РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 421 807** (13) **C2**

(51) МПК
G06F 21/20 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2007147634/08, 22.06.2006**

(24) Дата начала отсчета срока действия патента:
22.06.2006

Приоритет(ы):
(30) Конвенционный приоритет:
01.07.2005 US 60/695,944
15.02.2006 US 11/354,800

(43) Дата публикации заявки: **27.06.2009** Бюл. № 18

(45) Опубликовано: **20.06.2011** Бюл. № 17

(56) Список документов, цитированных в отчете о поиске: **WO 2005/008385 A2, 27.01.2005. RU 2238614 C2, 20.10.2004. RU 2144269 C1, 10.01.2000.**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **20.12.2007**

(86) Заявка PCT:
US 2006/024034 (22.06.2006)

(87) Публикация заявки PCT:
WO 2007/005281 (11.01.2007)

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
ХЬЮЗ Мл. Роберт К. (US),
АРРУИ Ив (US)

(73) Патентообладатель(и):
МАЙКРОСОФТ КОРПОРЕЙШН (US)

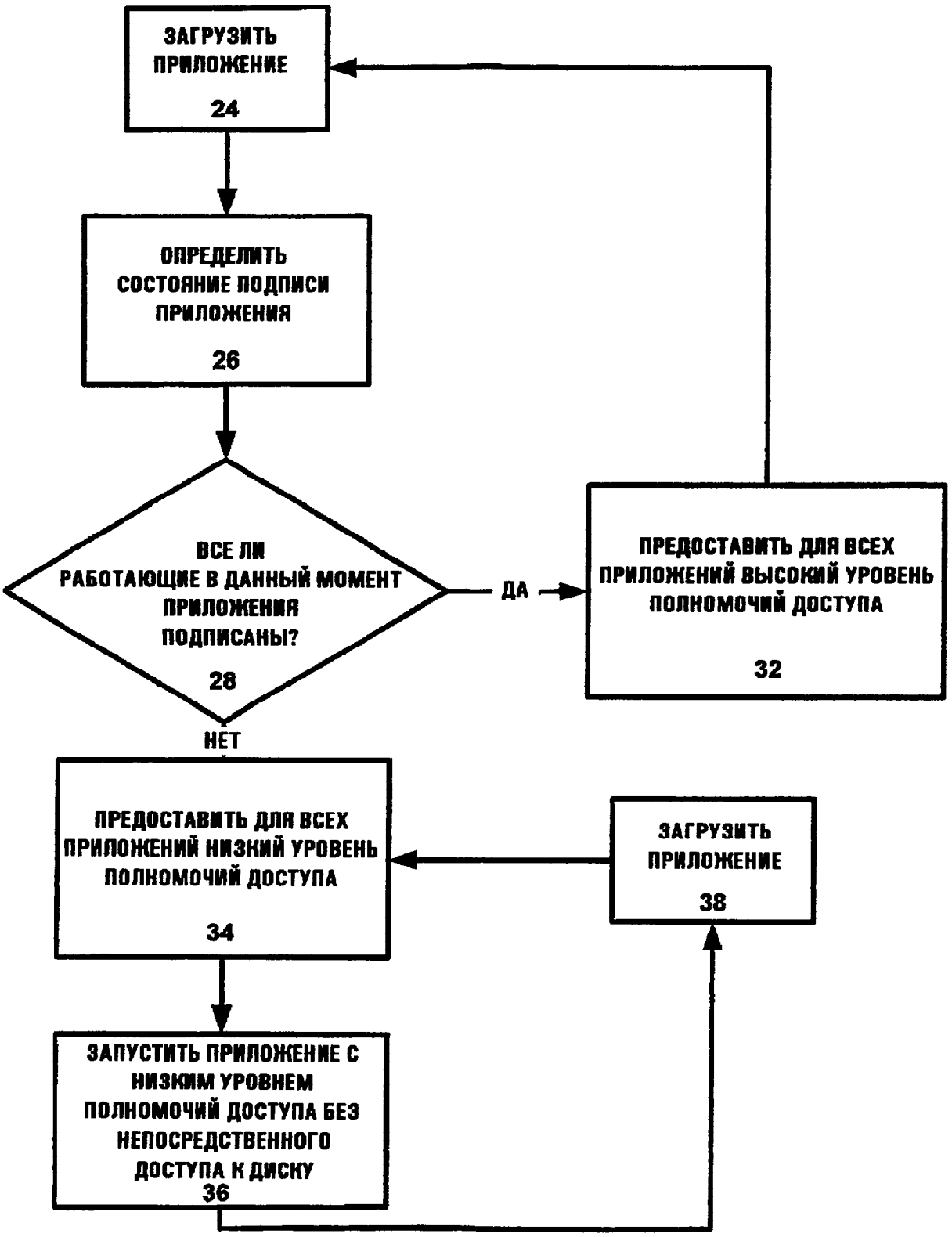
(54) БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЯ В СРЕДЕ ИНТЕРАКТИВНОГО НОСИТЕЛЯ

