

Способ и система заверки документов.

Изобретение относится к области информационных систем и системам электронного документооборота.

Известен патент РФ №2158956, от 10.11.2000 в котором раскрыта система для управления совершением сделок. Данная система включает множество устройств управления участников системы, соединенные посредством канала связи с устройством управления и устройством хранения и проверки сертификатов, соединенном с 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, устройство управления данными.

Недостатками данной системы является невозможность удостоверения оператором системы времени совершения юридически значимого действия, ограниченные функциональные возможности, обусловленные конструктивными особенностями системы, а также значительное количество устройств, которые должен приобрести пользователь. Система не предусматривает использование при заключении сделок электронных поверенных (договор поручения) или агентов (агентский договор), что существенно ограничивает сферу ее применения. Система ориентирована только на сферу купли-продажи товаров и услуг и не затрагивает другие сферы коммерческой и некоммерческой деятельности (например, подача юридически

значимых заявлений в государственные органы, коммерческие и некоммерческие организации; представление деклараций и отчетов в контролирующие органы; получение юридически значимых ответов; формирование и выдача юридически значимых поручений; деловая юридически значимая переписка и т.д.). При этом система не предполагает связи с другими аналогичными или близкими по функционалу системами.

Наиболее близким аналогом предлагаемого технического решения является патент РФ №117198, от 20.06.2012 в котором раскрыта система доверенного юридически значимого электронного документооборота. Данная система включает множество устройств управления участников системы, соединенных посредством канала связи с устройством управления и устройством хранения и проверки сертификатов, соединенным с 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, устройство управления данными. При этом система дополнительно снабжена устройством управления электронного поверенного (ЭП), сопряженным с устройством управления контентом, с базой данных сертификатов, базой данных документов и универсальным рабочим местом участника системы, включающим устройство управления, связанное с устройством ввода информации, устройством отображения информации, модулем печати, устройством кодирования/декодирования, модулем связи, при этом устройство управления ЭП снабжено хранилищами в виде баз данных

идентификаторов и шаблонов, определяемых требованиями организаторов сети передачи информации и получателей юридически значимой информации и через устройство кодирования/декодирования, модуль связи, посредством каналов связи сопряжено с устройством управления, системой управления совершением сделок, включающей устройство хранения и проверки сертификатов и устройство централизованного управления, финансовой системой, системой налоговых органов, системой органов государственной власти, ведомственной системой и с электронными торговыми площадками, при этом устройство управления дополнительно снабжено устройством считывания/записи, включающим носитель данных и носитель идентификаторов, и дополнительными хранилищами в виде баз данных идентификаторов, сертификатов, шаблонов и документов, определяющих требования к функционалу системы и получателей юридически значимой информации, причем база данных документов, соединенная с устройством управления, дополнительно связана с устройством кодирования/декодирования.

Недостатками данной системы является невозможность удостоверения оператором системы времени совершения юридически значимого действия, применение значительного числа устройств, что требует от пользователей покупки устройства/сертификата, что повышает порог входа на площадку для участников рынка и требует от участников рынка специальных знаний в области управления ключами и сертификатами, необходимость оформления электронной подписи участниками, что снижает мобильность участников при заключении сделок и требует наличия предустановленного

программного обеспечения на устройстве пользователя. При этом система не предполагает связи с другими аналогичными или близкими по функционалу системами.

Кроме того решение не может использоваться на мобильных устройствах и не использует иные возможные электронные каналы, которые как правило использует пользователь, так как требует подключения персонального компьютера, что существенно снижает мобильность решения.

Пользователь не может совершить действие в тот момент, когда это необходимо (допустим, подписать договор или удостоверить электронное доказательство в тот момент, когда он его обнаружил). При этом есть риск утраты времени реагирования. Когда пользователь будет готов, договор будет подписан с другим пользователем или информация будет стерта и факт нарушения зафиксировать не получится.

Техническая проблема, решаемая посредством использования разработанного способа, состоит в расширении возможностей электронного документооборота путем отказа от необходимости получения ЭП, отказа от необходимости использования устройств с предустановленным программным обеспечением и расширения возможностей пользователя, путем предоставления ему возможности задействовать любое устройство и любой доступный электронный канал связи, который позволяет обеспечить идентификацию. Любой пользователь, с любого устройства, имеющего выход в интернет (в том числе локальную сеть, с подключенным модулем защищенного обращения к серверу) может без предварительной подготовки, имея только электронную почту и/или номер мобильного телефона

зарегистрировать свой профиль и совершать юридически значимые действия, осуществляя реагирование за минуты.

