(19) Евразийское патентное ведомство

(11) 042414 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.02.10

(21) Номер заявки
201991297

(22) Дата подачи заявки
2018.01.05

(51) Int. Cl. ***G06F 21/33*** (2013.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(54) СИСТЕМА И СПОСОБ УСТАНОВЛЕНИЯ ПОДЛИННОСТИ СЕРТИФИКАТОВ БЕЗОПАСНОСТИ

(31) **17151051.4**
(32) **2017.01.11**
(33) **EP**
(43) **2019.12.30**
(86) **PCT/EP2018/050262**
(87) **WO 2018/130464 2018.07.19**

(71)(73) Заявитель и патентовладелец:
СИКПА ХОЛДИНГ СА (CH)

(72) Изобретатель:
Пападимитриу Панделис (CH)

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

(56) US-A1-2015358163
US-A1-2007083753
US-B1-9331856
US-A1-2012125997
US-A1-2012308003

(57) Настоящее изобретение относится к защищаемому изделию, содержащему сертификат безопасности, содержащий данные, которые были зашифрованы с помощью личного ключа шифрования. Данные выполнены с возможностью расшифрования с помощью открытого ключа расшифрования, связанного с личным ключом шифрования, с целью установления подлинности сертификата безопасности. Настоящее изобретение также относится к системам и способам установления подлинности сертификата безопасности.

042414 B1

042414 B1

Область техники изобретения

Настоящее изобретение относится в целом к системе и способу установления подлинности сертификатов безопасности.

Предпосылки создания изобретения

Желательно обеспечить надежное установление подлинности определенных документов, объектов или транзакций, чтобы определить, является ли документ или объект мошенническим или был подделан в попытке изменить учетные данные документа, объекта или транзакции.

Примеры документов и объектов, для которых будет полезно безопасное установление подлинности, включают документы, удостоверяющие личность, такие как: свидетельства о рождении, запись(-и) о школе, свидетельства о браке, документы о трудоустройстве, документы о подоходном налоге, документы о владении бизнесом, паспорт или другие проездные документы, въездные визы и другие связанные с паспортом въездные и выездные штампы, свидетельства о смерти и/или любые другие доказательства действительности или сертификации, такие как акции, облигации, международные банковские чеки и т. д. Другие примеры документов и объектов, для которых будет полезно безопасное установление подлинности, включают произведения искусства, артефакты, изготовляемые изделия, памятные вещи и/или коносаменты. Примеры транзакций, для которых будет полезно безопасное установление подлинности, включают транзакции с помощью карты, банкнот и/или цифровые транзакции.

Эти документы, объекты или транзакции могут быть целью фальсификации. В частности, сертификаты безопасности, используемые для показа учетных данных этих документов или объектов, могут быть сфальсифицированы в попытке убедить третью сторону в подлинности фальсификации.

Поэтому существует потребность в новой и улучшенной системе, которая позволила бы легко и безопасно установить подлинность таких документов или объектов.

Сущность изобретения

Соответственно, в предпочтительных вариантах осуществления настоящего изобретения предусмотрены система и способ установления подлинности, что обеспечивает легкое и безопасное установление подлинности сертификатов безопасности.

Согласно первому аспекту настоящего изобретения предусмотрен сертификат безопасности, содержащий данные, которые были зашифрованы с помощью личного ключа шифрования, при этом данные выполнены с возможностью расшифрования с помощью открытого ключа расшифрования, связанного с личным ключом шифрования, с целью установления подлинности сертификата безопасности.

Зашифрованные данные могут сохраняться в виде визуального изображения. Визуальное изображение может представлять собой QR-код, штрих-код или изображение в оттенках серого. Хранение зашифрованных данных в виде визуального изображения предусматривает визуальный контроль за уполномоченным представителем для определения того, не является ли сертификат безопасности явно подделанным, что повышает вероятность обнаружения подделки или фальсификаций. Следует отметить, что видимые средства в любых условиях освещения и не обязательно в условиях видимого освещения.

В качестве альтернативы, зашифрованные данные можно хранить в цифровой форме, например, на микропроцессорной БИС, ИС RFID или магнитной дорожке. Хранение зашифрованных данных в цифровой форме позволяет увеличить срок службы сертификата безопасности, а также позволяет уменьшить физическое пространство, необходимое для хранения данных в сертификате безопасности.

Зашифрованные данные могут включать динамические данные. Динамические данные, используемые в данном документе, означают данные, которые могут изменяться и/или обновляться, например, посредством ввода пользователем. Динамические данные могут храниться в виде штампа, кода или другого визуального изображения. В качестве альтернативы, динамические данные могут храниться в цифровой форме. Динамические данные могут обновляться или изменяться на центральном сервере. Другими словами, динамические данные, связанные с визуальным изображением (или динамические данные в цифровой форме), могут храниться на центральном сервере, и динамические данные могут обновляться и/или изменяться в любое время. Обновление и/или изменение динамических данных может быть предметом авторизации. Примеры динамических данных включают выездные и повторные штампы для визы.

