(19) Евразийское патентное ведомство

(11) 037018 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2021.01.27

(21) Номер заявки
201790385

(22) Дата подачи заявки
2015.06.15

(51) Int. Cl. ***G06F 21/32*** (2013.01)
G06F 21/62 (2013.01)
G06F 21/64 (2013.01)

(54) СПОСОБ ЦИФРОВОГО ПОДПИСАНИЯ ЭЛЕКТРОННОГО ФАЙЛА

(31) **P 14 00392; P 15 00259**
(32) **2014.08.18; 2015.05.29**
(33) **HU**
(43) **2017.09.29**
(86) **PCT/HU2015/000055**
(87) **WO 2016/027111 2016.02.25**

(71)(73) Заявитель и патентовладелец:
ЧИК БАЛАЖ; РОГАН АНТАЛЬ (HU)

(72) Изобретатель:
Чик Балаж, Лендьель Чаба, Роган Анталь (HU)

(74) Представитель:
Хмара М.В., Рыбаков В.М., Липатова И.И., Новоселова С.В., Дощечкина В.В., Пантелеев А.С., Ильмер Е.Г., Осипов К.В. (RU)

(56) WO-A1-0108352
JIN A T B: "Cancellable Biometrics and Multispace Random Projections", COMPUTER VISION AND PATTERN RECOGNITION WORKSHOP, 2006 CONFERENCE ON NEW YORK, NY, USA 17-22 JUNE 2006, PISCATAWAY, NJ, USA, IEEE, PISCATAWAY, NJ, USA, 17 June 2006 (2006-06-17), pages 164-164, XP010922679, DOI: 10.1109/CVPRW.2006.49 ISBN: 978-0-7695-2646-1 *Introduction* *3 Multispace Random Projection (MRP)*

(57) Настоящее изобретение представляет собой способ цифрового подписания электронного файла (48), содержащий следующие шаги, выполняемые сервером: формирование значения (50) запроса, содержащего параметр (52) проекции; передачу значения (50) запроса в клиентское устройство через канал связи; прием через канал связи доказательной записи (70), электронного файла (48), который должен быть подписан, и биометрических данных (54) пользователя из клиентского устройства; формирование редуцированных биометрических проверочных данных с применением проекции, использующей параметр (52) проекции; формирование проверочной доказательной записи и сравнение ее с доказательной записью (70), переданной клиентским устройством; формирование сертификата сервера; подписание сертификата сервера с использованием секретного ключа подписывания сервера, в результате чего формируется подписанный сертификат сервера; формирование цифровой подписи путем связывания, по меньшей мере, подписанного сертификата сервера и хэша (49) электронного файла (48); и связывание цифровой подписи с электронным файлом (48), в результате чего формируется подписанный цифровой подписью электронный файл. Настоящее изобретение также представляет собой способ аутентификации.

037018 B1

037018 B1

Область техники, к которой относится изобретение

Настоящее изобретение относится к способам осуществления цифровой подписи электронного файла и к способу аутентификации, основанному на использовании биометрических данных.

Уровень техники

Существуют разнообразные способы аутентификации и подписывания электронных файлов. В патенте WO 2007/034255 раскрывается способ с использованием для цифрового подписывания электронных файлов, направляемых в эту систему от имени удаленных пользователей, централизованной системы предоставления цифровой подписи, использующей цифровые подписи, содержащие биометрические данные этих пользователей. Посредством биометрических данных (например, данных, относящихся к рукописной подписи) цифровая подпись может быть связана с подписывающим лицом, однако в этом изобретении цифровая подпись может налагаться на электронный файл только под надзором и с аутентификацией. Изъяном этого способа является недостаточная защищенность проверки данных, передаваемых обратно удаленным пользователем, и работы с биометрическими данными.

В патенте США 6735695 B1 раскрыто техническое решение, в котором аутентификация осуществляется с использованием только части биометрических данных, а не всего биометрического образца. С целью повышения защищенности полный биометрический образец не передается. Частный биометрический образец, используемый для аутентификации, может выбираться и с использованием случайного числа. Недостаток этого известного технического решения состоит в том, что не выполняется редукция данных (преобразование), и поэтому перехватом частного набора биометрических данных на линиях связи неуполномоченные лица смогут, рано или поздно, получить полную биометрическую информацию. Еще одним недостатком этого решения является то, что биометрический датчик регистрирует полный биометрический образец, из которого выбирается частный набор биометрических данных. Регистрация полного биометрического образца создает значительную угрозу.

В патенте США 2008/0209227 A1 раскрывается техническое решение, в котором формируется преобразованная, редуцированная версия биометрического образца. Эти редуцированные биометрические данные или редуцированная биометрическая сводка может содержать различные характерные особенности биометрического образца, например его линейные отрезки. В патенте США 2010/0066493 A1 раскрывается техническое решение, относящееся к преобразованию биометрических данных случайной проекцией. Эти известные технические решения тоже имеют вышеуказанные недостатки.

Сущность изобретения

Целью настоящего изобретения является предложение способов цифрового подписывания и удостоверения, устраняющих настолько, насколько это возможно, недостатки технических решений известного уровня техники.

Цель настоящего изобретения достигается способами по пп.1, 16, 23, 26 или 27 формулы изобретения.

Предпочтительные варианты осуществления настоящего изобретения определены в зависимых пунктах формулы изобретения.

Краткое описание чертежей

Настоящее изобретение поясняется более подробно посредством предпочтительных вариантов осуществления, показанных на сопровождающих чертежах, в которых

фиг. 1 представляет собой функциональную схему основных устройств, используемых в информационных технологиях, применяемых в способе в соответствии с настоящим изобретением;

фиг. 2 представляет собой обобщенную схему последовательности операций способа в соответствии с настоящим изобретением;

фиг. 3 представляет собой схему последовательности шагов первого варианта осуществления способа в соответствии с настоящим изобретением на стороне клиента;

фиг. 4 представляет собой схему последовательности шагов проверки и аутентификации первого варианта осуществления способа в соответствии с настоящим изобретением на стороне сервера;

фиг. 5 представляет собой схему последовательности шагов еще одного варианта осуществления, полученного модификацией варианта осуществления, показанного на фиг. 3;

фиг. 6 представляет собой относящуюся к фиг. 5 схему последовательности шагов на стороне сервера, полученную модификацией варианта осуществления, показанного на фиг. 4;

фиг. 7 представляет собой схему последовательности шагов шифрования электронного файла сервером;

фиг. 8 представляет собой схему последовательности шагов создания и подписывания доказательной записи сервера.

Сведения, подтверждающие возможность осуществления изобретения

Основные устройства, используемые в информационных технологиях, и основные компоненты, используемые в способе в соответствии с настоящим изобретением, показаны на фиг. 1. Способ в соответствии с настоящим изобретением предназначен для подписывания сервером 20 электронного файла, сделанного доступным для клиентского устройства 10 или сформированного на клиентском устройстве 10. Клиентское устройство 10 может быть соединено с сервером 20 через канал 30 связи. Такой электронный канал 30 связи может быть установлен, например, в электронной сети связи 32, например, использующей

проводную и/ или беспроводную локальную вычислительную сеть (ЛВС), глобальную информационную сеть, например интернет, а также мобильные сети связи, соответствующие стандартам 3G или 4G, сеть GSM и т.д.

Клиентское устройство 10 может быть реализовано как любое из таких пользовательских устройств связи, содержащих один или более процессоров 12, хранилище 14 данных, клиентский модуль 16 связи и периферийные устройства 18. Например, клиентским устройством 10 может быть настольный компьютер, портативный компьютер или ноутбук, сотовый телефон (мобильный телефон), в особенности смартфон, планшетный компьютер и т.д.

В данном варианте осуществления хранилище 14 данных показано как неотъемлемая часть клиентского устройства 10, но хранилище 14 данных также может быть внешним средством хранения данных, соответственно компонент, называемый в настоящем документе хранилищем 14 данных, считается содержащим любые внутренние и внешние средства хранения данных, к которым может иметь доступ клиентское устройство 10. Хранилище 14 данных может быть осуществлено как средство хранения данных электронного, магнитного, оптического или любого другого типа (такого, например, как память, карта памяти, жесткий диск, внешний диск и т.д.). Хранилище 14 данных предпочтительно используется для хранения ключей PKI (Public Key Infrastructure, инфраструктура открытого ключа), по меньшей мере, открытого ключа 40a шифрования сервера, соответствующего серверу 20. Можно также представить себе вариант осуществления, в котором открытый ключ 40a шифрования сервера не хранится в хранилище 14 данных, а делается временно доступным для клиентского устройства 10 путем временной загрузки из интернета с целью выполнения операции шифрования.

Компонент, называемый клиентским модулем 16 связи, предполагается содержащим любые аппаратные и программные компоненты (т.е. сетевую карту, сетевое соединение, адаптер WiFi, антенну и т.д.), посредством которых клиентское устройство 10 может устанавливать, по меньшей мере, с сервером 20 электронный канал 30 связи, по которому может осуществляться обмен электронными данными.

Клиентское устройство 10 содержит как собственный компонент, или как подключенное к клиентскому устройству 10 периферийное устройство 18, или как другое внешнее устройство (т.е. устройство, каким-либо образом соединенное с клиентским устройством 10) модуль 18a получения биометрических данных и предпочтительно по меньшей мере один входной интерфейс 18b и по меньшей мере один выходной интерфейс 18c.

