(19) Евразийское патентное ведомство

(21) 201900350 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2020.12.30

(22) Дата подачи заявки
2019.06.05

(51) Int. Cl. ***G06F 13/00*** (2006.01)
G06F 21/60 (2006.01)

(54) СПОСОБ ХРАНЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННОМ РЕЕСТРЕ, ПОЛУЧЕНИЯ ИНФОРМАЦИИ ИЗ РАСПРЕДЕЛЕННОГО РЕЕСТРА И УСТАНОВЛЕНИЯ ПРАВ ДОСТУПА К ЗВЕНЬЯМ РАСПРЕДЕЛЕННОГО РЕЕСТРА

(96) **2019000055 (RU) 2019.06.05**

(71) Заявитель:
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ФИНТЕХ-ФОРЕНСИКА" (RU)

(72) Изобретатель:
Касперская Наталья Ивановна, Щербаков Андрей Юрьевич, Кузьменко Василий Владимирович (RU)

(74) Представитель:
Благополучная К.В. (RU)

(57) Изобретение относится к области техники и информатики, а более конкретно к способам хранения цифровой информации в распределенном реестре, получения информации из распределенного реестра и установления прав доступа к звеньям распределенного реестра. Настоящее изобретение может найти применение при создании, эксплуатации, управлении и мониторинге систем различного назначения, включая сложные финансовые, экономические и социальные системы, в которых интегрированы средства накопления и обмена различного рода информацией, информационными ресурсами, персональными данными и цифровыми активами. В основу настоящего изобретения положена задача создания таких способов хранения цифровой информации в распределенном реестре, получения информации из распределенного реестра и установления прав доступа к звеньям распределенного реестра, которые обеспечивали бы выполнение следующих свойств: наличие "точки входа" для пользователей - оператора распределенного реестра, который на основе заданных государственным или ведомственным регулятором регламентов обеспечивает обработку информации пользователей; авторизацию пользователя для оператора; безопасный транспорт (как минимум с сохранением неизменности информации (транзакции), получаемой от пользователя) для передачи информации от пользователя к оператору распределенного реестра; контроль целостности и авторства каждой информационной единицы, помещаемой в распределенный реестр; формирование подтверждений у оператора распределенного реестра о факте помещения информации в распределенный реестр (например, путем выдачи заверенных оператором квитанций пользователям); наличие механизма формирования и обработки запросов по выдаче информации из распределенного реестра по запросам его участников (клиентов), обеспечивающего защищенность данного запроса (также авторизацию и контроль неизменности запроса); реализацию у оператора распределенного реестра системы разграничения доступа к информации (к звеньям распределенного реестра).

201900350 A1

201900350 A1

ОПИСАНИЕ

Изобретение относится к области техники и информатики, а более конкретно – к способам хранения цифровой информации в распределенном реестре, получения информации из распределенного реестра и установления прав доступа к звеньям распределенного реестра.

Настоящее изобретение может найти применение при создании, эксплуатации, управлении и мониторинге систем различного назначения, включая сложные финансовые, экономические и социальные системы, в которых интегрированы средства накопления и обмена различного рода информацией, информационными ресурсами, персональными данными и цифровыми активами.

В основу настоящего изобретения положена задача создания таких способов хранения цифровой информации в распределенном реестре, получения информации из распределенного реестра и установления прав доступа к звеньям распределенного реестра, которые обеспечивал бы выполнение следующих свойств:

- наличие “точки входа” для пользователей – оператора распределенного реестра, который на основе заданных государственным или ведомственным регулятором регламентов обеспечивает обработку информации пользователей;

- авторизацию пользователя для оператора;

- безопасный транспорт (как минимум с сохранением неизменности информации (транзакции), получаемой от пользователя) для передачи информации от пользователя к оператору распределенного реестра;

- контроль целостности и авторства каждой информационной единицы, помещаемой в распределенный реестр, а также создание неизменной последовательности помещения информационных единиц в распределенный реестр;

- формирование подтверждений у оператора распределенного реестра о факте помещения информации в распределенный реестр (например, путем выдачи заверенных оператором квитанций пользователям);

- наличие механизма формирования и обработки запросов по выдаче информации из распределенного реестра по запросам его участников (клиентов), обеспечивающего защищенность данного запроса (также авторизацию и контроль неизменности запроса);

- реализацию у оператора распределенного реестра системы разграничения доступа к информации (к звеньям распределенного реестра).