Технический результат – упрощение заверения документов и повышение защиты хранимых заверенных документов.

Технический результат достигается тем, что первый вариант способа заверки документов, включает:

- создание и/или сохранение на электронном устройстве пользователя, по меньшей мере, одного заверяемого документа или ссылки на заверяемый документ,
- передача с электронного устройства пользователя через сеть передачи данных, по меньшей мере, одного заверяемого документа или ссылки на заверяемый документ на сервер приема заверяемых документов,
- сохранение системой, по меньшей мере, одного заверяемого документа в запоминающем устройстве сервера приема заверяемых документов,
- обработку каждого заверяемого документа блоком обработки данных, путем проставления в нем метки текущего времени, даты, месяца и года и заверения их электронной цифровой подписью лица уполномоченного на данное действие с получением, по меньшей мере, одного заверенного документа,
- сохранение, по меньшей мере, одного заверенного документа на сервере репозитория,
- направление, по меньшей мере, одного заверенного документа с сервера репозитория на электронное устройство пользователя,
- при необходимости формирование, по меньшей мере, одного заверенного документа в человеко-читаемую форму, которая

соответствует требованиям, предъявляемым к электронным доказательствам.

При этом передача заверяемого документа с электронного устройства пользователя на сервер приема заверяемых документов осуществляется посредством зашифрованного канала связи.

Также с сервера репозитория дополнительно направляют на электронное устройство пользователя, по меньшей мере, один заверенный документ.

Второй вариант способа заверки документов, включает:

- создание в системе создания данных и/или передачу в системе передачи данных и/или сохранение пользователем через сеть передачи данных в сторонней системе хранения данных, по меньшей мере, одного заверяемого документа в виде файла и/или архивной папки, (пользователь системы при регистрации подключает хранилище, в котором создает данные, например репозиторий типа git, и дальнейшую работу осуществляет уже в репозитории. Подключенная к репозиторию система по сценарию осуществляет формирование образа (эталона) и сохранения образа файла и времени создания данных во внешней системе с формированием электронного доказательства, подтверждающего факт создания произведения и содержащего необходимые элементы для обеспечения статуса доказательства.

Возможным сценарием является также подключение систем передачи данных и облачных платформ публикации контента типа deposit photo, перед публикацией система формирует эталонный образ и сохраняет образ и времени создания данных во внешней системе с формированием электронного доказательства, подтверждающего факт

создания произведения и содержащего необходимые элементы для обеспечения статуса доказательства.

- подключение пользователя через сеть передачи данных, к серверу приема заверяемых документов и указания на нем, сторонней системы генерации данных и/или передачи данных и/или хранения данных, где хранятся заверяемые документы, а также сценария заверки документа сторонних системах, (пользователь загружает файл в системное файловое хранилище для сохранения образа файла и времени создания данных во внешней системе с формированием электронного доказательства, подтверждающего факт создания произведения и содержащего необходимые элементы для обеспечения статуса доказательства)

- в соответствии с заданным сценарием или сценарием пользователя, сервером приема заверяемых документов осуществляется копирование и/или выгрузка и/или расчет хэш-суммы файла или архивной папки и/или иного средства идентификации образа файла, по меньшей мере, одного заверяемого документа из сторонней системы генерации данных и/или передачи данных и/или хранения данных, (пользователь системы при регистрации подключает хранилище, в котором создает данные, например репозиторий типа git, и дальнейшую работу осуществляет уже в репозитории. При этом обработка файла и расчет хэш-суммы, а также определение идентификационных параметров происходит во внешней системе, которая передает по API данные на блок обработки данных. Таким образом файлы и образы файлов не покидают стороннюю систему, во избежание утечки данных, вместе с тем сформированный охранный документ содержит ссылку к внешней системе, которая позволяет провести идентификацию и сличения файла).

