(19) Евразийское патентное ведомство

(21) 201791719 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2017.12.29

(22) Дата подачи заявки
2016.01.29

(51) Int. Cl. ***G05B 19/418*** (2006.01)
G06F 9/445 (2006.01)
G06F 21/30 (2013.01)

(54) БЕЗОПАСНАЯ ИДЕНТИФИКАЦИЯ И ВЕРИФИКАЦИЯ ПРОДУКТА

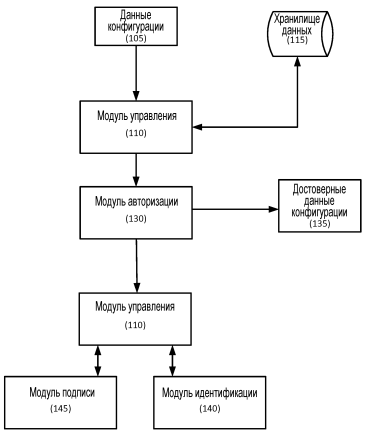
(31) **15153386.6**
(32) **2015.01.31**
(33) **EP**
(86) **PCT/EP2016/052008**
(87) **WO 2016/120487 2016.08.04**

(71) Заявитель:
ИНЕКСТО СА (CH)

(72) Изобретатель:
Борле-От Ален Лоран Робер, Фраде Эрван, Готье Янник Жорж Шарль (CH)

(74) Представитель:
Медведев В.Н. (RU)

(57) Предусматривается способ и система для аутентификации производства продуктов. Способ и система содержат определение, авторизованы ли данные конфигурации для серийного производства, и, если серийное производство авторизовано, генерирование жетона безопасности и ассоциирование жетона с данными конфигурации. Данные конфигурации подписываются цифровой подписью посредством генерирования цифровой подписи и ассоциирования цифровой подписи с данными конфигурации. Верифицируется цифровая подпись, ассоциированная с данными конфигурации с цифровой подписью. Продукты затем производятся в серийном производстве согласно данным конфигурации с цифровой подписью, и набор безопасных идентификаторов продуктов печатается на продуктах согласно данным конфигурации с цифровой подписью.



201791719 A1

201791719 A1

ОПИСАНИЕ ИЗОБРЕТЕНИЯ

2420-543927EA/019

БЕЗОПАСНАЯ ИДЕНТИФИКАЦИЯ И ВЕРИФИКАЦИЯ ПРОДУКТА

Настоящее изобретение относится в основном к способам для маркировки продуктов с помощью кодов безопасной идентификации и верификации этих кодов, и более конкретно к системам и способам для управления распространением инструкций безопасной конфигурации производства и генерирования безопасных идентификаторов продуктов.

Существующие способы для идентификации продуктов обычно предусматривают применение уникального идентификатора к продукту во время упаковки. Эти системы не масштабируются эффективно в организациях, имеющих многочисленные производственные базы, или на производственных линиях, способных упаковывать с очень большой скоростью. Дополнительно, существующие способы **идентификации** являются не достаточно безопасными, так как они не ассоциированы с инструкциями безопасной конфигурации производства и не несут дополнительной информации о продуктах, полезной для регулирующих органов и продавцов.

Существует необходимость улучшенного способа и устройства для безопасного управления и авторизации производства изготавливаемых товаров, также как и пометка изготавливаемых товаров с помощью безопасных идентификаторов продуктов, в частности которые могут быть использованы для верификации налогов, верификации объема производства и аутентификации изготовляемых товаров.

В одном аспекте данного раскрытия, предусматривается способ аутентификации производства продуктов, причем способ, включающий в себя хранение данных конфигурации в электронном виде для серийного производства, при этом данные конфигурации для серийного производства точно определяют параметры, используемые в производстве продуктов; определение, авторизованы ли данные конфигурации для серийного производства; если серийное производство авторизовано: генерирование жетона безопасности и ассоциирование жетона с данными конфигурации; и осуществление цифровой подписи данных конфигурации посредством генерирования

цифровой подписи и ассоциирования цифровой подписи с данными конфигурации; прием данных конфигурации с цифровой подписью и цифровой подписи в производственной машине; в производственной машине, верификацию цифровой подписи, ассоциированной с данными конфигурации с цифровой подписью; вычисление набора безопасных идентификаторов продуктов на основе данных конфигурации с цифровой подписью; произведение продуктов в серийном производстве согласно данным конфигурации с цифровой подписью; и печать набора безопасных идентификаторов продуктов на продуктах согласно данным конфигурации с цифровой подписью.

В нижеследующем описании вариантов осуществления, сделана ссылка на прилагаемые чертежи, которые формируют часть этой заявки, которые показывают способ иллюстрации конкретных вариантов осуществления заявленного объекта изобретения. Следует понимать, что могут быть использованы другие варианты осуществления, и что могут быть сделаны изменения или перемены, такие как структурные изменения. Такие варианты осуществления, изменения или перемены необязательно отступают от объема относительно предназначенного заявленного объекта изобретения. Хотя этапы ниже могут быть предоставлены в некотором порядке, в некоторых случаях порядок может быть изменен, так что некоторые вводы предоставляются в разное время или в разном порядке без изменения функции описанных систем и способов. Различные вычисления, которые описаны ниже, такие как вычисления в рамках процедур инициализации, генерирования и аутентификации кода, не должны выполняться в раскрытом порядке, и могут быть легко реализованы другие варианты осуществления, использующие альтернативные порядки вычислений. В дополнение к переупорядочиванию, вычисления могут также быть разложены на подвычисления с теми же результатами.

Как использовано в настоящем документе, объект может относиться к: i) физическому лицу, такому как потребитель продукта; ii) группе, такой как группа, имеющая общий интерес, такая как розничные торговцы; iii) вычислительному устройству; iv) вычислительному узлу в сетевой системе; v) месту хранения, такому как запоминающий блок, хранящий документ; vi) виртуальной

точке в сети, такой как представляющая бизнес-функцию с рамках бизнес-корпорации, и к подобному. Дополнительно, объект может представлять собой точку в рабочем процессе, таком как авторизация, которая может быть выполнена физическим лицом, ответственным за этот аспект рабочего процесса, или вычислительным устройством, которое предусматривает автоматическую обработку. Термин "объект" не предназначен для ограничения какого-либо из этих примеров и может распространяться на другие ситуации в соответствии с идеями, описанными в настоящем документе.