Например, модулем 18a получения биометрических данных может быть графический планшет, выполненный с возможностью приема и записи рукописной подписи в качестве биометрических данных. Графический планшет может быть дополнен цифровым пером, но в определенных случаях в качестве "пишущего устройства", воспринимаемого графическим планшетом, может использоваться и палец пользователя.

Модуль 18a получения биометрических данных может, например, быть реализован как сканер радужной оболочки глаза, и тогда принимается изображение радужной оболочки глаза, а цифровые данные, представляющие это изображение радужной оболочки глаза, сохраняются в качестве биометрических данных.

Модулем 18a получения биометрических данных может также быть считыватель отпечатка пальца, с использованием которого принимается отпечаток пальца, а цифровые данные, представляющие этот отпечаток пальца, сохраняются в качестве биометрических данных.

В дополнение к этому модулем 18a получения биометрических данных может быть устройство любого другого типа, выполненное с возможностью измерения/регистрации биометрического идентификатора (например, рисунка вен ладони, DNS) и записи полученных данных.

Можно также представить себе вариант осуществления, в котором модуль 18a получения биометрических данных одновременно функционирует и в качестве входного интерфейса. Например, в дополнение к приему рукописных подписей, графический планшет также может использоваться для ввода пользовательских команд управления программами, работающими на клиентском устройстве 10.

Клиентское устройство 10 предпочтительно содержит по меньшей мере один экран, используемый в качестве выходного интерфейса 18c. Можно представить себе и возможность использования других интерфейсов вывода 18c, например принтеров или оборудования для записи на различные цифровые носители (к примеру, CD, DVD, гибкий диск, съемные накопители, карты памяти и т.д.).

Указанный по меньшей мере один входной интерфейс 18b может быть осуществлен, например, в виде клавиатуры, мыши или другого типового устройства ввода. Выходной интерфейс 18c может одновременно быть и входным интерфейсом, как, например, сенсорный экран. Аналогично устройство записи данных на носитель может одновременно функционировать в качестве входного интерфейса, если это устройство выполнено с возможностью чтения и записи на носители. Клавиатура может быть реализована как виртуальная клавиатура, например, если в качестве экрана используется сенсорный экран, то на нем может отображаться виртуальная клавиатура, которая может быть использована в качестве входного интерфейса 18b.

Если в качестве входного интерфейса 18b и выходного интерфейса 18c используется сенсорный экран, то этот сенсорный экран также может выполнять функции модуля 18a получения биометрических

данных, т.е. в определенных случаях одно периферийное устройство может выполнять три функции.

Сервером 20 может быть любое устройство обработки информации (например, настольный или портативный компьютер), выполненное с возможностью функционирования в качестве сервера. Сервер 20 содержит один или более процессоров 22, хранилище 24 данных и серверный модуль 26 связи.

Хранилище 24 данных может быть осуществлено как средство хранения данных, выполненное по электронному, магнитному, оптическому или любому другому типу. В настоящем варианте осуществления хранилище 24 данных показано как составная часть сервера 20, но хранилищем 24 данных может также быть внешнее средство хранения данных, к которому сервер 20 имеет доступ, например, аппаратный модуль 24' защиты (hardware security module, HSM), показанный на фиг. 1. Таким образом, под хранилищем 24 данных понимается любое внутреннее и внешнее средство хранения данных (например, встроенное ПЗУ и ОЗУ, внешний модуль HSM, другое внешние средство хранения и т.д.), к которым сервер 20 может получить доступ непосредственно или опосредованно.

Сервер 20, предпочтительно, хранит ключи PKI и другие ключи подписывания, например секретный ключ 40b шифрования сервера и секретный ключ 41 подписывания сервера, соответствующий серверу 20, а также секретные ключи 42 подписывания пользователя, соответствующие пользователю, которые могут храниться в базе 43 данных ключей в хранилище 24 данных и, что является наиболее предпочтительным, в модуле 24' HSM. Хранилище 24 данных может предпочтительно также хранить базу 44 данных пользователей и в этой базе данных или отдельно от нее базу 45 биометрических данных, предназначенную для хранения биометрических образов 45a пользователя.

Секретным ключом 42 подписывания пользователя может, например, также быть секретный ключ шифрования на базе инфраструктуры PKI, который может быть использован кем угодно для расшифровки зашифрованных данных с использованием открытого ключа шифрования, но известны и другие алгоритмы подписывания, не основанные на шифровании. Например, для подписывания могут использоваться алгоритмы типа HMAC (hash-based message authentication code, код удостоверения сообщения на основе хэша). В этих алгоритмах используется формирование комбинированного значения хэша из значения ключа и самого сообщения. Хэш выполняет двойную функцию: с одной стороны, защищает идентичность сообщения, с другой стороны, подтверждает, что этот хэш мог быть сформирован только тем, у кого был ключ. Основное отличие от операций подписывания типа PKI (RSA) состоит в том, что данная операция, по сути, использует один тип ключа, т.е. секретный ключ 42 подписывания пользователя, а открытый ключ подписывания пользователя не используется, и алгоритм подписывания состоит в формировании хэша, а не в шифровании.

Как и выше, компонент, называемый серверным модулем 26 связи, предполагается содержащим любые аппаратные и программные компоненты (т.е. сетевую карту, сетевое соединение, адаптер WiFi, антенну и т.д.), посредством которых сервер 20 может устанавливать по меньшей мере с клиентским устройством 10 электронный канал 30 связи, по которому может осуществляться обмен электронными данными.

Далее представлены два варианта осуществления изобретения способа в соответствии с настоящим изобретением со ссылкой на используемые в качестве примера аппаратные компоненты, описанные выше.

На фиг. 2 показана обобщенная схема последовательности операций способа в соответствии с настоящим изобретением. Шаги способа, а также документы, данные, алгоритмы и файлы, используемые или формируемые в ходе выполнения этого способа, показаны более подробно на фиг. 2-8.

Хотя для упрощения шаги пронумерованы последовательно, специалисту очевидно, что порядок шагов во многих случаях может быть изменен, или некоторые шаги могут выполняться одновременно, могут быть объединены или разделены, а между представленными здесь шагами могут быть включены дополнительные шаги.

Перед выполнением способа в соответствии с настоящим изобретением целесообразно установить канал 30 связи между клиентским устройством 10 и сервером 20. Каналом 30 связи является предпочтительно защищенный канал, который может быть реализован с использованием, например, протоколов SSL, TLS, SNPv3, VPN, HTTPS, FTPS, TelnetS, IMAPS, IPSec и т.д., что хорошо известно специалисту в данной области техники. В ходе выполнения данного способа канал 30 связи, являющийся виртуальным каналом данных, может разрываться и переустанавливаться, при этом при необходимости между клиентским устройством 10 и сервером 20 может устанавливаться более одного виртуального канала данных, но для упрощения все они в общем называются каналом 30 связи.

Предоставление электронного файла 48, который должен быть подписан, также может рассматриваться как начальная точка способа в соответствии с настоящим изобретением. Электронный файл 48 может формироваться с использованием клиентского устройства 10, и, таким образом, этот файл может, например, быть документом, сформированным на клиентском устройстве 10, или файлом изображения, снятого камерой клиентского устройства 10, используемого в качестве входного интерфейса 18b. Также можно представить себе возможность формирования электронного файла 48, который должен быть подписан пользователем клиентского устройства 10, не самим клиентским устройством 10, а прием этого файла клиентским устройством 10 из внешнего источника, например, посредством электронной почты, или загрузку электронного файла 48 из интернета, считывание с носителя информации для хранения

данных (к примеру, с CD, DVD, съемного накопителя и т.д.) с использованием устройства записи/чтения в качестве входного интерфейса 18b, прием из сервера 20 или из другого места.

На фиг. 3 подробно рассматриваются шаги 1-8 первого варианта осуществления способа, представленного на фиг. 2, в соответствии с настоящим изобретением.

В качестве шага 1 способа в соответствии с настоящим изобретением с использованием сервера 20 формируется значение 50 запроса. Значение 50 запроса содержит один или более параметров 52 проекции (как правило, чисел). Значение 50 запроса может при необходимости содержать метку времени, которая либо формируется самим сервером 20, либо по запросу сервера 20 внешним сервером меток времени, например в соответствии с протоколом RFC3161.

На шаге 2 значение 50 запроса передается сервером 20 в клиентское устройство 10 через канал 30 связи.

На шаге 3 клиентское устройство 10 используется для извлечения одного или более параметров 52 проекции из значения 50 запроса. Этот шаг может, конечно, выполняться в любое время до использования параметров 52 проекции или одновременно с ним.

На шаге 4 на стороне клиентского устройства 10 с использованием модуля 18a получения биометрических данных записываются биометрические данные 54 пользователя, которые могут содержать один или более статических или динамических элементов данных (наборов данных), записанных на основании физических характеристик пользователя. Например, если в качестве модуля 18a получения биометрических данных используется графический планшет, то в качестве биометрических данных 54 принимается и записывается рукописная подпись, созданная с использованием цифрового пера или пальца пользователя в качестве пишущего устройства. В данном случае биометрическими данными 54 могут быть, например, координаты места прижима пишущего устройства к поверхности планшета, координаты места отрыва пишущего устройства от поверхности планшета, зависимость координат пишущего устройства от времени, зависимость скорости пишущего устройства от времени, зависимость ускорения пишущего устройства от времени, зависимость силы надавливания пишущего устройства от времени или комбинация более одного вида таких данных.