Наиболее близким к данному изобретению является RU 2 673 385 C1. Дата регистрации: 26.11.2018. Изобретение относится к способам и средствам управления

процессами документирования и оценки аутентичности объектов, состоящих из наборов бит данных, и предназначено для создания автоматизированных систем контроля и мониторинга перемещения объектов из одного места хранения в другое. Техническим результатом является простой, удобный и надежный способ управления процессами подготовки состава объектов, перемещаемых с использованием электросвязи. Изобретение реализуется электронными устройствами, названными Почтовые Модули Пользователей (ПМП), которые, при их подключении к электронному оборудованию для обмена электронными сообщениями (ЭС), позволяют отправлять и принимать специальным образом дополнительно подготовленные ЭС в Информационно-Телекоммуникационной Сети (ИТС), используя технические и программные средства электронного устройства, реализующего возможность работы всех используемых ПМП, названного Удостоверяющей Системой (УС), которое имеет свой вариант ПМП, названный Почтовый Модуль Удостоверяющей Системы (ПМУС), и позволяет объединить ПМП в единую сеть (СПМП). А при прохождении наборов бит ЭС через СПМП формируются связанные между собой цепочки из идентификаторов данных ЭС и субъектов СПМП, сетевого адреса оборудования с ПМП, отправляющего ЭС, сетевого адреса УС с ПМУС и сетевого адреса оборудования с ПМП, получающего ЭС, и при этом в составе наборов бит ЭС создаются цепочки бит хэш-кодов (ХК), в которых каждый последующий ХК определяется с учетом предыдущего.

Данный прототип имеет следующие недостатки:

- способ не обеспечивает авторизацию пользователя для оператора;

- способ не обеспечивает безопасный транспорт (с сохранением неизменности информации (транзакции), получаемой от пользователя) для передачи информации от пользователя к оператору распределенного реестра;

- способ не обеспечивает контроль целостности и авторства каждой информационной единицы, помещаемой в распределенный реестр;

- способ привязан к оборудованию (сетевому адресу оборудования), что существенно снижает его применимость (универсальность) и не позволяет построить чисто программные системы;

- способ не обеспечивает формирование подтверждений у оператора распределенного реестра о факте помещения информации в распределенный реестр;

- отсутствует механизм формирования и обработки запросов по выдаче информации из распределенного реестра по запросам его участников (клиентов);

- способ не обеспечивает реализацию у оператора распределенного реестра системы разграничения доступа к информации (к звеньям распределенного реестра).

Другим близким изобретением является RU 2004 130 423A СПОСОБ УПРАВЛЕНИЯ ПРАВАМИ НА ЗАШИФРОВАННЫЕ ДАННЫЕ, ХРАНЯЩИЕСЯ НА ЦИФРОВОМ РЕГИСТРАТОРЕ, согласно которому реализуется способ хранения события, зашифрованного с использованием одного или нескольких управляющих слов (CW) в приемнике/декодере (STB), подключенном к блоку (SC) безопасности, причем права доступа к указанному событию содержатся в сообщениях по контролю за доступом (ECM-сообщениях), отличающийся тем, что включает следующие операции: запись зашифрованного события, а также ECM-сообщения или ECM-сообщений в блок хранения; передача ECM-сообщений в блок (SC) безопасности, верификация того, что в блоке (SC) безопасности содержатся права на указанное событие, расчет, по всему ECM-сообщению или по его части, квитанции (Q), которая содержит сигнатуру (SGN) и формируется с использованием секретного ключа (K), содержащегося в блоке (SC) безопасности и специфичного для каждого блока безопасности, хранение указанной квитанции (Q) в блоке хранения.

Кроме недостатков, перечисленных для предыдущего прототипа, данный прототип имеет еще недостаток, связанный с необходимостью шифрования данных.

Задачи изобретения решены и недостатки прототипов устранены в реализованных согласно настоящему изобретению способах - способе хранения цифровой информации в системе, состоящей, по меньшей мере из двух пользователей, характеризующихся неповторяющимися именами, оператора и распределенного реестра, представляющего собой массив данных, **отличающийся тем, что массив данных состоит из звеньев, который формирует оператор** на основе цифровой информации, получаемой от пользователей, и заключающемся в том, что:

- пользователь формируют цифровую информацию и снабжает ее кодом аутентификации, представляющем собой данные, полученные путем вычисления функции, зависящей от содержания цифровой информации, сформированной пользователем и личной информации, известной пользователю и оператору и неизвестной другим пользователя, в результате чего получают цифровой конверт пользователя, содержащий по меньшей мере информацию пользователя и код аутентификации;

- полученный цифровой конверт передают оператору, который проверяет его код аутентификации и, в случае его правильности, принимает цифровой конверт в обработку;

- оператор обрабатывает цифровой конверт, используя его целиком или выделяя го часть, включающую, по меньшей мере, цифровую информацию пользователя, получая в результате единицу хранения;

- оператор, используя единицу хранения и личную информацию оператора, неизвестную никому из пользователей, а также номер последнего звена в распределенном реестре и код аутентификации этого звена, формирует следующее звено распределенного реестра, путем добавления к единице хранения, по меньшей мере, нового порядкового номер звена, не совпадающего с номером предыдущего звена и кода аутентификации, вычисленного от единицы хранения, нового номера звена и кода аутентификации предыдущего звена;

- полученное следующее звено записывают в распределенный реестр.