Теперь будут описаны варианты осуществления данного изобретения, только в качестве примера, со ссылкой на прилагаемые чертежи, на которых:

Фиг. 1 иллюстрирует примерный способ инициализации кода.

Фиг. 2 иллюстрирует примерный способ генерирования кода.

Фиг. 3 иллюстрирует примерный способ авторизации кода.

МОДУЛИ СИСТЕМЫ

Ниже описаны различные модули. Любой из модулей может быть физически размещен совместно или размещен удаленно друг от друга. Дополнительно, любой из модулей может быть логически или физически объединен в единый модуль без отступления от объема данного изобретения.

Модуль управления

Со ссылкой на Фиг. 1, модуль управления (также известный как "дирижер") (110) может принять ввод от любого из других модулей или внешних источников и может предоставить инструкции другим модулям в системе на основе предварительно сконфигурированной программы и/или вводов оператора в нее. Также он может сгенерировать панель сводных данных о статусе системы.

Ввод в модуль управления может включать в себя любые или все данные (105) конфигурации. Подаваемые данные конфигурации могут указывать любой или все из параметров, включающих в себя, но не ограниченных ими, машину для производства, линию производства, завод, продукт, который должен быть произведен, и объем продукта. Данные конфигурации могут указывать, какие товары (например, продукты) должны бить помечены с помощью

безопасных идентификаторов, и как эти товары могут быть произведены. Данные конфигурации могут указывать диапазон продуктов, такой как начальный и конечный идентификаторы продуктов. В некоторых вариантах осуществления, диапазоном может быть набор идентификаторов продуктов. Данные конфигурации могут быть предоставлены оператором системы или быть сгенерированы динамически или автоматически. Данные конфигурации могут включать в себя дополнительно исполняемые инструкции или интерпретируемый алгоритм. Данные конфигурации могут быть основаны на вводе оператора или выводе исполнительной системы изготовления, или другой централизованной системы для подачи инструкций, как и что производить.

Модуль (110) управления может передавать данные конфигурации любому модулю, в том числе, но не ограничиваясь этим, модулю (130) авторизации, модулю (140) идентификации и модулю (145) подписи.

Модуль управления может запросить авторизацию из модуля авторизации для исполнения производственной операции. Этот процесс предусматривает передачу запроса (включающего в себя некоторые или все данные конфигурации) модулю авторизации и прием подписанных или зашифрованных данных конфигурации. В некоторых вариантах осуществления, модуль авторизации может вернуть данные конфигурации модулю управления, включающие в себя цифровую подпись, примененную к этим данным конфигурации. Модуль авторизации определяет, авторизовать ли запрос из модуля управления на основе данных, которые он принимает. В дополнение, информация, возвращенная модулем авторизации, включенным в данные конфигурации, может быть использована для связывания кодов, сгенерированных с помощью предоставленной авторизации. Так как данные подписаны модулем авторизации, система может быть предохранена от модификации данных конфигурации. В качестве не ограничивающего примера, модификацией запроса на производство одной марки вместо другой можно управлять, позволять, или отклонять.

Авторизации, принятые из модуля авторизации, могут также быть переданы модулю верификации, так что запросы верификации

могут быть последовательно обработаны в отношении этих авторизаций. Данные, переданные модулю верификации, могут включать в себя безопасный идентификатор, также как и любые данные конфигурации. В некоторых примерах, данные конфигурации, отправленные модулю авторизации, могут включать в себя информацию о диапазоне продуктов.

Подписанными или достоверными данными конфигурации могут быть некоторые или все из набора входных параметров модуля управления, верифицированных и проверенных на достоверность модулем авторизации, которые действуют во время производства. Жетоном безопасности может быть вывод из модуля авторизации и/или входной параметр модуля управления. Жетон безопасности может быть доказательством, что идентификатор продукта соответствует достоверным данным конфигурации и вследствие этого авторизованному производству. Жетоном безопасности может быть ввод в модуль подписи для генерирования подписи для единого идентификатора продукта, или подпись единого идентификатора продукта, или сам идентификатор продукта, или диапазон продуктов или идентификаторы продуктов. Жетон безопасности может быть уникальным кодом, случайным кодом, или псевдослучайным кодом. Жетон безопасности может быть числовым, или буквенным, или комбинацией числовых и буквенных символов.

Модуль авторизации

Модуль авторизации функционирует для проверки достоверности запросов авторизации, чтобы предпринять действие в системе идентификации. В некоторых вариантах осуществления, он может функционировать как менеджер лицензий.

Модуль авторизации может принять данные конфигурации. Модуль авторизации может также принять информацию диапазона и/или алгоритма. В некоторых вариантах осуществления, модуль авторизации может принять входные данные конфигурации из модуля управления. Выходной диапазон может опционально идентифицировать диапазон продуктов, машины, заводы, диапазоны, или объемы продуктов, которые авторизованы. Вывод может также включать в себя информацию диапазона и/или включать в себя алгоритм, который содержит набор исполняемых или интерпретируемых

инструкций, который может быть использован для генерирования жетона безопасности. Модуль авторизации может быть централизован на уровне завода или быть децентрализован на каждой производственной линии, или их комбинации.

Модуль авторизации может хранить и/или сгенерировать один или более ключей шифрования. В некоторых вариантах осуществления, ключ, хранимый модулем авторизации, может быть **закрытым/открытым** ключом шифрования согласно инфраструктуре открытых ключей (PKI). В некоторых вариантах осуществления, модуль авторизации хранит только копию открытого ключа. В других вариантах осуществления, модуль авторизации распространяется среди нескольких экземпляров, которые реплицируют ключи между ними. В случае PKI, модуль авторизации может вывести подписанные данные конфигурации. В некоторых вариантах осуществления, модуль авторизации может зашифровать данные конфигурации и/или подписать выводимые данные конфигурации.

В некоторых вариантах осуществления, система сконфигурирована так, чтобы только модуль авторизации мог считать безопасные входные параметры модуля управления, требуемые для генерирования жетона безопасности. В некоторых вариантах осуществления, ключ предоставляется модулю авторизации из другого источника.

