(19) Евразийское патентное ведомство

(21) 202490626 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2024.04.15

(22) Дата подачи заявки
2022.08.31

(51) Int. Cl. ***H04L 9/32*** (2006.01)
G06F 21/12 (2013.01)
G06F 21/45 (2013.01)
H04L 9/40 (2022.01)
H04L 9/00 (2022.01)

(54) СПОСОБ И СИСТЕМА ДЛЯ ПРОВЕРКИ ДОСТОВЕРНОСТИ ЦИФРОВОГО СОДЕРЖИМОГО

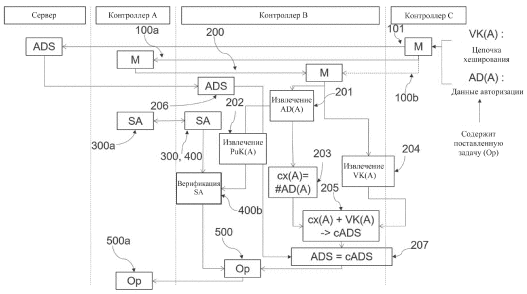
(31) **21194289.1**
(32) **2021.09.01**
(33) **EP**
(86) **PCT/EP2022/074262**
(87) **WO 2023/031310 2023.03.09**

(71) Заявитель:
СИКПА ХОЛДИНГ СА (CH)

(72) Изобретатель:
Тевоз Филипп (CH), Жилле Филипп (FR)

(74) Представитель:
Абильманова К.С. (KZ)

(57) Настоящее изобретение относится к области техники проверки достоверности и аутентификации цифровых данных, таких как, например, цифровой документ. В частности, настоящее изобретение относится к области техники проверки достоверности цифрового содержимого цифрового сообщения, такого как операция, сертифицированная объектом, который позволяет контроллеру выполнять указанную операцию.



202490626 A1

202490626 A1

СПОСОБ И СИСТЕМА ДЛЯ ПРОВЕРКИ ДОСТОВЕРНОСТИ ЦИФРОВОГО СОДЕРЖИМОГО

Область техники, к которой относится изобретение

[001] Настоящее изобретение относится к области техники проверки достоверности и аутентификации цифровых данных, таких как, например, цифровой документ. В частности, настоящее изобретение относится к области техники проверки достоверности цифрового содержимого цифрового сообщения, такого как операция, сертифицированная объектом, который позволяет контроллеру выполнять указанную операцию.

Предпосылки создания изобретения

[002] Проблема подделки и фальсификации цифровых данных хорошо известна и растет с каждым днем. Что касается промышленной сферы, то цифровизация некоторых процессов обычно очень подвержена кибератакам. Когда компьютер общается с другим компьютером, существующего протокола безопасности едва достаточно для защиты от хакерских технологий. Кроме того, существует так много отраслей, так много протоколов для взаимодействия компьютеров друг с другом, что известные решения этих проблем очень трудно реализовать, они стоят больших денег и их необходимо адаптировать в зависимости от каждой ситуации. Таким образом, существует острая необходимость в решении, обеспечивающем целостность процесса в недоверенной среде, например, когда нескольким устройствам приходится обмениваться данными или, например, выполнять санкционированную задачу.

[003] Поэтому сейчас как никогда важно иметь возможность проверять достоверность и аутентифицировать с высокой степенью безопасности цифровые данные или оператора, представляющего такой цифровой документ, содержащий такие цифровые данные. В то же время обязательно найти недорогое решение, которое можно легко и быстро реализовать.

[004] Действительно, как сегодня компьютер, робот или даже гражданин может с уверенностью идентифицировать, что оператор или должностное лицо, подписавшее в цифровом виде цифровой документ, имеет законное право подписывать и проверять достоверность такого документа от имени уполномоченного органа, который он представляет?

[005] В более общем смысле, как компьютер или робот может быть уверен, что компьютер или робот, стоящий за этой цифровой подписью, является правильным и что этот объект уполномочен подписывать такой документ от имени своей организации?

[006] Подводя итог, как объект может доверять данным с цифровой подписью и объекту, который их подписал?

[007] В физическом мире уверенность в бумажном документе дает подпись и особенно штамп или печать уполномоченного органа, выдавшего документ. Необходимо перенести эту ситуацию в цифровой мир.

[008] В цифровом мире главным образом используется цифровая подпись, сертифицированная цепочкой сертификатов. Например, специалист в данной области техники знает решения для защиты цифровых файлов от подделки, такие как решение, описанное в документе US 2021/258168 A1. Однако этому решению не хватает безопасности, и оно не гарантирует с высокой степенью уверенности, что подписавшее лицо имело полномочия и право подписывать в эту конкретную дату от имени уполномоченного органа, который представляет данный тип документа.

[009] Таким образом, цель изобретения состоит в том, чтобы с большей уверенностью проверить достоверность цифровых данных или цифрового документа и, следовательно, обеспечить аутентификацию оператора, представляющего эти цифровые данные или этот цифровой документ получателю.

Краткое описание сущности изобретения

[010] Согласно одному аспекту настоящее изобретение относится к способу проверки достоверности цифрового содержимого цифрового сообщения M, предпочтительно в виде защищенного от подделки цифрового файла, принятого устройством DB, управляемым контроллером B, по сети связи CN, при этом:

- устройство DA, управляемое контроллером A, содержит блок обработки CPU(A) с памятью, хранящей цифровое сообщение M, и модуль связи CM(A), выполненный с возможностью отправки и приема данных по сети связи CN;

- устройство DB, содержащее блок обработки CPU(B) с памятью, хранящей агрегированную цифровую подпись ADS, и модуль связи CM(B), выполненный с возможностью отправки и приема данных по сети связи CN, причем, предпочтительно, указанную агрегированную цифровую подпись ADS вычисляют путем применения одностороннего сумматора к множеству цифровых подписей, причем указанное множество цифровых подписей включает цифровую подпись x(A) данных авторизации AD(A), вычисленную с помощью односторонней функции;

- цифровое сообщение M содержит данные авторизации AD(A), указывающие на то, что контроллер A устройства DA уполномочен контроллером C осуществлять операцию Op с контроллером, устройство которого принимает указанное цифровое сообщение M; предпочтительно, цифровое сообщение M сертифицировано контроллером C;

- цифровое сообщение M также содержит ключ верификации VK(A), приписанный контроллером C, при этом указанный ключ верификации VK(A) вместе с данными авторизации AD(A) позволяют извлекать агрегированную цифровую подпись ADS, хранящуюся в памяти блока обработки CPU(B) устройства DB, предпочтительно, указанный ключ верификации VK(A) вместе с данными авторизации AD(A) используют для вычисления потенциальной агрегированной цифровой подписи cADS, причем блок обработки CPU(B)

выполнен с возможностью сравнения указанной потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, хранящейся в памяти блока обработки CPU(B) устройства DB;

способ включает следующие этапы, на которых:

- модуль связи CM(B) устройства DB принимает цифровое сообщение M; предпочтительно, модуль связи CM(B) устройства DB принимает цифровое сообщение M от модуль связи CM(A), и/или от контроллера C, и/или от сервера, содержащего, например, базу данных;

- предпочтительно, блок обработки CPU(B) устройства DB верифицирует то, что цифровое сообщение M сертифицировано контроллером C; и

- блок обработки CPU(B) устройства DB извлекает данные авторизации AD(A), содержащиеся в цифровом сообщении M, предпочтительно только в случае положительной верификации того, что цифровое сообщение M сертифицировано контроллером C;

- модуль связи CM(B) устройства DB принимает от модуля связи CM(A) устройства DA аккредитацию SA;

- блок обработки CPU(B) устройства DB верифицирует аккредитацию SA;

- блок обработки CPU(B) устройства DB:

- извлекает ключ верификации VK(A), содержащийся в цифровом сообщении M,

- вычисляет с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A), и

- вычисляет потенциальную агрегированную цифровую подпись cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

- блок обработки CPU(B) устройства DB проверяет, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся в его памяти, и только в случае положительной верификации данных аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) устройства DB передает посредством модуля связи CM(B) контроллеру B указание о том, что контроллер A действительно уполномочен контроллером C осуществлять операцию Op.

[011] Настоящее изобретение позволяет получателю проверять достоверность заданного цифрового содержимого с большей уверенностью, чем решения предшествующего уровня техники. Действительно, настоящее изобретение позволяет контроллеру B проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники.

[012] Более того, настоящее изобретение позволяет устройству DB управлять учетными данными, связанными с этим цифровым содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет.

[013] Настоящее изобретение позволяет контроллеру B проверять достоверность заданного цифрового содержимого на основе открытого ключа контроллера A без необходимости идентификации контроллера A.

[014] Согласно этой системе для контроллера A и контроллера B нет необходимости сверяться с контроллером C или иметь доступ к базе данных контроллера C, чтобы контроллер B мог проверять достоверность цифрового содержимого цифрового сообщения M, до тех пор, пока контроллер B содержит агрегированную цифровую подпись ADS.

[015] Согласно варианту осуществления память блока обработки CPU(A) устройства DA хранит закрытый ключ PrK(A), предпочтительно, в защищенном

анклаве памяти блока обработки CPU(A), причем блок обработки CPU(A) выполнен с возможностью подписывания данных с помощью закрытого ключа PrK(A); и блок обработки CPU(B) устройства DB выполнен с возможностью верификации подписанных данных с помощью соответствующего открытого ключа модулем связи CM(B); и цифровое сообщение M дополнительно содержит открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) и аккредитованный контроллером C как принадлежащий контроллеру A; и аккредитация SA представляет собой данные аккредитации, подписанные с помощью закрытого ключа PrK(A); и перед этапом верификации указанной аккредитации SA блоком обработки CPU(B) устройства DB, блок обработки CPU(B) устройства DB извлекает открытый ключ PuK(A) из цифрового сообщения M; и этап верификации указанной аккредитации SA включает верификацию аккредитации SA блоком обработки CPU(B) устройства DB с использованием указанного открытого ключа PuK(A).

[016] Это позволяет контроллеру B верифицировать то, что контроллер A, подписавший данные аккредитации, действительно является тем же контроллером A, который упомянут в цифровом сообщении M.

[017] Согласно варианту осуществления цифровое сообщение M сертифицировано контроллером C, и указанный способ включает, перед этапом извлечения блоком обработки CPU(B) устройства DB данных авторизации AD(A), содержащихся в цифровом сообщении M, этап верификации блоком обработки CPU(B) того, что цифровое сообщение M сертифицировано контроллером C, и только в случае положительной верификации того, что цифровое сообщение M сертифицировано контроллером C, блок обработки CPU(B) устройства DB извлекает данные авторизации AD(A), содержащиеся в цифровом сообщении M.

[018] Это позволяет верифицировать то, что цифровое сообщение M было надлежащим образом выдано контроллером C. Согласно примеру этап верификации блоком обработки CPU(B) того, что цифровое сообщение M

сертифицировано контроллером C, можно выполнять с использованием, например, криптографического процесса или криптографической подписи.

[019] Согласно другому аспекту настоящее изобретение относится к системе для проверки достоверности цифрового содержимого цифрового сообщения M, принятого устройством DB, управляемым контроллером B, по сети связи CN, причем система содержит:

- устройство DA, управляемое контроллером A и содержащее блок обработки CPU(A) с памятью, хранящей цифровое сообщение M, и модуль связи CM(A), выполненный с возможностью отправки и приема данных по сети связи CN;

- устройство DB, содержащее блок обработки CPU(B) с памятью, хранящей агрегированную цифровую подпись ADS, и модуль связи CM(B), выполненный с возможностью отправки и приема данных по сети связи CN, причем указанная агрегированная цифровая подпись ADS вычислена путем применения одностороннего сумматора к множеству цифровых подписей, причем указанное множество цифровых подписей включает цифровую подпись x(A) данных авторизации AD(A), вычисленную с помощью односторонней функции;

- цифровое сообщение M содержит данные авторизации AD(A), указывающие на то, что контроллер A устройства DA уполномочен контроллером C осуществлять операцию Op с контроллером, устройство которого принимает указанное цифровое сообщение M, предпочтительно, цифровое сообщение M сертифицировано контроллером C;

- цифровое сообщение M также содержит ключ верификации VK(A), приписанный контроллером C, при этом указанный ключ верификации VK(A) вместе с данными авторизации AD(A) позволяют извлекать агрегированную цифровую подпись ADS, хранящуюся в памяти блока обработки CPU(B) устройства DB, предпочтительно, указанный ключ верификации VK(A) вместе с данными авторизации AD(A) использованы для вычисления потенциальной

агрегированной цифровой подписи cADS, причем блок обработки CPU(B) выполнен с возможностью сравнения указанной потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, хранящейся в памяти блока обработки CPU(B) устройства DB;

и при этом:

- модуль связи CM(B) устройства DB выполнен с возможностью приема цифрового сообщения M; предпочтительно, модуль связи CM(B) устройства DB выполнен с возможностью приема цифрового сообщения M от модуля связи CM(A), и/или от контроллера C, и/или от сервера, содержащего, например, базу данных;

- предпочтительно, блок обработки CPU(B) устройства DB выполнен с возможностью верификации того, что цифровое сообщение M сертифицировано контроллером C; и

- блок обработки CPU(B) устройства DB выполнен с возможностью извлечения данных авторизации AD(A), содержащихся в цифровом сообщении M, предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано контроллером C;

- модуль связи CM(B) устройства DB выполнен с возможностью приема от модуля связи CM(A) устройства DA аккредитации SA;

- блок обработки CPU(B) устройства DB выполнен с возможностью верификации аккредитации SA;

- блок обработки CPU(B) устройства DB выполнен с возможностью:

- извлечения ключа верификации VK(A), содержащегося в цифровом сообщении M,

- вычисления с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальной цифровой подписи cx(A) данных авторизации AD(A), и

- вычисления потенциальной агрегированной цифровой подписи cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

○ блок обработки CPU(B) устройства DB выполнен с возможностью проверки того, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся в его памяти, и только в случае положительной верификации данных аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) устройства DB выполнен с возможностью передачи посредством модуля связи CM(B) контроллеру B указания о том, что контроллер A действительно уполномочен контроллером C осуществлять операцию Op.

[020] Настоящее изобретение позволяет, например, контроллеру A, такому как, например, робот, идентифицировать себя только с помощью аккредитации SA и своих учетных данных, причем указанные учетные данные содержатся в цифровом сообщении M и сертифицированы защищенным от подделки цифровым файлом, выданным контроллером C. Преимущественно, цифровое сообщение M содержит или представляет собой защищенный от подделки цифровой файл, выданный контроллером C. Контроллер B, такой как, например другой робот, может быть полностью уверен в достоверности представленных учетных данных.

[021] Следует отметить, что настоящее изобретение позволяет избежать использования биометрических данных в том случае, когда контроллером A является, например, человек. Его учетных данных и аккредитации SA достаточно, чтобы предоставить полную уверенность получателю, в данном случае контроллеру B, которым может быть, например, робот, компьютер или

другой человек. Преимущественно, настоящее изобретение позволяет избежать каких-либо биометрических данных, биометрического измерения или раскрытия частной информации.

[022] Согласно варианту осуществления настоящего изобретения контроллер A может иметь закрытый ключ и может использовать его в отношении указанной аккредитации SA, чтобы идентифицировать себя, например, посредством запроса на связь. Указанный закрытый ключ связан с открытым ключом. Преимущественно, контроллер C, который выдал защищенный от подделки цифровой файл, предпочтительно, сертифицировал указанный открытый ключ, позволяя получателю, то есть контроллеру B, проверять достоверность указанной аккредитации SA.

[023] Более того, получатель, т. е. контроллер B, может хранить защищенный от подделки цифровой файл, т. е. цифровое сообщение M, и использовать его для связи и запроса его эмитента, т. е. контроллера C, для идентификации контроллера A в случае возникновения каких-либо проблем, таких как жалоба на действия контроллера и/или любой производственный инцидент. Однако, контроллер A может оставаться анонимным для получателя, и только эмитент защищенного от подделки цифрового файла может его идентифицировать.

[024] Согласно другому аспекту настоящее изобретение относится к применению системы для проверки достоверности цифрового содержимого цифрового сообщения M согласно настоящему изобретению для проверки достоверности устройством DB выполнения операции Op, причем указанная операция Op осуществляется устройством DA, и где:

- устройство DB содержится в хранилище B и управляется им, устройство DA содержится в роботе A и управляется им, и операция Op относится к выборке роботом A конкретного товара, расположенного внутри хранилища B; или

- устройство DB содержится в компьютере B и управляется им, устройство DA содержится в смартфоне A и управляется им, и операция Op относится к отправке смартфоном A набора данных SeD(A) на компьютер B; или

- устройство DB содержится в медицинском устройстве B и управляется им, устройство DA содержится у медсестры A и управляется ею, и операция Op относится к введению медсестрой A конкретного лекарственного средства конкретному пациенту с использованием указанного медицинского устройства B; или

- устройство DB содержится у гражданина B и управляется им, устройство DA содержится у сотрудника полиции A и управляется им, и операция Op относится к проникновению сотрудника полиции A в дом гражданина B для поиска доказательств; или

- устройство DB содержится у гражданина B и управляется им, устройство DA содержится у государственного служащего A и управляется им, и операция Op относится к выдаче и подписыванию государственным служащим официального цифрового документа.

[025] Прежде чем приводить далее подробный обзор вариантов осуществления настоящего изобретения, ниже будут перечислены некоторые необязательные характеристики, которые могут использоваться совместно или альтернативно.

[026] Согласно примеру память блока обработки CPU(A) устройства DA хранит закрытый ключ PrK(A), предпочтительно, в защищенном анклаве памяти блока обработки CPU(A), причем блок обработки CPU(A) выполнен с возможностью подписывания данных с помощью закрытого ключа PrK(A).

[027] Согласно примеру блок обработки CPU(B) устройства DB выполнен с возможностью верификации подписанных данных с помощью соответствующего открытого ключа модулем связи CM(B).

[028] Согласно примеру цифровое сообщение M дополнительно содержит открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) и аккредитованный контроллером C как принадлежащий контроллеру A.

[029] Согласно примеру аккредитация SA представляет собой данные аккредитации, подписанные с помощью закрытого ключа PrK(A).

[030] Согласно примеру перед этапом верификации указанной аккредитации SA блоком обработки CPU(B) устройства DB, блок обработки CPU(B) устройства DB извлекает открытый ключ PuK(A) из цифрового сообщения M.

[031] Согласно примеру этап верификации указанной аккредитации SA включает верификацию аккредитации SA блоком обработки CPU(B) устройства DB с использованием указанного открытого ключа PuK(A).

[032] Согласно примеру сеть связи CN включает сеть связи ближнего радиуса действия NFCN.

[033] Согласно примеру модуль связи CM(A) выполнен с возможностью отправки и приема данных по сети связи ближнего радиуса действия NFCN, модуль связи CM(B) выполнен с возможностью отправки и приема данных по сети связи ближнего радиуса действия NFCN, предпочтительно, эта сеть связи ближнего радиуса действия NFCN обеспечивает связь между модулем связи CM(A) и модулем связи CM(B), когда расстояние между модулем связи CM(A) и модулем связи CM(B) составляет менее 50 см, предпочтительно менее 25 см, и преимущественно менее 10 см.

[034] Согласно примеру устройство DA содержит модуль отображения DD(A) и модуль оптического считывания OR(A), устройство DB содержит модуль отображения DD(B) и модуль оптического считывания OR(B).

[035] Согласно примеру этап приема цифрового сообщения M модулем связи CM(B) устройства DB включает этап считывания модулем оптического считывания OR(B) оптического считываемого представления блока графических

данных GDB, отображаемого модулем отображения DD(A), причем указанный блок графических данных GDB содержит цифровую метку DM.

[036] Согласно примеру указанная цифровая метка DM включает закодированную версию EAD(A) указанных данных авторизации AD(A) и закодированную версию EVK(A) указанного ключа верификации VK(A).

[037] Согласно примеру извлечение данных авторизации AD(A) включает декодирование указанных закодированных данных авторизации EAD(A).

[038] Согласно примеру извлечение ключа верификации VK(A) включает декодирование указанного закодированного ключа верификации EVK(A).

[039] Согласно примеру указанное оптическое считываемое представление блока графических данных GDB включает цифровое представление графических символов из заданного конечного набора графических символов, причем указанное цифровое представление графического символа выполнено с возможностью кодирования указанной цифровой метки MD и блока машиночитаемых данных с исправлением ошибок.

[040] Согласно примеру память устройства DB хранит закрытый ключ PrK(B), предпочтительно, в защищенном анклаве памяти блока обработки CPU(B), и соответствующий открытый ключ PuK(B), аккредитованный контроллером C как принадлежащий контроллеру B, причем блок обработки CPU(B) устройства DB выполнен с возможностью подписывания данных с помощью указанного закрытого ключа PrK(B).

[041] Согласно примеру блок обработки CPU(A) устройства DA выполнен с возможностью верификации подписанных данных с использованием соответствующего открытого ключа модулем связи CM(A).

[042] Согласно примеру способ включает, перед этапом приема модулем связи CM(B) от модуля связи CM(A) аккредитации SA, этап отправки от модуля связи CM(B) на модуль связи CM(A) секрета, сгенерированного устройством DB,

предпочтительно, в заданный момент времени, причем указанный секрет выполнен с возможностью генерирования указанной аккредитации SA.

[043] Согласно примеру указанный секрет выполнен с возможностью быть подписанным с помощью закрытого ключа PrK(A) блоком обработки CPU(A) для генерирования указанной аккредитации SA.

[044] Согласно примеру указанный этап отправки указанного секрета включает этап отображения модулем отображения DD(B) оптического считываемого представления графического элемента, кодирующего указанный секрет и выполненного с возможностью быть считанным модулем оптического считывания OR(A).

[045] Согласно примеру перед или после приема цифрового сообщения M, контроллер B принимает цифровой документ.

[046] Согласно примеру аккредитация SA включает подпись содержимого указанного цифрового документа, причем указанная подпись генерируется блоком обработки CPU(A) путем подписывания с помощью закрытого ключа PrK(A) указанного содержимого, предпочтительно, аккредитация SA включает подпись хеш-значения по меньшей мере части содержимого указанного цифрового документа, причем указанная подпись генерируется блоком обработки CPU(A) с использованием закрытого ключа PrK(A), и указанное хеш-значение вычисляется с помощью односторонней функции, запрограммированной в блоке обработки CPU(A).

[047] Согласно примеру цифровое сообщение M сертифицировано контроллером C.

[048] Согласно примеру способ включает, перед этапом извлечения блоком обработки CPU(B) устройства DB данных авторизации AD(A), содержащихся в цифровом сообщении M, этап верификации блоком обработки CPU(B) того, что цифровое сообщение M сертифицировано контроллером C, и только в случае положительной верификации того, что цифровое сообщение M

сертифицировано контроллером C, блок обработки CPU(B) устройства DB извлекает данные авторизации AD(A), содержащиеся в цифровом сообщении M.

[049] Согласно примеру память блока обработки CPU(A) устройства DA выполнена с возможностью хранения закрытого ключа PrK(A), предпочтительно, в защищенном анклаве памяти блока обработки CPU(A), причем блок обработки CPU(A) выполнен с возможностью подписывания данных с помощью закрытого ключа PrK(A).

[050] Согласно примеру блок обработки CPU(B) устройства DB выполнен с возможностью верификации подписанных данных с помощью соответствующего открытого ключа модулем связи CM(B).

[051] Согласно примеру цифровое сообщение M дополнительно содержит открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) и аккредитованный контроллером C как принадлежащий контроллеру A.

[052] Согласно примеру аккредитация SA представляет собой данные аккредитации, подписанные с помощью закрытого ключа PrK(A).

[053] Согласно примеру блок обработки CPU(B) устройства DB выполнен с возможностью извлечения открытого ключа PuK(A) из цифрового сообщения M.

[054] Согласно примеру блок обработки CPU(B) устройства DB выполнен с возможностью верификации указанной аккредитации SA с использованием указанного открытого ключа PuK(A).

[055] Согласно примеру устройство DB содержит модуль генерирования секрета SGM(B), выполненный с возможностью генерирования секрета, предпочтительно, в заданный момент времени, причем указанный секрет выполнен с возможностью быть отправленным модулем связи CM(B) устройства DB на модуль связи CM(A) устройства DA.

[056] Согласно примеру блок обработки CPU(A) устройства DA выполнен с возможностью генерирования указанной аккредитации SA с использованием указанного секрета.

[057] Согласно примеру блок обработки CPU(A) устройства DA выполнен с возможностью подписывания указанного секрета с помощью закрытого ключа PrK(A) для генерирования указанной аккредитации SA.

[058] Согласно примеру устройство DA содержит модуль отображения DD(A) и модуль оптического считывания OR(A), устройство DB содержит модуль отображения DD(B) и модуль оптического считывания OR(B).

[059] Согласно примеру модуль отображения DD(A) устройства DA выполнен с возможностью отображения оптического считываемого представления блока графических данных GDB.

[060] Согласно примеру модуль оптического считывания OR(B) устройства DB выполнен с возможностью считывания указанного оптического считываемого представления блока графических данных GDB, причем указанный блок графических данных GDB содержит цифровую метку DM.

[061] Согласно примеру указанная цифровая метка DM включает закодированную версию EAD(A) указанных данных авторизации AD(A) и закодированную версию EVK(A) указанного ключа верификации VK(A).

[062] Согласно примеру блок обработки CPU(B) устройства DB выполнен с возможностью извлечения данных авторизации AD(A) путем декодирования указанных закодированных данных авторизации EAD(A).

[063] Согласно примеру блок обработки CPU(B) устройства DB выполнен с возможностью извлечения ключа верификации VK(A) путем декодирования указанного закодированного ключа верификации EVK(A).

[064] Согласно примеру устройство DB содержится в хранилище B и управляется им, устройство DA содержится в роботе A и управляется им, и

операция Op относится к выборке роботом A конкретного товара, расположенного внутри хранилища B.

[065] Согласно примеру устройство DB содержится в компьютере B и управляется им, устройство DA содержится в смартфоне A и управляется им, и операция Op относится к отправке смартфоном A набора данных SeD(A) на компьютер B.

[066] Согласно примеру устройство DB содержится в медицинском устройстве B и управляется им, устройство DA содержится у медсестры A и управляется ею, и операция Op относится к введению медсестрой A конкретного лекарственного средства конкретному пациенту с использованием указанного медицинского устройства B.

[067] Согласно примеру устройство DB содержится у гражданина B и управляется им, устройство DA содержится у сотрудника полиции A и управляется им, и операция Op относится к проникновению сотрудника полиции A в дом гражданина B для поиска доказательств.

[068] Согласно примеру устройство DB содержится у гражданина B и управляется им, устройство DA содержится у государственного служащего A и управляется им, и операция Op относится к выдаче и подписыванию государственным служащим A официального цифрового документа.

[069] Согласно примеру ключ верификации VK выполнен с возможностью вычисления по меньшей мере одной потенциальной агрегированной цифровой подписи cADS с использованием потенциальной цифровой подписи cx данных авторизации AD, причем указанная потенциальная цифровая подпись cx данных авторизации AD вычисляется с использованием односторонней функции, запрограммированной в блоке обработки CPU(B), причем указанный блок обработки CPU(B) выполнен с возможностью сравнения указанной потенциальной агрегированной цифровой подписи cADS с агрегированной

цифровой подписью ADS, хранящейся в памяти блока обработки CPU(B) устройства DB.

[070] Согласно примеру ключ верификации включает последовательность значений цифровых подписей, упорядоченных согласно структуре данных, соответствующей дереву, причем эти значения цифровых подписей соответствуют значениям узлов и значениям листьев указанного дерева.

[071] Согласно примеру потенциальную агрегированную цифровую подпись cADS можно вычислять с использованием ключа верификации VK, включающего последовательность значений узлов, соответствующих значениям цифровых подписей, и с использованием вычисленной потенциальной цифровой подписи cx данных авторизации AD, причем указанная вычисленная потенциальная цифровая подпись cx вычисляется с использованием односторонней функции, запрограммированной в блоке обработки CPU(B).

[072] Согласно примеру ключ верификации VK включает последовательность значений узлов, упорядоченных согласно структуре дерева, причем указанные значения узлов соответствуют значениям цифровых подписей, и вычисленная потенциальная цифровая подпись cx данных авторизации AD вычисляется с использованием односторонней функции, запрограммированной в блоке обработки CPU(B), и вычисление потенциальной агрегированной цифровой подписи cADS включает следующие этапы:

a. извлечение из последовательности значений узлов в ключе верификации VK значения (т. е. значения цифровой подписи) каждого другого листового узла дерева, имеющего такой же родительский узел, что и у заданного листового узла, соответствующего вычисленной потенциальной цифровой подписи cx данных авторизации AD, и вычисление цифровой подписи конкатенации заданного значения узла и, соответственно, согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, извлеченного значения указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла заданного листового узла;

b. последовательно на каждом следующем уровне в дереве и до предпоследнего уровня узлов:

c. извлечение из последовательности значений узлов в ключе верификации VK значения (т. е. значения цифровой подписи) каждого другого узла, отличного от листового, дерева, имеющего такой же родительский узел, что и у предыдущего такого же родительского узла, рассмотренного на предшествующем этапе, и

d. вычисление цифровой подписи конкатенации значения указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, тем самым получая значение указанного такого же родительского узла указанного предыдущего такого же родительского узла; и

e. вычисление цифровой подписи конкатенации полученных значений узлов, отличных от листовых, соответствующих предпоследнему уровню узлов дерева согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, тем самым получая корневую цифровую подпись корневого узла дерева, причем указанная корневая цифровая подпись соответствует потенциальной агрегированной цифровой подписи cADS.

Краткое описание чертежей

[073] Цели, задачи, а также технические признаки и преимущества настоящего изобретения будут лучше понятны из подробного описания варианта осуществления настоящего изобретения, который иллюстрируется следующими фигурами, на которых:

- на фиг. 1 представлен общий схематический вид варианта осуществления настоящего изобретения.

- На фиг. 2 представлен схематический вид варианта осуществления настоящего изобретения согласно первому случаю применения.

- На фиг. 3 представлен схематический вид варианта осуществления настоящего изобретения согласно второму случаю применения.

- На фиг. 4 представлен схематический вид варианта осуществления настоящего изобретения согласно третьему случаю применения.

- На фиг. 5 представлен схематический вид варианта осуществления настоящего изобретения согласно четвертому случаю применения.

- На фиг. 6 представлен схематический вид варианта осуществления настоящего изобретения согласно пятому случаю применения.

- На фиг. 7 представлено схематическое изображение способа защиты содержимого цифрового сообщения согласно варианту осуществления настоящего изобретения.

- На фиг. 8 представлен схематический вид устройства DA и устройства DB согласно варианту осуществления настоящего изобретения.

[074] Чертежи даны в качестве примера и не ограничивают настоящее изобретение. Они изображают представления принципа, предназначенные для облегчения понимания настоящего изобретения, и не обязательно соответствуют масштабу практического применения.

Подробное описание

[075] Настоящее изобретение в данном случае подробно описано со ссылкой на неограничивающие варианты осуществления, проиллюстрированные на чертежах.

[076] Настоящее изобретение относится к системе и способу проверки достоверности цифрового содержимого цифрового сообщения M. Как описано в настоящем документе далее, преимущественно, цифровое сообщение M

представляет собой защищенный от подделки цифровой файл. В одном варианте осуществления указанное цифровое сообщение M может быть сгенерировано, например, из нецифрового сообщения, такого как рукописное сообщение или напечатанное сообщение, предпочтительно, используя преобразование рукописного сообщения в цифровое сообщение и/или напечатанного сообщения в цифровое сообщение, с использованием, например, сканера и/или камеры.

[077] Согласно варианту осуществления указанное цифровое сообщение M может содержать несколько видов данных, таких как учетные данные устройства или контроллера, поставленную задачу контроллера для осуществления операции Op, данные в отношении уполномоченного органа, доставившего указанные учетные данные, и т. д.

