РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 449 377** (13) **C2**

(51) МПК
G07F 7/08 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2008140114/08, 27.02.2007**

(24) Дата начала отсчета срока действия патента:
27.02.2007

Приоритет(ы):
(30) Конвенционный приоритет:
11.03.2006 DE 102006011402.7

(43) Дата публикации заявки: **20.04.2010** Бюл. № 11

(45) Опубликовано: **27.04.2012** Бюл. № 12

(56) Список документов, цитированных в отчете о поиске: **US 2003/0159044 A1, 21.08.2003. EP 1161055 A2, 05.12.2001. EP 1492095 A2, 29.12.2004. US 2004/0247118 A1, 09.12.2004. US 2005/0269410 A1, 08.12.2005. US 6367011 B1, 02.04.2002. RU 49311 U1, 10.11.2005. RU 50065 U1, 10.12.2005.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **13.10.2008**

(86) Заявка PCT:
EP 2007/001677 (27.02.2007)

(87) Публикация заявки PCT:
WO 2007/104423 (20.09.2007)

Адрес для переписки:
105064, Москва, а/я 88, "Патентные поверенные Квашнин, Сапельников и партнеры", В.П.Квашнину

(72) Автор(ы):
ФЕЛЬКЕНИНГ Штефан (DE),
ЮНГЕРМАНН Харди (DE),
ХУПЕ Торстен (DE)

(73) Патентообладатель(и):
БАЙЕР ИННОВЕЙШН ГМБХ (DE)

RU 2449377 C2

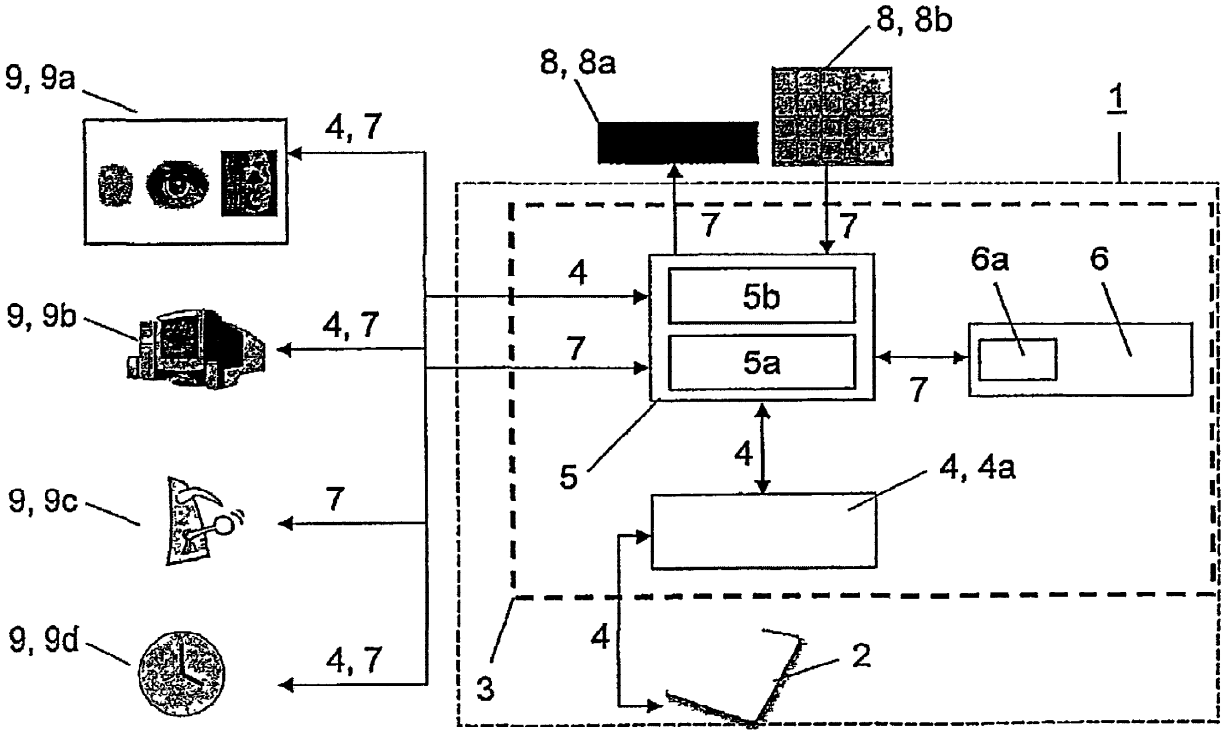
(54) СПОСОБ И АППАРАТУРА ДЛЯ БЕЗОПАСНОЙ ОБРАБОТКИ ИНФОРМАЦИИ, ПОДЛЕЖАЩЕЙ ЗАЩИТЕ

(57) Реферат:

Изобретение относится к области защиты информации, в частности защиты информации с помощью принципа подписи и/или шифрования. Техническим результатом является обеспечение надежности, быстроты и высокой помехозащищенности передачи большого количества данных, а также препятствия неавторизированного использования и применения данных. Система для безопасной обработки информации, в частности информации, подлежащей защите, с помощью принципа подписи и/или шифрования, включает в себя, по меньшей мере, пассивное мобильное первое запоминающее устройство (2) для сохранения первой информации с возможностью считывания, обрабатывающее устройство (3), выполненное для взаимодействия с первым запоминающим устройством (2), для

RU 2449377 C2

обработки информации недоступным для считывания извне, защищенным от манипуляций вторым запоминающим устройством (6) для надежного хранения второй информации, сочетающейся с первой информацией, вычислительным устройством (5) для обработки (криптографической обработки) информации, выполненным интегрированным во второе запоминающее устройство (6) по образцу смарт-карты или карты с чипом, устройством передачи информации (4) для передачи информации с первого и/или второго запоминающего устройства (2, 6) на вычислительное устройство (5), а также для передачи информации между обрабатывающим устройством (3) и подключенной периферией (9). 3 н. и 10 з.п. ф-лы, 1 ил.



ФИГ. 1

RU 2449377 C2

RU 2449377 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 449 377** (13) **C2**

(51) Int. Cl.
G07F 7/08 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2008140114/08, 27.02.2007**

(24) Effective date for property rights:
27.02.2007

Priority:
(30) Convention priority:
11.03.2006 DE 102006011402.7

(43) Application published: **20.04.2010** Bull. 11

(45) Date of publication: **27.04.2012 Bull. 12**

(85) Commencement of national phase: **13.10.2008**

(86) PCT application:
EP 2007/001677 (27.02.2007)

(87) PCT publication:
WO 2007/104423 (20.09.2007)

Mail address:
105064, Moskva, a/ja 88, "Patentnye poverennye Kvashnin, Sapel'nikov i partnery", V.P.Kvashninu

(72) Inventor(s):
FEL'KENING Shtefan (DE),
JuNGERMANN Khardi (DE),
KhUPE Torsten (DE)

(73) Proprietor(s):
BAJER INNOVEJShN GMBKh (DE)

RU 2449377 C2

(54) METHOD AND APPARATUS FOR SECURE PROCESSING OF PROTECTED INFORMATION

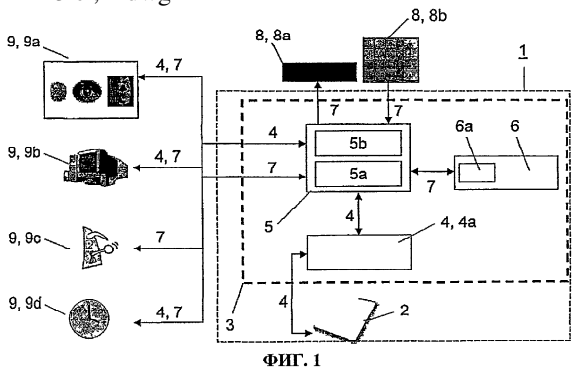
(57) Abstract:

FIELD: information technology.