Модуль авторизации может быть осуществлен как аппаратный модуль безопасности (HSM), или другой тип физического вычислительного устройства, который защищает и управляет цифровыми ключами для строгой аутентификации и предоставляет криптообработку. Функциональность модуля авторизации может быть осуществлена посредством компьютера со встроенной платой с ключом шифрования или открытым PKI-ключом. Модуль снабжен функциональными возможностями, такими чтобы попытки доступа к данным приводили к воспроизведению их нечитаемыми или без возможности доступа.

Если вводом в модуль авторизации является диапазон и алгоритм, модуль авторизации может вывести идентификационную информацию в диапазоне авторизации и жетон безопасности идентификатора. Например, выходной идентификационной информацией

может быть диапазон 0-1000 с жетоном безопасности для каждого товара в диапазоне.

Модуль авторизации может сгенерировать ключ из любого параметра, используемого в модуле управления. В некоторых вариантах осуществления, модуль авторизации может сгенерировать или получить ключ исходя из существующего ключа из любого параметра, используемого в модуле управления, так чтобы только конкретный модуль авторизации мог использовать этот ключ. Оборудование и программное обеспечение, реализующие этот способ с открытым ключом, могут быть осуществлены в асимметричной криптосистеме.

Выводом модуля авторизации может быть информация, такая как данные конфигурации и, опционально, один или более жетонов безопасности, с цифровой подписью, предоставленной модулем подписи. В качестве альтернативы, выводом модуля авторизации могут быть данные конфигурации, зашифрованные для ключа, удерживаемого модулем авторизации. Вывод модуля авторизации может быть предоставлен модулю управления.

Согласно одному варианту осуществления, способ аутентификации производства продуктов включает в себя хранение данных конфигурации в электронном виде для серийного производства, при этом данные конфигурации для серийного производства точно определяют параметры, используемые в производстве продуктов; определение, авторизованы ли данные конфигурации для серийного производства; если серийное производство авторизовано: генерирование жетона безопасности и ассоциирование жетона с данными конфигурации; и осуществление цифровой подписи данных конфигурации посредством генерирования цифровой подписи и ассоциирования цифровой подписи с данными конфигурации; прием данных конфигурации с цифровой подписью и цифровой подписи в производственной машине; в производственной машине, верификацию цифровой подписи, ассоциированной с данными конфигурации с цифровой подписью; вычисление набора безопасных идентификаторов продуктов на основе данных конфигурации с цифровой подписью; произведение продуктов в серийном производстве согласно данным конфигурации с цифровой подписью; и

печать набора безопасных идентификаторов продуктов на продуктах согласно данным конфигурации с цифровой подписью.

В дополнительных вариантах осуществления, данные конфигурации представляют собой диапазон продуктов, которые должны быть произведены. В дополнительных вариантах осуществления данные конфигурации представляет собой диапазон продуктов, машины, заводы, диапазоны или объемы продуктов, которые авторизованы. Дополнительные варианты осуществления включают в себя прием запроса верификации, причем запрос, содержащий идентификатор продукта и определение, авторизованы ли данные конфигурации для серийного производства, посредством ссылки на менеджер лицензий. Дополнительные варианты осуществления включают в себя генерирование жетона безопасности для диапазона продуктов; и ассоциирование жетона безопасности с диапазоном продуктов.

Модуль подписи

Модуль подписи может принять данные конфигурации, ключ авторизации, жетон безопасности или любую их комбинацию, также как и уникальный идентификатор продукта, сгенерированный модулем идентификации. В некоторых вариантах осуществления, модуль подписи может принять, в дополнение, одну или более характеристик, свойственных машине и/или продукту, и/или характеристик единицы продукта. Модуль подписи может создать цифровую подпись на основе любого или все этих вводов, обычно называемых здесь данными конфигурации.

Чтобы сгенерировать цифровую подпись, в некоторых вариантах осуществления, модуль подписи может сначала сгенерировать дайджест или другое представление данных конфигурации. В некоторых вариантах осуществления, дайджест может быть сгенерирован посредством вычисления криптографического хэш-значения для данных конфигурации согласно алгоритму цифровой подписи, предоставляемому модулем подписи, исполняющим алгоритм цифровой подписи. В качестве не ограничивающих примеров, хэш может быть вычислен согласно функциям MD5, SHA-1, SHA-2, SHA-3/Keccak. Дайджест может быть затем зашифрован с использованием открытого ключа, полученного модулем подписи, чтобы

сгенерировать цифровую подпись.

В некоторых вариантах осуществления, цифровая подпись может использовать технологию инфраструктуры открытых ключей (PKI) для установления аутентичности данных конфигурации. PKI-системы используют сертификаты и ключи для идентификации объектов, частных лиц или организаций. Модуль аутентификации использует закрытый ключ для подписи данных конфигурации и ассоциирует данные конфигурации с сертификатом, включающим в себя открытый ключ, используемый модулем аутентификации.

Модуль получателя использует открытый ключ для верификации цифровой подписи и, тем самым, аутентичности подписанных данных конфигурации. Поддерживающие технологии могут быть использованы для установления других неопровержимых признаков, таких как время подписи и статус ключей для подписи. Открытый ключ может быть предоставлен непосредственно объекту получателя, или посредством публикации в онлайн-репозитории или директории.

Модуль идентификации

Модуль идентификации может принять данные конфигурации и сгенерировать идентификаторы для товаров, которые должны быть помечены. Модуль идентификации может принять цифровую подпись, сгенерированную модулем подписи, которая будет объединена с уникальным идентификатором, чтобы сгенерировать составной уникальный идентификатор.

Идентификаторы могут включать в себя дату и/или время производства продукта, который должен быть помечен, и цифровую подпись, принятую из модуля подписи, или быть на них основаны. В некоторых вариантах осуществления, сгенерированные безопасные идентификаторы могут быть уникальными или по существу уникальными. В некоторых вариантах осуществления, безопасными идентификаторами может быть жетон безопасности.

В случае диапазонов, модуль идентификации может сгенерировать идентификатор диапазона и набор идентификаторов в пределах сгенерированного диапазона.

Созданные идентификаторы могут быть выведены в модуль управления печатью для прямой печати на продукте или могут быть введены для дополнительной обработки, чтобы сгенерировать другой

код, который печатается на упаковке продукта.

