РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **158 940**(13) **U1**

(51) МПК
H04L 29/06 (2006.01)
G06F 21/34 (2013.01)

(12) ТИТУЛЬНЫЙ ЛИСТ ОПИСАНИЯ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ

(21)(22) Заявка: **2014128023/08, 28.12.2012**

(24) Дата начала отсчета срока действия патента:
28.12.2012

Приоритет(ы):
(30) Конвенционный приоритет:
30.12.2011 US 61/581,897

(45) Опубликовано: **20.01.2016** Бюл. № **2**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **30.07.2014**

(86) Заявка PCT:
US 2012/071941 (28.12.2012)

(87) Публикация заявки PCT:
WO 2013/102003 (04.07.2013)

Адрес для переписки:
190000, Санкт-Петербург, ВОХ-1125, ПАТЕНТИКА

(72) Автор(ы):
МАРИЁН Дирк (BE)

(73) Патентообладатель(и):
ВАСКО Дата Секьюрити Интернэшнл ГмбХ (CH)

RU 158940 U1

(54) ТОКЕН СТРОГОЙ АУТЕНТИФИКАЦИИ С ВИЗУАЛЬНЫМ ВЫВОДОМ ПОДПИСЕЙ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ (PKI)

RU 158940 U1

(57) Формула полезной модели

1. Устройство аутентификации, содержащее по меньшей мере один компонент обработки данных и дисплей и выполненное с возможностью:

генерирования аутентификационного сообщения,

кодирования аутентификационного сообщения в одно или большее количество изображений,

отображения указанного одного или большего количества изображений на дисплее, отличающееся тем, что оно выполнено портативным и ручным, а также дополнительно выполнено с возможностью:

генерирования входного значения,

подачи сгенерированного входного значения в асимметричную криптографическую операцию, генерирующую результат на основании асимметричного криптографического алгоритма, параметризованного посредством первого закрытого ключа из пары открытого и закрытого ключей,

получения результата асимметричной криптографической операции,

генерирования аутентификационного сообщения, по существу, содержащего результат асимметричной криптографической операции.

2. Устройство аутентификации по п. 1, дополнительно содержащее интерфейс связи, выполненный с возможностью связи с отдельным устройством защиты, причем

отдельное устройство защиты выполнено с возможностью хранения первого закрытого ключа из пары открытого и закрытого ключей и с возможностью выполнения асимметричной криптографической операции, а указанное устройство аутентификации выполнено с возможностью получения результата асимметричной криптографической операции путем выдачи запроса на отдельное устройство защиты на генерирование результата асимметричной криптографической операции путем выполнения этой асимметричной криптографической операции по отношению ко входному значению с использованием первого закрытого ключа, сохраненного в отдельном устройстве защиты, и путем получения результата асимметричной криптографической операции, сгенерированного отдельным устройством защиты, от отдельного устройства защиты.

3. Устройство аутентификации по п. 2, в котором отдельное устройство защиты содержит съемную смарт-карту.

4. Устройство аутентификации по п. 2, дополнительно содержащее интерфейс ввода данных, выполненный с возможностью получения по меньшей мере одного переменного элемента данных, который является внешним по отношению к устройству аутентификации, причем входное значение сгенерировано с использованием указанного по меньшей мере одного внешнего переменного элемента данных.

5. Устройство аутентификации по п. 4, в котором интерфейс ввода данных содержит клавиатуру.

6. Устройство аутентификации по п. 4, в котором интерфейс ввода данных содержит оптический интерфейс ввода данных.

7. Устройство аутентификации по п. 4, в котором интерфейс ввода данных содержит акустический интерфейс ввода данных.

8. Устройство аутентификации по п. 4, в котором указанный по меньшей мере один внешний переменный элемент данных содержит запрос.

9. Устройство аутентификации по п. 4, в котором указанный по меньшей мере один внешний переменный элемент данных содержит данные транзакций.

10. Устройство аутентификации по п. 1 или 2, дополнительно выполненное с возможностью генерирования входного значения с использованием по меньшей мере одного переменного элемента данных, который является внутренним по отношению к устройству аутентификации.

11. Устройство аутентификации по п. 10, дополнительно содержащее часы реального времени, причем указанный по меньшей мере один внутренний переменный элемент данных содержит значение времени, выданное этими часами реального времени.

12. Устройство аутентификации по п. 11, дополнительно содержащее счетчик, причем указанный по меньшей мере один внутренний переменный элемент данных содержит значение счетчика, выданное этим счетчиком.

13. Устройство аутентификации по п. 2, дополнительно выполненное с возможностью включения данных, связанных со входным значением, в аутентификационное сообщение.

14. Устройство аутентификации по п. 13, в котором данные, связанные со входным значением, содержат входное значение.

