютерной системой позволяют компьютерной системе генерировать подпись без доступа компьютерной системы к секретному сертификату.

Пункт 20. Постоянный машиночитаемый носитель информации по п. 19, в котором при наличии набора из одного или более параметров подпись определяется при помощи процесса генерации подписи с применением совместно используемого секретного сертификата либо промежуточного ключа.

Пункт 21. Постоянный машиночитаемый носитель информации по п. 19, в котором получение промежуточного ключа включает в себя выполнение алгоритма, предусматривающего, что, по меньшей мере, одно выходное значение хэш-функции вводится с использованием, по меньшей мере, одного из параметров в хэш-функцию.

Пункт 22. Компьютерная система, содержащая:

один или более процессоров и

память, содержащую команды, которые при выполнении одним или более процессорами компьютерной системы обеспечивают осуществление компьютерной

системой, по меньшей мере:

приема одних или более электронных данных, которые совместно обеспечивают кодирование сообщения, подписи сообщения и одного или более параметров, причем подпись сгенерирована, по меньшей мере, частично на основе секретного сертификата и одного или более параметров;

анализа для определения, действительна ли подпись, по меньшей мере, частично на основе одного или более параметров, промежуточного сертификата, полученного, по меньшей мере, на основе фрагмента одного или более параметров и секретного сертификата, но без учета секретного сертификата, сообщения и подписи; и

выполнения одного или более действий, возможных при определении, что подпись является действительной.

Пункт 23. Компьютерная система по п. 22, в которой:

память и один или более процессоров являются частью первой серверной системы, размещенной в первом географическом местоположении;

компьютерная система содержит вторую серверную систему, размещенную во втором географическом местоположении, причем вторая серверная система сконфигурирована для генерирования отличной подписи, по меньшей мере, частично на основе секретного сертификата;

первая серверная система и вторая серверная система не содержат секретного сертификата;

анализ сообщения и подписи включает в себя ввод в функцию, по меньшей мере, фрагмента одного или более параметров и промежуточного сертификата; и

как первая серверная система, так и вторая серверная система не содержат информации, с использованием которой при помощи функции на основе сообщения может быть сгенерирована одинаковая подпись.

Пункт 24. Компьютерная система по п. 22, при этом:

компьютерная система соответствует определенной службе; и

упомянутое одно или более действий включают в себя предоставление доступа к этой службе.

Пункт 25. Компьютерная система по п. 24, в которой один или более параметров ограничивают использование промежуточного сертификата при реализации доступа к службе.

Пункт 26. Компьютерная система по п. 22, в которой:

анализ сообщения и подписи включает в себя применение хэш-функции к промежуточному сертификату;

один или более параметров включают в себя множество ограничений на использование промежуточного сертификата; и

при этом компьютерная система сконфигурирована для приведения в исполнение упомянутых ограничений.

Пункт 27. Компьютерная система по п. 22, в которой:

анализ сообщения и подписи включает в себя применение хэш-функции к ключу, который получен на основе секретного сертификата; и

команды при выполнении одним или более процессорами компьютерной системы дополнительно обеспечивают осуществление компьютерной системой приема полученного ключа от компьютерной системы авторизации ключей.

Пункт 28. Компьютерная система по п. 27, в которой команды, дополнительно обеспечивающие осуществление компьютерной системой приема полученного ключа от компьютерной системы авторизации ключей, обеспечивают осуществление

компьютерной системой приема полученного ключа от компьютерной системы авторизации ключей до момента приема сообщения.

Пункт 29. Компьютерная система по п. 22, в которой промежуточный сертификат определяется другой компьютерной системой, отличной от указанной компьютерной системы.

[0115] Также могут быть выполнены различные варианты реализации изобретения в широком диапазоне операционных сред, которые в некоторых случаях могут содержать один или более компьютеров пользователя, вычислительные устройства или устройства обработки, которые могут быть использованы для работы с любым количеством приложений. Пользовательские или клиентские устройства могут включать любое число персональных компьютеров общего применения, например, настольные или портативные компьютеры, работающие со стандартными операционными системами, а также сотовые, беспроводные и мобильные устройства, работающие с мобильным программным обеспечением и способные поддерживать ряд сетевых протоколов и протоколов сообщений. Такие системы также могут включать ряд рабочих станций, работающих с использованием любых разновидностей коммерчески доступных операционных систем и других известных приложений для таких целей, как разработка и управление базами данных. Эти устройства также могут включать другие электронные устройства, такие как терминалы, тонкие клиенты, игровые системы и другие устройства, способные обмениваться данными посредством сети.

[0116] Большинство осуществлений изобретения используют, по меньшей мере, одну сеть, которая может быть хорошо известна специалистам в данной области техники, для поддержания обмена данными при помощи любого из вариантов коммерчески-доступных протоколов, например, TCP/IP, OSI, FTP, UPnP, NFS, CIFS, и AppleTalk. Сеть может быть, например, вычислительной локальной сетью, глобальной сетью, виртуальной наложенной сетью, сетями интернет, интранет, экстранет, коммутируемой телефонной сетью общего пользования, инфракрасной сетью, беспроводной сетью и любой соответствующей их комбинацией.

[0117] В вариантах реализации, использующих веб-сервер, веб-сервер может выполнять любое из ряда серверных приложений или приложений среднего звена, включая HTTP серверы, FTP серверы, CGI серверы, серверы данных, Java серверы и серверы бизнес-приложений. Сервер(ы) также могут быть с функцией выполнения программ или скриптов в ответ на запросы от пользовательских устройств, например, выполняя одно или более веб-приложений, которые могут быть реализованы как один или более скриптов или программ, написанных на любом языке программирования, например, Java®, C, C# или C++, или любой язык для написания скриптов, например Perl, Python, или TCL, а также соответствующей их комбинацией. Сервер(ы) могут также включать серверы базы данных, включая без ограничения коммерчески доступные серверы от Oracle®, Microsoft®, Sybase®, и IBM®.

[0118] Вычислительная среда, которая может включать хранилища данных и другую память, а также носители информации, как описано ниже. Эти носители информации могут находиться во многих местах, например локально в хранилище данных (и/или размещены в них) одного или более компьютеров, или удаленно от всех компьютеров в сети. В той или иной совокупности вариантов реализации изобретения информация может постоянно храниться в сети хранения данных («SAN»), известной специалистам в данной области техники. Таким же образом файлы, необходимые для выполнения функций, характерных компьютерам, серверам или другим сетевым устройствам, могут сохраняться локально и/или, при необходимости, удаленно. В случае когда система

содержит компьютерные устройства, каждое такое устройство может содержать элементы аппаратного обеспечения, которые могут быть электрически соединены посредством шины, элементы, включающие, например, по меньшей мере, один центральный процессор (CPU), по меньшей мере, одно устройство ввода (например, мышь, клавиатуру, контроллер, сенсорный дисплей или дополнительную клавиатуру), и, по меньшей мере, одно устройство вывода (например, дисплейное устройство, принтер или громкоговоритель). Такая система может также содержать одно или более устройств хранения данных, например, дисковые накопители, оптические устройства хранения информации, полупроводниковые запоминающие устройства, например оперативная память («RAM») или постоянное запоминающее устройство («ROM»), а также и съемные носители информации, карты памяти, карты флэш-памяти, и так далее.

