РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 816 848**(13) **C2**

(51) МПК
H04W 4/029 (2018.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04W 4/029 *(2022.08);* ***G06Q 30/0185*** *(2022.08);* ***H04L 63/0876*** *(2022.08);* ***H04L 63/12*** *(2022.08);* ***H04L 63/20*** *(2022.08)*

(21)(22) Заявка: **2021120695, 17.12.2019**

(24) Дата начала отсчета срока действия патента:
17.12.2019

Дата регистрации:
05.04.2024

Приоритет(ы):
(30) Конвенционный приоритет:
20.12.2018 EP 18214512.8

(43) Дата публикации заявки: **20.01.2023** Бюл. № 2

(45) Опубликовано: **05.04.2024** Бюл. № 10

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **20.07.2021**

(86) Заявка PCT:
EP 2019/085552 (17.12.2019)

(87) Публикация заявки PCT:
WO 2020/144008 (16.07.2020)

Адрес для переписки:
105082, Москва, Спартаковский пер., д. 2, стр. 1, секция 1, этаж 3, "ЕВРОМАРКПАТ", Веселицкий Максим Борисович

(72) Автор(ы):
ЭНДРЕСС Томас (DE),
САБО Даниэль (DE),
БЕРКЕРМАН Фредерик (DE),
МЕЛЬГАРЕХО ДИАС Натали (DE)

(73) Патентообладатель(и):
МЕРК ПАТЕНТ ГМБХ (DE)

(56) Список документов, цитированных в отчете о поиске: **US 2011/0054979 A1, 03.03.2011. EP 2924916 A1, 30.09.2015. WO 2017/196655 A1, 16.11.2017. RU 2621625 C2, 06.06.2017.**

(54) СПОСОБЫ И СИСТЕМЫ ДЛЯ ПОДГОТОВКИ И ОСУЩЕСТВЛЕНИЯ ПРОВЕРКИ АУТЕНТИЧНОСТИ ОБЪЕКТА

(57) Реферат:

Изобретения относится к средствам проверки аутентичности физического объекта или группы физических объектов. Технический результат - повышение эффективности проверки аутентичности физического объекта. Получают спрогнозированные контекстные данные, представляющие спрогнозированное будущее местоположение, связанное с намеченным следующим получателем физического объекта или группы физических объектов, и связанное будущее время присутствия физического объекта или группы физических объектов в этом будущем местоположении. Получают случайные контекстные данные, указывающие на случайное местоположение и случайное время. Комбинируют согласно первой предварительно определенной схеме комбинирования спрогнозированных контекстных данных и случайных контекстных данных для получения посредством этого модифицированных

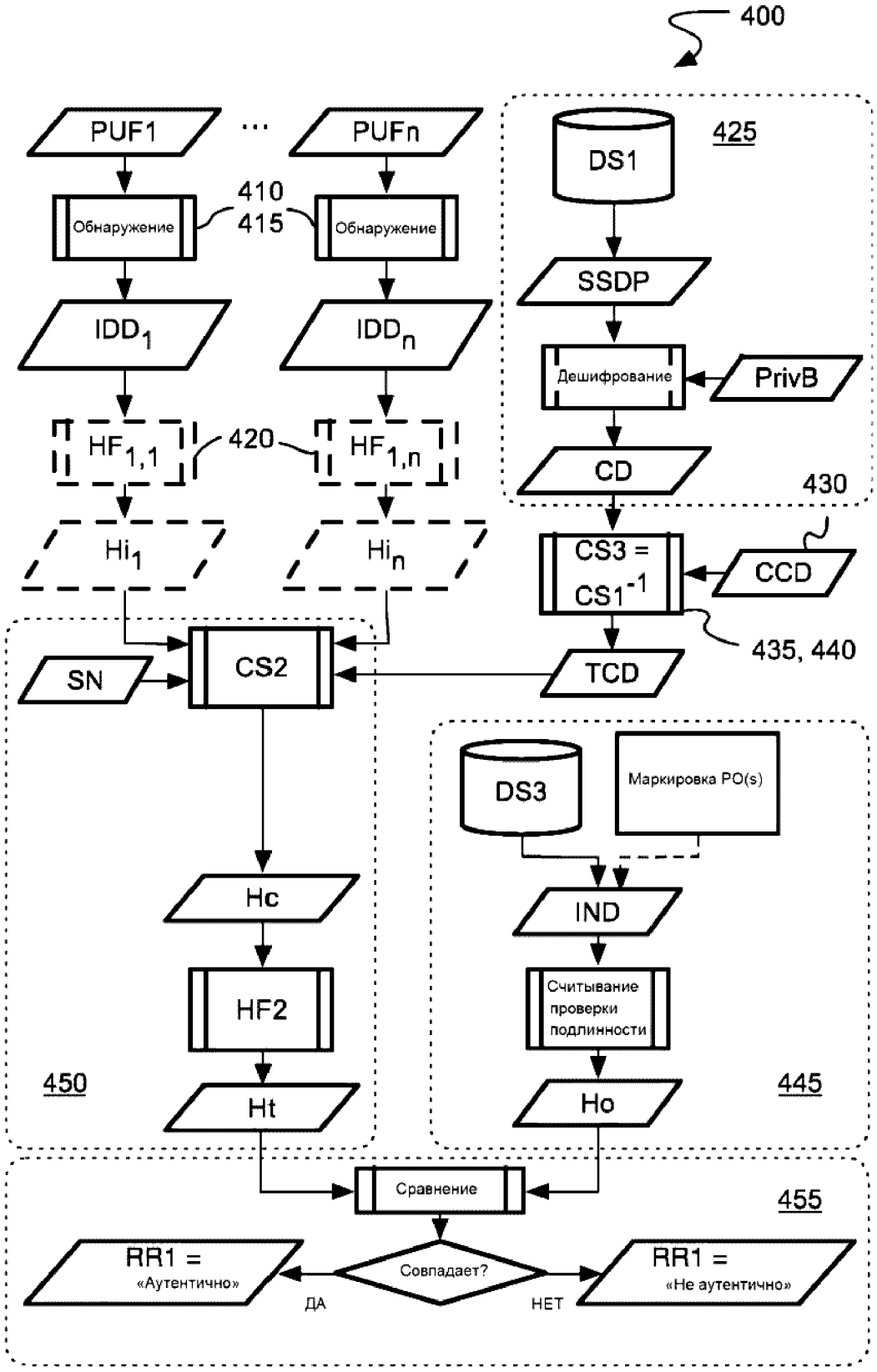
RU 2816848 C2

RU 2816848 C2

контекстных данных, представляющих модифицированное случайное местоположение и модифицированное случайное время, каждое из которых получается в результате комбинирования. Шифруют модифицированные контекстные данные для получения защищенного начального пакета данных, представляющего модифицированные контекстные данные. Сохраняют защищенный начальный пакет данных или побуждение к его сохранению в первом хранилище данных, доступном для обеспечения защищенного начального пакета данных для последующей защищенной проверки аутентичности физического объекта или группы физических объектов. 5 н. и 15 з.п. ф-лы, 14 ил.

RU 2816848 C2

RU 2816848 C2



Фиг. 5Б

RU 2816848 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 816 848**(13) **C2**

(51) Int. Cl.
H04W 4/029 (2018.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04W 4/029 (2022.08); G06Q 30/0185 (2022.08); H04L 63/0876 (2022.08); H04L 63/12 (2022.08); H04L 63/20 (2022.08)

(21)(22) Application: **2021120695, 17.12.2019**

(24) Effective date for property rights:
17.12.2019

Registration date:
05.04.2024

Priority:
(30) Convention priority:
20.12.2018 EP 18214512.8

(43) Application published: **20.01.2023** Bull. № **2**

(45) Date of publication: **05.04.2024** Bull. № **10**

(85) Commencement of national phase: **20.07.2021**

(86) PCT application:
EP 2019/085552 (17.12.2019)

(87) PCT publication:
WO 2020/144008 (16.07.2020)

Mail address:
105082, Moskva, Spartakovskij per., d. 2, str. 1, sektsiya 1, etazh 3, "EVROMARKPAT", Veselitskij Maksim Borisovich

(72) Inventor(s):
ENDRESS Thomas (DE),
SZABO Daniel (DE),
BERKERMANN Frederic (DE),
MELGAREJO DIAZ Natali (DE)

(73) Proprietor(s):
Merck Patent GmbH (DE)

RU 2816848 C2

RU 2816848 C2

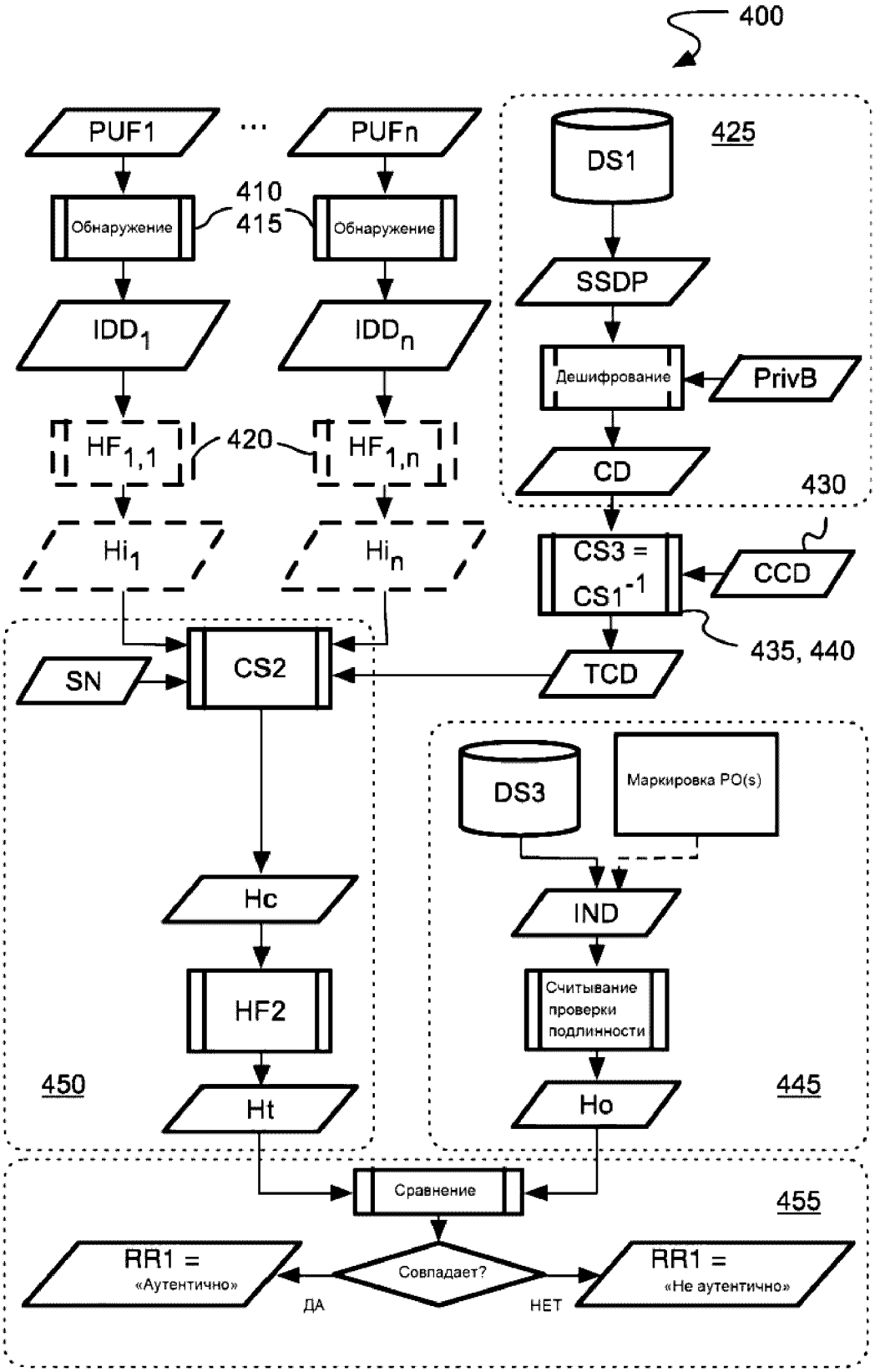
(54) METHODS AND SYSTEMS FOR PREPARING AND VERIFYING AUTHENTICITY OF OBJECT

(57) Abstract:

FIELD: physics.

SUBSTANCE: invention relates to means of verifying the authenticity of a physical object or a group of physical objects. Predicted context data representing the predicted future location associated with the intended next recipient of the physical object or group of physical objects is obtained and associated future time of physical object or group of physical objects presence in this future location. Random contextual data indicating a random location and random time are obtained. Combining according to a first predetermined combination scheme of predicted context data and random context data to obtain modified context data representing a modified random location and a modified random time, each of which is obtained as a result of combination. Modified context data is encrypted to obtain a secure initial data packet representing modified context data. Protected initial data packet or stimulation to its storage is stored in the first data storage, available for provision of protected initial data packet for further protected authenticity check of physical object or group of physical objects.

EFFECT: high efficiency of verifying the authenticity of a physical object.



Фиг. 5Б

RU 2816848 C2

RU 2816848 C2

Область изобретения

Настоящее изобретения относится к сфере отслеживания, антиконтрафактной защиты физических объектов, таких как продукты, как, например, фармацевтические средства или другие лечебно-оздоровительных продукты и, прежде всего, к подготовке и выполнению защищенной проверки аутентичности таких объектов. Прежде всего, изобретение относится к способу и системе для подготовки и последующей защищенной проверки аутентичности физического объекта или группы физических объектов посредством его получателя, к способу и системе проверки аутентичности физического объекта или группы физических объектов, к способу и к системе для защищенного обеспечения зависящей от времени схемы комбинирования для проверки аутентичности физического объекта или группы физических объектов согласно вышеупомянутым способам и к связанным компьютерным программам, соответствующим этим способам.

Предпосылки создания изобретения

Во многих отраслях промышленности контрафакция продуктов является существенной проблемой, которая не только оказывает значительное влияние на доходы производителя оригинального продукта, но может даже представлять серьезную опасность здоровью и даже жизни потребителя или оператора контрафактных, то есть поддельных товаров. Такие важные в отношении безопасности категории продуктов включают в себя, прежде всего, детали для автомобилей и воздушных судов, компоненты для сооружения зданий или других инфраструктур, пищевые продукты и даже медицинские прибора и лекарства.

Кроме того, в широком диапазоне разных отраслей промышленности важным требованием является отслеживание товаров и объектов. Прежде всего, это относится к логистике и инфраструктуре цепочки поставок и в высшей степени регулируемым/структурированным средам рабочего процесса. Примерами являются промышленные рабочие места, регулируемые официальными регуляторами, такими как FDA (управление по продовольствию и лекарствам США), и/или сертифицированные, например согласно GMP (качественная производственная практика), GLP (качественная лабораторная практика), GCP (качественная клиническая практика) или DIN ISO или другие подобные стандарты и правила. Каждая из этих регулируемых сред требует, прежде всего, аудиторского следа и контролируемых технологий. Другим примером является прослеживаемость высокоценных продуктов, таких как промышленные запасные части, для подтверждения аутентичности и предполагаемого использования этих деталей на вторичных рынках.

Для ограничения контрафакции и обеспечения цепочки поставок и целостности рабочего процесса, включая опознавание и проверку аутентичности продуктов в рабочем процессе, разные отрасли промышленности разработали несколько разных защитных мер и решений идентификации. Широко используемые меры защиты включают в себя добавление к продукту так называемого признака защиты, причем признак довольно сложно подделать. Например, голограммы, цветопеременные чернила, защитные нити и внедренные магнитные частицы являются известными признаками защиты, которые сложно воспроизвести фальсификатору. В то время как некоторые из этих признаков защиты являются "открытыми", то есть могут быть легко увидены или иным образом опознаны пользователем продукта, другие признаки защиты являются "скрытыми", то есть они спрятаны и могут быть обнаружены только посредством использования специальных приборов, таких как источники ультрафиолетового света, спектрометры, микроскопы или детекторы магнитного поля или даже более сложное криминалистическое оборудование. Примерами скрытых

признаков защиты являются, прежде всего, надпечатки люминесцентными чернилами или чернилами, которые видны только в инфракрасной части электромагнитного спектра, но не в видимой части, особые составы материала и магнитные пигменты.

Особая группа признаков защиты, которые используются, прежде всего, в криптографии, известна как "физические неклонируемые функции" (PUFs). PUF (единственное число от PUFs прим. переводчика) является физическим объектом, который воплощен в физической структуре и его можно просто оценить, но сложно предсказать даже для взломщика с физическим доступом к PUF. PUFs зависят от уникальности своей физической микроструктуры, которая типичным образом включает в себя случайный компонент, который, по существу, уже присутствует физическом объекте или явным образом внедрен в физический объект или сгенерирован в физическом объекте во время его изготовления и который, по существу, является неконтролируемым и непредсказуемым. Соответственно, даже PUFs, произведенные по абсолютно такому же производственному процессу, отличаются, по меньшей мере, своим случайным компонентом и, таким образом, могут быть различены. В то время как в большинстве случаев PUFs являются скрытыми признаками, это не является ограничением, и возможны также открытые PUFs. Кроме того, PUFs являются идеальными для предоставления возможности пассивной (то есть, без активного транслирования) идентификации физических объектов.

Прежде всего, PUFs известны в связи с их реализацией в интегральных электронные схемах посредством минимальных неизбежных вариаций в произведенных на микросхеме микроструктурах в заданных соотнесенных с процессом допусках и, прежде всего, используемых для получения из них криптографических ключей, например в микросхемах для смарт-карт или других соотнесенных с безопасностью микросхем. Пример разъяснения и применения таких соотнесенных с микросхемами PUFs раскрыт в статье "Background on Physical Unclonable Functions (PUFs) [Предпосылки физических неклонируемых функций ((PUFs)]", Virginia Tech, Department of Electrical and Computer Engineering, 2011, которая доступна в Интернете по ссылке: http://rijndael.ece.vt.edu/puf/background.html.

Однако известны также другие типы PUFs, такие как случайное распределение волокон в используемой в качестве субстрата для изготовления банкнот бумаге, причем распределение и ориентация волокон могу быть обнаружены специальными детекторами и использованы в качестве признака защиты банкноты. Также, в качестве PUFs могут быть использованы красители, преобразующие длинноволновое излучение в коротковолновое излучение (UCDs), прежде всего секретные смеси из них.

Для оценки PUF используется так называемая схема проверки аутентичности "вызов-отклик". "Вызов" является примененным к PUF физическим воздействием, а "отклик" является реакцией на воздействие. Отклик зависит от неконтролируемой и непредсказуемой природы физической микроструктуры и, следовательно, может быть использован для проверки аутентичности PUF и, следовательно, также физического объекта, часть которого образует PUF. Особый вызов и соответствующий ему отклик вместе образуют так называемую "пару вызов-отклик" (CRP).

Основанные на использовании PUFs для проверки аутентичности продуктов способы и системы защиты от фальсификации описаны в каждой из двух Европейских патентных заявках: EP 3 340212 A1 и EP 3 340 213 (A1) и в другой Европейской патентной заявке EP 18 170 044.4, содержание каждой из которых включено в полном объеме в данную заявку посредством ссылки. Другие способы и системы защиты от фальсифицирования, основанные на автоматическом распознавании объекта, и проверка аутентичности,

основанная на таком распознавании, описаны в другой Европейской патентной заявке EP 18 170 047.7, содержание которой также включено в полном объеме в данную заявку посредством ссылки.

Асимметричная криптография, которая иногда также называется "криптографией с открытым ключом" или "криптографией с открытым/личным ключом", является известной, основанной на криптографической системе технологией, причем каждая пара ключей включает в себя открытый ключ и личный ключ. Открытые ключи могут быть широко распространенными и обычно даже общедоступными, в то время как личные ключи держатся в секрете и обычно известны только их владельцу или держателю. Асимметричная криптография делает возможным как (i) проверку аутентичности, когда открытый ключ используется для проверки подлинности, что держатель спаренного открытого ключа является источником специфической информации, например содержащих информацию сообщения или хранимых данных, посредством цифрового подписывания с помощью своего личного ключа, так и (ii) защиту информации, например сообщения или хранимых данных, посредством шифрования, посредством чего только владелец/держатель спаренного личного ключа может дешифровать сообщение, зашифрованное с открытым ключом кем-то другим.

Недавно была разработана технология блокчейна, причем блокчейн является открытым реестром в виде содержащей множество блоков данных распределенной базы данных, который поддерживает непрерывно расширяющийся список записей данных и защищен от фальсифицирования и изменения посредством криптографических средств. Известным применением технологи блокчейна является виртуальная валюта "Биткойн", используемая для денежных операций в Интернете. Другая известная блокчейн-платформа разработана, например, проектом Ethereum. По существу, блокчейн может быть описан как децентрализованный протокол для записи сделок между контрагентами, который явно фиксирует и запоминает любые изменения в своей распределенной базе данных и хранит их "вечно", то есть до тех пор, пока существует блокчейн. Хранение информации в блокчейне включает в себя цифровое подписание подлежащей хранению в блоке блокчейна информации. Кроме того, поддержание блокчейна включает в себя процесс, называемый "майнинг блокчейна", причем так называемые "майнеры", являясь частью инфраструктуры блокчейна, проверяют подлинность и запечатывают каждый блок, так что содержащаяся в нем информация сохраняется "вечно", и блок больше не может быть изменен.