В предпочтительном варианте осуществления во время ввода рукописной подписи на экране клиентского устройства 10, используемого в качестве выходного устройства 18c, отображается изображение подписи, чем обеспечивается визуальная обратная связь с пользователем. Это особенно эффективно в случае, когда модуль 18a получения биометрических данных одновременно функционирует и в качестве экрана, как в карманных персональных компьютерах, планшетных компьютерах, сотовых телефонах с сенсорным экраном и т.д.

Если модуль получения биометрических данных реализован как сканер радужной оболочки глаза, то выполняется получение изображения радужной оболочки глаза, а цифровые данные, представляющие это изображение радужной оболочки глаза, записываются в качестве биометрических данных 54. Если модулем получения биометрических данных является считыватель отпечатка пальца, то записывается отпечаток пальца, а цифровые данные, представляющие этот отпечаток пальца, сохраняются в качестве биометрических данных 54.

На шаге 5 клиентское устройство 10 используется для формирования доказательной записи 70. При выполнении этого шага клиентское устройство 10 используется для формирование хэша 49 электронного файла 48 с использованием однонаправленного защищенного алгоритма 60a формирования хэша, например, алгоритма SHA-256, SHA-512 и т.д. Хэш 49, сформированный с использованием алгоритма 60a формирования хэша, представляет собой сжатые данные, из которых невозможно получить исходный электронный файл 48. Характерной особенностью алгоритмов 60a формирования хэша является то, что изменение любой части исходного электронного файла 48 лавинообразно влияет на хэш 49, в результате чего хэш становится совершенно другим. Сформировав хэш 49 еще раз, можно проверить, вносились ли (несанкционированные) изменения в электронный файл 48 и не был ли этот файл подделан. Еще одной важной особенностью алгоритма 60a формирования хэша является невозможность создания таких файлов данных, для которых данный алгоритм сформировал бы одинаковый хэш 49.

Формирование доказательной записи 70 также содержит формирование из биометрических данных 54 пользователя редуцированных биометрических данных 56 с применением алгоритма проекции, использующего один или более параметров 52 проекции. В настоящем изобретении термин "проекция" используется для обозначения однонаправленного математического отображения или других способов редукции данных, в результате которых получаются редуцированные данные, которые невозможно использовать для восстановления исходных данных, причем такие редуцированные данные может сформировать лишь лицо, имеющее исходные данные и знающее параметры проекции. Такие проекционные алгоритмы, использующие параметры проекции (или, иными словами, алгоритмы редукции данных) известны специалисту в данной области техники; в число таких алгоритмов входят, например, проекция записанных данных на заранее определенную плоскость или ось или обработка данных посредством нейронной сети. Примером является возможность формирования из динамических данных подписи, записанных при записи рукописной подписи в качестве биометрических данных 54, статического изображения подписи (редуцированных биометрических данных 56).

Редуцированные биометрические данные 56 специфичны для конкретного пользователя, но не могут быть использованы для восстановления исходных биометрических данных 54. Редуцированные биометрические данные 56 служат в качестве доказательства того, что их формирователь - в данном случае клиентское устройство 10 - обладал исходными биометрическими данными 54 и параметрами 52 проекции, переданными с использованием значения 50 запроса.

Затем клиентское устройство 10 используется для формирования хэша 58 редуцированных биометрических данных 56 с использованием однонаправленного защищенного алгоритма формирования хэша 60b, который может совпадать с алгоритмом 60a формирования хэша или отличаться от указанного алгоритма.

После этого клиентским устройством 10 путем связывания значения 50 запроса, хэша 58 редуцированных биометрических данных 56 и хэша 49 электронного файла 48 формируется доказательная запись 70. Связывание данных может быть выполнено путем использования любого известного способа, пригодного для этой цели, например, путем выполнения побитовой операции ИСКЛЮЧАЮЩЕЕ ИЛИ, которая, сохраняя возможность проверки, объединяет данные трех указанных видов так, что никакие из этих данных невозможно определить по результату. Как и в вышеприведенном случае, здесь также может быть использована хэш-функция, обладающая возможностью формирования хэша (доказательной записи 70) путем объединения данных указанных трех видов.

Доказательная запись 70 может, кроме того, содержать дополнительные данные.

Доказательная запись 70 подтверждает, что электронный файл 48 и биометрические данные 54 происходят из клиентского устройства 10. Атакующий извне злоумышленник, пытающийся ввести в систему ранее записанные биометрические данные 54, используя предназначенный для подписания документ, не сможет сформировать доказательную запись 70, соответствующую данному документу, поскольку не знает значение 50 запроса (которое может, при необходимости, с целью предотвращения подделки также содержать метку времени). Поскольку значение 50 запроса содержит уникальные параметры, формируемые для каждого акта подписания, биометрические данные 54 не могут быть, случайно или целенаправленно, использованы дважды.

Далее на шаге 6 доказательная запись 70 предпочтительно подписывается с использованием цифрового алгоритма 71 подписывания и клиентского устройства 10. Алгоритм 71 подписывания может быть основан, например, на PKI (к примеру, алгоритм RSA), на использовании пароля, на использовании одноразового пароля или на любом другом техническом решении, которое может быть адаптировано для использования в данной ситуации. Результатом данной операции подписывания является подписанная доказательная запись 72.

На шаге 7 биометрические данные 54 и/ или электронный файл 48, который должен быть подписан, предпочтительно подписываются клиентским устройством 10, что может осуществляться с применением основанного на PKI шифрования, использующего открытый ключ 40a шифрования сервера, в результате чего зашифрованные биометрические данные 64 и зашифрованный электронный файл 68, созданные указанным образом, могут быть расшифрованы с использованием секретного ключа 40b шифрования сервера, сохраненного в базе 43 данных ключей сервера 20.

Для шифрования биометрических данных 54 и/или электронного файла 48, который должен быть подписан, могут, конечно, применяться и другие способы. Например, особенно для шифрования больших файлов, может быть целесообразно формировать уникальный симметричный ключ для каждого акта шифрования и шифровать файл с использованием этого ключа (к примеру, по симметричному алгоритму AES), при этом указанный симметричный ключ шифруется с использованием открытого PKI-ключа 40a шифрования сервера и также передается в сервер 20 клиентским устройством 10. Соответственно на стороне сервера сначала с использованием секретного ключа 40b шифрования сервера должен быть расшифрован симметричный ключ шифрования, а затем с использованием этого симметричного ключа может быть расшифрован зашифрованный файл (файлы). Преимущество такой двухстадийной операции шифрования состоит в том, что симметричный алгоритм значительно быстрее асимметричных алгоритмов шифрования, с меньшим размером служебных данных в зашифрованных файлах данных, из-за чего даже большие файлы можно шифровать быстро.

На шаге 8 подписанная доказательная запись 72, биометрические данные 64, предпочтительно зашифрованные, и электронный файл 68, предпочтительно зашифрованный, передаются клиентским устройством 10 в сервер 20 через канал 30 связи. В дополнение к этому клиентским устройством 10 в сервер 20 до, во время или после завершения представленного выше способа предпочтительно передается один или более элементов данных 74 пользователя (например, идентификатор пользователя, персональный идентификационный номер пользователя (ПИН) и т.д.). Например, при формировании доказательной записи 70 с вышеперечисленными компонентами могут также связываться данные 74 пользователя. Данные 74 пользователя могут, однако, передаваться (предпочтительно зашифрованными) в сервер 20 отдельно от доказательной записи 70, обычно с целью идентификации пользователя, требующей по меньшей мере таких данных идентификатора, на основании которых сервер 20 смог бы, например, определить, какой секретный ключ 42 подписывания пользователя из числа ключей, сохраненных в базе 43 данных ключей, должен использоваться, или, например, определить, данные 74 пользователя какого

пользователя должны использоваться для формирования цифровой подписи (подробно описывается ниже) данных, хранимых в базе 44 данных пользователей, или, например, определить, биометрический образ 45a какого пользователя - уникальный биометрический образец (образ), соответствующий данному пользователю - должен быть извлечен из базы 45 биометрических данных. Функцию идентификатора пользователя, используемого в качестве данных 74 пользователя, может выполнять и другая информация, сделанная доступной для сервера 20 путем передачи данных, например, номер телефона (если в качестве клиентского устройства 10 используется смартфон), или статический IP-адрес (если в качестве клиентского устройства 10 используется настольный компьютер) и т.д.

Шаги 9-11 первого варианта способа в соответствии с настоящим изобретением, представленного на фиг. 2, подробно иллюстрируются на фиг. 4.

На шаге 9 сервер 20 используется для идентификации пользователя клиентского устройства 10 и для определения по меньшей мере одного элемента данных 74 пользователя. Этими данными пользователя могут быть данные 74 пользователя, переданные клиентским устройством 10, или дополнительные элементы данных 74 пользователя, извлеченные из базы 44 данных пользователей на основании данных 74 пользователя, переданных клиентским устройством.

Событием, относящимся к шагу 9, может быть аутентификация пользователя, в ходе которой, например, проверяется подпись доказательной записи 72, подписанной клиентским устройством 10, и соответственно выполняется аутентификация пользователя.