SUBSTANCE: system securely processing information, particularly protected information by means of a signature and/or encryption principle, comprises at least a mobile passive first storage unit (2) for retrievably storing first information, a processing device (3) which is adapted for interacting with the first storage unit (2) in order to process information, a decryption-protected second storage unit (6) for securely storing second information corresponding to the first information, a computer unit (5) for (cryptographically) processing information, which is integrated in the second storage unit (6) on the smart-card or card with chip model, an information transmission device (4), for transmitting the information from the first and/or the second storage unit (2, 6) to the computer unit (5), as well as for transmitting information between the processing device (3) and the connected peripheral devices (9).

EFFECT: reliability, high speed of operation and high noise-immunity of transmitting a large amount of data, and preventing unauthorised use and reception of data.

13 cl, 1 dwg



ФИГ. 1

RU 2449377 C2

Настоящее изобретение касается системы и способа безопасной обработки информации, в частности информации, подлежащей защите, применения системы и способа согласно соответствующим ограничительным частям формулы изобретения, пункты 1, 12, 13, 14.

Системы, способы и/или применение для безопасной обработки информации, в частности информации, подлежащей защите, общеизвестны.

Например, известны устройства контроля доступа, такие как, например, банкоматы, дающие возможность доступа или допуска только через идентификацию, например, посредством карты с магнитной полоской или карты с чипом либо же смарт-карты, частично также в сочетании с личным идентификационным номером (PIN-код). При этом на картах записана требующая защиты информация, которая для защиты от неавторизованного использования запрашивает дальнейшую информацию (например, PIN-код). В картах с магнитной полоской или картах с чипом для электронных денежных расчетов сохранены зашифрованные данные. В случае «пассивных» карт, таких как, например, карты с магнитной полоской, расшифровка этих данных проходит удаленно, т.е. в отдельном считывающем устройстве. В активных картах вычислительное устройство, такое как, например, чип, интегрировано в саму карту. Соответственно расшифровка информации может проходить в чипе. Чтобы воспрепятствовать неправомерному использованию карты с чипом, доступ к нему регулируют с помощью, например, PIN-кода или запроса биометрических признаков.

Как магнитные карты, так и карты с чипом обладают тем недостатком, что они легко подвержены повреждению, загрязнению или иным воздействиям, например механическим или электромагнитных полей. Кроме того, у магнитных карт и карт с чипом ограничен объем памяти, который очень мал ввиду указанных размеров карт. По сравнению с магнитными картами емкость памяти у карт с чипом выше, и они лучше защищены от копирования и нежелательных манипуляций.

Поэтому в настоящее время все процедуры идентификации ограничены картами с чипом. Так, например, карты подписи, с помощью которых человек может электронным способом подтвердить аутентичность и сохранность нуждающейся в защите информации, выполняют только в виде карт с чипом.

Однако карты с чипом сложны и очень дороги в производстве, во много раз дороже, чем, например, карты с магнитной полосой.

Задача изобретения состоит в том, чтобы создать систему и/или способ безопасной передачи информации, нуждающейся в защите, которые обладают большой областью применения, которые можно использовать в различных приложениях и которые, в частности, просты в обращении.

Еще одна задача - создать систему и/или способ безопасной передачи информации, нуждающейся в защите, которые способны надежно, быстро и с высокой помехозащищенностью передавать большие количества данных, а также препятствовать неавторизованному использованию или применению.

Эту задачу решают посредством системы согласно ограничительной части пункта 1 формулы, способа согласно ограничительно части пунктов 12 и/или 13 формулы.

Настоящее изобретение включает в себя следующее техническое изложение: система безопасной обработки информации, в частности информации, нуждающейся в защите, посредством принципа подписи и/или шифрования включает в себя, по меньшей мере: первое мобильное пассивное запоминающее устройство для сохранения первой информации, к которой возможно обращение, обрабатывающее устройство,

сконструированное для взаимодействия с первым запоминающим устройством, для сохранения второй информации, сочетающейся с первой, к которой также возможно обращение, вычислительное устройство для обработки, предпочтительно для криптографической обработки информации блок передачи информации для передачи информации с первого и/или второго запоминающего устройства на вычислительное устройство.

Под «обработкой» в дальнейшем подразумевают вообще обработку по принципу «ввод, обработка, вывод (сохранение)». В еще более общем виде можно говорить об обращении с информацией.

Под «информацией», в частности, подразумевают любую информацию, но в особенности информацию, которую необходимо защитить от неавторизованного доступа, то есть в общем смысле конфиденциальную и/или нуждающуюся в защите информацию, как, например, личные данные, включая поставленные диагнозы, лечение, финансовые данные, как то данные банковских счетов, и т.п.

Чтобы защитить информацию от неавторизованного доступа или просмотра третьими лицами и/или проверить полноту и/или аутентичность информации, предусмотрен принцип подписи и/или шифрования.

Система или устройство для обработки информации включает в себя, по меньшей мере, одно мобильное запоминающее устройство для сохранения первого набора информации, к которому возможно обращение. Первое запоминающее устройство, соответственно, связано с объектом или человеком, находится в распоряжении объекта или человека и хранится у него. Первое запоминающее устройство выполнено мобильным, чтобы возможно было его перемещение с объектом либо же с человеком. На первом мобильном запоминающем устройстве записаны данные или информация, которые при необходимости можно прочесть с помощью соответствующего устройства. Информация включает в себя, например электронный ключ, например, частный ключ из пары ключей и/или роспись или электронную подпись. Кроме того, информация может содержать данные, которые необходимо хранить под защитой от доступа прочих лиц или в недоступном виде. Это могут быть, например, данные банковского счета, данные пациента, данные личной идентификации и т.п. Целесообразно, чтобы эта информация была зашифрована соответствующим ключом и/или подписана.

Чтобы в случае потребности иметь возможность обработать эту информацию, в системе предусмотрено устройство обработки. Устройство обработки взаимодействует с первым запоминающим устройством таким образом, что происходит считывание конфиденциальной информации посредством устройства обработки с первого запоминающего устройства или ее запись на это устройство.