Другая новая технология распределенного реестра известна под названием "Tangle", которая является архитектурой безблокового распределенного реестра и разрешений, которая является масштабируемой, облегченной и обеспечивает консенсус в децентрализованной одноранговой системе. Известная родственная использующей Tangle в качестве технической базы технология известна как "IOTA", которая является уровнем целостности данных для Интернета вещей. Однако термин "безблоковый распределенный реестр" не предназначен быть ограниченным, прежде всего, технологией "Tangle".

Краткое изложение сущности изобретения

Предметом настоящего изобретения является разработка дополнительно улучшенного способа эффективной проверки аутентичности физического объекта, такого как продукт или группы таких объектов.

Решение этой проблемы обеспечено посредством прилагаемых независимых пунктов формулы изобретения. Разные предпочтительные варианты осуществления настоящего изобретения обеспечены посредством зависимых пунктов формулы изобретения. С

целью обеспечения улучшенного ориентирования для читателя были предусмотрены несколько заголовков для структурирования нижеприведенного обзора разных аспектов общего решения проверки аутентичности, обеспеченного настоящим изобретением. Однако эти заголовки никоим образом не предназначены для ограничения раскрытого в данной заявке изобретения. Прежде всего, любые определения или термины, используемые в данной заявке, применимы во всем этом документе и не ограничиваются применением к содержащемуся в заявке конкретному разделу, аспекту или варианту осуществления.

1. Подготовка к последующей проверке аутентичности

Первый аспект изобретения направлен на способ подготовки к последующей защищенной проверке аутентичности физического объекта или группы физических объектов посредством их получателя. Прежде всего, способ может быть реализован в виде реализуемого на компьютере способа.

Способ включает в себя: (i) получение или генерирование спрогнозированных контекстных данных, представляющих спрогнозированное будущее местоположение, связанное с намеченным следующим получателем физического объекта или группы физических объектов, и связанное будущее время присутствия физического объекта или группы физических объектов в этом будущем местоположении, (ii) получение или генерирование случайных контекстных данных, указывающих на случайное местоположение и случайное время, (iii) комбинирование согласно первой предварительно определенной схеме комбинирования спрогнозированных контекстных данных и случайных контекстных данных для получения посредством этого модифицированных контекстных данных, представляющих модифицированное случайное местоположение и модифицированное случайное время, причем каждое из них получается за счет комбинирования, (iv) шифрование модифицированных контекстных данных для получения защищенного начального пакета данных, представляющего модифицированные контекстные данные, и (v) сохранение защищенного начального пакета (SSDP) данных или побуждение к его сохранению в первом хранилище данных доступным для обеспечения защищенного начального пакета данных для последующей защищенной проверки аутентичности физического объекта или группы физических объектов.

Прежде всего, местоположение может быть определено с точки зрения географических координат, например на основании соответствующих данных геолокации посредством основанной на спутниках системы радионавигации, известной как GPS, GALILEO или GLONASS.

Термин "физический объект" или сокращенно "объект" в данном аспекте относится к любому виду физического объекта, прежде всего к любому виду искусственного продукта, такому как, например, и без ограничений, фармацевтические средства или другие лечебно-оздоровительных продукты, или природному объекту, такому как, например, и без ограничений, овощам или фрагменту природного сырьевого материала, или упаковке любого или более из вышеупомянутого. Сам физический объект может включать в себя несколько частей, например, как товарный продукт, так и его упаковку. Термин "группа физических объектов" в данном конспекте относится к группе объектов, которые сами по себе являются отдельными или разделяемыми, но которые предназначены для совместной поставки, например в одном физически и/или коммерчески связанном комплекте или упаковке, и которые, таким образом, находятся в определенной связи друг с другом в отношении их поставки одному или более получателям.

Термин "проверка аутентичности" в данном контексте относится к подтверждению истинности характерного признака физического объекта, прежде всего его вида и его подлинности, заявленных достоверными уполномоченной организацией. Термин "защищенная проверка аутентичности" в данном контексте относится к проверке аутентичности, которая защищена посредством одной или более мер защиты от неправомочного вмешательства в процесс проверки или в используемые для этого средства. В качестве примера и без ограничений такая защита может включать в себя шифрование и/или цифровое подписывание информации, на которой основывается такая проверка аутентичности, в качестве таких защитных мер. Прежде всего, "защищенный" начальный пакет данных может рассматриваться как информация, которая защищена посредством любой одной или более мер защиты, чтобы сделать возможной последующую защищенную проверку аутентичности физического объекта или группы физических объектов, основанную на этой защищенной информации.

Термин "контекстные данные" в данном контексте относится к данным, представляющим, по меньше мере, особое местоположение и время, которые, таким образом, вместе определяют особый контекст, например событие. Прежде всего, контекстные данные могут относиться к событию, определяемому или определенному посредством присутствия особого физического объекта или группы физических объектом в местоположении и во время, представленных посредством связанных контекстных данных. Определенное в контекстных данных местоположение может быть, прежде всего, связано с реальным физическим положением, например выраженным в географических координатах, или с виртуальным положением, таким как особый шаг или этап в определенном рабочем потоке или технологическом потоке, или в обоих.

Термин "схема комбинирования" в данном контексте относится к схеме, такой как, но без ограничений, математическая операция, согласно которой два или более элементов данных или наборы данных могут быть скомбинированы. Схема должна быть обратимой и может, прежде всего, быть обратимой математической функцией. Например и без ограничений, такая математическая функция может быть определена с точки зрения обратимого матричного умножения. Прежде всего, комбинирование может включать в себя без ограничений простое объединение, такое как соединение бит двух или более наборов двоичных данных.

Термины "сохранение" данных или "побуждение к сохранению" в данном контексте могут, прежде всего, включать в себя сохранение данных в блокчейне или распределенном реестре косвенным образом, то есть посредством запроса актуального выполнения такого сохранения от одного или более посредников, таких как одного майнера из нескольких майнеров в случае блокчейна, который тогда фактически выполняет сохранение.

Если "включающий в себя" или "включает в себя" используется в настоящем описании и пунктах формулы изобретения, он не исключает другие элементы или шаги. Если используется неопределенный или определенный артикль при ссылке на единственное число имени существительного, например "a" или "an", "the", то это включает с себя множество таких имен существительных, если только это не установлено иначе.

Термины "первый", "второй", "третий" и тому подобное в описании и в пунктах формулы изобретения используются для различения между похожими элементами и не обязательны для описания последовательного или хронологического порядка. Следует понимать, что использованные таким образом термины являются взаимозаменяемыми в соответствующих условиях, и что описанные здесь варианты осуществления изобретения, если только это однозначно исключено или технически

невозможно, допускают работу в иных последовательностях, чем описанные или показанные здесь.

Предусмотренные здесь заголовки предназначаются для обеспечения дополнительной структуры к этому описанию настоящего изобретения и, таким образом, улучшают его удобочитаемость, но они не предназначены для его ограничения любым образом.

Способ первого аспекта настоящего изобретения определяет один из нескольких аспектов полного представленного здесь решения проверки аутентичности объекта. В пределах полного решения оно служит для подготовки последующей защищенной проверки аутентичности физического объекта или группы физических объектов посредством их получателя, например посредством получателя, представляющего узел в цепочке поставок для физического объекта или объектов. Целью данного способа является обеспечение пакета данных, который защищен посредством шифрования и который делает доступным для уполномоченных получателей, которые способны расшифровать пакет данных, исходный набор информации, который необходим для последующего процесса проверки аутентичности. Отмечено, что этот способ подготовки последующей защищенной проверки аутентичности может быть и будет во многих случаях выполняться иной уполномоченной организацией, чем сама фактическая последующая проверка аутентичности. Прежде всего, зашифрованный пакет данных содержит информацию, которая основана частично на случайных данных, которые добавляют дальнейший уровень защищенности к процессу проверки аутентичности как целому, так как в отличие от связанных с фактической цепочкой поставок контекстных данных, таких как местоположение и время, в момент которого конкретный физический объект присутствует в данном местоположении, случайные данные типичным образом не могут быть спрогнозированы неуполномоченной третьей стороной.

Ниже описываются предпочтительные варианты осуществления данного способа, которые могут произвольно комбинироваться друг с другом или с другими аспектами настоящего изобретения, кроме случаев, когда это однозначно исключено или технически невозможно.

(A) Избранные варианты осуществления, имеющие отношение, прежде всего, к созданию защищенного начального пакета данных

В некоторых вариантах осуществления шифрование модифицированных контекстных данных включает в себя шифрование модифицированных контекстных данных посредством схемы асимметричного шифрования и связанного открытого ключа, принадлежащего намеченному следующему получателю. В отличие от симметричного шифрования, где ключ шифрования должен оставаться секретным и, таким образом, должен обмениваться защищенным образом, использование асимметричного шифрования позволяет использовать для шифрования открытые ключи. В отличие от ключей для симметричного шифрования, такими открытыми ключами можно обмениваться открыто без создания элементов защиты.

В некоторых вариантах осуществления шифрование модифицированных контекстных данных также включает в себя цифровое подписывание модифицированных контекстных данных или защищенного начального пакета данных, полученных в результате шифрования. Цифровое подписывание может, прежде всего, выполняться посредством схемы асимметричного шифрования и связанного личного ключа, принадлежащего поставщику физического объекта или группы физических объектов или подписывающей уполномоченной организации. Цифровое подписывание может быть использовано для дальнейшего усиления защиты последующей основанной на модифицированных контекстных данных проверки аутентичности, поскольку оно добавляет дальнейший

уровень защиты, разрешающий проверку подлинности зашифрованных модифицированных контекстных данных получателем.

Термин "цифровая подпись" или "цифровое подписывание" и т.п. в данном контексте относится к использованию комплекта из одного или более цифровых значений, которые подтверждают идентификатор отправителя или создателя цифровых данных и целостность последних. Часто используемый способ создания цифровой подписи включает в себя генерирование значения хеш-функции из подлежащих защите данных посредством применения подходящей криптографической хеш-функции. Это значение затем шифруется с личным ключом (также иногда называемым "защищенным ключом") асимметричной криптографической системы, например основанной на криптографической системе RSA, в которой личный ключ типичным образом известен только отправителю/создателю. Обычно цифровая подпись сама содержит цифровые данные, а также значение хеш-функции, полученное из них отправителем/получателем. Затем получатель может применить эту же криптографическую хеш-функцию к полученным цифровым данным, использовать открытый ключ, соответствующий личному ключу, для дешифрования значения хеш-функции, содержащейся в цифровой подписи, и сравнить дешифрованное значение хеш-функции из цифровой подписи со значением хеш-функции, сгенерированным посредством применения криптографической хеш-функции к полученным цифровым данным. Если оба значения хеш-функции совпадают, это указывает на то, что цифровая информация не модифицировалась и, таким образом, не была взломанной. Кроме того, аутентичность отправителя/создателя цифровых данных подтверждается посредством асимметричной криптографической системы, которая гарантирует, что шифрование с использованием открытого ключа работает, только если зашифрованная информация была зашифрована с личным ключом, математически спаренным с открытым ключом. Представление цифровой подписи может быть реализовано, прежде всего, с использованием RFID передатчика или одномерного или многомерного штрихкода, такого как QR-код или DATAMATRIX-код, или просто в виде многозначного числа.

Термин "криптографическая хеш-функция" в данном контексте относится к специальному типу хеш-функции, то есть математической функции или алгоритму, которая преобразует данные произвольного размера в битовую строку постоянного размера (значение хеш-функции), которая также предназначена быть односторонней функцией, то есть функцией, которая легко вычисляется для любого входного значения, но с трудом поддается инвертированию, если она является образом случайных входных данных. Предпочтительно, криптографическая хеш-функция является так называемой "устойчивой к конфликтам" хеш-функцией, то есть хеш-функцией, которая выполнена так, что сложно, прежде всего практически невозможно, найти два разных набора d1 и d2 данных так, что hash(d1)=hash(d2). Известными примерами таких хеш-функций являются хеш-функции SHA-семейства, например функция SHA-3, или хеш-функции BLAKE-семейства, например функция BLAKE2. Прежде всего, могут быть использованы так называемые "доказуемо защищенные криптографические хеш-функции". Они являются хеш-функциями, для которых может быть математически доказан некоторый достаточный уровень защиты.

В некоторых вариантах осуществления сохранение защищенного начального пакета данных в первом хранилище данных включает в себя сохранение защищенного начального пакета данных в блокчейне или в безблоковом распределенном реестре. Таким образом, начальный пакет данных может быть записан и сохранен таким способом, что по существу невозможно его фальсифицировать, например разрушить

или манипулировать с ним, неправомочным образом и, прежде всего, без того, что такая попытка фальсифицирования становится очевидной. Кроме того, сохранение защищенного начального пакета данных в блокчейне или в безблоковом распределенном реестре допускает легкий доступ к начальному пакету данных удаленно, например, авторизованным получателем вдоль цепочки поставок связанного физического объекта или группы объектов.

(Б) Избранные варианты осуществления, имеющие отношение, прежде всего, к созданию данных инициализации

В некоторых вариантах осуществления, в первом варианте, способ также включает в себя: (i) обнаружение посредством по меньшей мере одного или более датчиков по меньшей мере одной отличительной характеристики физического объекта или группы физических объектов для получения для каждой отличительной характеристики соответствующих данных идентификации, представляющих идентификатор связанного физического объекта или группы физических объектов, и (ii) применение второй предварительно определенной криптографической хеш-функции к набору данных, полученных из комбинирования согласно второй предварительно определенной схеме комбинирования, одних или более соответствующих данных идентификации, полученных из набора по меньшей мере из одной отличительной характеристики и случайных контекстных данных, для получения исходного значения хеш-функции.

Во втором варианте способ также включает в себя: (i) обнаружение посредством по меньшей мере одного или более датчиков по меньшей мере одной отличительной характеристики физического объекта или группы физических объектов для получения для каждой отличительной характеристики соответствующих данных идентификации, представляющих идентификатор связанного физического объекта или группы физических объектов, (ii) применение к каждым из данных идентификации соответствующей первой предварительно определенной криптографической хеш-функции для получения соответствующего исходного значения хеш-функции, связанного с соответствующей отличительной характеристикой, (iii) применение второй предварительно определенной криптографической хеш-функции к набору данных, полученных из комбинирования согласно второй предварительно определенной схеме комбинирования, одного или более соответствующих исходных значений хеш-функции, полученных из набора по меньшей мере из одной отличительной характеристики и случайных контекстных данных, для получения исходного значения (Но) хеш-функции. Соответственно, второй вариант отличается от первого варианта тем, что добавляется шаг (ii) применения первого предварительно определенного значения хеш-функции.

В третьем варианте способ также включает в себя применение второй предварительно определенной криптографической хеш-функции к случайным контекстным данным для получения исходного значения хеш-функции. Соответственно, третий вариант отличается от первого и второго вариантом тем, что он не основан на обнаружении любых отличительных характеристик физического объекта или группы физических объектов и получении основанного на них исходного значения Но хеш-функции. Вместо этого он основывается только на случайных контекстных данных в качестве основных входных данных.

Для всех трех вышеупомянутых вариантов способ включает в себя в дополнение данные инициализации, представляющие соответствующее исходное значение хеш-функции.

Прежде всего, подход согласно второму варианту основывается, таким образом, на стеке хешей, включающем в себя два последовательных уровня операции хеширования.

Первый уровень относится к применению соответствующей первой криптографической хеш-функции к соответствующим данным идентификации, и второй уровень относится к применению соответствующей второй криптографической хеш-функции к комбинации исходного значения хеш-функции, полученной из первого уровня, и случайных контекстных данных. Использование обоих исходных значений хеш-функции, полученных из отличительных характеристик и контекстной информации, увеличивает энтропию (в смысле теории информации и математики) получающихся данных инициализации. Это делает возможным очень высокий уровень защиты всего процесса проверки аутентичности даже в случаях, когда соответствующая индивидуальная энтропия исходных значений хеш-функции и/или контекстной информации довольно ограничена и сама не сделает возможным достаточный уровень защиты. В дополнение, это также делает возможным ограничение количества задействованных данных, прежде всего данных, которые должны быть обменены, непосредственно или опосредовано, с получателем и, таким образом, оптимизацию эффективности процесса проверки аутентичности. В отношении термина "схема комбинирования" ссылка дается на приведенное выше ее определение.

С другой стороны, первый и третий варианты имеют преимущество более низкой сложности по сравнению с первым преимуществом и может быть, прежде всего, пригодной для применений, где достаточна более низкая степень защиты, чем та, которая может быть достигнута посредством первого варианта.

В некоторых связанных вариантах осуществления отличительная характеристика обеспечивается в виде особого набора из одной или более индивидуальных отличительных свойств физического объекта или группы физических объектов, посредством которых они могут быть надежно идентифицированы. Такие свойства могут, прежде всего, включать в себя свойства, которые довольно сложно фальсифицировать, например, поскольку они, прежде всего, защищены от фальсификации и/или поскольку их очень трудно фальсифицировать уже по их природе. Европейская патентная заявка EP 18 170 047.7 подробно описывает такие отличительные характеристики и их использование с целью проверки аутентичности объекта.

В других связанных вариантах осуществления отличительная характеристика обеспечивается особыми признаками защиты, прежде всего, добавленными или созданными в или на физических объектах или группе физических объектов. Это, прежде всего, делает возможной проверку аутентичности таких физических объектов или групп физических объектов, которые сами по себе не обеспечивают надежные отличительные характеристики, на которых может базироваться защищенная проверки аутентичности.

В других связанных вариантах осуществления по меньшей мере одна из отличительный характеристик включает в себя физическую неклонируемую функцию PUF. Кроме того, (i) обнаружение по меньшей мере одной отличительной характеристики для получения связанных с ней соответствующих данных идентификации включает в себя: (i-1) применение соответствующего запроса соответствующей предварительно определенной схемы проверки аутентичности "запрос-ответ" к PUF для инициирования ответа посредством PUF согласно схеме проверки аутентичности в ответ на запрос, и (i-2) обнаружение соответствующего ответа и генерирование соответствующих данных идентификации, представляющих этот запрос, (ii) применение соответствующей первой предварительно определенной криптографической хеш-функции включает в себя применение соответствующей первой предварительно определенной криптографической хеш-функции к данным, представляющим ответ для получения соответствующего связанного с PUF исходного значения хеш-функции, и (iii) вывод данных инициализации

включает в себя вывод соответствующих данных идентификации, связанных с отличительной характеристикой, причем данные идентификации включают в себя представление соответствующего связанного с PUF исходного значения хеш-функции. Таким образом, особая отличительная характеристика физической неклонируемой функции может быть использована в качестве основания для предоставления возможности проверки аутентичности физического объектов или групп физических объектов, делает возможным еще больший уровень защиты из-за практически невозможного клонирования PUFs.

В некоторых вариантах осуществления применение второй предварительно определенной криптографической хеш-функции для получения исходного значения хеш-функции также включает в себя применение ее в дополнение к независимой от времени и от местоположения информации, идентифицирующей физический объект или группу физических объектов или связанной соответственно с ним или с ней. Прежде всего, физический объект или группа физических объектов может быть, соответственно, продуктом или группой продуктов, и независимая от времени или независимая от местоположения информация может содержать серийный номер, связанный с продуктом или группой продуктов. Применение второй предварительно определенной криптографической хеш-функции к независимой от времени или независимой от местоположения информации может быть, прежде всего, выполнено посредством применения хеш-функции к набору или другой комбинации данных, причем такой набор или другая комбинация данных представляет, среди прочего, независимую от времени или независимую от местоположения информацию. Добавление независимой от времени и местоположения информации к данным, к которым является прилагаемой вторая предварительно определенная криптографическая хеш-функция, добавляет дополнительную энтропию и может, таким образом, даже повысить достижимую защиту всего процесса проверки аутентичности. Независимая от времени и местоположения информация, такая как, например, один или более серийных номеров, может быть, прежде всего, представлена маркировкой на физическом объекте или группе физических объектов и/или может быть реализована с использованием RFID передатчика или одномерного или многомерного штрихкода, такого как QR-код или DATAMATRIX-код, или просто в виде многозначного числа.

В некоторых вариантах осуществления вывод данных инициализации включает в себя одно или более из следующего: (i) добавление представления данных инициализации к физическому объекту или группе физических объектов, (ii) сохранение представления данных инициализации или побуждение к его сохранению в третьем хранилище данных и добавление к физическому объекту или группе объектов представления указателя, указывающего, где данные инициирования могут быть доступными в третьем хранилище данных. Это третье хранилище данных может быть одинаковым или отличным от вышеупомянутого первого хранилища данных. Обе опции (i) и (ii) делают возможным особо простой способ передачи данных инициализации следующему получателю вдоль цепочки поставок для физического объекта или группы физических объектов. Прежде всего, не должен быть установлен прямой канал связи, такой как электронный обмен данными, между поставщиком и соответствующим получателем объектов или группы объектов.