[0119] Такие устройства также могут содержать устройство считывания машиночитаемых средств хранения данных, устройство связи (например, модем, сетевой адаптер (беспроводной или проводной), устройство инфракрасной связи, и т.д.), и функционирующую память, как описано выше. Устройство считывания машиночитаемых средств хранения данных может быть соединено с машиночитаемыми носителями информации, или сконфигурировано для приема машиночитаемых носителей информации, представленных удаленными, локальными, несъемными и/или съемными устройствами хранения данных, а также носителями информации для временного и/или более постоянного размещения, хранения, передачи, и извлечения машиночитаемой информации. Системы и различные устройства также обычно могут содержать ряд программных приложений, модулей, служб или других элементов, совмещенных с, по меньшей мере, одним функционирующим устройством памяти, включая операционную систему и программные приложения, например, клиентское приложение или веб-браузер. Следует принять во внимание, что альтернативные варианты реализации могут иметь вид описанных выше вариантов. Например, также могут использоваться настроенные пользователем аппаратные средства и/или конкретные элементы могут быть реализованы аппаратно, программно (включая мобильное программное обеспечение, например апплеты), или и тем, и другим способом. Также может быть задействовано соединение с другими компьютерными устройствами, например сетевыми устройствами ввода-вывода.

[0120] Носители информации и машиночитаемые носители информации для размещения кода, или фрагментов кода, которые могут содержать любые подходящие носители, известные специалистам в данной области, включая носители информации и коммуникационную среду, например, но не ограничиваясь этим, энергозависимые и энергонезависимые, съемные или несъемные носители, реализованные с помощью любого способа или технологии хранения информации и/или передачи информации, например машиночитаемых команд, структур данных, программных модулей, или других данных, включая RAM, ROM, EEPROM, флэш-память или другие технологии накопителей, CD-ROM, компакт-диски формата DVD или другие оптические носители, кассеты с магнитной лентой, магнитную ленту, накопитель на магнитных дисках или другие магнитные запоминающие устройства, или другие носители, которые могут быть использованы для хранения необходимой информации и доступ к которым может быть предоставлен системными устройствами. Основываясь на раскрытии сущности изобретения и предоставленной в настоящей заявке идее, специалист в данной области примет во внимание другие пути и/или способы реализации различных осуществлений изобретения.

[0121] Описание и графические материалы, соответственно, являются

пояснительными, а не ограничивающими. При этом будет очевидным, что различные модификации и изменения могут быть сделаны без отступления от существа и объема настоящего изобретения в силу предусмотренного формулой изобретения.

[0122] Другие варианты соответствуют идее настоящего раскрытия сущности изобретения. Следовательно, в то время как раскрытые алгоритмы подвержены различным модификациям и альтернативным конструкциям, отдельные варианты реализации изобретения показаны графически и детально описаны выше. Следует при этом понимать, что нет смысла ограничивать изобретение конкретной формой или формами раскрытия, но напротив, есть смысл в раскрытии всех модификаций, альтернативных конструкций и эквивалентов, вытекающих из идеи и объема изобретения, как определено в прилагаемой формуле изобретения.

[0123] Термины «включающий», «имеющий» и «содержащий» подразумевают неограничивающие термины (например, означающие «включая, без ограничений ими»), за исключением случаев, когда указано иначе. Термин «соединен» подразумевает, частично или целиком, «включен в», «подключен к» или «соединен вместе», даже если происходит что-либо. Перечисление диапазонов значений в настоящей заявке предназначено всего лишь, чтобы служить в качестве способа сокращения, относящегося по отдельности к каждому отдельно взятому значению, вытекающему из диапазона, за исключением случаев отображенных в настоящей заявке иным образом, и каждое отдельно взятое значение является включенным в описание, как если бы оно было изложено в настоящей заявке по отдельности. Все способы, описанные в настоящей заявке, могут быть выполнены в любом соответствующем порядке, за исключением случаев, отображенных в настоящей заявке иным образом или иным образом однозначно не противоречащих контексту. Использование любого и всех примеров, или иллюстративного языка (в том числе «например»), предоставленного в настоящей заявке, предназначено лишь для того, чтобы лучше осветить варианты реализации изобретения, и не предлагает ограничения на границы объема изобретения за исключением случаев, когда заявлено иным образом. Язык заявки в описании должен подразумевать отображение любого незаявленного элемента как неотъемлемую часть практической реализации изобретения.

[0124] Предпочтительный вариант реализации этого раскрытия сущности изобретения описан в настоящей заявке, включая наилучший вариант, известный изобретателям для реализации изобретения. Вариации этих предпочтительных вариантов изобретения могут стать очевидными для специалистов в данной области в результате чтения предшествующего описания. Изобретатели предполагают, что будут задействованы специалисты в данной области, и подразумевают, что изобретение может быть реализовано иным образом, чем конкретно описано в настоящей заявке. Соответственно, это изобретение, которое включает все модификации и эквиваленты предмета изобретения, изложенные в формуле изобретения и приложенные к настоящей заявке, в рамках действующего законодательства. Кроме того, любая комбинация вышеописанных элементов во всех возможных вариантах, соответственно, охвачена изобретением, за исключением отображенного в настоящей заявке иным образом, явно противоречащим контексту.

[0125] Все ссылки, включающие публикации, патентные заявки и патенты процитированы в настоящей заявке и включены в ее состав посредством ссылки в той же мере, как если бы каждая ссылка была отдельно и особо отображена включенной посредством ссылки и была изложена в настоящей заявке во всей полноте.

(57) Формула изобретения

1. Компьютерно-реализуемый способ управления доступом к одному или более вычислительным ресурсам провайдера вычислительных ресурсов, содержащий:

под управлением одной или более компьютерных систем, функционирующих на основе выполняемых команд,

прием от первого объекта запроса делегирования, выполнение которого включает в себя разрешение второму объекту привилегии доступа к вычислительному ресурсу;

генерирование ключа сеанса на основе, по меньшей мере частично, ограничения и секретного сертификата, совместно используемого с первым объектом;

предоставление ключа сеанса первому объекту;

прием от второго объекта запроса доступа на осуществление доступа к вычислительному ресурсу, причем запрос доступа включает в себя ключ сеанса, предоставленный первому объекту;

подтверждение запроса доступа на основе, по меньшей мере частично, ключа сеанса, содержащегося в запросе доступа; и

разрешение второму объекту доступа к вычислительному ресурсу.

2. Компьютерно-реализуемый способ по п.1, в котором ограничение соответствует подлинности зоны ключей из множества зон ключей.

3. Компьютерно-реализуемый способ по п.1, в котором:

запрос делегирования включает в себя подлинность объекта, для которого должен быть сгенерирован ключ сеанса; и

ограничение основано, по меньшей мере частично, на подлинности объекта.

4. Компьютерно-реализуемый способ по п.1, в котором ограничение соответствует ограничению в отношении предопределенного действия.

5. Компьютерно-реализуемый способ по п.1, в котором:

запрос доступа дополнительно включает в себя ограничение, предоставленное первым объектом; и

подтверждение запроса доступа включает в себя подтверждение, что ключ сеанса был сгенерирован на основе, по меньшей мере частично, ограничения, содержащегося в запросе доступа.

6. Компьютерно-реализуемый способ по п.1, в котором ограничение соответствует ограничению количества времени, когда ключ сеанса является действительным.

7. Компьютерная система для обеспечения доступа к вычислительным ресурсам, содержащая:

один или более процессоров; и память, включающую в себя команды, которые при исполнении одним или более процессорами побуждают систему:

принимать от первого объекта запрос делегирования, выполнение которого включает в себя разрешение второму объекту привилегии доступа к вычислительному ресурсу;

в ответ на прием запроса делегирования:

генерировать ключ сеанса на основе, по меньшей мере частично, передачи секретного сертификата, совместно используемого между первым объектом и одной или более компьютерными системами, и ограничения сеанса через алгоритм криптографического хэширования; и предоставлять ключ сеанса первому объекту;

принимать от второго объекта запрос доступа на осуществление доступа к вычислительному ресурсу, причем запрос доступа связан с ключом сеанса; и в ответ на прием запроса доступа:

подтверждать запрос доступа на основе, по меньшей мере частично, ключа сеанса;

и разрешать второму объекту доступ к вычислительному ресурсу.