Для этого в состав обрабатывающего устройства включено, по меньшей мере, одно второе запоминающее устройство. Второе запоминающее устройство предпочтительно выполнено защищенным от расшифровки. Это можно реализовать посредством физической защиты, например, закрытого корпуса, недоступного без авторизации и/или посредством других защитных устройств, например, защиты данных.

Во втором запоминающем устройстве сохраняют второй набор информации, обратиться к которому извне невозможно. Второй набор информации, в частности информации конфиденциальной и/или нуждающейся в защите, соотносится при этом с первой информацией на первом запоминающем устройстве. Например, второй набор информации может включать в себя ключ, соответствующий ключу первого

запоминающего устройства, например для формирования пары ключей. Кроме того, во втором запоминающем устройстве могут быть записаны существенные для идентификации данные, соответствующие данным в первом запоминающем устройстве.

Теперь, чтобы обработать хотя бы часть первой информации (первого набора информации), зашифрованной и/или подписанной, необходимо сначала расшифровать ее и/или проверить подпись. По этой причине в состав обрабатывающего устройства входит вычислительное устройство для обработки, в частности криптографической обработки, информации. Это вычислительное устройство обрабатывает данные, по меньшей мере, частично зашифрованные и/или подписанные, так что возможно проведение операции (трансакции), разрешение на которую может выдать только носитель первого запоминающего устройства.

Кроме того, для переноса информации с первого и/или второго запоминающего устройства на вычислительное устройство предусмотрен блок передачи информации. С его помощью соответствующую информацию можно передавать безопасно.

Кроме того, предпочтительно, чтобы, по меньшей мере, одно из запоминающих устройств было выполнено не как электронное запоминающее устройство, на которое возможна запись конфиденциальной информации, в частности первой информации, в ином виде нежели в электронном, и/или считывание ее. Иные нежели электронные запоминающие устройства включают в себя, например, магнитные или оптические запоминающие устройства.

Особо предпочтительно, чтобы, по меньшей мере, одно из запоминающих устройств было выполнено как оптическое запоминающее устройство, включающее в себя в виде средства записи полимеры с фотоадресацией, на которое можно оптическим способом записывать конфиденциальную информацию, в частности первую информацию, и/или считывать ее.

Полимеры с фотоадресацией образуют класс материалов, который отличается тем, что с помощью света в этом материале можно записать направленное двойное лучепреломление (Polymers as Electrooptical and Photooptical Active Media, V.P. Shibaev (Hrsg.), Springer Veriag, New York 1995; Natansohn et al., Chem. Mater. 1993, 403-411). Примерами этих полимеров с фотоадресацией являются полимеры с боковыми цепями с азобензольной функциональностью, описанные, например, в заявке на патент США US-A 5173381.

Посредством оптической записи большие количества информации можно надежно и в основном в защищенном от внешних воздействий виде располагать в малом пространстве. В частности, информация, записанная оптическим способом, надежно защищена от воздействия электричества или магнитных полей. Оптическая запись обеспечивает оптимальное соотношение емкости и размера памяти. Кроме того, оптические устройства записи дешевле в производстве, чем, например, электронные запоминающие устройства, как то чипы. Поэтому оптическая запись также характеризуется оптимальным соотношением емкости и стоимости.

Также предпочтительно, чтобы, по меньшей мере, одно из запоминающих устройств было выполнено в форме карточки, выбранной из группы, включающей карты с чипом, карты записи, смарт-карты. Изготовление в виде карты обеспечивает простое в обращении и мобильное исполнение запоминающего устройство. Целесообразно, чтобы карта имела те же размеры, что и прочие карты, находящиеся в повседневном обращении, как, например, кредитные карты и т.п. Эта форма карты позволяет легко размещать мобильное запоминающее устройство, например, в

кошельках и т.п. без необходимости приобретать новые средства хранения. Поэтому предпочтительно, чтобы карта имела формат ID-1, заданный стандартом ISO/IEC 7810.

Этот формат также предпочтителен в использовании с обычными считывающими устройствами и т.п.

Кроме того, для сохранения по возможности большего количества информации и/или данных на карточке и/или мобильном запоминающем устройстве целесообразно, чтобы, по меньшей мере, одно из запоминающих устройств обладало емкостью памяти, по меньшей мере, предпочтительно более 0,5 Мбайт, еще более предпочтительно более 1,0 Мбайт, а наиболее предпочтительно более 1,5 Мбайт. Обычные запоминающие устройства, как то магнитные полоски, чипы и т.п., обладают меньшей емкостью, которая позволяет хранить лишь очень ограниченный объем информации. Таким образом, записать возможно очень немного информации. Большие количества сохранить невозможно. При наличии предпочтительной емкости памяти согласно изобретению представляется возможным записывать более значительные объемы данных, при необходимости с более сложным шифрованием.

Чтобы обеспечить сохранение большого объема информации, средство записи, применяемое для создания запоминающего устройства, в частности первого мобильного запоминающего устройства, исполнено в виде полимера, в частности в виде полимера из группы полимеров с фотоадресацией.

Информацию на мобильное запоминающее устройство можно, в частности, записывать голографическим способом, особо предпочтительно в виде одной или нескольких поляризационных голограмм. Голографическая запись информации обеспечивает совершенную и эффективную защиту данных от несанкционированного доступа прочих лиц, как то от копирования или прочих манипуляций.

Голографическая запись данных представляет собой аналоговый способ записи, т.е. информация на первом мобильном запоминающем устройстве хранится в аналоговой форме.

Нуждающаяся в защите информация, сохраненная на первом мобильном запоминающем устройстве, перед записью на мобильное запоминающее устройство и/или после считывания с мобильного запоминающего устройства существует предпочтительно в цифровом виде.

Перед записью на мобильное запоминающее устройство и/или после считывания с мобильного запоминающего устройства она предпочтительно зашифрована и/или подписана.

Предпочтительный вариант исполнения предусматривает, что, по меньшей мере, одно из запоминающих устройств, предпочтительно второе запоминающее устройство, выполнено как цифровое запоминающее устройство, на которое возможна цифровая запись и/или с которого возможно цифровое считывание информации. На соответствующее запоминающее устройство, в частности на второе запоминающее устройство, информацию записывают в цифровом виде не в последнюю очередь из соображений емкости памяти. При этом цифровая конфиденциальная информация предпочтительно зашифрована и/или подписана цифровым способом. В случае, когда нуждающаяся в защите информация подписана, подпись предпочтительно сохранять на запоминающем устройстве вместе с нуждающейся в защите информации. По этой причине также предпочтительно, чтобы, по меньшей мере, одно из запоминающих устройств, предпочтительно второе запоминающее устройство, было выполнено как шифруемое запоминающее устройство, на которое возможна запись и/или с которого возможно считывание

информации с шифрованием/расшифровкой.

Для сохранения больших объемов информации соответствующее запоминающее устройство предпочтительно выполнено как пассивная память. В частности, мобильное запоминающее устройство сохраняет значительное количество информации. Поэтому пассивное запоминающее устройство не имеет участков, на которых с помощью соответствующих алгоритмов активно осуществляется расчет, обработка информации, ее расшифровка и т.д.