(57) Реферат:

Заявленное изобретение относится к системам безопасности для управления полномочиями приложений без подписи в области интерактивных мультимедийных приложений. Технический результат - обеспечиваются адекватные меры обеспечения безопасности. Система устанавливает структуру для обеспечения безопасности приложения, включая в себя систему подписи, и дополнительно определяет форматы файла, которые поддерживают безопасность. Подписанным приложениям предоставляют высокий уровень полномочий доступа, в то время как не подписанным приложениям предоставляют низкий уровень полномочий доступа. Комбинация подписанных и не подписанных приложений, например, на диске, обеспечивает низкий уровень полномочий для всех приложений, как подписанных, так и не подписанных. 2 н. и 15 з.п. ф-лы, 1 табл., 4 ил.

RU 2421807 C2

RU 2421807 C2



ФИГ.2

RU 2421807 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 421 807** (13) **C2**

(51) Int. Cl.
G06F 21/20 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2007147634/08, 22.06.2006**

(24) Effective date for property rights:
22.06.2006

Priority:
(30) Priority:
01.07.2005 US 60/695,944
15.02.2006 US 11/354,800

(43) Application published: **27.06.2009** Bull. 18

(45) Date of publication: **20.06.2011 Bull. 17**

(85) Commencement of national phase: **20.12.2007**

(86) PCT application:
US 2006/024034 (22.06.2006)

(87) PCT publication:
WO 2007/005281 (11.01.2007)

Mail address:
129090, Moskva, ul. B.Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
Kh'JuZ Ml. Robert K. (US),
ARRUI Iv (US)

(73) Proprietor(s):
MAJKROSOFT KORPOREJShN (US)

RU 2421807 C2

(54) SAFETY OF APPLICATION IN INTERACTIVE CARRIER ENVIRONMENT

(57) Abstract:

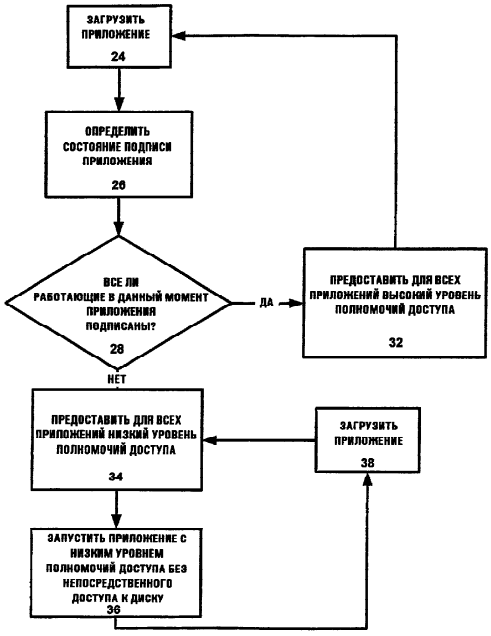
FIELD: information technologies.

SUBSTANCE: system establishes a structure to ensure safety of application, including a system of signature, and additionally defines formats of a file, which maintain safety. Subscribed applications are provided with a high level of access authorities, while unsubscribed applications are given a low level of access authorities. Combination of subscribed and unsubscribed applications, for instance, on a disk, ensures a low level of authorities for all applications, both subscribed and unsubscribed.

