(19) Евразийское патентное ведомство

(11) 040247 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.05.13

(21) Номер заявки
201990182

(22) Дата подачи заявки
2017.06.30

(51) Int. Cl. ***G06F 21/32*** (2013.01)
B42D 25/305 (2014.01)
B42D 25/313 (2014.01)
G06F 21/62 (2013.01)
G06K 19/07 (2006.01)
G06T 7/00 (2017.01)

(54) IC-КАРТА, ПОРТАТИВНОЕ ЭЛЕКТРОННОЕ УСТРОЙСТВО И СПОСОБ ОБРАБОТКИ ИНФОРМАЦИИ

(31) **2016-132496**
(32) **2016.07.04**
(33) **JP**
(43) **2019.06.28**
(86) **PCT/JP2017/024152**
(87) **WO 2018/008548 2018.01.11**

(71)(73) Заявитель и патентовладелец:
КАБУСИКИ КАЙСЯ ТОСИБА; ТОСИБА ИНФРАСТРАКЧЕ СИСТЕМЗ ЭНД СОЛЮШНЗ КОРПОРЕЙШН (JP)

(72) Изобретатель:
Окуно Томотака (JP)

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

(56) JP-A-200884044
JP-A-2006501583
JP-A-2012238126
JP-A-2009151528
JP-A-6364127

(57) В соответствии с вариантом осуществления IC-карта включает в себя модуль связи, модуль получения оценки верификации, модуль настройки, модуль обработки приема и модуль определения. Модуль связи передает и принимает данные к и от внешнего устройства. Модуль получения оценки верификации получает оценку верификации биометрической информации. Модуль настройки выбирает уровень безопасности, соответствующий оценке верификации, из множества уровней безопасности, каждый из которых указывает исполняемую команду, и устанавливает уровень безопасности, выбранный в качестве текущего уровня безопасности. Модуль обработки приема принимает команду посредством модуля связи. Модуль определения определяет, является ли команда исполняемой, на основе текущего уровня безопасности.

040247 B1

040247 B1

Область техники

Вариант осуществления изобретения относится к IC-карте, портативной электронной системе и способу обработки информации.

Уровень техники

Некоторые портативные электронные устройства, такие как IC-карты, имеют датчик отпечатка пальца. IC-карта, оснащенная датчиком отпечатка пальца, определяет, что аутентификация была успешна, если оценка (степень) верификации данных отпечатка пальца, зарегистрированных заранее, и данных отпечатка пальца, полученных от пользователя, превышает предопределенное пороговое значение.

Однако данные отпечатка пальца, полученные от пользователя, подвержены влиянию окружающей среды и т.п., и аутентификация может оказаться безуспешной, даже если пользователем является само данное лицо. Традиционно, когда оценка верификации не превышает предопределенного порогового значения, IC-карта имеет проблему, состоящую в том, что условие исполнения команды не удовлетворено, и ожидаемая операция не исполняется.

Документы уровня техники

Патентные документы.

Патентный документ 1 публикация № 2010-250475 японской патентной заявки.

Краткое описание сущности изобретения

Задача, решаемая изобретением.

Чтобы решить вышеуказанную задачу, обеспечены IC-карта, портативное электронное устройство и способ обработки информации, способный устанавливать исполняемые команды в соответствии с оценкой верификации.

Средства для решения задачи.

В соответствии с вариантом осуществления IC-карта оснащена модулем связи, модулем получения оценки верификации, модулем настройки, модулем обработки приема и модулем определения. Модуль связи передает/принимает данные к/от внешнего устройства. Модуль получения оценки верификации получает оценку верификации биометрической информации. Модуль настройки выбирает уровень безопасности, соответствующий оценке верификации, из множества уровней безопасности, причем каждый уровень показывает исполняемую команду и устанавливает уровень безопасности, выбранный в качестве текущего уровня безопасности. Модуль обработки приема принимает команду посредством модуля связи. Модуль определения определяет, является ли команда исполняемой на основе текущего уровня безопасности.

Краткое пояснение чертежей

Фиг. 1 является схематичным представлением, показывающим пример конфигурации системы обработки IC-карты, имеющей IC-карту и блок обработки IC-карты в соответствии с вариантом осуществления.

Фиг. 2 является блок-схемой, показывающей пример конфигурации IC-карты в соответствии с вариантом осуществления.

Фиг. 3 является диаграммой, показывающей пример таблицы уровня безопасности, сохраненной в IC-карте, в соответствии с вариантом осуществления.

Фиг. 4 является диаграммой, показывающей пример таблицы минимального уровня безопасности, сохраненной в IC-карте, в соответствии с вариантом осуществления.

Фиг. 5 является диаграммой последовательности, показывающей пример операции системы обработки IC-карты в соответствии с вариантом осуществления.

Фиг. 6 является блок-схемой последовательности действий, показывающей пример операции IC-карты в соответствии с вариантом осуществления.

Фиг. 7 является блок-схемой последовательности действий, показывающей пример операции IC-карты в соответствии с вариантом осуществления.

Фиг. 8 является схематичным представлением, показывающим функции, реализуемые посредством CPU IC-карты в соответствии с вариантом осуществления.

Вариант осуществления изобретения

Далее вариант осуществления будет описан со ссылкой на чертежи.

Фиг. 1 является блок-схемой для пояснения примера конфигурации системы 10 обработки IC-карты. Система 10 обработки IC-карты оснащена IC-картой 2 в соответствии с вариантом осуществления и устройством 1 обработки IC-карты, которое осуществляет связь с IC-картой 2. IC-карта 2 является портативным электронным устройством, и устройство 1 обработки IC-карты является внешним устройством для IC-карты 2.

В примере конфигурации, как показано на фиг. 1, устройство 1 обработки IC-карты имеет CPU 11, ROM 12, RAM 13, NVM 14, устройство 15 считывания/записи карты, операционный блок 16, дисплей 17 и т.д. Эти блоки соединены друг с другом через шину данных. Отметим, что в дополнение к конфигурации, как показано на фиг. 1, устройство 1 обработки IC-карты может иметь некоторую конфигурацию в соответствии с необходимостью исключать конкретную конфигурацию.

CPU 11 является центральным процессорным блоком и имеет функцию управления работой всего

устройства 1 обработки IC-карты. CPU 11 может быть оснащен внутренним кэшем, интерфейсами разного рода и т.д. CPU 11 реализует различные процессы путем исполнения программ, сохраненных во внутренней памяти, ROM 12 или NVM 14 заранее. Например, CPU 11 имеет функцию передачи команды на IC-карту 2 устройством 15 считывания/записи карты, функцию выполнения различных процессов на основе данных, таких как ответ, полученный от IC-карты 2, и другую функцию путем исполнения программы. Посредством этих функций CPU 11 передает на IC-карту 2 через устройство 15 считывания/записи карты команду записи, содержащую данные, введенные в операционный блок 16, предопределенные данные и т.п. Посредством вышеуказанной операции CPU 11 выполняет управление, чтобы запросить IC-карту 2 записать данные.