На втором запоминающем устройстве, напротив, обычно сохраняют значительно меньший объем информации, так что можно записать алгоритм для обработки информации. Поэтому предпочтительно, чтобы второе запоминающее устройство представляло собой активное запоминающее устройство. В известных на настоящий момент системах мобильное запоминающее устройство исполнено в виде активной памяти (карта с чипом) либо же мобильное запоминающее устройство располагает очень небольшим и незащищенным объемом памяти (карта с магнитной полосой).

Выполняя первое мобильное запоминающее устройство как пассивное защищенное запоминающее устройство, а второе запоминающее устройство как активную память или активное запоминающее устройство, создают надежную, прочную и недорогую систему.

В частности, поэтому предпочтительно, чтобы второе запоминающее устройство представляло собой электронное запоминающее устройство, запись второй информации на котором и/или считывание с которого возможны электронным способом. В отличие от исполнения в виде магнитного или неэлектронного запоминающего устройства, на электронном запоминающем устройстве можно без проблем реализовать электронную запись информации, в частности нуждающейся в защите, и алгоритмов, а также соответствующую коммуникацию со вычислительными устройствами, не подключая между ними, например, аналогово-цифровой преобразователь.

Таким образом, в предпочтительной форме исполнения первое запоминающее устройство выполнено в виде оптической памяти, то есть как пассивное запоминающее устройство, а второе запоминающее устройство называют также активной картой памяти, поскольку второе запоминающее устройство связано с вычислительным устройством.

Поэтому на первом запоминающем устройстве информацию сохраняют оптическим способом, предпочтительно голографическим. Теперь, чтобы с помощью устройства переноса информации перенести данные на второе, электронное запоминающее устройство, данные из аналогового состояния необходимо перевести в электронную или цифровую форму. Для этого в качестве устройства переноса информации используют источник света в сочетании с камерой. Голограмму на первом запоминающем устройстве для этого освещают с помощью источника света. По причине преломления светового луча на голограмме формируется изображение записанной информации. Камера воспринимает это сформированное изображение, которое содержит нуждающуюся в защите информацию, и, следовательно, отображает его. Камера формирует из оптических сигналов электронные или цифровые сигналы, соотносящиеся со вторым запоминающим устройством.

Для обработки нуждающейся в защите информации предназначено второе запоминающее устройство с первым вычислительным устройством. Доступ к информации на втором запоминающем устройстве есть только у этого первого вычислительного устройства. Возможность чтения информации, сохраненной на

втором запоминающем устройстве, и/или ее изменения со стороны посторонних лиц отсутствует. Только первое вычислительное устройство может контактировать со вторым запоминающим устройством так, чтобы между ними двумя происходила передача данных.

Первое вычислительное устройство обладает криптографическими функциями, с помощью которых информацию шифруют или расшифровывают либо же подписывают. В частности, среди этих функций есть возможность создания подписи и/или ее проверки. Первое вычислительное устройство защищено от доступа посторонних так же, как защищено от него и второе запоминающее устройство.

Целесообразно, чтобы вычислительное устройство, второе запоминающее устройство и устройство передачи информации для обмена данными между вычислительным устройством и вторым запоминающим устройством были выполнены в одном блоке или устройстве. В таком блоке возможен обмен информацией между первым и вторым запоминающим устройством.

Целесообразно, чтобы вычислительное устройство было выполнено интегрированным во второе запоминающее устройство по типу смарт-карты или карты с чипом. Чтобы воспрепятствовать манипуляциям несанкционированным манипуляциям, предпочтительно снабдить блок из вычислительного и запоминающего устройств сертификатом, например, согласно «общим критериям», („Common Criteria"), в частности, при этом достигают класса EAL 4+ или выше. Это обеспечивает очень высокий уровень безопасности.

Как уже описано предпочтительно, чтобы устройство переноса информации между мобильным первым запоминающим устройством и вторым запоминающим устройством было выполнено как оптическое устройство передачи информации, чтобы передавать информацию, по меньшей мере, по одному ходу лучей.

Целесообразно, чтобы вычислительное устройство обладало, по меньшей мере, одним каналом передачи, по которому возможна передача информации на другие вычислительные устройства и/или с них.

Предпочтительно, чтобы этот канал был выполнен как защищенный канал. Защищенный канал может представлять собой канал с шифрованием (логическая защита). Это, однако, может быть и канал, к которому не имеют доступа извне посторонние лица, поскольку он, например, находится под наблюдением или недоступен (физическая защита).

Для обмена данными между различными вычислительными устройствами необходимо, чтобы вычислительные устройства сначала взаимно «удостоверили» свою идентичность.

Устройство переноса информации можно предпочтительно изготавливать в виде устройства записи и/или считывания.

В предпочтительной форме исполнения предусматривается, что для того, чтобы оптическим способом переносить информацию посредством, по меньшей мере, одного луча, создают оптическое устройство переноса информации для испускания поляризованного света, включающего группу лазеров.

Целесообразно, чтобы было предусмотрено еще одно третье запоминающее устройство для записи третьей информации, соотносящейся с первой и/или второй информации, равно как и прочие вычислительные устройства, например, для повышения защищенности. Таким образом, можно, кроме того, организовать еще один контрольный запрос в целях безопасности, например в форме сканирования сетчатки, ввода PIN-кода, считывания других биометрических признаков, например,

отпечатка пальца и т.п.

Для управления, например, множественными ключами и/или сертификатами и им подобным, например, для различных пользователей предпочтительно, чтобы было предусмотрено также специальное устройство для управления множественными ключами и/или подписями.

Кроме того, изобретение включает в себя следующее техническое решение: предусмотрен способ безопасной криптографической обработки информации, обращения с ней и/или ее переноса, включающий в себя следующие шаги: считывание и/или запись первой зашифрованной информации на первом пассивном мобильном запоминающем устройстве, считывание и/или запись второй информации, соотносящейся с первой, перенос первой зашифрованной информации на вычислительное устройство, перенос второй информации на вычислительное устройство, криптографическая обработка первой информации в вычислительном устройстве с помощью второй информации, причем этапы считывания и/или записи первой информации и/или этап передачи первой информации, по меньшей мере, частично реализуют иным, нежели электронный, путем.

В частности, способ обработки конфиденциальной информации согласно изобретению включает в себя, в частности, описанные ниже этапы.

Информацию, в частности, подлежащую защите информацию, которая ранее была сохранена на мобильном запоминающем устройстве, переносят с первого мобильного запоминающего устройства на первое вычислительное устройство с помощью устройства переноса информации. Если информация зашифрована цифровым способом, ее расшифровывают с помощью первого вычислительного устройства и информации, сохраненной на втором запоминающем устройстве, например криптографических ключей. Если информация снабжена подписью, то эту подпись, соответственно, проверяют.

Информация на первом мобильном запоминающем устройстве зашифрована, в частности, симметричной системой шифрования. Для этого можно, например, использовать способ (алгоритм) шифрования по стандарту AES (Advanced Encryption Standard) подобный ему. Для подписи предпочтительно использовать какую-либо стандартную процедуру электронного шифрования. Для этого можно, например, применять способ по системе RSA или ECDSA (elliptic curve digital signature algorithm).