А также способе получения цифровой информации в системе **распределенного реестра**, состоящей, по меньшей мере из двух пользователей, характеризующихся неповторяющимися именами, оператора и распределенного реестра, **отличающийся тем, что распределенный реестр состоит из звеньев, которые предварительно сформированы оператором на основе цифровой информации, получаемой от пользователей** и заключающемся в том, что:

- пользователь формируют запрос на получение цифровой информации из распределенного реестра и снабжает его кодом аутентификации, представляющем собой данные, полученные путем вычисления функции, зависящей от содержания запроса и личной информации, известной пользователю и оператору и неизвестной другим пользователям, получая тем самым доверенный запрос пользователя, содержащий по меньшей мере запрос пользователя и код аутентификации;

- полученный доверенный запрос передают оператору, который проверяет его код аутентификации и, в случае его правильности, принимает доверенный запрос в обработку;

- оператор обрабатывает доверенный запрос, извлекая из распределенного реестра одну или несколько единиц хранения в соответствии с информацией, содержащейся в запросе и правилами хранения информации в распределенном реестре;

- извлеченные звенья передают пользователю, сформировавшему запрос.

И способе установления прав доступа к распределенному реестру, когда запросом является перечень имен пользователей и сведения о звеньях, к которым эти пользователи будут иметь доступ.

Технически целесообразно в качестве кода аутентификации использовать: имитовставку, хеш-функцию или электронную подпись.

За счет реализации заявленного авторами способа достигаются следующие технические результаты:

- обеспечивается наличие “точки входа” для пользователей – оператора распределенного реестра;

- обеспечивается авторизация пользователя для оператора;

- обеспечивается безопасный транспорт (с сохранением неизменности информации (транзакции), получаемой от пользователя) для передачи информации от пользователя к оператору распределенного реестра;

- обеспечивается контроль целостности и авторства каждой информационной единицы, помещаемой в распределенный реестр, а также создание неизменной последовательности помещения информационных единиц в распределенный реестр;

- обеспечивается формирование подтверждений у оператора распределенного реестра о факте помещения информации в распределенный реестр;

- обеспечивается механизм формирования и обработки запросов по выдаче информации из распределенного реестра по запросам его участников (клиентов), обеспечивающего защищенность данного запроса (также авторизацию и контроль неизменности запроса);

- обеспечивается реализация у оператора распределенного реестра системы разграничения доступа к информации (к звеньям распределенного реестра).

Настоящее изобретение будет раскрыто в нижеследующем описании системы, для которого мы первоначально опишем ее элементы. Итак, мы рассматриваем множество пользователей, передающих информацию в виде законченных блоков (единиц) друг другу через систему хранения данных, представляющих собой распределенный реестр. Далее единицы этой информации будем также именовать транзакциями. Существует внешний наблюдатель (нарушитель) который получает информацию о системе, не являясь ее легальным пользователем. Ситуация, когда нарушитель контролирует одного или нескольких легальных пользователей, нуждается в отдельном рассмотрении. В некоторых случаях нарушитель может искажать единицы информации и блокировать их (уничтожать их в канале связи или телекоммуникационной среде). Важным является то, что транзакции характеризуются их отправителем и получателем (получателями), т.е. в составе транзакции имеются имена отправителя и получателя. Требование нулевого разглашения информации о системе определяют необходимость того, что для внешнего наблюдателя имена отправителя и получателя должны быть неизвестны, либо каждую транзакцию изменяться. Это факт легко доказуем от противного, поскольку иначе нарушитель может определить число пользователей в системе и связи между ними, то есть требование нулевого разглашения оказывается не выполненным.

Исходя из архитектуры и сформулированного принципа нулевого разглашения для внешнего наблюдателя, система распределенных реестров должна в обязательном порядке обеспечивать:

- формирование приватного элемента для пользователя с гарантированными вероятностными свойствами, т.е. пользователь должен иметь приватный идентификатор или ключ, никому не известный кроме него, выработанный при помощи датчика случайных чисел с гарантированными статистическими свойствами;

- формирование сетевого имени (идентификатора, которым пользователь представляется в системе) на основе указанного выше приватного элемента, исключающего возможность выявления связей (со стороны внешнего наблюдателя) между сетевым именем и множеством данных о физическом лице или организации (далее – информация о пользователе), с другой стороны сетевое имя должно быть проверяемым, т.е. уполномоченный орган должен при помощи детерминированной процедуры иметь возможность убедиться в соответствии сетевого имени и информации о пользователе;

- безопасное хранение приватного элемента у пользователя для обеспечения защищенности от несанкционированного доступа к нему;

- наличие «точки входа» для пользователей – оператора распределенного реестра, который на основе заданных государственным или ведомственным регулятором регламентов обеспечивает обработку информации пользователей

