(19) Евразийское патентное ведомство

(11) 036643 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.12.03

(21) Номер заявки
201800623

(22) Дата подачи заявки
2018.12.19

(51) Int. Cl. ***G06Q 20/40*** (2006.01)
G06F 21/33 (2006.01)
H04L 9/14 (2006.01)

(54) СПОСОБ УПРАВЛЕНИЯ ЦИФРОВЫМИ АКТИВАМИ

(43) **2020.06.30**
(96) **2018000160 (RU) 2018.12.19**

(71)(73) Заявитель и патентовладелец:
АКЦИОНЕРНОЕ ОБЩЕСТВО "ИНФОВОТЧ" (RU)

(72) Изобретатель:
Касперская Наталья Ивановна, Щербаков Андрей Юрьевич, Домашев Алексей Владимирович (RU)

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

(56) WO-A1-2017139112
US-B1-8566247
WO-A1-9843152
US-A1-20180034642

(57) Изобретение относится к области информатики, а более конкретно - к способу управления цифровыми активами, и может найти применение при создании, эксплуатации, управлении и мониторинге систем различного назначения, включая сложные экономические и социальные системы, в которых интегрированы средства накопления и обмена различного рода информацией, информационными ресурсами и цифровыми активами. Основной задачей изобретения является создание такого способа управления цифровыми активами, который обеспечивал бы выполнение задач по проведению аутентификации участника, проведению сделок только между доверенными аутентифицированными участниками системы (замкнутость, изолированность системы управления и обмена ЦА), а также обеспечивал регистрацию операций с цифровыми активами, возможность легитимной отмены операций с цифровыми активами. Технический результат, на решение которого направлено данное изобретение, заключается в создании надежной системы управления цифровыми активами, которая бы позволила совершенствовать существующие системы управления цифровыми активами за счет того, что процесс производства, оборота ЦА становится прозрачен и контролируем, а система обмена ЦА была бы замкнута и преодолевала бы недостатки известных решений, в первую очередь Bitcoin и Etherium.

036643 B1

036643 B1

Изобретение относится к области информатики, а именно к системам обработки данных или способам, специально предназначенным для административных, коммерческих, финансовых, управленческих, надзорных или прогностических целей; а более конкретно - к способу управления цифровыми активами (под цифровыми активами будем понимать данные, находящиеся в электронных устройствах и предназначенные для выполнения целевых функций системы, в том числе, платежные системы/электронные деньги/криптовалюту).

Настоящее изобретение может найти применение при создании, эксплуатации, управлении и мониторинге систем различного назначения, включая сложные экономические и социальные системы (включая большие распределенные системы социального и экономического управления, системы больших данных и др.), в которых интегрированы средства накопления и обмена различного рода информацией, информационными ресурсами и цифровыми активами.

В основу настоящего изобретения положена задача создания такого способа управления цифровыми активами, который обеспечивал бы выполнение следующих задач:

проведение аутентификации участника, проведение сделок только между доверенными аутентифицированными участниками системы (замкнутость, изолированность системы управления и обмена ЦА),

регистрацию операций с цифровыми активами,

возможность легитимной (то есть доступной отправителю и согласованной с центром управления системой) отмены операций с цифровыми активами. Известна система для управления совершением сделок (патент №2158956, опубликовано 10.11.2000), включающая множество устройств управления участников системы, включающее в себя, по крайней мере, одно устройство управления банка, по крайней мере, одно устройство управления покупателя, по крайней мере, одно устройство управления продавца, отличающаяся тем, что упомянутые устройства управления участников системы соединены посредством канала связи с устройством централизованного управления и устройством хранения и проверки сертификатов, соединенном, по крайней мере, с одним упомянутым устройством централизованного управления, в состав которого входят: устройство регистрации участников системы, устройство формирования и хранения базы данных по операциям, совершаемым между участниками системы, устройство формирования и хранения базы данных по заключенным между участниками системы договорам, устройство управления данными, касающимися проведения финансовых операций, устройство контроля и анализа процесса совершения сделки между участниками системы, устройство управления процессом совершения сделки, устройство формирования и хранения базы данных по участникам системы, устройство формирования и хранения базы данных товаров и услуг, устройство управления документооборотом, при этом упомянутое устройство регистрации участников системы соединено с упомянутым устройством формирования и хранения базы данных по участникам системы и с входом и выходом упомянутого устройства централизованного управления, с которыми также соединено упомянутое устройство управления процессом совершения сделки, которое, в свою очередь, соединено с упомянутым устройством управления документооборотом, с упомянутым устройством управления данными, касающимися проведения финансовых операций, с упомянутым устройством формирования и хранения базы данных товаров и услуг, с упомянутым устройством контроля и анализа процесса совершения сделки между участниками системы, соединенным с выходом упомянутого устройства централизованного управления, с упомянутым устройством формирования и хранения базы данных по участникам системы и с упомянутым устройством формирования и хранения базы данных по операциям, совершаемым между участниками системы, которое, в свою очередь, соединено с упомянутым устройством формирования и хранения базы данных по заключенным между участниками системы договорам.