Модуль верификации

Со ссылкой на Фиг. 3, модуль (150) верификации может принять верифицированные данные конфигурации и, на основе этих достоверных данных конфигурации, проверить достоверность запроса авторизации (305) для завода, машины, продукта или сообщенного объема продукта. Вводы в модуль верификации могут включать в себя любые или все верифицированные данные конфигурации, вывод из модуля подписи, идентификаторы, жетоны безопасности и/или информацию диапазона. Модуль верификации может сгенерировать информацию для модуля авторизации с этими параметрами, для того, чтобы верифицировать/проверить достоверность идентификатора продукта.

Модуль верификации может сгенерировать дешифрование (320) запроса, который включает в себя один или более идентификаторов или диапазонов идентификаторов (315) и данные (310) подписи, включающие в себя один или более жетонов безопасности.

Если жетон безопасности вводится в модуль верификации, модуль верификации может вернуть информацию, относящуюся к авторизации, данным конфигурации, и/или диапазонам. Если для диапазона продуктов используется единый жетон безопасности, жетон безопасности может быть предоставлен модулю верификации для верификации параметров, ассоциированных с диапазоном продуктов, а не с отдельными продуктами. Этот вариант осуществления может быть в частности полезным в контексте регулирования экспорта.

Системные процессы

Инициализация идентификационного кода

Инициализация идентификационного кода может быть выполнена для проверки достоверности авторизации и параметров. В некоторых вариантах осуществления, по причинам производительности, это может быть выполнено один раз в начале производства. Со ссылкой на Фиг. 1, модуль (110) управления может осуществить доступ к хранилищу (115) данных для дополнительных параметров, или дополнительные параметры могут быть предоставлены модулю. Параметры и данные конфигурации, раз подписанные модулем (130)

авторизации, формируют достоверные данные (135) конфигурации. Модуль управления принимает верифицированные данные конфигурации, которые описаны выше, в ответ на его запрос модулю (130) авторизации.

Авторизация может быть авторизацией для произведения продукта, или пометки продукта с некоторым ID, или того и другого. Данные конфигурации и дополнительные параметры передаются модулю авторизации и используются модулем авторизации, чтобы сгенерировать жетон безопасности. Модуль авторизации может подписать данные конфигурации и дополнительные параметры, формируя подписанные данные конфигурации. Как рассмотрено выше, данные конфигурации могут точно определить некоторое серийное производство или другие продукты и активности. Модуль авторизации может сгенерировать блок авторизации, включающий в себя ключ, авторизованные идентификаторы и жетон безопасности. В некоторых вариантах осуществления, их ключ может быть сгенерирован модулем авторизации, или может быть ему предоставлен. Модуль авторизации может передавать блок авторизации модулю управления. Модуль управления может передавать модулю (145) подписи достоверные данные конфигурации и другую информацию, такую как список идентификаторов, диапазон идентификаторов и/или один или более жетонов безопасности. Модуль подписи может подписать данные и отправить подписанные данные и подпись модулю управления. Модуль (140) идентификации может затем принять из модуля управления блок инициализации, включающий в себя идентификаторы и/или диапазоны идентификаторов для продуктов.

Один вариант осуществления данного изобретения включает в себя способ инициализации процесса для безопасного управления производственной базой, содержащий: прием в электронном виде данных конфигурации из электронного хранилища данных; хранение данных конфигурации в электронном виде для серийного производства, при этом данные конфигурации для серийного производства точно определяют параметры, используемые в производстве продуктов; передачу данных конфигурации модулю авторизации; в модуле авторизации: определение, авторизовано ли

серийное производство; генерирование достоверных данных конфигурации, содержащих ключ, представление множества авторизованных идентификаторов продуктов и жетон безопасности; передачу достоверных данных конфигурации модулю подписи; и в модуле подписи, осуществление подписи достоверных данных конфигурации.

Дополнительные варианты осуществления могут включать в себя определение, авторизованы ли данные конфигурации для серийного производства; если серийное производство авторизовано: генерирование жетона безопасности и ассоциирование жетона с данными конфигурации; и осуществление цифровой подписи данных конфигурации посредством генерирования цифровой подписи и ассоциирования цифровой подписи с данными конфигурации.

Дополнительные варианты осуществления могут включать в себя прием данных конфигурации с цифровой подписью и цифровой подписи в производственной машине; в производственной машине, верификацию цифровой подписи, ассоциированной с данными конфигурации с цифровой подписью; и вычисление набора безопасных идентификаторов продуктов на основе данных конфигурации с цифровой подписью.

Дополнительные варианты осуществления могут включать в себя произведение продуктов в серийном производстве согласно данным конфигурации с цифровой подписью; и печать набора безопасных идентификаторов продуктов на продуктах согласно данным конфигурации с цифровой подписью.

Дополнительные варианты осуществления могут включать в себя определение, авторизовано ли серийное производство, которое дополнительно содержит получение данных лицензирования из сервера лицензирования.

Генерирование идентификационного кода

Со ссылкой на Фиг. 2, процесс генерирования кода генерирует коды во время процесса производства. Процесс генерирования идентификационного кода может начаться с запроса модулю (140) идентификации на предмет идентификатора или диапазона идентификаторов, которые затем возвращаются модулю (110) управления. Идентификаторы затем отправляются модулю (145)

подписи, который подписывает идентификаторы и возвращает подписанные идентификаторы модулю управления. Модуль подписи может принять жетон безопасности. В некоторых вариантах осуществления, модулю подписи не требуется управление посредством внешних инструкций, и если какой-либо идентификационный код должен быть посчитан, код может быть привязан к единому жетону безопасности. Модулем подписи можно управлять посредством модуля авторизации. Модуль управления может затем отправить выходные данные элементу управления печатью в модуле (210) принтера. Выходные данные, отправленные элементу управления печатью, могут быть зашифрованы до передачи. Данные конфигурации, могут быть переданы модулю (150) верификации для обработки последующих запросов верификации.