В особо предпочтительном варианте осуществления, однако, аутентификация осуществляется на основании биометрических данных 54. Для выполнения аутентификации на шаге 10 сначала зашифрованные биометрические данные 64, переданные клиентским устройством 10, расшифровываются с использованием секретного ключа 40b шифрования сервера (или, при необходимости, с использованием симметричного ключа, расшифрованного с использованием секретного ключа 40b шифрования сервера). Затем из базы 45 биометрических данных извлекается биометрический образ 45a, соответствующий пользователю, указываемому данными 74 пользователя, после чего биометрический образ 45a сравнивается сервером 20 с расшифрованными биометрическими данными 54 с использованием пригодной для этого программы (например, программы, содержащей алгоритм на основе нейронной сети, на основе проекции, на основе CRC или другие аналогичные алгоритмы). Например, подлинность рукописной подписи проверяется программой, работающей на сервере 20, с использованием ранее полученных в качестве биометрического образа 45a образцовых подписей данного пользователя. Если аутентификация прошла успешно, т.е. переданные биометрические данные 54 соответствуют одному или более биометрическим образам 45a, сохраненным для данного пользователя, то данная операция продолжается, в противном случае запрос на подписывание электронного файла 48 отклоняется и операция прекращается.

Преимущество аутентификации, выполняемой с использованием биометрических данных 54, состоит в том, что от пользователя не требуется запоминание каких-либо кодов ПИН. Аутентификация, выполняемая с использованием в качестве биометрических данных 54 рукописной подписи, особенно предпочтительна, поскольку наиболее близка к подписыванию бумажного документа привычным образом.

Предпочтительно все биометрические данные 54, передаваемые в сервер 20, сохраняются в базе 45 биометрических данных в виде биометрических образов 45a, соответствующих пользователям, при этом сервер 20 также проверяет, идентичны ли биометрические данные 54, предоставленные в данный момент, биометрическим образам 45a, сохраненным ранее, или их части, чем обеспечивается защита от повторного предоставления биометрических данных 54, полученных ранее.

На шаге 11 в соответствии с нижеследующим описанием (см. фиг. 4) с использованием сервера 20 формируется проверочная доказательная запись 70'.

Сервер 20 используется для формирования редуцированных биометрических проверочных данных 56' из биометрических данных 54 с применением проекции, использующей параметр 52 проекции, переданный в значении 50 запроса, по тому же алгоритму проекции, который был использован на стороне клиента для формирования редуцированных биометрических данных 56. Затем с использованием того же алгоритма 60b формирования хэша, который использовался на стороне клиента для формирования хэша 58 редуцированных биометрических данных 56, формируется хэш 58' редуцированных биометрических проверочных данных 56'.

Далее сервер 20 используется для формирования хэша 49' электронного файла 48 с использованием того же алгоритма 60a формирования хэша, который использовался для формирования хэша 49 электронного файла 48 на стороне клиента.

Затем сервером 20 формируется проверочная доказательная запись 70', связывающая значение 50 запроса, хэш 58' редуцированных биометрических проверочных данных 56' и хэш 49' электронного файла 48, которая сравнивается с доказательной записью 70, переданной клиентским устройством 10. Если проверочная доказательная запись 70' идентична доказательной записи 70, переданной клиентским устройством 10, то операция подписания цифровой подписью продолжается, в противном случае запрос отклоняется и операция прерывается.

Соответствующие шаги второго варианта способа в соответствии с настоящим изобретением показаны на фиг. 5 и 6, соответствующих модифицированным версиям фиг. 3 и 4 соответственно.

С точки зрения защиты от хищения и повторного использования биометрических данных желательно, чтобы не параметр (параметры) проекции, передаваемые вместе со значением запроса, использовался (использовались) для последующей редукции записанных биометрических данных, а записывались данные, уже редуцированные согласно редукции, соответствующей указанным параметрам. Действительно, при наличии доступа к сохраненным биометрическим данным редуцированный набор биометрических данных можно сформировать из записанных биометрических данных для любых значений параметров. Если же выполнять операцию записи с зависимостью от значений параметров, то записанные редуцированные биометрические данные нельзя будет затем использовать для выполнения редукции, соответствующей другим значениям параметров.

В случае рукописных подписей можно в качестве примера предложить решение, в котором часть указанного параметра содержит текст, который должен быть написан рукой подписывающего лица, и если один и тот же текст никогда не будет предъявлен к написанию дважды, то гарантируется невозможность последующего формирования рукописного текста, соответствующего другому значению параметра (тексту) с использованием ранее записанного неизменного текста.

Реализация параметра проекции и редукции биометрических данных в соответствии с этим параметром может быть подразделена на три основных категории. Каждая из этих категорий содержит преобразование, выполняемое в зависимости от параметра (эти три категории применимы и для первого варианта настоящего изобретения, показанного на фиг. 3 и 4).

1. Редукция биометрических данных, в которой преобразование задается непосредственно данным параметром.

Примеры:

проекция скорости на прямую линию заданного направления (подпись);

проекция ускорения на прямую линию заданного направления (подпись);

получение дискретных данных с использованием конкретных значений X, Y, Z (подпись);

информация изображения, взятая в конкретных положениях, определяемых указанным параметром (подпись, отпечаток пальца, радужная оболочка глаза);

проекция характеристических точек на прямую линию заданного направления (отпечаток пальца, радужная оболочка глаза).

2. Редукция биометрических данных, в которой указанный параметр предназначен для выбора алгоритма аутентификации (или одновременно более одного алгоритма). В данном случае результат проверки биометрических данных состоит из отдельных результатов проверки множества характерных особенностей. Например, проверяется изменение во времени скоростей в направлениях X и Y и углы касательных векторов, а окончательное решение принимается на основании результатов, получаемых в этих отдельных сравнениях. В данном случае параметр редукции определяет только тип редукции, который должен выполняться записывающим устройством. Если, например, параметр указывает, что аутентификация должна выполняться с использованием ускорения в направлении X и изменения угла касательного вектора, то записаны будут эти две серии данных (т.е. редуцированный набор биометрических данных), из которых невозможно восстановить исходный набор биометрических данных.

Примеры:

касательный вектор (подпись);

скорости и ускорения в направлениях X и Y (подпись);

сила надавливания (подпись).

3. Редукция биометрических данных, в которой преобразование задается данным параметром косвенно. Например, в эту категорию попадают технические решения, реализуемые с использованием нейронных сетей. Например, нейронная сеть, используемая для аутентификации, может состоять из трех уровней. Данная нейронная сеть имеет неизменную структуру, и для аутентификации данного человека всегда используется одна и та же сеть, определяемая своей структурой и весами. Для каждого человека, подлежащего аутентифицикации, обучается уникальная нейронная сеть, и эта сеть может использоваться для распознавания только данного человека. Целесообразно, чтобы при этом значение параметра содержало веса и при необходимости другие настройки первого уровня нейронной сети. В ходе операции регистрации на основании параметра 52 проекции, переданного сервером, вычисляются все входные параметры второго уровня; указанный параметр проекции фактически образует редуцированный набор биометрических данных, из которого невозможно восстановить подпись. Модулю аутентификации не нужно заново вычислять нейронную сеть на основании значения параметра (указанная сеть уже известна данному модулю, поскольку была построена в ходе выполнения операции регистрации подписи), и все, что требуется сделать серверу - это удостовериться, что первый уровень, определяемый указанным параметром, идентичен первому уровню уже известной нейронной сети, и если это так, то в модуле аутентификации будут запущены второй и третий уровни.

Если сеть имеет пять уровней и переданный параметр содержит данные первых двух уровней, то в качестве редуцированного набора биометрических данных из стороны клиента будут приняты входные данные третьего уровня, и сервер запустит в модуле аутентификации третий, четвертый и пятый уровни.

В трех вышеуказанных категориях используются следующие биометрические образы.

В категории 1 база 45 биометрических данных и содержащиеся в ней биометрические образы 45a, как правило, содержат сами ранее записанные биометрические образцы (например, подписи), поскольку эти биометрические образцы могут быть использованы для вычисления всей информации, требуемой в ходе операции аутентификации. Параметры редукции данных, например параметры линии проекции или параметры других способов выбора решения, различны для каждого сеанса, и должна быть возможность вычисления редуцирующих отображений и для образцов/подписей, содержащихся в данном образе. Особым случаем этой ситуации может быть использование конечного числа заранее записанных "проекций", т.е. редуцированных наборов биометрических данных (например, проекций на три заранее определенные линии); в этом случае нет необходимости повторно вычислять в модуле аутентификации серии опорных данных с использованием полного множества биометрических данных (записанных во время регистрации), поскольку эти данные могут быть вычислены заранее, в ходе операции регистрации. Поэтому могут быть реализованы даже такие варианты осуществления изобретения, в которых полный биометрический образец неизвестен даже самому модулю аутентификации.

В категориях 1 и 2 соответственно биометрический образ определенного человека может состоять из серий заранее рассчитанных редуцированных данных, поскольку эти данные могут формироваться во время регистрации этого человека.

Однако для варианта категории 3, использующего нейронную сеть, биометрический образ человека образуется значениями весов и настройками нейронной сети, обученной конкретно для этого человека. Нейронная сеть должна существовать к моменту передачи значения параметра (поскольку этот параметр образован первыми уровнями этой сети), и вследствие ее природы сеть не может быть сформирована (обучена) еще раз точно таким же образом, как ранее. Поэтому настройки нейронной сети должны храниться в биометрическом образе.

Резюмируя, можно представить себе, что биометрический образ может содержать

полные биометрические образы, записанные во время регистрации;

только определенные заранее вычисленные серии данных (редуцированные наборы биометрических данных), в этом случае невозможно использование произвольных проекций; или

комбинацию полных биометрических образцов и заранее вычисленных серий данных.