[078] Согласно предпочтительному варианту осуществления цифровое сообщение M содержит данные авторизации AD. Указанные данные авторизации AD выполнены с возможностью указания того, что контроллер устройства уполномочен другим контроллером осуществлять операцию Op, предпочтительно, с другим контроллером, устройство которого приняло указанное цифровое сообщение M. Предпочтительно, цифровое сообщение M может также содержать цифровую метку DM, описанную в настоящем документе далее. В более общем смысле это цифровое сообщение M может принимать любую форму, такую как графическое представление, набор данных, электромагнитную волну и т. д.

[079] Например, цифровое сообщение M может содержать данные авторизации AD(A), указывающие на то, что контроллер A устройство DA уполномочен контроллером C осуществлять операцию Op с контроллером B. Такой операцией Op может быть, например, загрузка данных, выгрузка данных, доступ к базе данных, передача команд, сбор данных, сбор товаров, доставка данных, доставка товаров и т. д., больше примеров будет описано в настоящем документе далее. Указанный контроллер C может быть уполномоченным органом, представленным устройством, учреждением или человеком. Указанный

уполномоченный орган имеет возможность уполномочить контроллера выполнять некоторые операции в отношении другого контроллера. Предпочтительно, контроллер C выполнен с возможностью доставки цифрового сообщения M в виде защищенного от подделки цифрового файла. Преимущественно, цифровое сообщение M сертифицировано контроллером C.

[080] Например, это цифровое сообщение M принимается устройством по сети связи CN. Это устройство управляется контроллером. Указанное устройство выполнено с возможностью проверки достоверности цифрового содержимого указанного цифрового сообщения M.

[081] Согласно варианту осуществления указанная сеть связи CN может включать сеть связи ближнего радиуса действия NFCN. Указанная сеть связи ближнего радиуса действия NFCN выполнена с возможностью обеспечения связи между по меньшей мере двумя устройствами, когда расстояние между ними составляет менее 50 см, предпочтительно менее 25 см, и преимущественно менее 10 см. Эта сеть связи может включать проводную связь и/или беспроводную связь. Эта сеть связи может включать сеть оптической связи.

[082] Согласно варианту осуществления настоящего изобретения контроллером может быть компьютер, робот, устройство интернета вещей (IoT), часть устройства, транспортное средство, пользователь и/или человек. Действительно, устройством может быть часть более крупного устройства, такого как, например, модуль внутри робота, и/или внутри смартфона, или внутри любой системы, которую может использовать человек. Этим устройством, например, является одно из следующих устройств: мобильный телефон, планшет, персональный компьютер, робот, устройство IoT и т. д.

[083] Указанное устройство содержит по меньшей мере блок обработки с памятью. Указанный блок обработки содержит по меньшей мере один процессор, выполненный с возможностью выполнения по меньшей мере одного ряда команд, предпочтительно, хранящихся в памяти. Предпочтительно, указанная память является постоянной памятью. Преимущественно, указанная

память содержит защищенный анклав, предпочтительно, выполненный с возможностью хранения, например, по меньшей мере одного закрытого ключа.

[084] Согласно варианту осуществления цифровое сообщение M содержит ключ верификации VK(A), приписанный контроллером C, причем указанный ключ верификации VK(A) вместе с данными авторизации AD(A) позволяет извлекать агрегированную цифровую подпись ADS.

[085] Согласно варианту осуществления указанный ключ верификации VK(A) представляет собой последовательность множества цифровых подписей x. Это множество цифровых подписей x можно сгенерировать с помощью нескольких хорошо известных механизмов, таких как использование дерева Меркла. При использовании этого последнего механизма, указанный ключ верификации VK(A) представляет собой последовательность множества цифровых подписей x, начиная от уровня листовых узлов до предпоследнего уровня узлов, каждого другого листового узла, имеющего такой же родительский узел в дереве, что и листовой узел, соответствующий подписи цифрового файла x(A) указанных данных авторизации AD(A), и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский узел в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне. Более подробная информация будет описана в настоящем документе далее в разделе «защищенный от подделки цифровой файл».

[086] Согласно варианту осуществления агрегированную цифровую подпись ADS, преимущественно, вычисляют путем применения одностороннего сумматора к множеству цифровых подписей, причем указанное множество цифровых подписей включает цифровую подпись x(A) данных авторизации AD(A). Указанную цифровую подпись x(A) данных авторизации AD(A) предпочтительно вычисляют с помощью односторонней функции. Как описано в настоящем документе далее, указанная агрегированная цифровая подпись ADS

предназначена для хранения в памяти устройства, принимающего указанное цифровое сообщение M.

[087] Согласно варианту осуществления настоящее изобретение может предусматривать этапы верификации того, что цифровое сообщение надлежащим образом сертифицировано контроллером C. Предпочтительно, этот этап верификации можно осуществлять контроллером A и/или контроллером B.

[088] Согласно варианту осуществления настоящее изобретение может предусматривать этап отправки запроса на связь между контроллером B и контроллером A. Действительно, чтобы проверить достоверность контроллера A, т. е. чтобы аутентифицировать, что контроллер A действительно является контроллером, упомянутым в цифровом сообщении M, контроллер B может использовать запрос на связь. Этот запрос на связь можно реализовать разными способами. Предпочтительно, этот запрос на связь включает прием контроллером B аккредитации SA от контроллера A, затем контроллер B может верифицировать аккредитацию SA, чтобы достоверно проверить, что контроллер A действительно является контроллером, упомянутым в цифровом сообщении M. Более подробная информация об этом этапе отправки запроса на связь представлена в настоящем документе далее.

[089] Согласно варианту осуществления, проиллюстрированному на фиг. 8, настоящее изобретение предусматривает прием контроллером B, предпочтительно, модулем связи CM(B) устройства DB, аккредитации SA от контроллера A, предпочтительно, от модуля связи CM(A) устройства DA. Эта аккредитация SA предназначена для верификации контроллером B, преимущественно, блоком обработки CPU(B) устройства DB. Предпочтительно, эта аккредитация SA включает данные, подписанные контроллером A. Согласно варианту осуществления аккредитация SA генерируется из секрета. Предпочтительно, указанный секрет генерируется контроллером B и/или контроллером C. Указанный секрет принимается контроллером A,

предпочтительно, модулем связи CM(A) устройства DA, от контроллера C и/или от контроллера B, предпочтительно, от модуля связи CM(B) устройства DB.

[090] Более того, согласно варианту осуществления цифровое сообщение M может содержать открытый ключ PuK, соответствующий закрытому ключу PrK, причем указанный открытый ключ PuK аккредитован контроллером C как принадлежащий контроллеру A. Следовательно, согласно варианту осуществления этап отправки запроса на связь можно инициировать между контроллером B и контроллером A, например, посредством обмена данными с использованием устройства DB и устройства DA и этих открытого и закрытого ключей, например, открытого ключа PuK(A) и соответствующего закрытого ключа PrK(A).

[091] Согласно варианту осуществления контроллер A содержит закрытый ключ PrK(A). Как, например, в традиционной инфраструктуре открытых ключей PKI, указанный закрытый ключ PrK(A) хранится в секрете контроллером A. Указанный закрытый ключ PrK(A) имеет связанный с ним открытый ключ PuK(A), предназначенный для публичной известности; указанный открытый ключ PuK(A) предназначен для отправки в другой контроллер, например, в контроллер B посредством модуля связи CM(B) устройства DB. Указанный открытый ключ PuK(A) аккредитован контроллером C. Действительно, контроллер C, уполномоченный орган, аккредитовал этот открытый ключ PuK(A) как принадлежащий контроллеру A.

[092] При использовании этого закрытого ключа PrK(A), устройство DA может подписывать данные, а затем отправлять эти подписанные данные, например, на устройство DB. С помощью открытого ключа PuK(A) устройство DB может верифицировать указанные подписанные данные.

[093] Согласно варианту осуществления устройство DB может отправлять сообщение на устройство DA, это сообщение может содержать, например, секрет, часто называемый запросом на связь, предпочтительно, одноразовый секрет, предпочтительно, сгенерированный на лету, т. е. в заданный момент

времени, и содержащий, например, случайное число. Затем устройство DA может подписывать с помощью своего закрытого ключа PrK(A) это сообщение или по меньшей мере, например, указанный секрет, и отправлять подписанное сообщение на устройство DB в виде аккредитации SA. Преимущественно, указанная аккредитация SA включает указанный подписанный секрет. Устройство DB может верифицировать указанную аккредитацию SA, т. е. указанное подписанное сообщение, с использованием соответствующего открытого ключа PuK(A) и сообщения, т. е. секрета, в частности, например, случайного числа. Этот запрос на связь позволяет устройству DB, а значит и контроллеру B, верифицировать то, что это действительно устройство DA, принадлежащее контроллеру A, который находится на связи с ним, предпочтительно, в указанный заданный момент времени.

[094] Согласно варианту осуществления аккредитация SA может включать подпись документа и указанный документ. Предпочтительно, указанная подпись генерируется блоком обработки CPU(A) путем подписывания указанного документа с помощью закрытого ключа PrK(A).

[095] Согласно варианту осуществления блок обработки CPU(A) устройства DA может быть выполнен с возможностью верификации подписанных данных, принятых вместе с соответствующим открытым ключом PuK модулем связи CM(A), например, от устройства DB. Действительно, поскольку у контроллера A есть закрытый ключ PrK(A), аккредитованный уполномоченным органом как принадлежащий контроллеру A, например, контроллером C, и связанный с ним открытый ключ PuK(A), у контроллера B также может быть закрытый ключ PrK(B), связанный с открытым ключом PuK(B). Предпочтительно, указанный открытый ключ PuK(B) аккредитован уполномоченным органом как принадлежащий контроллеру B, предпочтительно, тем же уполномоченным органом, как, например, контроллер C.

[096] Что касается устройства DA в отношении закрытого ключа PrK(A), память устройства DB хранит закрытый ключ PrK(B), предпочтительно, в защищенном

анклаве памяти, причем блок обработки CPU(B) выполнен с возможностью подписывания данных с помощью указанного закрытого ключа PrK(B).

[097] Согласно предпочтительному варианту осуществления каждый модуль связи CM содержит модуль отображения DD и модуль оптического считывания OR. Указанный модуль отображения DD выполнен с возможностью отображения оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB. Указанный блок графических данных GDB может включать часть или все цифровое сообщение M. Например, блок графических данных GDB может содержать цифровую метку DM.

[098] Согласно варианту осуществления указанная цифровая метка DM может включать закодированную версию EAD указанных данных авторизации AD. Согласно другому варианту осуществления цифровая метка DM может включать закодированную версию EVK ключа верификации VK. Согласно этим вариантам осуществления, чтобы получить данные авторизации AD(A), например, контроллера A, устройство DB должно декодировать закодированные данные авторизации EAD(A). Таким же образом, чтобы получить ключ верификации VK(A), например, контроллера A, устройство DB должно декодировать закодированный ключ верификации EVK(A). Согласно этим вариантам осуществления цифровое сообщение M может быть прикреплено к цифровому документу и/или может быть оптически принято в виде оптического считываемого представления блока графических данных GDB устройством DB, предпочтительно, модулем связи CM(B) устройства DB, преимущественно, модулем оптического считывания OR(B) модуля связи CM(B) устройства DB. Согласно этим вариантам осуществления цифровое сообщение M может оптически отображаться модулем отображения DD(A) модуля связи CM(A) устройства DA, или цифровое сообщение M отправляется по сети связи CN, или даже печатается, предпочтительно, в виде указанного блока графических данных GDB.

[099] Согласно примеру указанное оптическое считываемое представление блока графических данных GDB может содержать цифровое представление графических символов из заданного конечного набора графических символов, такого как, например, QR-код. Указанное цифровое представление графического символа выполнено с возможностью кодирования указанной цифровой метки MD и, предпочтительно, блока машиночитаемых данных с исправлением ошибок. Эти особенности описаны более подробно в настоящем документе далее.

[0100] Согласно конкретному варианту осуществления секрет, отправленный от устройства DB на устройство DA, можно отправлять через этап отображения графического представления указанного секрета модулем отображения DD(B) модуля связи CM(B) устройства DB и этап считывания указанного графического представления модулем оптического считывания OR(A) модуля связи (CMA) устройства DA. Затем, после подписания этого секрета и, следовательно, генерирования указанной аккредитации SA, устройство DA может отображать графическое представление аккредитации SA с использованием своего модуля отображения DD(A). Затем устройство DB считывает графическое представление аккредитации SA с использованием своего модуля оптического считывания OR(B).

[0101] Согласно варианту осуществления настоящее изобретение относится к системе для проверки достоверности цифрового содержимого цифрового сообщения M, принятого устройством DB, управляемым контроллером B, по сети связи CN.

[0102] Согласно варианту осуществления эта система предпочтительно содержит:

- устройство DA, управляемое контроллером A. Как указано ранее, устройство DA содержит блок обработки CPU(A) с памятью, хранящей цифровое сообщение M, и модуль связи CM(A), выполненный с возможностью отправки и приема данных по сети связи CN.

- устройство DB, управляемое контроллером B. Как указано ранее, устройство DB содержит блок обработки CPU(B) с памятью, хранящей указанную агрегированную цифровую подпись ADS, и модуль связи CM(B), выполненный с возможностью отправки и приема данных по сети связи CN. Преимущественно, блок обработки CPU(B) устройства DB выполнен с возможностью верификации подписанных данных с помощью соответствующего открытого ключа. Предпочтительно, его память хранит ранее раскрытую агрегированную цифровую подпись ADS.

[0103] Эта система выполнена таким образом, что:

- модуль связи CM(B) устройства DB выполнен с возможностью приема цифрового сообщения M;

- предпочтительно, цифровое сообщение M сертифицировано контроллером C, и преимущественно, блок обработки CPU(B) устройства DB выполнен с возможностью верификации того, что цифровое сообщение M сертифицировано контроллером C; и

- блок обработки CPU(B) устройства DB выполнен с возможностью извлечения данных авторизации AD(A), содержащихся в цифровом сообщении M, предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано контроллером C;

- модуль связи CM(B) устройства DB выполнен с возможностью приема от модуля связи CM(A) устройства DA аккредитации SA, предпочтительно, подписанной блоком обработки CPU(A) устройства DA с использованием своего закрытого ключа PrK(A), и/или содержащей данные, такие как секрет, подписанный блоком обработки CPU(A) устройства DA с использованием своего закрытого ключа PrK(A); предпочтительно, указанный секрет был принят модулем связи CM(A) устройства DA от устройства DB и/или от контроллера C;

- блок обработки CPU(B) устройства DB выполнен с возможностью верификации аккредитации SA, предпочтительно, с использованием открытого

ключа PuK(A), соответствующего указанному закрытому ключу PrK(A), преимущественно, после извлечения указанного открытого ключа PuK(A) из цифрового сообщения M;

- блок обработки CPU(B) устройства DB выполнен с возможностью:

- извлечения ключа верификации VK(A), содержащегося в сообщении M,

- вычисления с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальной цифровой подписи cx(A) данных авторизации AD(A), и

- вычисления потенциальной агрегированной цифровой подписи cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

- блок обработки CPU(B) устройства DB выполнен с возможностью проверки того, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся в его памяти, и только в случае положительной верификации аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) устройства DB выполнен с возможностью передачи посредством модуля связи CM(B) контроллеру B указания о том, что контроллер A действительно уполномочен контроллером C осуществлять операцию Op.

[0104] Эта система позволяет контроллеру B проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники. Более того, эта система позволяет устройству DB управлять учетными данными, связанными с этим цифровым содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет. Эта система позволяет контроллеру A, такому как, например, робот, идентифицировать себя только с помощью аккредитации SA и своих учетных данных, которые содержатся в цифровом сообщении M и которые

сертифицированы защищенным от подделки цифровым файлом, выданным контроллером C. Эта система позволяет контроллеру B, такому как, например, другой робот, быть полностью уверенным в достоверности представленных учетных данных.

[0105] Следует отметить, что эта система позволяет избежать использования биометрических данных в том случае, когда контроллером A является, например, человек, как будет раскрыто в настоящем документе далее. Его учетных данных и аккредитации SA достаточно, чтобы предоставить полную уверенность получателю, в данном случае контроллеру B, которым может быть, например, робот, компьютер или другой человек. Преимущественно, эта система позволяет избежать каких-либо биометрических данных, биометрического измерения или раскрытия частной информации.

[0106] Согласно варианту осуществления память блока обработки CPU(A) устройства DA выполнена с возможностью хранения указанного закрытого ключа PrK(A), предпочтительно, в защищенном анклаве памяти, причем блок обработки CPU(A) выполнен с возможностью подписывания данных с помощью закрытого ключа PrK(A).

[0107] Согласно варианту осуществления блок обработки CPU(B) устройства DB выполнен с возможностью верификации подписанных данных с помощью соответствующего открытого ключа PuK, предпочтительно, принятого модулем связи CM(B).

[0108] Согласно варианту осуществления цифровое сообщение M дополнительно содержит указанный открытый ключ PuK(A), соответствующий указанному закрытому ключу PrK(A), причем указанный открытый ключ PuK(A) аккредитован контроллером C.

[0109] Согласно варианту осуществления аккредитация SA включает данные аккредитации, подписанные с помощью указанного закрытого ключа PrK(A).

[0110] Согласно варианту осуществления блок обработки CPU(B) устройства DB выполнен с возможностью извлечения открытого ключа PuK(A) из цифрового сообщения M и верификации указанной аккредитации SA с использованием указанного открытого ключа PuK(A).

[0111] Согласно варианту осуществления, проиллюстрированному на фиг. 1, эта система выполнена с возможностью выполнения способа проверки достоверности цифрового содержимого цифрового сообщения M, принятого устройством DB, управляемым контроллером B, по сети связи CN. Предпочтительно, этот способ включает следующие этапы, на которых:

- модуль связи CM(B) устройства DB принимает 200, 100b цифровое сообщение M; указанное цифровое сообщение M может быть принято модулем связи CM(B) устройства DB от контроллера C 100b или от модуля связи CM(A) устройства DA 200; предпочтительно, контроллер C отправляет 100a цифровое сообщение M на модуль связи CM(A) устройства DA;

- предпочтительно, цифровое сообщение M сертифицировано 10 контроллером C, и преимущественно, блок обработки CPU(B) устройства DB верифицирует то, что цифровое сообщение M сертифицировано 10 контроллером C; и

- блок обработки CPU(B) устройства DB извлекает 201 данные авторизации AD(A), содержащиеся в цифровом сообщении M, предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано 10 контроллером C; как указано ранее, это цифровое сообщение M может исходить из напечатанного сообщения и/или рукописного сообщения, становясь цифровым сообщением после преобразования, например, с использованием сканера и/или камеры;

- модуль связи CM(B) устройства DB принимает 400 от модуля связи CM(A) устройства DA аккредитацию SA, предпочтительно, подписанную с помощью закрытого ключа PrK(A);

○ блок обработки CPU(B) устройства DB верифицирует 400b аккредитацию SA, предпочтительно, с использованием открытого ключа PuK(A), преимущественно, после извлечения 202 указанного открытого ключа PuK(A) из цифрового сообщения M;

○ блок обработки CPU(B) устройства DB:

- извлекает 204 ключ верификации VK(A), содержащийся в цифровом сообщении M,

- вычисляет 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A), и

- вычисляет 205 потенциальную агрегированную цифровую подпись cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

○ блок обработки CPU(B) устройства DB проверяет 207, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся в его памяти, указанная агрегированная цифровая подпись ADS могла быть выгружена 101 контроллером C на сервер и загружена 206 из указанного сервера, например, устройством DB, и только в случае положительной верификации данных аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) устройства DB передает 500 посредством модуля связи CM(B) контроллеру B указание о том, что контроллер A действительно уполномочен контроллером C осуществлять 500a операцию Op.

[0112] Этот способ позволяет контроллеру B проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники. Более того, этот способ позволяет устройству DB управлять учетными данными, связанными с этим цифровым

содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет. Этот способ позволяет контроллеру A, такому как, например, робот, идентифицировать себя только с помощью аккредитации SA и своих учетных данных, которые содержатся в цифровом сообщении M и которые сертифицированы защищенным от подделки цифровым файлом, выданным контроллером C. Этот способ позволяет контроллеру B, такому как, например, другой робот, быть полностью уверенным в достоверности представленных учетных данных.

[0113] Следует отметить, что этот способ позволяет избежать использования биометрических данных в том случае, когда контроллером A является, например, человек, как будет раскрыто в настоящем документе далее. Его учетных данных и аккредитации SA достаточно, чтобы предоставить полную уверенность получателю, в данном случае контроллеру B, которым может быть, например, робот, компьютер или другой человек. Преимущественно, этот способ позволяет избежать каких-либо биометрических данных, биометрического измерения или раскрытия частной информации.

[0114] Согласно варианту осуществления устройство DB посредством своего модуля связи CM(B) может принимать цифровое сообщение M разными способами. Например, цифровое сообщение M может быть принято от устройства A посредством своего модуля связи CM(A), и/или от контроллера C, и/или, например, от сервера.

[0115] Согласно варианту осуществления устройство DB, посредством своего модуля связи CM(B), может принимать цифровое сообщение M непосредственно в цифровом формате или сначала в бумажном формате, который преобразуется в цифровой формат. Например, модуль связи CM(B) может использовать модуль оптического считывания OR(B) для оптического считывания, т. е. сканирования, бумаги, содержащей напечатанное содержимое и/или рукописное содержимое, чтобы преобразовать указанное напечатанное содержимое и/или рукописное содержимое в цифровое сообщение M.

[0116] Согласно варианту осуществления сеть связи CN может включать сеть связи одного или нескольких видов, такую как сеть оптической связи, сеть проводной связи, сеть беспроводной связи, сеть радиочастотной связи и даже комбинацию нескольких видов сетей связи.

[0117] Согласно варианту осуществления, что касается приема цифрового сообщения M, открытый ключ PuK(A), соответствующий закрытому ключу PrK(A), принадлежащему контроллеру A, может быть принят контроллером B разными способами. Например, открытый ключ PuK(A) может быть принят, например, от контроллера C, и/или от сервера, и/или, преимущественно, из цифрового сообщения M. Действительно, в некоторых вариантах осуществления контроллер B может получить открытый ключ PuK(A) непосредственно из цифрового сообщения M с использованием блока обработки CPU(B) для извлечения его из цифрового сообщения M. Согласно другому варианту осуществления устройство DB может принимать посредством своего модуля связи CM(B) открытый ключ PuK(A) от контроллера C.

[0118] Один из способов описания настоящего изобретения согласно варианту осуществления заключается в следующем: поставленная задача в виде цифрового сообщения M, выполняемая контроллером A на благо контроллера B, выдана и сертифицирована контроллером C. Одна из основных целей настоящего изобретения состоит в том, чтобы дать указанному контроллеру B возможность убедиться в том, что указанная поставленная задача действительно является подлинной и выдана указанным контроллером C, и что указанный контроллер A имеет надлежащие полномочия от указанного контроллера C выполнять заданную поставленную задачу.

[0119] Согласно варианту осуществления контроллер B принимает цифровое сообщение M, соответствующее или содержащее указанную поставленную задачу от контроллера A и/или от контроллера C или через любой другой источник или маршрут. Затем контроллер B проверяет, что цифровое сообщение M, т. е. поставленная задача, действительно является достоверным, подлинным,

не подделанным и не сфальсифицированным, и что оно было надлежащим образом выдано контроллером C.

[0120] Согласно варианту осуществления контроллер B передает запрос на связь контроллеру A, предпочтительно, одноразовый запрос на связь. Затем, преимущественно, контроллер A подписывает запрос на связь с помощью своего закрытого ключа PrK(A) и отправляет обратно подписанный запрос на связь контроллеру B. Затем контроллер B проверяет, что подпись действительно является достоверной и, предпочтительно, что она надлежащим образом соответствует открытому ключу PuK(A), который, преимущественно, содержится в цифровом сообщении M, например, в поставленной задаче.

[0121] Затем согласно предпочтительному варианту осуществления, если обе верификации положительны, контроллер A может надлежащим образом выполнять поставленную задачу на благо контроллера B.

[0122] Согласно варианту осуществления контроллер A может быть выбран из робота, компьютера, устройства интернета вещей, смартфона или пользователя и т. д.

[0123] Как очевидно, настоящее изобретение может найти применение во многих областях техники. Чтобы проиллюстрировать некоторые виды технических применений, теперь будут раскрыты несколько примеров, проиллюстрированных на фиг. 2–7.

Роботы на охраняемом складе

[0124] Согласно первому примеру применения настоящего изобретения, проиллюстрированному на фиг. 2, настоящее изобретение можно реализовать для того, чтобы позволить роботу безопасно забирать ценные товары, такие как, например, золотые слитки или ювелирные изделия, внутри охраняемого склада.

[0125] Согласно этому примеру контроллер A представляет собой робот A, предназначенный для перемещения внутри охраняемого склада с целью сбора

и/или доставки товаров. Этот робот A содержит устройство DA. Предпочтительно, этот робот A оснащен моторизованным модулем, выполненным с возможностью перемещения робота A по меньшей мере внутри охраняемого склада. Следовательно, контроллер A может содержать колеса или гусеничную ленту или любые устройства, позволяющие ему перемещаться. Контроллер A может быть даже дроном, таким как, например, летающий дрон. Этот робот A выполнен с возможностью забирать товары из по меньшей мере одного хранилища на основании поставленной задачи, выданной логистическим центром C, который в этом случае применения является контроллером C. Контроллер A, т. е. робот A, содержит закрытый ключ PrK(A), предпочтительно, выданный контроллером A; указанный закрытый ключ PrK(A) связан с открытым ключом PuK(A), причем указанный открытый ключ PuK(A) сертифицирован контроллером C, т. е. логистическим центром C, как принадлежащий контроллеру A.

[0126] Согласно этому примеру контроллер B представляет собой хранилище B, предпочтительно, интеллектуальное хранилище, т. е. хранилище, содержащее устройство DB. Контроллер B также может быть механизированной дверью хранилища. Указанное хранилище B выполнено с возможностью доставки товаров или предоставления доступа роботу для получения товаров внутри хранилища B, если указанный робот имеет правильную поставленную задачу, выданную логистическим центром, выступающим в качестве контроллера C в этом примере.

[0127] Согласно этому примеру контроллером C является логистический центр C. Указанный логистический центр C выполнен с возможностью выдачи 100 поставленной задачи с использованием цифрового сообщения M, отправленного 100a контроллеру A. Согласно варианту осуществления цифровое сообщение M также отправляется 100b контроллеру B контроллером C. Например, цифровое сообщение M может содержать поставленную задачу в виде ряда данных, указывающих, например, что контроллер A должен сделать, когда контроллер A

должен это сделать и, например, где контроллер A должен это сделать. В этом примере поставленная задача может включать следующие данные:

- у робота A есть открытый ключ PuK(A);

- ключ верификации VK(A);

- операция Op: робот A должен выбрать конкретный товар, например, золотой слиток № 429, который находится внутри хранилища B;

- временной интервал: например, это необходимо сделать в промежутке времени с 10:25 до 10:30.

[0128] Согласно варианту осуществления, когда робот A, т. е. контроллер A, принимает цифровое сообщение M, он верифицирует 10a с использованием блока обработки CPU(A) то, что цифровое сообщение M сертифицировано 10 контроллером C, и только в случае положительной верификации того, что цифровое сообщение M сертифицировано 10 контроллером C, блок обработки CPU(A) устройства DA начинает извлечение данных авторизации AD(A), содержащихся в цифровом сообщении M. Предпочтительно, эти данные авторизации AD(A) включают данные поставленной задачи в отношении робота A.

[0129] Согласно предпочтительному варианту осуществления, когда хранилище B, т. е. контроллер B, принимает 200 цифровое сообщение M, оно верифицирует 10b с использованием блока обработки CPU(B) то, что цифровое сообщение M сертифицировано 10 контроллером C, и только в случае положительной верификации того, что цифровое сообщение M сертифицировано 10 контроллером C, блок обработки CPU(B) устройства DB начинает извлечение 201 данных авторизации AD(A), содержащихся в цифровом сообщении M. Предпочтительно, эти данные авторизации AD(A) включают данные поставленной задачи.

[0130] Затем контроллер B, т. е. хранилище B, извлекает 202, 204 из цифрового сообщения M разные данные, такие как открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) контроллера A, т. е. робота A, ключ верификации(A), данные, связанные с операцией Op, и, например, временной интервал, упомянутый в поставленной задаче.

[0131] Согласно варианту осуществления, когда контроллер A, т. е. робот A, находится перед контроллером B, т. е. хранилищем B, контроллер B отправляет 300 запрос на связь контроллеру A. Например, этот запрос на связь может быть случайным числом, сгенерированным модулем генерирования случайных чисел GRNM(B) устройства DB. Согласно варианту осуществления, когда контроллер A принимает указанный запрос на связь посредством своего устройства DA, преимущественно, посредством модуля связи CM(A) устройства DA, он подписывает 300a его с помощью своего закрытого ключа PrK(A), более конкретно, блок обработки CPU(A) устройства DA подписывает 300a запрос на связь с использованием закрытого ключа PrK(A), генерируя указанную аккредитацию SA. Затем контроллер A отправляет 400 обратно контроллеру B аккредитацию SA.

[0132] Затем контроллер B, т. е. хранилище B в этом примере, проверяет 400b достоверность аккредитации SA с использованием открытого ключа PuK(A), который был извлечен 202 блоком обработки CPU(B) из цифрового сообщения M, и, предпочтительно, который указан в поставленной задаче, т. е. данных авторизации AD(A).

[0133] Затем блок обработки CPU(B) устройства DB вычисляет 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A) и вычисляет 205 потенциальную агрегированную цифровую подпись cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и блок обработки CPU(B) устройства DB проверяет 207, совпадает ли потенциальная агрегированная цифровая подпись

cADS с агрегированной цифровой подписью ADS, хранящейся 206 в его памяти. Согласно варианту осуществления указанная агрегированная цифровая подпись ADS была принята контроллером B от контроллера C и/или от сервера. Затем указанная агрегированная цифровая подпись ADS была сохранена 206 в памяти блока обработки CPU(B) контроллера B, т. е. хранилища B в этом примере.

[0134] Согласно варианту осуществления хранилище B извлекает другие данные из цифрового сообщения M, такие как временной интервал, в течение которого должен работать робот A, как, например, с 10:25 до 10:30 в этом примере.

[0135] Затем, если на часах представлено время с 10:25 до 10:30, если верификация 400b аккредитации SA является положительной и если потенциальная агрегированная цифровая подпись cADS совпадает 207 с агрегированной цифровой подписью ADS, хранилище B, т. е. контроллер B, принимает 500 от своего блока обработки CPU(B) указание о том, что робот A действительно уполномочен логистическим центром C осуществлять 500a операцию Op, упомянутую в поставленной задаче, содержащейся в цифровом сообщении M. Следовательно, хранилище B доставляет роботу A золотой слиток № 429 или позволяет роботу A забирать золотой слиток № 429.

[0136] Согласно этому примеру случая применения настоящего изобретения система предпочтительно содержит:

- робот A, содержащий устройство DA и управляющий им, причем указанный робот A выполнен с возможностью перемещения по меньшей мере внутри охраняемого склада, причем указанный склад содержит логистический центр;

- хранилище B, содержащее устройство DB и управляющее им, причем указанное хранилище B выполнено с возможностью доставки товара санкционированному роботу и/или предоставления роботу возможности забрать товар, содержащийся в хранилище.