EFFECT: invention ensures adequate measures of safety provision.

17 cl, 4 dwg

RU 2421807 C2



ФИГ.2

RU 2421807 C2

RU 2421807 C2

Заявление о родственной заявке

В данной заявке заявлено преимущество предварительной заявки №60/695,944, поданной 1 июля 2005 г., которая приведена здесь в качестве ссылочного материала.

Уровень техники

Некоторые мультимедийные системы воспроизведения обеспечивают ограниченное интерактивное графическое изображение во время воспроизведения звука/видеоизображения. Большие возможности интерактивных систем воспроизведения представляют большие возможности для неправомерных действий. Очень важно поддерживать безопасность системы воспроизведения, защищая ее от вирусов, шпионских программ, другого злоумышленного программного обеспечения. Злоумышленное программное обеспечение может привести к неправильной работе интерактивной системы воспроизведения или может собирать и передавать частную информацию пользователя. Кроме того, интерактивная система воспроизведения может быть подключена к сети. Программное средство или информация пользователя могут распространяться через системы воспроизведения в другие вычислительные системы, подключенные к сети. Вследствие этого, важно, чтобы интерактивная система воспроизведения включала в себя адекватные меры обеспечения безопасности.

Сущность изобретения

Предложена система безопасности, которая управляет полномочиями приложений без подписи в области интерактивных мультимедийных приложений. Интерактивные мультимедийные приложения представляют собой среду, в которой приложения обычно управляют мультимедийными объектами, включающими в себя графику, звук и видеоизображение в соответствии с событиями ввода пользователя на синхронизированной основе в режиме реального времени, с точным соответствием кадрам. Здесь приложения называются "iHD" приложениями, поскольку они относятся к носителям DVD (цифровой универсальный диск), обеспечивающим высокую разрешающую четкость изображения. Однако в общем случае раскрытая система безопасности применима к другим интерактивным мультимедийным средам.

Система, в частности, относится к безопасности приложения, а не к безопасности содержимого, и устанавливает основу для безопасности приложений, включая в себя систему подписи, и дополнительно предоставляет форматы файла, которые поддерживают безопасность. Интерактивные мультимедийные приложения, работающие в интерактивной системе воспроизведения (которая воплощена в виде отдельного устройства, или, в качестве альтернативы, в виде программного приложения, работающего, например, в персональном компьютере), могут быть подписанными или не подписанными.

Подписанные приложения обеспечивают возможность фактически неограниченного применения. Не подписанные приложения значительно ограничены в своем доступе. Кроме того, если подписанные и не подписанные приложения работают одновременно, обоим им предоставляется только уровень безопасности и полномочия доступа не подписанного приложения. Не подписанные приложения позволяют обеспечить для дисков собственного изготовления возможность создания богатых интерактивных свойств, но они ограничивают доступ к сети, например, Интернет, и доступ к важной информации, сохраненной в системе воспроизведения, для уполномоченных сторон.

В подписанных приложениях могут быть предусмотрены специальные форматы файла, которые позволяют определять статус подписи, без необходимости анализа всего файла.

Краткое описание чертежей

На фиг.1 показана блок-схема последовательности операций, иллюстрирующая способ присвоения полномочий для приложений, когда состояние подписи приложений детектируют с диска.

На фиг.2 показана блок-схема последовательности операций, иллюстрирующая способ присвоения полномочий для приложений, когда состояние подписи приложений детектируют при загрузке в систему воспроизведения.

На фиг.3 показана блок-схема последовательности операций, иллюстрирующая создание директории, открываемой ключом-идентификатором автора.

На фиг.4 схематично представлен файл приложения.

Подробное описание изобретения

Интерактивные мультимедийные приложения представляют собой такие приложения, в которых они реагируют на события пользователя. Пример представляет собой меню, воплощенное в приложении, доступное для пользователя, в котором пользователь подает входные команды, которые заставляют приложение изменять свое состояние. В таком случае интерактивность обеспечивается тем, что графические меню представляют так, что на их фоне происходит воспроизведение видеоизображения, например, на уровне z=0, в режиме реального времени, синхронно с кадрами. Интерактивность может привести, например, к изменениям в отображении видеопотока.