Предпочтительно, чтобы этап „считывание и/или запись первой информации" и/или этап „перенос первой информации" проводили оптическим способом. Этот способ позволять реализовать перенос, оптимизированный с точки зрения скорости передачи и безопасности данных.

Кроме того, предпочтительно реализовывать, по меньшей мере, один из этапов способа согласно изобретению цифровым способом. Цифровая обработка дает преимущество простоты дальнейшей переработки на компьютерах без потребности в аналогово-цифровом преобразователе. Таким образом, можно упростить конструкцию и способ.

Чтобы обеспечить только авторизованный доступ к информации предпочтительно, чтобы, по меньшей мере, один из этапов „считывание и/или запись первой информации" и/или „перенос первой информации" был реализован с шифрованием. Таким образом, обеспечивают высокий уровень защиты данных. В частности, при оптической цифровой переработке шифрование обеспечивает высшую степень защиты данных так, что этим способом возможно обрабатывать и совершенно конфиденциальную информацию. Вообще, этот способ позволяет обеспечить очень

высокую степень безопасности данных.

Предпочтительно, чтобы первая информация имела форму, пригодную для переноса оптическим способом. Кроме того, предпочтительно, чтобы этап „считывание и/или запись первой информации" и/или этап „перенос первой информации" реализовывали электронным способом. Это позволяет легко обрабатывать с помощью вычислительного устройства вторую информацию, которая уже так или иначе защищена от неавторизованного доступа и которую, как правило, не сохраняют на мобильном запоминающем устройстве. Для этого, в частности, можно использовать уже известные на нынешнем техническом уровне устройства памяти и/или средства обработки, которые в каждом случае модифицируют для соответствующего применения согласно настоящему изобретению.

Особое преимущество состоит в том, что „этапы чтения и/или записи" второй информации и криптографическую обработку осуществляют в одной детали. Это позволяет разместить устройства, необходимые для шифрования или расшифровки в одной детали, экономя место. Эту деталь соответствующим образом защищают от доступа извне или со стороны третьих лиц. Благодаря тому, что эти этапы осуществляют в одной детали, также нет необходимости предусматривать средства переноса данных, требующие времени. Благодаря интеграции в одной детали необходимо защищать от нежелательного доступа только саму эту деталь.

Чтобы обеспечить эффективную защиту или аутентификацию информации, ее снабжают подписью и/или шифруют. По этой причине целесообразно, чтобы этап „чтение и/или запись" включал в себя также этап „чтение и/или запись подписи и/или данных ключа". Подпись и/или данные ключа можно сохранять на различных запоминающих устройствах, например, также и на мобильных запоминающих устройствах. Если данные записаны голографическим способом, можно обеспечить соответствие высоким стандартам безопасности, которые делают как минимум практически невозможным считывание подписи и/или ключа.

В частности, если конфиденциальную информацию считывают и/или записывают в виде голограммы, включая поляризационные голограммы, эти последние оказываются оптимальным образом защищены от случайного или нежелательного доступа, поскольку простое считывание именно голограмм третьим лицом крайне сложно либо невозможно.

Кроме того, запись в виде голограммы обеспечивает также и эффективную защиту от нежелательных манипуляций и/или копирования.

Для управления информационными пакетами по возможности большого количества пользователей, причем все пакеты предпочтительно снабжены подписью или могут быть зашифрованы соответствующими индивидуальными ключами, предпочтительно управлять информацией, особенно таковой, нуждающейся в защите, с помощью менеджмента шифров. Менеджмент шифров (управление ключами) является частью настоящего изобретения.

В менеджменте шифров задают, выбирают и/или формируют ключи и сертификаты и таким образом присваивают их различным компонентам системы, чтобы была обеспечена безопасная обработка подлежащей защите информации. Кроме того, менеджмент шифров обеспечивает возможность удалять компоненты из системы и/или интегрировать их в систему без необходимости полной замены ключей и/или сертификатов.

Для выбора и присвоения ключей сначала определяют группу компонентов, которые все принадлежат к одной системе. В каждой системе присутствует множество

мобильных запоминающих устройств, а также, по меньшей мере, одно или несколько устройств считывания или записи для этих мобильных запоминающих устройств. Устройства считывания или записи в каждом случае содержат, по меньшей мере, одно запоминающее устройство в форме описанного выше второго запоминающего устройства, в сочетании с вычислительным устройством.

Такую систему может представлять собой, например, фирма, выдающая всем сотрудникам удостоверения в целях контроля доступа. В этом случае компоненты, принадлежащие к одной системе, - это удостоверения сотрудников и устройства считывания/записи.

Системой может быть также, например, банк, выдающий своим клиентам банковскую карточку (мобильное запоминающее устройство). В этом случае компоненты, принадлежащие к одной системе, - это банковские карточки и устройства считывания/записи.

Для системы предусматривается ключ K. Этот ключ с соблюдением мер безопасности записан во втором запоминающем устройстве (в каждом устройстве считывания/записи системы). Для каждого мобильного запоминающего устройства (ID_i), что принадлежит к системе, формируют индивидуальный ключ $K_i=f(K, ID_i)$, причем f - это функция формирования ключа. Конфиденциальная информация зашифрована на первом мобильном запоминающем устройстве ключом K_i. При расшифровке информацию, зашифрованную ключом K_i и записанную на мобильном запоминающем устройстве, переносят на первое вычислительное устройство с помощью устройства переноса информации и расшифровывают с помощью ключа K, записанного во втором запоминающем устройстве.

Кроме того, система имеет глобальный сертификат <TC>, выданный, например, трастовым центром (TC). К сертификату <TC> принадлежит секретный ключ t Глобальный сертификат также записан во втором запоминающем устройстве (каждом устройстве считывания/записи системы). Для каждого мобильного запоминающего устройства ID_i существует сертификат $<ID_i>_t$. Для доказательства аутентичности и/или целостности информации m ее на мобильном записывающем устройстве снабжают подписью с помощью соответствующего секретного ключа k_i в виде $S:=Sig(m, k_i)$. Подпись S сохраняют на мобильном запоминающем устройстве вместе с сертификатом. При проверке подписи происходит перенос данных m, подписи S и сертификата $<ID_i>_t$ с мобильного запоминающего устройства на первое вычислительное устройство с помощью устройства переноса информации. С помощью первого вычислительного устройства и глобального сертификата <TC>, сохраненного во втором запоминающем устройстве, сначала сверяют (верифицируют) сертификат $<ID_i>_t$. Затем с помощью сертификата $<ID_i>_t$ верифицируют подпись S. Если все сверки успешны, подпись принимается.