[0137] Эта система выполнена таким образом, что:

- модуль связи CM(B) устройства DB выполнен с возможностью приема 100b, 200 цифрового сообщения M, содержащего поставленную задачу, причем указанная поставленная задача содержит открытый ключ PuK(A), принадлежащий роботу A, данные авторизации AD(A), указывающие на то, что робот A уполномочен логистическим центром C осуществлять операцию Op с хранилищем B, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д.;

- предпочтительно, блок обработки CPU(B) устройства DB выполнен с возможностью верификации 10b того, что цифровое сообщение M сертифицировано логистическим центром C; и

- блок обработки CPU(B) устройства DB выполнен с возможностью извлечения 201, 202, 204 данных, содержащихся в цифровом сообщении M, таких как открытый ключ PuK(A), данные авторизации AD(A), операция Op, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано логистическим центром C;

- модуль связи CM(B) устройства DB выполнен с возможностью приема 400 от модуля связи CM(A) устройства DA аккредитации SA, предпочтительно, подписанной 300a блоком обработки CPU(A) устройства DA с использованием своего закрытого ключа PrK(A), и/или содержащей данные, такие как секрет, подписанные 300a блоком обработки CPU(A) устройства DA с использованием своего закрытого ключа PrK(A); предпочтительно, указанный секрет был отправлен 300 от модуля связи CM(B) устройства DB на модуль связи CM(A) устройства DA;

- блок обработки CPU(B) устройства DB выполнен с возможностью верификации 400b аккредитации SA, предпочтительно, с использованием открытого ключа PuK(A), соответствующего указанному закрытому ключу

PrK(A), преимущественно, после извлечения 202 указанного открытого ключа PuK(A) из цифрового сообщения M;

- блок обработки CPU(B) устройства DB выполнен с возможностью:

- вычисления 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальной цифровой подписи cx(A) данных авторизации AD(A), и

- вычисления 205 потенциальной агрегированной цифровой подписи cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

- блок обработки CPU(B) устройства DB выполнен с возможностью проверки 207 того, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся 206 в его памяти, и только в случае положительной верификации аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) устройства DB выполнен с возможностью передачи 500 в хранилище указания о том, что робот действительно уполномочен логистическим центром осуществлять 500a операцию Op.

[0138] Эта система позволяет устройству DB проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники. Более того, эта система позволяет устройству DB управлять поставленной задачей, т. е. учетными данными, связанными с этим цифровым содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет. Эта система позволяет роботу A идентифицировать себя только с помощью аккредитации SA и цифрового сообщения M, которое сертифицировано, предпочтительно, защищенным от подделки цифровым файлом, выданным контроллером C. Эта система позволяет

хранилищу B быть полностью уверенным в достоверности представленной поставленной задачи.

[0139] Согласно этому примеру случая применения настоящего изобретения согласно варианту осуществления настоящее изобретение относится к способу, в котором:

- робот A содержит устройство DA и управляет им, причем указанный робот A выполнен с возможностью перемещения по меньшей мере внутри охраняемого склада, причем указанный склад содержит логистический центр;

- хранилище B содержит устройство DB и управляет им, причем указанное хранилище B выполнено с возможностью доставки товара санкционированному роботу и/или предоставления роботу возможности забрать товар, содержащийся в хранилище.

[0140] Этот способ включает следующие этапы, на которых:

○ модуль связи CM(B) устройства DB принимает 100b, 200 цифровое сообщение M, содержащее поставленную задачу, причем указанная поставленная задача содержит открытый ключ PuK(A), принадлежащий роботу, данные авторизации AD(A), указывающие на то, что робот уполномочен логистическим центром осуществлять операцию Op с хранилищем, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д.;

○ предпочтительно, блок обработки CPU(B) устройства DB верифицирует 10b то, что цифровое сообщение M сертифицировано логистическим центром склада; и

○ блок обработки CPU(B) устройства DB извлекает 201, 202, 204 данные, содержащиеся в цифровом сообщении M, такие как открытый ключ PuK(A), данные авторизации AD(A), операция Op, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д.,

предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано логистическим центром;

- модуль связи CM(B) устройства DB принимает 400 от модуля связи CM(A) устройства DA аккредитацию SA, предпочтительно, подписанную 300a блоком обработки CPU(A) устройства DA с использованием своего закрытого ключа PrK(A), и/или содержащую данные, такие как секрет, подписанные 300a блоком обработки CPU(A) устройства DA с использованием своего закрытого ключа PrK(A); предпочтительно, указанный секрет был отправлен 300 от модуля связи CM(B) устройства DB на модуль связи CM(A) устройства DA;

- блок обработки CPU(B) устройства DB верифицирует 400b аккредитацию SA, предпочтительно, с использованием открытого ключа PuK(A), соответствующего указанному закрытому ключу PrK(A), преимущественно, после извлечения 202 указанного открытого ключа PuK(A) из цифрового сообщения M;

- блок обработки CPU(B) устройства DB:

- извлекает 204 ключ верификации VK(A), содержащийся в цифровом сообщении M,

- вычисляет 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A), и

- вычисляет 205 потенциальную агрегированную цифровую подпись cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

- блок обработки CPU(B) устройства DB проверяет 207, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся 206 в его памяти, и только в случае положительной верификации аккредитации SA и положительного совпадения

потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) устройства DB передает 500 в хранилище указание о том, что робот действительно уполномочен логистическим центром осуществлять 500a операцию Op.

[0141] Эта система позволяет устройству DB проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники. Более того, эта система позволяет устройству DB управлять учетными данными, связанными с этим цифровым содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет. Эта система позволяет роботу A идентифицировать себя только с помощью аккредитации SA и цифрового сообщения M, которое сертифицировано защищенным от подделки цифровым файлом, выданным контроллером C. Эта система позволяет хранилищу B быть полностью уверенным в достоверности представленной поставленной задачи.

[0142] Согласно варианту осуществления настоящее изобретение позволяет контроллеру A выполнять операцию Op без необходимости обращения к центральной базе данных или серверу, содержащему поставленную задачу. Действительно, хранилище B, а также робот A могут находиться в автономной среде до тех пор, пока они могут связываться друг с другом в ходе реализации способа согласно варианту осуществления настоящего изобретения, и, предпочтительно, до тех пор, пока контроллер B содержит агрегированную цифровую подпись ADS, например, ранее загруженную из контроллера C или с сервера. Преимущественно, отправка цифрового сообщения M роботу A и хранилищу B может быть реализована через незащищенные каналы.

[0143] Согласно варианту осуществления настоящее изобретение относится к реализации способа согласно настоящему изобретению на защищенном складе, содержащем предыдущую систему согласно настоящему изобретению.

[0144] Согласно варианту осуществления настоящее изобретение можно использовать для передачи токенов от одного контроллера к другому контроллеру, т. е. от одного устройства к другому устройству.

[0145] Согласно варианту осуществления контроллер B может доставлять определенное количество токенов контроллеру A согласно поставленной задаче контроллера B и/или поставленной задаче контроллера A, т. е. золотой слиток № 429 может быть заменен по меньше мере одним цифровым активом.

[0146] В этом варианте осуществления устройство DA может быть смартфоном, смарт-картой, сервером или компьютером, а устройство DB может быть смартфоном, смарт-картой, сервером или компьютером, а контроллер C может быть финансовым учреждением или банком.

Защищенная связь интернета вещей (IoT)

[0147] Согласно второму примеру применения настоящего изобретения, проиллюстрированному на фиг. 3, настоящее изобретение можно реализовать в среде интернета вещей, обычно называемой сетью IoT, чтобы защитить связь между несколькими устройствами, такими как устройства интернета вещей, называемые устройствами IoT. В этом примере и согласно варианту осуществления настоящего изобретения система содержит контроллер A, контроллер B и контроллер C, такие как описанные ранее. Контроллер C — это, например, командный центр C. Контроллерами A и B являются, например, компьютеры, серверы, роботы и/или смартфоны. Каждый из контроллеров A и B может быть своего рода IoT, отличным от другого. Например, контроллером A может быть смартфон A, а контроллером B может быть компьютер B.

[0148] Предпочтительно, контроллеры A, B и C вместе образуют сеть IoT, используя сеть связи CN для связи.

[0149] Преимущественно, контроллер A выполнен с возможностью отправки данных по меньшей мере одному другому контроллеру, такому как, например, контроллер B. Например, устройство DA, управляемое контроллером A,

выполнено с возможностью отправки данных посредством своего модуля связи CM(A) на устройство DB, управляемое контроллером B. В этом примере устройство DB выполнено с возможностью приема данных посредством своего модуля связи CM(B) от модуля связи CM(A) устройства DA.

[0150] Согласно предпочтительному варианту осуществления контроллер A содержит закрытый ключ PrK(A), предпочтительно, выданный контроллером A и связанный с открытым ключом PuK(A); указанный открытый ключ PuK(A) аккредитован контроллером C, т. е., например, командным центром C. Предпочтительно, указанный закрытый ключ PrK(A) хранится в памяти блока обработки CPU(A) устройства DA, управляемого контроллером A, предпочтительно, в защищенном анклаве памяти.

[0151] Согласно варианту осуществления контроллер B выполнен с возможностью сбора данных, отправленных от другого контроллера, до тех пор, пока контроллер B получает и верифицирует поставленную задачу, выданную контроллером C, указывающую на то, что указанному другому контроллеру разрешено отправлять данные контроллеру B, и, например, в течение точного временного интервала. Эта поставленная задача, как описано в настоящем документе далее, может включать несколько других данных, которые, по мнению контроллера B, позволяют принимать данные, отправленные указанным другим контроллером.

[0152] Согласно варианту осуществления контроллер B выполнен с возможностью отправки данных по меньшей мере одному другому контроллеру, такому как, например, контроллер A. Например, устройство DB, управляемое контроллером B, выполнено с возможностью отправки данных посредством своего модуля связи CM(B) на устройство DA, управляемое контроллером A. В этом примере устройство DA выполнено с возможностью приема данных посредством своего модуля связи CM(A) от модуля связи CM(B) устройства DB.

[0153] Согласно варианту осуществления контроллер B содержит закрытый ключ PrK(B), предпочтительно, выданный контроллером B и связанный с открытым

ключом PuK(B); указанный открытый ключ PuK(B) аккредитован контроллером C, т. е., например, командным центром C. Предпочтительно, указанный закрытый ключ PrK(B) хранится в памяти блока обработки CPU(B) устройства DB, управляемого контроллером B, предпочтительно, в защищенном анклаве памяти.

[0154] Согласно варианту осуществления контроллер A выполнен с возможностью сбора данных, отправленных от другого контроллера, до тех пор, пока контроллер A получает и верифицирует поставленную задачу, выданную контроллером C, указывающую на то, что указанному другому контроллеру разрешено отправлять данные контроллеру A, и, например, в течение точного временного интервала. Эта поставленная задача, как описано в настоящем документе далее, может включать несколько других данных, которые, по мнению контроллера A, позволяют принимать данные, отправленные указанным другим контроллером.

[0155] Согласно варианту осуществления каждый из контроллеров A и B имеет одинаковые технические функции. В этом примере каждый из этих контроллеров может иметь поставленную задачу, выданную контроллером C, позволяющую ему выполнить операцию Op по отношению к другому контроллеру среди контроллеров A и контроллера B.

[0156] Согласно примеру контроллером C является командный центр C. Указанный командный центр C выполнен с возможностью выдачи поставленной задачи с использованием цифрового сообщения M, отправленного контроллеру A и/или B. Например, цифровое сообщение M может содержать поставленную задачу в виде множества данных, указывающих, например, что заданный контроллер должен сделать, и, например, когда этот заданный контроллер должен это сделать. В этом примере контроллер C выдает две поставленные задачи посредством двух цифровых сообщений M: одно с именем M(A) в отношении контроллера A, а другое с именем M(B) в отношении контроллера B.

[0157] Согласно варианту осуществления контроллер A предназначен для выполнения операции Op(A), связанной с контроллером B, только если контроллер A имеет поставленную задачу, выданную контроллером C в виде цифрового сообщения M(A), и этот контроллер B верифицировал несколько параметров, касающихся указанного цифрового сообщения M(A) и указанного контроллера A, прежде чем принять, что контроллер A выполняет операцию Op(A).

[0158] Согласно варианту осуществления контроллер B предназначен для выполнения операции Op(B), связанной с контроллером A, только если контроллер B имеет поставленную задачу, выданную контроллером C в виде цифрового сообщения M(B), и этот контроллер A верифицировал несколько параметров, касающихся указанного цифрового сообщения M(B) и указанного контроллера B, прежде чем принять, что контроллер B выполняет операцию Op(B).

[0159] Например, цифровое сообщение M(A) может содержать поставленную задачу, включающую следующие данные:

- у контроллера A есть открытый ключ PuK(A);
- ключ верификации VK(A);
- операция Op(A): контроллеру A разрешено отправлять набор данных SeD(A) контроллеру B и разрешено принимать набор данных SeD(B) от контроллера B;
- временной интервал: это можно будет сделать, например, только 10 июня 2021 года.

[0160] Например, цифровое сообщение M(B) может содержать поставленную задачу, включающую следующие данные:

- у контроллера B есть открытый ключ PuK(B);

- ключ верификации VK(B);

- операция Op(B): контроллеру B разрешено отправлять набор данных SeD(B) контроллеру A и разрешено принимать набор данных SeD(A) от контроллера A;

- временной интервал: это можно будет сделать, например, только 10 июня 2021 года.

[0161] Согласно предпочтительному варианту осуществления, когда контроллер A, такой как смартфон в этом примере, принимает цифровое сообщение M(B), он верифицирует с использованием своего блока обработки CPU(A) то, что цифровое сообщение M(B) сертифицировано контроллером C, и только в случае положительной верификации того, что цифровое сообщение M(B) сертифицировано контроллером C, блок обработки CPU(A) устройства DA, управляемого контроллером A, начинает извлечение данных авторизации AD(B), содержащихся в цифровом сообщении M(B). Предпочтительно, эти данные авторизации AD(B) включают данные поставленной задачи в отношении контроллера B.

[0162] Затем контроллер A, т. е. смартфон, извлекает из цифрового сообщения M(B) разные данные, такие как открытый ключ PuK(B), соответствующий закрытому ключу PrK(B) контроллера B, т. е. компьютера в этом примере, ключ верификации VK(B), данные, связанные с операцией Op(B), и, например, временной интервал, упомянутый в поставленной задаче.

[0163] Согласно предпочтительному варианту осуществления, когда контроллер B, такой как компьютер в этом примере, принимает цифровое сообщение M(A), он верифицирует с использованием своего блока обработки CPU(B) то, что цифровое сообщение M(A) сертифицировано контроллером C, и только в случае положительной верификации того, что цифровое сообщение M(A) сертифицировано контроллером C, блок обработки CPU(B) устройства DB, управляемого контроллером B, начинает извлечение данных авторизации

AD(A), содержащихся в цифровом сообщении M(A). Предпочтительно, эти данные авторизации AD(A) включают данные поставленной задачи в отношении контроллера A.

[0164] Затем контроллер B, т. е. компьютер, извлекает из цифрового сообщения M(B) разные данные, такие как открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) контроллера A, т. е. смартфона в этом примере, ключ верификации VK(A), данные, связанные с операцией Op(A), и, например, временной интервал, упомянутый в поставленной задаче.

[0165] Согласно варианту осуществления контроллер A содержит цифровое сообщение M(A), хранящееся в памяти блока обработки CPU(A) его устройства DA и, предпочтительно, принятое от контроллера C. В этом примере контроллер A — это смартфон, который должен загрузить набор данных на компьютер, т. е. контроллер B. В этом примере устройство DA — это часть смартфона.

[0166] Согласно варианту осуществления контроллер B содержит цифровое сообщение M(B), хранящееся в памяти блока обработки CPU(A) его устройства DA и, предпочтительно, принятое от контроллера C. В этом примере контроллер B — это компьютер, который должен загрузить набор данных на смартфон, т. е. контроллер A. В этом примере устройство DB — это часть компьютера.

[0167] Согласно варианту осуществления для выполнения операций Op(A) и Op(B):

- контроллер B принимает 100b цифровое сообщение M(A), предпочтительно, от контроллера C;

- контроллер A принимает 100a цифровое сообщение M(B), предпочтительно, от контроллера C;

- предпочтительно, контроллер B верифицирует 10b с использованием своего блока обработки CPU(B) то, что цифровое сообщение M(A) сертифицировано контроллером C;

- предпочтительно, контроллер A верифицирует 10a с использованием своего блока обработки CPU(A) то, что цифровое сообщение M(B) сертифицировано контроллером C;

- контроллер B, т. е. компьютер, извлекает 201, 202, 204 из цифрового сообщения M(A) разные данные, такие как открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) контроллера A, т. е. смартфона, ключ верификации(A), данные, связанные с операцией Op(A), и, например, временной интервал, упомянутый в поставленной задаче контроллера A, предпочтительно, только в случае положительной верификации того, что цифровое сообщение M(A) сертифицировано контроллером C. Предпочтительно, эти данные авторизации AD(A) включают данные поставленной задачи контроллера A;

- контроллер A, т. е. смартфон, извлекает из цифрового сообщения M(B) разные данные, такие как открытый ключ PuK(B), соответствующий закрытому ключу PrK(B) контроллера B, т. е. компьютера, ключ верификации(B), данные, связанные с операцией Op(B), и, например, временной интервал, упомянутый в поставленной задаче контроллера B, предпочтительно, только в случае положительной верификации того, что цифровое сообщение M(B) сертифицировано контроллером C. Предпочтительно, эти данные авторизации AD(B) включают данные поставленной задачи контроллера B;

- контроллер B отправляет 300 запрос на связь Ch(B) контроллеру A; предпочтительно, модуль связи CM(B) устройства DB отправляет 300 запрос на связь Ch(B) на модуль связи CM(A) устройства DA по сети связи CN; запрос на связь Ch(B) выполнен с возможностью позволить устройству DB верифицировать то, что контроллер B действительно осуществляет связь с контроллером A, упомянутым в цифровом сообщении M(A); указанный запрос на связь может включать секрет, предпочтительно, одноразовый секрет, такой как случайное число, преимущественно, сгенерированное модулем генерирования случайных чисел GRNM(B) устройства DB;

- контроллер A отправляет запрос на связь Ch(A) контроллеру B; предпочтительно, модуль связи CM(A) устройства DA отправляет запрос на связь Ch(A) на модуль связи CM(B) устройства DB по сети связи CN; запрос на связь Ch(A) выполнен с возможностью позволить устройству DA верифицировать то, что контроллер A действительно осуществляет связь с контроллером B, упомянутым в цифровом сообщении M(B); указанный запрос на связь может включать секрет, предпочтительно, одноразовый секрет, такой как случайное число, преимущественно, сгенерированное модулем генерирования случайных чисел GRNM(A) устройства DA;

- блок обработки CPU(A) устройства DA подписывает 300a запрос на связь Ch(B) с использованием закрытого ключа PrK(A), генерируя аккредитацию SA(A);

- блок обработки CPU(B) устройства DB подписывает запрос на связь Ch(A) с использованием закрытого ключа PrK(B), генерируя аккредитацию SA(B);

- контроллер A отправляет 400 аккредитацию SA(A) контроллеру B; предпочтительно, модуль связи CM(A) устройства DA отправляет 400 аккредитацию SA(A) на модуль связи CM(B) устройства DB по сети связи CN;

- контроллер B отправляет аккредитацию SA(B) контроллеру A; предпочтительно, модуль связи CM(B) устройства DB отправляет аккредитацию SA(B) на модуль связи CM(A) устройства DA по сети связи CN;

- контроллер B проверяет 400b достоверность аккредитации SA(A) с использованием открытого ключа PuK(A), который был извлечен 202 блоком обработки CPU(B) из цифрового сообщения M(A), и который, предпочтительно, указан в поставленной задаче контроллера A;

- контроллер A проверяет достоверность аккредитации SA(B) с использованием открытого ключа PuK(B), который был извлечен блоком

обработки CPU(A) из цифрового сообщения M(B), и который, предпочтительно, указан в поставленной задаче контроллера B;

- блок обработки CPU(B) устройства DB вычисляет 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A) и вычисляет 205 потенциальную агрегированную цифровую подпись cADS(A) из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A);

- блок обработки CPU(A) устройства DA вычисляет с помощью односторонней функции, запрограммированной в блоке обработки CPU(A), потенциальную цифровую подпись cx(B) данных авторизации AD(B) и вычисляет потенциальную агрегированную цифровую подпись cADS(B) из ключа верификации VK(B) и вычисленной потенциальной цифровой подписи cx(B) данных авторизации AD(B);

- блок обработки CPU(B) устройства DB проверяет 207, совпадает ли потенциальная агрегированная цифровая подпись cADS(A) с агрегированной цифровой подписью ADS(A), предпочтительно, хранящейся в его памяти; согласно варианту осуществления указанная агрегированная цифровая подпись ADS(A) была принята контроллером B от контроллера C и/или от сервера; затем указанная агрегированная цифровая подпись ADS(A) была сохранена 206 в памяти блока обработки CPU(B) контроллера B, т. е. компьютера в этом примере;

- блок обработки CPU(A) устройства DA проверяет, совпадает ли потенциальная агрегированная цифровая подпись cADS(B) с агрегированной цифровой подписью ADS(B), предпочтительно, хранящейся в его памяти; согласно варианту осуществления указанная агрегированная цифровая подпись ADS(B) была принята контроллером A от контроллера C и/или от сервера; затем указанная агрегированная цифровая подпись ADS(B) была сохранена в памяти блока обработки CPU(A) контроллера A, т. е. смартфона в этом примере;

- если дата надлежащим образом соответствует дате, упомянутой в цифровом сообщении M(A), например, 10 июня 2021 года, если верификация аккредитации SA(A) является положительной и если потенциальная агрегированная цифровая подпись cADS(A) совпадает 207 с агрегированной цифровой подписью ADS(A), компьютер, т. е. контроллер B, принимает 500 от своего блока обработки CPU(B) указание о том, что контроллер A действительно уполномочен контроллером C осуществлять операцию Op(A), упомянутую в поставленной задаче, содержащейся в цифровом сообщении M(A);

- если дата надлежащим образом соответствует дате, упомянутой в цифровом сообщении M(B), например, 10 июня 2021 года, если верификация аккредитации SA(B) является положительной и если потенциальная агрегированная цифровая подпись cADS(B) совпадает с агрегированной цифровой подписью ADS(B), смартфон, т. е. контроллер A, принимает от своего блока обработки CPU(A) указание о том, что контроллер B действительно уполномочен контроллером C осуществлять операцию Op(B), упомянутую в поставленной задаче, содержащейся в цифровом сообщении M(B);

- контроллер B принимает набор данных SeD(A), отправленных контроллером A; предпочтительно, блок обработки CPU(B) устройства DB отправляет команду на модуль связи CM(B) устройства DB, указывающую на то, что модуль связи CM(B) может принимать набор данных SeD(A), отправленных модулем связи CM(A) устройства DA;

- контроллер A принимает набор данных SeD(B), отправленных 510 контроллером B; предпочтительно, блок обработки CPU(A) устройства DA отправляет команду на модуль связи CM(A) устройства DA, указывающую на то, что модуль связи CM(A) может принимать набор данных SeD(B), отправленных модулем связи CM(B) устройства DB;

- таким образом, контроллер A и контроллер B могут обмениваться данными, полностью доверяя друг другу.

[0168] Согласно варианту осуществления настоящее изобретение можно использовать для передачи токенов от одного контроллера к другому контроллеру, т. е. от одного устройства к другому устройству.

[0169] Согласно варианту осуществления набор данных SeD(A) и/или SeD(B) может включать токены; следовательно, настоящее изобретение можно использовать для передачи токенов от одного контроллера к другому контроллеру.

[0170] Согласно варианту осуществления контроллер B может доставлять определенное количество токенов контроллеру A согласно поставленной задаче контроллера B и/или поставленной задаче контроллера A.

[0171] В другом варианте осуществления контроллер A может быть выполнен с возможностью доставки определенного количества токенов контроллеру B согласно поставленной задаче контроллера B и/или поставленной задаче контроллера A.

[0172] В этих вариантах осуществления устройство DA может быть смартфоном, смарт-картой, сервером или компьютером, а устройство DB может быть смартфоном, смарт-картой, сервером или компьютером, а контроллер C может быть финансовым учреждением или банком.

[0173] Согласно этому примеру случая применения настоящего изобретения система предпочтительно содержит:

- контроллер A, содержащий устройство DA и управляющий им, причем указанное устройство DA выполнено с возможностью отправки и приема данных; указанное устройство DA может быть, например, смартфоном или частью смартфона в случае, когда контроллер A является смартфоном;

- контроллер B, содержащий устройство DB и управляющий им, причем указанное устройство DB выполнено с возможностью отправки и приема

данных; указанное устройство DB может быть, например, компьютером или частью компьютера в случае, когда контроллер B является компьютером.

[0174] Эта система выполнена таким образом, что:

- модуль связи CM(B) устройства DB выполнен с возможностью приема 100b цифрового сообщения M(A), содержащего поставленную задачу, связанную с контроллером A, причем указанная поставленная задача содержит открытый ключ PuK(A), принадлежащий контроллеру A, данные авторизации AD(A), указывающие на то, что контроллер A уполномочен контроллером C осуществлять операцию Op(A) с контроллером B, ключ верификации VK(A), временной интервал, в течение которого можно выполнять эту операцию Op(A), и т. д.;

- модуль связи CM(A) устройства DA выполнен с возможностью приема 100a цифрового сообщения M(B), содержащего поставленную задачу, связанную с контроллером B, причем указанная поставленная задача содержит открытый ключ PuK(B), принадлежащий контроллеру B, данные авторизации AD(B), указывающие на то, что контроллер B уполномочен контроллером C осуществлять операцию Op(B) с контроллером A, ключ верификации VK(B), временной интервал, в течение которого можно выполнять эту операцию Op(B), и т. д.;

- предпочтительно, блок обработки CPU(B) устройства DB выполнен с возможностью верификации 10b того, что цифровое сообщение M(A) сертифицировано контроллером C;

- предпочтительно, блок обработки CPU(A) устройства DA выполнен с возможностью верификации 10a того, что цифровое сообщение M(B) сертифицировано контроллером C;

- блок обработки CPU(B) устройства DB выполнен с возможностью извлечения 201, 202, 204 данных, содержащихся в цифровом сообщении M(A), таких как открытый ключ PuK(A), данные авторизации AD(A), операция Op(A),

ключ верификации VK(A), временной интервал, в течение которого можно выполнять эту операцию Op(A), и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M(A) сертифицировано контроллером C;

- блок обработки CPU(A) устройства DA выполнен с возможностью извлечения данных, содержащихся в цифровом сообщении M(B), таких как открытый ключ PuK(B), данные авторизации AD(B), операция Op(B), ключ верификации VK(B), временной интервал, в течение которого можно выполнять эту операцию Op(B), и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M(B) сертифицировано контроллером C;

- модуль связи CM(B) устройства DB выполнен с возможностью приема 400 от модуля связи CM(A) устройства DA аккредитации SA(A), предпочтительно, подписанной 300a блоком обработки CPU(A) устройства DA с использованием своего закрытого ключа PrK(A), и/или содержащей данные, такие как секрет, подписанные 300a блоком обработки CPU(A) устройства DA с использованием своего закрытого ключа PrK(A); предпочтительно, указанный секрет был отправлен 300 от модуля связи CM(B) устройства DB на модуль связи CM(A) устройства DA;

- модуль связи CM(A) устройства DA выполнен с возможностью приема от модуля связи CM(B) устройства DB аккредитации SA(B), предпочтительно, подписанной блоком обработки CPU(B) устройства DB с использованием своего закрытого ключа PrK(B), и/или содержащей данные, такие как другой секрет, подписанные блоком обработки CPU(B) устройства DB с использованием своего закрытого ключа PrK(B); предпочтительно, указанный другой секрет был отправлен от модуля связи CM(A) устройства DA на модуль связи CM(B) устройства DB;

- блок обработки CPU(B) устройства DB выполнен с возможностью верификации 400b аккредитации SA(A), предпочтительно, с использованием

открытого ключа PuK(A), соответствующего указанному закрытому ключу PrK(A), преимущественно, после извлечения 202 указанного открытого ключа PuK(A) из цифрового сообщения M(A);

- блок обработки CPU(A) устройства DA выполнен с возможностью верификации аккредитации SA(B), предпочтительно, с использованием открытого ключа PuK(B), соответствующего указанному закрытому ключу PrK(B), преимущественно, после извлечения указанного открытого ключа PuK(B) из цифрового сообщения M(B);

- блок обработки CPU(B) устройства DB выполнен с возможностью:

- вычисления 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальной цифровой подписи cx(A) данных авторизации AD(A), и

- вычисления 205 потенциальной агрегированной цифровой подписи cADS(A) из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A);

- блок обработки CPU(A) устройства DA выполнен с возможностью:

- вычисления с помощью односторонней функции, запрограммированной в блоке обработки CPU(A), потенциальной цифровой подписи cx(B) данных авторизации AD(B), и

- вычисления потенциальной агрегированной цифровой подписи cADS(B) из ключа верификации VK(B) и вычисленной потенциальной цифровой подписи cx(B) данных авторизации AD(B);

- блок обработки CPU(B) устройства DB выполнен с возможностью проверки 207 того, совпадает ли потенциальная агрегированная цифровая подпись cADS(A) с агрегированной цифровой подписью ADS(A), хранящейся 206 в его памяти, и только в случае положительной верификации аккредитации SA(A) и положительного совпадения потенциальной агрегированной цифровой

подписи cADS(A) с агрегированной цифровой подписью ADS(A), блок обработки CPU(B) устройства DB выполнен с возможностью передачи 500 контроллеру B указания о том, что контроллер A действительно уполномочен контроллером C осуществлять 500a операцию Op(A);

- блок обработки CPU(A) устройства DA выполнен с возможностью проверки того, совпадает ли потенциальная агрегированная цифровая подпись cADS(B) с агрегированной цифровой подписью ADS(B), хранящейся в его памяти, и только в случае положительной верификации аккредитации SA(B) и положительного совпадения потенциальной агрегированной цифровой подписи cADS(B) с агрегированной цифровой подписью ADS(B), блок обработки CPU(A) устройства DA выполнен с возможностью передачи контроллеру A указания о том, что контроллер B действительно уполномочен контроллером C осуществлять 510 операцию Op(B).

[0175] Эта система позволяет контроллеру B проверять достоверность цифрового содержимого цифрового сообщения M(A) и контроллеру A проверять достоверность цифрового содержимого цифрового сообщения M(B), с большей уверенностью, чем решения предшествующего уровня техники. Более того, эта система позволяет контроллеру B управлять учетными данными, связанными с этим цифровым содержимым, чтобы проверить, является ли цифровое содержимое цифрового сообщения M(A) достоверным или нет, а контроллеру A управлять учетными данными, связанными с этим цифровым содержимым, чтобы проверить, является ли цифровое содержимое цифрового сообщения M(B) достоверным или нет. Эта система позволяет контроллеру A идентифицировать себя только с помощью аккредитации SA(A) и цифрового сообщения M(A), которое, предпочтительно, сертифицировано защищенным от подделки цифровым файлом, выданным контроллером C, а контроллеру B идентифицировать себя только с помощью аккредитации SA(B) и цифрового сообщения M(B), которое, предпочтительно, сертифицировано защищенным от подделки цифровым файлом, выданным контроллером C. Эта система позволяет контроллеру B быть полностью уверенным в достоверности представленной

поставленной задачи, и контроллеру A быть полностью уверенным в достоверности представленной поставленной задачи.

[0176] Согласно этому примеру случая применения настоящего изобретения согласно варианту осуществления настоящее изобретение относится к способу, в котором:

- контроллер A содержит устройство DA и управляет им, причем указанное устройство DA выполнено с возможностью отправки и приема данных;

- контроллер B содержит устройство DB и управляет им, причем указанное устройство DB выполнено с возможностью отправки и приема данных.