- сохранение, по меньшей мере, одного заверяемого документа и/или электронного доказательства факта заверения документа в запоминающем устройстве сервера приема заверяемых документов,

- обработку каждого заверяемого документа блоком обработки данных, путем расчета хэш суммы файла и/или иного средства идентификации образа файла проставления в нем метки текущего времени, даты, месяца и года и заверения их электронной цифровой подписью лица уполномоченного на данное действие с получением, по меньшей мере, одного заверенного документа,

- сохранение, по меньшей мере, одного заверенного документа на сервере репозитория,

- копирование, по меньшей мере, одного заверенного документа с сервера репозитория на сервер и/или в стороннюю систему хранения данных,

- расчет расчета хэш суммы файла и/или иного средства идентификации образа файла без копирования заверенного документа с сервера репозитория систему хранения данных,

- при необходимости формирование, по меньшей мере, одного заверенного документа и/или электронного доказательства факта заверения документа на локальном и английском языке в человеко-читаемую форму, которая соответствует требованиям, предъявляемым к электронным доказательствам.

Сторонней системой генерации данных является любая известная система генерации данных, в том числе машинных данных типа искусственный интеллект и/или нейронная сеть, сторонней системой передачи данных является любая известная система передачи данных, которая передает заверяемые документы и/или образы заверяемых документов, сторонней системой хранения данных

является любое известное «облачное» хранилище или репозиторий или сетевое хранилище какой-либо организации.

Сценарий заверки документа включает расчет хэш суммы файла или архивной папки и/или иного средства идентификации образа файла, идентификационные данные владельца файла/архивной папки, временные характеристики даты создания файла/архивной папки, генерацию электронного доказательства факта заверения документа или определения факта идентичности образа файла с уже созданным заверенным документом

В соответствии со сценарием заверки документа, первоначальный документ после прохождения обработки и расчета хэш суммы файла или архивной папки и/или иного средства идентификации образа файла удаляется с операционного сервера обработки данных, а на операционном сервере сохраняется только электронного доказательства факта заверения документа со ссылкой на место хранения исходного документа.

Указанные выше способы реализуются системой заверки документов, включающей:

- по меньшей мере, одно электронное устройство пользователя, выполненное с возможностью передачи заверяемого документа на сервер приема заверяемых документов,
- сервер приема заверяемых документов,
- устройство хранения заверяемых документов,
- блок обработки данных, выполненный с возможностью осуществления обработки каждого заверяемого документа, путем проставления в нем метки текущего времени, даты, месяца и года и заверения его электронной цифровой подписью лица

уполномоченного на данное действие с получением, по меньшей мере, одного заверенного документа,

- сервер репозитория, выполненный с возможностью безвременного хранения, по меньшей мере, одного заверенного документа и передачи на электронное устройство пользователя, по меньшей мере, одного заверенного документа.

В предлагаемой системе заверки документов электронное устройство пользователя, имеет возможность передачи заверяемого документа по проводной или беспроводной сети передачи данных.

Кроме того устройство хранения заверяемых документов и/или блок хранения сервера репозитория могут представлять собой облачные хранилища.

Кроме того сервер репозитория дополнительно связан с модулем печати для формирования, по меньшей мере, одного заверенного документа в человеко-читаемую форму, которая соответствует требованиям, предъявляемым к электронным доказательствам.

Схема работы по первому варианту способа показана на Fig.

Использование разработанного способа позволяет осуществить формирование и хранение различных видов заверенных документов или информации, необходимой для предоставления в судебные или правоохранительные органы, в том числе и по их официальному запросу этих документов. Также способ позволяет фиксировать и подтверждать факты свершения разных сделок, либо обмена информацией между интересующими их сторонами с указанием даты публикации и электронного канала связи, который использовался для идентификации пользователя.

Также использование разработанного способа позволяет обеспечить возможность участия в электронном обмене цифровой информации, переданной через клиентов предлагаемой системы, не имеющих собственных автоматизированных систем обработки информации, заверенные по разработанному способу документы и материалы могут быть направлены и подлежат принятию как доказательства любыми организациями, государственными органами, органами местного самоуправления, правоохранительными и судебными органами.

При этом, пользователь может осуществлять доступ к предлагаемой системе с любого устройства, путем прохождения двухфакторной идентификации – пара логин/пароль и получения динамической ссылки на любой выбранный канал связи пользователя (мобильный телефон, мессенджер, электронная почта), а также подтверждения действия пользователя путем осуществления тестового списания с банковской карты или иного платежного средства пользователя.

Выставление счета и списание денег пользователя может осуществляться:

- на базовом тарифе сразу после оказания услуги заверки,
- на продвинутом тарифе пользователь покупает лицензию и получает доступ к сервису без постоянного списания денежных средств с карты или выставления счетов. В системе реализован функционал счетов и пользователь видит за что он заплатил и какие платежи получил.