- авторизацию пользователя для оператора при помощи криптографических процедур, использующих приватный элемент пользователя (далее он назван сетевым ключом пользователя), известный также и оператору, но неизвестный другим пользователям;

- безопасный транспорт (как минимум с сохранение неизменности информации (транзакции), получаемой от пользователя) для передачи информации от пользователя к оператору распределенного реестра;

- контроль целостности и авторства каждой информационной единицы, помещаемой в распределенный реестр;

- формирование подтверждений у оператора распределенного реестра факте помещения информации в распределенный реестр (например, путем выдачи заверенных оператором квитанций пользователям);

- наличие механизма формирования и обработки запросов по выдаче информации из распределенного реестра по запросам его участников (клиентов), обеспечивающего защищенность данного запроса (также авторизацию и контроль неизменности запроса);

- реализацию у оператора распределенного реестра системы разграничения доступа к информации (к звеньям распределенного реестра) в распределенном реестре;

- наличие механизма обеспечения «нулевых знаний» о структуре системы, ее частниках и транзакциях за счет процедуры изменения имен отправителя и получателя, а также других данных транзакции, зависящей от сетевого ключа пользователя.

Сделаем важное замечание – оператор распределенного реестра является доверенным элементом и знает имена пользователей, поскольку он должен выполнять между ними разно рода действия, например, в общем случае передавать информацию, либо изменять состояния счетов пользователей, если транзакции носят финансовый характер.

Введем следующие обозначения

Xi – пользователь распределенного реестра,

Kpi – персональный ключ (персональная информация) пользователя РР,

Ksi – сетевой ключ пользователя (также являющийся частью персональной информации пользователя), предназначенный для связи с оператором РР,

Ci – ключевой контейнер пользователя, представляющий собой персональную информацию пользователя (персональный или сетевой ключ), закрытый на пароле пользователя при помощи обратимой криптографической процедуры,

Si – сетевое имя пользователя,

INFOij – информация i-го пользователя, сформированная на рабочем месте пользователя и направляемая для хранения и обработки в РР, имеющая условный номер j,

Kvij – квитанция, сообщающая о результате обработки j-го информационного блока для i-го пользователя

Vm – запрос на извлечение информации из РР,

Ko – ключ оператора, служащий для заверения цепочки данных в РР,

I=Im(x, k) – функция вычисления имитовставки от информации x на ключе k.

y=E(x,k) – функция зашифрования информации x на ключе k, и

x=D(y,k) – обратная операция – функция расшифрования информации y на ключе k.

В данном случае мы имеем дело с симметричными криптографическими алгоритмами, когда для зашифрования и расшифрования используется один и то же ключ.

Легко видеть, что функция вычисления имитовставки обладает возможностью как авторизации пользователя, так и контроля целостности передаваемой и хранимой информации. В связи с этим будем называть функцию вычисления и проверки имитовставки кодом аутентификации (КА).

Для обеспечения информационного взаимодействия пользователей и оператора необходимо обеспечить функционирование сервера оператора (сервер приема-выдачи информации распределенного реестра), имеющего следующие области для передачи данных:

- область приема данных сервера, в которую пользователи передают данные для помещения в распределенных реестр и запросы для выгрузки данных из распределенного реестра,

- область данных, в которую перемещаются объекты ошибочного формата (например, не имеющие кода аутентификации пользователя),

- область данных, содержащая квитанции о помещении информации в распределенный реестр,

- область данных выгрузки данных по запросам пользователей.

Полагаем, что пользователь системы имеет персональный вычислитель (ноутбук, смартфон или выделенный криптокомпьютер), подключенный при помощи каналов связи (телекоммуникационной среды) к серверу приема-выдачи информации РР.

Для регистрации в системе пользователь Xi при помощи датчика случайных чисел с гарантированными статистическим свойствами создает ключи Kpi – персональный ключ (персональная информация) пользователя РР и Ksi – сетевой ключ пользователя (также являющийся частью персональной информации пользователя), предназначенный для связи с оператором РР и формирует контейнеры Ci1=E(Kpi,Pi1) и Ci2=(Ksi,Pi2), где

Pi1, Pi2 – пароли пользователей для защиты соответствующих контейнеров.

Контейнер Ci2 может быть сформирован и оператором РР и передан пользователю при его регистрации, возможно выполненной в рамках национального законодательства, при этом пароль для раскрытия контейнера передается лично пользователю при физическом посещении представителя оператора и авторизации пользователя с предъявлением соответствующих документов. Пароль может быть передан и по альтернативным каналам связи, например, смс при регистрации пользователя с учетом номера его мобильного устройства.