[0177] Этот способ включает следующие этапы, на которых:

- модуль связи CM(B) устройства DB принимает 100b цифровое сообщение M(A), содержащее поставленную задачу, связанную с контроллером A, причем указанная поставленная задача содержит открытый ключ PuK(A), принадлежащий контроллеру A, данные авторизации AD(A), указывающие на то, что контроллер A уполномочен контроллером C осуществлять операцию Op(A) с контроллером B, ключ верификации VK(A), временной интервал, в течение которого можно выполнять эту операцию Op(A), и т. д.;

- модуль связи CM(A) устройства DA принимает 100a цифровое сообщение M(B), содержащее поставленную задачу, связанную с контроллером B, причем указанная поставленная задача содержит открытый ключ PuK(B), принадлежащий контроллеру B, данные авторизации AD(B), указывающие на то, что контроллер B уполномочен контроллером C осуществлять операцию Op(B) с контроллером A, ключ верификации VK(B), временной интервал, в течение которого можно выполнять эту операцию Op(B), и т. д.;

- предпочтительно, блок обработки CPU(B) устройства DB верифицирует 10b то, что цифровое сообщение M(A) сертифицировано контроллером C;

○ предпочтительно, блок обработки CPU(A) устройства DA верифицирует 10a то, что цифровое сообщение M(B) сертифицировано контроллером C;

○ блок обработки CPU(B) устройства DB извлекает 201, 202, 204 данные, содержащиеся в цифровом сообщении M(A), такие как открытый ключ PuK(A), данные авторизации AD(A), операция Op(A), ключ верификации VK(A), временной интервал, в течение которого можно выполнять эту операцию Op(A), и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M(A) сертифицировано контроллером C;

○ блок обработки CPU(A) устройства DA извлекает данные, содержащиеся в цифровом сообщении M(B), такие как открытый ключ PuK(B), данные авторизации AD(B), операция Op(B), ключ верификации VK(B), временной интервал, в течение которого можно выполнять эту операцию Op(B), и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M(B) сертифицировано контроллером C;

○ модуль связи CM(B) устройства DB принимает 400 от модуля связи CM(A) устройства DA аккредитацию SA(A), предпочтительно, подписанную 300a блоком обработки CPU(A) устройства DA с использованием своего закрытого ключа PrK(A), и/или содержащую данные, такие как секрет, подписанные 300a блоком обработки CPU(A) устройства DA с использованием своего закрытого ключа PrK(A); предпочтительно, указанный секрет был отправлен 300 от модуля связи CM(B) устройства DB на модуль связи CM(A) устройства DA;

○ модуль связи CM(A) устройства DA принимает от модуля связи CM(B) устройства DB аккредитацию SA(B), предпочтительно, подписанную блоком обработки CPU(B) устройства DB с использованием своего закрытого ключа PrK(B), и/или содержащую данные, такие как другой секрет, подписанные блоком обработки CPU(B) устройства DB с использованием своего закрытого ключа PrK(B); предпочтительно, указанный другой секрет был отправлен от модуля связи CM(A) устройства DA на модуль связи CM(B) устройства DB;

- блок обработки CPU(B) устройства DB верифицирует 400b аккредитацию SA(A), предпочтительно, с использованием открытого ключа PuK(A), соответствующего указанному закрытому ключу PrK(A), преимущественно, после извлечения указанного открытого ключа PuK(A) из цифрового сообщения M(A);

- блок обработки CPU(A) устройства DA верифицирует аккредитацию SA(B), предпочтительно, с использованием открытого ключа PuK(B), соответствующего указанному закрытому ключу PrK(B), преимущественно, после извлечения указанного открытого ключа PuK(B) из цифрового сообщения M(B);

- блок обработки CPU(B) устройства DB:

- извлекает 204 ключ верификации VK(A), содержащийся в цифровом сообщении M(A),

- вычисляет 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную 205 цифровую подпись cx(A) данных авторизации AD(A), и

- вычисляет потенциальную агрегированную цифровую подпись cADS(A) из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A);

- блок обработки CPU(A) устройства DA:

- извлекает ключ верификации VK(B), содержащийся в цифровом сообщении M(B),

- вычисляет с помощью односторонней функции, запрограммированной в блоке обработки CPU(A), потенциальную цифровую подпись cx(B) данных авторизации AD(B), и

- вычисляет потенциальную агрегированную цифровую подпись cADS(B) из ключа верификации VK(B) и вычисленной потенциальной цифровой подписи cx(B) данных авторизации AD(B);

  - блок обработки CPU(B) устройства DB проверяет 207, совпадает ли потенциальная агрегированная цифровая подпись cADS(A) с агрегированной цифровой подписью ADS(A), хранящейся 206 в его памяти, и только в случае положительной верификации аккредитации SA(A) и положительного совпадения потенциальной агрегированной цифровой подписи cADS(A) с агрегированной цифровой подписью ADS(A), блок обработки CPU(B) устройства DB передает 500 контроллеру B указание о том, что контроллер A действительно уполномочен контроллером C осуществлять 500a операцию Op(A);

  - блок обработки CPU(A) устройства DA проверяет, совпадает ли потенциальная агрегированная цифровая подпись cADS(B) с агрегированной цифровой подписью ADS(B), хранящейся в его памяти, и только в случае положительной верификации аккредитации SA(B) и положительного совпадения потенциальной агрегированной цифровой подписи cADS(B) с агрегированной цифровой подписью ADS(B), блок обработки CPU(A) устройства DA передает контроллеру A указание о том, что контроллер B действительно уполномочен контроллером C осуществлять 510 операцию Op(B).

[0178] Эта система позволяет контроллеру B проверять достоверность цифрового содержимого цифрового сообщения M(A) и контроллеру A проверять достоверность цифрового содержимого цифрового сообщения M(B) с большей уверенностью, чем решения предшествующего уровня техники. Более того, эта система позволяет контроллеру B управлять учетными данными, связанными с цифровым содержимым цифрового сообщения M(A), чтобы проверить, является ли это цифровое содержимое достоверным или нет, и позволяет контроллеру A управлять учетными данными, связанными с цифровым содержимым цифрового сообщения M(B), чтобы проверить, является ли это цифровое содержимое достоверным или нет. Эта система позволяет контроллеру A идентифицировать

себя только с помощью аккредитации SA(A) и цифрового сообщения M(A), которое сертифицировано защищенным от подделки цифровым файлом, выданным контроллером C, и позволяет контроллеру B идентифицировать себя только с помощью аккредитации SA(B) и цифрового сообщения M(B), которое сертифицировано защищенным от подделки цифровым файлом, выданным контроллером C. Эта система позволяет контроллеру B быть полностью уверенным в достоверности представленной поставленной задачи, и контроллеру A быть полностью уверенным в достоверности представленной поставленной задачи.

[0179] Согласно варианту осуществления настоящее изобретение позволяет контроллеру A выполнять операцию Op(A) и контроллеру B выполнять операцию Op(B) без необходимости обращения к центральной базе данных или серверу, содержащему поставленную задачу. Действительно, контроллер B, а также контроллер A могут находиться в автономной среде до тех пор, пока они могут связываться друг с другом в ходе реализации способа согласно варианту осуществления настоящего изобретения, и, предпочтительно, до тех пор, пока контроллер A содержит агрегированную цифровую подпись ADS(B), например, ранее загруженную из контроллера C или с сервера, и, предпочтительно, до тех пор, пока контроллер B содержит агрегированную цифровую подпись ADS(A), например, ранее загруженную из контроллера C или с сервера. Преимущественно, отправка цифровых сообщений M(A) и M(B) контроллеру A и контроллеру B может быть реализована через незащищенные каналы.

[0180] Согласно варианту осуществления настоящее изобретение относится к реализации способа согласно настоящему изобретению в сети связи CN, содержащей предыдущую систему согласно настоящему изобретению.

Медсестра, взаимодействующая с медицинским устройством

[0181] Согласно третьему примеру применения настоящего изобретения, проиллюстрированному на фиг. 4, настоящее изобретение можно реализовать

для того, чтобы позволить медсестре безопасно вводить заданное лекарственное средство заданному пациенту с помощью медицинского устройства.

[0182] Согласно этому примеру контроллером A является медсестра A. Медсестра A содержит устройство DA, которое может быть, например, смартфоном. Медсестра A должна ухаживать за несколькими пациентами и, следовательно, должна вводить различные лекарственные средства согласно разным поставленным задач, выданным, например, по меньшей мере одним врачом и/или больницей, которые в этом случае применения являются контроллером C. Контроллер A, т. е. медсестра A, содержит закрытый ключ PrK(A), предпочтительно, выданный контроллером A и связанный с открытым ключом PuK(A); указанный открытый ключ PuK(A) аккредитован контроллером C, т. е. врачом C и/или больницей. Этот закрытый ключ PrK(A) хранится в памяти блока обработки CPU(A) устройства DA, т. е., например, смартфона медсестры A, предпочтительно, в защищенном анклаве памяти.

[0183] Согласно этому примеру контроллер B представляет собой медицинское устройство B, предпочтительно, интеллектуальное медицинское устройство, т. е. медицинское устройство, содержащее устройство DB. Указанное медицинское устройство B выполнено с возможностью доставки или введения определенного заданного количества заданного лекарственного средства, если указанное медицинское устройство принимает надлежащую поставленную задачу, указывающую на то, что заданная медсестра может выполнять заданную операцию Op, такую как введение лекарственного средства пациенту; причем указанная поставленная задача выдана врачом C и/или больницей, выступающими в качестве контроллера C в этом примере.

[0184] Согласно этому примеру контроллер C является врачом C, и/или медицинским учреждением, и/или больницей. Указанный врач C выдает поставленную задачу с использованием цифрового сообщения M, отправленного медсестре A, например, по сети связи CN, такой как Интернет. Согласно варианту осуществления цифровое сообщение M также отправляется на

медицинское устройство B врачом C. Например, цифровое сообщение M может содержать поставленную задачу в виде ряда данных, указывающих, например, что медсестра A должна сделать и когда медсестра A должна это сделать. В этом примере поставленная задача может включать следующие данные:

- у медсестры A есть открытый ключ PuK(A);

- ключ верификации VK(A);

- операция Op: медсестра A должна ввести Y мл лекарственного средства X пациенту ABC;

- временной интервал: это необходимо сделать в промежутке времени с 9:30 до 9:45, например, 10 июня 2021 года.

- местоположение, соответствующее адресу пациента.

[0185] Согласно варианту осуществления, когда медсестра, т. е. контроллер A, принимает цифровое сообщение M, она верифицирует с использованием блока обработки CPU(A) то, что цифровое сообщение M сертифицировано врачом C, и, предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано врачом C, блок обработки CPU(A) устройства DA медсестры A начинает извлечение данных авторизации AD(A), содержащихся в цифровом сообщении M. Предпочтительно, эти данные авторизации AD(A) включают данные поставленной задачи медсестры A.

[0186] Затем блок обработки CPU(A) устройства DA медсестры A, т. е., например, ее смартфон DA, извлекает из цифрового сообщения M разные данные, такие как данные, связанные с операцией Op, и, например, временной интервал, упомянутый в поставленной задаче, и/или местоположение, упомянутое в поставленной задаче.

[0187] Согласно предпочтительному варианту осуществления, когда медицинское устройство, т. е. контроллер B, принимает цифровое сообщение M, оно верифицирует с использованием блока обработки CPU(B) то, что цифровое

сообщение M сертифицировано врачом C, и, предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано врачом C, блок обработки CPU(B) устройства DB медицинского устройства начинает извлечение данных авторизации AD(A), содержащихся в цифровом сообщении M. Предпочтительно, эти данные авторизации AD(A) включают данные поставленной задачи.

[0188] Затем контроллер B, т. е. медицинское устройство B, извлекает из цифрового сообщения M разные данные, такие как открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) медсестры A, т. е. контроллера A, ключ верификации(A), данные, связанные с операцией Op, и, например, временной интервал, упомянутый в поставленной задаче, и/или местоположение, упомянутое в поставленной задаче.

[0189] Согласно варианту осуществления, например, когда медсестра A подходит к медицинскому устройству B или когда медсестра A активирует медицинское устройство B, медицинское устройство B отправляет запрос на связь медсестре A; предпочтительно, модуль связи CM(B) устройства DB отправляет запрос на связь на модуль связи CM(A) устройства DA, которым в данном случае является, например, смартфон медсестры A.

[0190] Согласно варианту осуществления модуль связи CM(B) устройства DB, управляемого медицинским устройством B, содержит модуль отображения DD(B) и, предпочтительно, модуль оптического считывания OR(B). Указанный модуль отображения DD(B) выполнен с возможностью отображения оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB(). Блок графических данных GDB(B) может содержать данные различного типа, такие как, например, указанный запрос на связь. Преимущественно, этой блок цифровых данных GDB(B) может включать двумерный штрих-код, также называемый «QR-кодом».

[0191] Согласно варианту осуществления модуль связи CM(A) смартфона медсестры A содержит модуль оптического считывания OR(A) и, предпочтительно, модуль отображения DD(A). Указанный модуль оптического считывания OR(A) выполнен с возможностью считывания и декодирования оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB. Предпочтительно, модуль связи CM(A) выполнен с возможностью извлечения данных из блока графических данных GDB, таких как, например, указанный запрос на связь.

[0192] В этом примере медицинское устройство B отображает QR-код QRC(B) с использованием своего модуля отображения, причем указанный QR-код QRC(B) кодирует запрос на связь. Затем медсестра A использует свой смартфон для декодирования указанного QR-кода QRC(B) и извлечения указанного запроса на связь с использованием модуля оптического считывания OR(A) смартфона.

[0193] Преимущественно, этот запрос на связь может быть случайным числом, сгенерированным модулем генерирования случайных чисел GRNM(B) устройства DB. Согласно варианту осуществления, когда медсестра A принимает указанный запрос на связь посредством своего смартфона, преимущественно, посредством модуля связи CM(A) своего смартфона, смартфон подписывает запрос на связь с помощью ее закрытого ключа PrK(A), более конкретно, блок обработки CPU(A) смартфона подписывает запрос на связь с использованием закрытого ключа PrK(A), генерируя указанную аккредитацию SA. Затем смартфон отправляет обратно на медицинское устройство B аккредитацию SA, предпочтительно, модуль связи CM(A) смартфона отправляет указанную аккредитацию SA на модуль связи CM(B) устройства DB, управляемого медицинским устройством B.

[0194] Согласно варианту осуществления модуль связи CM(A) смартфона отображает оптическое считываемое представление данных, предпочтительно, оптическое считываемое представление блока графических данных GDB(A), с

использованием своего модуля отображения DD(A); предпочтительно, указанный блок графических данных GDB(A) включает закодированную версию аккредитации SA, например, в виде одного или нескольких QR-кодов QRC(A).

[0195] Согласно этому варианту осуществления модуль связи CM(B) устройства DB, управляемого медицинским устройством B, считывает и декодирует этот QR-код QRC(B) с использованием своего модуля оптического считывания OR(B) для извлечения указанной аккредитации SA.

[0196] Затем медицинское устройство B проверяет достоверность аккредитации SA с использованием открытого ключа PuK(A), который был извлечен блоком обработки CPU(B) из цифрового сообщения M, и который, предпочтительно, указан в поставленной задаче, т. е. содержится в цифровом сообщении M.

[0197] Затем блок обработки CPU(B) устройства DB медицинского устройства B вычисляет с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A) и вычисляет потенциальную агрегированную цифровую подпись cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и блок обработки CPU(B) устройства DB проверяет, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся в его памяти. Согласно варианту осуществления указанная агрегированная цифровая подпись ADS была принята медицинским устройством B от указанного врача C и/или от сервера. Затем указанная агрегированная цифровая подпись ADS была сохранена в памяти блока обработки CPU(B) устройства DB, управляемого медицинским устройством B.

[0198] Согласно варианту осуществления медицинское устройство B извлекает другие данные из цифрового сообщения M, такие как временной интервал, в течение которого должна работать медсестра A, как, например, с 9:30 до 9:45 10 июня 2021 года в этом примере, и/или местоположение пациента.

[0199] Затем, если медсестра находится по адресу пациента, если время соответствует временному интервалу, содержащемуся в поставленной задаче, например, с 9:30 до 9:45 10 июня 2021 года, если верификация аккредитации SA является положительной и если потенциальная агрегированная цифровая подпись cADS совпадает с агрегированной цифровой подписью ADS, медицинское устройство B принимает от блока обработки CPU(B) устройства DB указание о том, что медсестра A действительно уполномочена врачом C осуществлять операцию Op, упомянутую в поставленной задаче, содержащейся в цифровом сообщении M. Следовательно, медицинское устройство B уполномочивает медсестру A вводить Y мл лекарственного средства X пациенту ABC, и/или медицинское устройство B вводит Y мл лекарственного средства X пациенту ABC под наблюдением медсестры A, и/или медицинское устройство B доставляет Y мл лекарственного средства X медсестре A для введения пациенту ABC.

[0200] Согласно этому примеру случая применения настоящего изобретения система предпочтительно содержит:

- смартфон DA медсестры A, причем указанный смартфон DA выполнен с возможностью обеспечения аутентификации медсестры A медицинским устройством B, чтобы медсестра A могла выполнить операцию Op, предпочтительно, указанный смартфон содержит модуль связи CM(A), содержащий модуль отображения DD(A), выполненный с возможностью отображения оптического считываемого представления данных, преимущественно, оптического считываемого представления блока графических данных GDB(A); причем указанный блок графических данных GDB(A) включает закодированные данные, например, в виде QR-кода;

- медицинское устройство B, содержащее устройство DB и управляющее им, причем указанное медицинское устройство B выполнено с возможностью проверки полномочий заданной медсестры вводить заданное количество заданного лекарственного средства заданному пациенту, предпочтительно, в

заданный временной интервал, и/или доставки заданного количества заданного лекарственного средства заданному пациенту под наблюдением заданной медсестры, предпочтительно, в заданный временной интервал; устройство DB содержит модуль связи CM(B), содержащий модуль оптического считывания OR(B), выполненный с возможностью считывания и декодирования оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB, и, преимущественно, извлечения данных из блока графических данных GDB.

[0201] Эта система выполнена таким образом, что:

- модуль связи CM(B) устройства DB медицинского устройства B выполнен с возможностью приема 200 цифрового сообщения M, содержащего поставленную задачу, причем указанная поставленная задача содержит открытый ключ PuK(A), принадлежащий медсестре A, данные авторизации AD(A), указывающие на то, что медсестра A уполномочена врачом C осуществлять операцию Op, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д.;

- предпочтительно, блок обработки CPU(B) устройства DB выполнен с возможностью верификации 10b того, что цифровое сообщение M сертифицировано врачом C;

- блок обработки CPU(B) устройства DB выполнен с возможностью извлечения 201, 202, 204 данных, содержащихся в цифровом сообщении M, таких как открытый ключ PuK(A), данные авторизации AD(A), операция Op, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано врачом C;

- модуль связи CM(B) устройства DB выполнен с возможностью приема 400 аккредитации SA от модуля связи CM(A) смартфона DA, предпочтительно,

модуль оптического считывания OR(B) модуля связи CM(B) устройства DB выполнен с возможностью считывания и декодирования оптического считываемого представления блока графических данных GDB(A), отображаемого модулем отображения DD(A) смартфона DA; причем, предпочтительно, указанный блок графических данных GDB(A) включает закодированную версию аккредитации SA, преимущественно в виде двумерного штрих-кода, указанный модуль оптического считывания OR(B) выполнен с возможностью декодирования указанной закодированной версии аккредитации SA для извлечения указанной аккредитации SA; предпочтительно, указанная аккредитация SA подписывается 300a блоком обработки CPU(A) устройства DA с использованием его закрытого ключа PrK(A) и/или содержит данные, такие как секрет, подписанные 300a блоком обработки CPU(A) устройства DA с использованием его закрытого ключа PrK(A);

- блок обработки CPU(B) устройства DB выполнен с возможностью верификации 400b аккредитации SA, предпочтительно, с использованием открытого ключа PuK(A), соответствующего указанному закрытому ключу PrK(A), преимущественно, после извлечения 202 указанного открытого ключа PuK(A) из цифрового сообщения M;

- блок обработки CPU(B) устройства DB выполнен с возможностью:

- вычисления 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальной 205 цифровой подписи cx(A) данных авторизации AD(A), и

- вычисления потенциальной агрегированной цифровой подписи cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

- блок обработки CPU(B) устройства DB выполнен с возможностью проверки 207 того, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся 206 в его

памяти, и только в случае положительной верификации аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) устройства DB выполнен с возможностью передачи 500 на медицинское устройство B указания о том, что медсестра A действительно уполномочена врачом C осуществлять 500a операцию Op.

[0202] Эта система позволяет медицинскому устройству B проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники. Более того, эта система позволяет медицинскому устройству B управлять учетными данными, т. е. поставленной задачей, связанной с этим цифровым содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет. Эта система позволяет медсестре A идентифицировать себя только с помощью аккредитации SA и своих учетных данных, которые содержатся в цифровом сообщении M и которые, предпочтительно, сертифицированы защищенным от подделки цифровым файлом, выданным контроллером C. Эта система позволяет медицинскому устройству B быть полностью уверенным в достоверности представленной поставленной задачи.

[0203] Следует отметить, что эта система позволяет избежать использования биометрических данных медсестры A. Поставленной задачи и аккредитации SA достаточно, чтобы предоставить полную уверенность медицинскому устройству B. Преимущественно, эта система позволяет избежать каких-либо биометрических данных, биометрического измерения или раскрытия частной информации в отношении медсестры A.

[0204] Согласно этому примеру случая применения настоящего изобретения согласно варианту осуществления настоящее изобретение относится к способу, в котором:

- смартфон DA медсестры A выполнен с возможностью обеспечения аутентификации медсестры A медицинским устройством B, чтобы медсестра A

могла выполнить операцию Op, предпочтительно, указанный смартфон DA содержит модуль связи CM(A), содержащий модуль отображения DD(A), выполненный с возможностью отображения оптического считываемого представления данных, преимущественно, оптического считываемого представления блока графических данных GDB(A); причем указанный блок графических данных GDB(B) включает закодированные данные, например, в виде QR-кода;

- медицинское устройство B содержит устройство DB и управляет им, указанное медицинское устройство B выполнено с возможностью проверки полномочий заданной медсестры вводить заданное количество заданного лекарственного средства заданному пациенту, предпочтительно, в заданный временной интервал, и/или доставки заданного количества заданного лекарственного средства заданному пациенту под наблюдением заданной медсестры, предпочтительно, в заданный временной интервал; устройство DB содержит модуль связи CM(B), содержащий модуль оптического считывания OR(B), выполненный с возможностью считывания и декодирования оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB, и, преимущественно, извлечения данных из блока графических данных GDB.

[0205] Этот способ включает следующие этапы, на которых:

- модуль связи CM(B) устройства DB медицинского устройства B принимает 200 цифровое сообщение M, содержащее поставленную задачу, причем указанная поставленная задача содержит открытый ключ PuK(A), принадлежащий медсестре A, данные авторизации AD(A), указывающие на то, что медсестра A уполномочена врачом C осуществлять операцию Op, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д.;

- предпочтительно, блок обработки CPU(B) устройства DB верифицирует 10b то, что цифровое сообщение M сертифицировано врачом C;

○ блок обработки CPU(B) устройства DB извлекает 201, 202, 204 данные, содержащиеся в цифровом сообщении M, такие как открытый ключ PuK(A), данные авторизации AD(A), операция Op, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано врачом C;

○ модуль связи CM(B) устройства DB принимает 400 аккредитацию SA от модуля связи CM(A) смартфона DA, предпочтительно, модуль оптического считывания OR(B) модуля связи CM(B) устройства DB считывает и декодирует оптическое считываемое представление блока графических данных GDB(A), отображаемого модулем отображения DD(A) смартфона DA; причем, предпочтительно, указанный блок графических данных GDB(A) включает закодированную версию аккредитации SA, преимущественно, в виде двумерного штрих-кода, указанный модуль оптического считывания OR(B) декодирует указанную закодированную версию аккредитации SA для извлечения указанной аккредитации SA; предпочтительно, указанная аккредитация SA подписывается 300a блоком обработки CPU(A) устройства DA с использованием его закрытого ключа PrK(A) и/или содержит данные, такие как секрет, подписанные 300a блоком обработки CPU(A) устройства DA с использованием его закрытого ключа PrK(A);

○ блок обработки CPU(B) устройства DB верифицирует 400b аккредитацию SA, предпочтительно, с использованием открытого ключа PuK(A), соответствующего указанному закрытому ключу PrK(A), преимущественно, после извлечения 202 указанного открытого ключа PuK(A) из цифрового сообщения M;

○ блок обработки CPU(B) устройства DB:

- извлекает 204 ключ верификации VK(A), содержащийся в цифровом сообщении M,

- вычисляет 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A), и

- вычисляет 205 потенциальную агрегированную цифровую подпись cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

  - блок обработки CPU(B) устройства DB проверяет 207, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся в его памяти, и только в случае положительной верификации аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) устройства DB передает 500 на медицинское устройство B указание о том, что медсестра A действительно уполномочена врачом C осуществлять 500a операцию Op.

[0206] Этот способ позволяет медицинскому устройству B проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники. Более того, этот способ позволяет медицинскому устройству B управлять учетными данными, т. е. поставленной задачей, связанной с этим цифровым содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет. Этот способ позволяет медсестре A идентифицировать себя только с помощью аккредитации SA и своих учетных данных, которые содержатся в цифровом сообщении M и которые, предпочтительно, сертифицированы защищенным от подделки цифровым файлом, выданным контроллером C. Этот способ позволяет медицинскому устройству B быть полностью уверенным в достоверности представленной поставленной задачи.

[0207] Следует отметить, что этот способ позволяет избежать использования биометрических данных медсестры A. Этого цифрового сообщения M и аккредитации SA достаточно, чтобы предоставить полную уверенность

медицинскому устройству B. Преимущественно, этот способ позволяет избежать каких-либо биометрических данных, биометрического измерения или раскрытия частной информации медсестры A.

[0208] Согласно варианту осуществления настоящее изобретение позволяет медсестре A и медицинскому устройству B выполнять операцию Op без необходимости обращения к центральной базе данных или серверу, содержащему поставленную задачу. Действительно, медицинское устройство B, а также медсестра A могут находиться в автономной среде до тех пор. пока они могут связываться друг с другом в ходе реализации способа согласно варианту осуществления настоящего изобретения, и, предпочтительно, до тех пор, пока контроллер B содержит агрегированную цифровую подпись ADS, например, ранее загруженную из контроллера C или с сервера. Преимущественно, отправка цифрового сообщения M медсестре A и медицинскому устройству B может быть реализована через незащищенные каналы.

[0209] Согласно варианту осуществления настоящее изобретение относится к реализации способа согласно настоящему изобретению в медицинской среде, содержащей предыдущую систему согласно настоящему изобретению.

Ордер на обыск

[0210] Согласно четвертому примеру применения настоящего изобретения, проиллюстрированному на фиг. 5, настоящее изобретение можно реализовать для того, чтобы позволить сотруднику полиции безопасно выполнить ордер на обыск в отношении заданного гражданина.

[0211] Согласно этому примеру контроллером A является сотрудник полиции A. Сотрудник полиции A содержит устройство DA, которое может быть, например, смартфоном DA. Сотрудник полиции A должен выполнить задачу, содержащуюся в ордере, такую как, например, проникнуть в дом гражданина для поиска доказательств преступления; в этом случае ордером является, например, ордер на обыск. Предпочтительно, этот ордер был выдан судьей или судебным

учреждением; в этом случае применения указанный судья или судебное учреждение играет роль контроллера C. Сотрудник полиции A, т. е. контроллер A, содержит закрытый ключ PrK(A), предпочтительно, выданный контроллером A и связанный с открытым ключом PuK(A); причем указанный открытый ключ PuK(A) сертифицирован контроллером C, т. е., например, судьей C. Этот закрытый ключ PrK(A) хранится в памяти блока обработки CPU(A) устройства DA, т. е., например, смартфона DA сотрудника полиции A, предпочтительно, в защищенном анклаве памяти.

[0212] Согласно этому примеру контроллером B является гражданин, упомянутый в указанном ордере: в этом примере устройство DB может быть смартфоном DB гражданина B.

[0213] Таким образом, согласно этому примеру контроллер C является судьей C и/или судебным учреждением. Указанный судья C выдает ордер, т. е. поставленную задачу, с использованием цифрового сообщения M, отправленного сотруднику полиции A, например, по сети связи CN, такой как Интернет. Например, это цифровое сообщение M может содержать и/или быть в виде оптического считываемого представления блока графических данных GDB(A); преимущественно, указанный блок графических данных GDB(A) может включать двумерный штрих-код, такой как, например, QR-код QRC(A). Согласно варианту осуществления такой блок графических данных GDB(A) также можно называть цифровой меткой DM(A).

[0214] Согласно предпочтительному варианту осуществления цифровое сообщение M, содержащее ордер, имеет машиночитаемую форму, например, такую как QR-код QRC(A).

[0215] Например, цифровое сообщение M может содержать поставленную задачу в виде ряда данных, указывающих на то, например, что сотруднику полиции A разрешено делать и когда сотруднику полиции A разрешено это делать. В этом примере поставленная задача, т. е. ордер, может включать следующие данные:

- у сотрудника полиции A есть открытый ключ PuK(A);

- ключ верификации VK(A);

- операция Op: сотрудник полиции A уполномочен проникнуть в дом гражданина B, по адресу Y, для поиска доказательств;

- временной интервал: это необходимо сделать в промежутке времени с 15:00 до 18:30, например, 11 июня 2021 года.

[0216] Согласно предпочтительному варианту осуществления, когда сотрудник полиции A, т. е. контроллер A, принимает цифровое сообщение M от судьи C, он верифицирует с использованием своего блока обработки CPU(A) то, что цифровое сообщение M сертифицировано судьей C, т. е. контроллером C.

[0217] Например, оказавшись у двери дома гражданина B, сотрудник полиции A показывает цифровое сообщение M, т. е. указанный QR-код QRC(A) гражданину B. Согласно варианту осуществления смартфон DA, т. е. устройство DA, содержит модуль связи CM(A), содержащий модуль отображения DD(A) и, предпочтительно, модуль оптического считывания OR(B); указанный модуль отображения DD(A) выполнен с возможностью отображения оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB(A), такого как блок графических данных GDB(A), который включает закодированную версию цифрового сообщения M, т. е. ордера. Таким образом, согласно варианту осуществления, оказавшись у двери дома гражданина B, сотрудник полиции A использует свой смартфон DA для отображения QR-кода QRC(A), кодирующего указанное цифровое сообщение M, с использованием указанного модуля отображения DD(A).

[0218] Затем гражданин B использует свой смартфон DB для оптического считывания указанного QR-кода QRC(A), отображаемого модулем отображения DD(A) смартфона DA сотрудника полиции A. Затем гражданин B использует свой смартфон DB для извлечения цифрового сообщения M из указанного QR-

кода QRC(A). Согласно варианту осуществления смартфон DB гражданина B содержит модуль связи CM(B), содержащий модуль оптического считывания OR(B) и, предпочтительно, модуль отображения DD(B). Указанный модуль оптического считывания OR(B) выполнен с возможностью считывания и декодирования оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB. Предпочтительно, модуль связи CM(B) выполнен с возможностью извлечения данных из блока графических данных GDB, таких как, например, указанное цифровое сообщение M из указанного QR-кода QRC(A).

[0219] Согласно варианту осуществления смартфон DB гражданина B может содержать конкретное программное обеспечение, выполненное с возможностью считывания, декодирования и извлечения такого цифрового сообщения M, предпочтительно, с использованием своего блока обработки CPU(B). Когда цифровое сообщение принимается модулем связи CM(B) смартфона DB гражданина B, то блок обработки CPU(B) проверяет достоверность цифрового сообщения M, а также его содержимое, т. е. ордер в этом примере.

[0220] Согласно предпочтительному варианту осуществления, когда гражданин B, т. е. контроллер B, принимает цифровое сообщение M, он верифицирует с использованием своего смартфона DB, т. е. своего блока обработки CPU(B), то, что цифровое сообщение M сертифицировано судьей C, т. е. контроллером C, и только в случае положительной верификации того, что цифровое сообщение M сертифицировано судьей C, блок обработки CPU(B) смартфона DB, т. е. устройства DB, начинает извлечение данных авторизации AD(A), содержащихся в цифровом сообщении M. Предпочтительно, эти данные авторизации AD(A) включают данные поставленной задачи.

[0221] Согласно варианту осуществления после верификации того, что цифровое сообщение M сертифицировано судьей C, блок обработки CPU(B) извлекает из цифрового сообщения M разные данные, такие как открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) сотрудника полиции A, ключ

верификации(A), данные, связанные с операцией Op, и, например, временной интервал, упомянутый в поставленной задаче.

[0222] Затем гражданин B отправляет запрос на связь сотруднику полиции A. Согласно варианту осуществления этот запрос на связь может быть случайным числом, таким как случайное число, придуманное на лету гражданином B. Предпочтительно, модуль связи CM(B) смартфона DB гражданина B отправляет запрос на связь на модуль связи CM(A) смартфона DA сотрудника полиции A.