Отметим, что некоторые из различного рода функций, реализуемых посредством CPU 11, исполняющего программу, могут быть реализованы аппаратными схемами. В этом случае CPU 11 управляет функциями, исполняемыми аппаратными схемами.

ROM 12 является энергонезависимой памятью, в которой заранее сохранены программы для управления, данные управления и т.д. Управляющие программы и данные управления, сохраненные в ROM 12, вводятся заранее в соответствии со спецификациями устройства 1 обработки IC-карты. ROM 12 сохраняет, например, программу (например, BIOS) для управления печатной платой устройства 1 обработки IC-карты.

RAM 13 является энергозависимой памятью. RAM 13 временно хранит данные, находящиеся в процессе обработки CPU 11, и т.п. RAM 13 сохраняет различные прикладные программы на основе инструкций от CPU 11. Кроме того, RAM 13 может хранить данные, необходимые для исполнения прикладной программы, и т.п.

NVM 14 является энергонезависимой памятью с возможностью записи и перезаписи данных. NVM 14 состоит, например, из накопителя на жестком диске (HDD), твердотельного накопителя (SSD), EEPROM (зарегистрированный товарный знак) или флэш-памяти. NVM 14 хранит управляющие программы, приложения и различные данные в соответствии с операционным приложением устройства 1 обработки IC-карты.

Устройство 15 считывания/записи карты является интерфейсным устройством для передачи и приема данных к и от IC-карты 2. Устройство 15 считывания/записи карты образовано интерфейсом, соответствующим способу связи для IC-карты 2. Например, если IC-карта 2 является IC-картой контактного типа, устройство 15 считывания/записи карты образовано контактным участком для физического и электрического соединения с контактной частью IC-карты 2.

Если IC-карта 2 является IC-картой неконтактного типа, устройство 15 считывания/записи карты образовано антенной и блоком управления связью для выполнения беспроводной связи с IC-картой 2. Устройство 15 считывания/записи карты сконфигурировано, чтобы выполнять подачу электропитания, подачу тактового сигнала, управление сбросом и передачей и приемом данных на IC-карту 2.

При таких функциях на основе управления CPU 11 устройство 15 считывания/записи карты выполняет подачу электропитания на IC-карту 2, активацию (запуск) IC-карты 2, подачу тактового сигнала, управление сбросом, передачу различных команд и прием ответа (ответ) на переданную команду и т.д.

В операционный модуль 16 различные операционные инструкции вводятся оператором устройства 1 обработки IC-карты. Операционный модуль 16 передает данные операционной инструкции, введенной оператором в CPU 11. Операционный модуль 16 представляет собой, например, клавиатуру, десятиклавишную панель, панель касания или т.п.

Дисплей 17 представляет собой устройство отображения, которое отображает различную информацию под управлением CPU 11. Дисплей 17 представляет собой, например, жидкокристаллический монитор или т.п. Отметим, что дисплей 17 может быть выполнен совместно с операционным модулем 16.

Далее будет описана IC-карта 2.

IC-карта 2 сконфигурирована, чтобы быть активированной (подготовиться к работе) путем подачи на нее электропитания и т.п. от внешнего устройства, такого как устройство 1 обработки IC-карты. IC-карта 2 может выполнять связь контактного типа с устройством 1 обработки IC-карты или может выполнять связь бесконтактного типа с устройством 1 обработки IC-карты 1. Далее будет описан пример конфигурации IC-карты 2.

Фиг. 2 является блок-схемой, схематично показывающей пример конфигурации IC-карты 2 в соответствии с вариантом осуществления.

IC-карта 2 имеет подобное карте основное тело C, выполненное из пластика или т.п. Что касается IC-карты 2, модуль M встроен в основное тело C. Что касается модуля M, в состоянии, в котором IC-чип Ca и внешний интерфейс (например, модуль 25 связи) в качестве модуля связи соединены, IC-чип Ca и внешний интерфейс сформированы интегрально, и модуль M погружен в основное тело C IC-карты 2.

В примере конфигурации, показанном на фиг. 2, IC-карта 2 включает в себя модуль M, датчик отпечатка пальца 26 и т.д. Модуль M включает в себя модуль 25 связи, IC-чип Ca и т.д. IC-чип Ca включает в себя CPU 21, ROM 22, RAM 23, NVM 24 и т.п. ROM 22, RAM 23 и NVM 24 совместно упоминаются как память.

Эти модули соединены друг с другом через шину данных. Следует отметить, что касается IC-карты

2, необходимая конфигурация может быть соответственно добавлена, а ненужная конфигурация может быть удалена.

CPU 21 является центральным процессором и функционирует как модуль управления, который управляет IC-картой 2 в целом. CPU 21 выполняет различные процессы на основе управляющей программы и данных правления, сохраненных в ROM 22 или NVM 24. Например, CPU 21 исполняет программу, сохраненную в ROM 22, чтобы выполнять различные операции в соответствии с управлением операциями IC-карты 2 или режимом операции IC-карты 2.

Следует отметить, что некоторые из различного рода функций, реализуемых посредством CPU 21, исполняющего программу, могут быть реализованы аппаратными схемами. В этом случае CPU 21 управляет функциями, исполняемыми аппаратными схемами.

ROM 22 является энергонезависимой памятью, которая заранее сохраняет программы для управления и данные управления. ROM 22 вводится в IC-карту 2 в состоянии, когда управляющие программы, данные управления и т.п. сохраняются на стадии производства. То есть управляющие программы и данные управления, сохраняемые в ROM 22, вводятся заранее в соответствии со спецификациями IC-карты 2 или т.п.

RAM 23 является энергозависимой памятью. RAM 23 временно хранит данные в процессе обработки CPU 21 и т.п. Например, RAM 23 функционирует как буфер вычислений, буфер приема и буфер передачи. Буфер вычислений временно хранит результаты различной арифметической обработки, исполняемой посредством CPU 21, и т.п. Буфер приема хранит данные команд и т.п., принимаемые от устройства 1 обработки IC-карты через модуль 25 связи. Модуль передачи хранит сообщения (данные ответа) и т.п., подлежащие передаче на устройство 1 обработки IC-карты через модуль 25 связи.

NVM 24 образована энергонезависимой памятью записываемых и перезаписываемых данных, такой как EEPROM (зарегистрированный товарный знак) или флэш-ROM. NVM 24 хранит управляющую программу, приложение и различные данные в соответствии с применением IC-карты 2. Например, в NVM 24 создаются программные файлы, файлы данных и т.п. В каждом созданном файле записаны управляющая программа и различные данные.