(B) Избранные варианты осуществления, имеющие отношение, прежде всего, к подготовке другой последующей проверки аутентичности другим получателем

В некоторых вариантах осуществления способ также включает в себя: (i) получение запроса для определения другого защищенного начального пакета данных, связанного

с другими спрогнозированными контекстными данными, представляющими другое спрогнозированное будущее местоположение, связанное с разным другим намеченным следующим получателем физического объекта или группы физических объектов, и связанное будущее время присутствия физического объекта или группы физических объектов в этом другом будущем местоположении, и (ii) осуществление настоящего способа, основанного на этих других спрогнозированных контекстных данных, для определения и сохранения или побуждения к сохранению затребованного другого защищенного начального пакета данных, связанного с другими спрогнозированными контекстными данными. Этот подход делает возможным продвижение физических объектов или группы физических объектов вдоль цепочки поставок таким образом, что такой другой намеченный следующий получатель может запросить у соответствующего предшествующего узла вдоль цепочки поставок, который выполнен для осуществления способа согласно настоящим вариантам осуществления, генерирование соответствующего начального защищенного начального пакета данных для следующего скачка вдоль цепочки поставок, начиная с этого другого намеченного получателя. Соответственно, не каждый узел вдоль цепочки поставок пригоден для подготовки проверки аутентичности у другого получателя, а вместо этого такому предшествующему узлу, который может, прежде всего, играть роль центрального или общего органа для управления определением и сохранением других защищенных начальных пакетов данных, может быть вместо этого послан запрос на выполнения такой подготовки и обеспечения соответствующего начального пакета данных для следующего скачка. Прежде всего, затребованный другой начальный пакет данных может быть определен на основании, в дополнение к соответствующим спрогнозированным контекстным данным, вновь сгенерированных случайных контекстных данных или случайных контекстных данных, определенных ранее в ходе определения соответствующего начального пакета данных для предыдущего получателя.

В некоторых связанных вариантах осуществления способ также включает в себя сохранение полученного другого защищенного начального пакета данных или побуждение к его сохранению в хранилище данных, которое доступно другому намеченному следующему получателю. Прежде всего, без ограничений хранилище данных может быть вышеупомянутым первым хранилищем данных. Сохранение полученного другого защищенного начального пакета данных в хранилище данных обеспечивает эффективный способ сделать его доступным запрашивающему следующему получателю таким образом, когда не требуется прямой канал связи между обеспечивающим начальный пакет данных узлом и запрашивающим следующим получателем. Прежде всего, хранилище данных может снова быть блокчейном или безблоковым распределенным реестром, который обеспечивает очень высокий уровень безопасности против фальсифицирования этого другого защищенного начального пакета данных неуполномоченными третьими сторонами.

(Г) Варианты осуществления, связанные, прежде всего, с цифровым подписыванием исходного значения хеш-функции

В некоторых вариантах осуществления способ также включает в себя: (i) подписывание полученного исходного значения хеш-функции цифровой подписью, принадлежащей поставщику физического объекта или группы физических объектов соответствующему следующему получателю, и (ii) включение цифровой подписи в выводимые соответствующие данные инициализации или другие данные инициализации, соответственно. Поставщик может быть, прежде всего, исходным поставщиком или промежуточным поставщиком вдоль цепочки поставок для физического объекта или

группы физических объектов. Следовательно, соответствующие данные инициализации относятся к исходным данным инициализации в случае исходного поставщика и к соответственно другим данным инициализации в случае промежуточного поставщика. Добавление цифровой подписи дополнительно повышает уровень защиты, поскольку он обеспечивает защищенную возможность проверки соответствующим получателем подлинности аутентичности подписанного исходного значения хеш-функции в выводимых данных инициализации.

(Д) Система для подготовки последующей защищенной проверки аутентичности

Второй аспект настоящего изобретения относится к системе для подготовки последующей защищенной проверки аутентичности физического объекта или группы объектов согласно первому аспекту настоящего изобретения по любому из предшествующих пунктов формулы изобретения. Прежде всего, такая система включает в себя компьютер, средства для направления запроса к физической неклонируемой функции, относящейся к физическому объекту или группе физических объектов, и один или более датчиков для обнаружения ответа, сгенерированного в ответ на запрос посредством физической неклонируемой функции, и выполнена для осуществления данного способа согласно одному или более из описанных здесь его вариантов осуществления. Соответственно, описание данного способа и его вариантов осуществления и его преимуществ относится с соответствующими поправками к данной системе.

2. Способ проверки аутентичности физического объекта или группы физических объектов

Третий аспект настоящего изобретения относится к способу проверки аутентичности физического объекта или группы физических объектов. Прежде всего, способ включает в себя разные факультативные варианты и может быть осуществлен в виде реализуемого на компьютере способа.

Способ включает в себя:

(i) получение и дешифрование защищенного начального пакета данных, представляющего зашифрованные контекстные данные, представляющие местоположение и связанное время, для восстановления контекстных данных,

(ii) получение или определение текущих контекстных данных, представляющие текущее местоположения физического объекта или группы физических объектов и связанное текущее время присутствия физического объекта или группы физических объектов в этом текущем местоположении,

(iii) комбинирование согласно предварительно определенной схеме комбинирования текущих контекстных данных с дешифрованными контекстными данными для определения посредством этого тестовых контекстных данных, причем схема комбинирования определяет операцию, обратную соответствующей операции комбинирования, использованной прежде для генерирования полученных контекстных данных,

(iv) получение доступа к данным инициализации, связанным с физическим объектом или группой физических объектов, для восстановления из них исходного значения хеш-функции, представленного посредством данных инициализации.

Способ также включает в себя согласно разным вариантам (v) один из следующих процессов от A) до B):

A) обнаружение посредством одного или более датчиков по меньшей мере одной отличительной характеристики физического объекта или группы физических объектов для получения соответствующих данных идентификации, связанных с соответствующей

отличительной характеристикой, причем эти данные идентификации представляют предполагаемый идентификатор связанного физического объекта или группы физических объектов, и

генерирование тестового значения хеш-функции посредством применения второй предварительно определенной криптографической хеш-функции к комбинации, согласно другой предварительно определенной схеме комбинирования, тестовых контекстных данных и каждых из данных идентификации и, предпочтительно, независимой от времени и независимой от местоположения информации, идентифицирующей физический объект или группу физических объектов или связанной с ним или с ней, или

Б) обнаружение посредством одного или более датчиков по меньшей мере одной отличительной характеристики физического объекта или группы физических объектов для получения соответствующих данных идентификации, связанных с соответствующей отличительной характеристикой, причем эти данные идентификации представляют предполагаемый идентификатор связанного физического объекта или группы физических объектов,

применение соответствующей первой предварительно определенной криптографической хеш-функции к соответствующим данным идентификации для получения соответствующего исходного значения хеш-функции, связанного с отличительной характеристикой, и

генерирование тестового значения хеш-функции посредством применения второй предварительно определенной криптографической хеш-функции к комбинации, согласно другой предварительно определенной схеме комбинирования, из тестовых контекстных данных и каждого из исходных значений хеш-функции и, предпочтительно независимой от времени и независимой от местоположения, информации, идентифицирующей физический объект или группу физических объектов или связанной с ним или с ней,

В) генерирование тестового значения хеш-функции посредством применения второй предварительно определенной криптографической хеш-функции к тестовым контекстным данным или к комбинации, согласно другой предварительно определенной схеме комбинирования, из тестовых контекстных данных и независимой от времени и от местоположения информации, идентифицирующей физический объект или группу физических объектов или связанной с ним или с ней.

Для каждого из вышеупомянутых процессов А)-В) вторая предварительно определенная криптографическая хеш-функция равна соответствующей криптографической хеш-функции, использованной прежде для определения исходного значения хеш-функции, представленного данными инициализации, и причем другая схема комбинирования равна соответствующей схеме комбинирования, использованной прежде для определения исходного значения хеш-функции, представленного данными инициализации.

Способ также включает в себя: (vi) генерирование результата первого считывания, включающего в себя (vi-1) представление тестового значения хеш-функции и представление исходного значения хеш-функции, или (vi-2) сравнение выходных данных, указывающих, совпадают или нет, согласно по меньшей мере одному предварительно определенному критерию совпадения, тестовое значение хеш-функции и исходное значение хеш-функции и, таким образом, указывающих на аутентичность физического объекта или группы физических объектов.

В случае если один или более вышеупомянутых шагов способа по любой причине оказываются неудачными, например, если не может быть организован успешный доступ к данным инициализации или защищенный начальный пакет данных не может быть

считан, результат первого считывания может, прежде всего, включать в себя или состоять из выходных данных, указывающих на ошибку аутентификации.

Этот способ проверки аутентичности (способ проверки аутентичности) соотносится со способом первого аспекта настоящего изобретения (способ подготовки) в том отношении, что последний служит для подготовки последующей проверки аутентичности физического объекта или группы физических объектов в соответствии со способом проверки аутентичности согласно третьему аспекту настоящего изобретения. Кроме того, этот способ проверки аутентичности основывается на концепции, что проверка аутентичности может быть выполнена посредством сравнения двух значений хеш-функции, одно из которых было прежде сгенерировано посредством другой уполномоченной организации с помощью способа подготовки к последующей проверке аутентичности согласно первому аспекту, а другое из них получено посредством соответствующей проверки аутентичности самим получателем на основании как связанного защищенного начального пакета данных, обеспеченного в качестве результата способа подготовки, так и данных идентификации, полученных от подлежащего проверке аутентичности физического объекта или группы объектов.

Соответственно, начальный пакет данных обеспечивает информацию, связанную со спрогнозированными контекстными данными получателя, то есть прежде всего, местоположением и временем, где и когда получатель намеревается получить физический объект или группу физических объектов, и способ проверки аутентичности затем использует этот начальный пакет данных, полученное значение исходной хеш-функции, сгенерированное способом подготовки, его текущие контекстные данные, и для вариантов способа А) и Б) дополнительно данные идентификации (или соответствующие исходные значения хеш-функции), полученные из обнаружения одной или более отличительных характеристик физического объекта или группы физических объектов для генерирования тестового значения хеш-функции. Если физический объект или группа физических объектов являются оригинальными и получены получателем в спрогнозированном местоположении и времени (по меньшей мере, в некотором определенном поле допусков, которое может, прежде всего, соответствовать точности определения спрогнозированных контекстных данных и текущих контекстных данных), тестовое значение хеш-функции будет успешной реконструкцией исходного значения хеш-функции, сгенерированного посредством способа подготовки и, соответственно, второе и тестовое значения хеш-функции, полученные посредством способа проверки аутентичности, будут совпадать, указывая, таким образом, на удачную проверку аутентичности. Иначе проверка аутентичности будет неудачной. Процесс сравнения исходного и тестового значений хеш-функции может выполняться автоматически или вручную на основании выходных значений этих двух значений хеш-функции.

(А) Избранные варианты осуществления, связанные, прежде всего, с получением данных идентификации

В некоторых вариантах осуществления по меньшей мере одна из отличительных характеристик включает в себя физическую неклонируемую функцию PUF, и обнаружение связанной с ней отличительной характеристики для получения соответствующих данных идентификации включает в себя: (i) применение соответствующего запроса соответствующей предварительно определенной схемы проверки аутентичности "запрос-ответ" к PUF для инициирования в ответ на запрос ответа согласно схеме проверки аутентичности, и (ii) обнаружение соответствующего ответа PUF в соответствии с соответствующей схемой проверки аутентичности "запрос-ответ" в ответ на запрос и извлечение из него соответствующих данных идентификации.

Поскольку PUFs самих по себе практически невозможно клонировать или иным способом преобразовывать, их использование дополнительно повышает достижимый уровень защиты всего решения проверки аутентичности.

В некоторых вариантах осуществления получение данных идентификации включает в себя: (i) основанное на датчике обнаружение одной или более отличительных характеристик физического объекта или группы физических объектов, (ii) генерирование данных объекта, представляющих одну или более отличительных характеристик физического объекта или группы физических объектов, (iii) передачу данных объекта системе для автоматического распознавания объекта, и (iv) получение данных идентификации с цифровой подписью от системы в ответ на передачу данных объекта. Эти варианты осуществления относятся, прежде всего, к способу проверка аутентичности, такому как описанный в EP 18 170 044.4, где, прежде всего, одна или более характеристик подлежащего проверке аутентичности физического объекта или группы физических объектов, причем характеристики сами по себе образуют часть объекта или группы объектов и не должны добавляться в виде отдельного признака защиты, образуют основу идентификации и, таким образом, проверки аутентичности объекта или группы объектов. В этом случае система автоматического распознавания объекта типичным образом отличается от самого получателя и выполнена для получения данных объекта и обеспечения в ответ результата распознавания объекта в виде данных идентификации с цифровой подписью.

В некоторых вариантах осуществления физический объект или группа физических объектов включают в себя маркировку. Маркировка включает в себя представление данных инициализации и/или представление указателя, указывающего на местоположение, где может быть обеспечен доступ к данным инициализации, и обеспечение доступа к данным инициализации включает в себя, если применимо: (i) считывание представления данных инициализации в маркировке или (ii) считывание представление указателя в маркировке и получение данных инициализации из указанного указателем местоположения хранилища данных, и если данные инициализации включают в себя цифровую подпись, проверку подлинности соответствующего поставщика физического объекта или группы физических объектов на основании проверки подлинности цифровой подписи. Соответственно, эти варианты осуществления являются, прежде всего, полезными, если маркировка служит передаче данных инициализации непосредственно или опосредовано через указатель получателю в качестве входных данных способа проверки аутентичности. Таким образом, данные инициализации передаются самим объектом или группой объектов, так что не требуется установления другого накала связи от соответствующего поставщика к соответствующему следующему получателю.

(Б) Избранные варианты осуществления, связанные, прежде всего, с выводом и сохранением данных, связанных с проверкой аутентичности

В некоторых вариантах осуществления способ также включает в себя вывод представления текущих контекстных данных и их подмножества или полученной из них информации в качестве результата второго считывания. Соответственно, результат второго считывания может, прежде всего, представлять данные, связанные с управлением цепочкой поставок, поскольку он показывает контекстные данные, описывающие местоположение и время, в котором объект или группа объектов присутствует у получателя, определяющего узел вдоль цепочки поставок. Таким образом, способ проверки аутентичности в то же время служит в качестве источника данных управления цепочкой поставок.

В некоторых вариантах осуществления способ также включает в себя процесс, включающий в себя сохранение результата первого считывания или побуждение к его сохранению в блоке блокчейна первого набора из одного или более блокчейнов или в одном или более узлах безблокового распределенного реестра первого набора из одного или более безблоковых распределенных реестров. Прежде всего, побуждение к сохранению результата первого считывания может включать в себя побуждение другого устройства, такого как отдельный и факультативно даже расположенный удаленно компьютер, сконфигурированный для выполнения соответственно (i) майнинга блокчейна или (ii) записи в узел безблокового распределенного реестра, таким образом, для сохранения результата первого считывания. Эти варианты осуществления делают возможным защищенное, надежное сохранение с очень высокой целостностью данных, так что по существу невозможны манипулирование или удаление или их фальсифицирование иным образом или потеря таких данных, например вследствие непреднамеренного или преднамеренного удаления или вследствие повреждения данных. Таким образом, остается доступной вся история проверки аутентичности. Кроме того, может иметься доступ к сохраненной информации при наличии доступа к блокчейну соответственно распределенного реестра. Это делает возможным надежное и распределенное сохранение и получение доступа к сохраненным данным, например, для целей проверки целостности, такой как проверка, был ли поставщик продукта (объекта) фактически производителем продукта. На основании этого варианта осуществления материальный мир, частью которого являются объекты, может быть связан с возможностями технологии блокчейна или безблокового распределенного реестра. Таким образом, может быть достигнута высокая степень прослеживаемости происхождения и цепочки поставок физических объектов, таких как продукты.

В некоторых связанных вариантах осуществления (i) обнаружение отличительных характеристик физического объекта или группы физических объектов включает в себя обнаружение нескольких разных отличительных характеристик для получения основанных на нем для каждой отличительной характеристики соответствующего индивидуального набора данных идентификации, представляющих физический объект или группу физических объектов, (ii) генерирование тестового значения хеш-функции выполняется для каждого из индивидуальных наборов данных идентификации отдельно, так чтобы получить для каждого из индивидуальных наборов данных идентификации соответствующее индивидуальное тестовое значение хеш-функции, (iii) генерирование результата первого считывания выполняется для каждого из индивидуальных тестовых значений хеш-функции отдельно, так чтобы получить для каждой из отличительных характеристик соответствующий индивидуальный результат первого считывания, и (iv) процесс сохранения включает в себя сохранение соответственно каждого из индивидуальных результатов первого считывания, побуждая к их сохранению в блоке соответствующего индивидуально выделенного блокчейна в первом наборе блокчейнов или в одном или более узлов соответствующего индивидуально выделенного безблокового распределенного реестра в первом наборе безблоковых распределенных реестров. Таким образом, достигаемая защита может быть дополнительно усилена, поскольку, с одной стороны, привлекаются другие отличительные характеристики физического объекта или группы физических объектов, которые увеличивают сложность самой фальсификации и, с другой стороны, индивидуальные результаты первого считывания хранятся в разных индивидуально выделенных блокчейнах, что увеличивает сложность манипулирования ими или иным образом раскрытия несанкционированным способом связанной дорожки данных, хранящейся в среде блокчейна или в

соответствующей среде безблокового распределенного реестра. В некоторых вариантах эти варианты осуществления могут быть реализованы в дополнение к любому из вышеописанных процессов А) и Б).

В некоторых других связанных вариантах осуществления процесс сохранения также включает в себя сохранение результата второго считывания или побуждение к его сохранению соответственно в блоке блокчейна второго набора из одного или более блокчейнов, причем блокчейн является отдельным от блокчейнов в первом наборе блокчейнов, или в одном или более узлов безблокового распределенного реестра второго набора из одного или более безблоковых распределенных реестров, причем безблоковый распределенный реестр соответственно является отдельным от безблоковых распределенных реестров в первом наборе из безблоковых распределенных реестров. Эти варианты осуществления делают возможным дополнительное сохранение и, таким образом, сохранение результата второго считывания независимо от результата первого считывания в соответствующем другом блокчейне, обеспечивая, таким образом, преимущества, обсужденные в связи с непосредственно предшествующим вариантом осуществления также в связи с результатом второго считывания. Использование разных блокчейнов или безблоковых распределенных реестров для первого и второго результатов считывания также обеспечивает преимущество легкой поддержки комбинирования существующего (второго) блокчейна или безблокового распределенного реестра, соответственно, для результата второго считывания с дополнительным блокчейном или безблоковым распределенным реестром, соответственно, для результата первого считывания. Соответственно, могут быть легко сделаны возможными разные права доступа, и управление блокчейнами может быть в руках разных организаций. Прежде всего, эти варианты осуществления могут быть использованы для проверки, был ли поставщик продукта фактически его производителем, и была ли цепочка поставок такой, как ожидалось. В дополнение, это может быть использовано для дальнейшего повышения достижимого уровня защиты, поскольку контекстная информация может быть использована для определения задним числом местоположений или лиц, связанных с цепочкой поставок, где могла произойти возможная фальсификация, а также возможных дат или временных рамок.

В некоторых других связанных вариантах осуществления, где процесс сохранения связан с блокчейнами:

(i) сохранение соответствующего отдельного результата первого считывания в блоке соответствующего блокчейна в первом наборе блокчейнов также включает в себя сохранение указателя на кросс-блокчейн, который логически устанавливает соответствие блока блокчейна в первом наборе блокчейнов с соответствующим блоком соответствующего блокчейна во втором наборе блокчейнов, в блоке блокчейна в первом наборе блокчейнов, и

(ii) сохранение результата второго считывания в блоке блокчейна во втором наборе блокчейнов также включает в себя сохранение указателя на кросс-блокчейн, который логически устанавливает соответствие блока блокчейна во втором наборе блокчейнов с соответствующим блоком соответствующего блокчейна в первом наборе блокчейнов, в блоке блокчейна во втором наборе блокчейнов.

Аналогичным образом, в некоторых других связанных вариантах осуществления, где процесс сохранения связан с безблоковыми распределенными реестрами:

(i) сохранение соответствующего индивидуального результата первого считывания в узле соответствующего безблокового распределенного реестра в первом наборе безблоковых распределенных реестров включает в себя сохранение указателя на кросс-

реестр, который логически устанавливает соответствие узла безблокового распределенного реестра в первом наборе безблоковых распределенных реестров с соответствующим узлом безблокового распределенного реестра во втором наборе безблоковых распределенных реестров, в узле безблокового распределенного реестра в первом наборе безблоковых распределенных реестров, и

(ii) сохранение результата второго считывания в узле соответствующего безблокового распределенного реестра во втором наборе безблоковых распределенных реестров также включает в себя сохранение указателя на кросс-реестр, который логически устанавливает соответствие узла безблокового распределенного реестра во втором наборе безблоковых распределенных реестров с соответствующим узлом безблокового распределенного реестра в первом наборе безблоковых распределенных реестров, в узле безблокового распределенного реестра во втором наборе безблоковых распределенных реестров.

Таким образом, блокчейны или безблоковые распределенные реестры первого набора блокчейнов или безблоковых распределенных реестров могут быть взаимосвязанными посредством указателей соответственно кросс-блокчейнов или указателей кросс-реестров соответственно со вторым набором блокчейнов или безблоковых распределенных реестров, и наоборот.Это может быть использовано для дальнейшего повышения достижимого уровня защиты настоящего решения проверки аутентичности объекта. Прежде всего, это может быть использовано для обнаружения попыток фальсификации или контрафакции объектов в разных точках вдоль цепочки поставок. Например, настоящий вариант осуществления делает возможным обнаружение местоположения и/или момента времени такой попытки.