Существенными недостатками данной системы является ориентированность на участие банка, а также узкая область применения, ориентированная на совершение централизованной сделки, а также незамкнутость системы, что в современных экономических условиях в большинстве случаев нецелесообразно, поскольку банки достаточно редко обслуживают цифровые активы. Кроме того, в данной системе сертификаты решают только задачу защиты неизменности сделки, тогда как в современных условиях этого недостаточно, необходима аутентификация участников и проведение операций только между входящими в систему аутентифицированными участниками (замкнутость, изолированность).

Другим близким и более современным аналогом к данному изобретению является проект Биткойн (англ. Bitcoin, от bit – “бит” и coin – “монета”) - пиринговая платёжная система, использующая одноимённую расчётную единицу и одноимённый протокол передачи данных. Для обеспечения функционирования и защиты системы используются криптографические методы. Вся информация о транзакциях между адресами системы доступна в открытом виде.

Проводимые сделки необратимы, электронный платёж между двумя сторонами происходит без посредников. Но есть возможность привлечения третьей стороны-гаранта при помощи мультиподписи. Средства никто не может заморозить, даже временно, за исключением самого владельца.

Биткойны могут использоваться для обмена на товары или услуги у продавцов, которые согласны их принимать. Обмен на обычные валюты происходит через онлайн-сервис обмена цифровых валют, другие платёжные системы или обменные пункты.

Комиссия за проведение операций назначается отправителем добровольно, размер комиссии влияет

на приоритет при обработке транзакции. Обычно программа-клиент подсказывает рекомендуемый размер комиссии. Транзакции без комиссии возможны и также обрабатываются, однако не рекомендуются, поскольку время их обработки неизвестно и может быть довольно велико.

Одна из главных особенностей системы “Биткоин”, которая является и существенным недостатком - полная децентрализация и незамкнутость системы: нет центрального администратора или какого-либо его аналога. Это порождает возможность нерегулируемых операций с цифровыми активами. Необходимым и достаточным элементом этой платёжной системы является базовая программа-клиент, которая имеет открытый исходный код. Запущенные на множестве компьютеров программы-клиенты соединяются между собой в одноранговую сеть, каждый узел которой равноправен и самодостаточен. Невозможно государственное или частное управление системой, в том числе изменение суммарного количества биткойнов. Заранее известны объём и время выпуска новых биткойнов, но распределяются они относительно случайно среди тех, кто использует своё оборудование для вычислений, результаты которых являются механизмом регулирования и подтверждения правомочности операций в системе “Биткойн”.

Как видно из описания, данный прототип имеет следующие недостатки:

формирование (производство, майнинг) цифрового актива (ЦА) полностью бесконтрольны;

процесс производства ЦА и его оборота непрозрачен и неконтролируем;

система незамкнута от недобросовестных участников;

проводимые сделки необратимы, нет механизма отмены подтверждённой операции (включая случаи, когда платёж был отправлен на ошибочный или несуществующий адрес, или когда транзакция была подписана закрытым ключом, который стал известен другим лицам).