В качестве дополнения или альтернативы, зашифрованные данные могут включать статические данные. Под используемыми в данном документе статическими данными подразумеваются данные, которые не изменяются и/или не обновляются. Как описано выше в отношении динамических данных, статические данные могут храниться в виде визуального изображения или в цифровой форме. Примеры статических данных включают картинки и статистические отпечатки пальцев. Другие примеры статических данных включают другие типы биометрических данных, таких как радужная оболочка или данные о лице.

Сертификат безопасности может содержать дополнительные данные, которые были зашифрованы с помощью открытого ключа шифрования, при этом данные выполнены с возможностью расшифрования с помощью личного ключа расшифрования, связанного с открытым ключом шифрования. Использование открытого ключа шифрования для шифрования данных позволяет хранить дополнительные данные в сертификате безопасности наряду с данными, зашифрованными с помощью личного ключа шифрования. Некоторые или все дополнительные данные могут быть зашифрованы для конфиденциальности с помощью открытого ключа шифрования.

Различные открытые ключи шифрования могут быть использованы для шифрования различных частей дополнительных данных. Использование различных открытых ключей шифрования для шифрования и установления подлинности различных частей дополнительных данных позволяет различным сторонам получать доступ к различным частям дополнительных данных. В частности, разным сторонам может быть разрешен доступ к различным личным ключам расшифрования, связанным с различными открытыми ключами шифрования, используемыми для шифрования различных частей зашифрованных дополнительных данных. То, какие личные ключи расшифрования доступны для стороны, может зависеть, например, от уровня авторизации этой стороны. Например, дополнительные данные могут быть связаны с тем, просрочил ли человек визу в той или иной стране или нет. Видимость/доступность данных, касающихся того, просрочил ли человек визу или нет, может быть ограничена, например, органами по надзору за поездками в некоторых конкретных уполномоченных странах. В качестве альтернативы или дополнения, дополнительные данные могут быть связаны, например, с правом на получение пособий в конкретной стране.

Сертификат безопасности может образовывать часть въездной визы. Въездные визы представляют собой элемент, который был бы особенно полезен для безопасного установления подлинности с помощью открытого ключа шифрования, поскольку визы особенно восприимчивы к фальсификации или подделке, а также поскольку установление подлинности въездных виз требует сотрудничества между различными странами, при этом такое сотрудничество трудно эффективно координировать.

Зашифрованные данные могут быть в виде штампа. Использование в виде штампа для отображения зашифрованных данных является универсальным методом быстрого и эффективного связывания зашифрованных данных с документом или объектом. Штамп может быть штампом, нанесенным на въездную визу, таким как физический штамп, нанесенный путем физического штампования или печати на странице паспорта.

Данные могут отображаться на сертификате безопасности только в зашифрованной визуальной форме, так что никакие незашифрованные данные, соответствующие зашифрованным данным, не могут быть просмотрены на сертификате безопасности. Представляя таким образом только зашифрованные данные, нельзя проводить сравнение между зашифрованными данными и незашифрованными данными, что снижает вероятность подделки данных, что может быть возможным из-за визуального сравнения зашифрованных и незашифрованных данных.

Согласно второму аспекту настоящего изобретения предусмотрена система установления подлинности сертификатов безопасности, содержащая: генератор сертификатов безопасности, выполненный с возможностью шифрования данных с помощью личного ключа шифрования, а затем генерирования сертификата безопасности, содержащего зашифрованные данные; справочник открытых ключей расшифрования, выполненный с возможностью предоставления уполномоченному пользователю доступа к открытому ключу расшифрования, связанному с личным ключом шифрования; и блок установления подлинности, выполненный с возможностью расшифрования зашифрованных данных с помощью открытого ключа расшифрования, доступ к которому обеспечивается, связанного с личным ключом шифрования.

В варианте осуществления блок установления подлинности выполнен с возможностью определения успешного или неуспешного расшифрования зашифрованных данных с помощью открытого ключа расшифрования, доступ к которому обеспечивается. Автоматизация процесса определения того, были ли зашифрованные данные успешно расшифрованы с помощью открытого ключа расшифрования, доступ к которому обеспечивается, позволяет быстрее определить, является ли сертификат безопасности подлинным.