(B) Избранные варианты осуществления, связанные, прежде всего, с определением других данных инициализации для последующей защищенной проверки аутентичности

В некоторых других связанных вариантах осуществления способ также включает в себя определение другого защищенного начального пакета данных и, факультативно, других связанных данных инициализации для последующей защищенной проверки аутентичности физического объекта или группы физических объектов следующим его получателем. Эти варианты осуществления относятся к возможному варианту предоставления возможности одной или более других последующих защищенных проверок аутентичности физического объекта или группы физических объектов следующим получателем вдоль цепочки поставок. Фактически согласно настоящему варианту описанный здесь способ по существу повторяется для каждого следующего шага распространения, то есть скачка, вдоль цепочки поставок, так что для каждого такого скачка генерируются и используются новые специальные данные инициализации для следующей последующей проверки аутентичности следующим получателем. Это имеет преимущество, что один и тот же процесс может быть повторно использован для нескольких скачков вдоль цепочки поставок.

В некоторых связанных вариантах осуществления определение другого защищенного начального пакета данных (и факультативно других данных инициализации) включает в себя запрос на определение такого другого защищенного начального пакета данных (и факультативно других данных инициализации) для последующей защищенной проверки аутентичности физического объекта или группы физических объектов другим его получателем у авторизованного поставщика другого защищенного начального пакета данных (и факультативно других данных инициализации) и получение, например через блок-фейн или распределенный реестр или другое хранилище, в ответ на запрос запрошенного другого защищенного начального пакета данных (и факультативно

других данных инициализации). Это делает возможной, прежде всего, централизацию определения других защищенных начальных пакетов данных (и факультативно других данных инициализации) для нескольких скачков вдоль цепочки поставок у единственной уполномоченной организации, обеспечивая таким образом особо высокую эффективность. Центральный авторизованный поставщик может, прежде всего, совпадать с уполномоченной организацией, выполняющей исходное, то есть первое, определение соответствующего первого другого защищенного начального пакета данных (и факультативно других данных инициализации) в начале цепочки поставок, например, исходным производителем или распределителем физического объекта или группы физических объектов, поставляемых и проверяемых на аутентичность вдоль цепочки поставок.

В некоторых факультативных вариантах осуществления определение другого защищенного начального пакета данных включает в себя осуществление способа первого аспекта, так что спрогнозированные контекстные данные представляют спрогнозированное будущее местоположение следующего намеченного получателя физического объекта или группы физических объектов и связанное будущее время присутствия физического объекта или группы физических объектов в этом будущем местоположении. Согласно этим вариантам каждый соответствующий текущий получатель физического объекта или группы физических объектов сам определяет защищенный начальный пакет данных для соответствующего следующего получателя, то есть для соответственно следующего скачка вдоль цепочки поставок. Это имеет преимущество, что никакая центральная авторизованная уполномоченная организация не должна заботиться об определении всех защищенных начальных пакетов данных для соответствующих нескольких скачков вдоль цепочки поставок и, следовательно, и нет необходимости в наличии соответствующего канала связи между получателем и такой центральной уполномоченной организацией.

В некоторых связанных вариантах осуществления способ также включает в себя при осуществления способа первого аспекта согласно связанным вариантам осуществления, относящимся к определению данных инициализации, определение других данных инициализации на основании тех же случайных контекстных данных, что и другой защищенный начальный пакет данных, и сохранение или побуждение к сохранению других подлежащих сохранению данных инициализации. Здесь спрогнозированные контекстные данных представляют спрогнозированное будущее местоположение следующего намеченного получателя физического объекта или группы физических объектов и связанное будущее время присутствия физического объекта или группы физических объектов в этом будущем местоположении. Следовательно, согласно этим вариантам осуществления вместо повторного использования прежде существовавшего защищенного начального пакета данных для, по меньшей мере, следующей последующей проверки аутентичности используется сгенерированный новый защищенный начальный пакет данных. Факультативно, определяются даже новые (то есть, другие) данные инициации, например основанные на новых случайных контекстных данных. Эти разные меры могут дополнительно увеличить, поодиночке или в сочетании, достижимый уровень защиты, так как дополнительно повышается энтропия всего процесса проверки аутентичности.

(Г) Система проверки аутентичности объекта

Четвертый аспект настоящего изобретения относится к системе проверки аутентичности объекта, включающей в себя компьютер и выполненной для осуществления способа третьего аспекта, предпочтительно, согласно одному или более

описанных здесь вариантов его осуществления.

В некоторых вариантах осуществления система проверки аутентификации дополнительно выполнена для осуществления способа первого аспекта.

(Д) Компьютерная программа

Пятый аспект настоящего изобретения относится к компьютерной программе, включающей в себя команды, которые при выполнении на одном или более процессорах системы проверки аутентичности объекта, такой как соответствующей четвертому аспекту, побуждают ее к осуществлению способа проверки аутентичности согласно третьему аспекту настоящего изобретения.

3. Способ и система для защищенного обеспечения зависящей от времени схемы комбинирования

Шестой аспект настоящего изобретения относится к способу защищенного обеспечения зависящей от времени схемы комбинирования для проверки аутентичности физического объекта или группы физических объектов согласно способу проверки аутентичности третьего аспекта, включающему в себя: (i) получение и сохранение данных, представляющих предварительно определенную схему комбинирования, независимой от времени и от местоположения информации, идентифицирующей физический объект или группу физических объектов или связанной с ним или с ней, и метаданных, определяющих ограниченный период пригодности схемы CS комбинирования, (ii) получение запроса о схеме комбинирования и идентифицирующей информации, идентифицирующей физический объект или группу физических объектов или связанной с ним или с ней, от запрашивающей системы, (iii) проверку аутентичности запрашивающей системы, например посредством двухфакторной схемы проверки аутентичности, и (iv-1) если запрашивающая система успешно выдержала проверку аутентичности в качестве авторизованной и согласно прежде сохраненным метаданным, соответствующим полученной идентифицирующей информации, связанная схема комбинирования, к которой относятся метаданные, все еще является действительной, вывод данных, представляющих эту связанную схему комбинирования, через защищенный от перехвата канал данных к запрашивающей системе, и (iv-1) в противном случае отклонение запроса.

Таким образом, одна или более схем комбинирования, используемых в способах и системах других аспектов настоящего изобретения, могут быть надежно переданы к соответствующему узлу (запрашивающей системы) вдоль цепочки поставок, которая нуждается в проверки аутентичности физического объекта или группы физических объектов. Прежде всего, это делает возможным использование одной или более зависящей от времени схемы комбинирования с ограниченным периодом действия для таких проверок аутентичности, которые могут быть использованы для дополнительного повышения достижимого уровня защиты всего решения проверки аутентичности.

Другие аспекты относятся к системе и компьютерной программе, соответственно, для осуществления способа шестого аспекта.

Каждая из описанных здесь компьютерных программ может быть, прежде всего, реализована в виде носителя данных, на котором сохранена одна или более программ для осуществления способа. Предпочтительно, это носитель данных, такой как CD, DVD или модуль флеш-памяти. Это может быть выгодным, если компьютерный программный продукт предназначен для распределения как индивидуальный продукт, независимый от процессорной платформы, на которой должны выполняться одна или более программ. В другом варианте осуществления компьютерный программный продукт обеспечивается в виде файла на блоке обработки данных, прежде всего на

сервере, и может быть загружен через информационное соединение, например Интернет или специализированное информационное соединение, такое как личная или локальная сеть.

Краткое описание чертежей

Другие преимущества, признаки и применения настоящего изобретения приведены в следующем подробном писании и прилагаемых фигурах, причем:

Фиг. 1 схематически показывает служащий примером обзор системы общего решения безопасности, включающего в себя соответствующие предпочтительные варианты осуществления разных аспектов настоящего изобретения,

Фиг. 2А и 2Б показывают блок-схему предпочтительного варианта осуществления первой фазы способа подготовки последующей защищенной проверки аутентичности физического объекта или группы физических объектов их получателем согласно настоящему изобретению,

Фиг. 3А и 3Б показывают блок-схему, иллюстрирующую предпочтительный первый вариант осуществления второй фазы способа подготовки последующей защищенной проверки аутентичности согласно настоящему изобретению,

Фиг. 4А и 4Б показывают блок-схему, иллюстрирующую предпочтительный второй вариант осуществления второй фазы способа подготовки последующей защищенной проверки аутентичности согласно настоящему изобретению,

Фиг. 5А и 5Б показывают блок-схему, иллюстрирующую предпочтительный первый вариант осуществления способа проверки аутентичности физического объекта или группы физических объектов согласно настоящему изобретению, который сконфигурирован для использования в связи со способом согласно фиг. 2 и 3,

Фиг. 6А и 6Б показывают блок-схему, иллюстрирующую предпочтительный второй вариант осуществления способа проверки аутентичности физического объекта или группы физических объектов согласно настоящему изобретению, который сконфигурирован для использования в связи со способом согласно фиг. 2 и 4,

Фиг. 7 показывает блок-схему, иллюстрирующую предпочтительный вариант осуществления способа использования одной или более зависящих от времени схем комбинирования в связи со способами согласно фиг. 3А/3Б-6А/6Б, и

Фиг. 8А и 8Б показывают различные разные опции предоставления возможности дальнейших шагов (скачков) поставки вдоль цепочки поставок с использованием блокчейнов в качестве хранилищ данных в связи с одним или более способов, описанных выше в отношении фиг. 2-7.

На фигурах штриховые линии и контуры используются для иллюстрации дополнительных факультативных вариантов соответствующих систем и способов. Кроме того, одни и те же ссылочные обозначения на разных фигурах относятся к одним и тем же или соответствующим признакам. Следует понимать, что фигуры всего лишь описывают особые варианты осуществления и что один или более описанных здесь признаков или шагов могут быть фактически факультативными, даже если они не обозначены штриховыми линиями или явно описаны как "факультативные".

Подробное описание предпочтительных вариантов осуществления

На фиг. 1 схематически показан служащий примером обзор системы общего решения 10 безопасности, относящегося к цепочке поставок, имеющей узлы A, B и C и факультативно дальнейший узел B'. Например, A может относиться к начальному производителю продукта, поставляющему физический объект PO или группу физических объектов POs или группу физических объектов, называемых в дальнейшем совместно PO(s), которые являются соответственно продуктом или группой продуктов. В принципе

это может быть любой вид продукта(ов), и, прежде всего, эти продукты могут быть лекарственными препаратами или медицинскими приборами. Соответственно, настоящее изобретения является по существу независимым от вида физического объекта, к которому оно применяется. Узел B может быть логистическим объектом, таким как товарный склад, промежуточного оптового торговца, и C может быть местом продажи, например магазином, где PO(s), распространяемые вдоль цепочки поставок, в конечном счете продаются конечному потребителю. Другой узел B' может с коммерческой точки зрения относиться к B и может быть, например факультативным товарным складом, расположенным удаленно от B, так что B может выбирать поставку PO(s) поставщиком A или к товарному складу B, или к товарному складу B'.

В начале процесса поставки поставщик A использует систему 20 подготовки, которая может, прежде всего, включать в себя компьютер и средства для направления запроса к относящемуся к PO(s) PUF и один или более датчиков для обнаружения ответа, сгенерированного в ответ на запрос посредством PUF. Факультативно, или дополнительно, система 20 подготовки может включать в себя систему камеры, сконфигурированную для создания одного или более изображений PO(s) и направления их к системе распознавания объекта, которая сконфигурирована для распознавания PO(s) на основании одного или более изображений и возвращения соответствующего результата распознавания, включающего в себя по меньшей мере одну отличительную характеристику PO(s), к системе 20 подготовки, например, как подробно описано в Европейской патентной заявке EP 18 170 044.4.

Система 20 подготовки сконфигурирована для осуществления способа, показанного на фиг. 2 в сочетании с фиг. 3 или фиг. 4. Как будет подробно описано ниже со ссылкой на эти фигуры, система 20 подготовки генерирует, при осуществлении этих способов, защищенный начальный пакет SSDP данных и сохраняет его или побуждает к его сохранению в первом хранилище DS1 данных. Факультативно, система 20 подготовки также генерирует и зашифровывает и, предпочтительно, также подвергает цифровому подписыванию случайные контекстные данные RCD и сохраняет их или побуждает к их сохранению во втором хранилище DS2 данных. Дополнительно, система 20 подготовки генерирует данные IND инициализации и сохраняет их в третьем хранилище DS3 данных. Эти три хранилища DS1, DS2 и DS3 могут быть отдельными хранилищами данных или двумя из них или даже все три могут быть одним и тем же хранилищем. Прежде всего, каждое из хранилищ данных может быть реализовано, например и без ограничений, в виде блокчейна или безблокового распределенного реестра или в виде хранилища в инфраструктуре PKI с открытым ключом. Прежде всего, разные записи данных, хранящиеся в хранилищах данных, могут быть перекрестно связаны посредством одного или более перекрестных указателей, каждый из которых соединяет два соответствующих блока особой пары блокчейнов.

Каждый из других узлов B, B' и C включает в себя соответствующую систему 30a, 30b и 30 с проверки аутентичности, соответственно. Каждая из этих систем 30a, 30b и 30c проверки аутентичности сконфигурирована для осуществления способа проверки аутентичности согласно фиг. 5 и/или фиг. 6. Как будет подробно описано ниже со ссылкой на эти фигуры, соответствующая система 30a, 30b или 30c, выполняющая проверку аутентичности полученных PO(s), считывает защищенный начальный пакет данных из первого хранилища DS1 и данные IND инициализации из третьего хранилища DS3. Затем на основании этих результатов считывания выполняется проверка аутентичности.

На фиг. 2A показана блок-схема, иллюстрирующая предпочтительный вариант

осуществления первой фазы 100 способа подготовки последующей защищенной проверки аутентичности физического объекта или группы физических объектов их получателем согласно настоящему изобретению. Прежде всего, в случае цепочки поставок этот способ, предпочтительно, осуществляется в начале цепочки поставок ее первым узлом. В настоящем примере согласно фиг. 1 это узел A, соответственно его система 20 подготовки и соответственно нижеприведенное описание основано на этом неограничивающем примере. На фиг. 2Б показана компактная форма этого же способа согласно фиг. 2А, но в более компактной форме блок-схемы потоков данных.

На шаге 110 система 20 подготовки получает от другой уполномоченной организации, такой как центральный логистический центр, или сама генерирует спрогнозированные контекстные данные PCD, связанные со следующим узлом вдоль цепочки поставок, то есть в настоящем примере узлом B. Спрогнозированные контекстные данные PCD представляют местоположение xB узла B, или более конкретно ее системы 30a, и спрогнозированное время tB, в которое ожидается прибытие PO(s) в B. Спрогнозированные контекстные данные PCD могут, прежде всего, происходить из логистических планируемых данных, таких как график поставок, для цепочки поставок. Точность спрогнозированных контекстных данных (например, с точки зрения диапазона географических координат и единиц времени, например часов или дней или недель), предпочтительно, приспособлена для совпадения с точностью, с которой могут быть надежно спрогнозированы будущее местоположение и соответствующий момент времени, в который должна произойти проверка аутентичности PO(s) в следующем узле цепочки поставок, то есть в настоящем примере в узле B. Например, если согласно текущим данным логистического планирования PO(s) должны согласно графику прибыть в узел B в конкретную дату, и узел B относится к промышленным помещениям, имеющим пространственную протяженность примерно 500 м × 500 м, PCD могут быть определены с точностью по времени в сутки (24 часа) и точностью местоположения ±500 м.

На следующем шаге 120 система 20 подготовки получает от другой уполномоченной организации, такой как упомянутый центральный логистический центр или внешний компьютер, или сама генерирует случайные контекстные данные RCD, представляющие случайное местоположение x_r или случайное время t_r.

Затем на шаге 130 PCD и RCD комбинируются согласно первой предварительно определенной схеме CS1 комбинирования для получения посредством этого модифицированных контекстных данных MCD, представляющих модифицированное случайное местоположение xm и модифицированное случайное время tm. Первая предварительно определенная схема комбинирования CS1 может быть независимой от времени схемой, которую требуется установить и сделать доступной для каждого из узлов цепочки поставок, где PO(s) должны быть подвергнуты проверке аутентичности, только один раз. Факультативно, CS1 может быть зависимой от времени, что дополнительно увеличивает энтропию защищенного решения и, таким образом, достижимый уровень защиты. Пример использования зависимой от времени схемы CS1 комбинирования согласно вариантам осуществления настоящего изобретения будут приведены ниже в связи с обсуждением фиг. 7.

Каждые из RCD и PCD могут факультативно представлять дополнительно другую информацию, хотя это для настоящего способа не требуется. На следующем шаге 150 модифицированные контекстные данные шифруются, например с открытым ключом PubB следующего получателя B, для получения защищенного начального пакета SSDP данных, представляющего MCD.

В дополнение, MCD могут быть скреплены цифровой подписью отправляющим

узлом, то есть в настоящем примере узлом A, с цифровой подписью, принадлежащей A. Шаг подписывания может быть выполнен или (i) перед шифрованием согласно шагу 140 (опция 1) или (ii) после шифрования на шаге 160 (опция 2), причем вместо исходных MCD цифровому подписыванию посредством A с его личным ключом PrivA подвергается SSDP, получающийся в результате шифрования MCD. Затем на шаге 170, который завершает первую фазу 100, если не применен факультативный дальнейший шаг 180, SSDP сохраняется или побуждается к сохранению другой уполномоченной организацией, такой как внешний компьютер, в первом хранилище DS1 данных, как описано выше со ссылкой на фиг. 1.

Факультативный шаг 180 относится к особому варианту осуществления, подробно обсужденному ниже со ссылкой на фиг. 8. В этом варианте осуществления случайные контекстные данные сохраняются в третьем хранилище DS3 данных, чтобы предоставить возможность другому узлу в цепочке поставок принять на себя впоследствии роль узла A, например в момент времени, когда A больше не доступен для цепочки поставок, даже если этот другой узел сам не сохранял случайные контекстные данные RCD, полученные во время предшествующего процесса проверки аутентичности, например, согласно фиг. 5А/5Б или фиг. 6А/6Б.

На фиг. 3А показана блок-схема, иллюстрирующая последующую защищенную проверку аутентичности согласно настоящему изобретению. На фиг. 3Б показана соответствующая блок-схема потока данных. Прежде всего, этот первый вариант осуществления относится к случаю, где подлежащие проверке аутентичности вдоль цепочки поставок PO(s) имеют или сами являются количеством n=1, 2, 3,… особых отличительных характеристик, каждая из которых может быть, прежде всего, физической неклонируемой функцией PUF, например согласно одному или более описанных выше типов PUF.

На шаге 210 второй фазы 200 способа система 20 подготовки обнаруживает n отличительных характеристик, в настоящем примере PUFs, подлежащих проверке аутентичности PO(s) вдоль цепочки поставок для получения для каждой отличительной характеристики соответствующих данных 100 идентификации, представляющих идентификатор связанных PO(s).

Затем на факультативном шаге 220 для каждой из отличительных характеристик $k \in \{1,\ldots,n\}$ к полученным IDD_k [IDD - данные идентификации согласно разделу "перечень ссылочных обозначений" - прим. переводчика] соответствующей отличительной характеристики k применяется соответствующая первая криптографическая хеш-функция для получения соответствующего исходного значения Hi_k хеш-функции, связанного с этой особой отличительной характеристикой k. Соответствующие первые криптографические хеш-функции $HF_{1,k}$, связанные с разными отличительными характеристиками или IDDs, соответственно, могут быть или одинаковыми или разными. Также, возможно, что некоторые из них одинаковы, в то время как другие являются разными, до тех пор, пока отношение между особой отличительной характеристикой/IDD и соответствующей первой хеш-функцией $HF_{1,k}$ остается известной и не измененной. В случае если факультативный шаг пропущен, полученные IDD_k берут на себя роль соответствующего исходного значения Hi_k хеш-функции и, таким образом, сами формируют входные данные для описанного ниже последующего шага 240 комбинирования.

На следующем шаге 230 система 20 подготовки считывает с PO(s), например из соответствующей его маркировки, независимую от местоположения и независимую от

времени информацию, особо связанную с PO(s). Например, информация может включать в себя один или более серийных номеров, соотнесенных с PO(s). Факультативно, прежде всего, если такая информация еще не существует, система 20 подготовки может сама генерировать такую независимую от местоположения и независимую от времени информацию и соотнести ее с рассматриваемыми PO(s). В настоящем не ограничивающем примере независимая от местоположения и независимая от времени информация должна быть одним или более серийным номером, соотнесенным с соответствующими PO(s). Здесь серийные номера совместно обозначаются как SN.

На еще одном следующем шаге 240, если n>1, n начальных значений H1,…, Hn (если выполнен шаг 220) или значения IDD1,…, IDDn (если шаг 220 не выполнен) комбинируются со случайными контекстными данными RCD и серийными номерами SN согласно второй схеме CS2 комбинирования, приводя к набору H данных (который может быть, например, только единственным значением H), представляющему результат этой операции комбинирования.

Предпочтительно, схема CS2 комбинирования является сохраняющей информацию и/или идеально сохраняющей энтропию. Например, набор данных, получающийся из комбинирования согласно схеме CS2 комбинирования может принимать форму всего лишь комбинирования соответствующих входных данных, то есть подлежащих комбинированию значений. Комбинирование может быть, прежде всего, представлено посредством одномерной или многомерной матрицы или другого типа массива. Подобно первой схеме CS1 комбинирования, также и вторая схема CS2 комбинирования может быть независимой от времени схемой, которую необходимо создавать и делать доступной для каждого из узлов цепочки поставок, где PO(s) должны подвергаться проверке аутентичности только один раз. Факультативно, снова подобно CS1, она может быть также зависящей от времени, причем каждый из узлов цепочки поставок должен быть информирован о соответствующей применимой второй схеме CS2 комбинирования, чтобы сделать возможной соответствующую проверку аутентичности PO(s) в этом узле. Пример использования зависящей от времени схемы CS1 и/или CS2 комбинирования согласно вариантам осуществления настоящего изобретения будет представлен ниже в связи с обсуждением фиг. 7.