Кроме того, NVM 24 включает в себя область хранения 24a для хранения таблицы уровней безопасности, область хранения 24b (первый модуль хранения) для хранения таблицы минимальных уровней безопасности, область хранения 24c для хранения счетчика низкой вероятности верификации и область хранения 24d (второй модуль хранения) для хранения истории оценки верификации. Таблица уровней безопасности, таблица минимальных уровней безопасности, счетчик низкой оценки верификации и оценка верификации будут описаны ниже.

Модуль 25 связи является интерфейсом для передачи и приема данных на и от устройства 1 обработки IC-карты. То есть модуль 25 связи является интерфейсом для выполнения связи с устройством 15 считывания/записи карты устройства 1 обработки IC-карты. Когда IC-карта 2 реализована как IC-карта контактного типа, модуль 25 связи образован модулем управления связью и контактным участком для физического и электрического контактирования с устройством 15 считывания/записи карты устройства 1 обработки IC-карты и передачи и приема сигнала. Например, IC-карта 2 активируется путем приема подачи электрической мощности операции и тактового сигнала операции от устройства 1 обработки IC-карты через контактный участок.

Когда IC-карта 2 реализована как IC-карта бесконтактного типа, модуль 25 связи образован модулем управления связью, таким как схема модуляции и демодуляции для выполнения беспроводной связи с устройством 15 считывания/записи карты устройства 1 обработки IC-карты, и антенной. Например, IC-карта 2 принимает радиоволны от устройства 1 обработки IC-карты через антенну, схему модуляции и демодуляции и т.д. IC-карта 2 генерирует электрическую мощность операции и тактовый сигнал операции из радиоволн посредством блока подачи электропитания (не показан) и активируется.

Датчик 26 отпечатка пальца (модуль получения биометрической информации) получает биометрическую информацию на основе различных характеристик биологического тела человека. Например, датчик отпечатка пальца 26 получает данные отпечатка пальца в качестве биометрической информации от пальца пользователя (биологического тела человека). Например, данные отпечатка пальца являются данными, указывающими признаки отпечатка пальца пользователя, владеющего IC-картой 2. Датчик 26 отпечатка пальца получает изображение отпечатка пальца и генерирует данные отпечатка пальца из полученного изображения отпечатка пальца.

Кроме того, датчик 26 отпечатка пальца имеет внутреннюю память, в которой заранее сохранены данные отпечатка пальца. Датчик 26 отпечатка пальца вычисляет оценку верификации между данными отпечатка пальца, полученными от биологического тела человека, и данными отпечатка пальца, сохраненными во внутренней памяти. Например, датчик 26 отпечатка пальца вычисляет оценку (степень) соответствия между данными отпечатка пальца, полученными от биологического тела человека, и данными отпечатка пальца, сохраненными во внутренней памяти, в качестве коэффициента верификации. Метод вычисления оценки соответствия между данными отпечатка пальца, полученными от биологического тела человека, и данными отпечатка пальца, сохраненными во внутренней памяти, может представлять собой, например, метод характерных точек, метод отношения или другие известные методы.

Кроме того, датчик 26 отпечатка пальца передает команду, сохраняющую оценку верификации, на CPU 11. Например, датчик 26 отпечатка пальца передает на CPU 11 команду, сохраняющую оценку верификации, с предопределенным временным соотношением после вычисления оценки верификации.

Далее будет описана таблица уровней безопасности.

Фиг. 3 показывает пример конфигурации таблицы уровней безопасности.

Как показано на фиг. 3, таблица уровней безопасности хранит уровень безопасности и диапазон оценки верификации в ассоциации друг с другом.

Уровень безопасности указывает состояние безопасности IC-карты 2, установленный на основе оценки верификации. То есть уровень безопасности указывает исполняемую операцию в IC-карте 2. Здесь уровень безопасности указывает исполняемую команду в IC-карте 2.

Диапазон оценки верификации указывает нижний предел и верхний предел коэффициента верификации. В примере, показанном на фиг. 3, диапазон оценки верификации образован минимальной оценкой верификации (нижний предел) и максимальной оценкой верификации (верхний предел). Например, минимальная оценка верификации, соответствующая уровню безопасности "3", равна "99,5" и максимальная оценка верификации равна "100". Соответственно, таблица уровней безопасности указывает, что диапазон оценки верификации, соответствующий уровню безопасности "3", равен 99,5 или более (т.е. от 99,5 до 100). Таким образом, минимальная оценка верификации, соответствующая уровню безопасности "2", равна "99", и максимальная оценка верификации равна "99,5". Соответственно, таблица уровней безопасности указывает, что диапазон оценки верификации, соответствующий уровню безопасности "2", равен 99 или более и меньше чем 99,5.

Следует отметить, что в таблице уровней безопасности любой диапазон оценки верификации может быть ассоциирован с уровнем безопасности. Кроме того, таблица уровней безопасности может хранить четыре или более уровней безопасности. Пример конфигурации таблицы уровней безопасности не ограничен конкретной конфигурацией.

Далее будет описана таблица минимальных уровней безопасности.

Фиг. 4 показывает пример конфигурации таблицы минимальных уровней безопасности.

Как показано на фиг. 4, таблица минимальных уровней безопасности хранит команду и минимальный уровень безопасности, при котором команда может исполняться, в ассоциации друг с другом.

Команда является командой, которую может исполнять CPU 21 IC-карты 2. Например, команда передается от устройства 1 обработки IC-карты.

Минимальный уровень безопасности является минимальным уровнем безопасности, при котором команда может исполняться. То есть минимальный уровень безопасности представляет собой уровень безопасности, требуемый для исполнения команды. Например, если текущий уровень безопасности равен или больше, чем минимальный уровень безопасности, соответствующий предопределенной команде, CPU 21 может исполнять предопределенную команду.

Например, в примере, показанном на фиг. 4, когда текущий уровень безопасности равен "2", CPU 21 может исполнять "GET CHALLENGE" (получить запрос) и "READ BINARY" (считать двоичный код). Кроме того, поскольку уровень безопасности, соответствующий "SELECT" (выбрать) равен "1", CPU 21 может также исполнять "SELECT".

Следует отметить, что пример конфигурации таблицы минимальных уровней безопасности не ограничен конкретной конфигурацией. Любая комбинация команды в таблице минимальных уровней безопасности и минимального уровня безопасности может быть выбрана.

Например, оператор системы 10 обработки IC-карты устанавливает таблицу минимальных уровней безопасности путем комбинирования обработки (команды), исполняемой посредством IC-карты 2, и уровня безопасности.

Когда таблица минимальных уровней безопасности установлена, оператор определяет допустимую степень (оценку) ложного отклонения и степень ложного принятия для каждого уровня безопасности и устанавливает диапазон оценки верификации на основе степени ложного отклонения и степени ложного принятия. То есть оператор устанавливает таблицу уровней безопасности, соответствующую таблице минимальных уровней безопасности. Каждый из множества уровней безопасности указывает исполняемую команду посредством таблицы, в которой команда и минимальный уровень безопасности, при котором команда может исполняться, ассоциированы друг с другом.