Например, фоновое видеоизображение может представлять собой кинофильм высокой четкости. Наложенное графическое изображение может представлять собой часть комментария кинорежиссера этого фильма, схематично представляющую, например, различные места расположения фотокамер, наложенные поверх самой сцены. Пользователь может, используя пульт дистанционного управления, переключать точку обзора для любого из этих мест расположения камеры.

Как указано выше, большие возможности, предоставляемые интерактивными системами воспроизведения, создают большие возможности для неправомерных действий. Злоумышленные программные средства могут привести к неисправной работе системы воспроизведения или могут собирать и передавать частную информацию пользователя.

В существующей системе интерактивные приложения, предназначенные для использования в системе воспроизведения, могут быть подписанными или не подписанными. Подписанные приложения представляют собой такие приложения, которые унаследовали корневой сертификат от надежного корневого центра (например, киностудии) и которые считаются надежными.

Подписанные приложения получают полномочия высокого уровня доступа. Такие практически неограниченные полномочия позволяют обеспечивать доступ, например, к сети, вводу/выводу файлов, API (ИПП, интерфейс прикладного программирования) безопасности и диагностики, и позволяют обращаться к постоянному накопителю для сохранения и извлечения данных, которые должны сохраняться неизменными при каждом вызове приложения.

Неподписанные приложения, с другой стороны, получают полномочия низкого уровня доступа. Им отказано в доступе к функциям такого типа, которые предоставляются при высоком доступе. Они могут быть ограничены использованием языка разметки, а также, например, некоторых объектов из следующих примерных API в ECMAScript: XML (РЯР, расширяемый язык разметки гипертекста) (без функций ввода/вывода); глобализация; функции рисования, ассоциированные с графическими

элементами; и операции ввода пользователя.

Функции этого уровня запрещают доступ к каким-либо сетям, системам безопасности или вводу/выводу файлов. Любая попытка вызова функции из-за пределов упомянутых выше пространств имен или ресурсов загрузки с несъемного локального накопителя может привести к исключению, которое прекратит работу приложения.

В одном варианте воплощения набор прикладных программ присутствует на мультимедийном диске, например, HD-DVD, и он же используется для работы интерактивных графических и видеоприложений. Как показано на фиг.1, мультимедийный диск устанавливают в систему воспроизведения (этап 12). Система воспроизведения, которая может представлять собой компьютерную систему общего назначения или более специализированную систему - мультимедийный центр, определяет состояние подписи приложений на носителе (этап 14). Если состояние подписи всех приложений определено (этап 16), как подписанное, тогда всем приложениям предоставляют полномочия высокого уровня доступа (этап 18). Если состояние подписи любого одного из приложения будет определено, как не подписанное, тогда всем приложениям предоставляются полномочия низкого уровня доступа (этап 22). Таким образом, если работает не подписанное приложение, все одновременно работающие приложения, как подписанные, так и не подписанные, могут быть ограничены до уровня разрешений не подписанного приложения. Это предотвращает использование не подписанным приложением полномочий одновременно работающего подписанного приложения.

В другом варианте воплощения аналогичный способ можно применять непосредственно к приложениям, загруженным в систему воспроизведения. Как показано на фиг.2, приложение может быть загружено в систему воспроизведения (этап 24). Затем определяют состояние подписи приложения (этап 26). Если состояние подписи будет определено (этап 28), как подписанное, тогда приложение может работать с полномочиями с высоким уровнем доступа (этап 32). Однако если состояние подписи определено (этап 28) как не подписанное, тогда приложение работает с полномочиями с низким уровнем доступа (этап 34). В этом случае приложение работает непосредственно с носителя (этап 36), например, диска. Это обеспечивает улучшенную безопасность, поскольку для всех не подписанных приложений в этом случае предотвращается воспроизведение или загрузка ресурсов из локального несъемного накопителя системы воспроизведения. Если загружены дополнительные приложения (этап 38), тогда может быть проверено или нет состояние их подписи: обычно им будет предоставлен низкий уровень доступа (этап 34). Если приложение подписано и, таким образом, ему предоставляются полномочия высокого уровня доступа, и затем позднее загружается другое приложение, и оно является не подписанным, тогда приложение с высоким уровнем доступа понижают до низкого уровня доступа.