[0223] Преимущественно, этот запрос на связь может быть случайным числом, сгенерированным модулем генерирования случайных чисел GRNM(B) смартфона DB гражданина B.

[0224] Согласно варианту осуществления модуль связи CM(B) смартфона DB гражданина B отправляет указанный запрос на связь на модуль связи CM(A) смартфона DA сотрудника полиции A с использованием сети связи CN, предпочтительно, с использованием сети связи ближнего радиуса действия, такой как, например, сеть связи Bluetooth.

[0225] Согласно варианту осуществления запрос на связь отправляется посредством электромагнитных волн от модуля связи CM(B) смартфона DB гражданина B на модуль связи CM(A) смартфона DA сотрудника полиции A.

[0226] Согласно варианту осуществления запрос на связь представлен в виде строки данных.

[0227] Согласно примеру этот запрос на связь может быть закодирован в виде оптического считываемого представления блока графических данных GDB(B); преимущественно, указанный блок графических данных GDB(B) может включать двумерный штрих-код, такой как, например, QR-код QRC(B). Согласно варианту осуществления такой блок графических данных GDB(B) также можно называть цифровой меткой DM(B).

[0228] Согласно варианту осуществления запрос на связь имеет машиночитаемую форму, например, такую как QR-код QRC(B).

[0229] Согласно варианту осуществления гражданин B показывает указанный QR-код QRC(B) сотруднику полиции A. Согласно варианту осуществления модуль связи CM(B) смартфона DB гражданина B, т. е. устройства DB, содержит модуль отображения DD(B) и, предпочтительно, модуль оптического считывания OR(B); указанный модуль отображения DD(B) выполнен с возможностью отображения оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB(B), такого как блок графических данных GDB(B), который включает закодированную версию запроса на связь, т. е., например, случайного числа, или в более общем смысле секрета. Таким образом, согласно варианту осуществления гражданин B использует свой смартфон для отображения QR-кода QRC(B), кодирующего указанный запрос на связь, с использованием указанного модуля отображения DD(B).

[0230] Затем сотрудник полиции A использует свой смартфон DA для оптического считывания указанного QR-кода QRC(B), отображаемого модулем отображения DD(B) смартфона DB гражданина B. Затем сотрудник полиции A использует свой смартфон DA для извлечения запроса на связь, т. е. секрета или, например, случайного числа, из указанного QR-кода QRC(B). Согласно варианту осуществления модуль связи CM(A) смартфона DA сотрудника полиции A содержит модуль оптического считывания OR(A) и, предпочтительно, модуль отображения DD(A). Указанный модуль оптического считывания OR(A) выполнен с возможностью считывания и декодирования оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB. Предпочтительно, модуль связи CM(A) выполнен с возможностью извлечения данных из блока графических данных GDB, таких как, например, указанный запрос на связь из указанного QR-кода QRC(B).

[0231] Согласно варианту осуществления смартфон DA сотрудника полиции A может содержать конкретное программное обеспечение, выполненное с возможностью считывания, декодирования, извлечения и, предпочтительно, подписывания указанного запроса на связь, предпочтительно, с использованием своего блока обработки CPU(A). Когда запрос на связь принимается модулем связи CM(A) смартфона DA сотрудника полиции A, то блок обработки CPU(A) подписывает указанный запрос на связь с использованием закрытого ключа PrK(A) сотрудника полиции A. Затем модуль связи CM(A) смартфона DA сотрудника полиции A отправляет подписанный запрос на связь в виде аккредитации SA гражданину, т. е. на модуль связи CM(B) смартфона гражданина B.

[0232] Согласно варианту осуществления модуль связи CM(A) смартфона DA сотрудника полиции A отправляет указанную аккредитацию SA на модуль связи CM(B) смартфона DB гражданина B с использованием сети связи CN, предпочтительно, с использованием сети связи ближнего радиуса действия, такой как, например, сеть связи Bluetooth.

[0233] Согласно варианту осуществления аккредитация SA отправляется посредством электромагнитных волн от модуля связи CM(A) смартфона DA сотрудника полиции A на модуль связи CM(B) смартфона DB гражданина B.

[0234] Согласно варианту осуществления аккредитация SA представлена в виде строки данных.

[0235] Согласно примеру эта аккредитация SA может быть закодирована в виде оптического считываемого представления блока графических данных GDB(A2); преимущественно, указанный блок графических данных GDB(A2) может включать двумерный штрих-код, такой как, например, QR-код QRC(A2). Согласно варианту осуществления такой блок графических данных GDB(A2) также можно называть цифровой меткой DM(A2).

[0236] Согласно предпочтительному варианту осуществления аккредитация SA имеет машиночитаемую форму, например, такую как QR-код QRC(A2).

[0237] Согласно варианту осуществления сотрудник полиции A показывает указанный QR-код QRC(A2) гражданину B. Согласно варианту осуществления сотрудник полиции A использует свой смартфон DA для отображения QR-кода QRC(A2), кодирующего указанную аккредитацию SA, с использованием указанного модуля отображения DD(A).

[0238] Затем гражданин B использует свой смартфон DB для оптического считывания указанного QR-кода QRC(A2), отображаемого модулем отображения DD(A) смартфона DB сотрудника полиции A. Затем гражданин B использует свой смартфон DB для извлечения аккредитации SA, т. е. подписанного запроса на связь, из указанного QR-кода QRC(A2) с использованием своего модуля оптического считывания OR(B). Предпочтительно, модуль связи CM(B) выполнен с возможностью извлечения данных из блока графических данных GDB, таких как, например, указанная аккредитация SA из указанного QR-кода QRC(A2).

[0239] Согласно варианту осуществления модуль связи CM(B) смартфона DB гражданина B считывает и декодирует этот QR-код QRC(A2) с использованием своего модуля оптического считывания OR(B) для извлечения указанной аккредитации SA.

[0240] Согласно варианту осуществления смартфон гражданина B может содержать конкретное программное обеспечение, выполненное с возможностью считывания, декодирования и/или извлечения указанной аккредитации SA, предпочтительно, с использованием своего блока обработки CPU(A). Когда аккредитация SA принимается модулем связи CM(B) смартфона DB гражданина B, то блок обработки CPU(B) проверяет аккредитацию SA, т. е. подписанный запрос на связь, и, в частности то, что он был подписан с помощью закрытого ключа PrK(A), соответствующего открытому ключу PuK(A), извлеченного из цифрового сообщения M, т. е. который находится в ордере.

[0241] Затем блок обработки CPU(B) смартфона DB гражданина B вычисляет с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A) и вычисляет потенциальную агрегированную цифровую подпись cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и блок обработки CPU(B) проверяет, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся в его памяти. Согласно варианту осуществления указанная агрегированная цифровая подпись ADS была принята гражданином B от указанного судьи C и/или от сервера. Согласно варианту осуществления, когда гражданин B считывает указанный QR-код QRC(A) с использованием своего смартфона DB, предпочтительно, через специальное приложение, то смартфон DB гражданина B связывается с сервером с использованием своего модуля связи CM(B) для загрузки указанной агрегированной цифровой подписи ADS. Затем указанная агрегированная цифровая подпись ADS была сохранена в памяти блока обработки CPU(B) смартфона DB гражданина B.

[0242] Согласно варианту осуществления смартфон DB гражданина B извлекает другие данные из цифрового сообщения M, такие как временной интервал, в течение которого должен работать сотрудник полиции A, как, например, с 15:00 до 18:30 11 июня 2021 года в этом примере.

[0243] Затем, если время надлежащим образом соответствует времени, упомянутому в поставленной задаче, например, с 15:00 до 18:30 11 июня 2021 года, если верификация аккредитации SA является положительной и если потенциальная агрегированная цифровая подпись cADS совпадает с агрегированной цифровой подписью ADS, гражданин B принимает от своего смартфона, предпочтительно, от блока обработки CPU(B) своего смартфона DB, указание о том, что сотрудник полиции A действительно уполномочен судьей C осуществлять операцию Op, упомянутую в ордере, содержащемся в цифровом

сообщении M. Следовательно, гражданин B может уполномочить сотрудника полиции A проникнуть в его дом по адресу Y для поиска доказательств.

[0244] Согласно этому примеру случая применения настоящего изобретения система предпочтительно содержит:

- смартфон DA сотрудника полиции A, причем указанный смартфон DA выполнен с возможностью обеспечения аутентификации сотрудника полиции A гражданином B, чтобы сотрудник полиции A мог выполнить операцию Op; указанный смартфон DA содержит блок обработки CPU(A) и модуль связи CM(A), содержащий модуль отображения DD(A) и модуль оптического считывания OR(A), причем указанный модуль отображения DD(A) выполнен с возможностью отображения оптического считываемого представления данных, преимущественно, оптического считываемого представления блока графических данных GDB(A); причем указанный блок графических данных GDB(A) включает закодированные данные, например, в виде QR-кода; причем указанный модуль оптического считывания OR(A) выполнен с возможностью считывания и декодирования оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB, и, преимущественно, извлечения данных из блока графических данных GDB;

- смартфон DB гражданина B, причем указанный смартфон выполнен с возможностью проверки полномочий заданного сотрудника полиции выполнять операцию Op, предпочтительно, в заданный временной интервал; указанный смартфон DB содержит блок обработки CPU(B) и модуль связи CM(B), содержащий модуль отображения DD(B) и модуль оптического считывания OR(A), причем указанный модуль отображения DD(B) выполнен с возможностью отображения оптического считываемого представления данных, преимущественно, оптического считываемого представления блока графических данных GDB(B); причем указанный блок графических данных GDB(B) включает закодированные данные, например, в виде QR-кода; причем указанный модуль

оптического считывания OR(B) выполнен с возможностью считывания и декодирования оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB, и, преимущественно, извлечения данных из блока графических данных GDB.

[0245] Эта система выполнена таким образом, что:

- модуль связи CM(B) выполнен с возможностью приема 200 цифрового сообщения M, содержащего поставленную задачу, причем указанная поставленная задача содержит открытый ключ PuK(A), принадлежащий сотруднику полиции A, данные авторизации AD(A), указывающие на то, что сотрудник полиции A уполномочен судьей C осуществлять операцию Op, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д.;

- предпочтительно, блок обработки CPU(B) выполнен с возможностью верификации 10b того, что цифровое сообщение M сертифицировано судьей C;

- блок обработки CPU(B) выполнен с возможностью извлечения 201, 202, 204 данных, содержащихся в цифровом сообщении M, таких как открытый ключ PuK(A), данные авторизации AD(A), операция Op, ключ верификации VK(A), временной интервал, в течение должна быть выполнена эта операция Op, и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано судьей C;

- модуль связи CM(B) выполнен с возможностью приема 400 аккредитации SA от модуля связи CM(A), предпочтительно, модуль оптического считывания OR(B) модуля связи CM(B) выполнен с возможностью считывания и декодирования оптического считываемого представления блока графических данных GDB(A), отображаемого модулем отображения DD(A); причем, предпочтительно, указанный блок графических данных GDB(A) включает закодированную версию аккредитации SA, преимущественно, в виде двумерного

штрих-кода, указанный модуль оптического считывания OR(B) выполнен с возможностью декодирования указанной закодированной версии аккредитации SA для извлечения указанной аккредитации SA; предпочтительно, указанная аккредитация SA подписывается 300a блоком обработки CPU(A) с использованием его закрытого ключа PrK(A) и/или содержит данные, такие как секрет, подписанные 300a блоком обработки CPU(A) с использованием его закрытого ключа PrK(A);

- блок обработки CPU(B) выполнен с возможностью верификации 400b аккредитации SA, предпочтительно, с использованием открытого ключа PuK(A), соответствующего указанному закрытому ключу PrK(A), преимущественно, после извлечения 202 указанного открытого ключа PuK(A) из цифрового сообщения M;

- блок обработки CPU(B) выполнен с возможностью:

- вычисления 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальной цифровой подписи cx(A) данных авторизации AD(A), и

- вычисления 205 потенциальной агрегированной цифровой подписи cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

- блок обработки CPU(B) выполнен с возможностью проверки 207 того, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся 206 в его памяти, и только в случае положительной верификации аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) выполнен с возможностью передачи 500 гражданину B указания о том, что сотрудник полиции A действительно уполномочен судьей C осуществлять 500a операцию Op.

[0246] Эта система позволяет гражданину B проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники. Более того, эта система позволяет гражданину B управлять учетными данными, т. е. поставленной задачей, связанной с этим цифровым содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет. Эта система позволяет сотруднику полиции A идентифицировать себя только с помощью аккредитации SA и своих учетных данных, которые содержатся в цифровом сообщении M и которые, предпочтительно, сертифицированы защищенным от подделки цифровым файлом, выданным контроллером C. Эта система позволяет гражданину B быть полностью уверенным в достоверности представленной поставленной задачи.

[0247] Следует отметить, что эта система позволяет избежать использования биометрических данных сотрудника полиции A. Поставленной задачи и аккредитации SA достаточно, чтобы предоставить полную уверенность гражданину B. Преимущественно, эта система позволяет избежать каких-либо биометрических данных, биометрического измерения или раскрытия частной информации в отношении сотрудника полиции A.

[0248] Согласно этому примеру случая применения настоящего изобретения согласно варианту осуществления настоящее изобретение относится к способу, в котором:

- смартфон DA сотрудника полиции A выполнен с возможностью обеспечения аутентификации сотрудника полиции A гражданином B, чтобы сотрудник полиции A мог выполнить операцию Op, предпочтительно, указанный смартфон DA содержит блок обработки CPU(A) и модуль связи CM(A), содержащий модуль отображения DD(A) и, предпочтительно, модуль оптического считывания OR(A); причем указанный модуль отображения DD(A) выполнен с возможностью отображения оптического считываемого представления данных, преимущественно, оптического считываемого представления блока графических данных GDB(A); причем указанный блок

графических данных GDB(A) включает закодированные данные, например, в виде QR-кода; причем указанный модуль оптического считывания OR(B) выполнен с возможностью считывания и декодирования оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB, и, преимущественно, извлечения данных из блока графических данных GDB;

- смартфон DB гражданина B выполнен с возможностью проверки полномочий заданного сотрудника полиции выполнять операцию Op, предпочтительно, в заданный временной интервал; смартфон DB гражданина B содержит блок обработки CPU(B) и модуль связи CM(B), содержащий модуль оптического считывания OR(B) и, предпочтительно, модуль отображения DD(B); причем указанный модуль оптического считывания OR(B) выполнен с возможностью считывания и декодирования оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB, и, преимущественно, извлечения данных из блока графических данных GDB; причем указанный модуль отображения DD(B) выполнен с возможностью отображения оптического считываемого представления данных, преимущественно, оптического считываемого представления блока графических данных GDB(B); причем указанный блок графических данных GDB(B) включает закодированные данные, например, в виде QR-кода.

[0249] Этот способ включает следующие этапы, на которых:

- модуль связи CM(B) принимает 200 цифровое сообщение M, содержащее поставленную задачу, причем указанная поставленная задача содержит открытый ключ PuK(A), принадлежащий сотруднику полиции A, данные авторизации AD(A), указывающие на то, что сотрудник полиции A уполномочен судьей C осуществлять операцию Op, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д.;

- предпочтительно, блок обработки CPU(B) верифицирует 10b то, что цифровое сообщение M сертифицировано судьей C;

- блок обработки CPU(B) устройства DB извлекает 201, 202, 204 данные, содержащиеся в цифровом сообщении M, такие как открытый ключ PuK(A), данные авторизации AD(A), операция Op, ключ верификации VK(A), временной интервал, в течение которого должна быть выполнена эта операция Op, и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано судьей C;

- модуль связи CM(B) принимает 400 аккредитацию SA от модуля связи CM(A), предпочтительно, модуль оптического считывания OR(B) модуля связи CM(B) устройства DB считывает и декодирует оптическое считываемое представление блока графических данных GDB(A), отображаемого модулем отображения DD(A); причем, предпочтительно, указанный блок графических данных GDB(A) включает закодированную версию аккредитации SA, преимущественно, в виде двумерного штрих-кода, указанный модуль оптического считывания OR(B) декодирует указанную закодированную версию аккредитации SA для извлечения указанной аккредитации SA; предпочтительно, указанная аккредитация SA подписывается 300a блоком обработки CPU(A) устройства DA с использованием его закрытого ключа PrK(A) и/или содержит данные, такие как секрет, подписанные 300a блоком обработки CPU(A) устройства DA с использованием его закрытого ключа PrK(A);

- блок обработки CPU(B) верифицирует 400b аккредитацию SA, предпочтительно, с использованием открытого ключа PuK(A), соответствующего указанному закрытому ключу PrK(A), преимущественно, после извлечения 202 указанного открытого ключа PuK(A) из цифрового сообщения M;

- блок обработки CPU(B):

- извлекает 204 ключ верификации VK(A), содержащийся в цифровом сообщении M,

- вычисляет 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A), и

- вычисляет 205 потенциальную агрегированную цифровую подпись cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

- блок обработки CPU(B) проверяет 207, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся 206 в его памяти, и только в случае положительной верификации аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) передает 500 на смартфон DB гражданина B указание о том, что сотрудник полиции A действительно уполномочен судьей C осуществлять 500a операцию Op.

[0250] Этот способ позволяет гражданину B проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники. Более того, этот способ позволяет гражданину B управлять учетными данными, т. е. поставленной задачей, связанной с этим цифровым содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет. Этот способ позволяет сотруднику полиции A идентифицировать себя только с помощью аккредитации SA и своих учетных данных, которые содержатся в цифровом сообщении M и которые, предпочтительно, сертифицированы защищенным от подделки цифровым файлом, выданным контроллером C. Этот способ позволяет гражданину B быть полностью уверенным в достоверности представленной поставленной задачи.

[0251] Следует отметить, что этот способ позволяет избежать использования биометрических данных сотрудника полиции A. Этого цифрового сообщения M и аккредитации SA достаточно, чтобы предоставить полную уверенность гражданину B. Преимущественно, этот способ позволяет избежать каких-либо биометрических данных, биометрического измерения или раскрытия частной информации сотрудника полиции A.

[0252] Согласно варианту осуществления настоящее изобретение позволяет сотруднику полиции A и гражданину B выполнять операцию Op без необходимости обращения к центральной базе данных или серверу, содержащему поставленную задачу. Действительно, гражданин B, а также сотрудник полиции A могут находиться в автономной среде до тех пор, пока они могут связываться друг с другом в ходе реализации способа согласно варианту осуществления настоящего изобретения, и, предпочтительно, до тех пор, пока контроллер B содержит агрегированную цифровую подпись ADS, например, ранее загруженную из контроллера C или с сервера. Преимущественно, отправка цифрового сообщения M сотруднику полиции A и гражданину B может быть реализована через незащищенные каналы.

[0253] Согласно варианту осуществления настоящее изобретение относится к реализации способа согласно настоящему изобретению в судебной среде, содержащей предыдущую систему согласно настоящему изобретению.

Выпуск официального цифрового документа государственным служащим

[0254] Согласно пятому примеру применения настоящего изобретения, проиллюстрированному на фиг. 6, настоящее изобретение можно реализовать для того, чтобы безопасно уполномочить государственного служащего выдавать официальный документ, предпочтительно, официальный цифровой документ, такой как, например, цифровое свидетельство о рождении. Настоящее изобретение позволяет лицу, например, получателю этого официального документа, верифицировать, предпочтительно, бесспорным способом, что этот

официальный документ был подписан уполномоченным государственным служащим по официальному поручению от уполномоченного органа.

[0255] Согласно этому примеру контроллером A является государственный служащий A. Государственный служащий A управляет устройством DA и содержит его, которое может быть, например, компьютером DA. Государственный служащий A должен выдавать официальный цифровой документ, например, диплом или свидетельство о рождении. Предпочтительно, этот официальный документ представлен в цифровой форме, такой как, например, документ в формате PDF. Этот официальный цифровой документ может содержать различную информацию, такую как имена, даты, места, подписи и т. д.

[0256] Предпочтительно, этот официальный цифровой документ подписывается государственным служащим A по официальному поручению от уполномоченного органа, например, Службы регистрации населения города. В этом случае применения указанный уполномоченный орган выполняет роль контроллера C. Государственный служащий A, т. е. контроллер A, содержит закрытый ключ PrK(A), предпочтительно, выданный контроллером A и связанный с открытым ключом PuK(A); причем указанный открытый ключ PuK(A) сертифицирован контроллером C, т. е., например, уполномоченным органом. Этот закрытый ключ PrK(A) хранится в памяти блока обработки CPU(A) устройства DA, т. е., например, компьютера DA государственного служащего A, предпочтительно, в защищенном анклаве памяти.

[0257] Согласно этому примеру контроллер B является гражданином B, и/или другим уполномоченным органом, и/или другим государственным служащим, который хочет проверить достоверность этого официального цифрового документа, т. е. который хочет верифицировать то, что этот официальный цифровой документ был выдан уполномоченным государственным служащим. В этом примере устройство DB может быть смартфоном гражданина B.

[0258] Согласно этому примеру контроллером C является уполномоченный орган C. Указанный уполномоченный орган C делегирует право подписывать официальный цифровой документ заданному государственному служащему. Уполномоченный орган C выдает поставленную задачу с использованием цифрового сообщения M, отправленного государственному служащему A, например, по сети связи CN, такой как Интернет. Например, это цифровое сообщение M может содержать и/или быть в виде оптического считываемого представления блока графических данных GDB(A); преимущественно, указанный блок графических данных GDB(A) может включать двумерный штрих-код, такой как, например, QR-код. Согласно варианту осуществления такой блок графических данных GDB(A) также можно называть цифровой меткой DM(A).

[0259] Согласно предпочтительному варианту осуществления цифровое сообщение M, содержащее поставленную задачу, имеет машиночитаемую форму, например, такую как QR-код.

[0260] Например, цифровое сообщение M может содержать поставленную задачу в виде ряда данных, указывающих на то, например, что государственному служащему A разрешено делать и когда государственному служащему A разрешено это делать. В этом примере поставленная задача может включать следующие данные:

- у государственного служащего A есть открытый ключ PuK(A);

- ключ верификации VK(A);

- операция Op: этот государственный служащий A уполномочен выдавать и подписывать официальные цифровые документы, такие как, например, цифровые свидетельства о рождении, по официальному поручению от уполномоченного органа C, например, от имени Службы регистрации населения города Утопия;

- временной интервал: это можно сделать с даты 1 по дату 2, например, в рабочее время.

[0261] Согласно варианту осуществления, когда государственный служащий A, т. е. контроллер A, принимает цифровое сообщение M от уполномоченного органа C, он верифицирует с использованием своего компьютера DA, т. е. блока обработки CPU(A) своего компьютера DA, то, что цифровое сообщение M сертифицировано уполномоченным органом C, т. е. контроллером C.

[0262] Например, когда государственный служащий A выдает официальный цифровой документ, такой как свидетельство о рождении, например, в виде документа в формате PDF, государственный служащий A прикрепляет цифровое сообщение M к официальному цифровому документу, предпочтительно, в виде QR-кода QRC(A).

[0263] Например, цифровое свидетельство о рождении выдается государственным служащим A, включая QR-код QRC(A), причем указанный QR-код QRC(A) кодирует указанное цифровое сообщение M.

[0264] Предпочтительно, государственный служащий A подписывает официальный цифровой документ с использованием своего закрытого ключа PrK(A). Эта цифровая подпись также прикрепляется к официальному цифровому документу и, предпочтительно, выполняет роль аккредитации SA. Согласно варианту осуществления государственный служащий A подписывает хеш-значение официального цифрового документа с использованием своего закрытого ключа PrK(A), причем указанное хеш-значение официального цифрового документа вычисляется с помощью односторонней функции, запрограммированной в блоке обработки CPU(A) и применяемой к по меньшей мере части содержимого указанного официального цифрового документа.

[0265] Когда получатель указанного официального цифрового документа, назовем его гражданином B, хочет проверить достоверность указанного

официального цифрового документа, гражданин B использует, например, свой смартфон DB, который выступает как устройство DB в этом примере.

[0266] Согласно варианту осуществления гражданин B использует свой смартфон DB для считывания и/или декодирования указанного цифрового сообщения M, прикрепленного и/или присоединенного к указанному официальному цифровому документу.

[0267] Согласно варианту осуществления гражданин B использует свой смартфон DB для считывания QR-кода QRC(A), прикрепленного и/или присоединенного к указанному официальному цифровому документу. Согласно варианту осуществления гражданин B использует свой смартфон DB для оптического считывания указанного QR-кода QRC(A), отображаемого, например, модулем отображения.

[0268] Предпочтительно, гражданин B использует свой смартфон DB для извлечения цифрового сообщения M, например, из указанного QR-кода QRC(A). Согласно варианту осуществления смартфон гражданина B содержит модуль связи CM(B), предназначенный для приема, считывания и/или декодирования указанного цифрового сообщения M.

[0269] Согласно варианту осуществления смартфон гражданина B содержит модуль связи CM(B), содержащий модуль оптического считывания OR(B) и, предпочтительно, модуль отображения DD(B). Указанный модуль оптического считывания OR(B) выполнен с возможностью считывания и декодирования оптического считываемого представления данных, предпочтительно, оптического считываемого представления блока графических данных GDB. Предпочтительно, модуль связи CM(B) выполнен с возможностью извлечения данных из блока графических данных GDB, таких как, например, указанное цифровое сообщение M из указанного QR-кода QRC(A).

[0270] Согласно варианту осуществления государственный служащий A отправляет официальный цифровой документ гражданину B. Предпочтительно,

указанный официальный цифровой документ отправляется с цифровым сообщением M и/или может содержать указанное цифровое сообщение M. Согласно другому варианту осуществления официальный цифровой документ и цифровое сообщение M отправляются отдельно государственным служащим A гражданину B.

[0271] Согласно варианту осуществления компьютер DA, т. е. устройство DA, содержит модуль связи CM(A), выполненный с возможностью отправки указанного официального цифрового документа и указанного цифрового сообщения M.

[0272] Согласно варианту осуществления смартфон DB гражданина B может содержать конкретное программное обеспечение, выполненное с возможностью считывания, декодирования и извлечения такого цифрового сообщения M, предпочтительно, с использованием своего блока обработки CPU(B), например, из QR-кода QRC(A). Когда цифровое сообщение M принимается и/или декодируется модулем связи CM(B) смартфона DB гражданина B, то блок обработки CPU(B) проверяет достоверность цифрового сообщения M, а также его содержимого, т. е. поставленной задачи в этом примере.

[0273] Согласно предпочтительному варианту осуществления, когда гражданин B, т. е. контроллер B, принимает официальный цифровой документ, содержащий цифровое сообщение M, гражданин B верифицирует с использованием своего смартфона DB, т. е. блока обработки CPU(B) своего смартфона DB, то, что цифровое сообщение M сертифицировано уполномоченным органом C, т. е. контроллером C, и, предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано уполномоченным органом C, блок обработки CPU(B) смартфона DB, т. е. устройства DB, начинает извлечение данных авторизации AD(A), содержащихся в цифровом сообщении M. Предпочтительно, эти данные авторизации AD(A) включают данные поставленной задачи.

[0274] Согласно варианту осуществления после верификации того, что цифровое сообщение M сертифицировано уполномоченным органом C, блок обработки CPU(B) извлекает из цифрового сообщения M разные данные, такие как открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) государственного служащего A, ключ верификации(A), данные, связанные с операцией Op, и, например, временной интервал, упомянутый в поставленной задаче.

[0275] Согласно варианту осуществления, когда гражданин B принимает официальный цифровой документ, содержащий цифровое сообщение M, он также принимает аккредитацию SA. Эта аккредитация SA может быть включена или не включена в официальный цифровой документ. Эта аккредитация SA включает подпись официального документа государственным служащим A с использованием его закрытого ключа PrK(A). Согласно предпочтительному варианту осуществления аккредитация SA включает подпись закодированной версии по меньшей мере части содержимого официального цифрового документа. Предпочтительно, указанная закодированная версия по меньшей мере части содержимого официального цифрового документа включает хеш-значение официального цифрового документа, вычисленное с помощью односторонней функции, запрограммированной в блоке обработки CPU(A) и применяемой к указанной по меньшей мере части содержимого указанного официального цифрового документа.

[0276] Согласно варианту осуществления после верификации того, что цифровое сообщение M сертифицировано уполномоченным органом C, гражданин B использует свой смартфон DB для верификации с использованием блока обработки CPU(B) аккредитации SA, предпочтительно, для проверки, если аккредитация SA, т. е. хеш-значение по меньшей мере части содержимого официального цифрового документа, была подписана с помощью закрытого ключа PrK(A), соответствующего открытому ключу PuK(A), извлеченного из цифрового сообщения M, и, предпочтительно, что указанное хеш-значение соответствует хеш-значению официального цифрового документа или по

меньшей мере части официального цифрового документа, вычисленному с помощью одной и той же односторонней функции, причем указанная односторонняя функция запрограммирована в блоке обработки CPU(B).

[0277] Согласно варианту осуществления смартфон DB проверяет аккредитацию SA с использованием своего блока обработки CPU(B) путем проверки того, что хеш-значение официального цифрового документа было подписано с помощью закрытого ключа PrK(A), соответствующего открытому ключу PuK(A), извлеченного из цифрового сообщения M, и путем проверки того, что указанное хеш-значение соответствует хеш-значению официального цифрового документа, вычисленному с помощью односторонней функции, причем указанная односторонняя функция запрограммирована в блоке обработки CPU(B) и идентична односторонней функции, запрограммированной в блоке обработки CPU(A).

[0278] Согласно варианту осуществления односторонняя функция была отправлена на устройство DA и на устройство DB контроллером C.

[0279] Согласно варианту осуществления модуль связи CM(A) отправляет указанную аккредитацию SA на модуль связи CM(B) с использованием сети связи CN, предпочтительно, с использованием сети связи Интернет.

[0280] Согласно варианту осуществления аккредитация SA отправляется по Интернету от модуля связи CM(A) на модуль связи CM(B).

[0281] Согласно варианту осуществления аккредитация SA представлена в виде строки данных.

[0282] Согласно примеру эта аккредитация SA может быть закодирована в виде оптического считываемого представления блока графических данных GDB(A2); преимущественно, указанный блок графических данных GDB(A2) может включать двумерный штрих-код, такой как, например, QR-код QRC(A2). Согласно варианту осуществления такой блок графических данных GDB(A2) также можно называть цифровой меткой DM(A2).

[0283] Согласно предпочтительному варианту осуществления аккредитация SA имеет машиночитаемую форму, например, такую как QR-код.

[0284] Согласно варианту осуществления гражданин B может использовать свой смартфон DB для оптического считывания указанного QR-кода QRC(A2), связанного с официальным цифровым документом. Затем гражданин B использует свой смартфон DB для извлечения аккредитации SA из указанного QR-кода QRC(A2) с использованием своего модуля оптического считывания OR(B). Предпочтительно, модуль связи CM(B) выполнен с возможностью извлечения данных из блока графических данных GDB, таких как, например, указанная аккредитация SA из указанного QR-кода QRC(A2).

[0285] Согласно варианту осуществления модуль связи CM(B) смартфона DB гражданина B считывает и декодирует этот QR-код QRC(A2) с использованием своего модуля оптического считывания OR(B) для извлечения указанной аккредитации SA.

[0286] Согласно варианту осуществления смартфон DB гражданина B может содержать конкретное программное обеспечение, выполненное с возможностью считывания, декодирования и извлечения такой аккредитации SA, предпочтительно, с использованием своего блока обработки CPU(A). Когда аккредитация SA принимается модулем связи CM(B) смартфона DB гражданина B, то блок обработки CPU(B) проверяет аккредитацию SA, и, в частности то, что он был подписан с помощью закрытого ключа PrK(A), соответствующего открытому ключу PuK(A), извлеченного из цифрового сообщения M, и что подписанное хеш-значение, содержащееся в аккредитации SA, соответствует хеш-значению официального цифрового документа, вычисленному с помощью односторонней функции.

[0287] Затем блок обработки CPU(B) смартфона DB гражданина B вычисляет с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A) и вычисляет потенциальную агрегированную цифровую подпись cADS из ключа

верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и блок обработки CPU(B) проверяет, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся в его памяти. Согласно варианту осуществления указанная агрегированная цифровая подпись ADS была принята гражданином B от указанного уполномоченного органа C и/или от сервера.