Задачи изобретения решены и недостатки прототипов устранены в реализованном согласно настоящему изобретению способе управления цифровыми активами в компьютерной системе, состоящей из по меньшей мере одного отправителя транзакций, по меньше мере одного получателя транзакций, у каждого их которых имеется хранилище цифровых активов, по меньше мере одного оператора хранилищ цифровых активов, отличающемся тем, что все участники системы обладают сертификатами электронной подписи, генерируют запросы на проведение транзакций, которые зашифрованы и подписаны электронной подписью, а для доступа к хранилищу и осуществления транзакции отправителя используют секретный ключ, а для доступа к хранилищу и осуществления транзакции получателя - открытый ключ и предусматривающий следующие шаги:

1) отправитель транзакции формирует запрос на проведение транзакции, содержащий в зашифрованном виде секретный ключ транзакции, который может расшифровать только оператор хранилища цифровых активов, подписывает этот запрос своей электронной подписью и отправляет его оператору хранилищ цифровых активов;

2) оператор хранилища цифровых активов при необходимости проверяет правильность электронной подписи запроса отправителя транзакции и при положительном результате проверки электронной подписи переходит к шагу 3;

3) оператор хранилища цифровых активов расшифровывает запрос отправителя транзакции и получает секретный ключ хранилища цифровых активов отправителя;

4) оператор хранилища цифровых активов расшифровывает (при необходимости) открытый ключ получателя транзакции;

5) оператор хранилища цифровых активов проверяет правильность электронной подписи под открытым ключом получателя транзакции и при положительном результате проверки электронной подписи переходит к шагу 6;

6) оператор хранилища цифровых активов формирует запрашиваемую транзакцию на секретном ключе хранилища цифровых активов отправителя и отправляет сформированную транзакцию получателю, при этом транзакция фиксируется в сети соответствующего ей цифрового актива;

7) оператор хранилища цифровых активов отправляет отправителю и/или получателю транзакции подписанное электронной подписью подтверждение проведения транзакции.

Технический результат, на решение которого направлено данное изобретение, заключается в создании надежной системы управления цифровыми активами, которая бы позволила совершенствовать существующие системы управления цифровыми активами за счет того, что процесс производства, оборота ЦА становится прозрачен и контролируем, а система обмена ЦА была бы замкнута и преодолевала бы недостатки известных решений, в первую очередь Bitcoin и Etherium.

Эти задачи достигаются тем, что при выдаче сертификата клиенту будет проводиться его обязательная аутентификация, операции с хранилищем цифровых активов регистрируются и управляются путем управления соответствующими сертификатами электронной подписи, кроме того, возможна легитимная отмена транзакций без участия банка и необходимости обращения к нему.

Настоящее изобретение будет раскрыто в нижеследующем описании компьютерной системы, предназначенной для управления цифровыми активами со ссылками на чертеж , состоящей из по меньшей мере одного отправителя транзакций, по меньше мере одного получателя транзакций, у каждого из которых имеется хранилище цифровых активов, по меньше мере одного оператора хранилища цифровых активов, при этом все участники системы обладают сертификатами электронной подписи, генерируют за-

просы на проведение транзакций, которые зашифрованы и подписаны электронной подписью, при этом целью является перемещение цифрового актива из хранилища цифровых активов отправителя в хранилище цифровых активов получателя, а для доступа к хранилищу и осуществления транзакции отправителя используют секретный ключ, а для доступа к хранилищу и осуществления транзакции получателя - открытый ключ и предусматривающий стадии, подробно описанные ниже.

Введем следующие краткие обозначения (под сертификатом подразумевается сертификат электронной подписи, получаемый подписанием электронной подписью удостоверяющего центра открытого (публичного) ключа участника (клиента) системы - отправителей и получателей транзакций):

iccn_head_ca_cert	Сертификат Головного Удостоверяющего центра (УЦ)
ccw_op_head_ca_cert	Сертификат Головного УЦ оператора хранилищ ЦА
ccw_op_hsm_private_key	Секретный ключ HSM оператора хранилищ ЦА
ccw_op_hsm_cert	Сертификат HSM оператора хранилищ ЦА
iccn_op_head_ca_cert	Сертификат Головного УЦ оператора хранилищ ЦА
iccn_op_end_user_ca_cert	Сертификат УЦ Управления Клиентами оператора хранилищ ЦА
iccn_op_ccw_ca_cert	Сертификат УЦ хранилищ ЦА
end_user_iccn_cert	Сертификат клиента
end_user_iccn_perms	Разрешения клиента
end_user_ccw_cert	Сертификат хранилища ЦА клиента
end_user_ccw_perms	Разрешения хранилища ЦА клиента
ccw_private_key	Секретный ключ хранилища ЦА клиента, хранящийся в HSM
ccw_public_key	Открытый ключ хранилища ЦА клиента
ccw_private_key_token	Запрос секретного ключа хранилища ЦА клиента
ccw_public_key_token	Запрос открытого ключа хранилища ЦА клиента

В представленной схеме аутентификация и авторизация конечных пользователей базируется на сертификатах и разрешениях, которые соответствующий УЦ включит в них. Данная модель является статической в том смысле, что не позволяет динамически управлять разрешениями конечных пользователей и поэтому на практике может быть не достаточной и тогда необходимо реализовать более гибкие модели управления.