Один вариант осуществления данного изобретения включает в себя способ генерирования кода для безопасной идентификации продуктов, произведенных на производственной базе, включающий в себя прием в электронном виде данных конфигурации из электронного хранилища данных; хранение данных конфигурации в электронном виде для серийного производства, при этом данные конфигурации для серийного производства точно определяют параметры, используемые в производстве продуктов; передачу данных конфигурации модулю авторизации; в модуле авторизации: определение, авторизовано ли серийное производство; генерирование достоверных данных конфигурации, содержащих ключ, представление множества авторизованных идентификаторов продуктов и жетон безопасности; передачу достоверных данных конфигурации модулю подписи; в модуле подписи, осуществление подписи достоверных данных конфигурации; в модуле идентификации, прием запроса идентификатора продукта и генерирование идентификатора продукта в ответ на запрос; передачу идентификатора продукта из модуля идентификации модулю подписи; осуществление цифровой подписи идентификатора продукта в модуле подписи; и передачу идентификатора продукта с цифровой подписью модулю принтера.

Дополнительные варианты осуществления могут включать в себя прием в электронном виде данных конфигурации из электронного хранилища данных; хранение данных конфигурации в электронном

виде для серийного производства, при этом данные конфигурации для серийного производства точно определяют параметры, используемые в производстве продуктов; передачу данных конфигурации модулю авторизации; в модуле авторизации: определение, авторизовано ли серийное производство; генерирование достоверных данных конфигурации, содержащих ключ, представление множества авторизованных идентификаторов продуктов и жетон безопасности; передачу достоверных данных конфигурации модулю подписи; в модуле подписи, осуществление подписи достоверных данных конфигурации.

В дополнительных вариантах осуществления запрос является запросом диапазона идентификаторов. Дополнительные варианты осуществления могут включать в себя определение, авторизованы ли данные конфигурации для серийного производства; если серийное производство авторизовано: генерирование жетона безопасности и ассоциирование жетона с данными конфигурации; и осуществление цифровой подписи данных конфигурации посредством генерирования цифровой подписи и ассоциирования цифровой подписи с данными конфигурации.

Верификация идентификационного кода

Модуль верификации может принять запрос верификации. Запрос может включать в себя один или более идентификационных кодов. модуль верификации может дешифровать или иначе прояснить принятый код идентификатора. Результирующая информация, которая была дешифрована, может включать в себя компонент подписи и идентификатор. Результирующий идентификатор может быть затем связан с первоначальными данными конфигурации, сохраненными ранее в связи с идентификатором. Связанные данные могут включать в себя другие идентификаторы в диапазоне, жетон безопасности и другую информацию, сохраненную применительно к производству продукта, несущего этот идентификационный код.

Некоторые варианты осуществления могут включать в себя дополнительную функциональность для обработки идентификаторов, которые предоставлены модулю верификации на основе стороны, запрашивающей верификацию кода. Разным сторонам могут быть предоставлены разные средства для осуществления доступа к модулю

верификации. Например, розничный торговец или продавец другой формы, может быть снабжен другим входом или каналом связи, чем потребитель. Розничному торговцу может также потребоваться аутентифицировать себя для модуля верификации.

В некоторых вариантах осуществления, система может быть сконфигурирована так, чтобы верификация посредством потребителя приводила к пометке идентификатора, как верифицированного. Система может быть дополнительно выполнена с возможностью хранения этих кодов, для которых верификация запрашивается потребителем. Любые последующие запросы верификации этих уже верифицированных кодов могут быть отклонены или обработаны иным образом по выбору.

Функции экспорта

Варианты осуществления данного изобретения могут быть применены в контексте экспорта кода для третьих сторон. Эти варианты осуществления могут включать в себя функцию экспорта, выполненную с возможностью генерирования отдельного кода для этой цели. Экспортированный код может быть сгенерирован посредством сбора одного или более идентификаторов продуктов и/или жетонов безопасности, и осуществления подписи этих идентификаторов и/или жетонов. Идентификаторы и/или жетоны могут быть собраны в любой точке в процессе производства. Подписанные идентификаторы и/или жетоны в виде экспортированных кодов могут быть предоставлены третьей стороне, которая может хранить их и выполнять верификацию достоверности идентификаторов и/или жетонов.

Архитектуры системы

Системы и способы, описанные в настоящем документе, могут быть реализованы в виде программного обеспечения или аппаратных средств, или любой их комбинации. Системы и способы, описанные в настоящем документе, могут быть реализованы с использованием одного или более вычислительных устройств, которые могут или не могут быть физически или логически отделены друг от друга. Дополнительно, различные аспекты способов, описанных в настоящем документе, могут быть объединены или совмещены в другие функции. В некоторых вариантах осуществления, проиллюстрированные

элементы системы могут быть объединены в единое аппаратное устройство или разделены на многочисленные аппаратные устройства. Если используются многочисленные аппаратные устройства, аппаратные устройства могут быть физически размещены вблизи или отдаленно друг от друга.

Способы могут быть реализованы в компьютерном программном продукте, доступном с используемого компьютером или компьютерно-читаемого носителя информации, который предоставляет программный код для использования компьютером ли совместно с ним, или системой исполнения инструкций. Используемым компьютером или компьютерно-читаемым носителем информации может быть любое устройство, которое может содержать или хранить программу для использования компьютером или совместно с ним, или системой исполнения инструкций, или устройством.

Система обработки данных, подходящая для хранения и/или исполнения соответствующего программного кода, может включать в себя по меньшей мере один процессор, соединенный напрямую или ненапрямую с компьютеризированным устройством хранения данных, таким как элементы памяти. Устройства (I/O) (включающие в себя, но не ограниченные этим, клавиатуры, дисплеи, указывающие устройства, и т.д.) могут быть соединены с системой. Сетевые адаптеры могут также быть соединены с системой для обеспечения системе обработки данных возможности соединения с другими системами обработки данных или удаленными принтерами или устройствами хранения посредством промежуточных частных или публичных сетей. Для обеспечения взаимодействия с пользователем, функциональные возможности могут быть реализованы на компьютере с устройством отображения, таким как CRT (с катодно-лучевой трубкой), LCD (жидкокристаллический дисплей), или другой тип монитора для отображения информации пользователю, и клавиатурой и устройством ввода, таким как мышь или шаровый манипулятор, посредством которого пользователь может предоставить ввод в компьютер.