Затем на шаге 250 другое значение Ho хеш-функции, которое будет здесь называться "исходным значением Ho хеш-функции" генерируется посредством применения второй криптографической хеш-функции к набора данных H.

На следующем шаге 260 система 20 подготовки выполняет цифровое подписывание исходного значения Ho хеш-функции с личным ключом PrivA узла A, чтобы сделать возможной последующую проверку подлинности происхождения Ho в последующей проверке аутентичности узла в цепочке поставок, то есть в настоящем примере в узлах B, B' и C.

На еще одном следующем шаге 270, который может, прежде всего, выполняться вместе с шагом 260 в виде одного комбинированного шага, система 20 подготовки генерирует данные IND инициализации, представляющие исходное значение Ho хеш-функции, полученное шаге 250 вместе с его цифровой подписью, полученной на шаге 260.

Фаза 200 способа завершается дальнейшим шагом 280, в котором представление данных IND инициализации, например соответствующая маркировка, добавляется к PO(s) и/или представление IND сохраняется или побуждается к сохранению в третьем хранилище DS3 вместе с добавлением к PO(s) представления указателя, указывающего, где IND могут быть доступны в DS3. Местоположение хранилища для IND в DS3 и,

следовательно, также указатель, может быть, например, определено на основании одного или более серийных номеров SN объекта PO(s).

На фиг. 4А показана блок-схема, иллюстрирующая предпочтительный второй вариант осуществления 300 второй фазы способа подготовки последующей защищенной проверки аутентичности согласно настоящему изобретению. На фиг. 4Б показана соответствующая блок-схема потока данных. Прежде всего, этот второй вариант осуществления относится к случаю, когда подлежащие проверке аутентичности PO(s) вдоль цепочки поставок могут иметь или нести на себе особую отличительную характеристику, такую как, например, физическую неклонируемую функцию PUF.

На шаге 310, который эквивалентен шагу 230 на фиг. 2А/2Б, система 20 подготовки считывает с PO(s) или сама генерирует независимую от местоположения и независимую от времени информацию, особо связанную с PO(s), например один или более серийных номеров SN, соотнесенных с PO(s).

На еще одном следующем шаге 320 система 20 подготовки определяет набор H данных комбинации согласно предварительно определенной схеме CS3 комбинирования, случайных контекстных данных RCD и независящей от времени и местоположения информации, идентифицирующей PO(s) или особо связанной с ним/ними. Например, эта информация может быть одним или более серийных номеров SN объекта PO(s). Аналогично CS2, схема CS3 комбинирования может быть независимой от времени схемой или зависимой от времени схемой (см. фиг. 7).

На еще одном следующем шаге 330 система 20 подготовки генерирует исходное значение Ho хеш-функции посредством применения криптографической хеш-функции к полученного набору H данных.

В еще одном дальнейшем (факультативном) шаге 340 система 20 подготовки выполняет цифровое подписывание исходного значения Ho хеш-функции с личным ключом узла A, чтобы сделать возможной последующую проверку подлинности происхождения Ho в последующей проверке аутентичности узла в цепочке поставок, то есть в настоящем примере в узлах B, B' и C.

На еще одном следующем шаге 350, который может, прежде всего, выполняться вместе с шагом 340 в виде одного комбинированного шага, система 20 подготовки генерирует данные IND инициализации, представляющие исходное значение Ho хеш-функции, полученное на шаге 320 вместе с его цифровой подписью, полученной шаге 330, если он выполнялся.

Фаза 300 способа завершается дальнейшим шагом 360, в котором представление данных IND инициализации, например соответствующая маркировка, добавляется к PO(s) и/или представление IND сохраняется или побуждается к сохранению в третьем хранилище DS3 данных вместе с добавлением к PO(s) представления указателя, указывающего, где может быть обеспечен доступ к IND в DS3. Место хранения IND в DS3 и, следовательно, также указатель, может быть, например, определено на основании одного или более серийных номеров SN PO(s).

На фиг. 5А показана блок-схема, иллюстрирующая предпочтительный первый вариант 400 осуществления способа проверки аутентичности физического объекта или группы физических объектов согласно настоящему изобретению, который сконфигурирован для использования в связи со способом согласно фиг. 2 и 3. Фиг. 5Б показывает соответствующую блок-схему потоков данных.

Способ 400 предназначен для использования, прежде всего, такими узлами B, B' и C вдоль цепочки поставок, которые не являются начальной точкой A распределения PO(s) и которые, следовательно, имеют желание должным образом проверить

аутентичность PO(s), полученного из соответствующего непосредственно предшествующего узла в цепочке поставок. Теперь способ будет разъяснен для примера в связи с PO(s), которые имеют два или более разных PUFs в качестве отличительных характеристик. Конечно, вместо этого могут быть использованы подобные способы, основанные на других, не являющихся PUF отличительных характеристиках или смеси отличительных характеристик с PUF и не PUF согласно дальнейшим вариантам не показанных здесь вариантов осуществления.

Способ 400 включает в себя шаг 410, в котором соответствующие системы 40a, 30b или 30 с проверки аутентичности, которые осуществляет способ, применяются к каждому из PUFs объекта PO(s), подлежащего проверке аутентичности, соответствующий запрос соответствующей предварительно определенной схемы AS проверки аутентичности "запрос-ответ" для инициирования в ответ на запрос ответа согласно AS. Для упрощения нижеследующее описание согласно фиг. 5А, Б и 6 А, Б будет фокусироваться на системе 30a проверки аутентичности в узле B, хотя следует понимать, что этот же самый способ 400 может быть также использован всеми другими узлами вдоль цепочки поставок.

На шаге 415 каждый из ответов разных PUFs обнаруживается в соответствии с соответствующей схемой проверки аутентичности "запрос-ответ", и из них получаются соответствующие данные 100 идентификации, которые представляют ответ.

На дальнейшем (факультативном) шаге 420 для каждого из PUFs к соответствующая первая предварительно определенная криптографическая хеш-функция $HF_{1,k}$, равная соответствующей первой криптографической хеш-функции, которая была ранее использована в способе согласно фиг. 3 во время фазы 200 подготовки для этого же PUF, применяется к соответствующим IDD для получения соответствующего исходного значения Hi*k значения хеш-функции, связанного с IDD_k PUF_k, соответственно. Шаги 410-420 служат для обеспечения набора начальных значений $HF_{1,k}$ в качестве первого ввода информации в последующий шаг 450 комбинирования, который будет подробно описан ниже. Если шаг 420 не используется, соответствующим первым вводом информации в шаг 450 комбинирования вместо этого будут соответствующие значения IDD_k, полученные на шаге 415.

Дальнейшие шаги 425-440 предназначены для обеспечения второго ввода информации в шаг 450 комбинирования. На шаге 425 рассматриваемая система 30a, например, считывает из первого хранилища DS1 данных защищенный начальный пакет SSDP данных, представляющий зашифрованные контекстные данные CD, которые в свою очередь представляют местоположение x0 и связанное время t0. SSDP дешифруется для восстановления контекстных данных CD.

В дополнение, на шаге 430 текущие контекстные данные CCD, представляющие текущее местоположение x и связанное текущее время t присутствия PO(s) в его текущем местоположении x, генерируются посредством системы 30a или получаются от другой уполномоченной организации, такой как логистическая база данных. Предпочтительно, текущие контекстные данные CCD имеют такую же точность, как и спрогнозированные контекстные данные.

На следующем шаге 435 система 30a определяет подходящую схему CS3 комбинирования, которая определяет операцию, обратную соответствующей операции согласно соответствующей схеме CS1 комбинирования, использованной ранее для генерирования полученных контекстных данных CD. Это определение может быть, например, выполнено как описано ниже со ссылкой на фиг. 7.

Затем на шаге 440 текущие контекстные данные CCD комбинируются согласно

определенной схеме CS3 комбинирования с дешифрованными контекстными данными CD для определения посредством этого тестовых контекстных данных TCD. Эта операция комбинирования шага 440 фактически является обратной операцией операции, выполненной посредством шага 140 согласно фиг. 2. Если PCD и CCD имеют одинаковую точность, и эта точность совпадает с зависящей от контекста надежностью логистики цепочки поставок, проверка аутентичности становится более надежной в отношении допустимых различий между местоположениями и/или, прежде всего, моментами времени, указанными соответственно посредством PCD и CCD. Соответственно, если текущие контекстные данные CCD, по меньшей мере, с заданной точностью совпадают с соответствующими PCD, и SSDP не были повреждены, ожидается, что полученные TCD совпадают с исходными случайными контекстными данными RCD.

Третий шаг 445 предусмотрен для обеспечения третьего ввода информации в последующий шаг 450 комбинирования. На шаге 445 система 30a считывает из хранилища DS3 данных связанные с PO(s) данные IND инициализации, которые ранее были сохранены в DS3 согласно шагу 340 способа фазы 300. Если сохраненные данные IND инициализации были подвергнуты цифровому подписыванию перед их сохранением, считывание данных IND инициирования включает в себя проверку подлинности соответствующей цифровой подписи, посредством которой IND были подвергнуты цифровому подписыванию, и восстановление исходного значения Ho хеш-функции, представленного данными IND инициализации. Затем Ho доступно в качестве третьего ввода информации в последующий шаг комбинирования 450.

На шаге 450 комбинирования система 30a генерирует тестовое значение Ht хеш-функции посредством применения второй предварительно определенной криптографической хеш-функции к предварительно определенной комбинации Hc исходного значения Hi_k хеш-функции, TCD и одного или более серийных номеров, обеспеченных на PO(s). Вторая предварительно определенная криптографическая хеш-функция равна соответствующей криптографической хеш-функции HF2, использованной для определения Ho, представленного посредством IND на шаге 230 способа фазы 200.

Наконец, способ 400 завершается шагом 455, в котором система 30a генерирует и выводит первый результат RR1 считывания, указывающий, совпадает или нет согласно по меньшей мере одному предварительно определенному критерию совпадения Ht с Ho и, следовательно, указывающий на аутентичность PO(s).

На фиг. 6A показана блок-схема, иллюстрирующая предпочтительный второй вариант 500 осуществления способа проверки аутентичности физического объекта или группы физических объектов согласно настоящему изобретению, который сконфигурирован для использования в связи со способом согласно фиг. 2 и 4. На фиг. 6Б показана соответствующая блок-схема потока данных.

Второй вариант осуществления 500 отличается от описанного выше в связи с фиг. 5 первого варианта осуществления 400 тем, что отсутствуют или не используются отличительные характеристики PO(s).

Соответственно, в способе 500, с одной стороны, нет шагов, соответствующих шагам 410-420 способа 400, в то время как, с другой стороны, имеются шаги 510-530, которые соответствуют и могут быть, прежде всего, идентичными шагам 425-445. Дальнейший шаг 535 способа 500 отличается от соответствующего шага 450 способа 400 тем, что теперь тестовое значение Ht хеш-функции генерируется посредством применения соответствующей криптографической хеш-функции HF2 к предварительно определенной комбинации Hc тестовых контекстных данных TCD и одного или более серийных номеров SN, обеспеченных на PO(s). Финальный шаг 540 вывода способа 500 снова

идентичен шагу 455 способа 400.

В то время как вариант осуществления способа 400 (и способа 200) может быть использован для достижения более высоких уровней защищенности, чем те, которые имеются при использовании способа 500 (и способа 300), последний имеет преимущество меньшей сложности и, следовательно, может быть предпочтительным, когда с точки зрения умеренного желательного уровня защищенности является приоритетом поддержание низкой сложности и, следовательно, стоимости и затрат на осуществления системы.

На фиг. 7 показана блок-схема, иллюстрирующая предпочтительный вариант осуществления способа 600 использования одной или более зависящих от времени схем комбинирования в связи со способами согласно фиг. 3А/3Б-6А/6Б. Когда получатель, такой как узел В, нуждается в проверке аутентичности полученных PO(s), он сначала должен восстановить применимые зависящие от времени схемы CS, такие как, например, CS2 и/или CS3.

Решение этой проблемы согласно вариантам осуществления в соответствии с фиг. 7 основано на доверенном органе TC, таком как, например, центр управления безопасностью, как известно из инфраструктур (PKI) открытых ключей. В другом примере исходный поставщик А может сам представлять собой или обеспечивать центр (TC) безопасности.

Во время процесса подготовки последующей проверки аутентичности, например в процессе согласно способам 100/200 или 100/300, описанным выше со ссылкой на фиг. 2 и фиг. 3А/3Б или фиг. 2 и фиг. 4А/4Б, на шаге 605 узел А сохраняет или побуждает к сохранению в хранилище DS данных, например DS1, центра TC безопасности одного или более серийных номеров SN, принадлежащих определенным PO(s), подлежащим распространению и проверке аутентичности вдоль данный цепочки поставок, подходящую схему CS комбинирования, такую как обратимую математическую формулу или другую подходящую обратимую схему обработки данных, и метаданные MD(CS (SN)), связанные со схемой CS комбинирования, применимую для PO(s) с серийным номером(ами) SN. Метаданные MD(CS(SN)) могут, прежде всего, включать в себя информацию, определяющую ограниченный период действия схемы CS комбинирования, так что она является больше не применимой, когда истек период действия.

Когда В получает PO(s) и нуждается в проверке их аутентичности, он направляет на шаге 610 соответствующий запрос к центру (TC) безопасности вместе с серийным номером(ами) SN и предварительно определенной идентификационной информацией, которая делает возможной двухфакторную проверку 2FA аутентичности, то есть добавочную проверку идентичности В центром безопасности, которая является независимой от личного ключа PrivB В (который, например, использовался для шифрования SSDP во время процесса проверки аутентичности для PO(s)). Идентификационная информация может, например, включать в себя PIN и TAN, аналогично известным процедурам при онлайн-банкинге, фотографию TAN, пароль или может быть основана на другой независимой паре открытого/личного ключей.

Затем центр TC безопасности в 2FA-шаге 615 проверяет подлинность полученной от В идентификационной информации для проверки аутентичности В и также получает на шаге 620 метаданные MD(CS(SN)) из хранилища DS данных. На шаге 625 метаданные MD(CS(SN)) проверяются для определения, является ли запрошенная схема CS комбинирования все еще действующей, и оценивается результат шага 615 проверки аутентичности. Если эта проверка аутентичности В и/или проверка (625 - НЕТ) оказалась неудачной, сообщение об ошибке возвращается к В на шаге 630. Иначе (625 - ДА)

полученный серийный номер(а) SN используется на шаге 625 в качестве индекса к запросу базы данных в хранилище DS данных для получения на шаге 640 желаемой схемы CS(SN) комбинирования и шифрования на следующем шаге 645, например с открытым ключом B. Когда B получает зашифрованную схему CS(SN) комбинирования, она дешифруется на шаге 650, например с личным ключом, для получения желаемой схемы CS(SN) комбинирования. В то время как использование асимметричного шифрования является подходящим подходом к осуществлению шифрования/дешифрования в шагах 645 и 650, вместо этого могут быть использованы другие подходы для достаточной защиты связи между TC и B от перехвата. На фиг. 7 защищенная связь между B и TC показана в виде соответствующего защищенного "туннеля" T, который может быть отдельным для каждой из связей или объединенным туннелем для двух или более каналов связи. Например, может быть использовано симметричное шифрование. Также, если для этой цели используется асимметричное шифрование, может быть использована иная пара ключей, чем в других описанных выше шагах способов.

Таким образом, для B с целью удачной проверки аутентичности полученных PO(s) должны выполняться три условия (фактора): (1) B должен обрабатывать свой личный ключ PrivB, (2) проверка аутентичности должна иметь место в правильном местоположении (узел B) и во временных рамках, определенных посредством A в спрогнозированных контекстных данных PCD во время фазы 200 подготовки, и (3) B нуждается в достоверной идентификационной информации, требуемой для получения доступа к соответствующим одной или более зависящим от времени схемам CS комбинирования, например CS2 и/или CS3. Соответственно, проверка аутентичности PO(s) будет неудачной, если исходно было запланировано прибытие PO(s) в узел B в определенный момент времени, как определено в связанных спрогнозированных контекстных данных PCD, но PO(s) вместо этого были фактически доставлены в другое местоположение B' товарного склада (узел B'), то есть в другое время и другое местоположение (ср. фиг. 1). Следовательно, если B желает перенаправить распределение PO(s) от узла A к узлу B' (вместо узла B), B должен информировать A об этом желании и затем A должен подготовить и сохранить обновленный начальный пакет SSDP данных, отображающих перенаправление к узлу B'.

На фиг. 8A и 8Б показаны различные другие опции предоставления возможности дальнейших шагов поставки (скачков) вдоль цепочки поставки с использованием блокчейна в качестве хранилища данных в связи с одним или более способами, описанными выше в отношении фиг 2-7. Прежде всего, фиг. 8A относится к вариантам осуществления, где узел A определен как единственный полномочный орган вдоль цепочки поставок для определения соответствующего начального пакета данных для каждого скачка. В дополнение, A может быть единственным полномочным органом для определения также дальнейших данных 100 инициализации, замещающих исходные данные инициализации, связанные с конкретным PO(s). В то время как для каждого скачка вдоль цепочки поставок требуется новый защищенный начальный пакет данных, который основывается на соответствующих спрогнозированных контекстных данных PCD для получателя в соответствующем следующем скачке, данные инициализации могут или сохраняться неизмененными или также изменяться.

Например, когда в варианте осуществления согласно фиг. 5A поставляемые вдоль цепочки поставки от A до C PO(s) достигли узла B и был там успешно подвергнуты проверке аутентичности, B посылает запрос R единственному уполномоченному органу, который является узлом A, на выдачу необходимого нового SSDP(C) для скачка от B

до C. Типичным образом, B направит спрогнозированные контекстные данные для C узлу A, чтобы сделать возможным определение правильного SSDP(C), или через одно из хранилищ данных DS1-DS3, или через отдельный, предпочтительно защищенный, канал связи. Факультативно, B может также запросить, например, в качестве части запроса R, новые данные IND(C) инициализации, основанные на новых случайных контекстных данных RCD. Поскольку RCD необходимы для определения как запрошенного SSDP(C), так и IND(C), эти два элемента данных взаимосвязаны, так как они основываются на одних и тех же RCD. На каждый запрос A определяет SSDP(C) и, факультативно, также IND(C) и сохраняет результат соответственно в связанном хранилище данных DS1 и DS3. Когда PO(s), отправленные узлом B, достигают узла C, система 30 с узла C может считывать SSDP(C) и, если применимо, IND(C) и на их основании успешно выполнять проверку аутентичности PO(s) при условии, что текущие контекстные данные (CCD) узла C совпадают с PCD, на основании которых SSDP(C) был определен посредством A.

Фиг. 8Б, наоборот, относится к вариантам осуществления, где предшествующий получатель PO(s) может сам взять на себя роль определения необходимого SSDP и, факультативно, также связанных других IND для следующего начинающегося в этом узле скачка. Например, узел B может взять на себя предшествующую роль, которую A выполнял в связи со скачком от A до B, для дальнейшего скачка от B до C. В любом случае B должен определить нового SSDP(C) для C, основанного на связанных спрогнозированных контекстных данных для C.Использованные для этого определения случайные контекстные данные RCD могут оставаться такими же, как и для предшествующего скачка. Соответственно, в первом варианте B может использовать RCD, определенные как результат предшествующей проверки аутентичности PO(s) в узле B после прибытия из узла A. Однако во втором варианте B требуется сгенерировать или получить новые случайные контекстные данные и, следовательно, также определить основанные на них SSDP(C) и новые данные IND(C) инициализации и сохранить их соответственно в DS1 и DS2. Затем процесс проверки аутентичности для PO(s) в узле C подобен процессу в случае фиг. 5A.

Другим связанным вариантом осуществления согласно фиг. 8Б является случай, где новый SSDP(C) и факультативно новые данные IND(C) инициализации должны определяться на основании исходных случайных контекстных данных RCD, исходно определенных узлом A, но где такие RCD уже больше не имеются в A и B или может быть даже A или их данные вообще больше не существуют. Это может произойти, например, в случаях, где общее время перемещения PO(s) вдоль цепочки поставок является довольно долгим (например годы), как это может иметь место для товаров, типичным образом имеющих длительное время хранения между последовательными скачками, например в случае (необработанных) алмазов. Тогда решением может быть, как показано на фиг. 1 и 8Б, что A сохраняет свои RCD в хранилище данных, например DS2, защищенным образом, например зашифрованными, так что B или любой авторизованный другой узел B может получить к ним доступ, даже если исходные RCD иным образом для B не доступны. Затем, B может получить доступ к RCD и DS2 и, основываясь на них, продолжить поток данных, соответствующих цепочке поставок, основанной на способе согласно фиг. 8Б и исходных RCD.

В то время как выше был описан по меньшей мере один служащий примером вариант осуществления настоящего изобретения, следует отметить, что существует большое число его вариаций. Кроме того, следует понимать, что описанные служащие примером варианты осуществления только иллюстрируют неограничивающие примеры того, как

может быть выполнено настоящее изобретение, и что они не предназначены для ограничения объема патента, применения или конфигурации описанных здесь устройств и способов. Наоборот, предшествующее описание будет обеспечивать специалиста в определенной области техники инструкциями для реализации по меньшей мере одного служащего примером варианта осуществления изобретения, причем следует понимать, что возможны различные изменения функциональности и расположения элементов служащего примером варианта осуществления без отклонения от определенных посредством прилагаемых пунктов изобретения предметов и их законных эквивалентов.