[0288] Согласно варианту осуществления, когда гражданин B принимает указанное цифровое сообщение M, то смартфон DB гражданина B связывается с сервером с использованием своего модуля связи CM(B) для загрузки указанной агрегированной цифровой подписи ADS.

[0289] Согласно варианту осуществления, когда гражданин B считывает указанный QR-код QRC(A) с использованием своего смартфона DB, предпочтительно, через специальное приложение, то смартфон DB гражданина B связывается с сервером с использованием своего модуля связи CM(B) для загрузки указанной агрегированной цифровой подписи ADS.

[0290] Предпочтительно, указанная агрегированная цифровая подпись ADS сохраняется в памяти блока обработки CPU(B) смартфона гражданина B.

[0291] Согласно варианту осуществления смартфон DB гражданина B извлекает другие данные из цифрового сообщения M, такие как временной интервал, в течение которого государственный служащий A имеет право работать, как, например, с даты 1 по дату 2, в рабочее время в этом примере.

[0292] Затем, если время соответствует временному интервалу, упомянутому в поставленной задаче, например, с даты 1 по дату 2, в рабочее время, если верификация аккредитации SA является положительной и если потенциальная агрегированная цифровая подпись cADS совпадает с агрегированной цифровой подписью ADS, гражданин B принимает от своего смартфона, предпочтительно, от блока обработки CPU(B) своего смартфона, указание о том, что государственный служащий A действительно уполномочен уполномоченным

органом C осуществлять операцию Op, упомянутую в поставленной задаче, содержащейся в цифровом сообщении M. Следовательно, это означает, что официальный документ был надлежащим образом выдан государственным служащим, имеющим на это полномочия, выданные уполномоченным органом C.

[0293] Согласно этому примеру случая применения настоящего изобретения система предпочтительно содержит:

- компьютер DA государственного служащего A, причем указанный компьютер DA выполнен с возможностью выдачи официального цифрового документа, такого как свидетельство о рождении, например, в виде документа в формате PDF, и прикрепления цифрового сообщения M к официальному цифровому документу, необязательно, в виде QR-кода QRC(A), и генерирования аккредитации SA путем подписывания официального цифрового документа с использованием закрытого ключа PrK(A) государственного служащего A, и, предпочтительно, путем подписывания с использованием закрытого ключа PrK(A) в виде отпечатка пальца / хеш-значения официального цифрового документа, вычисленного с помощью специальной односторонней функции, запрограммированной в блоке обработки CPU(A); указанный компьютер DA содержит модуль связи CM(A);

- смартфон DB гражданина B, причем указанный смартфон выполнен с возможностью верификации того, что заданный официальный цифровой документ был надлежащим образом выдан государственным служащим, имеющим на это полномочия, выданные уполномоченным органом C, предпочтительно, в заданный временной интервал; указанный смартфон DB содержит блок обработки CPU(B) и модуль связи CM(B), предпочтительно, указанный модуль связи CM(B) может содержать модуль оптического считывания OR(B) и, предпочтительно, модуль отображения DD(B); причем указанный модуль оптического считывания OR(B) выполнен с возможностью считывания и декодирования оптического считываемого представления данных,

предпочтительно, оптического считываемого представления блока графических данных GDB и, преимущественно, извлечения данных из блока графических данных GDB.

[0294] Эта система выполнена таким образом, что:

- смартфон DB гражданина B выполнен с возможностью приема официального цифрового документа, содержащего цифровое сообщение M, причем указанное цифровое сообщение M содержит поставленную задачу, причем указанная поставленная задача содержит открытый ключ PuK(A), принадлежащий государственному служащему A, данные авторизации AD(A), указывающие на то, что государственный служащий A уполномочен уполномоченным органом C осуществлять операцию Op, ключ верификации VK(A), временной интервал, в течение которого можно выполнять эту операцию Op, и т. д.;

- предпочтительно, блок обработки CPU(B) выполнен с возможностью верификации 10b того, что цифровое сообщение M сертифицировано уполномоченным органом C;

- блок обработки CPU(B) выполнен с возможностью извлечения 201, 202, 204 данных, содержащихся в цифровом сообщении M, таких как открытый ключ PuK(A), данные авторизации AD(A), операция Op, ключ верификации VK(A), временной интервал, в течение которого можно выполнять эту операцию Op, и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано уполномоченным органом C;

- модуль связи CM(B) выполнен с возможностью приема аккредитации SA от государственного служащего A, предпочтительно, прикрепленной к официальному цифровому документу, причем указанная аккредитация SA соответствует подписи 300a официального цифрового документа, предпочтительно, подписи хеш-значения по меньшей мере части содержимого официального цифрового документа, вычисленного с использованием

односторонней функции, запрограммированной в блоке обработки CPU(A), блоком обработки CPU(A) с использованием его закрытого ключа PrK(A);

- блок обработки CPU(B) выполнен с возможностью верификации 400a аккредитации SA, предпочтительно, с использованием открытого ключа PuK(A), соответствующего указанному закрытому ключу PrK(A), преимущественно, после извлечения 202 указанного открытого ключа PuK(A) из цифрового сообщения M и, предпочтительно, с использованием указанной односторонней функции, запрограммированной в блоке обработки CPU(B), для верификации указанного хеш-значения;

- блок обработки CPU(B) выполнен с возможностью:

- вычисления 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальной цифровой подписи cx(A) данных авторизации AD(A), и

- вычисления 205 потенциальной агрегированной цифровой подписи cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

- блок обработки CPU(B) выполнен с возможностью проверки 207 того, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся 206 в его памяти, и только в случае положительной верификации аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) выполнен с возможностью передачи 500 гражданину B указания о том, что государственный служащий A был действительно уполномочен уполномоченным органом C осуществлять 500a операцию Op.

[0295] Эта система позволяет гражданину B проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники. Более того, эта система позволяет

гражданину B управлять учетными данными, т. е. поставленной задачей, связанной с этим цифровым содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет, даже если государственный служащий A находится на расстоянии от гражданина B. Эта система позволяет государственному служащему A идентифицировать себя только с помощью аккредитации SA и своих учетных данных, которые содержатся в цифровом сообщении M и которые, предпочтительно, сертифицированы защищенным от подделки цифровым файлом, выданным контроллером C. Эта система позволяет гражданину B быть полностью уверенным в достоверности официального документа, который был выдан.

[0296] Согласно этому примеру случая применения настоящего изобретения согласно варианту осуществления настоящее изобретение относится к способу, в котором:

- компьютер DA государственного служащего A выполнен с возможностью выдачи официального цифрового документа, такого как свидетельство о рождении, например, в виде документа в формате PDF, и прикрепления цифрового сообщения M к официальному цифровому документу, необязательно, в виде QR-кода QRC(A), и генерирования аккредитации SA путем подписывания официального цифрового документа с использованием закрытого ключа PrK(A) государственного служащего A, и, предпочтительно, путем подписывания с использованием закрытого ключа PrK(A) в виде отпечатка пальца / хеш-значения официального цифрового документа, вычисленного с помощью специальной односторонней функции, запрограммированной в блоке обработки CPU(A); указанный компьютер DA содержит модуль связи CM(A);

- смартфон DB гражданина B выполнен с возможностью верификации того, что заданный официальный цифровой документ был надлежащим образом выдан государственным служащим, имеющим на это полномочия, выданные уполномоченным органом C, предпочтительно в заданный временной интервал; указанный смартфон DB содержит блок обработки CPU(B) и модуль связи

CM(B), предпочтительно указанный модуль связи CM(B) может содержать модуль оптического считывания OR(B) и предпочтительно модуль отображения DD(B); причем указанный модуль оптического считывания OR(B) выполнен с возможностью считывания и декодирования оптически считываемого представления данных, предпочтительно оптически считываемого представления блока графических данных GDB и преимущественно для извлечения данных из блока графических данных GDB.

[0297] Этот способ включает следующие этапы, на которых:

- смартфон DB гражданина B принимает 200 официальный цифровой документ, содержащий цифровое сообщение M, причем указанное цифровое сообщение M содержит поставленную задачу, причем указанная поставленная задача содержит открытый ключ PuK(A), принадлежащий государственному служащему A, данные авторизации AD(A), указывающие на то, что государственный служащий A уполномочен уполномоченным органом C осуществлять операцию Op, ключ верификации VK(A), временной интервал, в течение которого можно выполнять эту операцию Op, и т. д.;

- предпочтительно, блок обработки CPU(B) верифицирует 10b то, что цифровое сообщение M сертифицировано уполномоченным органом C;

- блок обработки CPU(B) извлекает 201, 202, 204 данные, содержащиеся в цифровом сообщении M, такие как открытый ключ PuK(A), данные авторизации AD(A), операция Op, ключ верификации VK(A), временной интервал, в течение которого можно выполнять эту операцию Op, и т. д., предпочтительно, только в случае положительной верификации того, что цифровое сообщение M сертифицировано уполномоченным органом C;

- модуль связи CM(B) принимает аккредитацию SA от государственного служащего A, предпочтительно, прикрепленную к официальному цифровому документу, причем указанная аккредитация SA соответствует подписи 300a официального цифрового документа, предпочтительно, подписи хеш-значения

по меньшей мере части содержимого официального цифрового документа, вычисленного с использованием односторонней функции, запрограммированной в блоке обработки CPU(A), блоком обработки CPU(A) с использованием его закрытого ключа PrK(A);

○ блок обработки CPU(B) верифицирует 400a аккредитацию SA, предпочтительно, с использованием открытого ключа PuK(A), соответствующего указанному закрытому ключу PrK(A), преимущественно, после извлечения 202 указанного открытого ключа PuK(A) из цифрового сообщения M и, предпочтительно, с использованием указанной односторонней функции, запрограммированной в блоке обработки CPU(B), для верификации указанного хеш-значения;

○ блок обработки CPU(B):

- извлекает 204 ключ верификации VK(A), содержащийся в цифровом сообщении M,

- вычисляет 203 с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A), и

- вычисляет 205 потенциальную агрегированную цифровую подпись cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

○ блок обработки CPU(B) проверяет 207, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся 206 в его памяти, и только в случае положительной верификации аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) передает 500 гражданину B указание о том, что государственный служащий A был действительно уполномочен уполномоченным органом C осуществлять 500a операцию Op.

[0298] Этот способ позволяет гражданину B проверять достоверность цифрового содержимого цифрового сообщения M с большей уверенностью, чем решения предшествующего уровня техники. Более того, этот способ позволяет гражданину B управлять учетными данными, т. е. поставленной задачей, связанной с этим цифровым содержимым, чтобы проверить, является ли это цифровое содержимое достоверным или нет, даже если государственный служащий A находится на расстоянии от гражданина B. Этот способ позволяет государственному служащему A идентифицировать себя только с помощью аккредитации SA и своих учетных данных, которые содержатся в цифровом сообщении M и которые, предпочтительно, сертифицированы защищенным от подделки цифровым файлом, выданным контроллером C. Этот способ позволяет гражданину B быть полностью уверенным в достоверности официального документа, который был выдан.

[0299] Согласно варианту осуществления настоящее изобретение позволяет государственному служащему A и гражданину B выполнять операцию Op без необходимости обращения к центральной базе данных или серверу, содержащему поставленную задачу. Действительно, гражданин B, а также государственный служащий A могут находиться в автономной среде до тех пор, пока они могут связываться друг с другом в ходе реализации способа согласно варианту осуществления настоящего изобретения, и, предпочтительно, до тех пор, пока контроллер B содержит агрегированную цифровую подпись ADS, например, ранее загруженную из контроллера C или с сервера. Преимущественно, отправка цифрового сообщения M государственному служащему A и отправка официального документа гражданину B может быть реализована через незащищенные каналы.

[0300] Согласно варианту осуществления настоящее изобретение относится к реализации способа согласно настоящему изобретению в административной среде, содержащей предыдущую систему согласно настоящему изобретению.

Защищенный от подделки цифровой файл

[0301] Как описано ранее, согласно предпочтительному варианту осуществления контроллер C может выдавать цифровое сообщение M в виде защищенного от подделки цифрового файла, что позволяет контроллеру B быть полностью уверенным в достоверности представленного цифрового сообщения M.

[0302] Для генерирования указанного цифрового сообщения M в виде защищенного от подделки цифрового файла можно использовать несколько способов.

[0303] Согласно предпочтительному варианту осуществления в настоящем изобретении используют способ защиты нескольких элементов и соответственных связанных с ними цифровых данных, используя дерево цифровых подписей элементов. Эти элементы могут быть нескольких видов, например, данные авторизации AD, т. е., например, поставленные задачи. Соответственные связанные с ними цифровые данные могут включать несколько видов данных, таких как, например, подробности поставленной задачи, идентификаторы контроллеров, открытый ключ PuK, подробности операции и т. д. Предпочтительно, по меньшей мере один из элементов представляет собой поставленную задачу.

[0304] На фиг. 7 показан пакет из восьми элементов $A_1,\ldots,A_8$ и проиллюстрирован указанный способ генерирования цифрового сообщения M в виде защищенного от подделки цифрового файла путем защиты элементов $A_1,\ldots,A_8$ и соответственных связанных с ними цифровых данных $D_1,\ldots D_8$ посредством дерева цифровых подписей элементов. Защищенный элемент может представлять собой цифровое сообщение M. Эти элементы могут содержать, например, один или несколько данных авторизации AD, т. е. поставленные задачи. Согласно варианту осуществления один из этих элементов может содержать поставленную задачу, причем указанный элемент, когда он защищен, может образовывать по меньшей мере часть указанного цифрового сообщения M. Хорошо известны деревья, связанные с цифровыми подписями

(двоичные хеш-деревья, n-арные хеш-деревья или деревья Меркла), они обычно имеют базовые узлы или листовые узлы, которые используются для создания узлов следующего (промежуточного) уровня путем цифрового подписывания конкатенации цифровых подписей, связанных с листовыми узлами согласно определенной группировке листовых узлов. В случае двоичного дерева цифровые подписи, связанные с узлами первого промежуточного уровня, соответственно вычисляют путем цифрового подписывания (например, с помощью односторонней хеш-функции H или односторонней функции эллиптической кривой и т. д.) конкатенации цифровых подписей, связанных с двумя последовательными листовыми узлами. В случае n-арного дерева значения узлов первого промежуточного уровня получают путем конкатенации значений n последовательных листовых узлов. Дерево также может иметь более сложную структуру (смешанные деревья), так как конкатенацию листовых узлов можно осуществлять парами последовательных узлов для определенных листовых узлов, тройкой узлов для других последовательных листовых узлов и т. д.

[0305] Из соображений упрощения, простое двоичное дерево с восемью листовыми узлами показано на фиг. 7: соответственные значения восьми листовых узлов a(1,1),…,a(1,8) дерева, соответственно, соответствуют цифровым подписям элементов $x_1=H(D_1)$,…, $x_8=H(D_8)$. Значение первого индекса, т. е. «1», для всех листовых узлов указывает на первый уровень (или базовый уровень) дерева, а второй индекс, идущий от 1 до 8, указывает на упорядоченность (листовых) узлов дерева. Значения узлов (отличных от листовых) следующего уровня, т. е. четырех узлов второго уровня a(2,1), a(2,2), a(2,3) и a(2,4), получают путем цифрового подписывания конкатенации (символически представленной оператором «+»), в данном случае посредством хеш-функции, значений пар листовых узлов, т. е. пар их дочерних узлов в дереве. Эта группировка дочерних узлов для получения значений узлов следующего уровня определяет упорядоченность конкатенации дерева. Для упрощения обозначений авторы используют символ узла a(i,j), чтобы также представлять связанное с ним значение (т. е. связанную с ним цифровую подпись). В данном случае дерево

имеет только два промежуточных уровня выше уровня листовых узлов и корневой узел на верхнем уровне. Уровень корневого узла фактически является последним уровнем узла, отличного от листового, дерева. Таким образом, значения четырех узлов, отличных от листовых, следующего промежуточного уровня представляют собой:

- a(2,1)=H(a(1,1)+a(1,2)), т. е. a(2,1)=H(H(D1)+ H(H(D2)), (где a(1,1) и a(1,2) представляют собой дочерние узлы узла a(2,1))
- a(2,2)=H(a(1,3)+a(1,4))
- a(2,3)=H(a(1,5)+a(1,6))
- a(2,4)=H(a(1,7)+a(1,8))

и для следующего, предпоследнего, уровня узлов (в данном случае третьего уровня) представлены два значения узлов:

- a(3,1)=H(a(2,1)+a(2,2))
- a(3,2)=H(a(2,3)+a(2,4)).

[0306] Авторы отмечают, что для каждого узла, отличного от листового, можно выбрать другую упорядоченность конкатенации дерева: например, вместо значения a(2,4)=H(a(1,7)+a(1,8)), авторы определяют значение a(2,4)=H(a(1,8)+a(1,7)), что приводит к другому значению узла.

[0307] Наконец, значение корневого узла R дерева или контрольную корневую цифровую подпись или также называемую агрегированной цифровой подписью ADS, раскрытой ранее, получают следующим образом: R=H(a(3,1)+a(3,2)).

[0308] Из-за каскада конкатенаций, задействованных в дереве, практически невозможно извлечь корневое значение, в случае изменения какого-либо бита цифровых данных в узле (в частности, в листовом узле). Более того, если в пакет включены некоторые конкретные элементы (цифровые данные которых

известны только системе, создающей цифровые подписи листовых узлов дерева, т. е. известны только контроллеру C), фальшивомонетчик не сможет получить корневую цифровую подпись, даже зная цифровые данные всех элементов пакета.

[0309] Согласно настоящему изобретению контрольная корневая цифровая подпись R, т. е. агрегированная цифровая подпись ADS, пакета элементов более не подлежит изменению и, следовательно, защищена от подделки, ввиду ее публикации в (общедоступной) среде, открытой для пользователя, который должен проверить аутентичность элемента, т. е. данных авторизации AD, т. е. поставленной задачи (или связанных с ними данных), или ее хранения в доступной для поиска корневой базе данных, открытой для контроллера, или, в предпочтительном варианте – ее хранения в блокчейне или, предпочтительно, в базе данных, защищенной блокчейном, открытой для контроллера. Затем контроллер может сохранить контрольное значение R, полученное из этих доступных источников.

[0310] Для каждого элемента A_i пакета соответствующий ключ верификации элемента VK_i (или путь верификации) связанного дерева затем вычисляют как последовательность соответственных цифровых подписей, начиная от уровня листовых узлов до предпоследнего уровня узлов, каждого другого листового узла, имеющего такой же родительский узел в дереве, что и листовой узел, соответствующий цифровой подписи элемента, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский узел в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне.

[0311] Согласно варианту осуществления по меньшей мере один из элементов A_i содержит поставленную задачу, т. е. данные авторизации AD, указанные данные авторизации AD указывают на то, контроллер A устройства DA уполномочен контроллером C осуществлять операцию Op с контроллером, устройство

которого принимает указанное цифровое сообщение M, например, с контроллером B.

[0312] Предпочтительно, связанные цифровые данные D_i по меньшей мере одного элемента A_i включают данные авторизации AD, указывающие на то, что контроллер A устройства DA уполномочен контроллером C осуществлять операцию Op с контроллером, устройство которого принимает указанное цифровое сообщение M, например, с контроллером B.

[0313] Как будет описано далее, настоящее изобретение позволяет контроллеру C выдавать цифровое сообщение M в виде защищенного от подделки файла, содержащего:

- указанные данные авторизации AD_i, т. е. элемент A_i;

- ключ верификации VK_i, связанный с данными авторизации AD_i, т. е. элементом A_i

[0314] Преимущественно, указанный ключ верификации VK_i вместе с данными авторизации AD_i позволяет извлекать агрегированную цифровую подпись ADS, которую можно хранить, например, в памяти блока обработки CPU устройства DB контроллера B.

[0315] Согласно варианту осуществления каждый элемент A_i пакета элементов A_i может соответствовать данным авторизации AD_i. Действительно, контроллер C, выдающий несколько цифровых сообщений M_i в отношении разных контроллеров и, следовательно, разные поставленные задачи, может создавать это дерево с использованием нескольких данных авторизации AD_i, необязательно, контроллер C может использовать любой вид данных до тех пор, пока хотя бы один из элементов относится к данным авторизации AD_i.

[0316] В примере на фиг. 7 представлены восемь ключей верификации $VK_1,\ldots,VK_8$, соответственно, соответствующих восьми элементам $A_1,\ldots,A_8$ пакета и их соответствующим восьми листовым узлам a(1,1),…,a(1,8):

1) для листового узла $a(1,1)=x_1=H(D_1)$, соответствующего элементу A_1, ключ верификации представляет собой $VK_1=\{a(1,2),a(2,2),a(3,2)\}$, из которого можно извлечь значение корневой цифровой подписи R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

a) из листового узла $a(1,1)=x_1$ и листового узла $a(1,2)=x_2$ в VK_1 ($a(1,2)$ представляет собой другой листовой узел, имеющий такой же родительский узел, т. е. узел $a(2,1)$, что и листовой узел, соответствующий цифровой подписи элемента x_1, т. е. узел $a(1,1)$), получают значение родительского узла $a(2,1)$ посредством $a(2,1)=H(a(1,1)+a(1,2))$ (т. е. $a(2,1)=H(x_1 + x_2)$),

b) из полученного $a(2,1)$ и значения следующего узла в VK_1, т. е. $a(2,2)$ следующего уровня узлов, отличных от листовых, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т. е. узел $a(3,1)$, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т. е. узел $a(2,1)$, получают значение родительского узла $a(3,1)$ посредством $a(3,1)=H(a(2,1)+a(2,2))$,

c) из полученного $a(3,1)$ и значения следующего узла в VK_1, т. е. $a(3,2)$ предпоследнего уровня узлов, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т. е. корневой узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т. е. узел $a(3,1)$, получают значение корневого узла R посредством $R=H(a(3,1)+a(3,2))$.

В этом примере представлено три этапа a), b) и c), поскольку дерево имеет три уровня ниже уровня корневых узлов и, таким образом, ключ верификации содержит три значения узлов. Таким образом, значение корневого узла дерева можно получить следующим образом: $R=H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2))$.

2) для листового узла $a(1,2)=x_2=H(D_2)$, соответствующего элементу A_2, ключ верификации представляет собой $VK_2=\{a(1,1),a(2,2),a(3,2)\}$, из которого можно

извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

a) из $a(1,2)=x_2$ и $a(1,1)=x_1$ в VK_1 ($a(1,1)$ представляет собой другой листовой узел, имеющий такой же родительский узел, т. е. узел $a(2,1)$, что и листовой узел, соответствующий цифровой подписи элемента x_2, т. е. узел $a(1,2)$), получают значение родительского узла $a(2,1)$ посредством $a(2,1)=H(a(1,1)+a(1,2))$,

b) из полученного $a(2,1)$ и значения следующего узла в VK_2, т. е. $a(2,2)$ следующего уровня узлов, отличных от листовых, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т. е. узел $a(3,1)$, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т. е. узел $a(2,1)$, получают значение родительского узла $a(3,1)$ посредством $a(3,1)=H(a(2,1)+a(2,2))$,

c) из полученного $a(3,1)$ и значения следующего узла в VK_2, т. е. $a(3,2)$ предпоследнего уровня узлов, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т. е. корневой узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т. е. узел $a(3,1)$, получают значение корневого узла R посредством $R=H(a(3,1)+a(3,2))$.

Таким образом, значение корневого узла дерева можно получить следующим образом: $R=H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2))$.

3) для листового узла $a(1,3)=x_3=H(D3)$, соответствующего элементу A_3, ключ верификации представляет собой $VK_3=\{a(1,4),a(2,1),a(3,2)\}$, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

a) из $a(1,3)=x_3$ и $a(1,4)=x_4$ в VK_3 ($a(1,4)$ представляет собой другой листовой узел, имеющий такой же родительский узел, т. е. узел $a(2,2)$, что и листовой узел,

соответствующий цифровой подписи элемента x3, т. е. узел a(1,3)), получают значение родительского узла a(2,2) посредством a(2,2)=H(a(1,3)+a(1,4)),

b) из полученного a(2,2) и значения следующего узла в VK_3, т. е. a(2,1) следующего уровня узлов, отличных от листовых, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т. е. узел a(3,1), что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т. е. узел a(2,2), получают значение родительского узла a(3,1) посредством a(3,1)=H(a(2,1)+a(2,2)),

c) из полученного a(3,1) и значения следующего узла в VK_3, т. е. a(3,2) предпоследнего уровня узлов, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т. е. корневой узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т. е. узел a(3,1), получают значение корневого узла R посредством R=H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить следующим образом: R=H(H(a(2,1)+H(a(1,3)+a(1,4)))+a(3,2)).

4) для листового узла $a(1,4)=x_4=H(D_4)$, соответствующего элементу A_4, ключ верификации представляет собой VK_4={a(1,3),a(2,1),a(3,2)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

a) из $a(1,4)=x_4$ и $a(1,3)=x_3$ в VK_4 получают значение родительского узла a(2,2) посредством a(2,2)=H(a(1,3)+a(1,4)),

b) из полученного a(2,2) и значения следующего узла в VK_4, т. е. a(2,1) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,1) посредством a(3,1)=H(a(2,1)+a(2,2)),

c) из полученного a(3,1) и значения следующего узла в VK_4, т. е. a(3,2) предпоследнего уровня узлов, получают значение корневого узла R посредством R=H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить следующим образом: R=H(H(a(2,1)+H(a(1,3)+a(1,4)))+a(3,2)).

5) для узла $a(1,5)=x_5=H(D_5)$, соответствующего элементу A_5, ключ верификации представляет собой VK_5={a(1,6),a(2,4),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

a) из $a(1,5)=x_5$ и $a(1,6)=x_6$ в VK_5 получают значение родительского узла a(2,3) посредством a(2,3)=H(a(1,5)+a(1,6)),

b) из полученного a(2,3) и значения следующего узла в VK_5, т. е. a(2,4) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2)=H(a(2,3)+a(2,4)),

c) из полученного a(3,2) и значения следующего узла в VK_5, т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R=H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить следующим образом: R=H(a(3,1)+H(H(a(1,5)+a(1,6))+a(2,4))).

6) для узла $a(1,6)=x_6=H(D_6)$, соответствующего элементу A_6, ключ верификации представляет собой k6={a(1,5),a(2,4),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

a) из $a(1,6)=x_6$ и $a(1,5)=x_5$ в VK_6 получают значение родительского узла a(2,3) посредством a(2,3)=H(a(1,5)+a(1,6)),

b) из полученного a(2,3) и значения следующего узла в VK_6, т. е. a(2,4) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2)=H(a(2,3)+a(2,4)),

c) из полученного a(3,2) и значения следующего узла в VK_6, т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R=H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить следующим образом: R=H(a(3,1)+H(H(a(1,5)+a(1,6))+a(2,4))).

7) для узла $a(1,7)=x_7=H(D_7)$, соответствующего элементу A_7, ключ верификации представляет собой k7={a(1,8),a(2,3),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

a) из $a(1,7)=x_7$ и $a(1,8)=x_8$ в VK_7 получают значение родительского узла a(2,4) посредством a(2,4)=H(a(1,7)+a(1,8)),

b) из полученного a(2,4) и значения следующего узла в VK_7, т. е. a(2,3) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2)=H(a(2,3)+a(2,4)),

c) из полученного a(3,2) и значения следующего узла в VK_7, т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R=H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить следующим образом: R=H(a(3,1)+H(a(2,3)+H(a(1,7)+a(1,8)))).

8) для узла $a(1,8)=x_8=H(D_8)$, соответствующего элементу A_8, ключ верификации представляет собой k8={a(1,7),a(2,3),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных

согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

a) из $a(1,8)=x_8$ и $a(1,7)=x_7$ в VK_8 получают значение родительского узла a(2,4) посредством a(2,4)=H(a(1,7)+a(1,8)),

b) из полученного a(2,4) и значения следующего узла в VK_8, т. е. a(2,3) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2)=H(a(2,3)+a(2,4)),

c) из полученного a(3,2) и значения следующего узла в VK_8, т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R=H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить следующим образом: R=H(a(3,1)+H(a(2,3)+H(a(1,7)+a(1,8)))).

[0317] Как правило, для извлечения (потенциального) значения корневого узла, т. е. потенциальной агрегированной цифровой подписи cADS, начиная с заданного значения листового узла и значений узлов, определенных в ключе верификации, связанном с указанным заданным листовым узлом, осуществляют следующие этапы:

- извлечение из последовательности значений узлов в ключе верификации VK значения (т. е. значения цифровой подписи) каждого другого листового узла дерева, имеющего такой же родительский узел, что и у заданного листового узла, и вычисление цифровой подписи конкатенации заданного значения узла и, соответственно, согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, извлеченного значения указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла заданного листового узла;

- последовательно на каждом следующем уровне в дереве и до предпоследнего уровня узлов:

- извлечение из последовательности значений узлов в ключе верификации VK значения каждого другого узла, отличного от листового, дерева, имеющего такой же родительский узел, что и у предыдущего такого же родительского узла, рассмотренного на предшествующем этапе, и

- вычисление цифровой подписи конкатенации значения указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, тем самым получая значение указанного такого же родительского узла указанного предыдущего такого же родительского узла; и

- вычисление цифровой подписи конкатенации полученных значений узлов, отличных от листовых, соответствующих предпоследнему уровню узлов дерева согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, тем самым получая корневую цифровую подпись корневого узла дерева.

[0318] Как ясно из вышеуказанного примера, значение корневого узла R, также называемое агрегированной цифровой подписью ADS, можно наконец извлечь из любого заданного значения листового узла посредством цифровой подписи конкатенации этого значения листового узла только со значениями узлов, определенными в соответствующем ключе верификации. Таким образом, объем данных в информации о верификации V_i, который необходим для извлечения значения корневого узла R, явно намного меньше, чем объем данных, необходимый для вычисления контрольного значения корневого узла R (т. е. на основании только значений листовых узлов путем вычисления всех значений узлов, отличных от листовых, промежуточных уровней дерева): это преимущество настоящего изобретения с учетом ограничения ограниченного размера, доступного для защитной маркировки (например, двумерного штрих-кода). Согласно варианту осуществления эта информация о верификации V_i включает цифровые данные D_i, т. е. данные авторизации AD, т. е. данные поставленной задачи, и соответствующий ключ верификации VK_i, $V_i=(D_i,VK_i)$.

[0319] Согласно настоящему изобретению цифровое сообщение M, соответствующее заданному элементу A_i пакета элементов, включает информацию о верификации V_i, которая позволяет как в режиме «онлайн», так и в автономном режиме проверять аутентичность цифрового сообщения M, соответствие связанных с ним данных относительно данных авторизации AD, содержащихся в указанном заданном элементе A_i, путем обеспечения уникальной, не подлежащей изменению и защищенной от подделки связи между данными элемента D_i и принадлежностью элемента A_i к заданному пакету подлинных элементов, сохраняя при этом битовый размер цифрового представления этой информации о верификации V_i на уровне, совместимом с содержимым данных двумерного машиночитаемого штрих-кода, который можно легко считать обычным считывателем, например, модулем оптического считывания OR.

[0320] Операции проверки включают извлечение значения пакета или контрольной корневой цифровой подписи R дерева, связанного с пакетом, т. е. агрегированной цифровой подписи ADS, путем предварительного считывания цифровых данных элемента D_i, т. е. данных авторизации AD, и соответствующего ключа верификации VK_i в машиночитаемой форме, такой как, например, QR-код QRC(A), а затем вычисление потенциальной цифровой подписи cx_i с помощью односторонней функции считанных цифровых данных элемента D_i как $cx_i=H(D_i)$, и вычисление потенциальной корневой цифровой подписи cR, также называемой потенциальной агрегированной цифровой подписью cADS, как объяснено выше, из цифровой подписи конкатенации x_i и значений узлов дерева согласно последовательности значений узлов, указанных в ключе верификации VK_i. Эта схема защиты, преимущество которой заключается в том, что нет необходимости в шифровании данных и, следовательно, управлении ключами шифрования/дешифрования (в частности, криптографический ключ не включен в защитную маркировку), является гораздо более надежной в отношении криптоаналитической атаки по сравнению с обычным шифрованием данных с помощью открытого ключа шифрования -

закрытого ключа дешифрования (например, системы RSA «Ривест-Шамир-Адлеман»).