8. Система по п.7, в которой команды, которые подтверждают запрос доступа, включают в себя команды, которые побуждают систему подтверждать, соответствует ли запрос ограничению сеанса.

9. Система по п.7, в которой запрос доступа является первым запросом доступа и команды дополнительно включают в себя команды, которые побуждают систему:

принимать второй запрос доступа от третьего объекта для осуществления доступа к вычислительному ресурсу, причем второй запрос доступа связан с ключом сеанса; и

в ответ на прием второго запроса доступа:

подтверждать второй запрос доступа на основе, по меньшей мере частично, ключа сеанса; и разрешать третьему объекту доступ к вычислительному ресурсу.

10. Система по п.7, дополнительно содержащая первый объект, причем первый объект содержит одну или более компьютерных систем, функционирующих на основе первых команд, которые при исполнении одной или более компьютерными системами побуждают одну или более компьютерных систем, в результате приема ключа сеанса, предоставлять ключ сеанса второму объекту без предоставления секретного сертификата второму объекту.

11. Система по п.10, в котором первые команды, которые предоставляют ключ сеанса второму объекту, включают в себя команды, которые побуждают одну или более компьютерных систем предоставлять информацию, применяемую вторым объектом для получения ключа сеанса, на электронный адрес получателя, доступный второму объекту.

12. Система по п.11, в которой электронный адрес получателя представляет собой адрес электронной почты.

13. Система по п.7, в которой команды, которые побуждают систему подтверждать запрос доступа, включают в себя команды, которые побуждают систему применять алгоритм криптографического хэширования как к первому набору входных значений, так и ко второму набору входных значений, при этом:

первый набор входных значений включает в себя секретный сертификат, запрос доступа и ограничение сеанса; и

второй набор входных значений включает в себя ключ сеанса и запрос доступа.

14. Система по п.13, в которой алгоритм криптографического хэширования представляет собой хэш-функцию кода аутентификации сообщений.

15. Система по п.7, в которой запрос доступа связан с ключом сеанса за счет обеспечения цифровой подписи с запросом доступа, сгенерированным с использованием ключа сеанса.

16. Система по п.15, в которой команды, которые побуждают систему подтверждать запрос доступа, включают в себя команды, которые побуждают систему:

применять алгоритм криптографического хэширования к секретному сертификату, запросу доступа и ограничению сеанса для получения результата хэширования; и

сравнивать результат хэширования с цифровой подписью.

17. Постоянный машиночитаемый носитель информации, на котором хранятся исполняемые команды, которые при исполнении одним или более процессорами компьютерной системы по любому из пп. 7-16 побуждают компьютерную систему, по меньшей мере:

принимать от первого объекта первый запрос, выполнение которого включает в себя разрешение второму объекту привилегии доступа к вычислительному ресурсу;

генерировать ключ сеанса на основе, по меньшей мере частично, ограничения и

секретного сертификата, совместно используемого между объектом и компьютерной системой;

предоставлять ключ сеанса, применяемый, по меньшей мере частично, для подтверждения владения привилегией доступа к вычислительному ресурсу, первому объекту;

принимать второй запрос доступа к вычислительному ресурсу, выполнение которого включает в себя предоставление второму объекту доступа к вычислительному ресурсу, причем второй запрос связан с ключом сеанса;

подтверждать второй запрос на основе, по меньшей мере частично, ключа сеанса; и

выполнять второй запрос за счет предоставления доступа к вычислительному ресурсу в зависимости от, по меньшей мере частично, подтверждения ключа сеанса.

18. Постоянный машиночитаемый носитель информации по п. 17, в котором исполняемые команды, которые побуждают компьютерную систему выполнять второй запрос, включают в себя исполняемые команды, которые побуждают компьютерную систему выполнять второй запрос без предоставления второму объекту доступа к секретному сертификату.

19. Постоянный машиночитаемый носитель информации по п.17, в котором исполняемые команды дополнительно включают в себя исполняемые команды, которые побуждают компьютерную систему:

принимать третий запрос доступа к вычислительному ресурсу, выполнение которого включает в себя предоставление третьему объекту доступа к вычислительному ресурсу, причем третий запрос связан с ключом сеанса;

подтверждать третий запрос на основе, по меньшей мере частично, ключа сеанса; и

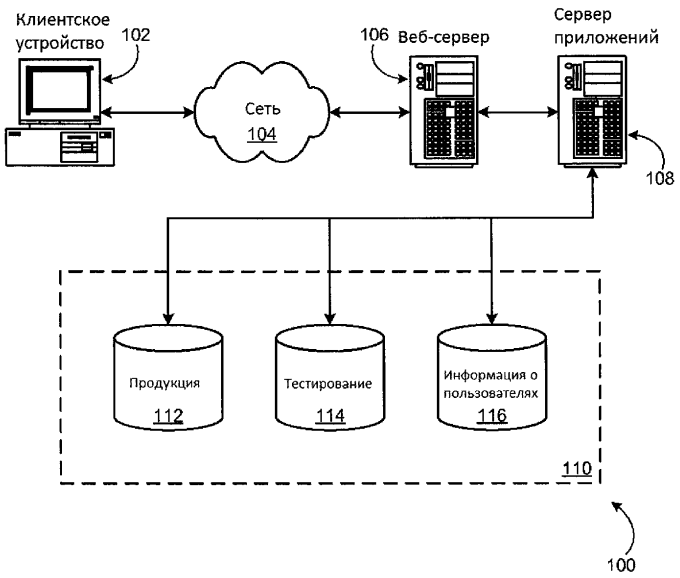
выполнять третий запрос за счет предоставления доступа к вычислительному ресурсу в зависимости от, по меньшей мере частично, подтверждения ключа сеанса.

20. Постоянный машиночитаемый носитель информации по п.17, в котором:

второй запрос включает в себя цифровую подпись, сгенерированную с использованием ключа сеанса; и

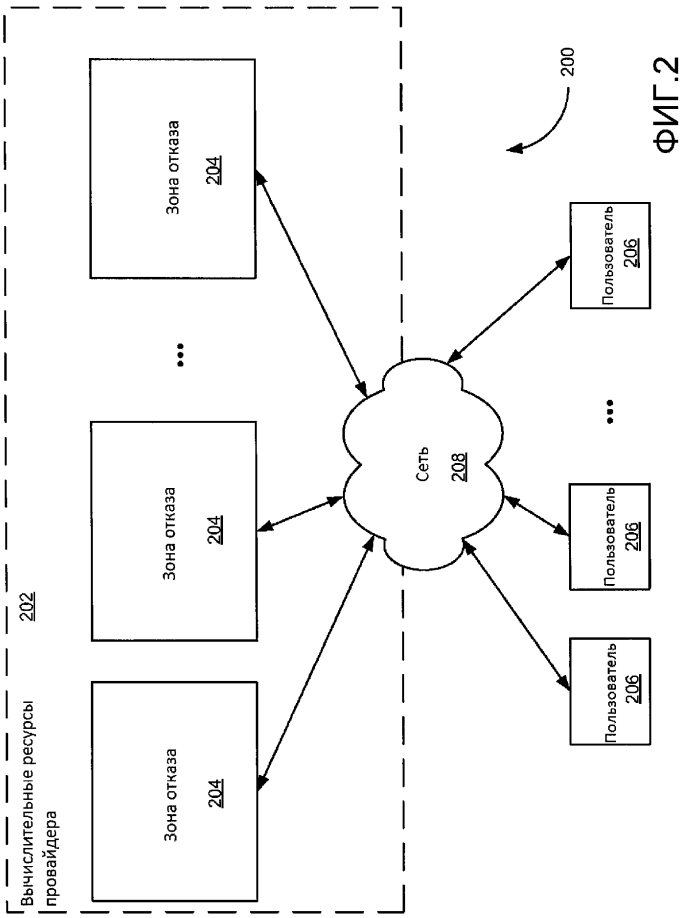
подтверждение второго запроса дополнительно включает в себя подтверждение аутентификации цифровой подписи.