В приведенном выше описании таблица минимальных уровней безопасности установлена, но в настоящем изобретении без установки таблицы минимальных уровней безопасности обработка (команда), которую IC-карта может исполнять, может быть ассоциирована с каждым уровнем безопасности в таблице уровней безопасности.

Далее будут описаны функции, реализуемые посредством CPU 21, исполняющего программу, сохраненную в памяти. Как показано на фиг. 8, функции, реализуемые посредством CPU 21, включают в себя, например, модуль 21a получения оценки верификации, модуль 21b настройки, модуль 21c отсчета частоты низкой оценки верификации, модуль 21d обработки приема, модуль 21e определения и модуль 21f обработки передачи. Прежде всего, CPU 21 имеет функцию получения оценки верификации данных отпечатка пальца (модуль 21a получения оценки верификации).

Например, CPU 21 принимает команду сохранения оценки верификации данных отпечатка пальца от датчика 26 отпечатка пальца посредством модуля 25 связи. CPU 21 извлекает оценку верификации из команды.

После получения оценки верификации CPU 21 дополнительно сохраняет полученную оценку верификации в области хранения 24d NVM 24 во временной последовательности. То есть CPU 21 сохраняет историю оценки верификации в области хранения 24d. Например, CPU 21 может циклически сохранять оценку верификации в области хранения 24d.

Кроме того, CPU 21 имеет функцию выбора (определения) уровня безопасности на основе оценки верификации из множества уровней безопасности и установки выбранного (определенного) уровня безопасности на текущий уровень безопасности (модуль 21b настройки).

Например, CPU 21 получает уровень безопасности, включающий в себя оценку верификации в пределах диапазона оценки верификации, со ссылкой на таблицу уровней безопасности. Например, когда оценка верификации равна 99,4, CPU 21 получает уровень безопасности "2". CPU 21 сохраняет полученный уровень безопасности как текущий уровень безопасности в RAM 23.

Здесь, когда уровень безопасности равен от "1" до "3", предполагается, что аутентификация успешна. Кроме того, когда уровень безопасности равен "0", предполагается, что аутентификация безуспешна.

Кроме того, CPU 21 имеет функцию подсчета числа раз, когда уровень безопасности равен или ниже, чем предопределенный уровень безопасности, установленный на текущий уровень безопасности (модуль 21c отсчета частоты низкой оценки верификации). То есть при установке уровня безопасности, равного или ниже, чем предопределенный уровень безопасности, на текущий уровень безопасности CPU 21 увеличивает отсчет в прямом направлении счетчика низкой оценки верификации.

Например, при установке уровня безопасности, равного или ниже, чем предопределенной уровень безопасности, на текущий уровень безопасности, даже хотя аутентификация была успешной, CPU 21 увеличивает отсчет в прямом направлении счетчика низкой оценки верификации. Здесь при установке уровня безопасности, равного или ниже чем "2", на текущий уровень безопасности (т.е. когда текущий уровень безопасности равен "1" или "2"), CPU 21 увеличивает отсчет в прямом направлении счетчика низкой оценки верификации.

Кроме того, CPU 21 имеет функцию приема команды от устройства 1 обработки IC-карты (модуль 21d обработки приема). Например, CPU 21 принимает команду от устройства 15 считывания/записи карты устройства 1 обработки IC-карты посредством модуля 25 связи.

Кроме того, CPU 21 имеет функцию определения, является ли команда выполнимой, на основе текущего уровня безопасности (модуль 21e определения).

Например, CPU 21 получает минимальный уровень безопасности, соответствующий принятой команде, со ссылкой на таблицу минимальных уровней безопасности. Например, когда принятой командой является "GET CHALLENGE", CPU 21 получает "2" в качестве минимального уровня безопасности.

CPU 21 сравнивает текущий уровень безопасности, сохраненный в RAM, с полученным минимальным уровнем безопасности. Когда текущий уровень безопасности равен или выше, чем минимальный уровень безопасности, CPU 21 определяет, что команда может быть исполнена. Кроме того, когда текущий уровень безопасности не равен или не выше, чем минимальный уровень безопасности, то CPU 21 определяет, что команда не может быть исполнена.

Кроме того, когда оценка верификации снижается, CPU 21 имеет функцию передачи уведомления на устройство 1 обработки IC-карты, указывающее, что оценка верификации снизилась посредством модуля 25 связи (модуль 21f обработки передачи).

Например, при исполнении команды CPU 21 определяет, имеет ли оценка верификации тенденцию к снижению, со ссылкой на историю оценки верификации, сохраненную в области хранения 24d. Например, CPU 21 определяет, превышает ли значение отсчета счетчика низкой оценки верификации предопределенное пороговое значение.

Когда значение отсчета счетчика низкой оценки верификации превышает предопределенное пороговое значение, CPU 21 передает уведомление, указывающее, что оценка верификации снизилась, как ответ на устройство 1 обработки IC-карты. То есть CPU 21 генерирует ответ, указывающий результат исполнения команды и снижение в оценке верификации, и передает ответ на устройство 1 обработки IC-карты.

Следует отметить, что при определении, что команда не может быть исполнена, CPU 21 может определить, снижается ли оценка верификации. Временное соотношение, с которым CPU 21 определяет, снижается ли оценка верификации, и передает уведомление, указывающее, что оценка верификации снизилась, не ограничено конкретным временным соотношением.

Кроме того, в качестве уведомления, указывающего, что оценка верификации снизилась, CPU 21 может передать уведомление, предлагающее обновить данные отпечатка пальца, или уведомление, указывающее, что датчик 26 отпечатка пальца мог быть поврежден.

Далее будут описаны функции, реализуемые посредством CPU 11 устройства 1 обработки IC-карты.

При приеме уведомления, указывающего, что оценка верификации снизилась, от IC-карты 2 посредством устройства 15 считывания/записи карты, CPU 11 представляет предопределенную информа-

цию. Например, CPU 11 отображает сообщение или т.п., указывающее, что оценка верификации IC-карты 2 снизилась посредством дисплея 17. Кроме того, CPU 11 может отображать на дисплее 17 сообщение, предлагающее обновить данные отпечатка пальца, сообщение, предлагающее заменить IC-карту 2, или т.п.

Далее будет описан пример операции системы 10 обработки IC-карты.

Фиг. 5 является диаграммой последовательности для пояснения примера операции системы 10 обработки IC-карты.

Сначала пользователь, владеющий IC-картой 2, удерживает IC-карту 2 над устройством 15 считывания/записи карты (S11). Следует отметить, что пользователь может установить IC-карту 2 в предопределенное гнездо для вставки.