В варианте осуществления блок установления подлинности выполнен с возможностью указания того, что сертификат безопасности является подлинным в случае успешного расшифрования зашифрованных данных. Таким образом, можно определить, является ли сертификат безопасности подлинным или нет. Кроме того, с автоматическим определением того, были ли зашифрованные данные успешно расшифрованы или нет, указание блока установления подлинности в отношении подлинности сертификата безопасности может быть перепроверено с помощью визуальной проверки, осуществляемой уполномоченным представителем для обеспечения запасных вариантов в процессе установления подлинности, тем самым уменьшая вероятность ложноположительного результата.

Аналогичным образом, блок установления подлинности может (в качестве дополнения или альтернативы) быть выполнен с возможностью указания того, что сертификат безопасности не является подлинным, если сертификат безопасности не был успешно расшифрован, с теми же преимуществами, которые подробно описаны выше.

В качестве дополнения или альтернативы, блок установления подлинности может быть выполнен с возможностью приложения алгоритма контрольной суммы для проверки действительности расшифрованных данных.

Кроме того, также можно анализировать защитную краску, используемую для печати сертификата безопасности, предпочтительно на первом этапе, чтобы определить, является ли краска подлинной или нет.

В варианте осуществления справочник открытых ключей расшифрования может содержать базу данных, содержащую по меньшей мере один открытый ключ расшифрования. В варианте осуществления

справочник открытых ключей расшифрования может содержать базу данных, содержащую множество открытых ключей расшифрования. База данных может быть организована так, чтобы назначать по меньшей мере один идентификатор открытому ключу расшифрования, при этом по меньшей мере один идентификатор связан со связанным личным ключом шифрования. Например, в случае въездных виз открытые ключи расшифрования могут быть заказаны страной-эмитентом, так что данные о въездной визе, выданной конкретной страной-эмитентом, легко идентифицировать, и сертификат безопасности, содержащий данные, зашифрованные с помощью личного ключа шифрования этой страны, может быть легко идентифицирован, чтобы обеспечить возможность быстрого и эффективного доступа к соответствующему связанному открытому ключу расшифрования. В качестве альтернативы, база данных может быть упорядочена по ключевой функции - с ключами, которые могут шифровать различные сегменты данных, которые группируются.

База данных может быть доступна для поиска. База данных может быть управляемой базой данных, где один уполномоченный менеджер является единственным менеджером. В качестве альтернативы, более одного уполномоченного менеджера могут управлять базой данных.

В варианте осуществления генератор сертификатов безопасности выполнен с возможностью использования открытого ключа шифрования для шифрования данных при генерировании сертификата безопасности. Использование открытого ключа шифрования для шифрования данных в сертификате безопасности позволяет зашифровать некоторые или все данные штампа для обеспечения конфиденциальности, как подробно описано выше. Кроме того, генератор сертификатов безопасности может быть выполнен с возможностью использования различных открытых ключей шифрования, чтобы обеспечить уровни шифрования для разных частей данных штампа, таким же образом, как подробно описано выше.

Система может дополнительно содержать блок расшифрования конфиденциальных данных, выполненный с возможностью приема от уполномоченного пользователя данных, зашифрованных с помощью открытого ключа шифрования, при этом блок расшифрования конфиденциальных данных выполнен с возможностью расшифрования принятых зашифрованных данных с помощью связанного личного ключа расшифрования. Личный ключ расшифрования может храниться в справочнике личных ключей расшифрования, выполненном с возможностью предоставления уполномоченному пользователю доступа к личному ключу шифрования, связанному с открытым ключом шифрования. Блок расшифрования конфиденциальных данных затем может быть выполнен с возможностью передачи или иного представления расшифрованных данных уполномоченному пользователю.

Таким образом, конфиденциальные данные, зашифрованные с помощью открытого ключа шифрования, могут быть расшифрованы уполномоченными пользователями без обмена личными ключами между пользователями.

В частности, справочник личных ключей расшифрования может быть безопасным местом для обеспечения централизованного расшифрования зашифрованных конфиденциальных данных. Справочник личных ключей расшифрования может быть базой данных, хранящей по меньшей мере один личный ключ расшифрования. База данных может быть доступна для поиска. База данных может быть управляемой базой данных, где уполномоченный менеджер является единственным менеджером. В качестве альтернативы, более одного уполномоченного менеджера могут управлять базой данных.

Блок расшифрования конфиденциальных данных может быть тем же или дополнительным блоком установления подлинности. Использование блока установления подлинности также для расшифрования конфиденциальных данных позволяет снизить затраты на оборудование и повысить безопасность обработки данных.

Уполномоченный пользователь может получить доступ к личному ключу расшифрования путем извлечения личного ключа расшифрования из справочника личных ключей расшифрования. Уполномоченный пользователь может расшифровать зашифрованные конфиденциальные данные локально, на блоке расшифрования конфиденциальных данных, с помощью извлеченного личного ключа расшифрования.