Перечень ссылочных обозначений:

10 - общее решение безопасности
20 - система подготовка узла A
30 a, b, c - система проверки аутентичности соответственно узлов B, B' и C
2FA - двухфакторная проверка аутентичности
A, B, C - узлы цепочки поставок
CCD - текущие контекстные данные
CP - кросс-указатель, например кросс-блокчейн
CO - зашифрованные контекстные данные
CS - схема комбинирования, например одна из CS1, CS2 и CS3
CS1 - первая схема комбинирования
CS2 - вторая схема комбинирования
CS3 - третья схема комбинирования, обратная CS1
Dec - дешифрование
DS - хранилище данных, прежде всего одно из DS1, DS2 и DS3
DS1,…,DS3 - хранилища данных, например блокчейны
Enc - шифрование
H - набор данных, например единственное значение
HF1, HF2 - хеш-функции
Hc - предварительно определенная комбинация начальных значений хеш-функции
Hi - начальное значение хеш-функции
Ho - исходное значение хеш-функции
Ht - тестовое значение хеш-функции
100 - данные идентификации
IND - данные инициализации
k - отличительная характеристика или соответствующий индекс к ней, соответственно
MCD - модифицированные контекстные данные
PCD - спрогнозированные контекстные данные
PIN - личный идентификационный номер
PO(s) - физические объекты или группы физических объектов
PrivA - личный ключ A
PrivB - личный ключ B
PubA - открытый ключ A
PubB - открытый ключ B
PUF1-PUFn - физические неклонируемые функции (PUF)
R - запрос
RCD - случайные контекстные данные
RR1 - первый результат считывания
Sign - создание цифровой подписи
SN - серийный номер(а)

SSDP - защищенный начальный пакет данных

T - защищенный канал, туннель

TAN - номер сделки

TC - система защищенного выполнения зависящей от времени схемы комбинирования, центр безопасности

TCD - тестовые контекстные данные

(57) Формула изобретения

1. Способ (100, 200, 300) подготовки последующей защищенной проверки аутентичности физического объекта или группы физических объектов (PO(s)) его получателем (B, B'), причем способ включает в себя:

получение или генерирование (110) спрогнозированных контекстных данных (PCD), представляющих спрогнозированное будущее местоположение, связанное с намеченным следующим получателем (B, B') физического объекта или группы физических объектов (PO(s)), и связанное будущее время присутствия физического объекта или группы физических объектов (PO(s)) в этом будущем местоположении,

получение или генерирование (120) случайных контекстных данных (RCD), указывающих на случайное местоположение и случайное время,

комбинирование (130) согласно первой предварительно определенной схеме комбинирования спрогнозированных контекстных данных (PCD) и случайных контекстных данных (RCD) для получения посредством этого модифицированных контекстных данных (MCD), представляющих модифицированное случайное местоположение и модифицированное случайное время, каждое из которых получается в результате комбинирования,

шифрование (150) модифицированных контекстных данных (MCD) для получения защищенного начального пакета (SSDP) данных, представляющего модифицированные контекстные данные (MCD), и

сохранение (170) защищенного начального пакета (SSDP) данных или побуждение к его сохранению в первом хранилище (DS1) данных, доступном для обеспечения защищенного начального пакета (SSDP) данных для последующей защищенной проверки аутентичности физического объекта или группы физических объектов (PO (s)).

2. Способ (100, 200, 300) по п. 1, причем сохранение (170) защищенного начального пакета (SSDP) данных в первом хранилище данных (DS1) включает в себя сохранение защищенного начального пакета (SSDP) данных в блокчейне или безблоковом распределенном реестре (DS1).

3. Способ (100, 200, 300) по одному из предшествующих пунктов, также включающий в себя:

A) обнаружение (210) посредством одного или более датчиков по меньшей мере одной отличительной характеристики (k) физического объекта или группы физических объектов (PO(s)) для получения для каждой отличительной характеристики (k) соответствующих данных (IDD_k) идентификации, представляющих идентификатор связанного физического объекта или группы физических объектов (PO(s)),

применение (250) второй предварительно определенной криптографической хеш-функции (HF2) к набору данных, полученных из комбинирования согласно второй предварительно определенной схеме (CS2) комбинирования, одних или более соответствующих данных (IDD_k) идентификации, полученных из набора по меньшей мере из одной отличительной характеристики (k) и случайных контекстных данных

(RCD), для получения исходного значения (Ho) хеш-функции, обнаружение (210) посредством одного или более датчиков по меньшей мере одной отличительной характеристики (k) физического объекта или группы физических объектов (PO(s)) для получения для каждой отличительной характеристики (k) соответствующих данных (IDD_k) идентификации, представляющих идентификатор связанного физического объекта или группы физических объектов (PO(s)), или

Б) применение (220) к каждым из данных (IDD_k) идентификации соответствующей первой предварительно определенной криптографической хеш-функции ($HF_{1,k}$) для получения соответствующего исходного значения (Hi_k) хеш-функции, связанного с соответствующей отличительной характеристикой (k), и

применение (250) второй предварительно определенной криптографической хеш-функции (HF2) к набору (H) данных, полученных из комбинирования согласно второй предварительно определенной схеме (CS2) комбинирования, одного или более соответствующих исходных значений (Hi_k) хеш-функции, полученных из набора по меньшей мере из одной отличительной характеристики и случайных контекстных данных (RCD), для получения исходного значения (Ho) хеш-функции, или

В) применение (330) второй предварительно определенной криптографической хеш-функции (HF2) к случайным контекстным данным (RCD) для получения исходного значения (Ho) хеш-функции, и

вывод (270, 280; 350, 360) данных (IND) инициализации, представляющих соответствующее исходное значение (Ho) хеш-функции.

4. Способ (100, 200) по п. 3, причем:

по меньшей мере одна из отличительных характеристик (k) включает в себя физическую неклонируемую функцию PUF (PUF_k), и

обнаружение (210) по меньшей мере одной отличительной характеристики (k) для получения связанных с ней соответствующих данных (IDD_k) идентификации включает в себя:

применение соответствующего запроса соответствующей предварительно определенной схемы проверки аутентичности к PUF для инициирования в ответ на запрос ответа PUF согласно схеме проверки аутентичности, и

обнаружение соответствующего ответа и генерирование соответствующих данных (IDD_k) идентификации, представляющих этот ответ,

применение (220) соответствующей первой предварительно определенной криптографической хеш-функции ($HF_{1,k}$) включает в себя применение соответствующей первой предварительно определенной криптографической хеш-функции ($HF_{1,k}$) к данным, представляющим ответ, для получения соответствующего связанного с PUF исходного значения хеш-функции (Hi_k), и

вывод (270, 280) данных (IND) инициализации включает в себя вывод соответствующих данных (IDD_k) идентификации, связанных с отличительной характеристикой (k), причем данные (IDD_k) идентификации включают в себя представление соответствующего связанного с PUF исходного значения (Hi_k) хеш-функции.

5. Способ (100, 200, 300) по п. 3 или 4, причем применение (250, 330) второй предварительно определенной криптографической хеш-функции (HF2) для получения исходного значения (Ho) хеш-функции также включает в себя применение этого значения в дополнение к независимой от времени и от местоположения информации (SN),

идентифицирующей физический объект или группу физических объектов (PO(s)) или связанной с ним или с ней, соответственно.

6. Способ (100, 200, 300) по одному из пп. 3-5, причем вывод (270, 280; 350, 360) данных (IND) инициализации включает в себя одно или более из следующего:

добавление представления данных (IND) инициализации к физическому объекту или группе физических объектов (PO(s)),

сохранение представления данных (IND) инициализации или побуждение к его сохранению в третьем хранилище данных (DS3) и добавление к физическому объекту или группе физических объектов (PO(s)) представления указателя, указывающего, где может быть получен доступ к данным (IND) инициализации в третьем хранилище (DS3) данных.

7. Способ (100, 200, 300) по одному из пп. 3-6, также включающий в себя:

получение запроса для определения другого защищенного начального пакета (SSDP) данных, связанного с другими спрогнозированными контекстными данными (PCD), представляющими другое спрогнозированное будущее местоположение, связанное с другим дальнейшим намеченным следующим получателем (C) физического объекта или группы физических объектов (PO(s)), и связанное будущее время присутствия физического объекта или группы физических объектов (PO(s)) в этом другом будущем местоположении, и

осуществление способа по п. 1 или 2 на основании этих других спрогнозированных контекстных данных (PCD) и случайных контекстных данных для определения и сохранения запрошенного другого защищенного начального пакета (SSDP) данных, связанного с другими спрогнозированными контекстными данными (PCD).

8. Способ (100, 200, 300) по одному из пп. 3-7, также включающий в себя:

подписывание (260, 340) полученного исходного значения (Ho) хеш-функции цифровой подписью, принадлежащей поставщику (A) физического объекта или группы физических объектов (PO(s)), соответствующему следующему получателю (B, B'), и

включение цифровой подписи в вывод соответствующих данных (IND) инициализации или других данных (IND) инициализации, соответственно.

9. Система (20) для подготовки последующей защищенной проверки аутентичности физического объекта или группы физических объектов (PO(s)), включающая в себя компьютер, средства для направления запроса к физической неклонируемой функции (PUF), относящейся к физическому объекту или группе физических объектов (PO(s)), и один или более датчиков для обнаружения ответа, сгенерированного в ответ на запрос посредством физической неклонируемой функции (PUF), причем система выполнена для осуществления способа по одному из предшествующих пунктов.

10. Способ (400, 500) проверки аутентичности физического объекта или группы физических объектов (PO(S)), причем способ включает в себя:

получение (425, 510) и дешифрование защищенного начального пакета (SSDP) данных, представляющего зашифрованные контекстные данные (CD), представляющие местоположение и связанное время, для восстановления контекстных данных (CD),

получение или определение (430, 515) текущих контекстных данных (CCD), представляющих текущее местоположение физического объекта или группы физических объектов (PO(s)) и связанное текущее время присутствия физического объекта или группы физических объектов (PO(s)) в этом текущем местоположении,

комбинирование (440, 525) согласно предварительно определенной (435, 520) схеме (CS3) комбинирования текущих контекстных данных (CCD) с дешифрованными контекстными данными (CD) для определения посредством этого тестовых контекстных

данных (TCD), причем схема (CS3) комбинирования определяет операцию, обратную соответствующей операции (CS1) комбинирования, использованной прежде для генерирования полученных контекстных данных (CD),

получение доступа (445, 530) к данным (IND) инициализации, связанным с физическим объектом или группой физических объектов, для восстановления из них исходного значения (Ho) хеш-функции, представленного посредством данных (IND) инициализации,

причем способ также включает в себя один из следующих процессов A)-C):

A) обнаружение (410, 415) посредством одного или более датчиков по меньшей мере одной отличительной характеристики (k) физического объекта или группы физических объектов (PO(s)) для получения соответствующих данных (IDD_k) идентификации, связанных с соответствующей отличительной характеристикой (k), причем эти данные (IDD_k) идентификации представляют предполагаемый идентификатор связанного физического объекта или группы физических объектов (PO(s)), и

генерирование (450) тестового значения (Ht) хеш-функции посредством применения второй предварительно определенной криптографической хеш-функции (HF2) к комбинации (Hc), согласно другой предварительно определенной схеме (CS2) комбинирования, из тестовых контекстных данных (TCD) и каждых из данных (IDD_k) идентификации и, предпочтительно, независимой от времени и от местоположения информации (SN), идентифицирующей физический объект или группу физических объектов (PO(s)) или связанной с ним или с ней, или

Б) обнаружение (410, 415) посредством одного или более датчиков по меньшей мере одной отличительной характеристики (k) физического объекта или группы физических объектов (PO(s)) для получения соответствующих данных (IDD_k) идентификации, связанных с соответствующей отличительной характеристикой (k), причем эти данные (IDD_k) идентификации представляют предполагаемый идентификатор связанного физического объекта или группы физических объектов (PO(s)),

применение (420) соответствующей первой предварительно определенной криптографической хеш-функции ($HF_{1,k}$) к соответствующим данным (IDD_k) идентификации для получения соответствующего исходного значения (Hi_k) хеш-функции, связанного с отличительной характеристикой (k), и

генерирование (450) тестового значения (Ht) хеш-функции посредством применения второй предварительно определенной криптографической хеш-функции (HF2) к комбинации (Hc), согласно другой предварительно определенной схеме (CS2) комбинирования, из тестовых контекстных данных (TCD) и каждого из исходных значений (Hi_k) хеш-функции и, предпочтительно, независимой от времени и от местоположения информации, идентифицирующей физический объект или группу физических объектов или связанной с ним или с ней,

B) генерирование (535) тестового значения (Ht) хеш-функции посредством применения второй предварительно определенной криптографической хеш-функции (HF2) к тестовым контекстным данным (TCD) или к комбинации (Hc), согласно другой предварительно определенной схеме (CS2) комбинирования, из тестовых контекстных данных (TCD) и независимой от времени и независимой от местоположения информации, идентифицирующей физический объект или группу физических объектов или связанной с ним или с ней,

причем для каждого из вышеупомянутых процессов A)-B) эта вторая предварительно определенная криптографическая хеш-функция (HF2) равна соответствующей

криптографической хеш-функции, использованной прежде для определения исходного значения (Ho) хеш-функции, представленного данными (IND) инициализации, и причем другая схема (CS2) комбинирования равна соответствующей схеме комбинирования, использованной прежде для определения исходного значения (Ho) хеш-функции, представленного данными (IND) инициализации, и

способ также включает в себя:

генерирование (455, 540) первого результата (RR1) считывания, включающего в себя:

- представление тестового значения (Ht) хеш-функции и представление исходного значения (Ho) хеш-функции, или

- сравнение выходных данных, указывающих, совпадают или нет, согласно по меньшей мере одному предварительно определенному критерию совпадения, тестовое значение хеш-функции и исходное значение хеш-функции и, таким образом, указывающих на аутентичность физического объекта или группы физических объектов.

11. Способ по п. 10, причем по меньшей мере одна из отличительных характеристик (k) включает в себя физическую неклонируемую функцию (PUF), и

обнаружение отличительной характеристики для получения связанных с ней соответствующих данных идентификации включает в себя:

применение (410) соответствующего запроса соответствующей предварительно определенной схемы проверки аутентичности "запрос-ответ" к PUF для инициирования в ответ на запрос ответа согласно схеме проверки аутентичности, и

обнаружение (415) в ответ на запрос соответствующего ответа PUF в соответствии с соответствующей схемой проверки аутентичности "запрос-ответ" и получение из него соответствующих данных идентификации.

12. Способ по п. 10 или 11, причем получение данных (IDD_k) идентификации включает в себя:

основанное на датчике обнаружение одной или более отличительных характеристик (k) физического объекта или группы физических объектов (PO(s)),

генерирование данных объекта, представляющих одну или более отличительных характеристик (k) физического объекта или группы физических объектов (PO(s)),

передачу данных объекта системе для автоматического распознавания объекта, и

получение данных идентификации с цифровой подписью от системы в ответ на передачу данных объекта.

13. Способ по одному из пп. 10-12, также включающий в себя процесс сохранения, включающий в себя сохранение первого результата (RR1) считывания или побуждение к его сохранению в блоке блокчейна первого набора из одного или более блокчейнов или в одном или более узлов безблокового распределенного реестра первого набора из одного или более безблоковых распределенных реестров.

14. Способ по п. 13, причем:

обнаружение (410, 415) отличительных характеристик физического объекта или группы физических объектов (PO(s)) включает в себя обнаружение нескольких разных отличительных характеристик для получения на их основании для каждой отличительной характеристики (k) соответствующего индивидуального набора данных (IDD_k) идентификации, представляющих физический объект или группу физических объектов (PO(s)),

генерирование тестового значения (Ht) хеш-функции выполняется для каждого из индивидуальных наборов данных (IDD_k) идентификации отдельно, так чтобы получить для каждого из индивидуальных наборов данных (IDD_k) идентификации

соответствующее индивидуальное тестовое значение (Hi_k) хеш-функции,

генерирование результата первого считывания выполняется для каждого из индивидуальных тестовых значений хеш-функции отдельно, так чтобы получить для каждой из отличительных характеристик соответствующий индивидуальный результат первого считывания, и

процесс сохранения включает в себя сохранение соответственно каждого из индивидуальных результатов первого считывания, побуждая к их хранению в блоке соответствующего индивидуально выделенного блокчейна в первом наборе блокчейнов или в одном или более узлов соответствующего индивидуально выделенного безблокового распределенного реестра в первом наборе безблоковых распределенных реестров.

15. Способ по одному из пп. 10-14, также включающий в себя определение другого защищенного начального пакета (SSDP) данных для еще последующей защищенной проверки аутентичности физического объекта или группы физических объектов (PO(s)) у еще другого их получателя (C).

16. Способ по п. 15, причем определение другого защищенного начального пакета (SSDP) данных включает в себя:

выдачу запроса (R) для определения такого другого защищенного начального пакета (SSDP) данных для еще последующей защищенной проверки аутентичности физического объекта или группы физических объектов (PO(s)) у еще другого их получателя (C) авторизованному производителю (A) другого защищенного начального пакета (SSDP) данных и получение в ответ на запрос запрошенного другого защищенного начального пакета (SSDP) данных.

17. Способ по п. 15, причем определение другого защищенного начального пакета (SSDP) данных включает в себя:

осуществление способа по одному из пп. 1 или 2 так, что спрогнозированные контекстные данные (PCD) представляют спрогнозированное будущее местоположения другого намеченного получателя (C) физического объекта или группы физических объектов (PO(s)) и связанное будущее время присутствия физического объекта или группы физических объектов (PO(s)) в этом будущем местоположении.

18. Способ по п. 17, также включающий в себя:

посредством осуществления способа по одному из пп. 3-9 определение других данных (IND) инициализации на основании тех же случайных контекстных данных (RCD), как и другой защищенный начальный пакет (SSDP) данных, и сохранение или побуждение к сохранению других данных (IND) инициализации.

19. Система (30a, 30b, 30c) проверки аутентичности объекта, включающая в себя компьютер и выполненная для осуществления способа по одному из пп. 10-18.

