(19) Евразийское патентное ведомство

(11) 044726 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.09.27

(21) Номер заявки
201792129

(22) Дата подачи заявки
2016.09.20

(51) Int. Cl. ***H04L 9/08*** (2006.01)
H04L 9/32 (2006.01)
G06F 21/64 (2013.01)
G07D 7/00 (2016.01)
G06K 19/06 (2006.01)

(54) ПОВТОРНАЯ СЕРТИФИКАЦИЯ ДОКУМЕНТОВ

(31) **15186653.0; 15186695.1**
(32) **2015.09.24**
(33) **EP**
(43) **2018.08.31**
(86) **PCT/EP2016/072256**
(87) **WO 2017/050736 2017.03.30**

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

(72) Изобретатель:
Талверди Мехди (CA)

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

(56) WO-A1-2015058948
WO-A2-2006010019
US-A1-2005243199

(57) Изобретение относится к системам, единицам и способам сертификации и сертифицирования документов, таких как паспорта, лицензии, свидетельства об образовании и ценные изделия, такие как произведения искусства и т.п. Более конкретно, изобретение относится к повторной сертификации изделия/документа в смысле проверки и/или продления действия уже существующего сертификата/свидетельства.

044726 B1

044726 B1

Область техники

Настоящее изобретение относится к системам, единицам и способам сертификации изделий, таких как документы, паспорта, лицензии, свидетельства об образовании и ценные изделия, такие как произведения искусства и т.п. Более конкретно, настоящее изобретение относится к повторной сертификации изделия/документа в смысле проверки и/или продления действия уже существующего сертификата/свидетельства.

Уровень техники

В публикации US 7314162 раскрыт способ и система для оповещения об использовании идентификационного документа путем сохранения в базе данных и оповещения владельцу идентификационного документа случаев, при которых водительские права, паспорт или другие идентификационные документы государственного образца, принадлежащие этому лицу, представлены в форме идентификационных данных, тем самым упрощая раннее уведомление о хищении персональных данных.

Кроме того, в публикации US 7503488 раскрыт способ оценки риска фальсификации перед выдачей заявителю водительских прав на основе относительной вероятности фальсификации, связанной, по имеющимся сведениям, с конкретной комбинацией дополнительных идентификационных документов (например, свидетельством о рождении, паспортом, студенческим билетом и т.д.), представленных заявителем при его подаче на водительские права.

Желательной является повторная сертификация, корректировка и/или обновление официальных (т.е. государственного образца) карт или других свидетельств (например, свидетельства о рождении), документов об ученой степени и дипломов, и других свидетельств и т.д., особенно тех, которые не имеют специфического срока действия или продления. Кроме того, может быть желательной печать сертификационного знака на коммерческом документе в целях проверки подлинности.

Кроме того, желательным является проставление сертификационного знака на изделиях, таких как произведения (предметы) искусства и другие изделия, представляющие ценность ("ценные изделия"), без уменьшения ценности ценного изделия (например, без изменения внешнего вида произведения искусства). Кроме того, желательным является наиболее эффективное использование существующей инфраструктуры, в которой специальное(ые) считывающе-печатающее(ие) устройство(а) является(ются) коммерчески доступными для использования с целью печати на документах, таких как паспорта.

Целью настоящего изобретения является обеспечение системы и способа, удовлетворяющих данные потребности и устраняющих недостатки решений из предшествующего уровня техники.

Раскрытие сущности изобретения

Решение вышеуказанных проблем и недостатков известных решений обеспечивается за счет объекта изобретения в вариантах реализации настоящего изобретения.

Осуществление изобретения

Карты и свидетельства могут быть повторно выданы для внесения корректировок или для обновления их защитных признаков, а старые карты или свидетельства подвергаются утилизации. В некоторых картах и свидетельствах может быть отображен срок действия и может требоваться их периодическое продление (например, паспорта, водительские права и т.д.). Специальные считывающе-печатающие устройства являются коммерчески доступными для использования с целью печати повторно выдаваемых карт и свидетельств.