1


Клиентское устройство
102
Сеть
104
106 Веб-сервер
Сервер приложений
108
Продукция
112
Тестирование
114
Информация о пользователях
116
110
100

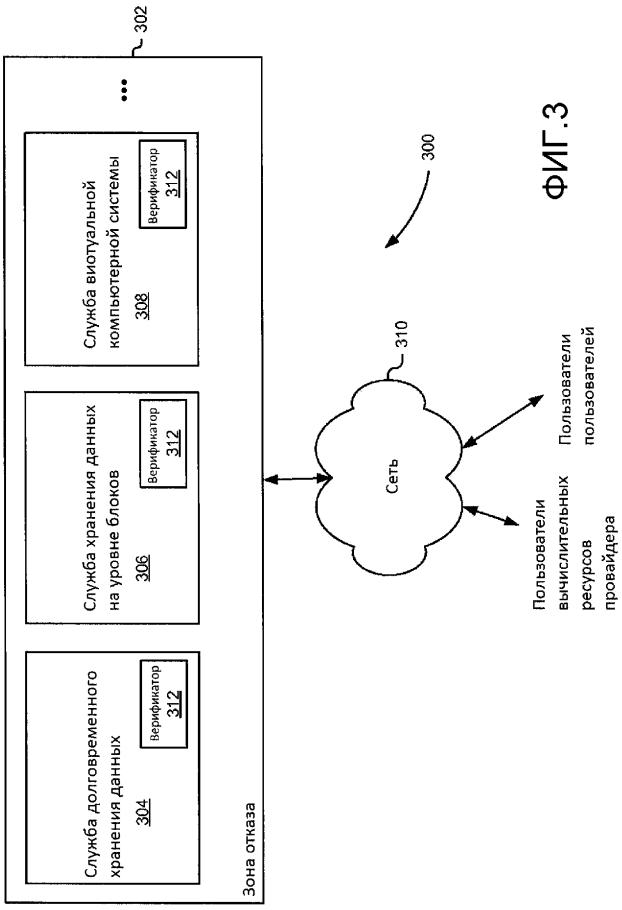
ФИГ.1

2


200
Вычислительные ресурсы провайдера
202
Зона отказа
204
Зона отказа
204
Зона отказа
204
Сеть
208
Пользователь
206
Пользователь
206
Пользователь
206

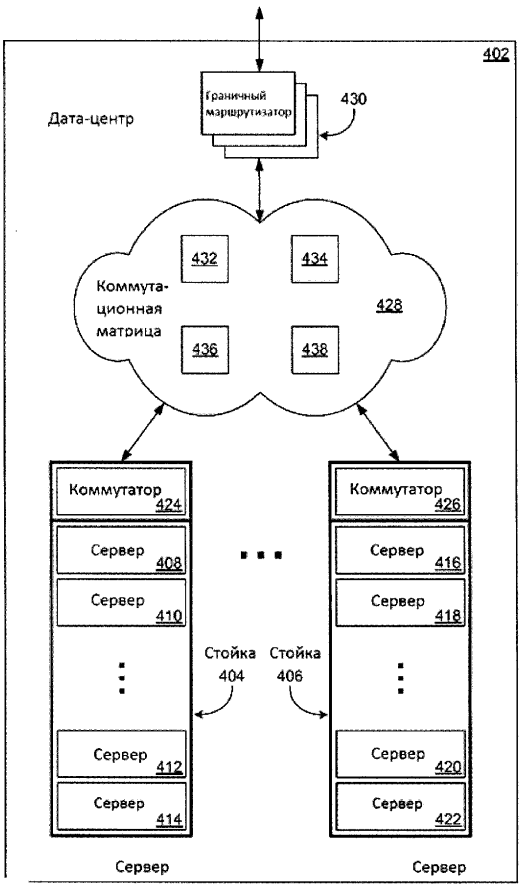
ФИГ.2

3

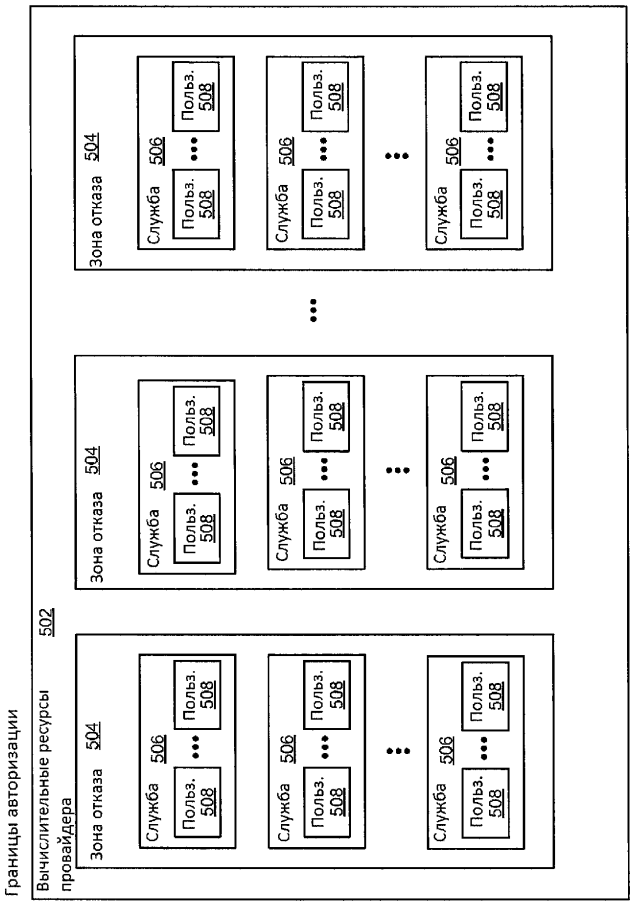

302
Служба виртуальной компьютерной системы
308
Верификатор
312
Служба хранения данных на уровне блоков
306
Верификатор
312
Служба долговременного хранения данных
304
Верификатор
312
Зона отказа
300
310
Сеть
Пользователи вычислительных ресурсов провайдера
Пользователи пользователей

ФИГ.3

4

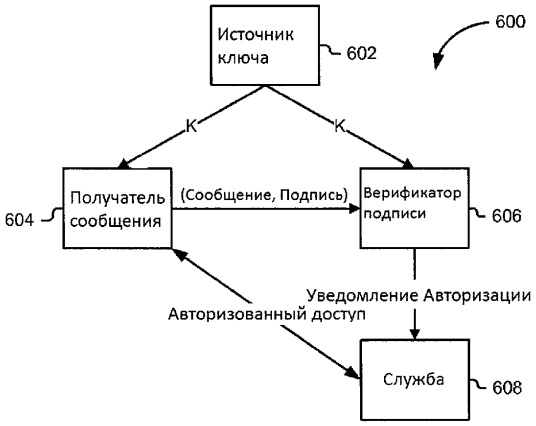

402
Дата-центр
Граничный маршрутизатор
430
Коммута-ционная матрица
432
434
436
438
428
Коммутатор 424
Коммутатор 426
Сервер 408
Сервер 410
Сервер 412
Сервер 414
Сервер 416
Сервер 418
Сервер 420
Сервер 422
Стойка 404
Стойка 406
Сервер
Сервер