Когда пользователь удерживает IC-карту 2 над устройством 15 считывания/записи карты, устройство 15 считывания/записи карты подает электропитание на датчик 26 отпечатка пальца (S12) и подает электропитание на CPU 21 (S13). Следует отметить, что IC-чип Ca, получающий электропитание от устройства 15 считывания/записи карты, может подавать электропитание на датчик 26 отпечатка пальца.

Здесь предполагается, что пользователь приводит палец в контакт с датчиком 26 отпечатка пальца.

Когда устройство 15 считывания/записи карты подает электропитание на CPU 21, датчик 26 отпечатка пальца получает данные отпечатка пальца пользователя (S14). При получении данных отпечатка пальца, датчик 26 отпечатка пальца вычисляет оценку верификации (S15). При вычислении оценки верификации, датчик 26 отпечатка пальца передает оценку верификации на CPU 21 (S16).

CPU 21 принимает оценку верификации от датчика 26 отпечатка пальца. При приеме оценки верификации CPU 21 сохраняет оценку верификации в качестве истории в области хранения 24d (S17). При сохранении оценки верификации CPU 21 определяет уровень безопасности на основе оценки верификации (S18). При определении уровня безопасности CPU 21 сохраняет определенный уровень безопасности в качестве текущего уровня безопасности в RAM 23 (S19).

При сохранении определенного уровня безопасности в RAM 23 CPU 21 передает предопределенный ответ на датчик 26 отпечатка пальца (S20). При передаче ответа на датчик 26 отпечатка пальца CPU 21 ожидает приема команды от устройства 15 считывания/записи карты.

Устройство 15 считывания/записи карты передает предопределенную команду на IC-карту 2 на основе сигнала от CPU 11 (S21).

CPU 21 принимает команду. При приеме команды CPU 21 определяет, может ли команда быть исполнена на основе текущего уровня безопасности (S22). То есть CPU 21 определяет, является ли текущий уровень безопасности равным или выше, чем минимальный уровень безопасности, соответствующий команде.

При определении, что команда может быть исполнена (S22, ДА), CPU 21 исполняет команду (S23).

При исполнении команды CPU 21 передает ответ, указывающий результат исполнения команды, на устройство 15 считывания/записи карты (S24). Когда устройство 15 считывания/записи карты принимает ответ, система 10 обработки IC-карты 10 заканчивает операцию.

Когда определено, что команда не может быть исполнена (S22, НЕТ), CPU 21 передает уведомление об ошибке на устройство 15 считывания/записи карты, указывающее, что команда не может быть исполнена (S25). Когда устройство 15 считывания/записи карты принимает уведомление об ошибке, система 10 обработки IC-карты заканчивает операцию.

Далее будет описан пример операции CPU 21 IC-карты 2.

Сначала будет описан пример операции, в которой CPU 21 устанавливает текущий уровень безопасности.

Фиг. 6 является блок-схемой последовательности операций для пояснения примера операции IC-карты в соответствии с вариантом осуществления.

Сначала CPU 21 определяет, была ли принята команда от датчика 26 отпечатка пальца (S31). Когда определено, что команда не была принята (S31, НЕТ), CPU 21 возвращается к S31.

Когда определено, что команда была принята (S31, ДА), CPU 21 определяет, является ли команда соответствующей (S32). Например, CPU 21 проверяет код избыточности или т.п. и определяет, была ли команда повреждена или нет.

Когда определено, что команда является соответствующей (S32, ДА), CPU 21 получает оценку верификации из команды (S33). При получении оценки верификации CPU 21 сохраняет оценку верификации как историю в области хранения 24d (S34) (соответствует S17).

При сохранении коэффициента верификации в области хранения 24d CPU 21 определяет уровень безопасности на основе оценки верификации (S35) (соответствует S18). При определении уровня безопасности CPU 21 определяет, был ли определенный уровень безопасности равным или ниже, чем предопределенной уровень безопасности (например, 1 или 2) (S36). При определении, что определенный уровень безопасности равен или ниже, чем предопределенной уровень безопасности (S36, ДА), CPU 21 увеличивает отсчет в прямом направлении счетчика низкой оценки верификации, сохраняемый в области хранения 24c (S37).

При определении, что определенный уровень безопасности не равен или не ниже, чем предопреде-

ленный уровень безопасности (S36, НЕТ), или отсчитывании в прямом направлении счетчика низкой оценки верификации (S37), CPU 21 сохраняет определенный уровень безопасности, как текущий уровень безопасности в RAM 23 (S38) (соответствует S19). То есть CPU 21 устанавливает определенный уровень безопасности на текущий уровень безопасности.

При сохранении определенного уровня безопасности в RAM 23 CPU 21 передает предопределенной ответ на датчик 26 отпечатка пальца (S39) (соответствует S20).

При определении, что команда не является соответствующей (S32, НЕТ), CPU 21 передает ответ, включающий SW, указывающее ошибку, на датчик 26 отпечатка пальца (S40).

При передаче ответа на датчик 26 отпечатка пальца (S39) или при передаче ответа, включающего SW, указывающее ошибку, на датчик 26 отпечатка пальца (S40) CPU 21 заканчивает операцию.

Далее будет описан пример операции, когда CPU 21 принимает команду от устройства 15 считывания/записи карты.

Фиг. 7 является блок-схемой для объяснения примера операции, когда CPU 21 принимает команду от устройства 15 считывания/записи карты.

Сначала CPU 21 определяет, была ли команда принята от устройства 15 считывания/записи карты (S41). При определении, что команда не была принята от устройства 15 считывания/записи карты (S41, НЕТ), CPU 21 возвращается к S41.

При определении, что команда была принята от устройства 15 считывания/записи карты (S41, ДА), CPU 21 определяет минимальный уровень безопасности, соответствующий принятой команде (S42) (соответствует S22).

При определении минимального уровня безопасности CPU 21 определяет, является ли принятая команда исполняемой, на основе минимального уровня безопасности (S43) (соответствует S22). То есть CPU 21 определяет, является ли текущий уровень безопасности равным или выше, чем минимальный уровень безопасности.

При определении, что принятая команда является исполняемой (S43, ДА), CPU 21 исполняет принятую команду (S44) (соответствует S23). При исполнении команды CPU 21 определяет, является ли отсчет счетчика низкой оценки верификации большим, чем предопределенное пороговое значение (S45).

При определении, что отсчет счетчика низкой оценки верификации не больше, чем предопределенное пороговое значение (S45, НЕТ), CPU 21 передает ответ, указывающий результат исполнения команды, на устройство 15 считывания/записи карты посредством модуля 25 связи (S46) (соответствует S24).

При определении, что отсчет счетчика низкой оценки верификации не больше, чем предопределенное пороговое значение (S45, ДА), CPU 21 передает ответ, указывающий уменьшение оценки верификации и результат исполнения, на устройство 15 считывания/записи карты посредством модуля 25 связи (S47) (соответствует S24).