Как показано на фиг.3, для подписанных приложений система воспроизведения может включать в себя использование набора идентификаторов автора, которые детектируют (этап 44) при вводе носителя (этап 42) в систему воспроизведения. Таким образом, каждый носитель или приложение, могут быть ассоциированы с идентификатором автора, который уникально идентифицирует авторов содержимого, что является особенно важным для обеспечения безопасности приложений на постоянном накопителе, то есть, таких приложений, которые могут обращаться к несъемному накопителю для сохранения и извлечения данных, которые должны

сохраняться постоянными при каждом вызове приложения.

Идентификатор автора затем ассоциируют с созданием (этап 46) директории, ассоциированной с этим идентификатором автора. Приложение с этого носителя может обращаться только к директории, соответствующей ее идентификатору автора на несъемном накопителе. Файловая система, как ее видит приложение, расположена с корнем в этой директории. Хотя приложение может управлять поддиректориями, оно не может выходить за пределы своей корневой директории и видеть данные другого автора.

Идентификатор автора может быть ассоциирован либо с диском, включающим в себя все приложения на этом диске, или с отдельным приложением, которое находится либо на этом диске, распределено по нескольким дискам, или загружено другим способом в систему воспроизведения, например, путем загрузки через Интернет. Кроме того, с данным носителем может быть ассоциирован один идентификатор автора, но данные идентификатора этого автора можно найти на множестве носителей. В другом варианте воплощения может использоваться идентификатор, связанный с ключом, которым подписано приложение. Если предположить, что разные приложения могут быть подписаны разными лицами на одном носителе, такой вариант выполнения приводит к еще большему разделению накопителя. При использовании цепочки сертификатов вместо последней подписи такое положение дополнительно усугубляется.

СТРУКТУРА ПРИЛОЖЕНИЯ

Ниже будет описана структура подписанного приложения. Как показано на фиг.4, подписанное приложение 50 может включать в себя файл 52 объявления и, по меньшей мере, один файл 54 ресурсов. Файл 52 объявления подписан подписью автора и сертификатом и аутентифицирует все ресурсы, на которые он ссылается.

Приложение может иметь свой файл 52 объявления и все файлы 54-58 ресурсов, упакованные в несжатый архив 48. Формат файла для архива 48 даже не должен поддерживать шифрование. Файл 48 архива, по существу, представляет собой контейнер и обычно не требует независимой подписи. Файл 52 объявления может ссылаться на каждый из файлов 54-58 ресурсов интерактивного приложения. Архитектура архива 48 может быть определена так, что архив 48 может быть эффективно распределен по потокам, например, подписанный файл 52 объявления может быть первым файлом в архиве 48, что обеспечивает возможность проверки подписи без считывания всего архива. Последующие версии формата архива могут обладать обратной совместимостью с предыдущими.

Аутентификация данных в архиве 48 может быть обеспечена при использовании, например, подписи XML, которая определена в соответствии с RFC 3275.

ФОРМАТ ФАЙЛА ОБЪЯВЛЕНИЯ

В одном примере в формате подписанного файла 52 объявления может использоваться поднабор Рекомендаций W3C для Синтаксиса XML-подписи и обработки, определенных RFC 3275. Таким образом, следующий поднабор элементов может быть включен и могут поддерживаться:

ds: Signature
ds: SignatureValue
ds: SignatureType
ds: Reference
ds: Reference/ds: DigestValue

Другие элементы могут быть определены системой. Значения дайджеста для

каждого элемента ресурса, включенные в объявление, могут быть представлены как список элементов ds:Reference.

СЕРТИФИКАТЫ И ПОДПИСИ

В качестве примера, требуемый тип сертификата может представлять собой, например, X.509. Способ подписи, определенный в соответствии с ds:SignatureMethod, может представлять собой RSA-SHA1. Способ приведения к классическому виду может быть специфицирован как Exclusive XML Canonicalization 1.0. Метод дайджеста может быть тем же, что и метод подписи, RSA-SHA1. Информация ключа может быть логически выведена системой из идентификатора носителя или локального накопителя, с которого было загружено приложение.