15. Устройство аутентификации по п. 1, дополнительно содержащее первый компонент хранения данных защиты, выполненный с возможностью хранения первого закрытого ключа, причем указанное устройство аутентификации дополнительно выполнено с возможностью выполнения асимметричной криптографической операции и с возможностью генерирования результата асимметричной криптографической операции путем выполнения этой асимметричной криптографической операции по отношению ко входному значению с использованием первого закрытого ключа, хранящегося в

RU 158940 U1

первом компоненте хранения данных защиты.

16. Устройство аутентификации по п. 2, дополнительно содержащее второй компонент хранения данных защиты, выполненный с возможностью хранения элемента секретных данных.

17. Устройство аутентификации по п. 16, дополнительно выполненное с возможностью генерирования данных, криптографически связанных со входным значением, путем криптографического комбинирования первого криптографического ключа с данными, связанными со входным значением, и с возможностью включения сгенерированных данных, криптографически связанных со входным значением, в аутентификационное сообщение, причем первый криптографический ключ входит в состав элемента секретных данных или извлечен из него.

18. Устройство аутентификации по п. 17, в котором первый криптографический ключ содержит симметричный криптографический ключ, совместно используемый устройством проверки, а криптографическое комбинирование выполнено с использованием алгоритма симметричного шифрования.

19. Устройство аутентификации по п. 17, в котором первый криптографический ключ содержит асимметричный криптографический ключ, а криптографическое комбинирование выполнено с использованием алгоритма асимметричного шифрования.

20. Устройство аутентификации по п. 17, в котором первый криптографический ключ содержит ключ шифрования, а криптографическое комбинирование выполнено с использованием алгоритма шифрования.

21. Устройство аутентификации по п. 16, дополнительно выполненное с возможностью генерирования данных, криптографически связанных с результатом асимметричной криптографической операции, путем криптографического комбинирования второго криптографического ключа по меньшей мере с частью результата асимметричной криптографической операции и с возможностью включения сгенерированных данных, криптографически связанных с результатом асимметричной криптографической операции, в аутентификационное сообщение, причем второй криптографический ключ входит в состав элемента секретных данных или извлечен из него.

22. Устройство аутентификации по п. 21, в котором второй криптографический ключ содержит симметричный криптографический ключ, совместно используемый устройством проверки, а криптографическое комбинирование выполнено с использованием алгоритма симметричного шифрования.

23. Устройство аутентификации по п. 21, в котором второй криптографический ключ содержит асимметричный криптографический ключ, а криптографическое комбинирование выполнено с использованием асимметричного криптографического алгоритма.

24. Устройство аутентификации по п. 21, в котором второй криптографический ключ содержит ключ шифрования, а криптографическое комбинирование включает шифрование по меньшей мере части результата асимметричной криптографической операции с использованием алгоритма шифрования.

25. Устройство аутентификации по п. 2, дополнительно выполненное с возможностью включения ссылки на открытый ключ, соответствующий первому закрытому ключу, в аутентификационное сообщение.

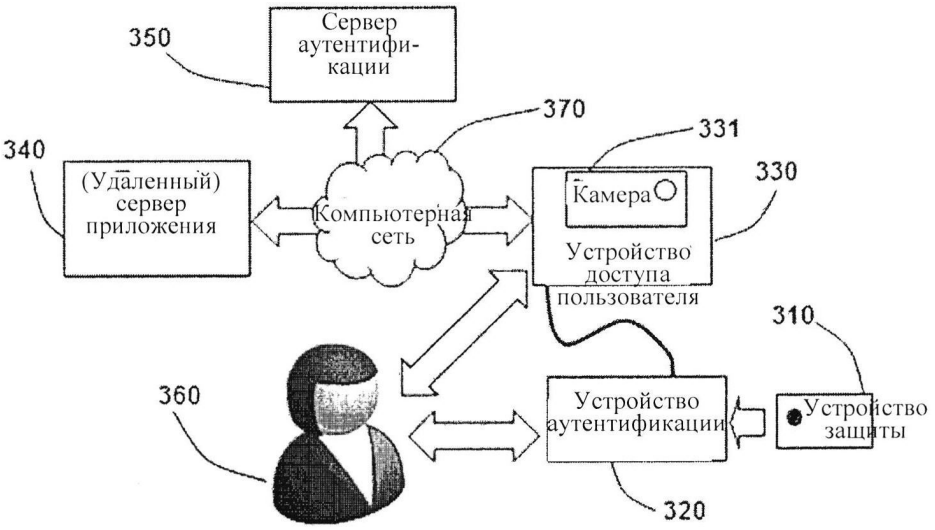
26. Устройство аутентификации по п. 1 или 2, дополнительно выполненное с возможностью включения элемента данных в аутентификационное сообщение для идентификации устройства аутентификации.

27. Устройство аутентификации по п. 2, дополнительно выполненное с возможностью включения элемента данных в аутентификационное сообщение для идентификации пользователя.

RU 158940 U1

RU 158940 U1

28. Устройство аутентификации по п. 2, дополнительно выполненное с возможностью включения элемента данных в аутентификационное сообщение для идентификации отдельного устройства защиты.



RU 158940 U1

RU 158940 U1