Компьютерная программа может быть набором инструкций, который может быть использован, напрямую или ненапрямую, в компьютере. Системы и способы, описанные в настоящем документе,

могут быть реализованы с использованием языков программирования, таких как FlashTM, JAVATM, C++, C, C#, Visual BasicTM, JavaScriptTM, PHP, XML, HTML, и т.д., или комбинации языков программирования, включающих в себя компилируемые или интерпретируемые языки, и могут быть развернуты в любом виде, включающем в себя в качестве самостоятельной программы или в качестве модуля, компонент, стандартную подпрограмму или другой блок, подходящий для использования в вычислительном окружении. Программное обеспечение может включать в себя, но не ограничено этим, программно-аппаратные средства, резидентное программное обеспечение, микрокод и т.д. Протоколы, такие как SOAP/HTTP, могут быть использованы при реализации интерфейсов между модулями программирования. Компоненты и функциональность, описанные в настоящем документе, могут быть реализованы в любой настольной операционной системе, исполняющейся в виртуализированном или невиртуализированном окружении, с использованием любого языка программирования, подходящего для разработки программного обеспечения, в том числе, но не ограничиваясь этим, разные версии Microsoft WindowsTM, AppleTM MacTM, iOSTM, UnixTM/X-WindowsTM, LinuxTM, и т.д.

Подходящие процессоры для исполнения программы из инструкций включают в себя, но не ограничены этим, микропроцессоры общего и специального назначения, и одиночный процессор или один из многочисленных процессоров или ядер, для компьютера любого вида. Процессор может принимать и сохранять инструкции и данные из компьютеризированного устройства хранения данных, такого как постоянная память, оперативная память, и то и другое, или любая комбинация устройств хранения данных, описанных в настоящем документе. Процессор может включать в себя любую схему обработки или схему управления, функционирующую с возможностью управления операциями и эксплуатационными характеристиками электронного устройства.

Процессор может также включать в себя, одно или более устройств хранения данных для хранения данных, или быть оперативно соединенным для осуществления с ними связи. Такие устройства хранения данных могут включать в себя, в качестве не

ограничивающих примеров, магнитные диски (в том числе внутренние жесткие диски и съемные диски), магнито-оптические диски, оптические диски, постоянную память, оперативную память и/или flash-накопитель. Устройства хранения, подходящие для осуществления компьютерных программных инструкций и данных материальным образом, могут также включать в себя все виды энергонезависимой памяти, включающие в себя, например, полупроводниковые запоминающие устройства, такие как EPROM, EEPROM, и устройства flash-памяти; магнитные диски, такие как внутренние жесткие диски и съемные диски; магнито-оптические диски; и CD-ROM и DVD-ROM диски. Процессор и память могут быть дополнены ASIC (специализированными интегральными схемами), или включены в них.

Системы, модули и способы, описанные в настоящем документе, могут быть реализованы с использованием любой комбинации программных или аппаратных элементов. Системы, модули и способы, описанные в настоящем документе, могут быть реализованы с использованием одной или более виртуальных машин, функционирующих самостоятельно или совместно друг с другом. Любое применимое решение виртуализации может быть использовано для встраивания платформы физической вычислительной машины в виртуальную машину, которая исполняется под управлением программного обеспечения виртуализации, запущенного на аппаратной вычислительной платформе или хосте. Виртуальная машина может иметь как аппаратные средства виртуальной системы, так и программное обеспечение гостевой операционной системы.

Системы и способы, описанные в настоящем документе, могут быть реализованы в компьютерной системе, которая включает в себя серверный компонент, такой как сервер данных, или которая включает в себя компонент с программным обеспечением промежуточного уровня, такой как сервер приложений или Интернет-сервер, или которая включает в себя клиентский компонент, такой как клиентский компьютер, имеющий графический пользовательский интерфейс или Internet-браузер, или любую их комбинацию. Компоненты системы могут быть соединены посредством любого вида или среды передачи цифровых данных, такой как, сети связи.

Примеры сетей связи включают в себя, например, LAN, WAN и компьютеры и сети, которые формируют Интернет.

Один или более вариантов осуществления данного изобретения могут быть применены на практике с другими конфигурациями компьютерной системы, включая карманные устройства, микропроцессорные системы, микропроцессорную или программируемую потребительскую электронику, миникомпьютеры, мейнфреймы и т.д. Данное изобретение может быть также применено на практике в распределенных вычислительных окружениях, где задания выполняются устройствами удаленной обработки, которые сопряжены через сеть.

Хотя было описано одно или более вариантов осуществления данного изобретения, различные перемены, дополнения, перестановки и их эквиваленты включены в рамки объема данного изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ инициализации процесса для безопасного управления производственной базой, содержащий этапы, на которых:

принимают в электронном виде данные конфигурации из электронного хранилища данных;

хранят данные конфигурации в электронном виде для серийного производства, при этом данные конфигурации для серийного производства точно определяют параметры, используемые в производстве продуктов;

передают данные конфигурации модулю авторизации;

в модуле авторизации:

определяют, авторизовано ли серийное производство;

генерируют достоверные данные конфигурации, содержащие ключ, представление множества авторизованных идентификаторов продуктов и жетон безопасности;

передают достоверные данные конфигурации модулю подписи; и

в модуле подписи, осуществляют подпись достоверных данных конфигурации.

2. Способ по п. 1, дополнительно содержащий этапы, на которых:

определяют, авторизованы ли данные конфигурации для серийного производства;

если серийное производство авторизовано:

генерируют жетон безопасности и ассоциируют жетон с данными конфигурации; и

осуществляют цифровую подпись данных конфигурации посредством генерирования цифровой подписи и ассоциирования цифровой подписи с данными конфигурации.

3. Способ по одному или более предшествующим пунктам, дополнительно содержащий этапы, на которых:

принимают данные конфигурации с цифровой подписью и цифровую подпись в производственной машине;

в производственной машине, верифицируют цифровую подпись, ассоциированную с данными конфигурации с цифровой подписью; и

вычисляют набор безопасных идентификаторов продуктов на основе данных конфигурации с цифровой подписью.

4. Способ по одному или более предшествующим пунктам, дополнительно содержащий этапы, на которых:

производят продукты в серийном производстве согласно данным конфигурации с цифровой подписью; и

печатают набор безопасных идентификаторов продуктов на продуктах согласно данным конфигурации с цифровой подписью.