Еще в одной форме исполнения изобретения вышестоящая организация (TC) подписывает данные m непосредственно с помощью секретного ключа t. Это может иметь смысл, например, для биометрического контроля доступа. При этом вышестоящая организация сначала проверяет, действительно ли информация, подлежащая записи на мобильное запоминающее устройство, принадлежит к нему. В случае биометрического контроля доступа вышестоящая организация проверяет, действительно ли биометрические данные (информация m), подлежащие записи на карточку-удостоверение (мобильное запоминающее устройство), относятся к владельцу карты, и подтверждает правильность подписью.

Описанную выше схему подписи изменяют в этом случае так, что информацию m

подписывают как S:=Sig(m, t). Подпись S сохраняют на мобильном запоминающем устройстве вместе с данными m. Проверить ее можно, используя <TC>.

Возможно, как сначала подписывать информацию, а затем шифровать данные и подпись, так и сначала шифровать данные и потом подписывать шифрованные данные.

Как уже сказано выше, возможно соединять первое вычислительное устройство с другими вычислительными устройствами посредством каналов передачи. В этом случае особо целесообразно, чтобы эти дальнейшие вычислительные устройства были включены в систему безопасной передачи информации, подлежащей защите. В этом случае к системе относятся прочие вычислительные устройства, которые в общем смысле обозначают как аппараты.

Для системы существует групповой сертификат <G> с соответствующим секретным ключом g. Групповой сертификат <G> записан в каждом аппарате, относящемся к системе. Каждый аппарат с идентификационным номером ID_i обладает сертификатом $<ID_i, A_i>_g$, который подписан секретным ключом g. Сертификат содержит атрибуты A_i, которые могут сообщить о виде аппарата (например, система биометрического считывания, база данных и т.д.). Два аппарата, которые общаются между собой по зашифрованному каналу, обмениваются сертификатами. Они сверяют подпись сертификата $<ID_i, A_i>_g$ с использованием <G> и сверяют атрибуты. Безопасный путь передачи формируется между аппаратами только в том случае, когда проверка подписей проходит без ошибок.

Предпочтительно, чтобы сертификат $<ID_i, A_i>_g$ имел ограниченный срок действия. Сертификат можно ввести в аппараты, например, в виде смарт-карты, так, чтобы замена была проста.

По истечении срока действия сертификата ключ обновляют. В случае решения с помощью смарт-карты это можно сделать просто путем замены смарт-карт в аппаратах.

Для исключения аппаратов из системы безопасного обмена информацией их блокируют. Каждый аппарат содержит список (CRL) отозванных сертификатов. Это могут быть групповые сертификаты или сертификаты аппаратов. В случае группового сертификата происходит блокирование целой группы аппаратов, а в случае сертификата аппаратов - отдельных аппаратов. Такой список блокированных аппаратов необходимо загрузить в каждый аппарат. Список блокированных аппаратов подписан глобальным сертификатом, например, вышеуказанным сертификатом <TC>. Список блокированных аппаратов загружают в аппараты вместе с подписью Sig(CRL, t). Таким образом, аппараты, например, похищенные злоумышленником, оказываются блокированы, так что злоумышленник не имеет возможности добраться до конфиденциальной информации с помощью похищенных аппаратов.

Список блокированных аппаратов можно обновлять либо обращаться к нему посредством запроса центрального сервера. На сервере происходит проверка, есть ли запись о сертификате, о котором в настоящий момент подан запрос.

Особо предпочтительно применение системы согласно изобретению и/или способа согласно изобретению в качестве и/или в составе:

Систем контроля допуска,

Систем контроля доступа,

Систем банкоматов,

Системы удостоверений,

Системы управления медицинскими данными (например, «карточка здравоохранения»).

Дальнейшие предпочтительные признаки подробно описаны в зависимых пунктах или на следующей фигуре.

На фиг.1 схематически представлена система обработки информации с помощью принципа подписи и/или шифрования согласно изобретению.

На фиг.1 схематически представлена система 1 обработки информации, в частности информации, подлежащей защите согласно настоящему изобретению. Система 1 включает в себя запоминающее устройство 2, которое, как представлено, выполнено как мобильное запоминающее устройство, а в частности, как пассивное мобильное запоминающее устройство. Запоминающее устройство может быть выполнено в любой форме, оно, однако, представлено выполненным в виде карточки памяти, которая символически изображена в соответствующей рамке. Как представлено, запоминающее устройство 2 выполнено для оптической записи информации или данных. Подлежащая записи информация - это конфиденциальная либо же подлежащая защите информация, к которой, в частности, относятся биометрические данные и/или данные подписи, включая данные коррекции ошибок. Данные сохранены на запоминающем устройстве голографическим способом и/или с цифровым шифрованием.

Кроме запоминающего устройства 2, система 1 включает в себя также устройство обработки 3, которое схематически представлено штриховой линией. Обрабатывающее устройство 3 выполнено так, что оно может взаимодействовать с запоминающим устройством 2, в частности, производить считывание с запоминающего устройства 2 и/или запись на него. Стрелки от запоминающего устройства 2 к устройству обработки 3 и обратно схематически представляют считывание данных с запоминающего устройства 2 или запись на него.

В состав устройства обработки 3 для передачи информации с запоминающего устройства 2 введено устройство (блок) переноса информации 4, которое, как представлено, включает в себя датчик (камеру) 4а, пригодный для обработки сигнала. Понятие «устройство переноса информации» включает в себя в общем смысле все средства передачи между различными блоками, деталями и т.п. Как схематически показывают соответствующие стрелки, ведущие к первому устройству переноса информации 4а или от него, первое устройство переноса информации 4 или датчик 4а предназначен для передачи информации.

Кроме того, в состав системы 1 входит вычислительное устройство 5 для криптографической обработки информации. Для этого данные или информацию с датчика 4а либо же вообще с первого устройства переноса информации 4 перемещают на вычислительное устройство 5 или от него.

Также в состав системы 1 входит второе запоминающее устройство 6. Второе запоминающее устройство 6 изготовлено в защищенном от расшифровки исполнении и служит для сохранения с возможностью чтения второй информации, соотносящейся с первой информацией. В частности, это прочие данные, относящиеся к безопасности, которые в сочетании с первой информацией открывают допуск или доступ. В числе прочего в состав второго запоминающего устройства входит участок 6а, в котором хранятся соответствующие ключи для расшифровки подлежащей защите информации. Прочие данные, чтение которых возможно на этом участке, - это данные для расшифровки, подписи MAC (Message Authentication Code, кода идентификации сообщения) или же наоборот, например, для шифрования или аутентификации.

Через защищенное второе устройство переноса информации 7 соответствующие данные, относящиеся к данным, прочитанным с первого запоминающего устройства 2, передают со второго запоминающего устройства 6 либо же 6a на вычислительное устройство 5. Устройство переноса информации 7 выполнено так, что оно обладает эффективными защитными механизмами от злоумышленников, так что перехват сообщения и/или манипуляция информацией, которой обмениваются, невозможна.

В качестве примера вычислительное устройство 5 представлено на фиг.1 состоящим из двух модулей 5a и 5b. Модуль 5a берет на себя криптографические расчеты, в то время как модуль 5b управляет всей процедурой и отвечает за связь с прочими подключенными компонентами (8, 9).