Для подготовки данных для отправки их в РР пользователь может использовать конструктор атомов РР [6], позволяющий создать зашифрованный, подписанный (снабженный имитовставкой) или открытый блок данный. При этом зашифрованный или подписанный блок формируется на персональном ключе пользователя и доступен только самому пользователю, что позволяет обеспечить дополнительно невозможность ознакомления оператора РР с информацией пользователя, либо возможность контроля неизменности информации, отправленной оператору РР.

Далее пользователь формирует запрос Zij = Im([INFOij,Si,Tk],Ksi) и направляет его на сервер приема-выдачи данных. Сервер приема данных проверяет имитовставку пользователя по запросом, тем самым проводя как аутентификацию отправителя, так и проверку целостности данных.

При положительном результате проверки информация передается серверу записи в РР, который передает информацию для обработки в сервер оператора РР, хранящий ключ оператора Ko. Данный сервер записывает в систему хранения данных (СХД) блок Zij (цифровой конверт). При положительном результате записи в СХД для пользователя формируется квитанция Kvij, содержащая номер блока, куда помещена информация пользователя, номер транзакции, время помещения в РР и подпись оператора под данными пользователя.

Приведем пример такой квитанции

DNum:3

TNum:c09f9ae8a8921d91b41691c061cd6b61

Sign:ad3fed45df10834c

File:a01

NetName:b944928487491bde8f5bba9a64b33f4d

AddTime:01:37:11 13.01.2019

В данном случае квитанция удостоверяет для пользователя с сетевым именем NetName помещение файла a01 в звено распределенного реестра с номером 3 при этом имитовставка в СХД, выработанная оператором РР, принимает значение Sign, а номер транзакции составляет значение Tnum, время формирования записи (звена РР) AddTime.

Для извлечения данных или для изменения прав доступа к записи (по умолчанию доступ к записи предоставляется пользователю, который ее выполнил) пользователь использует специальные запросы.

Приведем пример таких запросов.

access

dnum:1

+:b944928487491bde8f5bba9a64b33f4d

запрос означает, что доступ к записи с номером 1 дополнительно предоставлен (+) пользователю с приведенным выше сетевым именем «Alisa».

или

load

dnum:1

запрос означает, что из РР будет выгружена запись с номером 1.

При запросе на извлечение данных или изменение прав доступа запрос Vm снабжается имитовставкой пользователя и передается в сервер оператора РР, который обращается к СХД в режиме чтения и по номеру записи, либо другой информации поиска (сетевом имени, дате) извлекает информацию и передает серверу приема-выдачи данных, либо формирует квитанцию о неуспешном поиске и невозможности извлечении данных.

В целях обеспечения основных свойств распределенного реестра [7], следующих из названия технологии blockchein – «цепь» или «цепочка» блоков, блокчейн в первую очередь должен обеспечивать свойства цепи – неразрывность и прочность, которые являются парафразом свойства целостности.

Неразрывность определяется как свойство следования блоков (звеньев цепи) одного за другим, в заданной в процессе создания блокчейна последовательности, а прочность – невозможность замены или удаления звена из цепочки.

Если рассматривать блокчейн как системную целостность, то он должен состоять из отдельных элементов – звеньев, каждое из которых в свою очередь делится на элементарные компоненты (назовем их атомами блокчейна). В данном случае для СХД формируется последовательность записей в нотации языка С:

l1=fwrite(dnum ,1, 16,fl);

l2=fwrite(ntran ,1, 16,fl);

l3=fwrite(tdt ,1, 8,fl);

l4=fwrite(buf ,1,buflen,fl);

l6=fwrite(imi ,1, 8,fl);

l5=fwrite(&buflen,4, 1,fl);

l7=fwrite(dnum1 ,1, 16,fl);

dmum – уже упомянутый нами выше номер записи (номер звена),

ntran – номер транзакции,

tdt – время и дата формирования звена,

buf – данные пользователя, записываемые в СХД длиной buflen,

dnum1=dnum+1, обеспечивающих неразрывность перехода к следующему звену,

imi=Im(dnum|ntran|tdt|buf, Ko) – имитовставка от конкатенации данных.

Кроме того, старшая область поля dnum заполняется значением imi от предыдущего звена, что позволяет добиться того же свойства, как и в блокчейне Bitcoin – зависимости хеш-значений (в данном случае вычисленных при помощи приватного элемента Ko) от всей последовательности предыдущих данных.

Приведем пример последовательного формирования описанных полей:

DNum:13

Полное значение: 6c006896973848d7000000000000000d

TNum:44f98f920985679580a8b7bee17de548

Sign:dabfd993c75f3366

File:a01

AddTime:01:10:48 20.01.2019

и

DNum:14

Полное значение: dabfd993c75f3366000000000000000e

TNum:ec2120a826f51e32255daa1f6002f5a2

Sign:baa49fb79db3805b

File:a01

AddTime:01:11:09 20.01.2019

Как легко видеть, поле imi предыдущего блока заполняет старшие разряды (8 байт) поля dnum текущего блока (предыдущий блок с номерами 13, текущий с номером 14), что позволяет обеспечить зависимость от всей предыдущей информации, помещенной в распределенный реестр.