Конечно, при проверке биометрического идентификатора могут иметь место все возможные комбинации вышеприведенных параметров, т.е. возможна ситуация, в которой параметр 52 проекции из значения 50 запроса указывает, что для аутентификации требуются заданная проекция ускорения в направлении X, значения, получаемые заданным алгоритмом (к примеру, на основании силы надавливания), и входные значения второго уровня нейронной сети, соответствующие данному человеку. Затем путем комбинирования результатов этих частных аутентификаций выполняется итоговая аутентификация.

Фиг. 5 представляет схему последовательности шагов, содержащую шаги стороны клиента второго варианта настоящего изобретения. Из сравнения фиг. 3 и фиг. 5 можно видеть, что этот второй вариант настоящего изобретения отличается от варианта осуществления, описанного выше, тем, что для более качественной защиты полные биометрические данные на стороне клиента не записываются, а вместо этого параметр 52 проекции, передаваемый в значении 50 запроса, уже определяет способ записи биометрических данных, иными словами, вместо полного набора биометрических данных на стороне клиента записываются только редуцированные биометрические данные 56. Редуцированные данные могут записываться различными способами. В предлагаемом в качестве примера случае можно представить себе, что, принимая во внимание параметр 52 проекции, модуль 18a получения биометрических данных сохраняет в своей памяти и передает для дальнейшей обработки только редуцированные биометрические данные 56. Также можно представить себе вариант, в котором полные биометрические данные временно помещаются в память модуля 18a получения биометрических данных, но записываются и передаются только частные данные, определяемые параметром 52 проекции.

В дополнение к этому вариант осуществления в соответствии с фиг. 5 отличается от варианта осуществления, показанного на фиг. 3, тем, что в ходе выполнения этого способа для передачи в сервер 20 доступны только редуцированные биометрические данные 56, предпочтительно в зашифрованной форме, т.е. в виде зашифрованных редуцированных биометрических данных 65.

В соответствии с вышеизложенным во всех без исключения вариантах осуществления способа в соответствии с настоящим изобретением информационное наполнение параметра 52 проекции, включаемого в значение 50 запроса, может меняться очень широко. Можно представить себе случай, в котором значение 50 запроса образуется самим параметром 52 проекции, т.е. состоит только из одного параметра. Также можно представить себе, что значение 50 запроса, помимо параметра 52 проекции, содержит дополнительные данные, не используемые в операции редукции данных. Параметром 52 проекции может быть один параметр или даже множество параметров в соответствии с требованием входного уровня, веса уровней, при необходимости другие параметры сети в случае обработки данных нейронной сетью. В контексте настоящей патентной заявки под параметром 52 проекции в наиболее широком возможном смысле понимается любой параметр или множество параметров, описанных выше. Термин "проекция" в этом контексте не означает, что редукция данных может выполняться только путем проекции, понимаемой в узком смысле, а под параметром 52 проекции понимается любой параметр, посредством которого

может быть выполнена редукция данных биометрического образца. Таким образом, под параметром 52 проекции понимается параметр или множество параметров редукции данных любого типа, понимаемый в наиболее широком возможном смысле.

На фиг. 6 показаны операции, относящиеся к шагам стороны сервера во втором варианте настоящего изобретения, показанном на фиг. 5. Сравнив фиг. 6 и 4, можно увидеть, что во втором варианте осуществления на стороне сервера принимается не полное множество биометрических данных, а лишь редуцированные биометрические данные, предпочтительно зашифрованные (зашифрованные редуцированные биометрические данные 65). При использовании шифрования из этих данных путем расшифровки с использованием секретного ключа 40b шифрования сервера получаются редуцированные биометрические данные 56, которые могут быть затем использованы для формирования проверочной доказательной записи 70' или предпочтительно для целей аутентификации.

В операции в соответствии с фиг. 6 редуцированные биометрические данные 56 доступны на стороне сервера, параметр 52 проекции для их формирования не требуется. Как можно видеть, данный вариант осуществления настоящего изобретения является более защищенным, чем варианты осуществления в соответствии с фиг. 3 и 4, поскольку полный биометрический образец не передается, даже в зашифрованной форме.

В данном варианте осуществления редуцированные биометрические данные 56 могут быть использованы для аутентификации на стороне сервера. Биометрический образ 45a, соответствующий данному пользователю, отыскивается среди биометрических образов 45a, хранимых в базе 45 биометрических данных, с использованием соответствующих данных 74 пользователя, а затем с использованием параметра 52 проекции, передаваемого в значении 50 запроса, из данного биометрического образа 45a создаются проверочные данные 56" редуцированного биометрического образа. Соответственно аутентификация может выполняться путем сравнения редуцированных биометрических данных 56 (принимаемых из стороны клиента в зашифрованной форме, а затем расшифровываемых) и проверочных данных 56" редуцированного биометрического образа.

Шаги 12-16 способа в соответствии с настоящим изобретением подробно показаны на фиг. 7. На шаге 12 сервер 20 используется для формирования сертификата 80 сервера путем связывания по меньшей мере хэша 49 электронного файла 48, по меньшей мере одного элемента данных 74 пользователя и по меньшей мере данных 78 подписи, относящихся ко времени данной подписи.

Указанный по меньшей мере один элемент данных 74 пользователя может быть данными 74 пользователя, переданными клиентским устройством 10, или другими данными, извлеченными из базы 44 данных пользователей на основании данных 74 пользователя, переданных указанным клиентским устройством. Данные 74 пользователя, используемые для формирования сертификата 80 сервера, содержат, как правило, один или более следующих элементов данных: имя пользователя (подписывающего лица), дата рождения, место рождения, имя матери, адрес, номер идентификационной карты и т.д.

Данные 78 подписи представляют собой метаданные, описывающие "обстоятельства" подписи, в число которых, как правило, входит один или более из следующих элементов: дата подписывания, информация о клиентском устройстве 10, информация о сервере 20, имя подписанного электронного файла 48 и т.д.

На шаге 13 сертификат 80 сервера, предпочтительно, подписывается сервером 20 с использованием секретного ключа 41 подписывания сервера с целью формирования подписанного сертификата 82 сервера, который позднее может использоваться для однозначного установления факта того, что данная подпись происходила из сервера 20. Секретный ключ 41 подписывания сервера может быть идентичным секретному ключу 40b шифрования сервера, использовавшемуся на предыдущих шагах. Подписанный сертификат 82 сервера может тем не менее формироваться с использованием другого ключа или другого алгоритма подписывания; в число пригодных для этой цели алгоритмов подписывания входят, например, алгоритмы типа HMAC (код удостоверения сообщения на основе хэша).

На шаге 14 (который может предшествовать шагам 12 и 13) сервер 20 используется для формирования визуально представимых биометрических данных 54a, в качестве одной из возможностей из биометрических данных 54 (или, в случае варианта осуществления в соответствии с фиг. 5 и 6, из редуцированных биометрических данных 56) с использованием однонаправленного алгоритма 84 отображения. Например, из динамических данных рукописной подписи формируют статическое изображение подписи. Также можно представить себе создание визуально представимых биометрических данных 54a из биометрических данных 54 других типов (например, отпечатков пальцев, изображений вен ладони, изображений радужной оболочки глаза), но в случае биометрических данных этих типов визуальные биометрические данные 54a, как правило, не формируют. Алгоритм 84 отображения может, в качестве одной из возможностей, иметь в своей основе алгоритм проекции, реализуемый с использованием параметра 52 проекции.

На шаге 15 сервер 20 используется для формирования цифровой подписи 85 путем связывания подписанного сертификата 82 сервера, хэша 49 электронного файла 48 и, при их наличии, визуально представимых биометрических данных 54. В этом шаге связывание данных выполняется предпочтительно путем объединения указанных данных в блок данных. Затем с электронным файлом 48 связывается циф-

ровая подпись 85, например, путем ее встраивания в указанный файл, или путем включения как указанного файла, так и указанной подписи в файл общеизвестного стандартного типа, например в файл XML, в результате чего получается подписанный цифровой подписью электронный файл 86. Встраивание предпочтительно выполняется таким образом, чтобы при открытии подписанного цифровой подписью электронного файла 86 визуально представимые биометрические данные 54a можно было увидеть в виде изображения подписи. Цифровая подпись 85 может, конечно, содержать и другие данные.

На шаге 16 предпочтительно подписанный цифровой подписью электронный файл 86 также подписывается от имени пользователя с использованием сервера 20, например путем использования секретного ключа 42 подписывания пользователя, в результате чего получается дважды подписанный электронный файл 88. Используя открытый ключ подписывания пользователя, любой может удостовериться, что дважды подписанный электронный файл 88 был подписан секретным ключом 42 подписывания пользователя, соответствующим данному пользователю (подписывающему лицу).

Шаг 17 способа в соответствии с настоящим изобретением подробно показан на фиг. 8.