Чтобы обеспечить дополнительную защиту посредством ввода со стороны предполагаемого носителя мобильного запоминающего устройства 2, в системе 1 предусмотрены средства внешней коммуникации с предполагаемым носителем мобильного запоминающего устройства 2. Для этого система предусматривает в составе устройства обработки интерфейсы для внешней коммуникации.

Первый интерфейс 8a служит для вывода или представления запроса на ввод или вопросов, предназначенных для проверки носителя. Этот первый интерфейс 8a выполнен в данном случае как индикатор или экран. На индикаторе отображается, например, требование ввести личный идентификационный номер (PIN-код).

Второй интерфейс 8b служит для ввода информации пользователем обрабатывающего устройства 3. Этот второй интерфейс 8b, как показано, реализован в виде панели ввода цифр с возможностью управлять вводом посредством движений курсора. С помощью этого ввода или устройства ввода пользователь устройства обработки 3 может вводить параметры управления или личные данные, например PIN-код.

Первый интерфейс 8a однонаправлено связан с вычислительным устройством 5, точнее со вторым модулем 5b, посредством защищенного второго устройства переноса информации 7, причем направление - от второго модуля к первому интерфейсу 8a.

Второй интерфейс 8b однонаправлено связан с вычислительным устройством 5, точнее со вторым модулем 5b, посредством защищенного второго устройства переноса информации 7, причем направление - от второго интерфейса 8b ко второму модулю 5b.

Представленная на фиг.1 система 1 включает в себя, помимо мобильного запоминающего устройства 2 и устройства обработки 3, образующих ядро системы, еще и периферию (периферийные устройства) 9 или подключаемые системы, с которыми посредством соответствующих соединений возможен обмен данными или информацией. Так, в этой периферии 9 первая подключаемая система 9a может служить целям замера биометрических параметров и сравнения информации. Для этого второй модуль 5b связан в обоих направлениях с первой подключаемой системой 9a для передачи сигналов управления. С другой стороны, второй модуль 5b связан в обоих направлениях с первой подключаемой системой 9a защищенным каналом для передачи биометрических данных и ответного сообщения о результате проверки. Защищенный канал (защищенное соединение) - это соединение, недоступное для злоумышленника извне. Первая подключаемая система 9a может, например, представлять собой устройство для сканирования сетчатки или любое другое устройство для замера биометрических параметров, например отпечатков пальцев,

узора сетчатки, голоса и т.п.

Кроме того, в состав периферии 9 может входить вторая подключаемая система 9b. Эта вторая подключаемая система 9b может представлять собой базу данных, в состав которой входят, например, компьютерная сеть или просто сервер. В базе данных может храниться соответствующая информация, к которой пользователь может обратиться после верификации. Вторая подключаемая система 9b посредством защищенного или простого соединения связана с устройством обработки 3, точнее со вторым модулем 5, и между ними осуществляется перенос данных или информации M. Если происходит обмен информацией, подлежащей защите, то соединение выполнено в виде защищенного второго устройства переноса информации 7. Если происходит обмен информацией, не имеющей критического значения, можно выбрать простое первое устройство переноса информации 4.

К тому же периферия 9 может включать третью подключаемую систему 9c. Третья подключаемая система 9c может быть выполнена как средство допуска, например, представлять собой дверной замок, который после верификации или идентификации обеспечивает пользователю проход. Третья подключаемая система 9c ist связана с вычислительным устройством 5 соединением, работающим в обоих направлениях. Чтобы помешать злоумышленнику посылать извне сигнал на выполненную как средство допуска подключаемую систему 9c в целях получения доступа, подключаемую систему 9c предпочтительно соединять с вычислительным устройством 5 посредством защищенного соединения 7.

Кроме того, в состав периферии 9 может входить четвертая подключаемая система 9d. Четвертая подключаемая система 9d может, например, представлять собой систему отсчета времени, которая, например, регистрирует время или предоставляет ограниченный во времени допуск. Четвертая подключаемая система 9d связана с вычислительным устройством 5 соединением, работающим в обоих направлениях, в числе прочего происходит передача временных данных.

Если происходит обмен информацией, подлежащей защите, то соединение выполнено в виде защищенного второго устройства переноса информации 7. Если происходит обмен информацией, не имеющей критического значения, можно выбрать простое соединение или первое устройство переноса информации 4.

В общем случае периферия 9 может включать только одну из подключаемых систем от 9a до 9d либо же любое сочетание подключаемых систем.

Список условных обозначений

1 Система

2 Первое запоминающее устройство

3 Обрабатывающее устройство

4 Первое устройство переноса информации

4a Камера

5 Вычислительное устройство

5a Первый модуль

5b Второй модуль

6 Второй запоминающее устройство

7 Второе (защищенное) устройство переноса информации

8 Интерфейс(ы)

8a Первый интерфейс

8b Второй интерфейс

9 Периферия

9a Первая подключаемая система
9b Вторая подключаемая система
9c Третья подключаемая система
9d Четвертая подключаемая система

Формула изобретения

1. Система для безопасной обработки информации, в частности информации, подлежащей защите, с помощью принципа подписи и/или шифрования, включающая в себя, по меньшей мере:

пассивное мобильное первое запоминающее устройство (2) для сохранения первой информации с возможностью считывания, с однозначным идентификационным номером IDS_i, причем индекс i указывает на количество принадлежащих к системе первых запоминающих устройств (2),

обрабатывающее устройство (3), выполненное для взаимодействия с первым запоминающим устройством (2), для обработки информации, с:

однозначным идентификационным номером IDV_n, причем индекс n указывает на количество принадлежащих к системе обрабатывающих устройств (3),

недоступным для считывания извне, защищенным от манипуляций вторым запоминающим устройством (6) для надежного хранения второй информации, сочетающейся с первой информацией,

вычислительным устройством (5) для обработки (криптографической обработки) информации, выполненным интегрированным во второе запоминающее устройство (6) по образцу смарт-карты или карты с чипом,

устройством передачи информации (4) для передачи информации с первого и/или второго запоминающего устройства (2, 6) на вычислительное устройство (5), а также для передачи информации между обрабатывающим устройством (3) и подключенной периферией (9).

2. Система по п.1, отличающаяся тем,

что, по меньшей мере, одно из запоминающих устройств (2, 6) выполнено в виде оптического запоминающего устройства, предпочтительно - голографического запоминающего устройства в форме карточки, выполненного с возможностью оптической, предпочтительно голографической записи информации и/или с возможностью считывания информации,

и что, по меньшей мере, одно из устройств передачи информации (4) выполнено в виде оптического устройства передачи информации, чтобы передавать информацию, по меньшей мере, по одному ходу лучей.

3. Система по п.1 или 2, отличающаяся тем,

что в недоступном для считывания извне, защищенном от манипуляций втором запоминающем устройстве (6) хранится криптографический ключ К (глобальный),

что информация m сохраняется на одном из первых запоминающих устройств (2) в зашифрованном виде с помощью ключа K_i, причем ключ производится уникальным образом с помощью функции формирования ключа f из ключа К во втором запоминающем устройстве (6): $K_i=f(K, IDS_i)$.