Таким образом, пользователь может использовать систему, даже если у него отсутствует доступ к возможностям мобильного оператора (пользователь находится в роуминге и не желает использовать

мобильную связь), пользователь не может принять и прочитать электронную почту (в связи с утратой доступа или отсутствием электронной почты) и отсутствием банковской карты (но наличием иного платежного средства, допустим мессенджера).

Ключевое отличие технического решения от всех представленных ранее технических решений является возможность осуществления операций по заверению документов и удостоверения оператором системы времени совершения данного действия, производимого пользователем на любом устройстве без требований к определенному конечному устройству или требования о предустановленном программном обеспечении или ключе (сертификате) и обеспечение полной мобильности пользователя, а также снятии всех барьеров, как временных, так и технологических при совершении юридически значимого действия или удостоверения доказательства.

Ключевое отличие предложенного способа состоит также в расширении возможностей пользователя, путем предоставления ему возможности задействовать любое устройство и любой доступный электронный канал связи, который позволяет обеспечить идентификацию. Любой пользователь, с любого устройства, имеющего выход в интернет (в том числе локальную сеть) может без предварительной подготовки, имея только номер мобильного телефона зарегистрировать свой профиль и совершать юридически значимые действия, осуществляя реагирование за минуты.

Указанный способ позволяет оформлять любое количество действий с минимальными нагрузками на систему, что обеспечивает высокий уровень быстродействия, который зависит исключительно от скорости пользователя и может составлять до 10 операций в минуту.

Разработанный способ применим в двух вариантах:

- по первому варианту для осуществления действий по фиксации и заверению факта совершения юридически значимого действия пользователем, например, договора. При необходимости можно получить ссылку на сохраненную копию или заказать подтверждающий сертификат;
- по второму варианту для осуществления действий по фиксации и удостоверению информации, содержащейся на сайтах (интернет-страницах) в сети Интернет путем копирования url ссылки в соответствующее окно разработанной системы, при котором система автоматически совершит следующие действия – выполнит скриншот страницы целиком и сохранит его в электронной форме, выполнить скриншот всех страниц и элементов, которые будут доступны по ссылке, проставит системные метки времени для обеспечения удостоверения доказательств.

Второй вариант предпочтительно применим для:

- фиксации условий договоров-оферт, условий оказания услуг и их стоимости, а также продажи товаров через Интернет;
- фиксации фактов оказания услуг и их качества, когда содержанием этих услуг являются создание, поддержание и наполнение Интернет-ресурсов;
- фиксации условий тендеров и торгов на поставку продукции и оказание услуг, условий госзакупок и иной информации;
- фиксации неправомерного или незаконного размещения материалов на Интернет-страницах;
- незаконное использование товарных знаков, знаков обслуживания, фото- и видеоматериалов,
- нарушения авторских, смежных и патентных прав,

- клевета, публикация сведений, порочащих честь и достоинство,
- плагиат,
- недостоверная информация.

В условиях цифровой экономики стороны совершают юридически значимые действия в любое время, место и с любого устройства, в котором может не быть предустановленного программного обеспечения, необходимого для обмена юридически значимыми электронными документами.

Требование обеспечения максимальной мобильности заставляет стороны разрабатывать принципиально другую схему взаимодействия, которая не требует совершения предварительных действий типа авторизации и подтверждения личности и доступна на любом устройстве, которое есть у пользователя и не имеет предустановленного программного обеспечения.

Если пользователи используют сервис они могут в любой момент времени без предварительной подготовки, без специальных технических знаний совершить юридически значимое действие по заключению договора, одобрению сделки, предложению условий договора или удостоверению доказательств без получения своей электронной цифровой подписи.

Когда пользователю требуется доказательства совершения юридически значимого действия, то он без труда представляет в суд свидетельство, подтверждающее факт совершения юридически значимого действия путем предоставления заверенных документов хранящихся в системе, при этом данные документы могут предоставляться пользователю, как в цифровом виде, так и в виде распечатки свидетельства подписью лица уполномоченного на заверение,

Часто как меру обеспечения доказательства необходимо представить скриншот интернет-ресурса, подтверждающего, что в такое-то время на нем находилась спорная информация. Распечатанный скриншот сайта не заверен и в случае судебных споров не будет надлежащим доказательством. Однако если его фиксирует независимая сторона, с помощью предлагаемого способа и системы, о чем выдается свидетельство, то правдивость скриншота сложно опровергнуть.