СПИСКИ ОТМЕНЫ СЕРТИФИКАТОВ

Для обеспечения механизма отмены и замены скомпрометированных приложений автор каждого интерактивного видео- и графического приложения может включать список отмены содержимого ("CRL", COC), в котором представлены в виде списка значения дайджеста упакованного файла отмененных приложений. Такой CRL может быть включен в отдельный файл. Этот файл содержит список упакованных дайджестов подписи, которые были отменены, и подпись автора содержимого, который создал этот диск. Если предположить, что исходная подпись автора каждого отмененного приложения соответствует подписи файла CRL, дайджесты приложений, представленные в списке, будут сохранены в области с ограниченным доступом провайдера содержимого локального накопителя, и запуск этих приложений больше не будет разрешен. Если CRL включен в приложение, ему может быть предоставлено распознаваемое имя, такое как Revocation.xml.

Автор приложения может захотеть заменить отмененное приложение новой версией. Это может быть выполнено несколькими разными путями. Для интерактивных приложений, работающих в проигрывателях, подключенных к Интернет, может быть обеспечена проверка на их домашних серверах наличия обновленных списков воспроизведения или архивов интерактивных видео- и графических изображений, которые определяют вновь загруженные приложения. В качестве альтернативы, носитель, отменяющий приложение, также мог бы сам предоставлять замену.

В следующей таблице описан один возможный формат архивного файла, вместе с комментариями, описывающими поля. Следует отметить, что можно использовать множество других форматов. В этой таблице для представления типов используются сокращения: Uin представляет целое число без знака из *n* битов. Например, Ui8 представляет собой целое число без знака размером 8 битов, и Ui32 представляет собой число размером 32 бита. Массив типа обозначен с использованием квадратных скобок, и длина массива обозначена между этими скобками. Если длина зависит от предыдущего поля, тогда название поля, или более короткое название, обозначенное в этом поле, можно использовать для обращения к значению в этом поле. Шестнадцатеричные значения обозначены с использованием условных обозначений 0xdd. Все строки переменной длины и, следовательно, имена ресурсов, могут быть кодированы с использованием UTF-8, с применением обозначения строки Паскаля (длиной 8 бит, после которой следуют байты).

	Поле	Тип	Комментарий
Заголовок архива	Системный код	Ui8[5]	значения из 5 байт должны быть: 0x69, 0x48, 0x44, 0x61,0x72.
	Версия	Ui8	Версия формата. Значение должно быть 0x01.

Каталог ресурса	Элемент ресурса № 1	Длина элемента ресурса	Ui16	Длина элемента этого ресурса.
		Смещение ресурса	Ui32	Смещение в байтах ресурса в блоке данных ресурса.
		Длина ресурса	Ui32	Длина ресурса в байтах.
		Проверочная сумма ресурса	Ui32	Проверочная сумма CRC-32 байтов ресурса.
		Тип ресурса		
		Длина имени ресурса	Ui8	RNL (ДНР)
		Имя ресурса	Ui8[RNL]	Имя ресурса в файловой системе.
	Элемент ресурса № n	Длина элемента ресурса	Ui16	Длина элемента этого ресурса.
		Смещение ресурса	Ui32	Смещение в байтах ресурса в блоке данных ресурса.
		Длина ресурса	Ui32	Длина ресурса в байтах.
		Проверочная сумма ресурса	Ui32	Проверочная сумма CRC-32 байтов ресурса.
		Тип ресурса		
		Длина имени ресурса	Ui8	RNL
		Имя ресурса	Ui8[RNL]	Имя ресурса в файловой системе.
		Все данные ресурса в непрерывных блоках.		
Блок данных ресурса				

Определенные правила могут применяться для отмеченных выше ресурсов приложения. Например, имена ресурсов должны представлять собой имена в файловой системе или логические URI (УИР, унифицированный идентификатор ресурса). Директорию, в которой будет развернут архивный файл, можно рассматривать как корневую директорию для этой файловой системы во время такого разворачивания. Таким образом, все имена будут составлены относительно этой директории, поэтому абсолютные пути будут вести себя так же, как относительные пути. Если имя будет указывать на местоположение за пределами этой директории, это имя и элемент можно рассматривать как недействительные.