Вариант реализации настоящего изобретения содержит сервер специального назначения, который содержит один или более сервер приложений, модуль сбора данных, модуль аналитических операций, модуль сигнала тревоги, модуль сетевой защиты и защиты от несанкционированного доступа, и/или модуль защищенной связи. Указанный сервер приложений может обеспечивать частное облачное оперативное управление устройством считывания, принтером и/или интегрированным считывающе-печатающим устройством, вне зависимости от того, какое установлено, и другие административные функции, тем самым устраняя необходимость интегрирования считывающе-печатающего устройства в существующие сторонние электронные системы.

Модуль сбора данных собирает и хранит в базе данных все данные, разрешенные национальным законодательством (например, законами о неприкосновенности), которое связано с каждым случаем использования или выбранными случаями использования паспорта или другого ценного изделия, в том числе: (i) изображения ценного изделия, отсканированные устройством считывания или интегрированным считывающе-печатающим устройством, в том числе множество отсканированных изображений при множестве длин волн электромагнитного излучения, ультразвуковые отсканированные изображения (например, частей жидкости в ценных изделиях), рентгеновские отсканированные изображения, лазерные отсканированные изображения; (ii) идентификационные данные ценного изделия, такие как номер паспорта, изображение(я) или другие идентификационные данные паспорта и его содержания, в том числе места в паспорте с любыми предыдущими официальными штампами (например, визами) в данном конкретном паспорте; (iii) биометрические и биографические данные собственника или владельца ценного изделия, такие как отпечатки пальцев, отсканированные изображения глаза, отсканированные изображения лица, отсканированные изображения тела, данные инфракрасного термодатчика, аудиовизуальные записи (описаны далее ниже) и т.д.; (iv) дата, время и место каждого случая использования или выбран-

ных случаев использования ценного изделия, в том числе, например, при каждом сканировании паспорта на объекте сканирования паспорта, таком как объект пересечения государственной границы, транспортный узел, такой как в аэропортах, корабельные доки и железнодорожные станции, или в банках, гостиницах и т.д., или при каждом сканировании ценного изделия на объекте сканирования (т.е. объекте с устройством считывания или считывающе-печатающим устройством); (v) записи звука, изображения или видео взаимодействий между собственниками паспорта и сотрудниками на объекте сканирования паспорта или другие записи, относящиеся к использованию ценного изделия, связанные мультимедийные метаданные (например, количество записанных кадров, частотные сигнатуры голоса или другие записанные данные) и метрики, вычисленные из таких мультимедийных метаданных (которые, например, могут быть зашифрованы и использованы для дополнения существующих технологий по борьбе с несанкционированным доступом); (vi) видеоданные, показывающие лиц, использующих паспорт или другое ценное изделие; (vii) туристическая информация, связанная с собственником или владельцем ценного изделия, например, информация о прибытии и/или пункте назначения, такая как номер авиарейса, связанный с паспортом, сканируемым в аэропорту или на другом объекте сканирования паспорта; (viii) медицинская информация (например, состояние здоровья, подверженность инфекционным заболеваниям в прошлом, медицинские отчеты и т.д., связанные с собственником паспорта, лицом (например, беглецом), присутствующим на официальном объекте по сбору данных, или владельцем ценного изделия; (ix) соответствующая документация, такая как отсканированное изображение таможенных форм, отсканированные изображения вторичных документов идентификации, примечания, сделанные вовлеченными сотрудниками, и т.д.; (x) личность ответственного сотрудника, оперирующего с паспортом или другим ценным изделием, как, например, место, где сотрудник идентифицирован, например, по отпечатку пальца с помощью соответствующего оборудования, если оно установлено, или по другим биометрическим данным; и (xi) RFID-контент, причем в паспорте, этикетке или бирке (например, прикрепленной к объекту) или ценном изделии установлен RFID-чип и отсканирован на объекте сканирования (паспорта). База данных также может хранить информацию в отношении визы, въезде в страну, выезде из страны, таможенной форме, отметках о пересечении границы, штампы в паспорте или другие официальные штампы для использования при центральном (т.е. удаленном) управлении сканером, устройством считывания, принтером и/или интегрированным считывающе-печатающим устройством, вне зависимости от того, что может быть установлено.