ФИГ.4


Границы авторизации
Вычислительные ресурсы провайдера 502
Зона отказа 504
Служба 506
Польз. 508

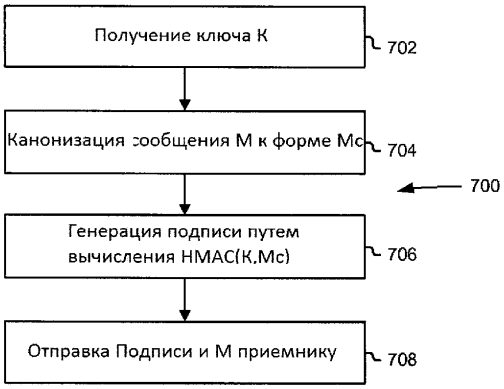
ФИГ.5

6

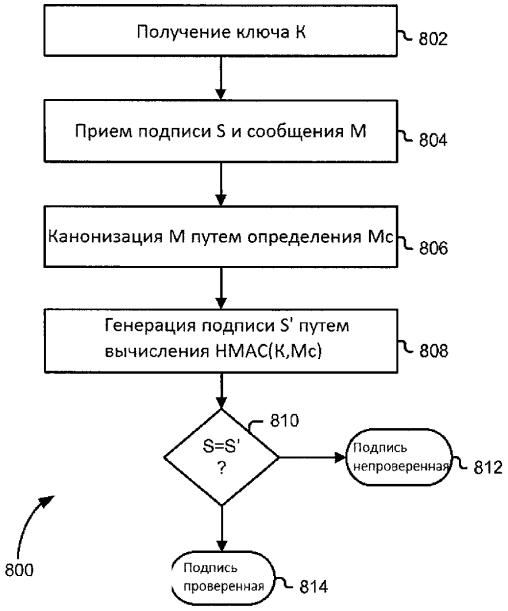

Источник ключа
602
600
K
K
Получатель сообщения
604
(Сообщение, Подпись)
Верификатор подписи
606
Уведомление Авторизации
Авторизованный доступ
Служба
608

ФИГ.6

7

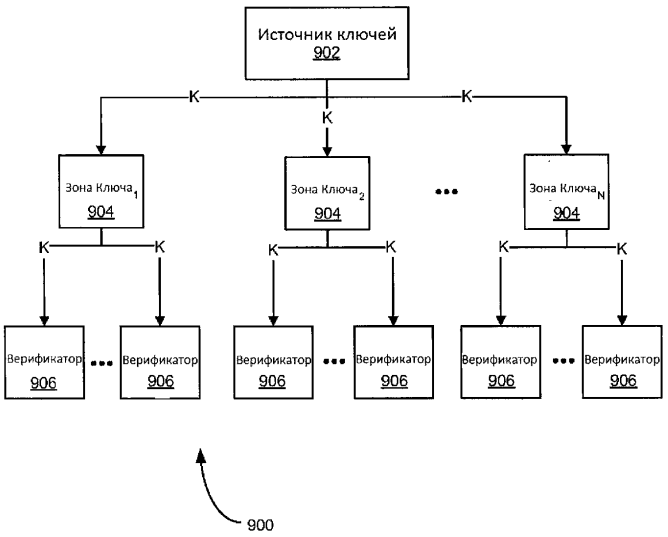

Получение ключа К
702
Канонизация сообщения М к форме Мс
704
700
Генерация подписи путем вычисления HMAC(K,Mc)
706
Отправка Подписи и М приемнику
708

ФИГ.7


Получение ключа K
802
Прием подписи S и сообщения M
804
Канонизация M путем определения Mc
806
Генерация подписи S' путем вычисления HMAC(K,Mc)
808
810
S=S' ?
Подпись непроверенная
812
800
Подпись проверенная
814

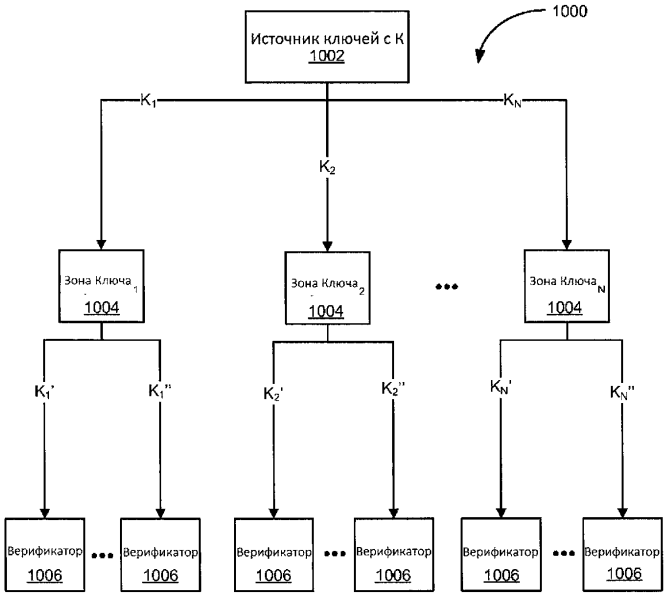
ФИГ.8

9

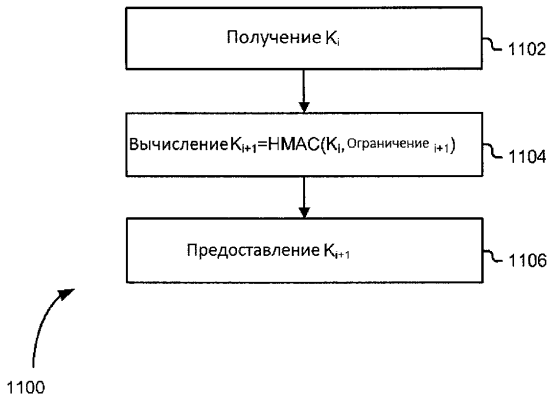

Источник ключей
902
K
K
K
K
Зона Ключа1
904
Зона Ключа2
904
Зона КлючаN
904
Верификатор
906
900