Помимо возможности отображения зашифрованных и незашифрованных данных на сертификате безопасности, данные могут отображаться на сертификате безопасности только в зашифрованной визуальной форме, так что никакие незашифрованные данные, соответствующие зашифрованным данным, не могут быть просмотрены на сертификате безопасности. Представляя, таким образом, только зашифрованные данные, нельзя проводить сравнение между зашифрованными данными и незашифрованными данными, что снижает вероятность подделки данных, что может быть возможным из-за визуального сравнения зашифрованных и незашифрованных данных.

Согласно третьему аспекту настоящего изобретения предусмотрен способ установления подлинности сертификата безопасности, включающий: сбор зашифрованных данных, хранящихся в сертификате безопасности, при этом данные были зашифрованы с помощью личного ключа шифрования; передачу зашифрованных данных в блок установления подлинности для предпринятого расшифрования зашифрованных данных с помощью открытого ключа расшифрования, связанного с личным ключом шифрования; и определение успеха или неудачи предпринятого расшифрования зашифрованных данных, при этом успешное расшифрование зашифрованных данных устанавливает подлинность сертификата безопасности.

Согласно четвертому аспекту настоящего изобретения предусмотрен способ установления подлинности сертификата безопасности, включающий: сбор зашифрованных данных, хранящихся в сертификате безопасности, при этом данные были зашифрованы с помощью личного ключа шифрования; извлечение открытого ключа расшифрования, связанного с личным ключом шифрования, из справочника открытых ключей расшифрования; предприятие попытки расшифрования зашифрованных данных с помощью открытого ключа расшифрования, связанного с личным ключом шифрования; и определение успеха или неудачи предпринятого расшифрования зашифрованных данных, при этом успешное расшифрование зашифрованных данных устанавливает подлинность сертификата безопасности.

Любой из третьего или четвертого аспектов может быть выполнен с помощью компьютера. Зашифрованные данные могут сохраняться в виде визуального изображения или в цифровой форме, как подробно описано выше. Визуальное изображение может представлять собой QR-код, штрих-код или изображение в оттенках серого. Визуальное изображение может быть скрытым изображением в изображении или последовательностью частот, генерируемых устройством, например, нажатием клавиши на цифровом телефоне, эти частоты могут генерироваться считывающим устройством или записанным звуком.

В любом из третьего или четвертого аспектов предпринятое расшифрование может выполняться блоком установления подлинности.

Сертификат безопасности может образовывать часть въездной визы. Как подробно описано выше, эти способы особенно полезны для въездных виз, которые особенно восприимчивы к фальсификации, и, поскольку многие различные страны-участницы выдают въездные визы, важно, чтобы информация могла передаваться между странами-участницами безопасным и эффективным способом.

Зашифрованные данные могут отображаться в виде штампа.

Любой из способов третьего или четвертого аспектов могут осуществлять несколько раз, например, для установления подлинности зашифрованных данных несколько раз в разных местах.

В любом из третьего или четвертого аспектов данные могут отображаться на сертификате безопасности только в зашифрованной визуальной форме, так что никакие незашифрованные данные, соответствующие зашифрованным данным, не могут быть просмотрены на сертификате безопасности. Представляя, таким образом, только зашифрованные данные, нельзя проводить сравнение между зашифрованными данными и незашифрованными данными, что снижает вероятность подделки данных, что может быть возможным из-за визуального сравнения зашифрованных и незашифрованных данных.

В любом из вышеупомянутых аспектов или вариантов осуществления передачу зашифрованных данных и/или извлечение ключа можно осуществлять с помощью защищенного канала связи.

Каждый из вышеупомянутых аспектов или вариантов осуществления может быть объединен с каждым из других аспектов или вариантов осуществления, где это применимо.

Краткое описание графических материалов

С целью лучшего понимания настоящего изобретения, чтобы показать, как его можно осуществить, ссылка будет сделана только в качестве примера на следующие графические материалы, на которых:

на фиг. 1 показан способ генерирования сертификата безопасности; и

на фиг. 2 показан способ установления подлинности сертификата безопасности.

Подробное описание

Следующее описание подробно иллюстрирует типичный вариант осуществления раскрытого изобретения. Специалистам в данной области техники будет понятно, что существуют многочисленные варианты и модификации настоящего изобретения, которые охватываются объемом прилагаемой формулы изобретения. Соответственно, описание конкретного типичного варианта осуществления не должно рассматриваться как ограничивающее объем настоящего изобретения.

В последующем описании термин "доступ" является широким термином и, когда он относится к "разрешению доступа к открытому или личному ключу расшифрования", он охватывает оба варианта: (1) передачу зашифрованных данных в удаленный блок установления подлинности, а затем направление запроса на удаленный блок установления подлинности для расшифрования данных с помощью ключа расшифрования; и (2) извлечение ключа расшифрования для осуществления локального расшифрования.