Модуль аналитических операций анализирует данные, хранящиеся в базе данных, для определения, в режиме реального времени, потенциально неправомерного использования паспорта или другого ценного изделия, такого как когда собственником паспорта предпринимается попытка въезда в страну или выезда из нее без соответствующего въезда или выезда в прошлом, или когда собственник ценного изделия проявляет выразительные манеры поведения, такие как взволнованность. Кроме того, модуль аналитических операций выполняет мониторинг внешних баз 220 данных, например, Интерпола, Европола, национальных баз криминальных данных и других баз данных, для идентификации интересующих лиц, предпринимающих попытку использования паспорта на объекте сканирования паспорта или другого ценного изделия на объекте сканирования. Модуль аналитических операций выполняет мониторинг ограничений продолжительности пребывания для выдачи сигнала тревоги, если срок пребывания собственника паспорта превышен (например, не выехал из страны до даты истечения срока своей визы) или срок его пребывания недостаточен (например, не находился на протяжении достаточного времени в стране для получения права на специальный иммиграционный статус).

Модуль сигнала тревоги - модуль сигнала тревоги выдает сигнал тревоги ответственному сотруднику или другому официальному лицу, когда паспорт или другое ценное изделие, отсканированное сотрудником, было отмечен модулем аналитических операций как связанное с неправомерным использованием или вызывающее иное сомнение. Сигналы тревоги также могут быть сгенерированы при обнаружении несанкционированного доступа или другого физического повреждения сервера специального назначения или его модуля. Для этой цели может быть обеспечен датчик 26 (например, температуры, давления, вибрации, местоположения и т.д.), выполненный с возможностью обнаружения несанкционированного доступа. Сигналы тревоги могут быть выданы ответственному сотруднику или другому официальному лицу посредством модуля защищенной связи (который описан ниже) и/или по электронной почте, через текстовое и/или голосовое сообщение (например, на мобильный телефон) и т.д. Сигналы тревоги могут быть предоставлены любому официальному органу по всему миру в рамках закона в целях превентивной безопасности.

Модуль сетевой защиты и защиты от несанкционированного доступа защищает сервер специального назначения от внешних атак, исходящих из сети Интернет, а также выполняет мониторинг физического несанкционированного доступа, вмешательства или другого повреждения компонентов аппаратного обеспечения специального назначения.

Модуль защищенной связи обеспечивает шифрование связей между сервером специального назначения и электронными системами вовлеченных национальных правительств, их органов, коммерческих предприятий или других потребителей с использованием технологий шифрования в соответствии с предпочтениями потребителя и требованиями законодательства. Модуль защищенной связи упрощает

связи между сервером специального назначения и клиентскими компьютерами, в том числе конкретными устройствами считывания, принтерами и/или интегрированными считывающе-печатающими устройствами на объектах сканирования (паспорта). Модуль защищенной связи выполнен с возможностью связи с клиентскими компьютерами в пределах каждой страны по специфической для страны VPN (Virtual Private Network - виртуальная частная сеть). В некоторых вариантах реализации используется отдельная VPN для каждого объекта сканирования (паспорта). Специфические для страны связи упрощают обмен информацией между странами (в рамках законодательства обеих стран) посредством сервера специального назначения, несмотря на несовместимость между соответствующими относящимися к паспортам электронными системами различных стран. В более общем смысле, модуль защищенной связи упрощает обмен информацией между обслуживаемыми потребителями, несмотря на несовместимости между их соответствующими системами путем приема данных от первого обслуживаемого потребителя, согласно первому протоколу передачи данных, с последующей передачей данных от сервера специального назначения второму обслуживаемому потребителю, согласно второму протоколу передачи данных, причем первый и второй протоколы передачи данных не обязательно совместимы друг с другом.

Любое количество модулей сервера специального назначения может быть интегрировано в индивидуально настроенный блок черного ящика и любой предоставленный модуль может быть серийно произведен в качестве автономного блока, подходящего для интегрирования с существующими сторонними электронными системами.