Опишем также рактическую реализация описанных методик в виде платформы

Обмен данными между клиентом и сервером

Обмен данными между клиентскими и серверным приложениями осуществляется путём передачи сообщений, имеющими следующий набор блоков данных, располагающихся непосредственно друг за другом в теле передаваемого сообщения:

- заголовок сообщения (32 байта)
- время создания сообщения (8 байт)
- сетевое имя автора сообщения (16 байт)
- размер блока, содержащего текстовую команду (4 байта)
- размер блока, содержащего бинарные данные (4 байта)
- команда в текстовом формате, описывающая действие, которое получатель команды должен осуществить (добавить запись в реестр, извлечь запись из реестра, изменение прав доступа к записи и пр.). Формат и примеры описываются ниже
- произвольные данные (payload) (это, например, может быть непосредственно содержимое добавляемой в реестр записи)
- подпись для верификации сообщения

Формат текстовой команды

Текстовые команды в передаваемых сообщениях состоят из последовательности строк, первая из которых содержит идентификатор команды (ADD, GET, ACCESS и т.д.), а остальные - пары "ключ-значение", для передачи имён параметров их значений.

Примеры команд.

Команда для добавления записи в реестр:

ADD

file: file_name.txt

Команда на извлечение записи из реестра:

GET

dnum: 0000000000000001

core.h

Классы, реализующие работу с примитивами, использующимися при написании кода библиотеки:

- CUserMasterKey - мастер ключ пользователя (тот, который размером 32 байта)
- CUserKey - ключ шифрования для "кузнечика"
- CKeyContainer - ключевой контейнер
- CReceipt - квитанция, выдаваемая пользователю при записи данных в реестр
- CMessage - сообщение для передачи данных и команд между клиентом и сервером

command.h

Реализация функций для парсинга и формирования текстовых команд в сообщениях, передаваемых между клиентом и сервером.

Если возникает необходимость расширить/поменять формат команд, то это всё сконцентрировано в этом файле и таким образом подобные изменения не затронут остальную часть кода.

api.h

Описание и реализация API для создания приложений, использующих библиотеку.

Ниже даётся краткое описание интерфейсов и базовых классов API:

IDB

Данный интерфейс описывает минимально необходимый набор функций, которые должны быть реализованы в создаваемом серверном хранилище, для нормальной работы сервера реестра.

Через данный интерфейс сервер реестра осуществляет:

- получение сетевых ключей и паролей пользователей системы
- добавление и извлечение записей реестра

IServerClient

Описание интерфейса, через который сервер реестра осуществляет передачу сообщений клиенту в процессе обработки пришедшего от него сообщения.

Если в процессе обработки пришедшего сообщения серверу необходимо отправить клиенту какие-то данные (например, обрабатывается запрос на извлечение записи из реестра и необходимо отправить клиенту содержимое записи), то делается это именно через этот интерфейс.

CClient

Реализация базового класса для создания клиентских приложений для взаимодействия с реестром.

Алгоримт создания клиентских приложений на основе данного класса, описан ниже.

CServer

Реализация базового класса для создания сервера реестра.

Алгоритм создания серверных приложений на основе данного класса, описан ниже.

Создание прикладных приложений

Ниже будет описан процесс создания прикладных приложений (клиентской и серверной частей) на основе библиотеки.

Создание клиентского приложения

Для реализации клиентского приложения необходимо создать класс-наследник от CClient

Авторизация пользователя

Авторизация пользователя на локальной машине происходит через вызов функции login, которой передаются сетевой пароль, сетевое имя и ключевой контейнер пользователя. Т.е. классы, которые в прикладных приложениях будут наследоваться от CClient, должны каким-то образом получить эти данные от пользователя (ввод в окне, чтение из какого-то определённого файла на локальной машине, чтение из токена) и передать их в эту функцию.

Передача запросов на сервер

Для передачи запросов на добавление данных в реестр, реализованы функции:

- send_file - для отправки на сервер содержимого файла с локальной машины
- send_data - для отправки на сервер произвольных данных, хранящихся в памяти

Для отправки на сервер запроса на извлечение данных реализована функция get_data, принимающая в качестве параметра строковый идентификатор записи в реестре.

Обработка ответов сервера

Прикладное приложение должно самостоятельно реализовывать определение наличия входящих данных от сервера реестра и их получение (постоянное прослушивание сокета или периодический "пинг" сервера на предмет наличия новых сообщений, или как-то иным способом...).

После получения данных от сервера реестра, приложение должно вызывать функцию parse_message, осуществляющую парсинг и валидацию пришедших данных. В случае удачного парсинга, данной функцией вызывается виртуальная функция on_message, предназначенная для обработки поступившего сообщения.