20. Способ (600) защищенного обеспечения переменной по времени схемы (CS) комбинирования для проверки аутентичности физического объекта или группы физических объектов (PO(s)) способом по одному из пп. 10-18, включающий в себя:

получение и сохранение (605) данных, представляющих предварительно определенную схему (CS) комбинирования, независимую от времени и местоположения информацию (SN), идентифицирующую физический объект или группу физических объектов или связанную с ним или с ней, и метаданные (MD(CS(SN))), определяющие ограниченный период пригодности схемы (CS) комбинирования,

получение (610) запроса о схеме (CS) комбинирования и идентифицирующей информации (SN), идентифицирующей физический объект или группу физических объектов (PO(s)) или связанной с ним или с ней, от запрашивающей системы (30a, 30b,

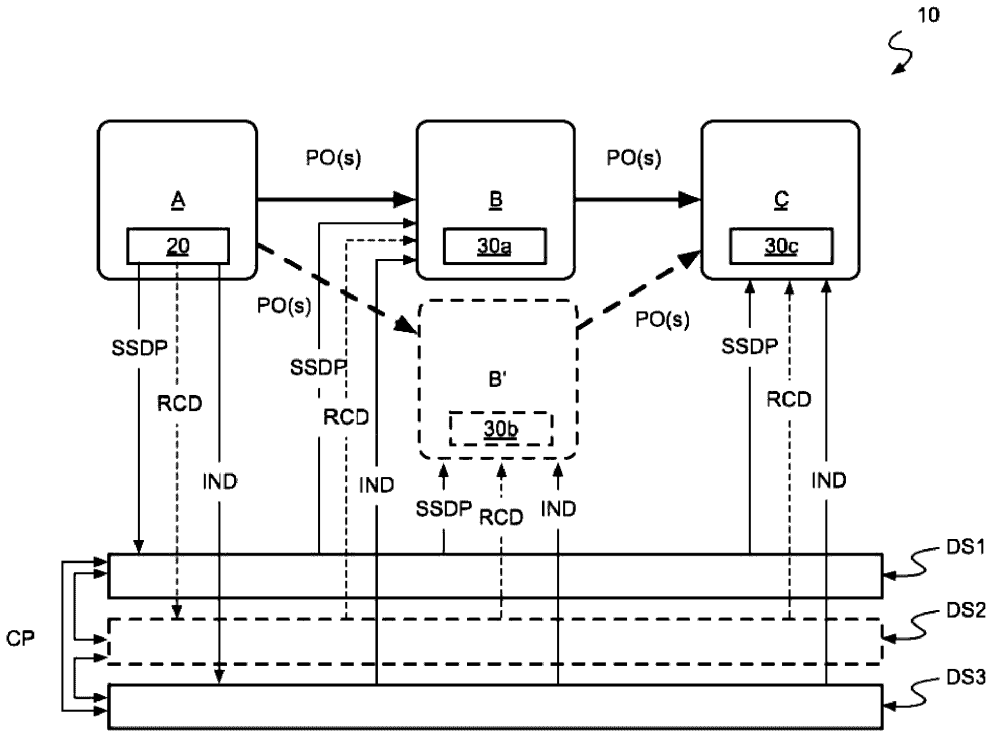
30c) проверки аутентичности,

проверку (615) аутентичности запрашивающей системы (30a, 30b, 30c), и

если запрашивающая система (30a, 30b, 30c) успешно выдержала проверку (615) аутентичности в качестве авторизованной и, согласно прежде сохраненным метаданным (MD(SN)), соответствующим полученной идентифицирующей информации (SN), связанная схема комбинирования (CS(SN)), к которой относятся метаданные, все еще является действительной, вывод (640) данных, представляющих эту связанную схему (CS(SN)) комбинирования, через защищенный (645) от перехвата канал (T) данных к запрашивающей системе (30a, 30b, 30c), или

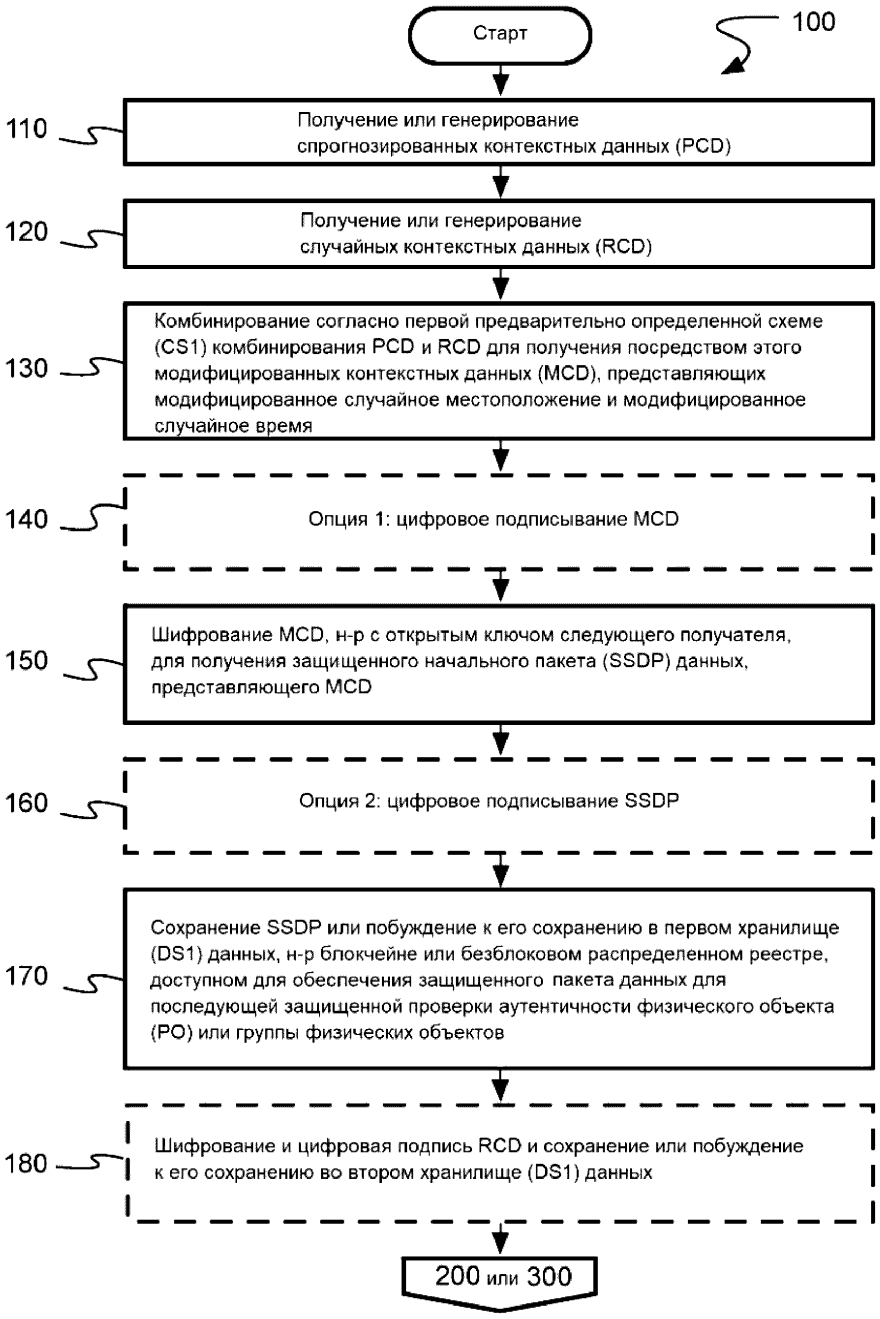
в противном случае отклонение запроса.

1


10
A
20
B
30a
C
30c
B'
30b
PO(s)
PO(s)
PO(s)
PO(s)
SSDP
RCD
IND
SSDP
RCD
IND
SSDP
RCD
IND
SSDP
RCD
IND
CP
DS1
DS2
DS3

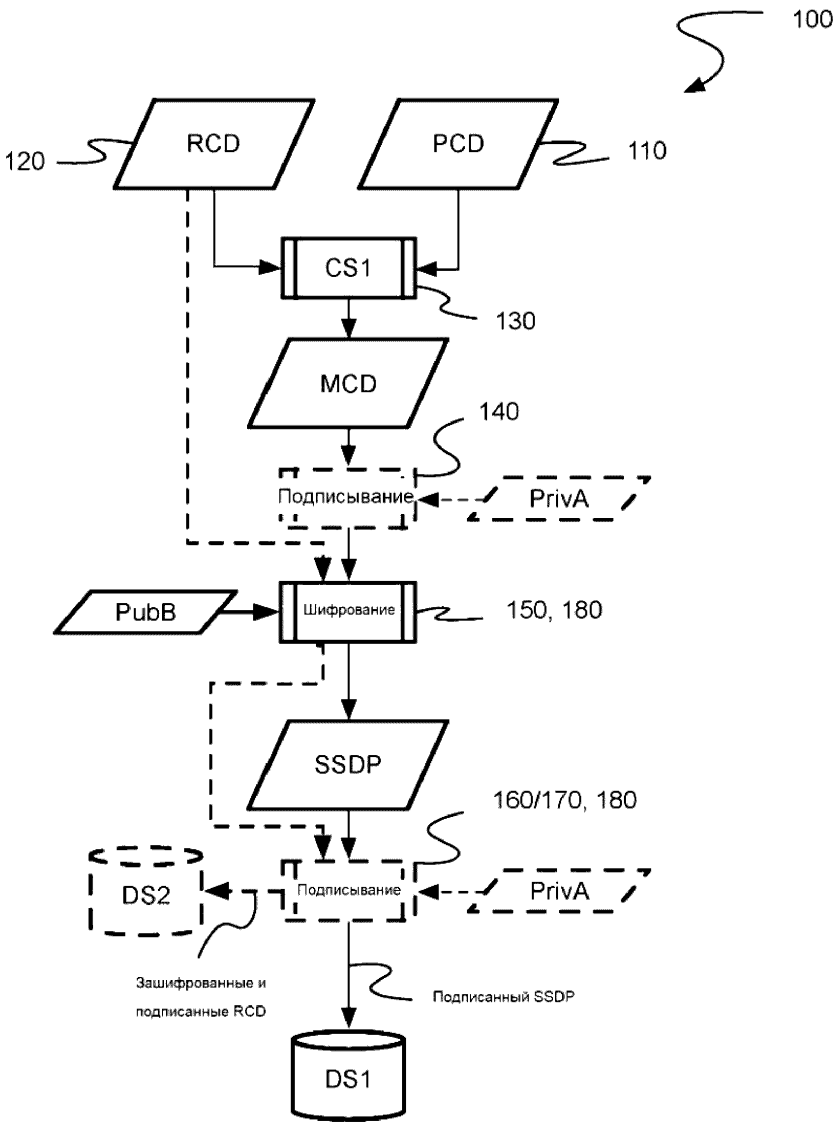
Фиг. 1

2


Старт
100
110
Получение или генерирование спрогнозированных контекстных данных (PCD)
120
Получение или генерирование случайных контекстных данных (RCD)
130
Комбинирование согласно первой предварительно определенной схеме (CS1) комбинирования PCD и RCD для получения посредством этого модифицированных контекстных данных (MCD), представляющих модифицированное случайное местоположение и модифицированное случайное время
140
Опция 1: цифровое подписывание MCD
150
Шифрование MCD, н-р с открытым ключом следующего получателя, для получения защищенного начального пакета (SSDP) данных, представляющего MCD
160
Опция 2: цифровое подписывание SSDP
170
Сохранение SSDP или побуждение к его сохранению в первом хранилище (DS1) данных, н-р блокчейне или безблоковом распределенном реестре, доступном для обеспечения защищенного пакета данных для последующей защищенной проверки аутентичности физического объекта (PO) или группы физических объектов
180
Шифрование и цифровая подпись RCD и сохранение или побуждение к его сохранению во втором хранилище (DS1) данных
200 или 300

Фиг. 2 A

3

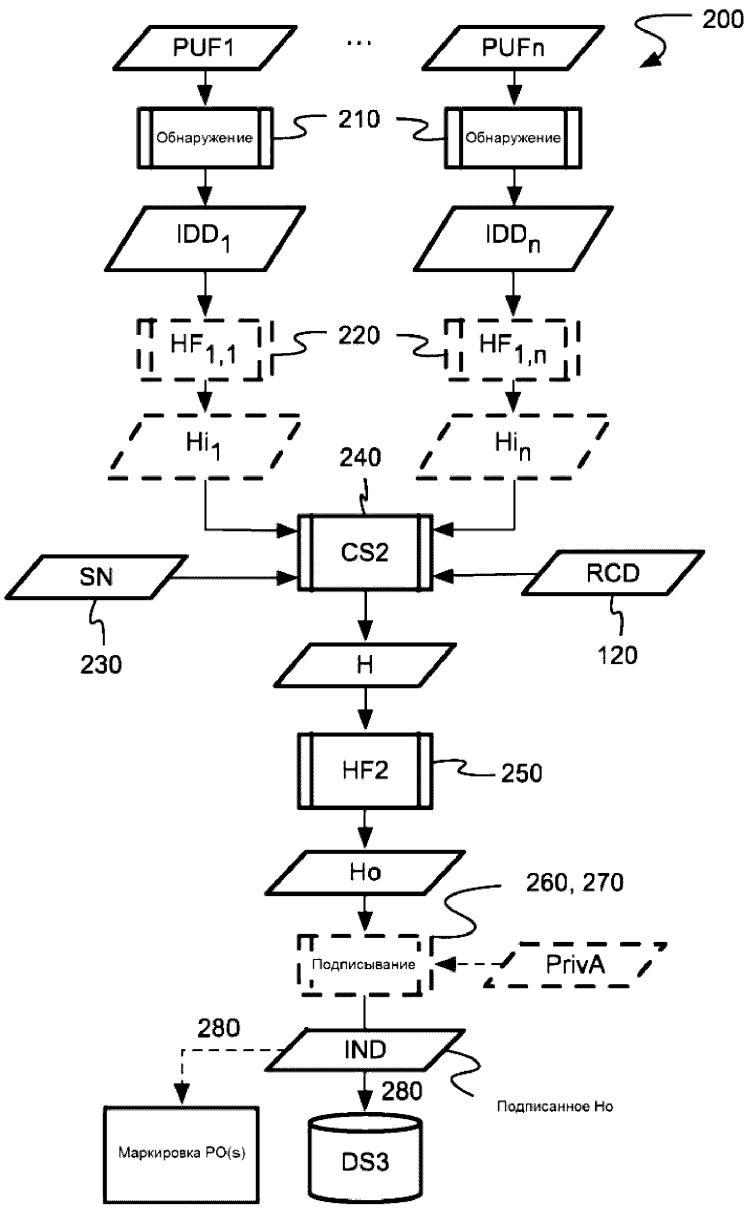

100
RCD
PCD
120
110
CS1
130
MCD
140
Подписывание
PrivA
PubB
Шифрование
150, 180
SSDP
160/170, 180
DS2
Подписывание
PrivA
Зашифрованные и
подписанные RCD
Подписанный SSDP
DS1

Фиг. 2 Б

4


100
200
210
Обнаружение по меньшей мере одной отличительной характеристики, н-р PUF, физического объекта PO(s) или группы физических объектов (PO(s)) для получения для каждой отличительной характеристики соответствующих данных (IDD) идентификации, представляющих идентификатор связанного PO(s)
220
Применение хеш-функции посредством соответствующей первой криптограф. хеш-функции (HF1) к полученным IDD соответствующей отличительной характеристики для получения соответствующего исходного значения (Hi) хеш-функции, связанного с соответствующей отличительной характеристикой
230
Генерирование или считывание с маркировки PO(s) независимого от местоположения и независимого от времени серийного номера SN
240
Определение набора H данных комбинации согласно второй схеме (CS2) комбинирования одного или нескольких, соответственно а) первых значений Hi хеш-функции, или б) IDD значений, случайных контекстных данных RCD, и серийного номера(-ов) SN PO(s)
250
Применение второй криптографической хеш-функции к комбинации H для получения исходного значения (Ho) хеш-функции
260
Цифровое подписывание исходного значения Ho хеш-функции
270
Генерирование данных (IND) инициализации, представляющих Ho (и, если применимо, полученную на шаге 260 его цифровую подпись)
280
Добавление к PO(s) представления IND, например соответствующей маркировки, и/или сохранение или побуждение к сохранению представления IND в третьем хранилище (DS3), и добавление к PO(s) представления указателя, указывающего, где IND могут быть доступны в DS3

Фиг. 3A


PUF1
...
PUFn
200
Обнаружение
210
Обнаружение
IDD1
IDDn
HF1,1
220
HF1,n
Hi1
Hin
240
CS2
SN
RCD
230
120
H
HF2
250
Ho
260, 270
Подписывание
PrivA
280
IND
280
Подписанное Ho
Маркировка PO(s)
DS3

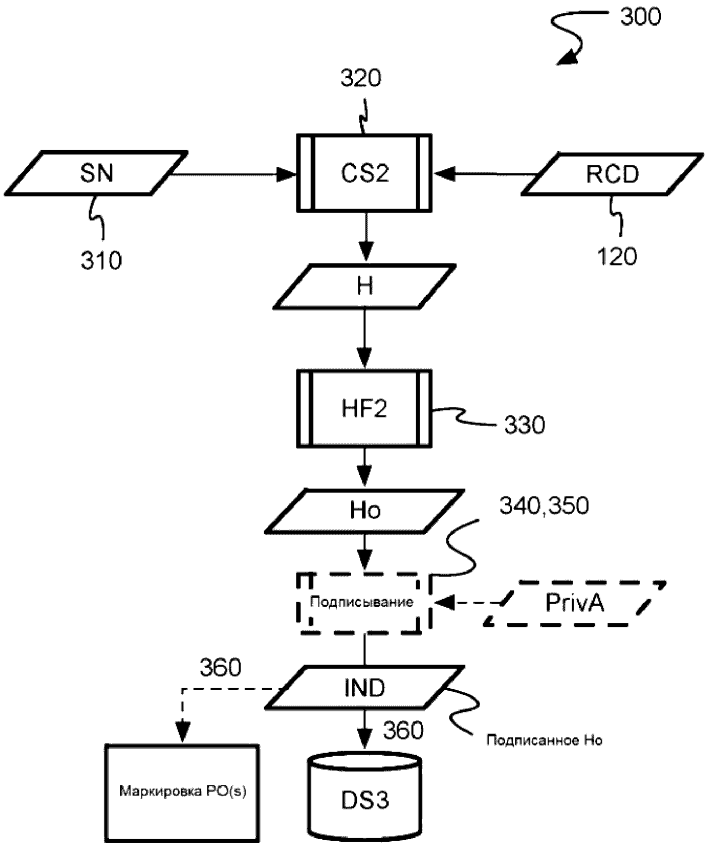
Фиг. 3Б

6

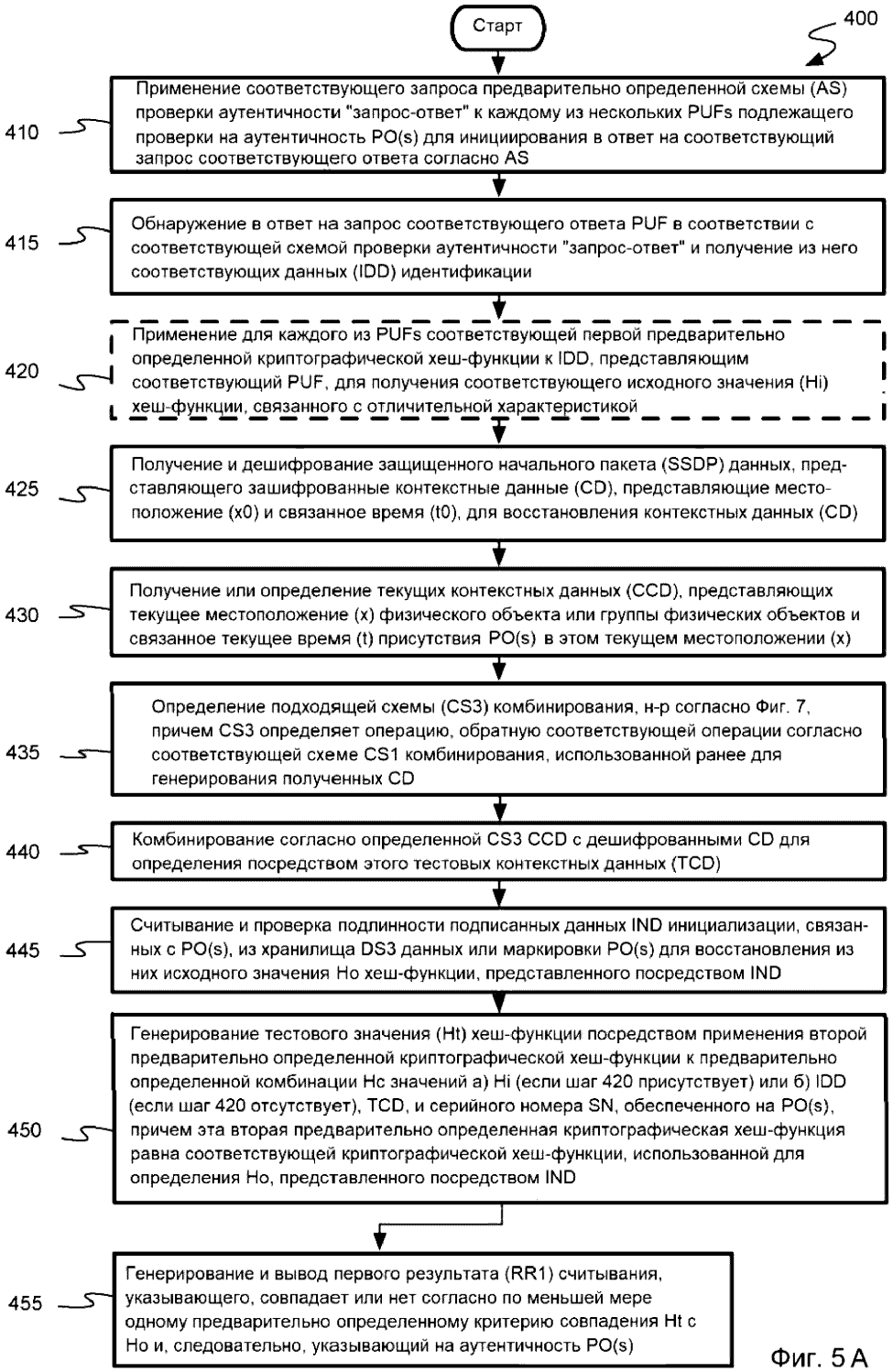

100
300
310
Генерирование или считывание с маркировки PO(s) независимого от местоположения и независимого от времени серийного номера(ов) SN
320
Определение значения H комбинации, согласно предварительно определенной схеме (CS2) комбинирования, случайных контекстных данных RCD и серийного номера(ов) SN PO(s)
330
Применение хеш-функции посредством криптографической хеш-функции к полученному в результате значению H комбинации, согласно предварительно определенной схеме (CS2) комбинирования, случайной контекстной информации и серийного номера(ов) SN PO(s) для получения исходного значения (Ho) хеш-функции
340
Цифровое подписывание исходного значения Ho хеш-функции
350
Генерирование данных (IND) инициализации, представляющих Ho (и, если применимо, полученную на шаге 340 его цифровую подпись)
360
Добавление к PO(s) представления IND, например соответствующей маркировки, и/или сохранение или побуждение к сохранению представления IND в третьем хранилище (DS3), и добавление к PO(s) представления указателя, указывающего, где IND могут быть доступны в DS3