В последующем описании раскрыты конкретные способы шифрования данных с помощью криптографии с открытым ключом.

В криптографии с открытым ключом используются пары ключей: открытый ключ, который может быть широкодоступным, и личный ключ, связанный с открытым ключом, причем этот личный ключ известен только владельцу личного ключа. Открытый ключ и личный ключ могут быть связаны таким образом, чтобы обеспечить шифрование и/или расшифрование данных с помощью соответствующих ключей, но там, где трудно или невозможно вычислить личный ключ, только из информации, связанной с открытым ключом. Например, открытый и личный ключи могут быть факторами произведения двух больших простых чисел. Путем вычислений очень сложно определить ассоциированный фактор произведения больших простых чисел, зная только один фактор и не зная простых чисел.

С помощью связанных открытого и личного ключей могут быть достигнуты две разные функции. Во-первых, данные могут быть зашифрованы с помощью личного ключа, при этом затем данные расшифровываются с помощью открытого ключа. Этот процесс позволяет установить подлинность того, что

данные были зашифрованы владельцем личного ключа. Если зашифрованные данные, следовательно, можно успешно расшифровать с помощью открытого ключа, то зашифрованные данные, следовательно, должны быть зашифрованы владельцем личного ключа, и, следовательно, являются подлинными.

В качестве альтернативы, шифрование данных с помощью открытого ключа означает, что только участник со связанным личным ключом может расшифровать данные. Таким образом, данные остаются конфиденциальными для всех, кроме участника, имеющего доступ к правильному связанному личному ключу.

На фиг. 1 показан способ генерирования сертификата безопасности. Хотя конкретный сертификат безопасности, проиллюстрированный на фиг. 1, связан с въездной визой для паспорта, будет понятно, что такая же технология может быть использована для генерирования сертификатов безопасности для других объектов и документов.

С целью генерирования сертификата безопасности каждый уполномоченный пользователь (например, страна-участница) имеет центр сертификации подписи (SCA) 10, который генерирует личный ключ шифрования этого участника и связанный с ним открытый ключ 7 расшифрования. По соображениям безопасности SCA 10 каждой страны-участницы обычно надежно хранит личный ключ шифрования.

Как показано на фиг. 1, центр 10 сертификации подписи выдает открытый ключ 7 расшифрования в справочник (PKD) 1 открытых ключей расшифрования. Справочник (PKD) 1 открытых ключей расшифрования может быть базой данных, в которой хранятся открытые ключи каждого SCA вместе с другими данными. Например, PKD 1 может также хранить списки отзыва сертификатов и основные списки сертификатов SCA, что будет описано более подробно ниже.

При необходимости выдачи данных о конкретном человеке или изделии (например, паспорта 9 путешественника) с сертификатом безопасности (например, въездной визой), эти данные могут быть собраны официальным представителем 11 в незашифрованном виде. Для путешественника незашифрованные данные 100 могут включать информацию, касающуюся номера паспорта, даты въезда, времени въезда, места въезда, такого как название аэропорта и номер выхода, номера маршрутного полета, связанного с въездом, типа выданной визы, права на государственные пособия, максимально допустимой продолжительности пребывания, биометрических и биографических данных, связанных с паспортом и/или путешественником, других идентификационных характеристик путешественника, даты истечения срока действия паспорта, цели поездки, истории поездок, записей, сделанных в ходе собеседования с официальным представителем, дополнительных комментариев, представленных официальным представителем, информации об официальном сборе данных и/или другой информации. Официальный представитель 11 также может проверять и подтверждать другую информацию, касающуюся путешественника 9, на этом этапе, а результаты проверки и подтверждения могут составлять часть собранных незашифрованных данных 100.

Незашифрованные данные 100 могут затем быть введены в генератор 5 сертификатов безопасности. Генератор 5 сертификатов безопасности выполнен с возможностью шифрования собранных данных 100 с помощью соответствующего личного ключа 8 шифрования участника. Шифрование данных с помощью личного ключа 8 шифрования участника в цифровой форме "подписывает" данные, чтобы обозначить пункт происхождения данных. Генератор 5 сертификатов безопасности может иметь защищенную связь с SCA 10 для того, чтобы получить личный ключ 8 шифрования. Использование защищенного канала связи между генератором 5 сертификатов безопасности и SCA 10 позволяет легко обновлять личные и открытые ключи, при этом ключи хранятся централизованно. В качестве альтернативы, копия личного ключа шифрования может храниться в генераторе 5 сертификатов безопасности. Далее в качестве альтернативы, генератор сертификатов безопасности может формировать защищенную связь с PKD 1 и получать доступ к копии 9 личного ключа шифрования, хранящегося на PKD 1, для шифрования собранных данных 100.