При определении, что принятая команда не может быть исполнена (S43, НЕТ), CPU 21 передает ответ, включающий SW, указывающее, что исполнение команды невозможно, на устройство 15 считывания/записи карты посредством модуля 25 связи (S48) (соответствует S25).

Когда ответ, указывающий результат исполнения команды, передан на устройство 15 считывания/записи карты (S46), когда ответ, указывающий уменьшение оценки верификации и результат исполнения, передан на устройство 15 считывания/записи карты (S47), или когда ответ, включающий SW, указывающее, что исполнение команды невозможно, передан на устройство 15 считывания/записи карты (S48), CPU 21 заканчивает операцию.

Следует отметить, что CPU 21 может выполнять S34 в любое время после S34.

Кроме того, CPU 21 может принимать данные отпечатка пальца пользователя от устройства 1 обработки IC-карты. Например, устройство 1 обработки IC-карты включает в себя датчик отпечатка пальца, который получает данные отпечатка пальца. CPU 21 получает данные отпечатка пальца от устройства 1 обработки IC-карты. CPU 21 может сравнивать полученные данные отпечатка пальца с данными отпечатка пальца, сохраненными в NVM 24 или т.п. заранее, чтобы вычислить оценку верификации.

Кроме того, CPU 21 может получать оценку верификации с использованием другой биометрической информации вместо данных отпечатка пальца. Например, CPU 21 может получать оценку верификации с использованием биометрической информации биологического тела человека, такого как радужная оболочка или кровеносные сосуды. Биометрическая информации не ограничена конкретной конфигурацией.

IC-карта, сконфигурированная, как описано выше, устанавливает уровень безопасности в соответствии с оценкой верификации биометрической информации. Кроме того, IC-карта устанавливает исполняемые команды в соответствии с текущим уровнем безопасности. Поэтому IC-карта может устанавливать исполняемые команды в соответствии с оценкой верификации. В результате, IC-карта может работать гибко в соответствии с оценкой верификации, даже когда оценка верификации снижается.

Кроме того, IC-карта сохраняет оценку верификации как историю. Поэтому оператор системы обработки IC-карты может проверить изменчивость оценки верификации. В результате оператор может устанавливать диапазон оценки верификации, соответствующий уровню безопасности для каждого пользователя. Например, оператор получает историю оценки верификации во время замены карты или т.п.

Оператор может устанавливать соответствующий диапазон оценки верификации для пользователя исходя из перехода оценки верификации.

Кроме того, устройство обработки IC-карты может получать историю оценки верификации из IC-карты.

Устройство обработки IC-карты определяет из истории полученной оценки верификации, является ли уровень безопасности, установленный в ассоциации с оценкой верификации в IC-карте, соответствующим (т.е. является ли диапазон оценки верификации для каждого уровня безопасности соответствующим), и перезаписывает таблицу уровней безопасности.

Хотя было описано несколько вариантов осуществления настоящего изобретения, эти варианты осуществления были представлены в качестве примера и не предназначены, чтобы ограничивать объем изобретения. Эти новые варианты осуществления могут быть реализованы в различных других формах, и различные пропуски, подстановки и изменения могут быть сделаны без отклонения от сущности изобретения. Эти варианты осуществления и их модификации включены в объем и сущность изобретения и включены в изобретение, описанное в пунктах формулы изобретения и их эквивалентном объеме.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. IC-карта, содержащая

модуль связи, который передает и принимает данные к и от внешнего устройства;

модуль получения биометрической информации, который получает биометрическую информацию от пользователя и вычисляет оценку соответствия между полученной биометрической информацией и биометрической информацией, зарегистрированной заранее, в качестве оценки верификации;

модуль получения оценки верификации, который получает упомянутую оценку верификации от модуля получения биометрической информации;

модуль настройки, который выбирает уровень безопасности, соответствующий оценке верификации, из множества уровней безопасности со ссылкой на таблицу уровней безопасности, которая хранит каждый из множества уровней безопасности и диапазон оценки верификации в ассоциации друг с другом, и устанавливает уровень безопасности, выбранный в качестве текущего уровня безопасности;

первый модуль хранения, который хранит таблицу минимального уровня безопасности, в которой команда и минимальный уровень безопасности, при котором упомянутая команда может быть выполнена, ассоциированы друг с другом;

модуль обработки приема, который принимает команду посредством модуля связи;

модуль определения, который определяет минимальный уровень безопасности, соответствующий упомянутой команде, принятой модулем обработки приема со ссылкой на таблицу минимального уровня безопасности, сравнивает текущий уровень безопасности с минимальным уровнем безопасности, соответствующим упомянутой принятой команде, и определяет, является или нет принятая команда исполняемой на основе результата сравнения.

2. IC-карта по п.1, в которой модуль определения определяет, что принятая команда является исполняемой, когда текущий уровень безопасности равен или выше, чем минимальный уровень безопасности, соответствующий принятой команде.

3. IC-карта по любому одному из пп.1, 2, в которой биометрическая информация является данными отпечатка пальца.

4. IC-карта по любому одному из пп.1, 2, дополнительно содержащая второй модуль хранения, который хранит оценку верификации как историю.

5. IC-карта по п.4, дополнительно содержащая модуль обработки передачи, который передает предопределенное уведомление на внешнее устройство посредством модуля связи, когда оценка верификации снижается.

6. IC-карта по п.1, причем модуль связи, модуль получения оценки верификации, модуль настройки, первый модуль хранения, модуль обработки приема и модуль определения объединены в модуль, встроенный в основное тело упомянутой IC-карты.

7. Портативное электронное устройство, содержащее IC-карту по п.1.

8. Способ обработки информации, выполняемый в IC-карте по п.1, причем способ содержит

получение биометрической информации от пользователя;

вычисление оценки соответствия между полученной биометрической информацией и биометрической информацией, зарегистрированной заранее, в качестве оценки верификации;

получение упомянутой оценки верификации;

выбор уровня безопасности, соответствующего оценке верификации из множества уровней безопасности, со ссылкой на таблицу уровней безопасности, которая хранит каждый из множества уровней безопасности и диапазон оценки верификации в ассоциации друг с другом;

установление уровня безопасности, выбранного в качестве текущего уровня безопасности;

прием команды;