Управление конкретным принтером или интегрированным считывающе-печатающим устройством может осуществляться непосредственно в качестве автономного блока или централизованно сервером специального назначения для печати отметок о повторной сертификации на официальных картах и свидетельствах, тем самым печатая корректирующую информацию и/или используя новые защитные признаки. В качестве примера, официальная карта или свидетельство, которое принимается в качестве подлинного, может быть отсканировано устройством для считывания или интегрированным считывающе-печатающим устройством, при этом результаты сканирования могут быть сохранены сервером специального назначения в его базе данных, сертификационный знак генерируется на основе выбранного шаблона и данных динамической области (которые необязательно содержат кодированные данные, полученные на основе результатов сканирования); и сертификационный знак печатают на официальной карте или свидетельстве.

В случае билетов на мероприятия или других приобретенных билетов для коммерческих услуг (например, билеты на транспорт), использование считывающе-печатающего устройства для проставления штампа или иной печати на билете для указания того, что он уже был использован, обеспечивает возможность использования защитных признаков (например, защитных признаков, включенных в краску, используемую для печати). Выполнение напечатанного штампа видимым свидетельствует о ненадлежащем повторном использовании таких билетов другими лицами.

В качестве еще одного примера, транспортная накладная, которую принимают в качестве подлинной, перед использованием отображает информацию, описывающую поставляемые товары (например, стандарт качества, количество и т.д.). Такая информация из транспортной накладной зашифровывается и генерируется сертификационный знак, содержащий зашифрованную информацию. Сертификационный знак печатают на транспортной накладной с помощью принтера или интегрированного считывающе-печатающего устройства перед поставкой. Как правило, в пункте назначения сравнивают транспортную накладную и товары, фактически содержащиеся в поставленном контейнере. Если найдено любое расхождение, зашифрованные данные в сертификационном знаке дешифруют и сравнивают с информацией, отображенной на транспортной накладной, для определения того, была ли изменена (т.е. к ней был получен несанкционированный доступ) транспортная накладная во время поставки. Дополнительно или в качестве альтернативы, дешифрованная информация может быть сравнена с полученными товарами.

В качестве еще одного примера, пачки наличных денег могут удерживаться вместе с помощью бумажной обертки с сертификацией, содержащей зашифрованное указание на денежную сумму в пачке, напечатанной на ней с помощью принтера или интегрированного считывающе-печатающего устройства перед транспортировкой, хранением и т.д.

В вариантах, множество сертификационных знаков могут быть напечатаны во множестве мест, которые могут быть случайными местами или могут быть выбраны человеком, и т.д.

В качестве необязательного этапа, изображение ценного изделия, имеющее сертификационный(е) знак(и), нанесенные на него, могут быть взяты (например, внутренней камерой считывающе-печатающего устройства) и затем сохранены сервером специального назначения для последующего использования при определении того, имел ли место несанкционированный доступ к сертификационному(ым) знаку(ам). В качестве примера, в котором множество сертификационных знаков расположены в случайно выбранных местах (например, в пределах конкретных границ), далее могут быть проверены относительные или абсолютные места сертификационных знака(ов). В варианте, объект, имеющий сертификационный знак(и), нанесенный на него, сканируют устройством считывания или интегрированным считывающе-печатающим устройством, и результаты сканирования сохраняются сервером специального назначения для последующей проверки подлинности ценного изделия и его сертификационных зна-

ка(ов).

В соответствии с другим вариантом реализации настоящего изобретения, предусмотрены модификации механических элементов, так что считывающе-печатающее устройство может быть выполнено с возможностью поддержки печати на объектах различных форм и размеров. Например, специальное устройство считывания/принтер может быть портативным переносным блоком для сканирования объектов различных форм и размеров.

В соответствии с вариантами реализации способа работы по настоящему изобретению, ценное изделие, которое принято в качестве подлинного, необязательно сканируют и отсканированные данные сохраняются сервером специального назначения; генерируют сертификационный знак на основе выбранного шаблона и данных динамической области (которые необязательно содержат кодированные данные, полученные на основе результатов сканирования); и сертификационный знак печатают на ценном изделии с помощью непроникающей, непоглощающей краски, которая видима только под действием специального электромагнитного излучения (например, ультрафиолетового света).