В процессе описания схемы работы управления цифровым активом (УЦА) будут рассмотрены различные подходы к тому факту, известен ли конечному пользователю его реальный адрес в среде (сети) цифрового актива.

Первый заключается в том, что несмотря на то, что отправитель не может воспользоваться самостоятельно секретным ключом хранилища ЦА, реальный адрес хранилища ЦА конечному пользователю известен (это означает, что ему известен открытый ключ хранилища ЦА).

Второй подход заключается в том, что конечному пользователю не известен и открытый ключ хранилища ЦА, то есть он не знает и адреса хранилища ЦА, которым он управляет. Выбор того или иного подхода определяется исключительно характеристиками деятельности, которую хочет организовать Центр управления (ЦУП) ЦА. Однако очевидно, что знание пользователем его реального адреса оказывает прямое влияние на характеристики анонимности в среде УЦА.

Общая схема УЦА приведена на чертеже. Рассмотрим основные этапы инициализации и работы УЦА.

Этап 1. Инициализация ГУЦ УЦА.

Инициализация головного УЦ УЦА.

Головной УЦ может быть связан с органами государственного регулирования, либо другим органом, регулирующим деятельность операторов цифровых активов.

Этап 2. Инициализация Оператор хранилищ ЦА.

Инициализация оператора хранилища ЦА начинается с получения его головным УЦ сертификата (ccw_op_head_ca_cert) у ГУЦ ЦУП ЦА (шаг 2.1). Шаг 2.1 является регистрацией нового хранилища ЦА в системе.

Оператор хранилищ ЦА, состоит из двух основных элементов: головного УЦ и HSM. Для заверше-

ния инициализации хранилища ЦА HSM генерирует секретный ключ (ccw_op_hsm_private_key) и получает сертификат (ccw_.op_hsm_cert) открытого ключа у своего ГУЦ (шаг 2.2). Также сертификат открытого ключа помещается в каталог хранилищ ЦА (шаг 2.3).

Этап 3. Инициализация ЦУП ЦА.

Инициализация ЦУП ЦА, как и оператора хранилища ЦА, начинается с получения его головным УЦ сертификата (dapc_op_head_ca_cert) у ГУЦ ЦУП ЦА (шаг 3.1). Шаг 3.1 является регистрацией нового ЦУП ЦА в системе.

Оператор хранилища ЦА состоит из четырех основных элементов: головного УЦ, УЦ УК, УЦ хранилища ЦА и БД АВ хранилища ЦА. Для завершения инициализации УЦ УК и УЦ хранилища ЦА запрашивают сертификаты открытых ключей (dapc_op_end_user_ca_cert и dapc_op_ccw_ca_cert), необходимых для их активации (шаг 3.2 и шаг 3.3 соответственно).

После активации всех УЦ инициализируется БД операторов восстановления. Для этого оператор (операторы) восстановления генерирует(ют) секретные ключи и запрашивают сертификаты открытых ключей у своего головного УЦ (шаг 3.4).

Этап 4. Регистрация отправителя транзакции в ЦУП ЦА.

Этап регистрации, как и в остальных случаях, представляет собой запрос и получение сертификата (end_user_dapc_cert) у ЦУП ЦА. Обработку этих запросов в рамках ЦУП ЦА ведет УЦ УК. Таким образом, клиент получает сертификат открытого ключа с включенными в него разрешениями (end_user_dapc_perms), который в дальнейшем он будет использовать для аутентификации при обращении к сервисам УЦА.

Какие данные клиент должен предъявить для получения сертификата, а также какие данные будут внесены в его сертификат, зависит от политики соответствующего ЦУП ЦА. Кроме этого, важным моментом, который должен определить ЦУП ЦА, это параметры доступа к каталогу сертификатов. Будет ли он публичным, доступным только аутентифицированным клиентам или закрыт - также определяется текущей политикой.

Этап 5. Получение сертификата хранилища ЦА.

К настоящему моменту клиент, зарегистрировавшись в ЦУП ЦА и получив соответствующий сертификат, имеет возможность обращаться к сервисам УЦА.