Реализация функции on_message в классе-наследнике CClient и является реализацией реакции прикладной программы на сообщения, поступаемые от сервера реестра.

Таким образом создание клиентского приложения сводится к следующему набору задач:

1. получение сетевого имени, пароля, ключа (через пользовательский ввод, чтение из файла, получение через токен...), и последующий вызов login для авторизации
2. запрос у пользователя данных для отправки на сервер (окно ввода, выбор файла на локальной машине) и последующий вызов send_data/send_file
3. обеспечение непосредственной передачи данных на сервер реализовав функцию send (отправка данных через tcp, http, файлы в общей папке...)
4. обеспечение получения данных от сервера (например, прослушиванием сокета после отправки сообщения) и последующий вызов parse_message для парсинга и валидации пришедших данных
5. непосредственно описать реакцию на пришедшие от сервера данные (отображение пользователю в окне, запись в файл на диск...) реализовав функцию on_message, которая будет вызываться в случае удачного парсинга и валидации данных

Создание серверного приложения

Для создания серверного приложения необходимо создать класс-наследник от класса CServer. При создании необходимо проинициализировать указатель на интерфейс IDB для работы с серверным хранилищем данных (чтобы сервер имел доступ к сетевым ключам пользователей системы, а также, непосредственно, к бд с записями реестра).

Авторизация оператора

Для авторизации оператора реестра используется функция login, который передаются пароль и ключевой контейнер оператора. Таким образом, на создаваемое приложение возлагается функция получения этих данных у пользователя-оператора (непосредственный ввод, чтение из файла или токена).

Получение и обработка запросов

Реализуемое серверное приложение должно самостоятельно обеспечить определение наличия и получение данных запросов пользователей реестра (прослушивание и чтение из сокета или периодическая проверка общей папки на наличие файлов, ожидающих обработку или какой-то иной способ получения данных от клиентов).

После получения входящих данных вызывается функция process, которая осуществляет парсинг и валидацию пришедших данных. Для связи с клиентом (в случае появления необходимости отправить ему данные) в процессе обработки запроса, данной функции передаётся указатель на объект реализующий интерфейс IServerClient.

В классе CServer реализована реакция сервера на поступление запросов на добавление и извлечение данных. Если у создаваемого приложения есть необходимость расширить список поддерживаемых команд, в нём необходимо реализовать собственную реализацию виртуальной функции exec_cmd.

По сравнению со способами, известными авторам, заявляемый способ позволяет обеспечить наличие “точки входа” для пользователей (оператора), авторизацию пользователя для оператора, безопасный транспорт (с сохранением неизменности информации (транзакции), получаемой от пользователя) для передачи информации от пользователя к оператору распределенного реестра, контроль целостности и авторства каждой информационной единицы, помещаемой в распределенный реестр, а также создание неизменной последовательности помещения информационных единиц в распределенном реестре, обеспечить формирование подтверждений у оператора распределенного реестра о факте помещения информации в распределенный реестр, а также механизм формирования и обработки запросов по выдаче информации из распределенного реестра по запросам его участников (клиентов), обеспечивающего защищенность данного запроса (также авторизацию и контроль неизменности запроса) и реализацию у оператора распределенного реестра системы разграничения доступа к информации к звеньям распределенного реестра.

Данная заявка может являться методологической основой для формулирования ведомственных или национальных регулирующих требований в области цифровой экономики, а также послужить технической основой для разработки конкретных проектов

в области защищенных систем, использующих распределенные реестры в сфере государственного управления, финансов и учетно-сервисных систем.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ хранения цифровой информации в системе, состоящей, по меньшей мере из двух пользователей, характеризующихся неповторяющимися именами, оператора и распределенного реестра, представляющего собой массив данных, отличающийся тем, что массив данных состоит из звеньев, который формирует оператор на основе цифровой информации, получаемой от пользователей, и заключающийся в том, что:

- пользователь формируют цифровую информацию и снабжает ее кодом аутентификации, представляющем собой данные, полученные путем вычисления функции, зависящей от содержания цифровой информации, сформированной пользователем и личной информации, известной пользователю и оператору и неизвестной другим пользователя, в результате чего получают цифровой конверт пользователя, содержащий по меньшей мере информацию пользователя и код аутентификации;

- полученный цифровой конверт передают оператору, который проверяет его код аутентификации и, в случае его правильности, принимает цифровой конверт в обработку;

- оператор обрабатывает цифровой конверт, используя его целиком или выделяя го часть, включающую, по меньшей мере, цифровую информацию пользователя, получая в результате единицу хранения;

- оператор, используя единицу хранения и личную информацию оператора, неизвестную никому из пользователей, а также номер последнего звена в распределенном реестре и код аутентификации этого звена, формирует следующее звено распределенного реестра, путем добавления к единице хранения, по меньшей мере, нового порядкового номер звена, не совпадающего с номером предыдущего звена и кода аутентификации, вычисленного от единицы хранения, нового номера звена и кода аутентификации предыдущего звена;

- полученное следующее звено записывают в распределенный реестр.