Собранные незашифрованные данные 100 могут храниться в PKD 1, или альтернативной базе данных, или хранилище в зашифрованном или незашифрованном виде. Сохраненные собранные данные могут управляться уполномоченной третьей стороной. Сохраненные собранные данные могут быть разделены между странами-участницами или могут быть проанализированы по соображениям бизнеса или безопасности. Доступ к сохраненным собранным данным может отслеживаться и может быть предоставлен только уполномоченным пользователям.

При шифровании незашифрованных данных 100 генератором 5 сертификатов безопасности зашифрованные данные 200 затем включают в сертификат безопасности, подлежащий связыванию с защищаемым изделием. Например, зашифрованные данные могут быть распечатаны в виде штампа штрих-кода с помощью устройства 13 для печати штампов, а затем нанесены на въездную визу в паспорте путешественника 9. В качестве альтернативы, зашифрованные данные могут быть включены в цифровой форме в магнитную дорожку, а затем нанесены на въездную визу в паспорте путешественника 9.

В качестве дополнения или альтернативы, некоторые или все собранные незашифрованные данные 10 могут быть зашифрованы с помощью отдельного открытого ключа шифрования, сгенерированного SCA. Использование открытого ключа шифрования обеспечивает конфиденциальность некоторых из собранных данных. Такие данные не могут быть расшифрованы с помощью открытого ключа расшифрования. Вместо этого для расшифрования этих данных необходимо использовать личный ключ расшиф-

рования, связанный с открытым ключом шифрования. Уровни шифрования могут быть использованы для защиты и установления подлинности различных частей зашифрованных данных, например, для предоставления различным участникам доступа к различным частям зашифрованных данных.

Например, в случае штампа для визы информация в штампе для паспорта дипломата может быть зашифрована иначе, чем данные для штампа в паспорте обычного туриста.

Открытые ключи шифрования могут также храниться локально соответствующим SCA 10 или могут быть получены из PKD 1. В качестве альтернативы, открытые ключи шифрования могут храниться отдельно в справочнике PrKD 3 личных ключей, который является доступным так же, как и PKD1.

Любые из собранных данных 100 также могут быть загружены в базу данных основного списка, хранящуюся в PKD 1. Отдельный центр может проводить поиск и управлять этой базой данных основного списка.

Данные в этом основном списке могут быть разделены между участниками или могут быть проанализированы и разделены по конкретным запросам.

Установление подлинности сертификата безопасности будет теперь описано со ссылкой на фиг. 2.

Для установления подлинности сертификата безопасности, связанного с паспортом, другой официальный представитель может собирать зашифрованные данные с помощью блока 6 установления подлинности. Блок 6 установления подлинности может собирать зашифрованные данные 200 с помощью различных средств, как, например, считывание штрих-кода с помощью устройства для считывания штампов, захват изображения визуального изображения или части визуального изображения с помощью устройства для формирования изображения, извлечение зашифрованных данных из ИС памяти или магнитной дорожки, или другие методы. Блок установления подлинности может быть нелокальным для официального представителя. Например, официальный представитель может собирать зашифрованные данные 200 с помощью устройства для считывания штампов, и устройство для считывания штампов может быть выполнено с возможностью передачи зашифрованных данных 200 на удаленный блок 6 установления подлинности.

После сбора зашифрованных данных 200 или их приема на блоке 6 установления подлинности данных, блок 6 установления подлинности данных может определять происхождение личного ключа шифрования, используемого для шифрования зашифрованных данных 200. Это определение происхождения может быть выполнено на основании некоторых незашифрованных данных, связанных с "цифровой подписью" сертификата безопасности, таких как страна-эмитент въездной визы.

После определения происхождения личного ключа шифрования, блок 6 установления подлинности данных может запросить PKD 1 разрешить доступ к связанному открытому ключу 7 расшифрования. Как подробно описано ранее, доступ к связанному открытому ключу 7 расшифрования может включать извлечение открытого ключа 7 расшифрования для локального расшифрования или передачу зашифрованных данных 200 в PKD 1 для удаленного расшифрования зашифрованных данных 200. Эти два типа доступа теперь будут объяснены более подробно.

В одном варианте осуществления после приема запроса от блока 6 установления подлинности PKD 1 может установить защищенный канал связи между собой и блоком установления подлинности, чтобы безопасно передать открытый ключ 7 расшифрования в блок 6 установления подлинности. Затем блок 6 установления подлинности пытается расшифровать зашифрованные данные 200 с помощью извлеченного открытого ключа 7 расшифрования. Если расшифрование зашифрованных данных 200 является успешным, открытый ключ расшифрования должен был быть правильно связан с личным ключом 8 шифрования. Таким образом, подтверждается, что сертификат безопасности является подлинным, т.е. сертификат безопасности содержит данные, которые были зашифрованы с помощью ожидаемого правильного личного ключа шифрования. Блок 6 установления подлинности может указывать на успех или неудачу расшифрования, чтобы обеспечить указание на подлинность сертификата безопасности, который может быть перепроверен официальным представителем. Блок 6 установления подлинности также отображает незашифрованные данные 100 официальному представителю.