ФИГ.9

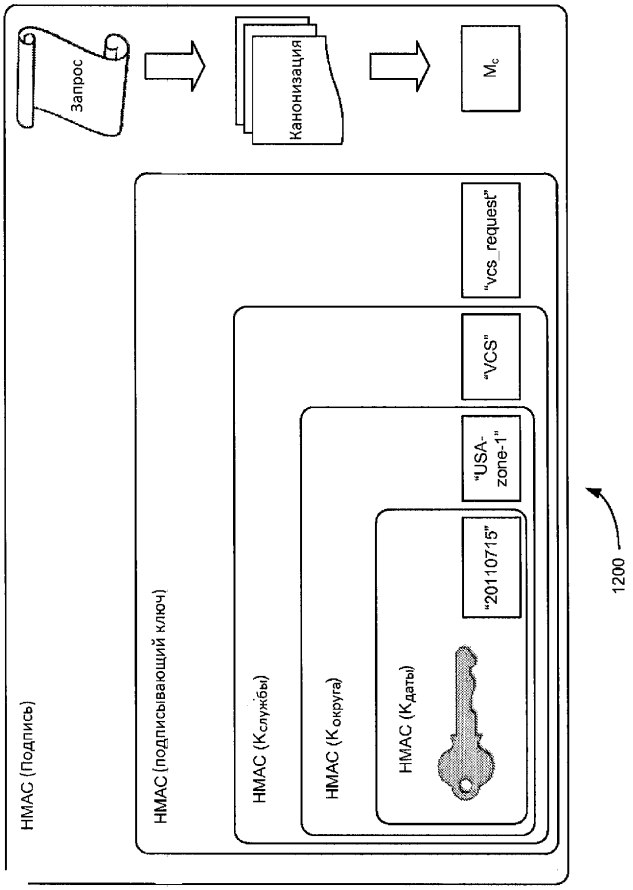
10


1000
Источник ключей с K
1002
K1
KN
K2
Зона Ключа1
1004
Зона Ключа2
1004
Зона КлючаN
1004
K1'
K1''
K2'
K2''
KN'
KN''
Верификатор
1006
Верификатор
1006
Верификатор
1006
Верификатор
1006
Верификатор
1006
Верификатор
1006

ФИГ.10

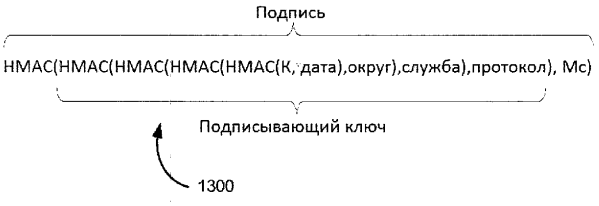

Получение K_i
1102
Вычисление K_{i+1}=HMAC(K_i, Ограничение $_{i+1}$)
1104
Предоставление K_{i+1}
1106
1100

ФИГ.11


Запрос
Канонизация
M_c
HMAC (Подпись)
HMAC (подписывающий ключ)
HMAC ($K_{службы}$)
HMAC ($K_{округа}$)
HMAC ($K_{даты}$)
"20110715"
"USA-zone-1"
"VCS"
"vcs_request"
1200

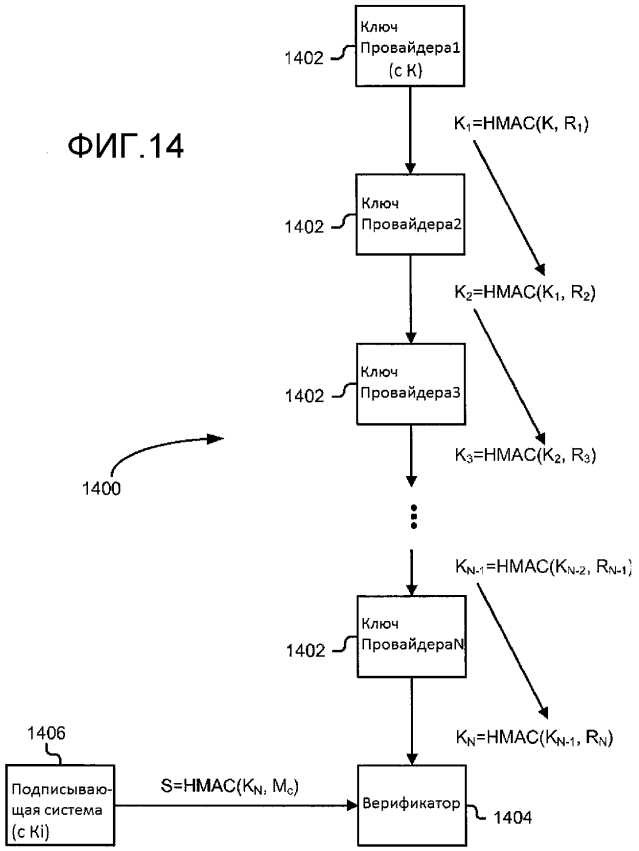
ФИГ.12

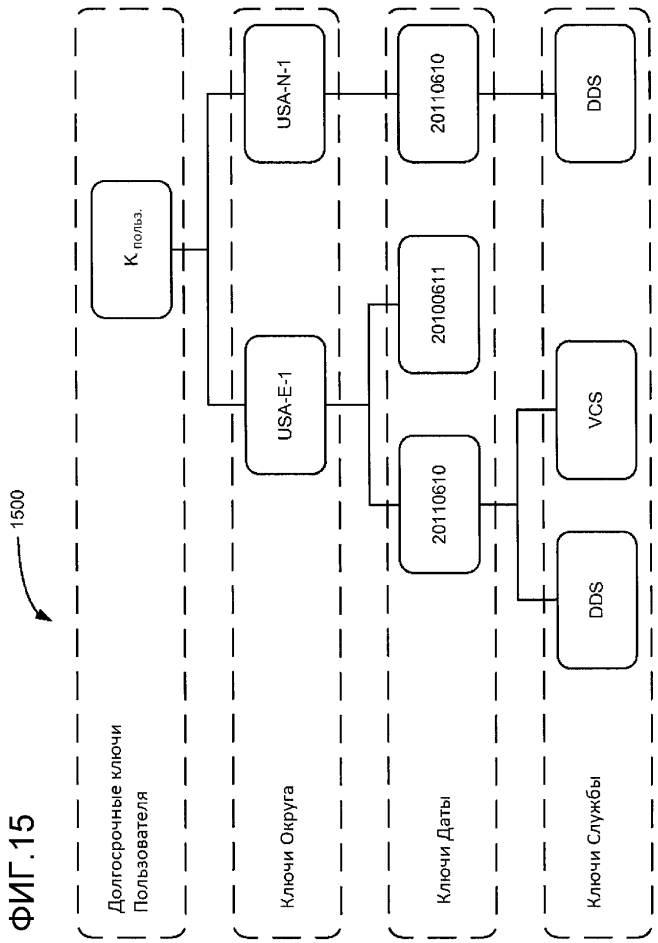
13


Подпись
HMAC(HMAC(HMAC(HMAC(HMAC(K, дата),округ),служба),протокол), Mc)
Подписывающий ключ
1300

ФИГ.13

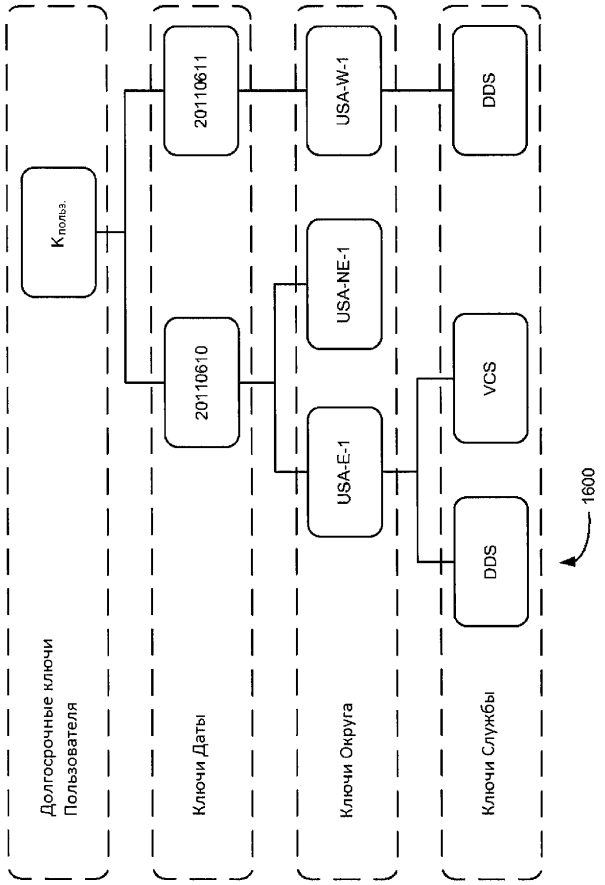
ФИГ.14


Ключ Провайдера1 (с K)
1402
K1=HMAC(K, R1)
Ключ Провайдера2
1402
K2=HMAC(K1, R2)
Ключ Провайдера3
1402
K3=HMAC(K2, R3)
1400
KN-1=HMAC(KN-2, RN-1)
Ключ ПровайдераN
1402
KN=HMAC(KN-1, RN)
1406
Подписывающая система (с Ki)
S=HMAC(KN, Mc)
Верификатор
1404