На шаге 17 сервер 20 используется для формирования доказательной записи 90 сервера путем связывания, по меньшей мере, значения 50 запроса, биометрических данных 54 (или, в варианте осуществления в соответствии с фиг. 5 и 6, редуцированных биометрических данных 56) и хэша 49 электронного файла 48 (например, путем выполнения вышеупомянутой побитовой операции ИСКЛЮЧАЮЩЕЕ ИЛИ или с использованием алгоритма формирования хэша), доказательная запись 90 сервера затем подписывается секретным ключом 41 подписывания сервера, и подписанная доказательная запись 92 сервера, полученная указанным образом, сохраняется. Обстоятельства акта подписывания, а также данные, использованные в ходе указанного акта, могут быть определены из подписанной доказательной записи 92 сервера с использованием открытого ключа 40a подписывания сервера. Доказательная запись 90 сервера может быть использована позднее (даже через годы) для доказательства того, что данная транзакция подписывания с данным содержанием действительно имела место. Это может требоваться, например, для судебных слушаний. В таких случаях могут требоваться полные биометрические данные 54, и соответственно в доказательную запись 90 сервера включается предпочтительно полное множество биометрических данных, а не только редуцированные биометрические данные 56, хэш 58 или визуальные биометрические данные 54a.

Вышеописанная операция может быть выполнена и в случае множества подписывающих лиц, естественно, в этом случае с использованием модуля 18a получения биометрических данных записываются биометрические данные 54 более одного пользователя и для каждого набора биометрических данных 54 выполняются соответствующие операции, а на стороне сервера из всех наборов биометрических данных 54 создаются визуальные биометрические данные 54a и все они включаются в цифровую подпись 85.

Как можно понять из вышеприведенного обсуждения, настоящее изобретение идет вразрез с общепринятым инженерным подходом, в котором предпочтение отдается более простым решениям. Исходя из здравого смысла, следовало бы использовать общую цифровую подпись и для биометрических данных, и для исходного документа, тем самым "соединяя" их имеющим законную силу образом. В этом случае, при условии, что набор биометрических данных и документ известны, можно проверить, соответствует ли данный набор биометрических данных данному документу. Однако кто-либо, завладевший набором биометрических данных, сможет использовать эти данные путем копирования для создания другого документа. Настоящее изобретение делает это обычное решение более защищенным: чтобы предотвратить раскрытие набора биометрических данных, он хранится и используется в зашифрованной/редуцированной форме.

В известном уровне техники соответствие набора биометрических данных и документа может быть удостоверено только доверенным органом, которому предоставлены полномочия на расшифровку набора биометрических данных. Однако можно распространить возможность проведения проверки и на органы, не считающиеся доверенными. Техническое решение в соответствии с настоящим изобретением дает недоверенному органу возможность проверки подлинности документов без расшифровки зашифрованного набора биометрических данных.

Таким образом, решение в соответствии с настоящим изобретением противоречит принципам упрощения в следующем.

Данное техническое решение рассчитано на создание на основе запроса редуцированного набора биометрических данных, которые включаются в доказательную запись, подписываемую с использованием как самого документа, так и параметров указанного запроса. Подписанная доказательная запись и редуцированный набор биометрических данных могут быть переданы в любой недоверенный орган, поскольку не могут быть использованы для восстановления исходного набора биометрических данных из-за особенностей алгоритма проекции, при этом указанное редуцированное значение будет уникальным для каждой подписи, поскольку его можно сформировать, только используя каждый раз разные параметры (т.е. два идентичных редуцированных изображения не должны использоваться даже в случае идентичных наборов биометрических данных). Поскольку подлинность подписанной доказательной записи может быть удостоверена недоверенным органом, этот орган может гарантировать, что с данным документом связан должный набор биометрических данных.

Способ аутентификации в соответствии с настоящим изобретением также содержит вышеописанные шаги, и любой из представленных выше предпочтительных вариантов осуществления пригоден для данного способа аутентификации. В способе аутентификации в соответствии с настоящим изобретением

из сервера 20 через канал 30 связи в клиентское устройство 10 передается значение 50 запроса, содержащее параметр 52 проекции;

для записи редуцированных биометрических данных 56 с использованием проекции, использующей параметр 52 проекции, используется модуль 18a получения биометрических данных, соединенный с клиентским устройством 10;

для передачи редуцированных биометрических данных 56 в сервер 20 через канал 30 связи используется клиентское устройство 10;

для идентификации пользователя клиентского устройства 10 используется сервер 20;

с использованием проекции, содержащей параметр 52 проекции, из биометрического образа 45a пользователя формируются проверочные данные 56" редуцированного биометрического образа, и путем сравнения редуцированных биометрических данных 56 с проверочными данными 56" редуцированного биометрического образа осуществляется аутентификация.

В предпочтительном варианте осуществления пользователь идентифицируется на основании редуцированных биометрических данных 56.

Поскольку вышеуказанные шаги можно найти на фиг. 5 и 6, данный способ аутентификации отдельно не иллюстрируется. В основе данного способа аутентификации лежит клиент-серверная архитектура получения биометрических данных, в которой значение запроса, переданное сервером, используется модулем получения биометрических данных, соединенным с клиентом или являющимся частью клиента, для записи редуцированных биометрических данных.

Указанным модулем получения биометрических данных может быть, например, планшетное устройство или сотовый телефон (смартфон) с исполняемой на этих устройствах программой, т.е. модуль получения биометрических данных встроен в клиентское устройство. Указанным сервером может быть, например, центральная служба, выполненная с возможностью идентификации пользователя на основании набора биометрических данных, записанных устройством, и на доступ к определенным службам в зависимости от результата идентификации. Указанный набор биометрических данных может образовываться, например, рукописной подписью на сенсорном экране, изображением радужной оболочки глаза, полученным камерой устройства, отпечатком пальца, записанным устройством (если устройство имеет необходимую для этого техническую возможность), или движениями частей тела, распознавание которых выполняется камерой устройства. В данном варианте осуществления редукцию рационально выполнять программой, работающей на планшете.

Устройством для получения биометрических данных может быть "планшет для подписывания" (графический планшет с пером, и, возможно, собственным дисплеем - в сущности, такое же планшетное устройство), подключенный к компьютеру через разъем USB. В данном случае указанным сервером даже может быть тот компьютер, на котором исполняется прикладная программа, предназначенная для работы с записанными данными рукописной подписи. Конечно, и в этом случае может использоваться удаленный сервер, тогда компьютер передает данные в этот сервер через канал связи. В данном варианте осуществления лучше всего выполнять операцию редукции данных прямо внутри этого "планшета для подписывания", поскольку в этом случае полный набор биометрических данных не покинет пределов физически ограниченного и защищенного устройства.

Указанным модулем получения биометрических данных может быть и простая компьютерная мышь, подключенная к компьютеру. С помощью прикладной программы могут записываться движения мыши, выполняемые пользователем во время просмотра страниц в интернете. Движения мыши/руки могут рассматриваться в качестве биометрических данных, характерных для данного человека. На основании записанных таким образом данных также могут быть получены психологические характеристики пользователя, которые могут использоваться даже для отображения специально подобранной для этого пользователя рекламы. Как вариант, камера, подключенная к компьютеру, может использоваться для записи в качестве биометрических данных движений глаз пользователя. В этих примерах редукцию данных лучше всего выполнять прикладной программой, исполняемой на указанном компьютере.

В особом случае с планшета для подписывания во время акта подписывания может выполняться получение информации двух типов:

редуцированного набора биометрических данных (который позднее будет использоваться сервером для идентификации человека);

статического изображения подписи (которое может быть визуально скопировано в документ, но само по себе непригодно для воспроизведения набора биометрических данных этой подписи).

Вышеуказанный способ является предпочтительным, поскольку при этом из устройства невозможно получить критически важные биометрические данные (лишь редуцированный набор информации, необходимый для идентификации), но изображение подписи, тем не менее, может быть создано. В данном случае значение запроса может содержать

параметр (или множество параметров), определяющий редукцию, требуемую для идентификации

человека; и

еще один параметр, определяющий редукцию динамических биометрических данных к статическим данным (т.е. на практике параметры времени и силы надавливания удаляются из исходного набора данных, а из оставшейся серии точек формируется изображение, которое, предпочтительно, преобразуется к заранее определенному размеру).

В данном случае редуцированный набор биометрических данных представляет собой объединение редуцированной информации двух типов, и эти две части используются сервером двумя различными способами.

Данный способ аутентификации, основанный на редуцированном наборе биометрических данных, имеет преимущество, состоящее в возможности выполнения личной идентификации органами/службами, которые

по закону не имеют права обладать полными биометрическими данными; или

не обладают уровнем защищенности, позволяющим защитить идентификационную информацию человека; или

не являются достаточно доверенными, как поставщики услуг, для людей, подлежащих идентификации.

Способ аутентификации в соответствии с настоящим изобретением также применим для построения анонимной системы идентификации, поскольку биометрические данные, представляющие интерес для хищения, не хранятся в клиенте и не передаются внутри системы. В предпочтительном варианте осуществления в магазинах и коридорах торговой галереи может быть установлено множество камер. Эта система камер может собирать редуцированную информацию, относящуюся к форме/движению лица/тела отдельных людей, и передавать в сервер только эту редуцированную информацию. На основании этой редуцированной информации сервер пытается распознать человека. Человек, которого не удалось распознать, идентифицируется как новый клиент, и соответствующий биометрический образец (редуцированные данные) сохраняется совместно с соответствующим идентификационным номером. Затем система отслеживает перемещение этого человека в торговой галерее (в какие магазины он заходит, у витрин каких магазинов останавливается, сколько времени проводит в определенных местах, в каком ресторане обедает, какие товары покупает - эти названные последними данные могут быть получены с использованием камеры на кассе и информации из кассы), иными словами, система обладает возможностью определения клиентских привычек и предпочтений. На основании клиентских предпочтений ранее распознанных и идентифицированных людей система может отображать персонализированную рекламу в любом месте (например, на динамической телевизионной стене). Такая система распознавания/идентификации дает возможность делать людям, входящим в магазин, персональные предложения по продаже.