Поскольку в рамках УЦА клиент работает с хранилищем ЦА посредством хранилища ЦА и не владеет секретным ключом хранилища ЦА, то для идентификации хранилища ЦА предлагается использовать специальный сертификат, к которому оператор хранилища ЦА и будет привязывать реальные хранилища ЦА и на котором будет производиться шифрование и ЭП информации, связанной с этим хранилищем ЦА. Кроме того, использование для каждого хранилища ЦА отдельного сертификата позволит ЦУП ЦА проводить в случае необходимости целевую блокировку хранилища ЦА просто путем отзыва соответствующего сертификата.

Таким образом, на этом этапе клиент обращается к УЦ хранилища ЦА, проходит аутентификацию и запрашивает сертификат хранилища ЦА (end_user_ccw_cert). Аутентификация может быть проведена по протоколу TLS с использованием штатной возможности клиентской аутентификации. При обращении за сертификатом хранилища ЦА клиент может указать разрешения (end_user_ccw_perms), которые он хотел бы получить. Например, тип цифрового актива, максимальный объем хранилища, возможность обращение к внешним шлюзам УЦА и др. Конкретный перечень разрешений сертификата и требования к его получению определяются политикой ЦУП ЦА.

После успешного получения сертификата хранилища ЦА клиент может обращаться с запросами к оператору хранилища ЦА.

Этап 6. Подключение реального хранилища ЦА к сертификату клиента.

На этом этапе клиент обращается к соответствующему оператору хранилища ЦА для создания для него хранилища ЦА. Запрос подписывается на сертификате, полученном от ЦУП ЦА на этапе 6. Таким образом, оператор хранилища ЦА имеет возможность проверить полномочия клиента для создания хранилища ЦА.

После проверки валидности запроса HSM оператора создает (или использует уже созданную) ключевую пару хранилища ЦА (ccw_private_key и ccw_public_key). Из открытого ключа формируется запрос открытого ключа (ccw_public_key_token), а из секретного ключа запрос секретного ключа (ccw_private_key_token).

Запрос ccw_private_key_token получается путем шифрования и подписи ccw_private_key на сертификате оператора хранилища ЦА ccw_op_hsm_cert, полученном на этапе 2 (шаг 2.2). В состав запроса также входит идентификатор сертификата конечного пользователя end_user_ccw_cert_id. Включение идентификатора необходимо, чтобы оператор хранилища ЦА мог при обращении проверить соответствие идентификатора сертификата конечного пользователя, который к нему обратился и идентификатора сертификата из запроса.

Запрос ccw_public_key_token также может быть получен путем шифрования и подписи на сертификате оператора хранилища ЦА ccw_op_hsm_cert, если есть необходимость в скрытии от клиента реального адреса хранилища ЦА. В противном случае достаточно только подписи. В состав

ccw__public_key_token также входит идентификатор сертификата end_user_ccw_cert_id.

После этого оба запроса (ccw_private_key_.token и ccw_public_key_token) направляются клиенту в ответ на его запрос.

Таким образом после этого шага клиент владеет всей необходимой информацией для осуществления транзакций в УЦА.

Этап 7. Проведение транзакции для хранилища ЦА.

Теперь для проведения транзакции клиенту необходимо сформировать параметры транзакции и подписать запрос сертификатом end_user_ccw_cert, полученным на этапе 5.

Для формирования транзакции конечный пользователь должен по соответствующим каналам получить целевые адреса в виде запросов ccw_public_key_token. Получить он их может как в результате непосредственно взаимодействия с другими пользователями (например, по электронной почте) или ЦУП ЦА может предусмотреть какой-либо общедоступный каталог для размещения такой информации (например, непосредственно в свойствах сертификатов в каталоге УЦ хранилища ЦА) (шаг 7.1).

Получив запрос, оператор хранилища ЦА проводит следующие действия (шаг 7.2):

1. Проверяет валидность подписи запроса.

2. Расшифровывает (если необходимо) ccwpublickeytoken отправителя транзакции.

3. Проверяет подпись ccw_public_key_token отправителя транзакции.

4. Расшифровывает ccw_private_key_token отправителя транзакции и получает секретный ключ хранилища ЦА ccw_private_key.

5. Проверяет подпись ccw_private_key_token отправителя транзакции.

6. Расшифровывает (если необходимо) ccw_public_key_token получателей транзакции.

7. Проверяет подпись ccw_public_key_token получателей транзакции.