1500
Долгосрочные ключи Пользователя
Ключи Округа
Ключи Даты
Ключи Службы
K польз.
USA-N-1
USA-E-1
20110610
20100611
20110610
DDS
VCS
DDS

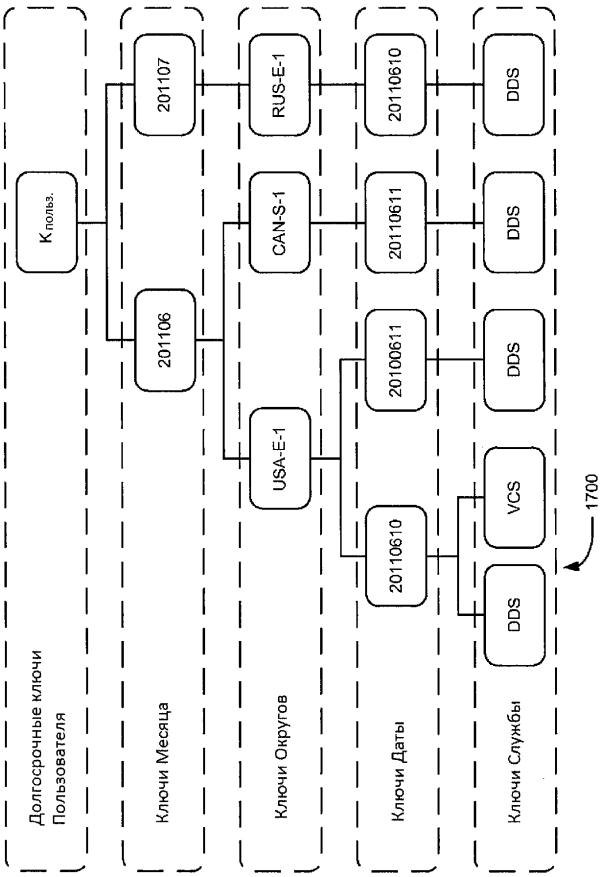
ФИГ.15

16

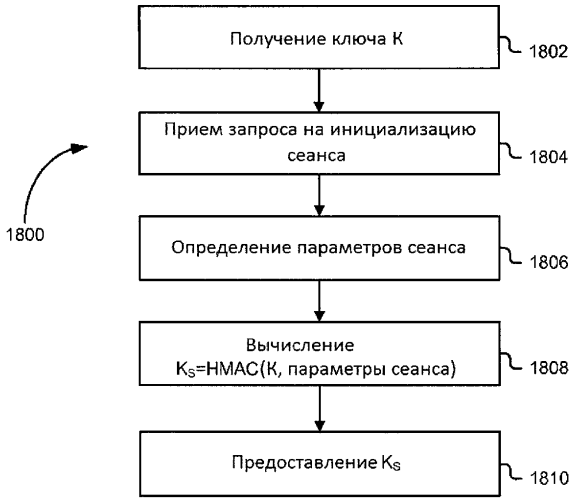

Долгосрочные ключи Пользователя
$K_{польз.}$
Ключи Даты
20110611
20110610
Ключи Округа
USA-W-1
USA-NE-1
USA-E-1
Ключи Службы
DDS
VCS
DDS
1600

ФИГ.16

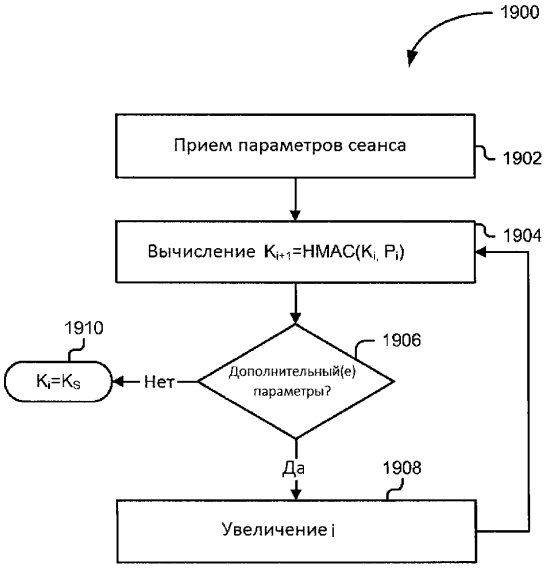
17


Долгосрочные ключи Пользователя
Ключи Месяца
Ключи Округов
Ключи Даты
Ключи Службы
Kполь.
201107
201106
RUS-E-1
CAN-S-1
USA-E-1
20110610
20110611
20100611
20110610
DDS
DDS
DDS
VCS
DDS
1700

ФИГ.17

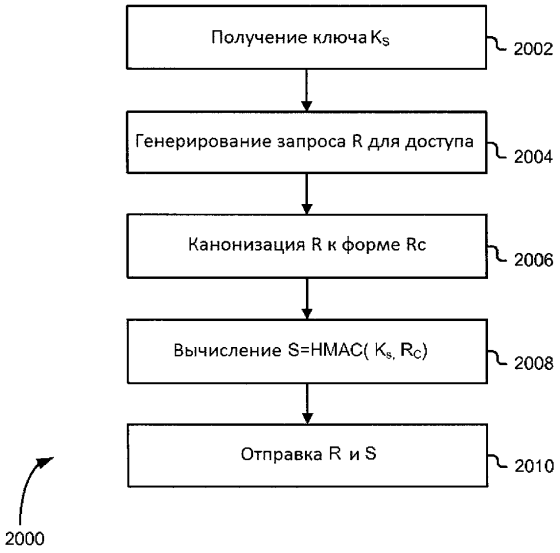

Получение ключа К
1802
Прием запроса на инициализацию сеанса
1804
1800
Определение параметров сеанса
1806
Вычисление
K_S=HMAC(K, параметры сеанса)
1808
Предоставление K_S
1810

ФИГ.18


1900
Прием параметров сеанса
1902
Вычисление K_{i+1}=HMAC(K_i, P_i)
1904
1910
1906
K_i=K_S
Нет
Дополнительный(е) параметры?
Да
1908
Увеличение i