В следующих разделах представлена более подробная информация о различных полях и секциях в представленном выше примерном архивном файле.

Архивный заголовок

Поле системного кода

Для уникальной идентификации архивов используется - "системный код". Он может состоять из строки "iHDar", то есть, архив iHD, кодированный как последовательность значений из 5 знаков в UTF-8, ASCII (АСКОИ, Американский стандартный код обмена информацией) и т.д., то есть, 0x69, 0x48, 0x44, 0x61, 0x72.

Поле версии

Поле версии позволяет считывателю архива считывать разные версии формата архива. По этому полю версии можно определить, что можно ожидать в разных секциях файла, и, таким образом, считывать информацию, которая не представлена в некоторых версиях формата файла. Значение этого поля может быть, например, 0x01. Будущие версии могут иметь значения от 0x02 до 0xff.

Каталог ресурсов и элементы ресурса

Каталог ресурсов включает в себя множество элементов ресурса. Каждый элемент представлен в одном и том же формате.

Длина элемента ресурса

Представляет собой длину в байтах элемента самого ресурса. Это значение используется считывателями, которые считывают формат, версию которого они не понимают. Если предположить, что архив, записанный с использованием версии 2 формата, просматривается считывателем, выполненным для версии 1, такой

считыватель может считать поля, которые он знает, и затем может перейти к следующему элементу ресурса, поскольку он знает длину текущего элемента.

Смещение ресурса

Обозначает смещение в байтах ресурса в блоке данных ресурса. Смещение первого ресурса составляет 0x0000.

Длина ресурса

Представляет собой длину ресурса в байтах.

Если ресурсы A и B расположены непрерывно в архивном файле, тогда смещение ресурса для B равно сумме смещения ресурса A и длины ресурса.

Проверочная сумма ресурса

Представляет проверочную сумму CRC-32 ресурса, в соответствии с определением ISO 3309. Следует отметить, что эту проверочную сумму следует использовать только для простой проверки целостности ресурса, переданного через ненадежную среду. Поскольку проверочная сумма CRC-32 не защищена ни ключом, ни имеет защиты от коллизий, ее не следует использовать с целью аутентификации. Если требуется аутентифицировать ресурсы, можно использовать механизм подписи, описанный выше.

Тип ресурса

Представляет собой тип MIME (МРЭП, многоцелевые расширения электронной почты в Интернет) ресурса.

Длина имени ресурса

Представляет собой длину имени ресурса в байтах. Имя ресурса следует немедленно после этого поля.

Имя ресурса

Представляет собой имя самого ресурса.

Блок данных ресурса

Блок данных ресурса содержит все байты для ресурсов, в порядке, который представлен в каталоге ресурсов. Между двумя ресурсами обычно нет какого-либо явного разделения, поскольку значения их смещения и длины представляют собой хорошо известные величины.

Система может быть описана в общем контексте исполняемых компьютером инструкций, таких как программные модули, выполняемые компьютером. Обычно программные модули включают в себя процедуры, программы, объекты, компоненты, структуры данных и т.д., которые выполняют определенные задачи или воплощают определенные абстрактные типы данных. Система и способ также могут быть выполнены на практике в распределенных вычислительных средах, задачи в которых выполняются с помощью устройств дистанционной обработки, соединенных через сеть передачи данных. В распределенной вычислительной среде программные модули могут быть расположены на накопителе информации, как локальном, так и в удаленном компьютере, включая запоминающие устройства.

Инструкции, которые выполняют способ и систему, могут быть сохранены на разных считываемых компьютером носителях. Считываемый компьютером носитель может представлять собой любой доступный носитель, к которому может обращаться компьютер, и включает в себя как энергозависимый, так и энергонезависимый носитель, съемный и несъемный носитель. В качестве примера и не для ограничения, считываемые компьютером носители могут содержать компьютерный носитель информации и среду передачи данных. Компьютерные носители информации включают в себя как энергозависимые, так и энергонезависимые, съемные и