8. Проверяет валидность сертификатов end_user_ccw_cert получателей транзакции.

9. Проверяет валидность сертификатов end_user_dapc_cert получателей транзакции.

10. Формирует и подписывает запрашиваемую транзакцию на ключе ccw_private_key отправителя транзакции.

11. Отправляет транзакцию в сеть соответствующего цифрового актива.

12. Отправляет конечному пользователю подписанное подтверждение проведения транзакции.

Таким образом представленная схема гарантирует, что конечные пользователи УЦА имеют возможность передавать транзакции только другим зарегистрированным пользователям УЦА.

После приведения описания работы УЦА более понятным становится предложенное техническое решение по делению “полнофункционального” ЦУП ЦА на два независимых компонента: собственно ЦУП ЦА и оператора хранилища ЦА. В области оператора хранилища ЦА собраны компоненты, работающие непосредственно с транзакциями конечных пользователей и средами (сетями) цифровых активов. Организация, заинтересованная в создании для каких-либо целей ЦУП ЦА может и не иметь таких специфических компетенций. Задача "малого" ЦУП ЦА это управление подключением конечных пользователей к УЦА. Кроме того, введение дополнительного независимого оператора безусловно повышает и уровень доверия конечных пользователей к системе в целом.

Сделаем еще одно замечание в отношении оператора хранилища ЦА. Как можно заметить из приведенного описания, оператор хранилища ЦА не хранит результатов своих операций. Результаты всех проведенных им операций отправляются или конечным пользователям или в сеть цифрового актива. Это очень выгодное свойство с точки зрения простоты реализации HSM и оператора в целом. Однако конечные возможности такой реализации могут не удовлетворить запросы организатора ЦУП ЦА.

В следующих разделах рассматриваются дополнительные компоненты УЦА, которые позволяют динамически управлять разрешениями конечных пользователей.

Дополнительные компоненты УЦА.

При описании базовых принципов функционирования УЦА, изложенных в предыдущем разделе, были для упрощения опущены несколько важных компонентов. Этими компонентами являются каталог хранилища ЦА, а также операторы аудита и управления, описанные на схеме шагами 8 и 9.

Как уже отмечалось, “статическая” модель управления разрешениями в которой разрешения конечных пользователей хранятся в сертификате и соответственно могут быть изменены только перевыпуском соответствующего сертификата, что не всегда может удовлетворять запросам ЦУП ЦА. Таким образом для хранения каталога конечных пользователей, связанных с ними хранилищ ЦА и соответствующих разрешений вводится компонент каталог хранилища. Со стороны ЦУП ЦА текущими разрешениями, хранящимися в каталоге, управляет оператор управления хранилища ЦА.

В связи с введением новых компонент этап 6 может быть дополнен шагом 9, на котором будут проверены текущие разрешения конечного пользователя на проведение запрошенной транзакции.

Помимо управления разрешениями, ЦУП ЦА безусловно может быть заинтересован в текущем аудите транзакций конечных пользователей. Для этого оператор аудита хранилища ЦА может также обратиться в каталог хранилища ЦА и, получив соответствующую информацию, проводить аудит целевой сети цифрового актива.

ЦУП ЦА может быть заинтересован в том, чтобы при необходимости проводить операции с храни-

лища ЦА конечных пользователей. Это может быть прежде всего связано с необходимостью обеспечения возможности возвращение средств транзакции, признанной по каким-либо причинам недействительной. Для этого оператор администрирования хранилища ЦА должен иметь доступ к секретным ключам хранилища ЦА. Наиболее очевидная схема реализации данного требования это дополнение этапа 6 шагом создания запроса секретного ключа, зашифрованного на сертификате оператора администрирования хранилища ЦА, полученном на шаге 3. Этот запрос может быть, в зависимости от требований оператора, сохранен в каталог хранилища ЦА или напрямую передан ЦУП ЦА для хранения и использования.

Таким образом, дополненная компонентами каталога хранилища ЦА и операторами аудита и администрирования, УЦА приобретает возможности динамического управления разрешениями при работе с хранилища ЦА, аудита пользовательских транзакций и возможностью возвращать полностью или частично уже проведенные транзакции.

По сравнению с известными способами заявляемый способ позволяет в полной мере учесть интересы государства и регулирующих органов в инфраструктуре обслуживания цифровых активов. При выдаче сертификата клиенту будет проводиться его обязательная аутентификация, операции с хранилищем цифровых активов регистрируются и управляются путем управления соответствующими сертификатами, кроме того, возможна легитимная отмена транзакций.