2. Способ получения цифровой информации в системе распределенного реестра, состоящей, по меньшей мере из двух пользователей, характеризующихся неповторяющимися именами, оператора и распределенного реестра, отличающийся тем, что распределенный реестр состоит из звеньев, которые предварительно сформированы оператором на основе цифровой информации, получаемой от пользователей и заключающийся в том, что:

- пользователь формируют запрос на получение цифровой информации из распределенного реестра и снабжает его кодом аутентификации, представляющем собой данные, полученные путем вычисления функции, зависящей от содержания запроса и личной информации, известной пользователю и оператору и неизвестной другим пользователям, получая тем самым доверенный запрос пользователя, содержащий по меньшей мере запрос пользователя и код аутентификации;

- полученный доверенный запрос передают оператору, который проверяет его код аутентификации и, в случае его правильности, принимает доверенный запрос в обработку;

- оператор обрабатывает доверенный запрос, извлекая из распределенного реестра одну или несколько единиц хранения в соответствии с информацией, содержащейся в запросе и правилами хранения информации в распределенном реестре;

- извлеченные звенья передают пользователю, сформировавшему запрос.

3. Способ установления прав доступа к распределенному реестру на основе способа по п.2, когда запросом является перечень имен пользователей и сведения о звеньях, к которым эти пользователи будут иметь доступ.

4. Способ по п.1, п.2 или п.3, отличающийся тем, что в качестве кода аутентификации используется: имитовставка, хеш-функция, электронная подпись.

ЕВРАЗИИСКОЕ ПАТЕНТНОЕ ВЕДОМСТВО

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки: 201900350

Дата подачи: 05 июня 2019 (05.06.2019) | Дата испрашиваемого приоритета:

Название изобретения: СПОСОБ ХРАНЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННОМ РЕЕСТРЕ, ПОЛУЧЕНИЯ ИНФОРМАЦИИ ИЗ РАСПРЕДЕЛЕННОГО РЕЕСТРА И УСТАНОВЛЕНИЯ ПРАВ ДОСТУПА К ЗВЕНЬЯМ РАСПРЕДЕЛЕННОГО РЕЕСТРА

Заявитель: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ФИНТЕХ-ФОРЕНСИКА"

☐ **Некоторые пункты формулы не подлежат поиску (см. раздел I дополнительного листа)**

☐ **Единство изобретения не соблюдено (см. раздел II дополнительного листа)**

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

МПК: ***G06F 13/00*** *(2006.01)* СПК: ***G06F 13/605*** *(2013-01)*
G06F 21/60 *(2013.01)* ***G06F 21/60*** *(2015-01)*

Согласно Международной патентной классификации (МПК) или национальной классификации и МПК

Б. ОБЛАСТЬ ПОИСКА:

Минимум просмотренной документации (система классификации и индексы МПК)
H04N 19/00-19/91

Другая проверенная документация в той мере, в какой она включена в область поиска:

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
Y	US 2018/0278427 A1 (CABLE TELEVISION LABORATORIES, INC) 27.09.2018, реферат, [0006], [0025], [0042], пп. 1, 19 формулы	1-4
Y	US 2018/0068130 A1 (THE TORONTO-DOMINION BANK) 08.03.2018, [0048], [0049], [0052], [0060], [0066]-[0069] п. 1 фомулы, фиг. 1	1-4
Y	US 2017/0264428 A1 (MANIFOLD TECHNOLOGY, INC.) 14.09.2017, реферат, [0024]-[0027], [0040], [0042], [0048], [0050], п. 14 формулы, фиг. 1	1-4
A	US 2018/0260212 A1 (SALESFORCE.COM, INC.) 13.09.2018	1-4

☐ последующие документы указаны в продолжении графы В ☐ данные о патентах-аналогах указаны в приложении

* Особые категории ссылочных документов:
"A" документ, определяющий общий уровень техники
"E" более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее
"O" документ, относящийся к устному раскрытию, экспонированию и т.д.
"P" документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета
"D" документ, приведенный в евразийской заявке
"T" более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения
"X" документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности
"Y" документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории
"&" документ, являющийся патентом-аналогом
"L" документ, приведенный в других целях

Дата действительного завершения патентного поиска: 15 ноября 2019 (15.11.2019)

Наименование и адрес Международного поискового органа:
Федеральный институт промышленной собственности
РФ, 125993,Москва, Г-59, ГСП-3, Бережковская наб., д. 30-1.Факс: (499) 243-3337, телетайп: 114818 ПОДАЧА

Уполномоченное лицо :
Т.М. Иванова
Телефон № (499) 240-25-91