4. Система по п.1 или 2, отличающаяся тем,

что в недоступном для считывания извне, защищенном от манипуляций втором запоминающем устройстве (6) хранится сертификат <TC> (глобальный), к которому принадлежит секретный ключ t,

что, по меньшей мере, в одном принадлежащем к системе первом запоминающем

устройстве IDS_i (2) записан производящийся от глобального сертификата <TC> сертификат $<IDS_i>_t$, к которому принадлежит секретный ключ k_i,

что, по меньшей мере, в одном принадлежащем к системе первом запоминающем устройстве IDS_i (2) записана подпись S, сформированная из информации m посредством ключа k_i, как $S:=Sig(m, k_i)$.

5. Система по п.1 или 2, отличающаяся тем,

что в недоступном для считывания извне, защищенном от манипуляций втором запоминающем устройстве (6) хранится сертификат <TC> (глобальный), к которому принадлежит секретный ключ t,

что, по меньшей мере, в одном, принадлежащем к системе первом запоминающем устройстве IDS_i (2) записана подпись S, сформированная из информации m посредством ключа t, как $S:=Sig(m, t)$.

6. Система по п.3, отличающаяся тем, что в недоступном для считывания извне, защищенном от манипуляций втором запоминающем устройстве (6) хранится сертификат <TC> (глобальный), к которому принадлежит секретный ключ t,

что, по меньшей мере, в одном принадлежащем к системе первом запоминающем устройстве IDS_i (2) записан производящийся от глобального сертификата <TC> сертификат $<IDS_i>_t$, к которому принадлежит секретный ключ k_i,

что, по меньшей мере, в одном принадлежащем к системе первом запоминающем устройстве IDS_i (2) записана подпись S, сформированная из информации, зашифрованной K_i, посредством ключа k_i.

7. Система по п.3, отличающаяся тем,

что в недоступном для считывания извне, защищенном от манипуляций втором запоминающем устройстве (6) хранится сертификат <TC> (глобальный), к которому принадлежит секретный ключ t,

что, по меньшей мере, в одном принадлежащем к системе первом запоминающем устройстве IDS_i (2) записана подпись S, сформированная из информации, зашифрованной K_i, посредством ключа t.

8. Система по п.1 или 2, отличающаяся тем,

что в недоступном для считывания извне, защищенном от манипуляций втором запоминающем устройстве (6) хранится криптографический ключ К (глобальный),

что в недоступном для считывания извне, защищенном от манипуляций втором запоминающем устройстве (6) хранится сертификат <TC> (глобальный), к которому принадлежит секретный ключ t,

что, по меньшей мере, в одном принадлежащем к системе первом запоминающем устройстве IDS_i, (2) записан производящийся от глобального сертификата <TC> сертификат $<IDS_i>_t$, к которому принадлежит секретный ключ k_i,

что от криптографического ключа К, по меньшей мере, для одного из принадлежащих к системе первых запоминающих устройств IDS_i (2) производится уникальный ключ K_i с помощью функции формирования ключа f: $K_i=f(K, IDS_i)$,

что от информации m посредством ключа k_i производится подпись S как $S:=Sig(m, k_i)$, которая шифруется с помощью ключа K_i и сохраняется, по меньшей мере, на одном из принадлежащих к системе запоминающих устройств IDS_i (2).

9. Система по п.1 или 2, отличающаяся тем,

что в недоступном для считывания извне, защищенном от манипуляций втором запоминающем устройстве (6) хранится криптографический ключ К (глобальный),

что в недоступном для считывания извне, защищенном от манипуляций втором

запоминающем устройстве (6) хранится сертификат <TC> (глобальный), к которому принадлежит секретный ключ t,

что от криптографического ключа K, по меньшей мере, для одного из принадлежащих к системе первых запоминающих устройств IDS_i (2) производится уникальный ключ K_i с помощью функции формирования ключа $f:K_i=f(K, IDS_i)$,

что от информации m посредством ключа k_i производится подпись S как $S:=Sig(m, k_i)$, которая шифруется с помощью ключа K_i и сохраняется, по меньшей мере, на одном из принадлежащих к системе запоминающих устройств IDS_i (2).

10. Система по п.1 или 2, отличающаяся тем,

что для группы из нескольких (по меньшей мере 2) обрабатывающих устройств (3) и/или компонентов подключенной периферии (9) существует групповой сертификат <G> с соответствующим секретным ключом g, который сохранен в принадлежащем к группе обрабатывающем устройстве/компоненте,

что для каждого принадлежащего к группе обрабатывающего устройства (3) и/или компонента подключенной периферии (9) существует сертификат $<IDV_n, A_n>_g$, который подписан секретным ключом g и сохранен в каждом принадлежащем к группе обрабатывающем устройстве и/или компоненте, причем A_n означают атрибуты, которые могут дать информацию о свойствах обрабатывающего устройства и/или компонента,

что в каждом принадлежащем к группе обрабатывающем устройстве (3) и/или компоненте подключенной периферии (9) сохранен список отозванных сертификатов, причем список подписан сертификатом <TC>, и эта подпись также сохранена в каждом принадлежащем к группе обрабатывающем устройстве и/или компоненте.

11. Способ безопасной (криптографической) обработки информации (обращения с ней/ ее переноса) с помощью системы по любому из пп.1-10, характеризующийся следующими этапами:

передачей информации посредством устройства передачи информации (4) с первого мобильного запоминающего устройства (2) на одно из обрабатывающих устройств (3) системы,

при необходимости - расшифровкой перенесенной информации, если таковая зашифрована, с помощью ключа K, записанного в защищенном от манипуляций втором запоминающем устройстве (6),

при необходимости - проверкой сертификата $<IDS_i>_t$, если таковой существует, с помощью сертификата <TC>, записанного в защищенном от манипуляций втором запоминающем устройстве (6),

при необходимости - проверкой подписи $S:=Sig(m, k_i)$, если таковая существует, с помощью проверенного сертификата $<IDS_i>_t$,

при необходимости - проверкой подписи $S:=Sig(t, k_i)$, если таковая существует, с помощью сертификата <TC>,

передачей информации с помощью устройства передачи информации (4) с системы на подключенную периферию (9).

12. Способ по п.11, отличающийся тем,

что обрабатывающее устройство (3) и периферия (9) перед обменом подлежащей защите информацией сначала обмениваются сертификатами $<IDV_n, A_n>_g$ и проверяют их с применением <G>,

что обрабатывающее устройство (3) и периферия (9) перед обменом подлежащей защите информацией проверяют действительность сертификатов друг друга на основании списка отозванных сертификатов,

что передача подлежащей защите информации между обрабатывающим устройством (3) и периферией (9) предпочтительно происходит в зашифрованном и/или защищенном режиме.

13. Применение системы по любому из пп.1-10 в качестве и/или в составе:
системы контроля допуска,
системы контроля доступа,
системы банкоматов,
системы удостоверений,
системы управления медицинскими данными.