В вариантах, множество сертификационных знаков могут быть напечатаны во множестве мест, которые могут представлять собой случайные места или могут быть выбраны человеком, и т.д. В качестве примера, сертификационные знаки могут быть использованы с задней стороны картины на спае между задней стороной полотна и рамой. Такие сертификационные знаки на задней стороне, например, не должны быть невидимыми.

В варианте, отсканированное изображение ценного изделия, имеющего сертификационный(е) знак(и), нанесенные на него, может быть взято устройством считывания или интегрированным считывающе-печатающим устройством в выбранных длинах волн электромагнитного излучения и затем сохранено сервером специального назначения для последующего использования при определении того, имел ли место несанкционированный доступ к сертификационному(ым) знаку(ам). В качестве примера, когда множество сертификационных знаков расположено в случайно выбранных местах (в пределах конкретных границ), далее могут быть проверены относительные или абсолютные места сертификационного(ых) знака(ов).

Несмотря на то, что были описаны подробные варианты реализации, они служат лишь для обеспечения улучшенного понимания настоящего изобретения, определенного независимыми пунктами формулы изобретения, и их не следует рассматривать в качестве ограничения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Система для повторной сертификации ценного изделия, содержащая считывающе-печатающее устройство для повторной сертификации ценного изделия, принятого в качестве подлинного, и сервер специального назначения, содержащий модуль сбора данных, при этом указанное считывающе-печатающее устройство управляется сервером специального назначения, при этом система выполнена с возможностью: сканирования считывающе-печатающим устройством указанного ценного изделия;

сохранения сервером специального назначения в электронной базе данных модуля сбора данных результата сканирования указанного ценного изделия, выполненного считывающе-печатающим устройством;

генерирования по меньшей мере одного сертификационного знака, содержащего кодированные данные, полученные на основе результата сканирования указанного ценного изделия, сохраненного в электронной базе данных;

печати считывающе-печатающим устройством сгенерированного по меньшей мере одного сертификационного знака на указанном ценном изделии,

отличающаяся тем, что считывающе-печатающее устройство дополнительно выполнено с возможностью печати множества сгенерированных сертификационных знаков с использованием непроникающей, непоглощающей краски, которая видима только под действием специального электромагнитного излучения, во множестве мест на указанном ценном изделии и сканирования указанного ценного изделия, на котором напечатаны сгенерированные сертификационные знаки во множестве мест, при выбранных длинах волн специального электромагнитного излучения, и сервер специального назначения выполнен с возможностью сохранения в электронной базе данных отсканированного изображения указанного ценного изделия, на котором напечатаны сгенерированные сертификационные знаки во множестве мест, с возможностью последующей проверки сервером специального назначения соответствующего относительного или абсолютного места по меньшей мере одного из сгенерированных сертификационных знаков, напечатанных во множестве мест на указанном ценном изделии,

сервер специального назначения дополнительно содержит модуль аналитических операций, выполненный с возможностью определения, в режиме реального времени, неправомерного использования указанного ценного изделия путем мониторинга баз криминальных данных для идентификации интересующих лиц, предпринимающих попытку использования физического ценного изделия.

2. Система по п.1, в которой считывающе-печатающее устройство дополнительно выполнено с возможностью печати на документе, в том числе любом из паспорта, лицензии, свидетельства об образова-

нии и карты.

3. Система по любому из пп.1, 2, в которой считывающе-печатающее устройство дополнительно выполнено с возможностью печати на объектах различных форм и размеров.

4. Система по п.1, в которой специальное электромагнитное излучение представляет собой ультрафиолетовый свет.

5. Система по п.1, в которой множество мест представляет собой места, выбранные случайным образом, или места, выбранные человеком.

6. Система по п.1, в которой сервер специального назначения дополнительно содержит одно или более из сервера приложений, модуля сигнала тревоги, модуля сетевой защиты и защиты от несанкционированного доступа, и/или модуля защищенной связи.

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2