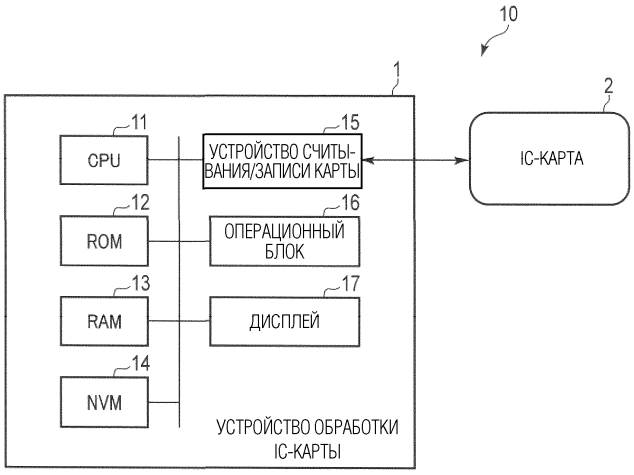
определение минимального уровня безопасности, соответствующего упомянутой команде, приня-

той со ссылкой на таблицу минимального уровня безопасности, в которой команда и минимальный уровень безопасности, при котором упомянутая команда может быть выполнена, ассоциированы друг с другом;

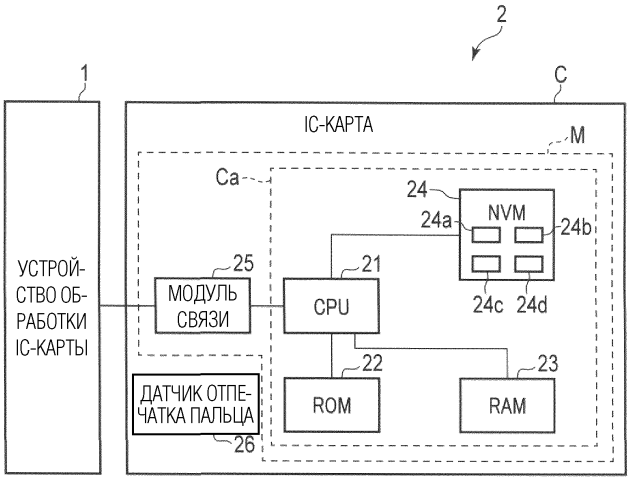
сравнение текущего уровня безопасности с минимальным уровнем безопасности, соответствующим упомянутой принятой команде; и

определение, является или нет принятая команда исполняемой на основе результата сравнения.

9. Способ обработки информации по п.8, в котором каждый из множества уровней безопасности указывает исполняемую команду посредством таблицы минимального уровня безопасности.