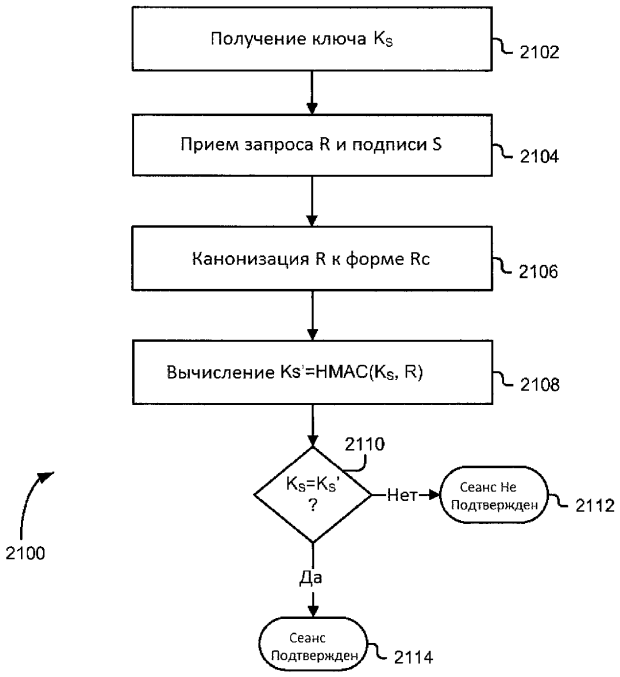
ФИГ.19

20


Получение ключа K_S
2002
Генерирование запроса R для доступа
2004
Канонизация R к форме Rc
2006
Вычисление S=HMAC(K_S, R_C)
2008
Отправка R и S
2010
2000

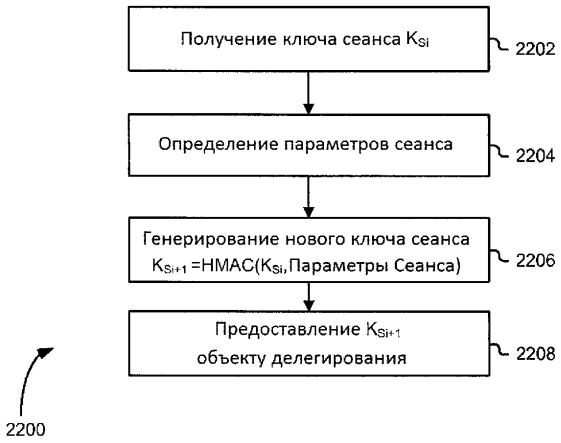
ФИГ.20

21


Получение ключа K_S
2102
Прием запроса R и подписи S
2104
Канонизация R к форме Rc
2106
Вычисление Ks'=HMAC(K_S, R)
2108
2110
K_S=K_S' ?
Нет
Сеанс Не Подтвержден
2112
Да
Сеанс Подтвержден
2114
2100

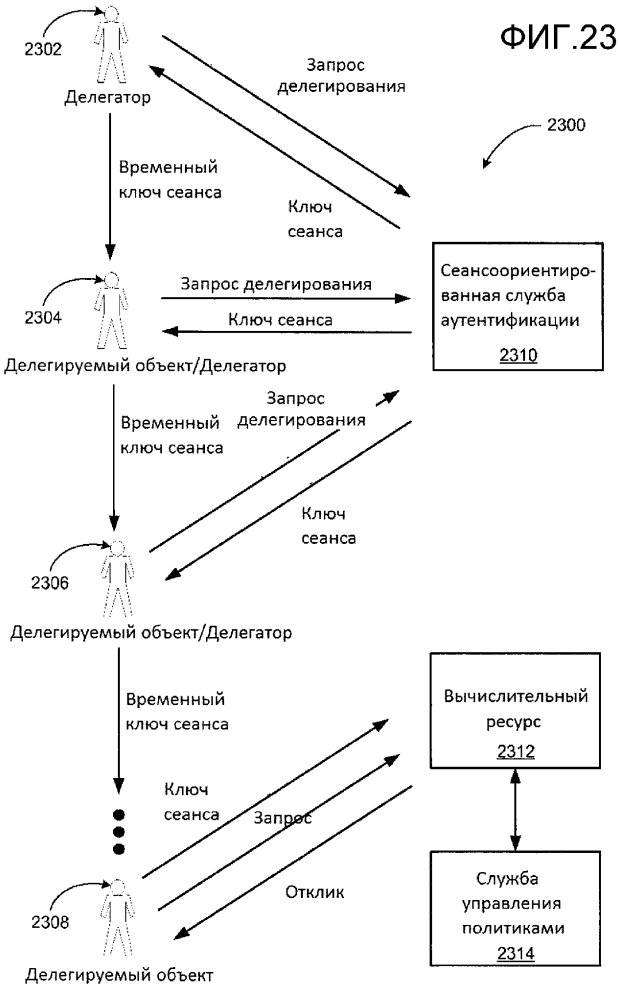
ФИГ.21

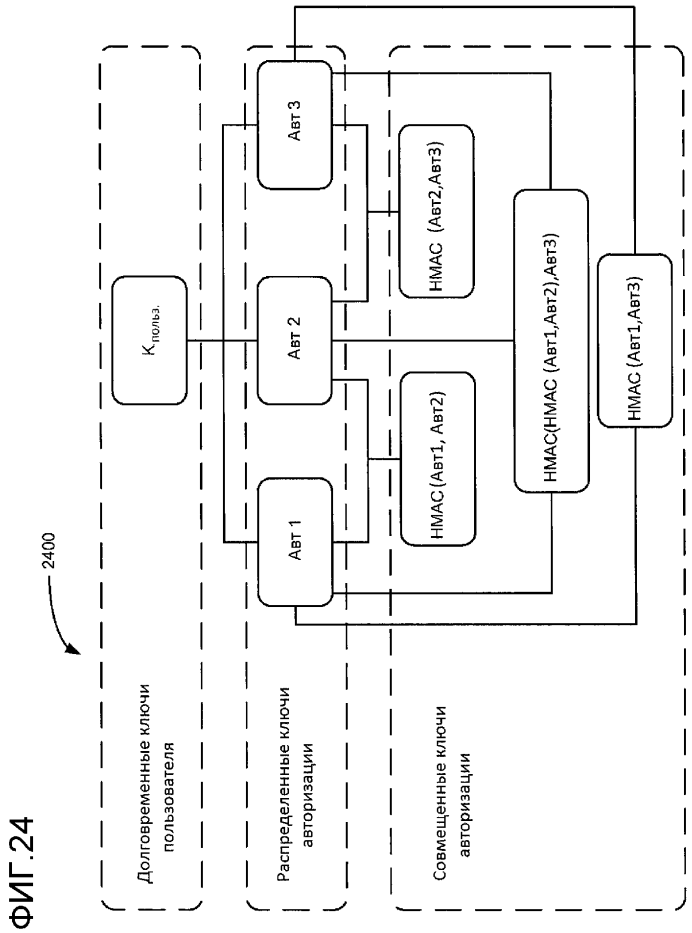
22


Получение ключа сеанса K_{Si}
2202
Определение параметров сеанса
2204
Генерирование нового ключа сеанса
K_{Si+1} =HMAC(K_{Si},Параметры Сеанса)
2206
Предоставление K_{Si+1}
объекту делегирования
2208
2200

ФИГ.22

ФИГ.23


2302
Делегатор
Запрос делегирования
2300
Временный ключ сеанса
Ключ сеанса
Сеансоориентированная служба аутентификации
2310
Запрос делегирования
Ключ сеанса
2304
Делегируемый объект/Делегатор
Временный ключ сеанса
Запрос делегирования
Ключ сеанса
2306
Делегируемый объект/Делегатор
Временный ключ сеанса
Вычислительный ресурс
2312
Ключ сеанса
Запрос
Отклик
2308
Делегируемый объект
Служба управления политиками
2314


2400
Долговременные ключи пользователя
Распределенные ключи авторизации
Совмещенные ключи авторизации
$K_{польз.}$
Авт 1
Авт 2
Авт 3
HMAC (Авт1, Авт2)
HMAC (Авт2,Авт3)
HMAC(HMAC (Авт1,Авт2),Авт3)
HMAC (Авт1,Авт3)

ФИГ.24