Если зашифрованные данные 200 были подделаны после шифрования, или если зашифрованные данные 200 сфальсифицированы, открытый ключ расшифрования, связанный с личным ключом 8 шифрования, используемым конкретной страной-эмитентом, не будет расшифровывать зашифрованные данные 200. Таким образом, целостность данных не может быть обеспечена и может быть сфальсифицирована или иным образом подделана. Любое изменение данных после шифрования делает недействительной цифровую подпись, так что расшифрование с помощью связанного открытого ключа расшифрования приведет к неразборчивому расшифрованному сообщению.

В другом варианте осуществления блок установления подлинности может безопасно передавать зашифрованные данные 200 в справочник 1 открытых ключей, и сам PKD 1 идентифицирует правильный открытый ключ расшифрования, чтобы использовать его для расшифрования зашифрованных данных с помощью незашифрованных данных, связанных с сертификатом безопасности, таких как страна-эмитент. Затем PKD 1 пытается расшифровать зашифрованные данные 200 с помощью выбранного открытого ключа расшифрования. После предпринятого расшифрования PKD 1 надежно передает расшифрованные данные 100 или указание на успех или неудачу предпринятого расшифрования в блок 6 установления

подлинности. Блок установления подлинности может затем указывать на успех или неудачу попытки расшифрования и отображать незашифрованные данные 100 официальному представителю, например, с помощью индикатора или специального программного обеспечения.

Сертификат безопасности, подлинность которого установлена, может быть использован для разрешения различных вопросов официальным представителем, связанных с путешественником.

В случаях, когда первый участник зашифровал все или часть данных для конфиденциальности (т.е. некоторые или все зашифрованные данные 200 были зашифрованы с помощью открытого ключа шифрования), блок установления подлинности может запросить PrKD 3 разрешить доступ к личному ключу расшифрования для расшифрования этих зашифрованных данных 200, так же, как запрашивает открытый ключ расшифрования. PrKD может отслеживать полномочия, связанные с различными блоками установления подлинности, чтобы определить, разрешен ли доступ блоку 6 установления подлинности к личному ключу расшифрования. PrKD может определить, разрешать или нет доступ к определенному личному ключу расшифрования на основании этого полномочия.

Если личный ключ становится скомпрометированным, т.е. становится общеизвестным, может быть выполнено обновление открытых и личных ключей. В этом случае устаревшие открытые и/или личные ключи могут быть представлены в списке отзыва сертификатов, хранящемся в PKD 1, и ключи могут быть перепроверены с этим списком для дополнительной защиты от фальсификаций.

Дальнейшие модификации будут очевидны для специалистов в данной области техники при рассмотрении раскрытого в данном документе описания. Следовательно, предполагается, что настоящее изобретение не ограничено конкретными вариантами осуществления, представленными в данном документе, а что оно охватывает все модификации и альтернативы, находящиеся в рамках сущности и объема прилагаемой формулы изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Защищаемое физическое изделие, содержащее сертификат безопасности, содержащий первые данные, представляющие собой общедоступные данные, которые были зашифрованы с помощью личного ключа шифрования, при этом зашифрованные общедоступные данные выполнены с возможностью расшифрования с помощью открытого ключа расшифрования, связанного с личным ключом шифрования, с целью установления подлинности сертификата безопасности, отличающееся тем, что сертификат безопасности дополнительно содержит вторые данные, представляющие собой конфиденциальные данные, разные части которых были зашифрованы с помощью разных открытых ключей шифрования, при этом разные части зашифрованных конфиденциальных данных выполнены с возможностью расшифрования с помощью разных личных ключей расшифрования, связанных с разными открытыми ключами шифрования, с целью предоставления доступа разным участникам к разным частям конфиденциальных данных, при этом каждые из зашифрованных первых и вторых данных нанесены на защищаемое изделие в виде визуального изображения или в цифровой форме на микропроцессорной БИС или магнитной дорожке, и при этом личный ключ шифрования и открытые ключи шифрования сохранены централизованно в отдельных справочниках с защищенным доступом.

2. Защищаемое изделие по п.1, отличающееся тем, что визуальное изображение представляет собой QR-код, штрих-код или изображение в оттенках серого.

3. Защищаемое изделие по любому из предыдущих пунктов, отличающееся тем, что сертификат безопасности образует часть въездной визы.