В современных условиях часто общение и обмен актами оказания услуг, претензиями и т.п. документами по договорам осуществляется через электронную почту, что обеспечивает оперативность в решении проблем. Однако при обмене информацией и документами через электронные сервисы, возможна ситуация, когда недобросовестная сторона умышленно отрицает факт получения направленной ей информации и/или документов, основываясь на том, что пользователь мог удалить информацию или ему будет затруднительно обращаться к оператору за восстановлением письма.

В свою очередь данные обстоятельства приводили к нарушению прав и интересов отправителя, который в случае возникновения конфликта, либо судебного спора не мог ссылаться на подобную переписку и обмен документами по ряду причин, в том числе из-за отсутствия гарантий достоверности и подтверждения факта отправки документов. Поэтому, если организация пользуется указанным способом, то она без труда представляет в суд свидетельство, подтверждающее факт совершения юридически значимого действия путем активации системной ссылки, что является надлежащим доказательством.

В настоящее время достаточно часто возникают ситуации, связанные с тем, что в сети Интернет размещаются недостоверные сведения о товарах, услугах и т.д., публикуются сведения, порочащие честь и достоинство граждан, незаконно используются чужие товарные знаки, выкладываются на сайтах фотографии, без согласия их владельца на публикацию и демонстрацию и т.д. Порой, для того, чтобы гражданину восстановить свои права, свое доброе имя, требуется длительное время, за которое те сведения, которые были опубликованы, могут быть удалены с этих страниц или заменены, исправлены, что позволит нарушителям избежать ответственности, а распечатанный скриншот сайта не заверен и в случае судебных споров не будет надлежащим доказательством. С помощью указанного способа можно зафиксировать информацию, содержащуюся на сайтах (интернет-страницах) в сети Интернет. Сохраненные Интернет-страницы будут доступны в любой момент в «Личном кабинете» информационной системы, и в случае необходимости, заверенную информационной системой Интернет-страницу можно использовать в качестве доказательства в любой спорной ситуации, в том числе в суде, в случае если в дальнейшем доступ на интернет-сайт недоступен.

Способ позволяет удаленно фиксировать, сохранять в собственной базе данных и подтверждать факт достоверности и неизменности хранящейся на сервере системы информации: снимки с экрана, почтовую переписку, файлы любых типов.

Способ также может позволять посредством программы удаленного доступа и через оператора заходить на сервер информационной системы и с него заходить на ресурсы, требующие авторизации, и фиксировать любую информацию.

Способ позволяет хранить на сервере информационной системы под персональной учетной записью пользователя все зафиксированные материалы с возможностью заказа заверенной копии, в том числе, и на бумажном носителе.

Способ позволяет информационной системе заверить запрашиваемую пользователем информацию, хранящуюся на сервере системы, и подтверждает ее целостность и неизменность.

Способ позволяет информационной системе делать снимки с экрана, обращаясь по указанному адресу в Интернет по созданному пользователем расписанию.

Способ позволяет информационной системе сохранять на сервере копии отправляемых пользователем электронных писем и хранить их в неизменном виде.

Способ позволяет информационной системе фиксировать и подтверждать факт наличия на различных сайтах: видео, флеш, графику и контент иного рода, который может быть сохранен в системной памяти.

Реализация способа осуществляется по следующему алгоритму:

1. Пользователь проходит авторизацию на сервере загрузки документов с любого устройства путем пары логин-пароль и/или предоставления своей фотографии с паспортом в развернутом виде.
2. Пользователь выбирает на своем устройстве предварительно сохраненный документ либо url ссылку на ресурс, который необходимо заверить и посредством программно-аппаратного обеспечения передает его на сервер приема документов предлагаемой системы.
3. Сервер приема документов предлагаемой системы идентифицирует пользователя, находит или формирует для данного

пользователя выделенный для него объем памяти в устройстве хранения документов и сохраняет туда необходимую для заверения информацию или документы.

4. Далее в сохраненную информацию или документы, блоком обработки информации, проставляется время, дата и год и заверяется цифровой электронной цифровой подписью лица уполномоченного на данное действие с получением, по меньшей мере, одного заверенного документа. При этом данная операция может осуществляться, как в ручную, лицом уполномоченного на данное действие, так и программным обеспечением.

5. Далее документ, сформированный предлагаемой системой, хранится в сервере репозитория, откуда копия его в любое время может быть передана пользователю, и может быть при необходимости распечатан с дополнительным заверением лицом уполномоченного на данное действие.