Должно быть совершенно понятно, что специалист сможет представить себе технические решения, представляющие собой варианты, альтернативные подробно изложенным выше вариантам осуществления настоящего изобретения, и эти варианты входят в объем защиты, определяемый нижеприведенной формулой изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ цифрового подписания электронного файла, характеризующийся выполнением сервером следующих шагов:

формирование значения (50) запроса, содержащего уникальный параметр (52) проекции, причем уникальный параметр (52) проекции формируют для конкретного акта подписания;

передачу значения (50) запроса в клиентское устройство (10) через канал (30) связи;

прием из клиентского устройства (10) через канал (30) связи доказательной записи (70), электронного файла (48), который должен быть подписан, и биометрических данных (54) пользователя, причем доказательная запись (70) подтверждает, что электронный файл (48) и биометрические данные (54) происходят из данного клиентского устройства (10), при этом доказательная запись (70) сформирована клиентским устройством (10) путем связывания

значения (50) запроса,

хэша (58), полученного путем выполнения операции хэширования сформированных редуцированных биометрических данных (56), причем редуцированные биометрические данные (56) сформированы из биометрических данных (54), применяя проекцию, использующую параметр (52) проекции, так что параметр (52) проекции обеспечивает уникальность редуцированных биометрических данных (56) для каждой подписи, причем проекция представляет собой редукцию данных, формирующую редуцированные данные, которые не могут быть использованы для восстановления исходных данных и формирование которых возможно только обладая исходными данными и параметром проекции, и

хэша (49) электронного файла (48);

формирование из биометрических данных (54) редуцированных биометрических проверочных данных (56'), применяя проекцию, использующую параметр (52) проекции;

формирование хэша (58') редуцированных биометрических проверочных данных (56');

формирование хэша (49) электронного файла (48);

формирование проверочной доказательной записи (70') путем связывания значения (50) запроса, хэша (58') редуцированных биометрических проверочных данных (56') и хэша (49) электронного файла (48) и сравнение проверочной доказательной записи (70') с доказательной записью (70), переданной клиентским устройством (10), при этом процесс цифрового подписания продолжают только в том случае, если проверочная доказательная запись (70') идентична доказательной записи (70), переданной клиентским устройством (10);

идентификация пользователя клиентского устройства (10) на основании данных (74) пользователя, доступных для сервера (20), причем меньшей мере один элемент данных (74) пользователя используют на следующем шаге;

формирование сертификата (80) сервера путем связывания, по меньшей мере, хэша (49) электронного файла (48), указанного по меньшей мере одного элемента данных (74) пользователя и данных (78) подписи, относящихся, по меньшей мере, ко времени указанной подписи;

подписание сертификата (80) сервера, применяя секретный ключ (41) подписания сервера, тем самым формируя подписанный сертификат (82) сервера;

формирование цифровой подписи (85) путем связывания, по меньшей мере, подписанного сертификата (82) сервера и хэша (49) электронного файла (48); и

связывание цифровой подписи (85) с электронным файлом (48), тем самым формируя подписанный цифровой подписью электронный файл (86).

2. Способ по п.1, отличающийся тем, что осуществляют подписание подписанного цифровой подписью электронного файла (86) от имени пользователя, предпочтительно с использованием секретного ключа (42) подписания пользователя.

3. Способ по п.1 или 2, отличающийся тем, что осуществляют формирование визуально представимых биометрических данных (54a) из биометрических данных (54) посредством однонаправленного отображения, причем визуально представимые биометрические данные (54a) связаны с сертификатом (80) сервера и с хэшем (49) электронного файла (48) для формирования цифровой подписи (85).

4. Способ по любому из пп.1-3, отличающийся тем, что аутентификацию пользователя выполняют на основании биометрических данных (54).

5. Способ по п.4, отличающийся тем, что при аутентификации биометрические данные (54) сравнивают с биометрическим образом (45a).

6. Способ по любому из пп.1-5, отличающийся тем, что осуществляют прием биометрических данных (64) и/или электронного файла (68), зашифрованных клиентским устройством (10), в качестве биометрических данных (54) и/или в качестве электронного файла (48) и осуществляют расшифровку зашифрованных биометрических данных (64) и/или зашифрованного электронного файла (68) перед формированием редуцированных биометрических данных (56).

7. Способ по п.6, отличающийся тем, что осуществляют прием зашифрованных биометрических данных (64) и/или зашифрованного электронного файла (68), зашифрованных с использованием открытого ключа (40a) шифрования сервера, и осуществляют их расшифровку с использованием секретного ключа (40b) шифрования сервера или осуществляют прием зашифрованных биометрических данных (64) и/или зашифрованного электронного файла, зашифрованных с использованием открытого ключа (40a) шифрования сервера, и осуществляют расшифровку зашифрованного симметричного ключа с использованием секретного ключа (40b) шифрования сервера и последующую расшифровку зашифрованных биометрических данных (64) и/или электронного файла (68) с использованием указанного симметричного ключа.

8. Способ по любому из пп.1-7, отличающийся тем, что осуществляют формирование доказательной записи (90) сервера путем связывания, по меньшей мере, значения (50) запроса, биометрических данных (54) и хэша (49) электронного файла (48), подписание доказательной записи (90) сервера, предпочтительно с использованием секретного ключа (41) подписания сервера, и сохранение получившейся в результате подписанной доказательной записи (92) сервера.

9. Способ по любому из пп.1-8, отличающийся тем, что запись биометрических данных (54) пользователя осуществляют посредством модуля (18a) получения биометрических данных, и клиентское устройство (10) выполняет следующие операции:

формирование редуцированных биометрических данных (56) из биометрических данных (54), применяя проекцию, использующую параметр (52) проекции;

формирование хэша (58) редуцированных биометрических данных (56);

формирование хэша (49) электронного файла (48);

формирование доказательной записи (70) путем связывания, по меньшей мере, значения (50) запроса, хэша (58) редуцированных биометрических данных (56) и хэша (49) электронного файла (48);

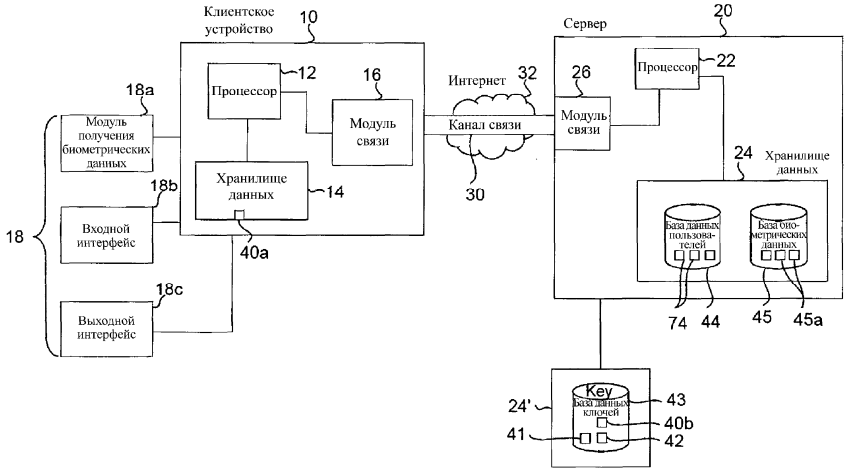
передача доказательной записи (70), электронного файла (48), который должен быть подписан, и биометрических данных (54) в сервер (20) через канал (30) связи.

10. Способ по п.9, отличающийся тем, что осуществляют подписание доказательной записи (70)

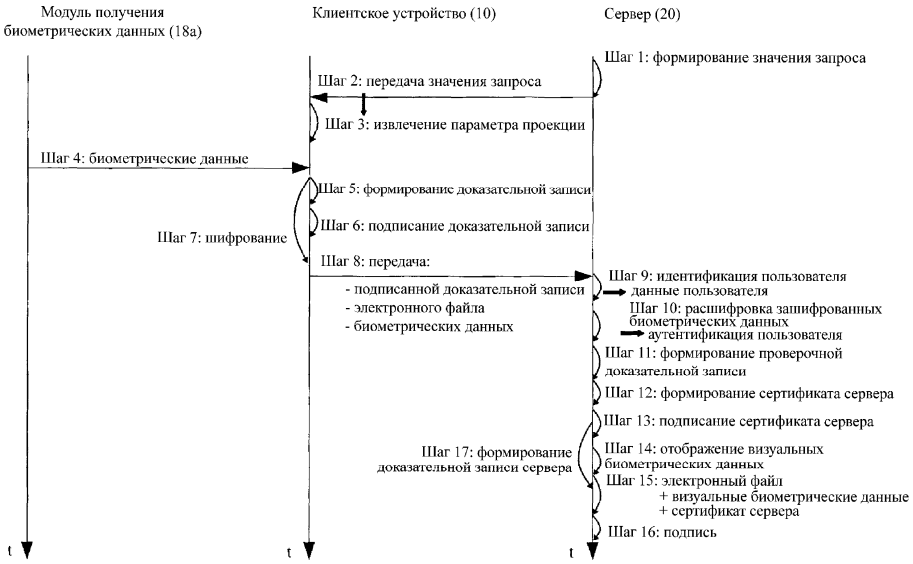
клиентским устройством (10) и проверку указанной подписи сервером (20).