Фиг. 1



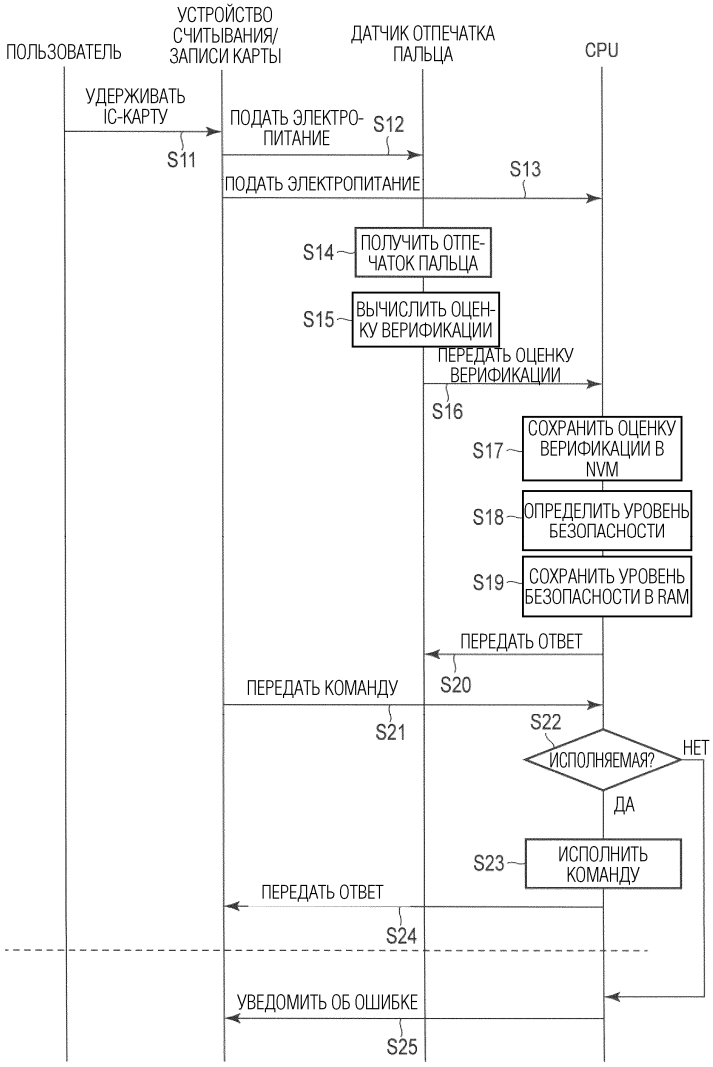
Фиг. 2

УРОВЕНЬ БЕЗОПАСНОСТИ	МИНИМАЛЬНЫЙ УРОВЕНЬ СВЕРКИ	МАКСИМАЛЬНЫЙ УРОВЕНЬ СВЕРКИ
3	99.5	100
2	99	99.5
1	98	99
0	0	98

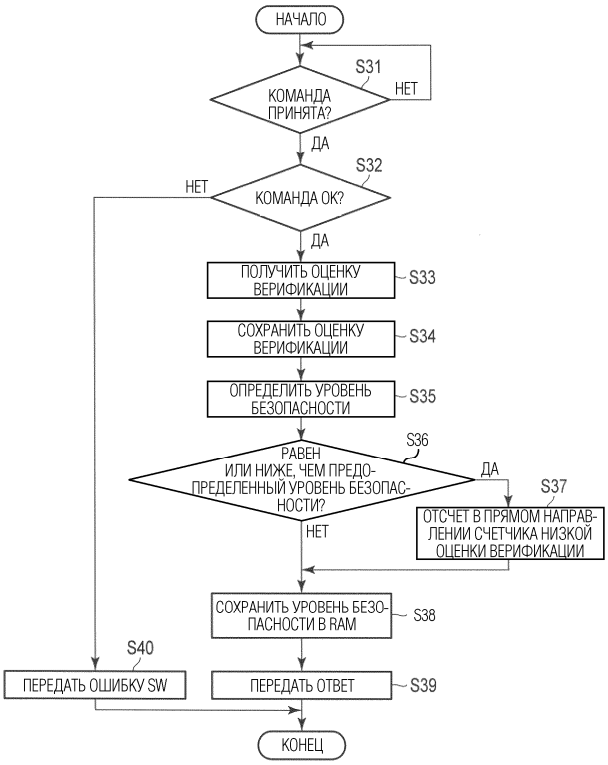
Фиг. 3

КОМАНДА	МИНИМАЛЬНЫЙ УРОВЕНЬ БЕЗОПАСНОСТИ
ВЗАИМНО АУТЕНТИФИЦИРОВАТЬ	3
ПОЛУЧИТЬ ЗАПРОС, СЧИТАТЬ ДВОИЧНЫЙ КОД	2
ВЫБРАТЬ	1

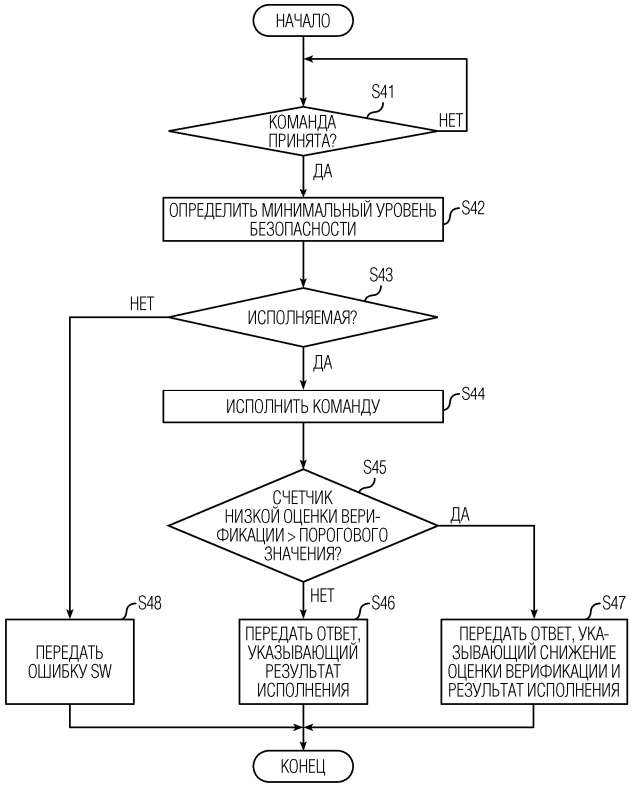
Фиг. 4


ПОЛЬЗОВАТЕЛЬ
УСТРОЙСТВО СЧИТЫВАНИЯ/ ЗАПИСИ КАРТЫ
ДАТЧИК ОТПЕЧАТКА ПАЛЬЦА
CPU
УДЕРЖИВАТЬ IC-КАРТУ
S11
ПОДАТЬ ЭЛЕКТРО-ПИТАНИЕ
S12
ПОДАТЬ ЭЛЕКТРОПИТАНИЕ
S13
S14
ПОЛУЧИТЬ ОТПЕ-ЧАТОК ПАЛЬЦА
S15
ВЫЧИСЛИТЬ ОЦЕН-КУ ВЕРИФИКАЦИИ
ПЕРЕДАТЬ ОЦЕНКУ ВЕРИФИКАЦИИ
S16
S17
СОХРАНИТЬ ОЦЕНКУ ВЕРИФИКАЦИИ В NVM
S18
ОПРЕДЕЛИТЬ УРОВЕНЬ БЕЗОПАСНОСТИ
S19
СОХРАНИТЬ УРОВЕНЬ БЕЗОПАСНОСТИ В RAM
ПЕРЕДАТЬ ОТВЕТ
S20
ПЕРЕДАТЬ КОМАНДУ
S21
S22
ИСПОЛНЯЕМАЯ?
НЕТ
ДА
S23
ИСПОЛНИТЬ КОМАНДУ
ПЕРЕДАТЬ ОТВЕТ
S24
УВЕДОМИТЬ ОБ ОШИБКЕ
S25

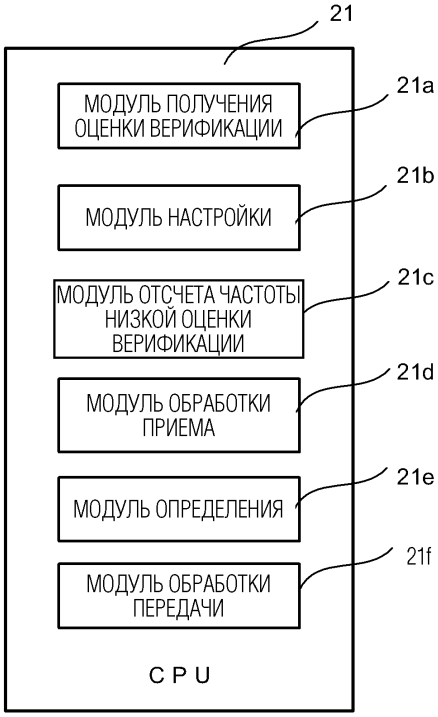
Фиг. 5


НАЧАЛО
S31
КОМАНДА ПРИНЯТА?
НЕТ
ДА
S32
КОМАНДА ОК?
НЕТ
ДА
ПОЛУЧИТЬ ОЦЕНКУ ВЕРИФИКАЦИИ
S33
СОХРАНИТЬ ОЦЕНКУ ВЕРИФИКАЦИИ
S34
ОПРЕДЕЛИТЬ УРОВЕНЬ БЕЗОПАСНОСТИ
S35
S36
РАВЕН ИЛИ НИЖЕ, ЧЕМ ПРЕДОПРЕДЕЛЕННЫЙ УРОВЕНЬ БЕЗОПАСНОСТИ?
ДА
S37
ОТСЧЕТ В ПРЯМОМ НАПРАВЛЕНИИ СЧЕТЧИКА НИЗКОЙ ОЦЕНКИ ВЕРИФИКАЦИИ
НЕТ
СОХРАНИТЬ УРОВЕНЬ БЕЗОПАСНОСТИ В RAM
S38
S40
ПЕРЕДАТЬ ОШИБКУ SW
ПЕРЕДАТЬ ОТВЕТ
S39
КОНЕЦ

Фиг. 6


НАЧАЛО
S41
КОМАНДА ПРИНЯТА?
НЕТ
ДА
ОПРЕДЕЛИТЬ МИНИМАЛЬНЫЙ УРОВЕНЬ БЕЗОПАСНОСТИ
S42
S43
НЕТ
ИСПОЛНЯЕМАЯ?
ДА
ИСПОЛНИТЬ КОМАНДУ
S44
S45
СЧЕТЧИК НИЗКОЙ ОЦЕНКИ ВЕРИФИКАЦИИ > ПОРОГОВОГО ЗНАЧЕНИЯ?
ДА
НЕТ
S48
ПЕРЕДАТЬ ОШИБКУ SW
S46
ПЕРЕДАТЬ ОТВЕТ, УКАЗЫВАЮЩИЙ РЕЗУЛЬТАТ ИСПОЛНЕНИЯ
S47
ПЕРЕДАТЬ ОТВЕТ, УКАЗЫВАЮЩИЙ СНИЖЕНИЕ ОЦЕНКИ ВЕРИФИКАЦИИ И РЕЗУЛЬТАТ ИСПОЛНЕНИЯ
КОНЕЦ

Фиг. 7



Фиг. 8

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