ФОРМУЛА ИЗОБРЕТЕНИЯ

Способ управления цифровыми активами в компьютерной системе, состоящей из по меньшей мере одного отправителя транзакций, по меньше мере одного получателя транзакций, у каждого их которых имеется хранилище цифровых активов, по меньше мере одного оператора хранилища цифровых активов, отличающийся тем, что все участники системы обладают сертификатами электронной подписи, генерируют запросы на проведение транзакций, которые зашифрованы и подписаны электронной подписью, а для доступа к хранилищу и осуществления транзакции отправителя используют секретный ключ, а для доступа к хранилищу и осуществления транзакции получателя - открытый ключ и предусматривающий следующие шаги:

1) отправитель транзакции формирует запрос на проведение транзакции, содержащий в зашифрованном виде секретный ключ транзакции, который может расшифровать только оператор хранилища цифровых активов, подписывает этот запрос своей электронной подписью и отправляет его оператору хранилища цифровых активов;

2) оператор хранилища цифровых активов при необходимости проверяет правильность электронной подписи запроса отправителя транзакции и при положительном результате проверки электронной подписи переходит к шагу 3;

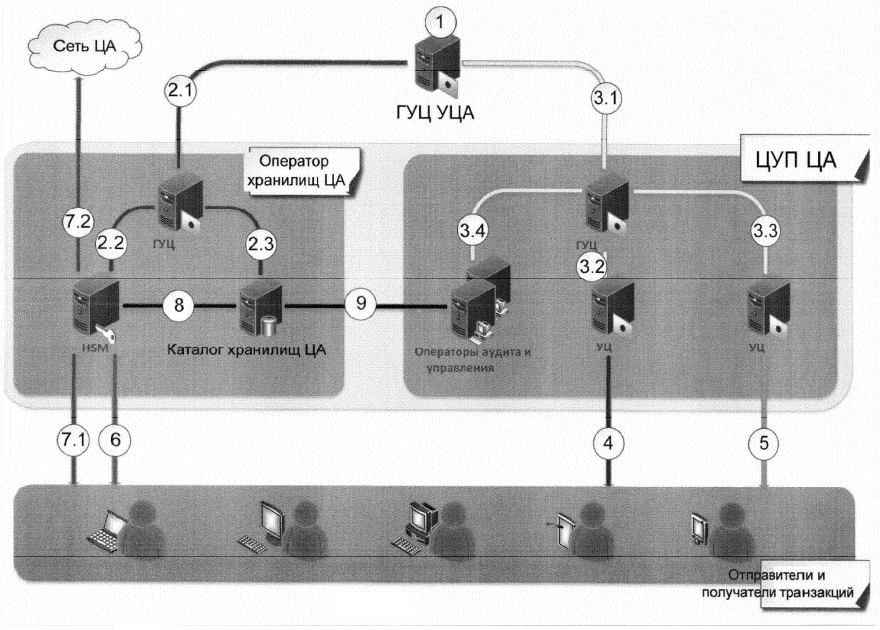
3) оператор хранилища цифровых активов расшифровывает запрос отправителя транзакции и получает секретный ключ хранилища цифровых активов отправителя;

4) оператор хранилища цифровых активов расшифровывает (при необходимости) открытый ключ получателя транзакции;

5) оператор хранилища цифровых активов проверяет правильность электронной подписи под открытым ключом получателя транзакции и при положительном результате проверки электронной подписи переходит к шагу 6;

6) оператор хранилища цифровых активов формирует запрашиваемую транзакцию на секретном ключе хранилища цифровых активов отправителя и отправляет сформированную транзакцию получателю, при этом транзакция фиксируется в сети соответствующего ей цифрового актива;

7) оператор хранилища цифровых активов отправляет отправителю и/или получателю транзакции подписанное электронной подписью подтверждение проведения транзакции.


Сеть ЦА
1
ГУЦ УЦА
2.1
3.1
Оператор хранилищ ЦА
ЦУП ЦА
7.2
2.2
ГУЦ
2.3
3.4
ГУЦ
3.3
3.2
8
9
HSM
Каталог хранилищ ЦА
Операторы аудита и управления
УЦ
УЦ
7.1
6
4
5
Отправители и получатели транзакций