11. Способ по п.9 или 10, отличающийся тем, что осуществляют шифрование биометрических данных (54) и/или электронного файла (48), который должен быть подписан, клиентским устройством (10) до передачи биометрических данных (54) и/или электронного файла (48), который должен быть подписан.

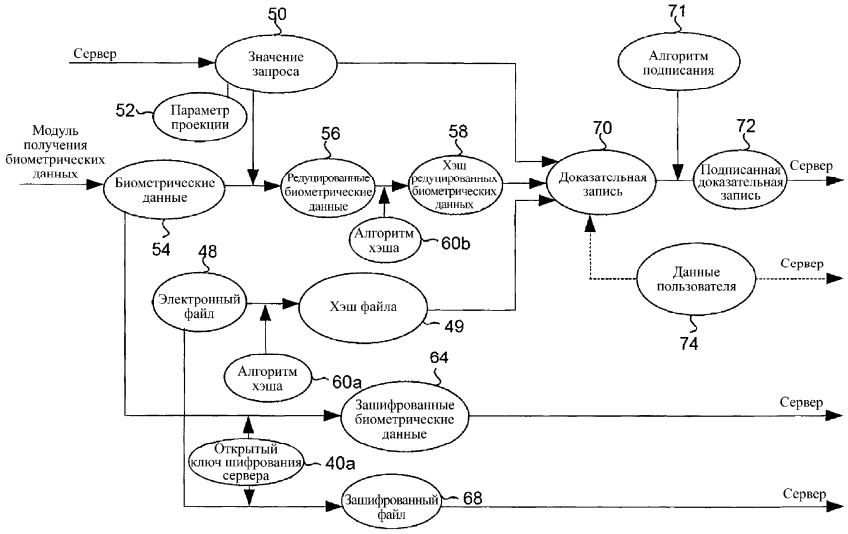
12. Способ по любому из пп.9-11, отличающийся тем, что модулем (18a) получения биометрических данных является графический планшет, при этом происходит прием и запись рукописной подписи в качестве биометрических данных (54), предпочтительно в качестве по меньшей мере одного типа биометрических данных (54), выбранного из следующей группы: координаты места нажатия пишущего устройства, координаты места подъема пишущего устройства, зависимость координат пишущего устройства от времени, зависимость скорости пишущего устройства от времени, зависимость ускорения пишущего устройства от времени, зависимость силы надавливания пишущего устройства от времени.



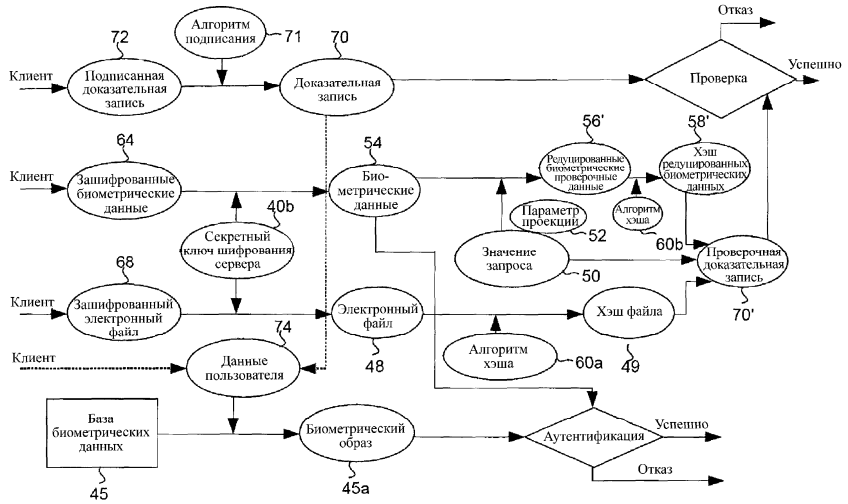
Фиг. 1



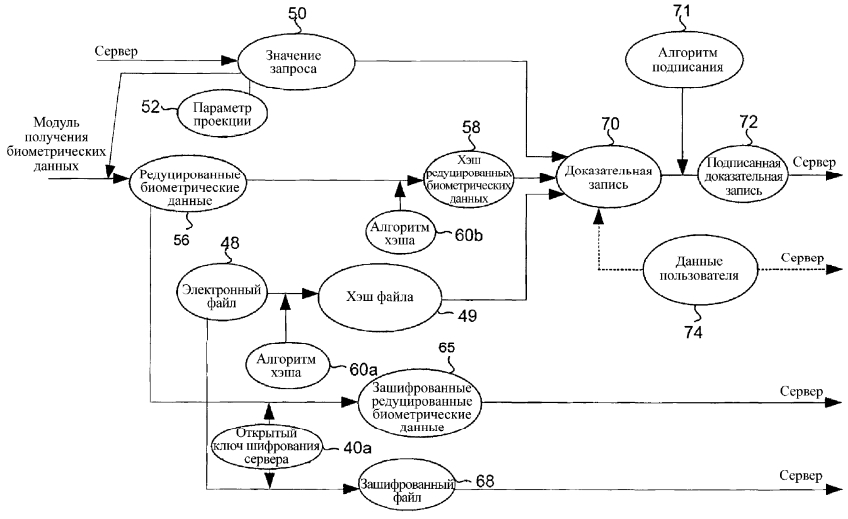
Фиг. 2



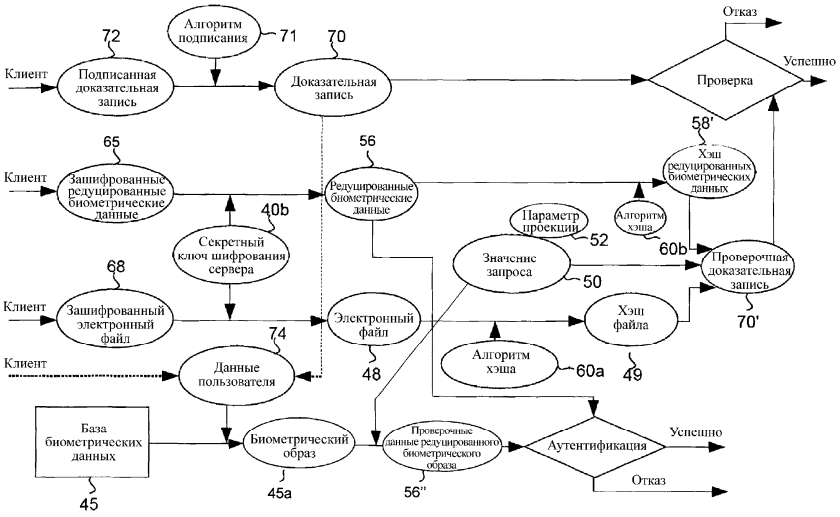
Фиг. 3



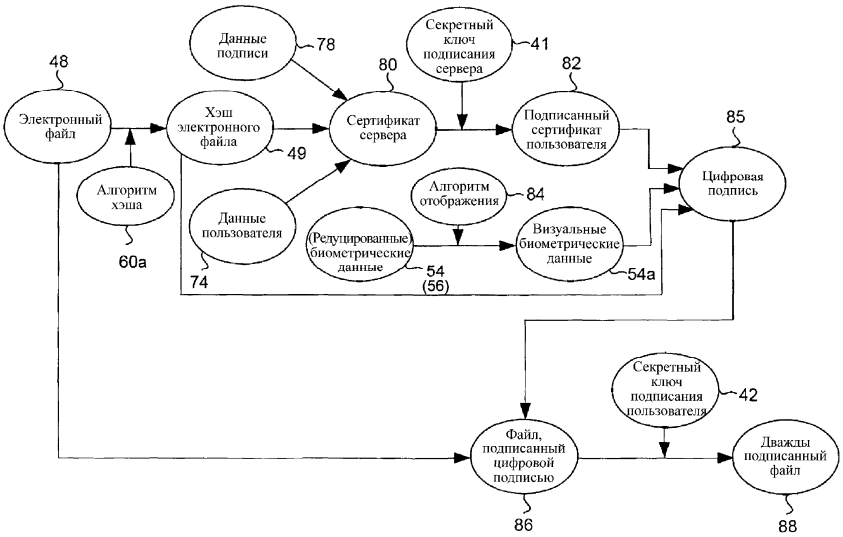
Фиг. 4



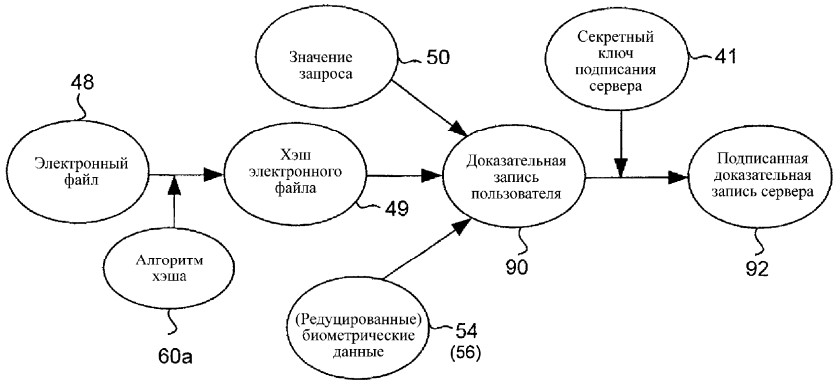
Фиг. 5



Фиг. 6



Фиг. 7



Фиг. 8