[0321] В результате, размер цифровых данных, которые должны быть представлены в защитной маркировке согласно настоящему изобретению, является компактным и позволяет использовать обычные двумерные штрих-коды (например, QR-код) и, следовательно, обычные считыватели штрих-кодов (или даже простой запрограммированный смартфон, имеющий камеру), обеспечивая при этом очень высокий уровень надежности относительно криптоаналитических атак. Более того, эта машиночитаемая форма совместима как с проверкой в режиме «онлайн» (через сервер, связывающийся со считывателем кода), так и с автономной (через запрограммированный считыватель кода) проверкой аутентичности цифрового сообщения M и соответствия его данных относительно данных авторизации AD. Кроме того, согласно настоящему изобретению представление цифровых данных D_i и представление данных ключа VK_i могут отличаться, схема конкатенации данных и/или односторонняя функция могут зависеть от уровня узла в дереве, что обеспечивает дополнительные уровни надежности в отношении криптоаналитических атак.

[0322] Предпочтительно, чтобы дополнительно уменьшить размер цифровых данных (т. е. информацию о верификации V), которые должны быть включены в машиночитаемую форму, если цифровые данные D_i соответственного оригинального элемента Ai пакета распределены между заданными полями, которые являются общими для всех элементов пакета, цифровые данные, относящиеся к этим полям, не включены в каждые цифровые данные элемента D_i, но сгруппированы в отдельном блоке данных полей FDB, связанном с пакетом элементов, и:

- цифровую подпись xi элемента A_i пакета затем вычисляют с помощью односторонней функции H конкатенации соответствующих цифровых данных Di и цифровых данных блока данных полей FDB, т. е. $xi=H(D_i+FDB)$; и

- контрольную корневую цифровую подпись R, т. е. агрегированную цифровую подпись ADS, предоставляют в распоряжение контроллера вместе со связанным блоком данных полей FDB (что также обеспечивает неизменность блока данных полей).

[0323] В варианте настоящего изобретения блок данных полей FDB становится доступным для контроллера независимо от контрольной корневой цифровой подписи, т. е. агрегированной цифровой подписи ADS.

[0324] Существует множество известных методов кодирования информации таким образом, чтобы ее можно было печатать на документе, наносить на физические поверхности или отображать, например, модулем отображения DD. Любой такой метод можно использовать в реализациях любого варианта осуществления настоящего изобретения. Одной из распространенных форм оптической машиночитаемой формы является хорошо известный QR-код, как раскрыто ранее.

[0325] Как хорошо известно, для заданной области, чем больше данных может кодировать QR-код, тем выше плотность модуля (грубо говоря, плотность черных/белых «квадратов») и тем большее разрешение требуется для печати и считывания. Помимо плотности (в количестве квадратов модулей), QR-коды также обычно классифицируются в зависимости от того, какой уровень исправления ошибок они включают. В настоящее время четыре разных стандартных «уровня», L, M, Q и H, каждый из которых представляет степень «повреждения», то есть потери данных, изображение QR-кода может выдержать и из которых может восстановиться. Уровни L, M, Q и H могут выдержать приблизительно 7%, 15%, 25% и 30% повреждения, соответственно.

[0326] В следующей таблице приведены по меньшей мере приблизительные значения для разных версий QR-кода:

Версия	Размер (в модулях)	Количество кодируемых битов	
		уровень L ECC	уровень H ECC

110	57×57	22192	9976
225	117×117	110208	44304
440	177×177	223648	110208

[0327] Однако, не все биты можно использовать для кодирования «загрузки» данных, поскольку некоторые модули используются для объектов сканирования, шаблона маски и модулей исправления ошибок. Таким образом, существует компромисс между количеством информации, которую может кодировать QR-код, и тем, сколько информации включено в информацию о верификации V_i и должно быть закодировано.

[0328] Следовательно, для выбранного типа оптической машиночитаемой формы, такой как QR-код, с ограниченной способностью кодирования также должна быть выбрана подходящая односторонняя функция H: функцию, выходные данные которой слишком велики с точки зрения требуемых битов, невозможно использовать вообще, а функция, диапазон которой слишком мал, может быть недостаточно надежной. Более того, во многих приложениях может возникнуть проблема с масштабируемостью. Например, некоторые схемы защиты данных включают подписи, которые растут по мере увеличения количества элементов пакета, и которые могут недопустимо ограничивать размер пакета с точки зрения того, сколько битов может кодировать оптическая машиночитаемая форма. Вот почему согласно предпочтительному варианту осуществления настоящего изобретения выбран следующий тип функции – односторонняя хеш-функция семейства SHA-2.

[0329] Предпочтительно, модуль вычисления содержится в контроллере C и управляется им для выполнения кода, предусмотренного для осуществления вычислений для цифрового подписывания цифровых данных D элементов пакета, для определения ключей верификации для различных элементов и для вычисления контрольной корневой цифровой подписи соответствующего дерева.

[0330] Согласно варианту осуществления блок обработки устройства, управляемого контроллером, выполнен с возможностью выполнения кода, предусмотренного для осуществления вычислений для цифрового подписывания цифровых данных элементов пакета, для определения ключей верификации для различных элементов и для вычисления контрольной корневой цифровой подписи соответствующего дерева.

[0331] Контроллер C также может содержать и управлять подходящими модулями для ввода (заранее запрограммированных) значений, соответствующих цифровым данным D_s конкретного(-ых) элемента(-ов) A_s. Например, пакет элементов может содержать один элемент, содержащий данные авторизации AD, и несколько конкретных элементов, чтобы позволить блоку обработки устройства контроллера C осуществлять настоящее изобретение и выдавать указанное цифровое сообщение на основе указанного дерева.

[0332] Можно было бы осуществлять хеш-вычисления, связанные с элементами, извне (например, на подключенном удаленном сервере), например, везде, где создаются элементы, чтобы избежать необходимости передавать необработанные данные элемента D_i по сети с этого сайта (или сайтов) контроллеру C, если это вызывает беспокойство.

[0333] Для каждого элемента A_i, такого как поставленные задачи, т. е. данные авторизации AD_i, например, компилируется соответствующая информация о верификации V_i, которая кодируется (предоставляется), например, в некотором виде оптической машиночитаемой формы, которая затем распечатывают, или наносят физически, или отображают в цифровом виде, или иным образом связывают с соответственным цифровым сообщением M или документом, или даже цифровым документом. Например, цифровое сообщение M, содержащее по меньшей мере информацию о верификации $V_{i,}$, может быть закодировано на оптически или магнитно считываемой этикетке, метке RFID и т. д., которая прикрепляется к поставленной задаче или официальному цифровому документу или печатается непосредственно на документе.

[0334] Для любого конкретного элемента A_s его соответствующая информация о верификации $V_s=(D_s,k_s)$ может быть связана с ним внутри контроллером C. Информация о верификации, как правило, по меньшей мере включает, для любого элемента A_i пакета элементов, соответствующие цифровые данные D_i и соответствующий ключ верификации k_i: т. е. $V_i=(D_i,VK_i)$. Как упомянуто ранее, цифровые данные D_i могут включать подробности поставленной задачи.

[0335] Дополнительные данные элемента могут быть дополнительно связаны с элементом и могут включать, например, значение пакета, т. е. контрольную корневую цифровую подпись R, или любую другую информацию, которую контроллер C решает включить, такую как открытый ключ PuK заданного контроллера, временной интервал для выполнения операции Op, серийный номер изделия, идентификатор пакета, информация о дате/времени, название продукта, URL-адрес, который указывает на другую онлайн-информацию, связанную либо с заданным контроллером (например, изображение контроллера или его этикетка и т. д.), либо с пакетом, либо с поставщиком/производителем, номер телефона, по которому можно позвонить для верификации, и т. д. Дополнительные данные элемента могут храниться в доступной для поиска информационной базе данных, открытой для контроллера (посредством интерфейса информационной базы данных).

[0336] После вычисления ключа верификации VK_i элемента A_i и включения его (т. е. посредством кодирования или любого выбранного представления данных) вместе с соответствующими цифровыми данными элемента D_i в оптическую машиночитаемую форму, соответствующую цифровому сообщению M, полученное в результате цифровое сообщение M и связанные с ним данные фактически защищены от подделки и фальсификации.

[0337] Контроллер, получатель цифрового сообщения M, относящегося к элементу A_1 и в виде QR-кода, может затем сканировать (или иным образом считывать) посредством модуля оптического считывания OR своего устройства оптическую машиночитаемую форму цифрового сообщения M и извлекать

цифровые данные элемента D_1 и ключ верификации VK_1 (и любую другую информацию, которая могла быть закодирована в оптическую машиночитаемую форму, как раскрыто ранее). Для верификации цифрового сообщения M и, следовательно, элемента A_1, контроллер должен сначала извлечь информацию о верификации $V_1=(D_1,VK_1)$ из указанного QR-кода и, таким образом, вычислить цифровую подпись x_1 из извлеченных цифровых данных элемента D_1: для этого контроллер, или по меньшей мере его устройство, должен знать одностороннюю функцию, которая используется для вычисления цифровой подписи элемента, в данном случае это односторонняя функция H() (например, хеш-значение SHA-256), а затем осуществлять операцию $x_1=H(D_1)$ для получения полных данных (x_1,VK_1), необходимых для вычисления соответствующей потенциальной корневой цифровой подписи cR, т. е. соответствующей потенциальной агрегированной цифровой подписи cADS. Контроллер может, например, безопасно принять одностороннюю функцию (например, используя пару открытого и закрытого ключей), либо запросив ее у поставщика элементов, либо у любого другого объекта, который создал подписи и ключи или уже запрограммировал их в блок обработки CPU контроллера его устройства, например, устройства DB, раскрытого ранее.

[0338] Затем, чтобы вычислить такуюпотенциальную корневую цифровую подпись cR, контроллеру необходимо дополнительно знать тип схемы конкатенации данных (для конкатенации значений узлов через H(a(i,j)+a(i,k)), которая используется для следующего: контроллер может принимать эту информацию любым способом, либо защищенным (например, используя пару открытого и закрытого ключей), либо просто запрашивая эту информацию у поставщика элементов или любого другого лица, создавшего данные верификации, т. е. контроллера C, или запрограммировавшего ее в блоке обработки CPU контроллера. Однако, схема конкатенации может фактически соответствовать простому обычному сквозному соединению двух блоков цифровых данных, соответственно, соответствующих значениям двух узлов: в этом случае контроллеру не должна передаваться никакая конкретная схема. В некоторых вариантах схема конкатенации может дополнительно вставлять блок

конкатенации, который может содержать данные, определенные для позиции или уровня конкатенированных блоков цифровых данных в дереве, в результате чего еще более затрудняется криптоаналитическая атака.

[0339] Зная схему конкатенации данных, контроллер может затем вычислить (например, посредством запрограммированного подходящим образом устройства) потенциальную корневую цифровую подпись cR, т. е. потенциальную агрегированную цифровую подпись cADS, как объяснено выше, путем пошагового цифрового подписывания конкатенации цифровой подписи элемента x_1 и значений узлов согласно последовательности узлов, определенных в ключе верификации VK_1, см. пункт 1) выше, относящемуся к узлу a(1,1), выполненному, например, согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева. В данном случае потенциальную корневую цифровую подпись cR получают следующим образом (упорядоченность узлов в дереве задается соответственными индексами (i,j) уровня и позиции на уровне): cR=H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2)).

[0340] Эта вычисленная потенциальная корневая цифровая подпись cR должна затем быть равна доступному (или опубликованному) контрольному значению R: это значение может быть ранее получено контроллером и/или уже сохранено в памяти процессора CPU устройства указанного контроллера, это также может быть значение, которое контроллер запрашивает и принимает от контроллера C любым известным способом. При совпадении потенциальной cR, т. е. cADS, и доступных контрольных корневых цифровых подписей R, т. е. ADS, это вычисление затем верифицирует информацию в цифровом сообщении M и подтверждает, что поставленная задача A_1 была выдана контроллером C.

[0341] Ссылка для доступа к контрольной корневой цифровой подписи R для пакета, соответствующего элементу A_1, может быть включена в цифровую метку DM (например, веб-адрес, если R можно извлечь на соответствующем веб-сайте).

[0342] В некоторых реализациях получатели цифрового сообщения M могут быть способны «визуально» извлекать информацию о верификации V_i непосредственно из цифрового сообщения M. Например, информация о верификации V_i может быть текстовой, такой как серийный номер или текст в описательном письме, или некоторой буквенно-цифровой кодировкой в другом месте на элементе и читаемой человеком из самих элементов или чего-то, прикрепленного к ним или включенного в них.

[0343] Получателям цифрового сообщения M также может быть предоставлено приемлемое программное обеспечение, такое как модуль оптического считывания в их устройстве, таком как смартфон, который либо вводит данные, либо считывает данные оптически через камеру смартфона, а затем вычисляет $x_i=H(D_i)$. Например, с помощью оптической машиночитаемой формы, содержащейся в цифровом сообщении M, относящемся к данным авторизации AD_1 и представляющим собой стандартный QR-код, контроллер может легко получить путем сканирования QR-кода посредством своего модуля оптического считывания OR, используя стандартное приложение для считывания QR-кода, запущенное на его устройстве, цифровые данные D_1 и VK_1, приложение для верификации на устройстве контроллера затем сможет вычислить x_1 и cR, а также сравнить это значение с доступным контрольным значением пакета R, как объяснено выше.

[0344] Предпочтительно, контрольная корневая цифровая подпись R, т. е. ADS, хранится в доступной для поиска корневой базе данных, к которой может получить доступ (через канал связи) контроллер с помощью своего устройства, оснащенного модулем связи CM. Контроллер, которому необходимо верифицировать цифровое сообщение M, может просто отправить корневой запрос с помощью своего смартфона на адрес базы данных через интерфейс доступа к базе данных, причем запрос содержит информацию о верификации V_1, считанную с оптической машиночитаемой формы цифрового сообщения M (или вычисленной цифровой подписи $x_1=H(D_1)$), что позволяет извлекать соответствующее контрольное значение пакета R, а интерфейс доступа вернет

контрольную корневую цифровую подпись R на смартфон. База данных может быть защищена блокчейном, чтобы усилить неизменность сохраненных корневых цифровых подписей.

[0345] Согласно варианту осуществления содержимое цифрового сообщения M защищено с использованием способа защиты от подделки или фальсификации заданного элемента, содержащего указанное содержимое указанного цифрового сообщения M, причем указанный заданный элемент принадлежит к пакету из множества элементов, причем каждый элемент имеет свои собственные связанные с ним данные элемента и соответствующие цифровые данные элемента, причем способ характеризуется тем, что включает этапы:

- для каждого элемента пакета, вычисления с помощью односторонней функции связанной с элементом цифровой подписи его соответствующих цифровых данных элемента;

- формирования дерева на основании множества вычисленных цифровых подписей элементов для оригинальных элементов пакета, содержащего узлы, расположенные согласно заданной упорядоченности узлов в дереве, причем указанное дерево содержит уровни узлов, начиная от листовых узлов, соответствующих множеству цифровых подписей элементов, соответственно, связанных с множеством оригинальных элементов в пакете, до корневого узла дерева, каждый узел, отличный от листового, дерева, соответствует цифровой подписи с помощью односторонней функции конкатенации соответственных цифровых подписей его дочерних узлов согласно упорядоченности конкатенации дерева, корневой узел соответствует контрольной корневой цифровой подписи, т. е. цифровой подписи с помощью односторонней функции конкатенации цифровых подписей узлов предпоследнего уровня узлов в дереве согласно указанной упорядоченности конкатенации дерева;

- связывания с заданным элементом соответствующего ключа верификации, представляющего собой последовательность соответственных цифровых подписей, начиная от уровня листовых узлов до предпоследнего уровня узлов,

каждого другого листового узла, имеющего такой же родительский узел в дереве, что и листовой узел, соответствующий цифровой подписи заданного элемента, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский узел в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне;

- предоставления в распоряжение контроллера контрольной корневой цифровой подписи дерева; и

- предпочтительно, в случае печати цифрового сообщения M, нанесения на заданный документ оптической машиночитаемой формы, кодирующей указанное цифровое сообщение M и, таким образом, включающей представление указанных цифровых данных и его соответствующего ключа верификации,

- тем самым предпочтительно получая маркированный документ с указанным напечатанным цифровым сообщением M, содержимое которого защищено от подделки или фальсификации.

[0346] Согласно варианту осуществления контрольная корневая цифровая подпись корневого узла дерева либо публикуется в среде, открытой для контроллера, либо хранится в доступной для поиска корневой базе данных, открытой для контроллера, либо хранится в блокчейне, либо, предпочтительно, в базе данных, защищенной блокчейном, открытой для контроллера.

[0347] Согласно варианту осуществления цифровое сообщение M может дополнительно содержать данные по доступу к корневому узлу, напечатанные или закодированные в нем и содержащие информацию, достаточную для обеспечения доступа контроллеру к контрольной корневой цифровой подписи корневого узла дерева, соответствующего пакету элементов, причем указанная информация представляет собой ссылку на интерфейс доступа, выполненный с возможностью приема от контроллера корневого запроса, содержащего

цифровые данные или цифровую подпись цифровых данных, полученные из цифрового сообщения M или из другой печатной оптической машиночитаемой формы, и отправки обратно контрольной корневой цифровой подписи соответствующего дерева, причем интерфейс доступа обеспечивает доступ, соответственно, к одному из следующего:

- среда, в которой опубликована контрольная корневая цифровая подпись;
- доступная для поиска корневая база данных, в которой сохранена контрольная корневая цифровая подпись; и
- блокчейн, или соответственно база данных, защищенная блокчейном, в котором сохранена контрольная корневая цифровая подпись с временной меткой.

[0348] Согласно варианту осуществления дополнительные цифровые данные, соответствующие цифровым данным, связанным с цифровым сообщением M, хранятся в доступной для поиска информационной базе данных, открытой для контроллера, посредством интерфейса информационной базы данных, выполненного с возможностью приема от контроллера запроса на информацию, содержащего цифровые данные или цифровую подпись цифровых данных, полученных из цифрового сообщения M или из другой напечатанной оптической машиночитаемой формы, и отправки обратно соответствующих дополнительных цифровых данных.

[0349] Таким образом, настоящее изобретение позволяет получателю проверить достоверность заданного цифрового содержимого с высокой уверенностью.

Формула изобретения

1. Способ проверки достоверности цифрового содержимого цифрового сообщения M, принятого устройством DB, управляемым контроллером B, по сети связи CN, отличающийся тем, что:

- устройство DA, управляемое контроллером A, содержит блок обработки CPU(A) с памятью, хранящей цифровое сообщение M, и модуль связи CM(A), выполненный с возможностью отправки и приема данных по сети связи CN;

- устройство DB содержит блок обработки CPU(B) с памятью, хранящей агрегированную цифровую подпись ADS, и модуль связи CM(B), выполненный с возможностью отправки и приема данных по сети связи CN, причем указанную агрегированную цифровую подпись ADS вычисляют путем применения одностороннего сумматора к множеству цифровых подписей, причем указанное множество цифровых подписей включает цифровую подпись x(A) данных авторизации AD(A), вычисленную с помощью односторонней функции;

- цифровое сообщение M содержит данные авторизации AD(A), указывающие на то, что контроллер A устройства DA уполномочен контроллером C осуществлять операцию Op с контроллером, устройство которого принимает указанное цифровое сообщение M;

- цифровое сообщение M также содержит ключ верификации VK(A), приписанный контроллером C, при этом указанный ключ верификации VK(A) вместе с данными авторизации AD(A) используют для вычисления потенциальной агрегированной цифровой подписи cADS, причем блок обработки CPU(B) выполнен с возможностью сравнения указанной потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, хранящейся в памяти блока обработки CPU(B) устройства DB;

способ включает следующие этапы, на которых:

- модуль связи CM(B) устройства DB принимает (100b, 200) цифровое сообщение M;

- блок обработки CPU(B) устройства DB извлекает (201) данные авторизации AD(A), содержащиеся в цифровом сообщении M;

- модуль связи CM(B) устройства DB принимает (400) от модуля связи CM(A) устройства DA аккредитацию SA;

- блок обработки CPU(B) устройства DB верифицирует (400b) аккредитацию SA;

- блок обработки CPU(B) устройства DB:

- извлекает (204) ключ верификации VK(A), содержащийся в цифровом сообщении M,

- вычисляет (203) с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальную цифровую подпись cx(A) данных авторизации AD(A), и

- вычисляет (205) потенциальную агрегированную цифровую подпись cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

- блок обработки CPU(B) устройства DB проверяет (207), совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся (206) в его памяти, и только в случае положительной верификации данных аккредитации SA и положительного совпадения потенциальной агрегированной цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) устройства DB передает (500) посредством модуля связи CM(B) контроллеру B указание о том, что контроллер A действительно уполномочен контроллером C осуществлять (500a) операцию Op.

2. Способ по п. 1, отличающийся тем, что:

○ память блока обработки CPU(A) устройства DA хранит закрытый ключ PrK(A), причем блок обработки CPU(A) выполнен с возможностью подписывания данных с помощью закрытого ключа PrK(A); и

○ блок обработки CPU(B) устройства DB выполнен с возможностью верификации подписанных данных с помощью соответствующего открытого ключа модулем связи CM(B); и

○ цифровое сообщение M дополнительно содержит открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) и аккредитованный контроллером C как принадлежащий контроллеру A; и

○ аккредитация SA представляет собой данные аккредитации, подписанные с помощью закрытого ключа PrK(A);

и при этом:

○ перед этапом верификации (400b) указанной аккредитации SA блоком обработки CPU(B) устройства DB, блок обработки CPU(B) устройства DB извлекает (202) открытый ключ PuK(A) из цифрового сообщения M;

и при этом:

○ этап верификации (400b) указанной аккредитации SA включает верификацию аккредитации SA блоком обработки CPU(B) устройства DB с использованием указанного открытого ключа PuK(A).

3. Способ по любому из пп. 1–2, отличающийся тем, что сеть связи CN включает сеть связи ближнего радиуса действия NFCN, и при этом модуль связи CM(A) выполнен с возможностью отправки и приема данных по сети связи ближнего радиуса действия NFCN, модуль связи CM(B) выполнен с возможностью отправки и приема данных по сети связи ближнего радиуса действия NFCN, эта сеть связи ближнего радиуса действия NFCN обеспечивает

связь между модулем связи CM(A) и модулем связи CM(B), когда расстояние между модулем связи CM(A) и модулем связи CM(B) составляет менее 50 см.

4. Способ по любому из пп. 1–3, отличающийся тем, что устройство DA содержит модуль отображения DD(A) и модуль оптического считывания OR(A), устройство DB содержит модуль отображения DD(B) и модуль оптического считывания OR(B), и при этом этап приема цифрового сообщения M модулем связи CM(B) устройства DB включает этап считывания модулем оптического считывания OR(B) оптического считываемого представления блока графических данных GDB, отображаемого модулем отображения DD(A), причем указанный блок графических данных GDB содержит цифровую метку DM, и при этом указанная цифровая метка DM включает закодированную версию EAD(A) указанных данных авторизации AD(A) и закодированную версию EVK(A) указанного ключа верификации VK(A), и при этом извлечение данных авторизации AD(A) включает декодирование указанных закодированных данных авторизации EAD(A), и при этом извлечение ключа верификации VK(A) включает декодирование указанного закодированного ключа верификации EVK(A).

5. Способ по п. 4, отличающийся тем, что указанное оптическое считываемое представление блока графических данных GDB включает цифровое представление графических символов из заданного конечного набора графических символов, причем указанное цифровое представление графического символа выполнено с возможностью кодирования указанной цифровой метки MD и блока машиночитаемых данных с исправлением ошибок.

6. Способ по любому из пп. 1–5, отличающийся тем, что память устройства DB хранит закрытый ключ PrK(B) и соответствующий открытый ключ PuK(B), аккредитованный контроллером C как принадлежащий контроллеру B, причем блок обработки CPU(B) устройства DB выполнен с возможностью подписывания данных с помощью указанного закрытого ключа PrK(B), и при этом блок обработки CPU(A) устройства DA выполнен с возможностью

верификации подписанных данных с использованием соответствующего открытого ключа модулем связи CM(A).

7. Способ по любому из пп. 1–6, включающий, перед этапом приема (400) модулем связи CM(B) от модуля связи CM(A) аккредитации SA, этап отправки (300) от модуля связи CM(B) на модуль связи CM(A) секрета, сгенерированного устройством DB, причем указанный секрет выполнен с возможностью генерирования указанной аккредитации SA.

8. Способ по п. 7 вместе с п. 2, отличающийся тем, что указанный секрет выполнен с возможностью быть подписанным (300a) с помощью закрытого ключа PrK(A) блоком обработки CPU(A) для генерирования указанной аккредитации SA.

9. Способ по любому из пп. 7–8 вместе с любым из пп. 4–5, отличающийся тем, что указанный этап отправки (300) указанного секрета включает этап отображения модулем отображения DD(B) оптического считываемого представления графического элемента, кодирующего указанный секрет и выполненного с возможностью быть считанным модулем оптического считывания OR(A).

10. Способ по любому из пп. 1–9 вместе с п. 2, отличающийся тем, что, перед или после приема цифрового сообщения M, контроллер B принимает цифровой документ, и при этом аккредитация SA включает подпись содержимого указанного цифрового документа, причем указанная подпись генерируется блоком обработки CPU(A) путем подписывания с помощью закрытого ключа PrK(A) указанного содержимого.

11. Способ по любому из пп. 1–10, отличающийся тем, что цифровое сообщение M сертифицировано (10) контроллером C, и при этом способ включает, перед этапом извлечения (201) блоком обработки CPU(B) устройства DB данных авторизации AD(A), содержащихся в цифровом сообщении M, этап верификации (10b) блоком обработки CPU(B) того, что цифровое сообщение M

сертифицировано контроллером C, и только в случае положительной верификации того, что цифровое сообщение M сертифицировано (10) контроллером C, блок обработки CPU(B) устройства DB извлекает (201) данные авторизации AD(A), содержащиеся в цифровом сообщении M.

12. Система для проверки достоверности цифрового содержимого цифрового сообщения M, принятого устройством DB, управляемым контроллером B, по сети связи CN, причем система содержит:

- устройство DA, управляемое контроллером A и содержащее блок обработки CPU(A) с памятью, хранящей цифровое сообщение M, и модуль связи CM(A), выполненный с возможностью отправки и приема данных по сети связи CN;

- устройство DB, содержащее блок обработки CPU(B) с памятью, хранящей агрегированную цифровую подпись ADS, и модуль связи CM(B), выполненный с возможностью отправки и приема данных по сети связи CN, причем указанная агрегированная цифровая подпись ADS вычислена путем применения одностороннего сумматора к множеству цифровых подписей, причем указанное множество цифровых подписей включает цифровую подпись x(A) данных авторизации AD(A), вычисленную с помощью односторонней функции;

- цифровое сообщение M содержит данные авторизации AD(A), указывающие на то, что контроллер A устройства DA уполномочен контроллером C осуществлять операцию Op с контроллером, устройство которого принимает указанное цифровое сообщение M;

- цифровое сообщение M также содержит ключ верификации VK(A), приписанный контроллером C, при этом указанный ключ верификации VK(A) вместе с данными авторизации AD(A) использованы для вычисления потенциальной агрегированной цифровой подписи cADS, причем блок обработки CPU(B) выполнен с возможностью сравнения указанной потенциальной агрегированной цифровой подписи cADS с агрегированной

цифровой подписью ADS, хранящейся в памяти блока обработки CPU(B) устройства DB;

и отличающаяся тем, что:

- модуль связи CM(B) устройства DB выполнен с возможностью приема (100b, 200) цифрового сообщения M;

- блок обработки CPU(B) устройства DB выполнен с возможностью извлечения (201) данных авторизации AD(A), содержащихся в цифровом сообщении M;

- модуль связи CM(B) устройства DB выполнен с возможностью приема (400) от модуля связи CM(A) устройства DA аккредитации SA;

- блок обработки CPU(B) устройства DB выполнен с возможностью верификации (400b) аккредитации SA;

- блок обработки CPU(B) устройства DB выполнен с возможностью:

- извлечения (204) ключа верификации VK(A), содержащегося в цифровом сообщении M,

- вычисления (203) с помощью односторонней функции, запрограммированной в блоке обработки CPU(B), потенциальной цифровой подписи cx(A) данных авторизации AD(A), и

- вычисления (205) потенциальной агрегированной цифровой подписи cADS из ключа верификации VK(A) и вычисленной потенциальной цифровой подписи cx(A) данных авторизации AD(A); и

- блок обработки CPU(B) устройства DB выполнен с возможностью проверки (207) того, совпадает ли потенциальная агрегированная цифровая подпись cADS с агрегированной цифровой подписью ADS, хранящейся (206) в его памяти, и только в случае положительной верификации данных аккредитации SA и положительного совпадения потенциальной агрегированной

цифровой подписи cADS с агрегированной цифровой подписью ADS, блок обработки CPU(B) устройства DB выполнен с возможностью передачи (500) посредством модуля связи CM(B) контроллеру B указания о том, что контроллер A действительно уполномочен контроллером C осуществлять (500a) операцию Op.

13. Система по п. 12, отличающаяся тем, что:

- память блока обработки CPU(A) устройства DA выполнена с возможностью хранения закрытого ключа PrK(A), причем блок обработки CPU(A) выполнен с возможностью подписывания данных с помощью закрытого ключа PrK(A); и

- блок обработки CPU(B) устройства DB выполнен с возможностью верификации подписанных данных с помощью соответствующего открытого ключа модулем связи CM(B); и

- цифровое сообщение M дополнительно содержит открытый ключ PuK(A), соответствующий закрытому ключу PrK(A) и аккредитованный контроллером C как принадлежащий контроллеру A; и

- аккредитация SA представляет собой данные аккредитации, подписанные с помощью закрытого ключа PrK(A);

и при этом:

- блок обработки CPU(B) устройства DB выполнен с возможностью извлечения (202) открытого ключа PuK(A) из цифрового сообщения M;

и при этом:

- блок обработки CPU(B) устройства DB выполнен с возможностью верификации (400b) указанной аккредитации SA с использованием указанного открытого ключа PuK(A).

14. Система по любому из пп. 12–13, отличающаяся тем, что устройство DA содержит модуль отображения DD(A) и модуль оптического считывания OR(A), устройство DB содержит модуль отображения DD(B) и модуль оптического считывания OR(B), и при этом модуль отображения DD(A) устройства DA выполнен с возможностью отображения оптического считываемого представления блока графических данных GDB, и при этом модуль оптического считывания OR(B) устройства DB выполнен с возможностью считывания указанного оптического считываемого представления блока графических данных GDB, причем указанный блок графических данных GDB содержит цифровую метку DM, и при этом указанная цифровая метка DM включает закодированную версию EAD(A) указанных данных авторизации AD(A) и закодированную версию EVK(A) указанного ключа верификации VK(A), и при этом блок обработки CPU(B) устройства DB выполнен с возможностью извлечения данных авторизации AD(A) путем декодирования указанных закодированных данных авторизации EAD(A), и при этом блок обработки CPU(B) устройства DB выполнен с возможностью извлечения ключа верификации VK(A) путем декодирования указанного закодированного ключа верификации EVK(A).