5. Способ по одному или более предшествующим пунктам, при этом определение, авторизовано ли серийное производство, дополнительно содержит этап, на котором получают данные лицензирования из сервера лицензирования.

6. Способ генерирования кода для безопасной идентификации продуктов, произведенных на производственной базе, содержащий этапы, на которых:

принимают в электронном виде данные конфигурации из электронного хранилища данных;

хранят данные конфигурации в электронном виде для серийного производства, при этом данные конфигурации для серийного производства точно определяют параметры, используемые в производстве продуктов;

передают данные конфигурации модулю авторизации;

в модуле авторизации:

определяют, авторизовано ли серийное производство;

генерируют достоверные данные конфигурации, содержащие ключ, представление множества авторизованных идентификаторов продуктов и жетон безопасности;

передают достоверные данные конфигурации модулю подписи;

в модуле подписи, осуществляют подпись достоверных данных конфигурации;

в модуле идентификации, принимают запрос идентификатора продукта и генерируют идентификатор продукта в ответ на запрос;

передают идентификатор продукта из модуля идентификации модулю подписи;

осуществляют цифровую подпись идентификатора продукта в модуле подписи; и

передают идентификатор продукта с цифровой подписью модулю принтера.

7. Способ по одному или более предшествующим пунктам, дополнительно содержащий этапы, на которых:

принимают в электронном виде данные конфигурации из электронного хранилища данных;

хранят данные конфигурации в электронном виде для серийного производства, при этом данные конфигурации для серийного производства точно определяют параметры, используемые в производстве продуктов;

передают данные конфигурации модулю авторизации;

в модуле авторизации:

определяют, авторизовано ли серийное производство;

генерируют достоверные данные конфигурации, содержащие ключ, представление множества авторизованных идентификаторов продуктов и жетон безопасности;

передают достоверные данные конфигурации модулю подписи;

в модуле подписи, осуществляют подпись достоверных данных конфигурации.

8. Способ по одному или более предшествующим пунктам, при этом запросом является запрос диапазона идентификаторов.

9. Способ по одному или более предшествующим пунктам, дополнительно содержащий этапы, на которых:

определяют, авторизованы ли данные конфигурации для серийного производства;

если серийное производство авторизовано:

генерируют жетон безопасности и ассоциируют жетон с данными конфигурации; и

осуществляют цифровую подпись данных конфигурации посредством генерирования цифровой подписи и ассоциирования цифровой подписи с данными конфигурации.

10. Способ аутентификации производства продуктов, содержащий этапы, на которых:

хранят данные конфигурации в электронном виде для серийного производства, при этом данные конфигурации для серийного производства точно определяют параметры, используемые в производстве продуктов;

определяют, авторизованы ли данные конфигурации для

серийного производства;

если серийное производство авторизовано:

генерируют жетон безопасности и ассоциируют жетон с данными конфигурации; и

осуществляют цифровую подпись данных конфигурации посредством генерирования цифровой подписи и ассоциирования цифровой подписи с данными конфигурации;

принимают данные конфигурации с цифровой подписью и цифровую подпись в производственной машине;

в производственной машине, верифицируют цифровую подпись, ассоциированную с данными конфигурации с цифровой подписью;

вычисляют набор безопасных идентификаторов продуктов на основе данных конфигурации с цифровой подписью;

производят продукты в серийном производстве согласно данным конфигурации с цифровой подписью; и

печатают набор безопасных идентификаторов продуктов на продуктах согласно данным конфигурации с цифровой подписью.

11. Способ по одному или более предшествующим пунктам, при этом данные конфигурации представляют собой диапазон продуктов, которые должны быть произведены.

12. Способ по одному или более предшествующим пунктам, при этом данные конфигурации представляют собой диапазон продуктов, машины, заводы, диапазоны или объемы продуктов, которые авторизованы.

13. Способ по одному или более предшествующим пунктам, дополнительно содержащий этап, на котором принимают запрос верификации, причем запрос, содержащий идентификатор продукта.

14. Способ по одному или более предшествующим пунктам, дополнительно содержащий этап, на котором определяют, авторизованы ли данные конфигурации для серийного производства, посредством ссылки на менеджер лицензий.

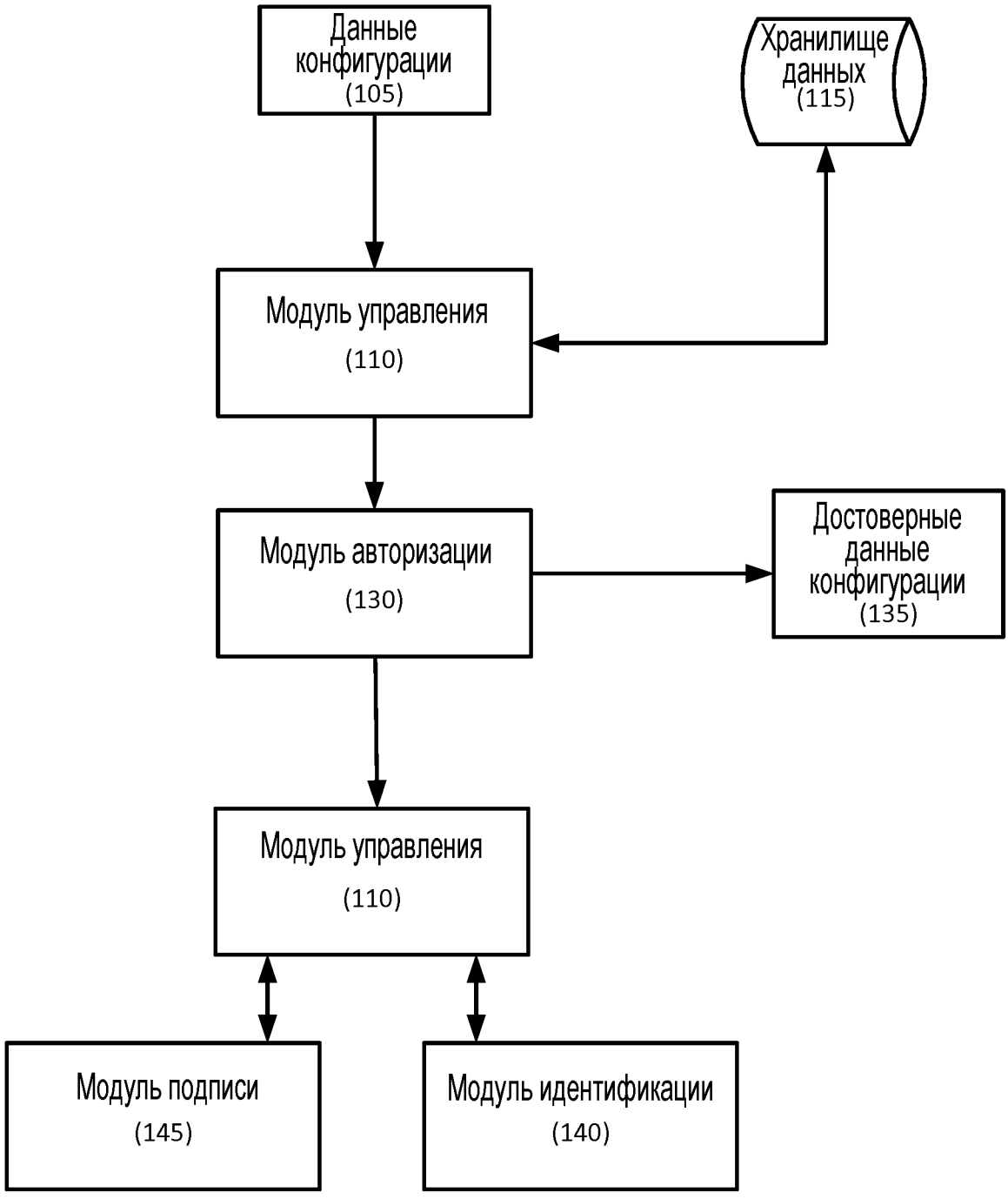
15. Способ по одному или более предшествующим пунктам, дополнительно содержащий этапы, на которых:

генерируют жетон безопасности для диапазона продуктов; и

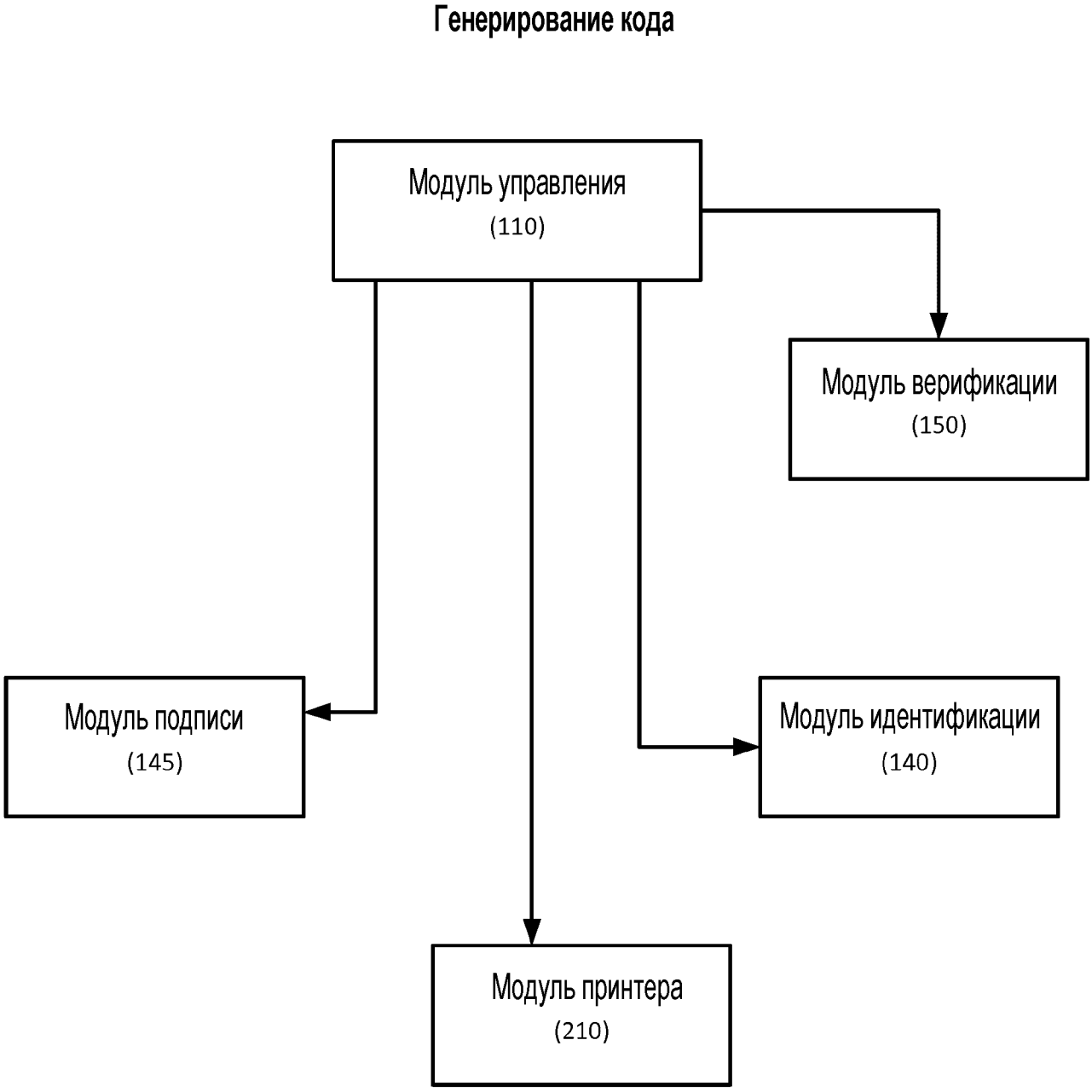
ассоциируют жетон безопасности с диапазоном продуктов.

По доверенности

ФИГ. 1


Инициализация кода
Данные конфигурации (105)
Хранилище данных (115)
Модуль управления (110)
Модуль авторизации (130)
Достоверные данные конфигурации (135)
Модуль управления (110)
Модуль подписи (145)
Модуль идентификации (140)

ФИГ. 2


Генерирование кода
Модуль управления
(110)
Модуль верификации
(150)
Модуль подписи
(145)
Модуль идентификации
(140)
Модуль принтера
(210)

Аутентификация кода

ФИГ. 3