Фиг. 4 A

7

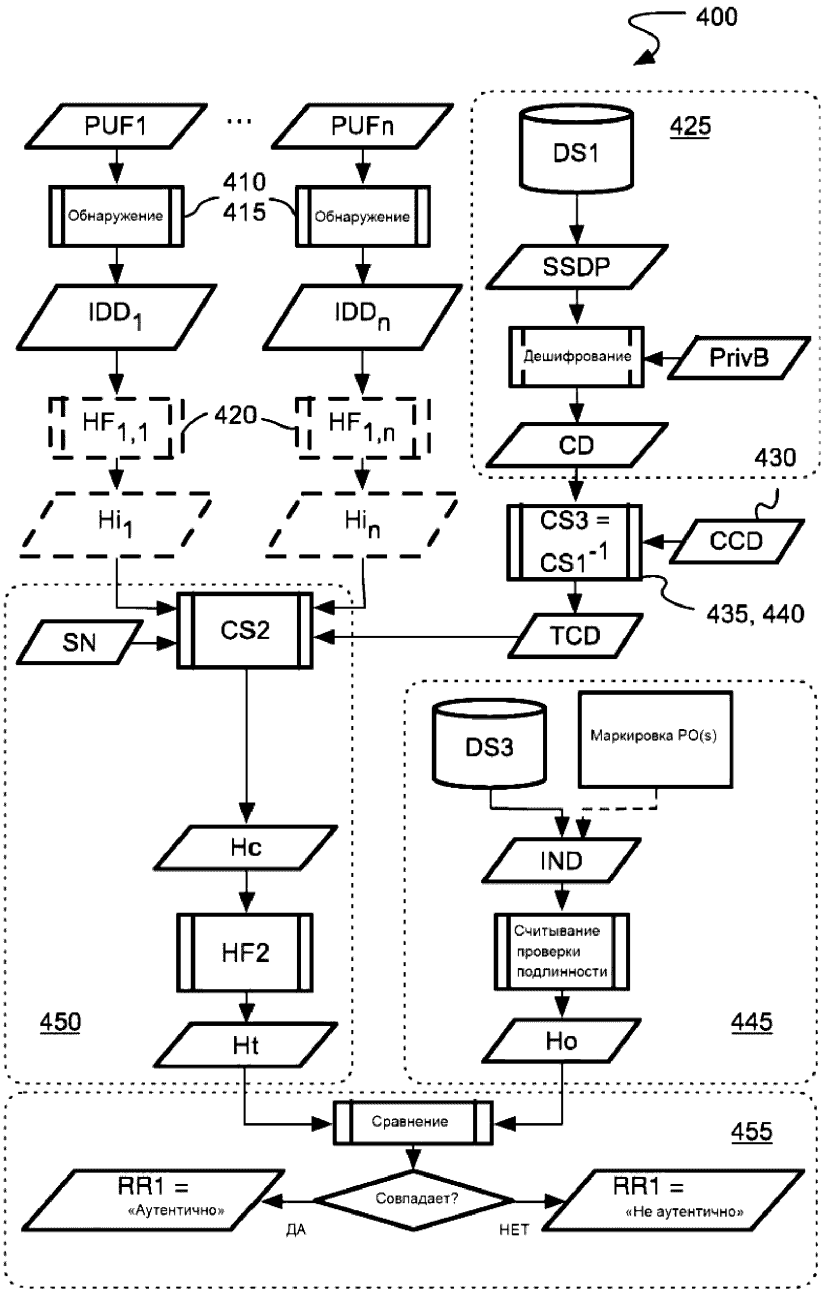

300
320
SN
CS2
RCD
310
120
H
HF2
330
Ho
340,350
Подписывание
PrivA
360
IND
360
Подписанное Ho
Маркировка PO(s)
DS3

Фиг. 4Б

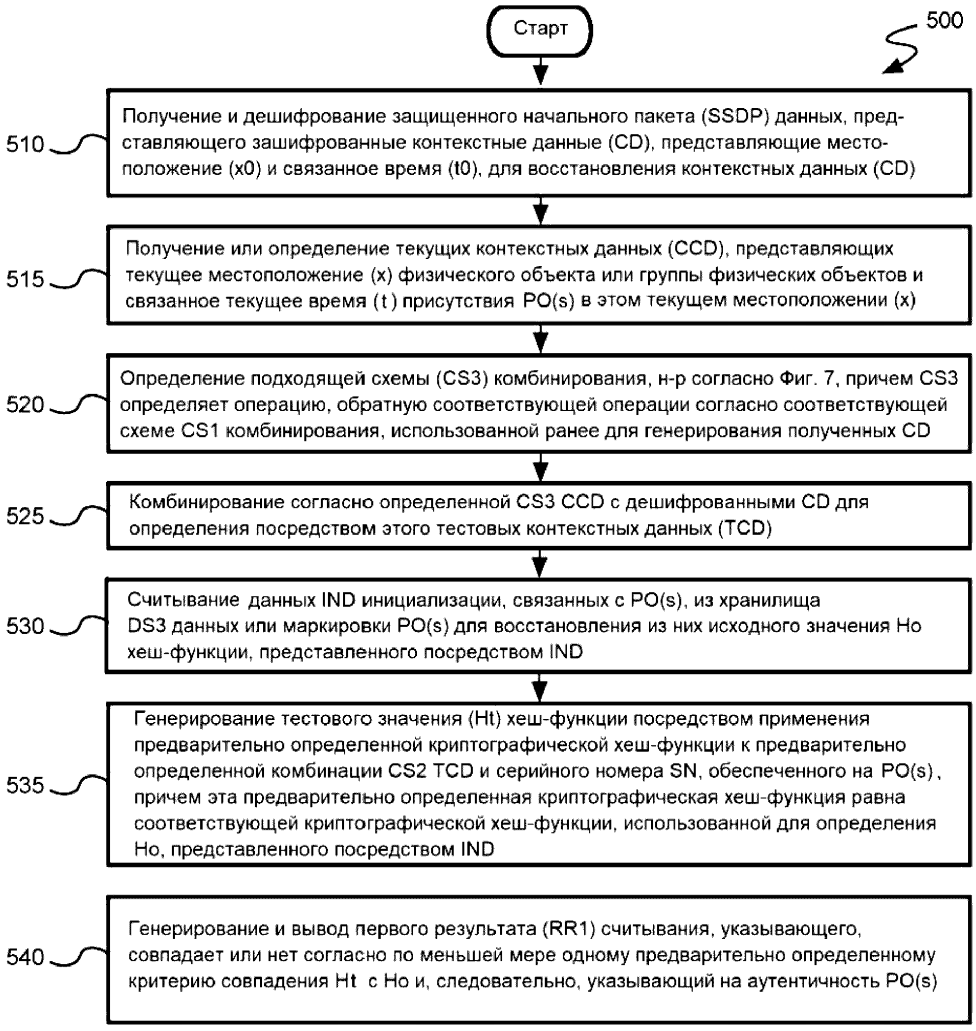

Старт
400
410
Применение соответствующего запроса предварительно определенной схемы (AS) проверки аутентичности "запрос-ответ" к каждому из нескольких PUFs подлежащего проверки на аутентичность PO(s) для инициирования в ответ на соответствующий запрос соответствующего ответа согласно AS
415
Обнаружение в ответ на запрос соответствующего ответа PUF в соответствии с соответствующей схемой проверки аутентичности "запрос-ответ" и получение из него соответствующих данных (IDD) идентификации
420
Применение для каждого из PUFs соответствующей первой предварительно определенной криптографической хеш-функции к IDD, представляющим соответствующий PUF, для получения соответствующего исходного значения (Hi) хеш-функции, связанного с отличительной характеристикой
425
Получение и дешифрование защищенного начального пакета (SSDP) данных, представляющего зашифрованные контекстные данные (CD), представляющие местоположение (x0) и связанное время (t0), для восстановления контекстных данных (CD)
430
Получение или определение текущих контекстных данных (CCD), представляющих текущее местоположение (x) физического объекта или группы физических объектов и связанное текущее время (t) присутствия PO(s) в этом текущем местоположении (x)
435
Определение подходящей схемы (CS3) комбинирования, н-р согласно Фиг. 7, причем CS3 определяет операцию, обратную соответствующей операции согласно соответствующей схеме CS1 комбинирования, использованной ранее для генерирования полученных CD
440
Комбинирование согласно определенной CS3 CCD с дешифрованными CD для определения посредством этого тестовых контекстных данных (TCD)
445
Считывание и проверка подлинности подписанных данных IND инициализации, связанных с PO(s), из хранилища DS3 данных или маркировки PO(s) для восстановления из них исходного значения Ho хеш-функции, представленного посредством IND
450
Генерирование тестового значения (Ht) хеш-функции посредством применения второй предварительно определенной криптографической хеш-функции к предварительно определенной комбинации Hc значений а) Hi (если шаг 420 присутствует) или б) IDD (если шаг 420 отсутствует), TCD, и серийного номера SN, обеспеченного на PO(s), причем эта вторая предварительно определенная криптографическая хеш-функция равна соответствующей криптографической хеш-функции, использованной для определения Ho, представленного посредством IND
455
Генерирование и вывод первого результата (RR1) считывания, указывающего, совпадает или нет согласно по меньшей мере одному предварительно определенному критерию совпадения Ht с Ho и, следовательно, указывающий на аутентичность PO(s)

Фиг. 5 А

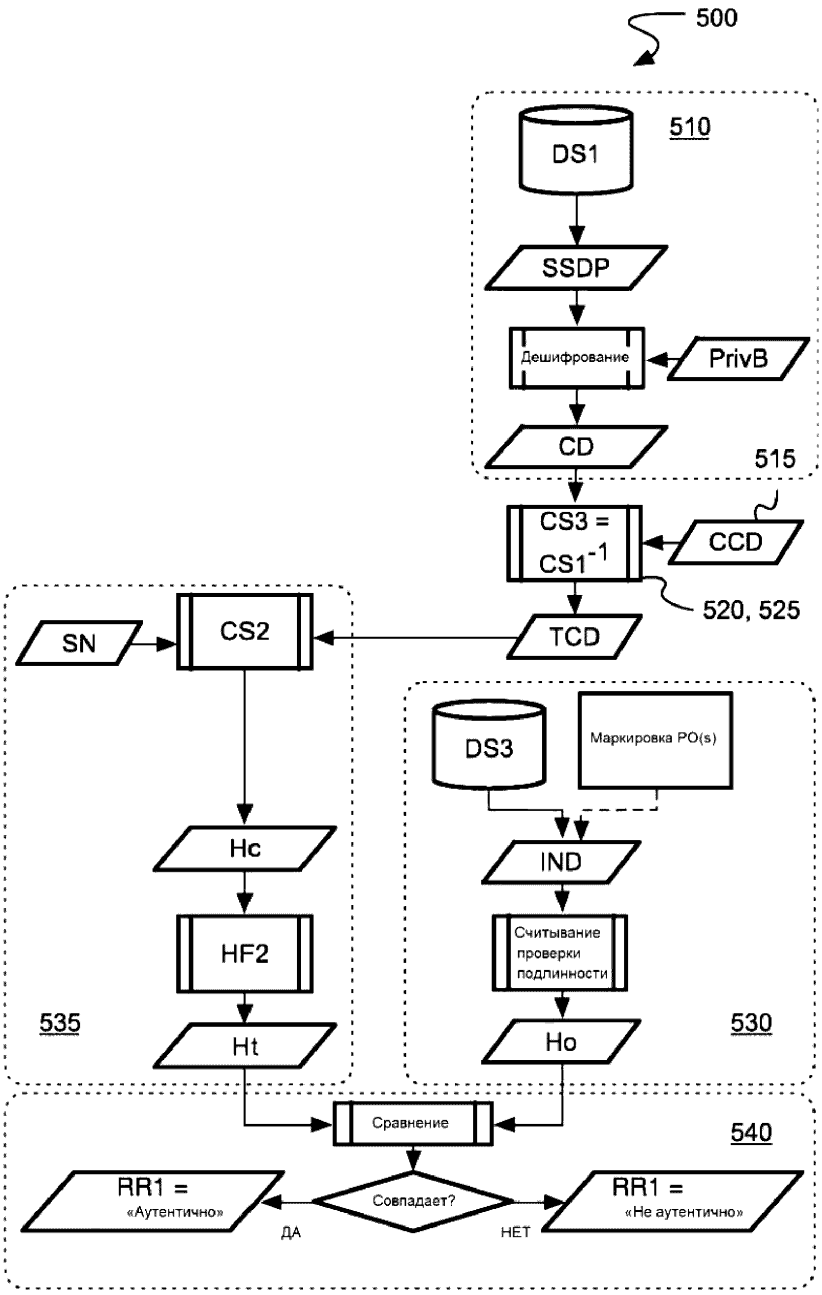
9


400
PUF1
PUFn
410
415
Обнаружение
Обнаружение
IDD1
IDDn
HF1,1
420
HF1,n
Hi1
Hin
425
DS1
SSDP
Дешифрование
PrivB
CD
430
CS3 = CS1-1
CCD
435, 440
TCD
SN
CS2
DS3
Маркировка PO(s)
Hc
IND
HF2
Считывание проверки подлинности
450
Ht
Ho
445
Сравнение
455
RR1 = «Аутентично»
Совпадает?
ДА
НЕТ
RR1 = «Не аутентично»

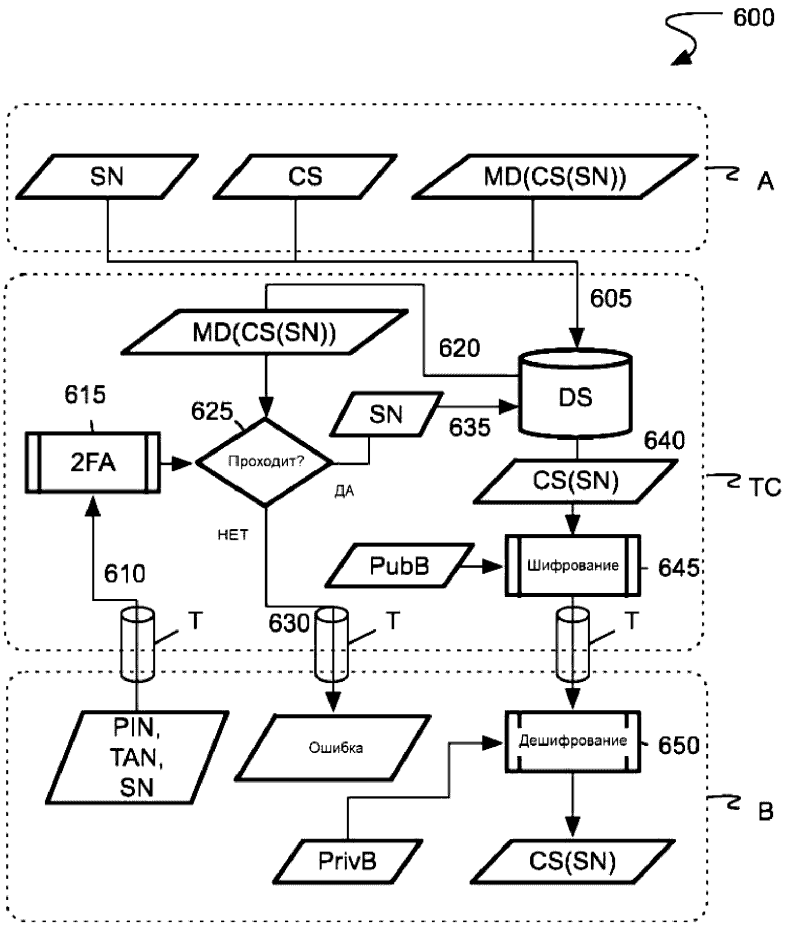
Фиг. 5Б


Старт
500
510
Получение и дешифрование защищенного начального пакета (SSDP) данных, представляющего зашифрованные контекстные данные (CD), представляющие местоположение (x0) и связанное время (t0), для восстановления контекстных данных (CD)
515
Получение или определение текущих контекстных данных (CCD), представляющих текущее местоположение (x) физического объекта или группы физических объектов и связанное текущее время (t) присутствия PO(s) в этом текущем местоположении (x)
520
Определение подходящей схемы (CS3) комбинирования, н-р согласно Фиг. 7, причем CS3 определяет операцию, обратную соответствующей операции согласно соответствующей схеме CS1 комбинирования, использованной ранее для генерирования полученных CD
525
Комбинирование согласно определенной CS3 CCD с дешифрованными CD для определения посредством этого тестовых контекстных данных (TCD)
530
Считывание данных IND инициализации, связанных с PO(s), из хранилища DS3 данных или маркировки PO(s) для восстановления из них исходного значения Ho хеш-функции, представленного посредством IND
535
Генерирование тестового значения (Ht) хеш-функции посредством применения предварительно определенной криптографической хеш-функции к предварительно определенной комбинации CS2 TCD и серийного номера SN, обеспеченного на PO(s), причем эта предварительно определенная криптографическая хеш-функция равна соответствующей криптографической хеш-функции, использованной для определения Ho, представленного посредством IND
540
Генерирование и вывод первого результата (RR1) считывания, указывающего, совпадает или нет согласно по меньшей мере одному предварительно определенному критерию совпадения Ht с Ho и, следовательно, указывающий на аутентичность PO(s)

Фиг. 6 A

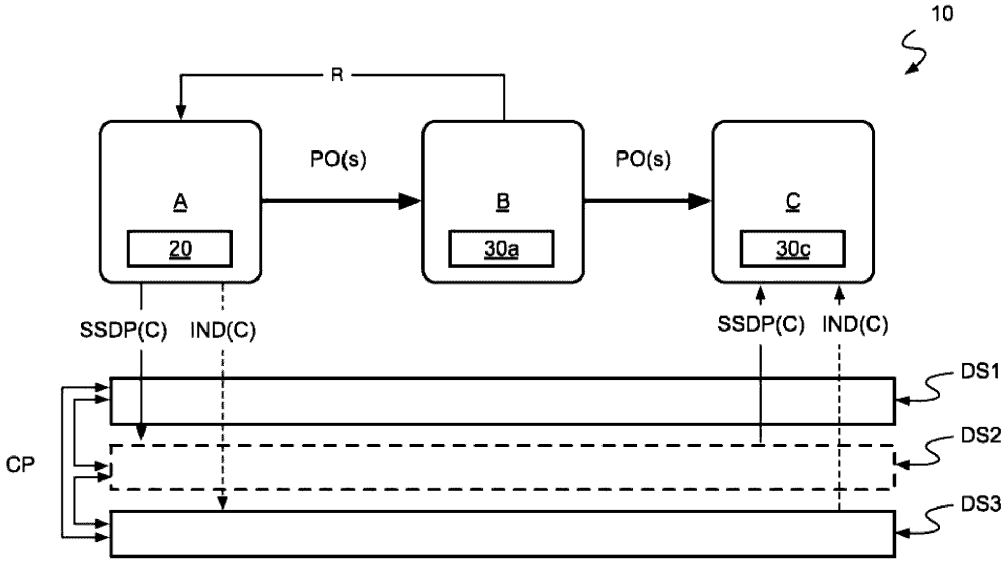

500
510
DS1
SSDP
Дешифрование
PrivB
CD
515
CS3 =
CS1-1
CCD
520, 525
TCD
SN
CS2
Hc
HF2
Ht
535
DS3
Маркировка PO(s)
IND
Считывание проверки подлинности
Ho
530
Сравнение
540
RR1 =
«Аутентично»
Совпадает?
ДА
НЕТ
RR1 =
«Не аутентично»

Фиг. 6Б

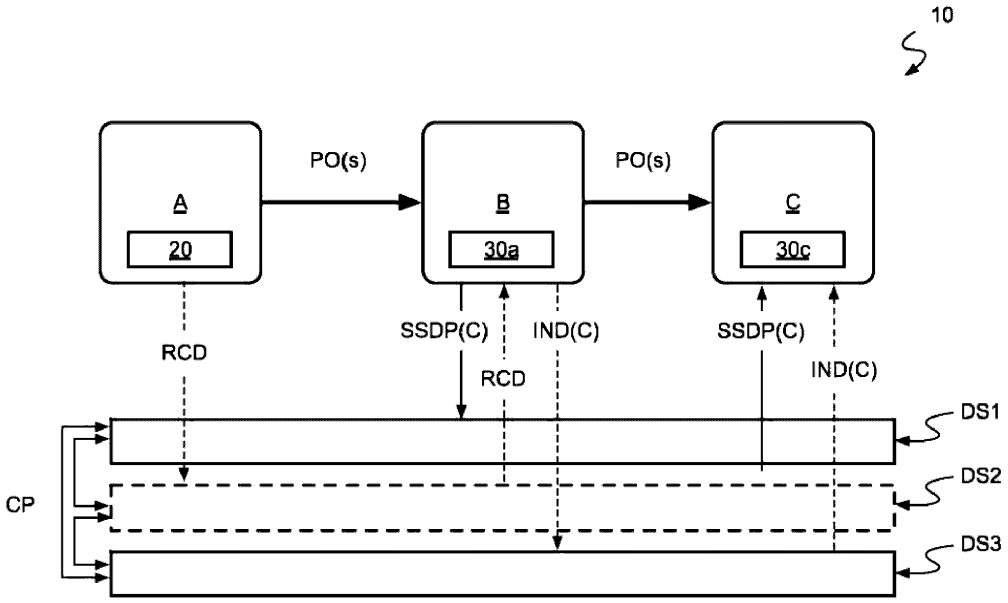

600
SN
CS
MD(CS(SN))
A
605
MD(CS(SN))
620
DS
615
625
SN
635
640
2FA
Проходит?
ДА
CS(SN)
TC
НЕТ
PubB
Шифрование
645
610
T
630
T
T
PIN,
TAN,
SN
Ошибка
Дешифрование
650
B
PrivB
CS(SN)

Фиг. 7

13


10
R
A
20
PO(s)
B
30a
PO(s)
C
30c
SSDP(C)
IND(C)
SSDP(C)
IND(C)
DS1
DS2
DS3
CP

Фиг. 8 А


10
A
20
PO(s)
B
30a
PO(s)
C
30c
RCD
SSDP(C)
RCD
IND(C)
SSDP(C)
IND(C)
DS1
DS2
DS3
CP

Фиг. 8 Б