15. Применение системы для проверки достоверности цифрового содержимого цифрового сообщения M по любому из пп. 12–14 для проверки достоверности устройством DB выполнения операции Op, причем указанная операция Op выполняется устройством DA, и где:

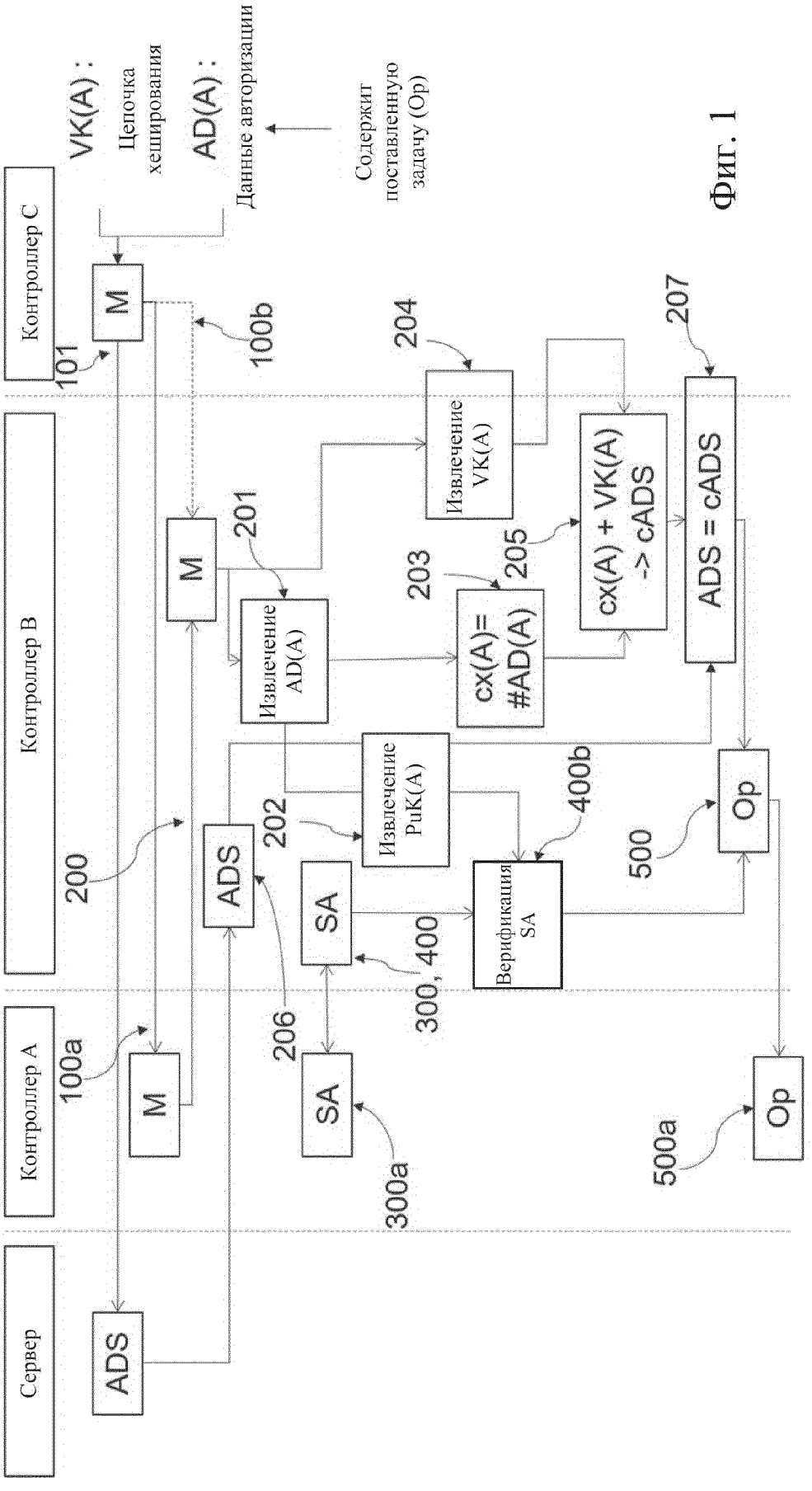
- устройство DB содержится в хранилище B и управляется им, устройство DA содержится в роботе A и управляется им, и операция Op относится к выборке роботом A конкретного товара, расположенного внутри хранилища B; или

- устройство DB содержится в компьютере B и управляется им, устройство DA содержится в смартфоне A и управляется им, и операция Op относится к отправке смартфоном A набора данных SeD(A) на компьютер B; или

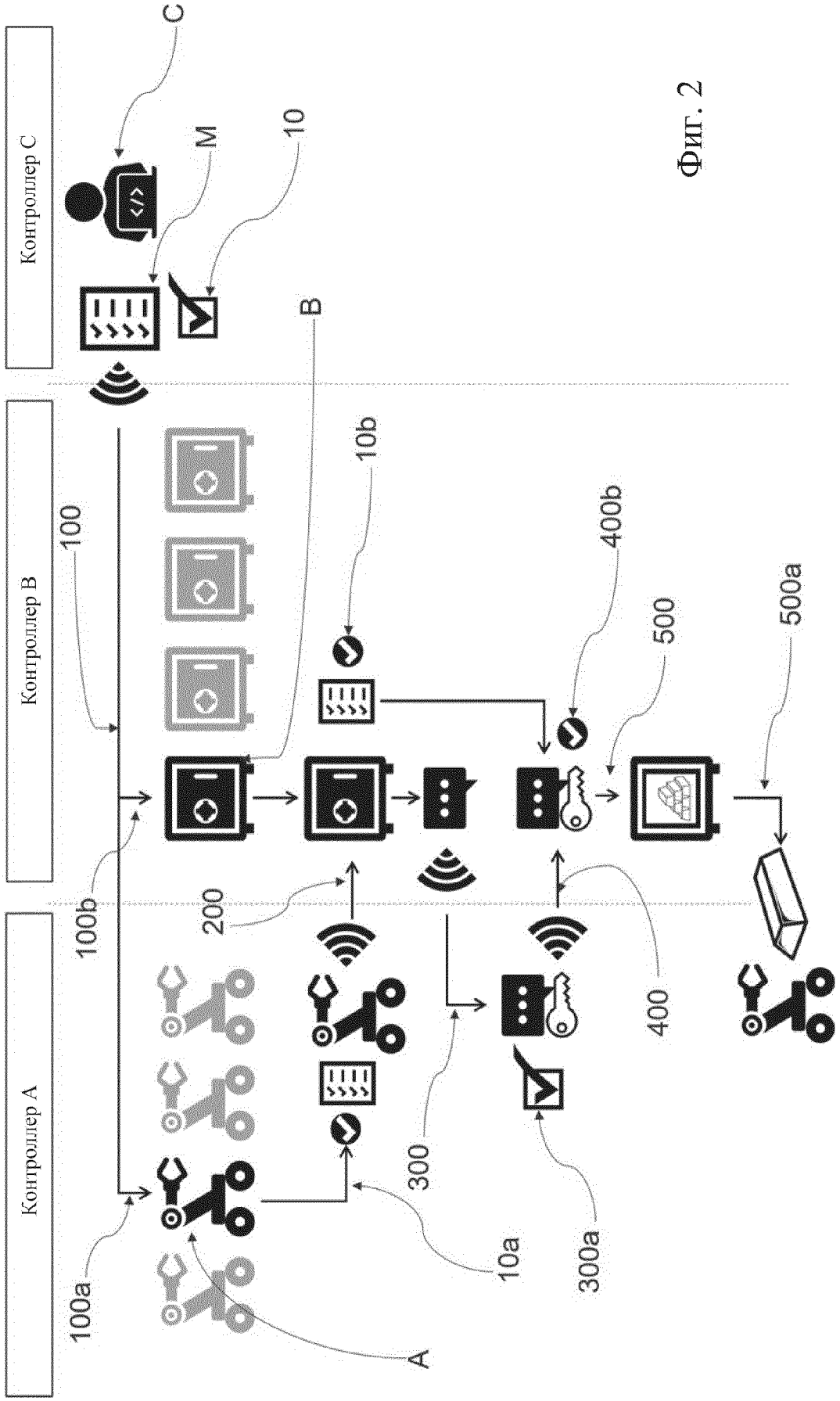
- устройство DB содержится в медицинском устройстве B и управляется им, устройство DA содержится у медсестры A и управляется ею, и операция Op относится к введению медсестрой A конкретного лекарственного средства конкретному пациенту с использованием указанного медицинского устройства B; или

- устройство DB содержится у гражданина B и управляется им, устройство DA содержится у сотрудника полиции A и управляется им, и операция Op относится к проникновению сотрудника полиции A в дом гражданина B для поиска доказательств; или

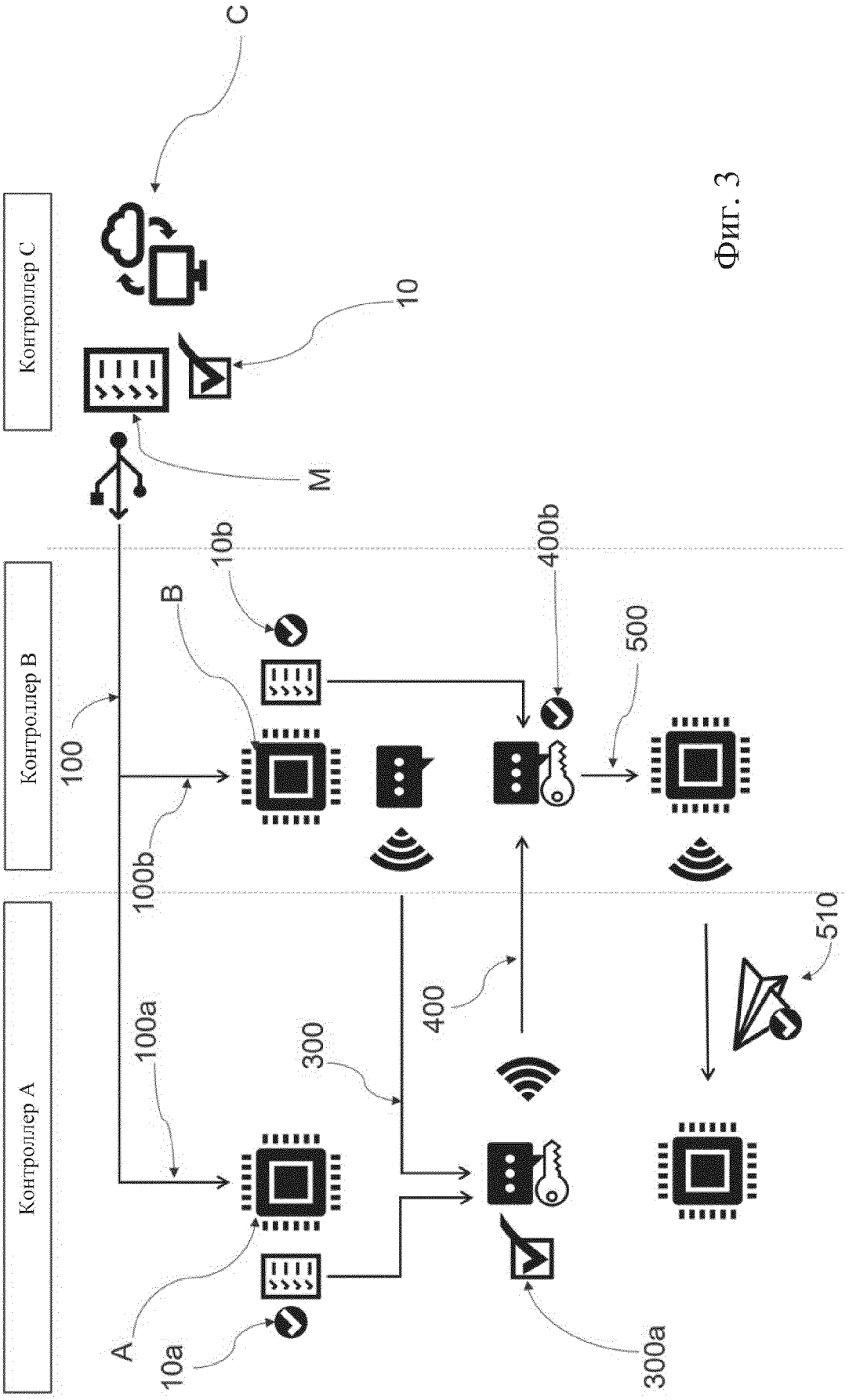
- устройство DB содержится у гражданина B и управляется им, устройство DA содержится у государственного служащего A и управляется им, и операция Op относится к выдаче и подписыванию государственным служащим A официального цифрового документа.


Контроллер C
Контроллер B
Контроллер A
Сервер
VK(A) :
Цепочка хеширования
AD(A) :
Данные авторизации
Содержит поставленную задачу (Op)
M
ADS
SA
Op
101
100a
100b
200
201
202
203
204
205
206
207
300, 400
300a
400b
500
500a
Извлечение AD(A)
Извлечение PuK(A)
Извлечение VK(A)
cx(A)= #AD(A)
cx(A) + VK(A) -> cADS
ADS = cADS
Верификация SA

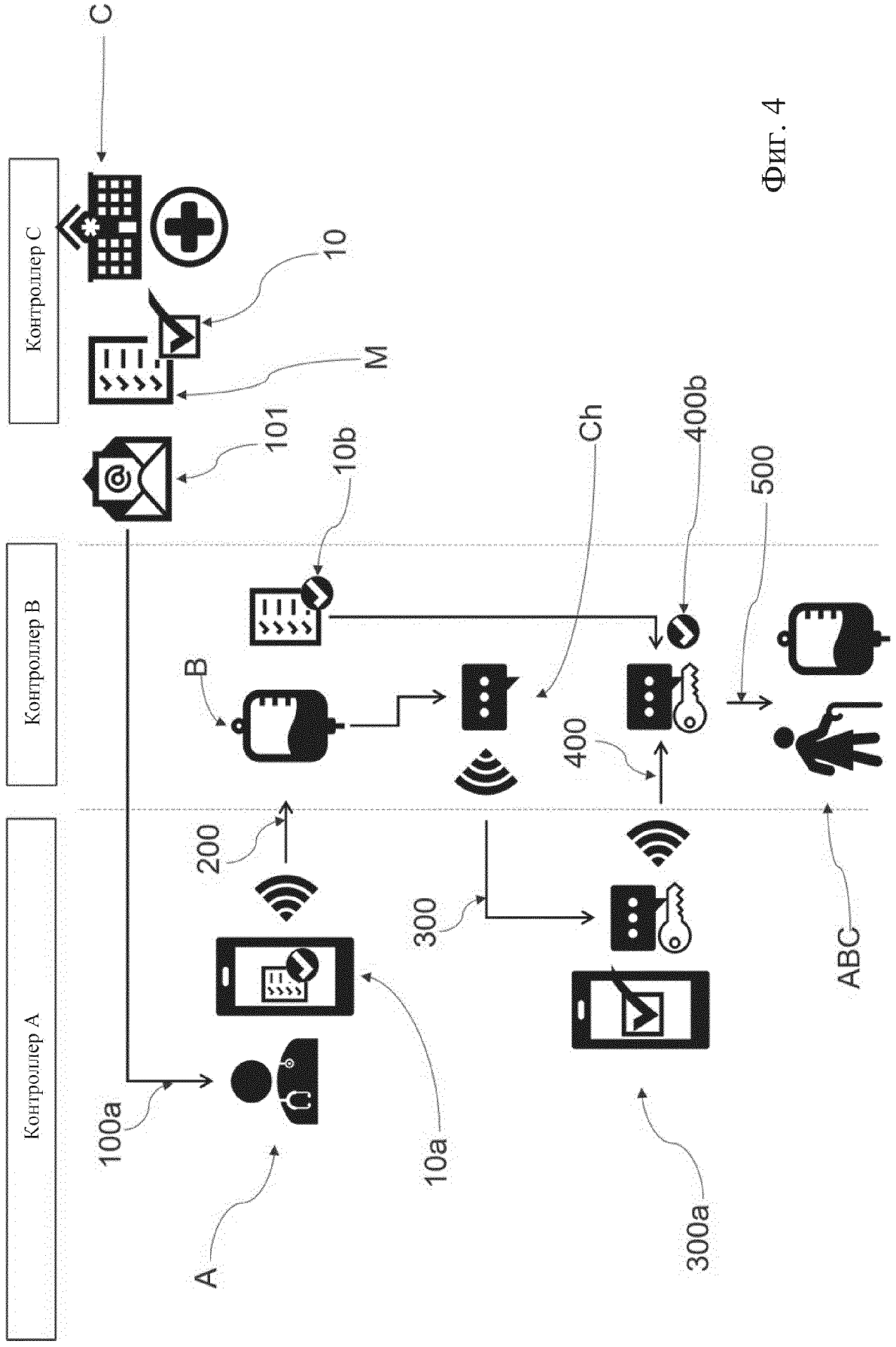
Фиг. 1


Контроллер C
Контроллер B
Контроллер A
C
M
10
B
100
10b
400b
500
500a
100b
200
400
300
10a
300a
100a
A

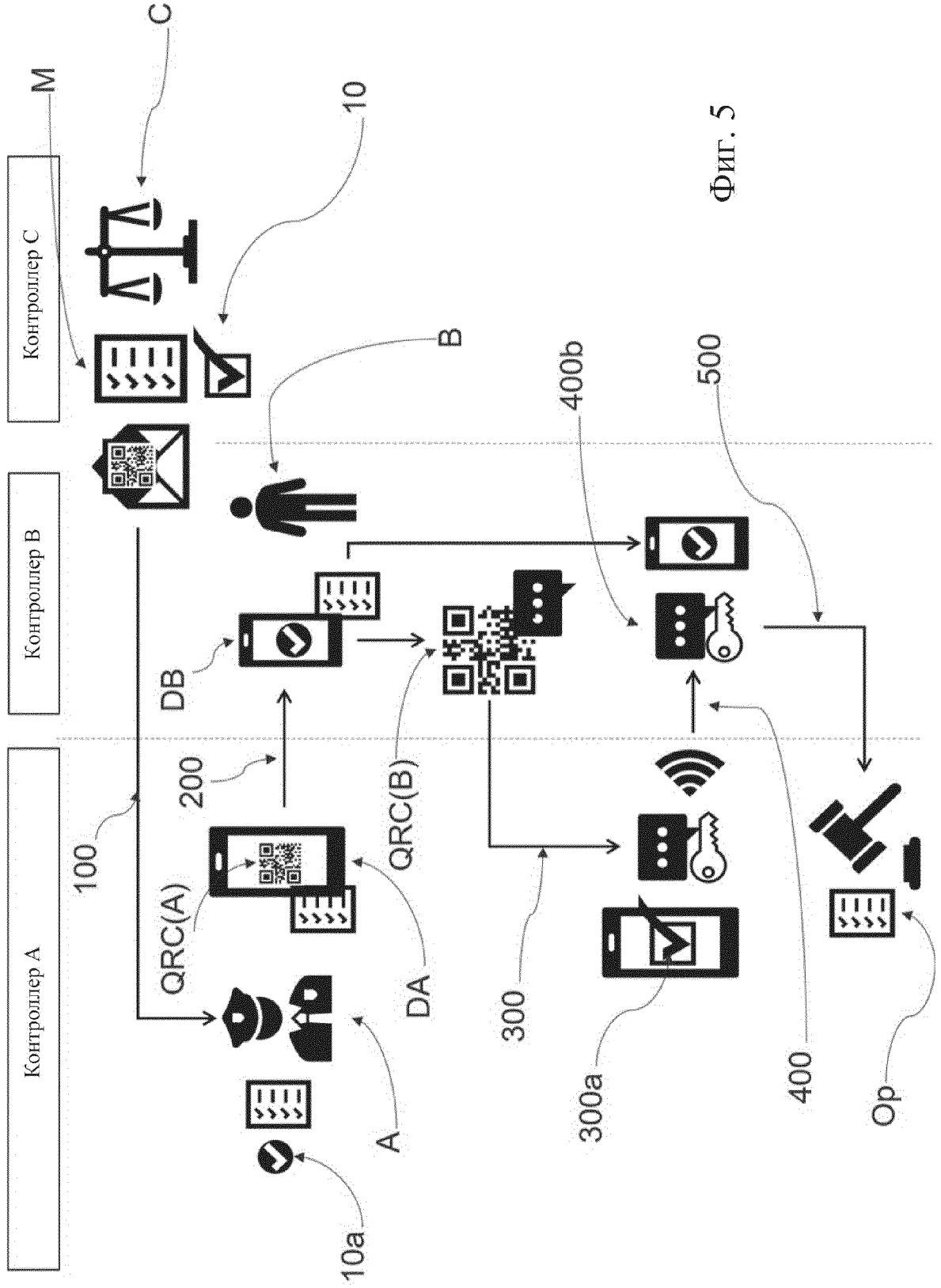
Фиг. 2


Контроллер C
Контроллер B
Контроллер A
C
10
M
10b
B
400b
500
100
100b
100a
300
400
510
A
10a
300a

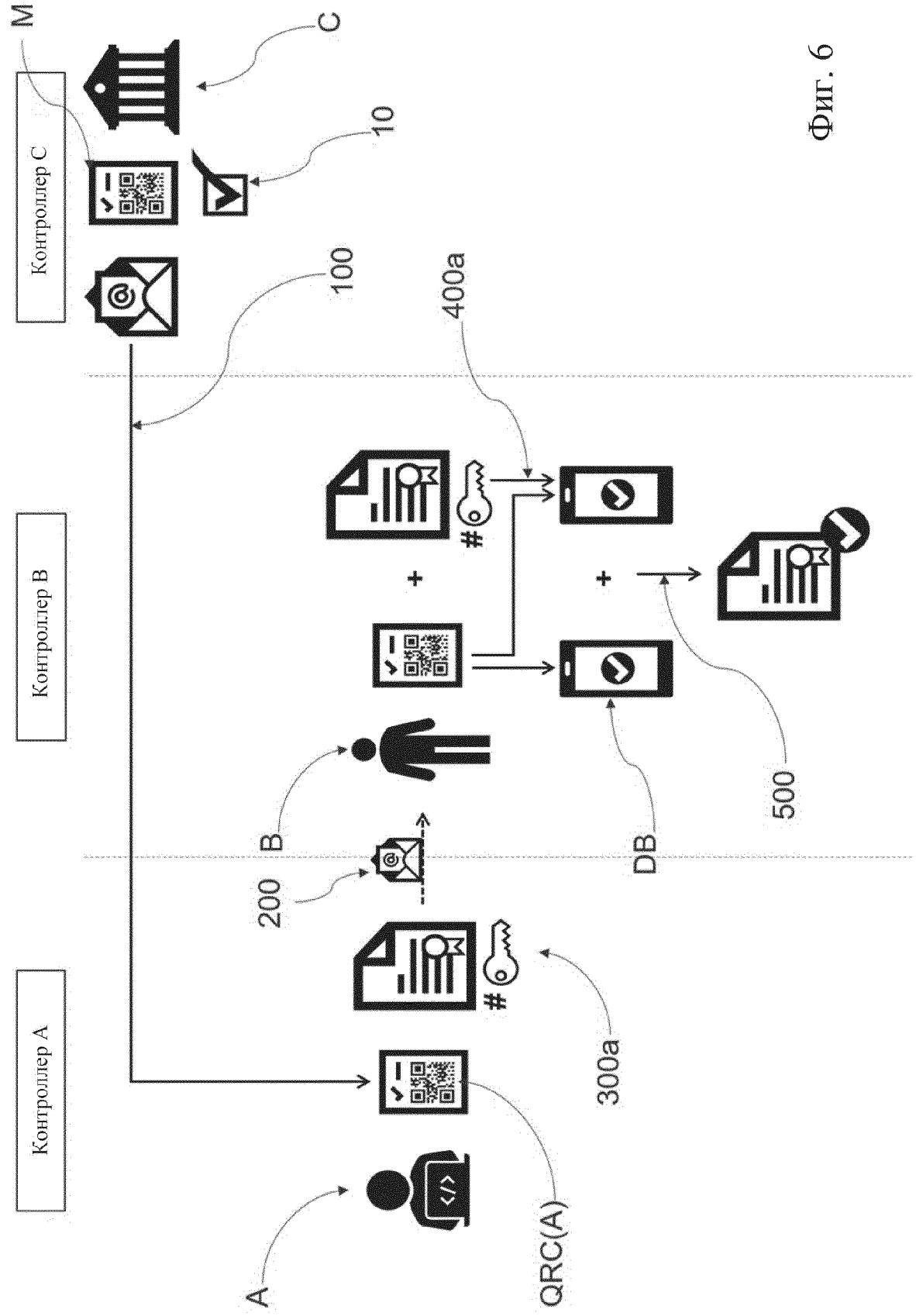
Фиг. 3


Контроллер A
Контроллер B
Контроллер C
C
10
M
101
10b
Ch
400b
500
B
400
200
300
100a
10a
A
300a
ABC

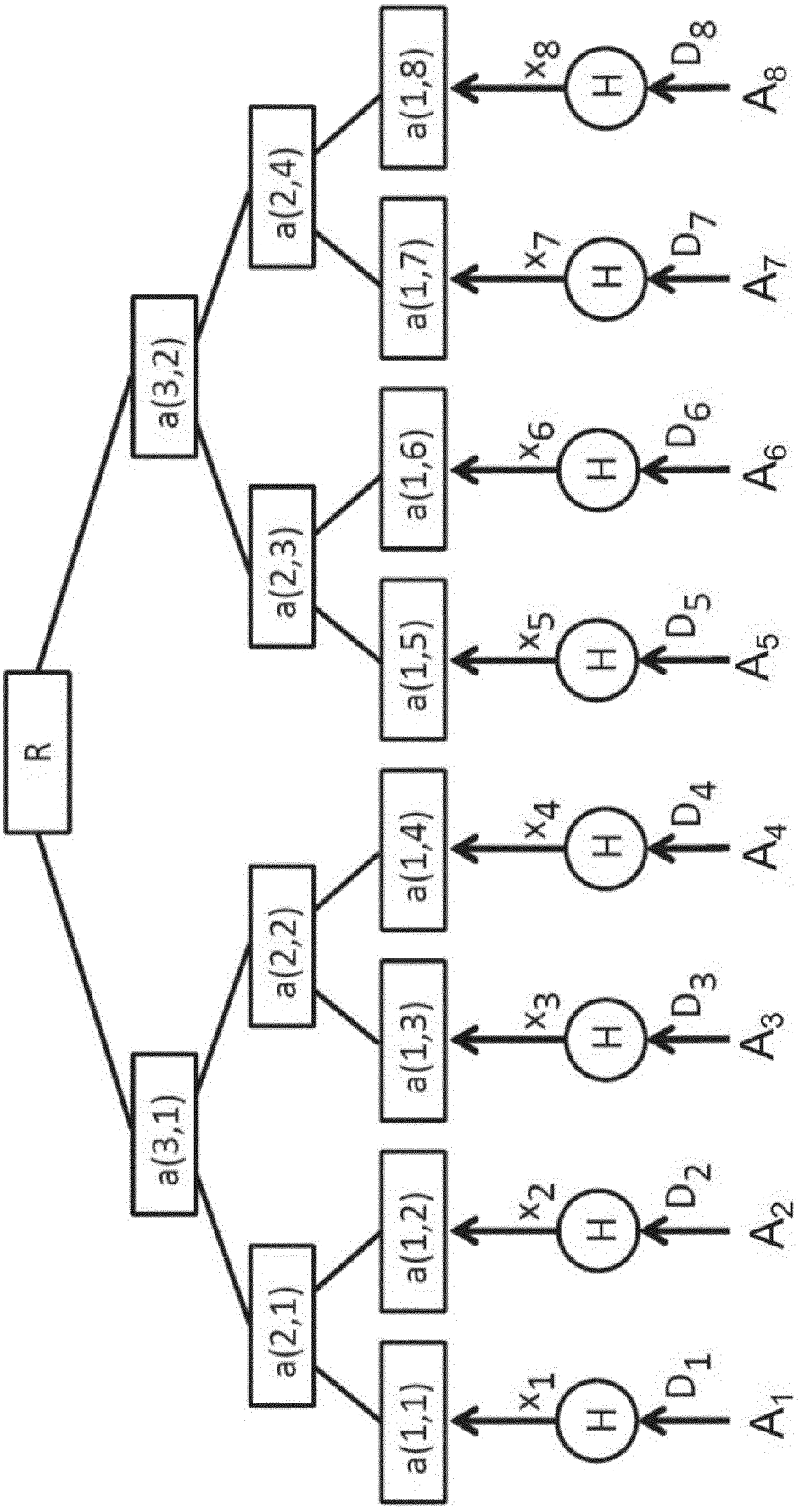
Фиг. 4


Контроллер A
Контроллер B
Контроллер C
M
C
10
B
400b
500
DB
200
100
QRC(A)
QRC(B)
DA
300
300a
400
Op
A
10a

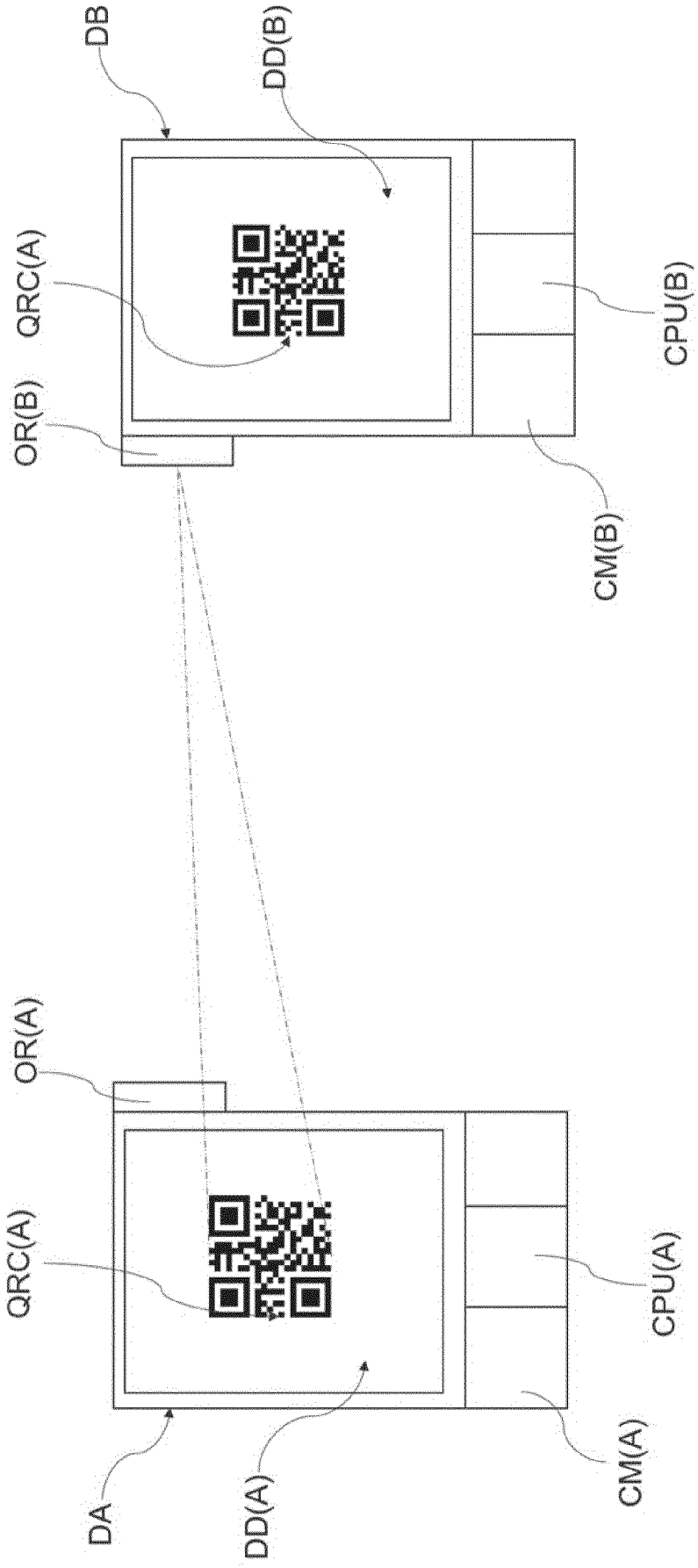
Фиг. 5


M
C
10
Контроллер C
100
400a
Контроллер B
B
200
DB
500
Контроллер A
A
QRC(A)
300a

Фиг. 6


R
a(3,1)
a(3,2)
a(2,1)
a(2,2)
a(2,3)
a(2,4)
a(1,1)
a(1,2)
a(1,3)
a(1,4)
a(1,5)
a(1,6)
a(1,7)
a(1,8)
x1
x2
x3
x4
x5
x6
x7
x8
H
D1
D2
D3
D4
D5
D6
D7
D8
A1
A2
A3
A4
A5
A6
A7
A8

Фиг. 7



Фиг. 8