4. Система установления подлинности сертификата безопасности защищаемого физического изделия по любому из пп.1-3, содержащая

защищенный справочник открытых ключей расшифрования, выполненный с возможностью предоставления уполномоченному пользователю доступа к открытому ключу расшифрования, связанному с личным ключом шифрования, при этом зашифрованные общедоступные данные расшифровывают с помощью открытого ключа расшифрования, доступ к которому обеспечивается, связанного с личным ключом шифрования,

блок расшифрования конфиденциальных данных, выполненный с возможностью приема от уполномоченного пользователя зашифрованных конфиденциальных данных, разные части которых зашифрованы с помощью разных открытых ключей шифрования, и расшифрования принятых разных частей зашифрованных конфиденциальных данных с помощью разных личных ключей расшифрования, связанных с разными открытыми ключами шифрования, с целью предоставления доступа разным участникам к разным частям конфиденциальных данных, при этом личный ключ расшифрования хранится в защищенном справочнике личных ключей расшифрования, выполненном с возможностью предоставления уполномоченному пользователю доступа к личному ключу шифрования, связанному с открытым ключом шифрования.

5. Система по п.4, отличающаяся тем, что система выполнена с возможностью определения успешного или неуспешного расшифрования зашифрованных общедоступных данных с помощью открытого ключа расшифрования, доступ к которому обеспечивается.

6. Система по п.5, отличающаяся тем, что система выполнена с возможностью указания того, что сертификат безопасности является подлинным в случае успешного расшифрования зашифрованных общедоступных данных, и/или выполнен с возможностью указания того, что сертификат безопасности не является подлинным в случае неуспешного расшифрования сертификата безопасности.

7. Система по любому из пп.4-6, отличающаяся тем, что защищенный справочник открытых ключей расшифрования содержит базу данных, содержащую по меньшей мере один открытый ключ расшифрования.

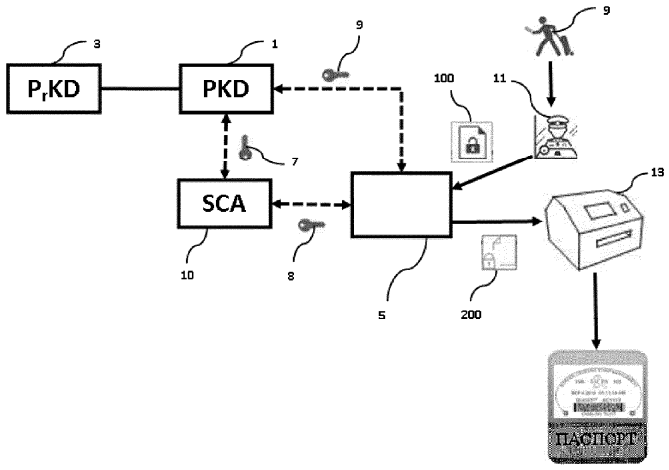
8. Способ установления подлинности сертификата безопасности защищаемого физического изделия по любому из пп.1-3, включающий

сбор зашифрованных первых и вторых данных, хранящихся в сертификате безопасности;

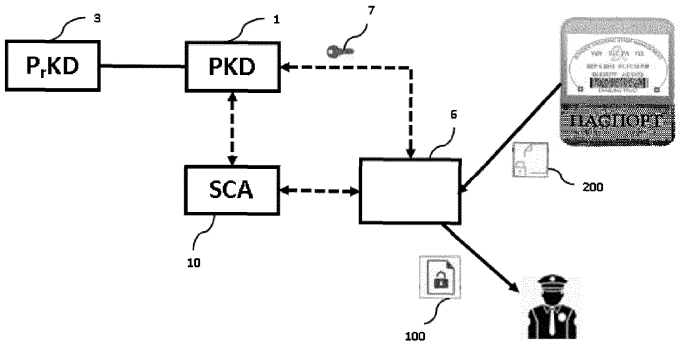
извлечение открытого ключа расшифрования зашифрованных общедоступных данных, связанного с личным ключом шифрования, из защищенного справочника открытых ключей расшифрования, и личных ключей расшифрования зашифрованных разных частей конфиденциальных данных, связанных с соответствующими открытыми ключами шифрования, из защищенного справочника личных ключей расшифрования;

расшифрование зашифрованных общедоступных данных с помощью открытого ключа расшифрования, связанного с личным ключом шифрования, и зашифрованных разных частей конфиденциальных данных с помощью разных личных ключей расшифрования, связанных с разными открытыми ключами шифрования, соответственно, с целью предоставления доступа разным участникам к разным частям конфиденциальных данных; и

определение успеха или неудачи предпринятого расшифрования зашифрованных первых и вторых данных, при этом успешное расшифрование зашифрованных первых и вторых данных устанавливает подлинность сертификата безопасности.



Фиг. 1



Фиг. 2