несъемные носители, воплощенные с использованием любого способа или технологии, предназначенные для сохранения информации, такой как считываемые компьютером инструкции, структуры данных, программные модули или другие данные. Носители информации компьютера включают в себя, но без ограничений, ОЗУ, ПЗУ, СППЗУ, запоминающее устройство типа флэш или запоминающее устройство на основе другой технологии, CD-ROM, цифровые универсальные диски (DVD) или другие оптические дисковые накопители; магнитные кассеты, магнитную ленту, накопитель на магнитном диске или другие устройства магнитных накопителей, или любой другой носитель, который может использоваться для сохранения требуемой информации и к которому может обращаться компьютер. Среды передачи данных обычно воплощают считываемые компьютером инструкции, структуры данных, программные модули или другие данные, в виде модулированного сигнала данных, такого как колебания несущей частоты или другой механизм транспортировки, и включает в себя любую среду передачи информации. Термин "модулированный сигнал данных" обозначает сигнал, одна или больше характеристик которого установлена или изменена таким образом, чтобы кодировать информацию в этом сигнале. В качестве примера, и не для ограничения, среда передачи данных включает в себя проводную среду, такую как кабельная сеть или прямое кабельное соединение, и беспроводную среду, такую как акустическая, РЧ, инфракрасная и другая беспроводная среда. Комбинация любой из упомянутых выше также должна быть включена в объем считываемого компьютером носителя информации.

Хотя система описана в связи с примерной средой вычислительной системы, включающей в себя компьютер, такая система может работать с множеством других сред или конфигураций вычислительной системы общего назначения или специального назначения. Среда вычислительной системы не предназначена для какого-либо ограничения объема использования или функциональности. Кроме того, среду вычислительной системы не следует интерпретировать как имеющую какую-либо зависимость, или как среду, к которой предъявлено требование, относящееся к любому одному или комбинации компонентов, иллюстрируемых в примерной рабочей среде. Примеры хорошо известных вычислительных систем, сред и/или конфигураций, которые могут быть пригодны для использования, включают в себя, но не ограничиваются этим, персональные компьютеры, компьютеры - серверы, карманные компьютеры или переносные устройства, многопроцессорные системы, системы на основе микропроцессора, телевизионные приставки, программируемые бытовые электронные устройства, мобильные телефоны, сетевые ПК, миникомпьютеры, большие вычислительные машины, распределенные вычислительные среды, которые могут включать в себя любые из представленных выше систем или устройств, и т.п.

Системы и способы, описанные здесь, могут быть воплощены с использованием программных и/или аппаратных средств с использованием методик, которые хорошо известны в данной области техники.

Порядок выполнения или работы способов, представленных и описанных здесь, не является существенным, если только не указано другое. Таким образом, элементы способа могут быть выполнены в любом порядке, если только не указано другое, и способ может включать в себя большее или меньшее количество элементов, чем описано здесь.

При вводе элементов в соответствии с настоящим изобретением или его вариантом (вариантами) выполнения, считается, что артикли "a", "an", "the" и "said" обозначают, что имеется один или больше элементов. Термины "содержащий", "включающий в

себя" и "имеющий" следует понимать во включительном смысле, и они означают, что могут присутствовать дополнительные элементы, помимо представленных элементов.

Различные изменения могут быть выполнены в описанных выше конструкциях, продуктах и способах, без выхода за пределы объема изобретения, при этом предполагается, что предмет, составляющий содержание представленного выше описания, следует интерпретировать, как иллюстративный, а не как ограничительный.

Хотя предмет изобретения был описан с использованием формулировок, специфичных для структурных свойств и/или методологических действий, следует понимать, что предмет изобретения, определенный в приложенной формуле изобретения, не обязательно ограничен конкретными свойствами или действиями, описанными выше. Скорее определенные свойства и действия, описанные выше, раскрыты в форме примера, воплощающего формулу изобретения.

Формула изобретения

1. Способ обеспечения безопасности приложения в интерактивной мультимедийной среде, содержащий этапы, на которых

a) принимают приложение, содержащее инструкции для синхронного управления графикой, аудио и видео мультимедийными объектами в ответ на события пользовательского ввода, причем упомянутые инструкции не обеспечивают при их исполнении реализацию политики безопасности для упомянутого приложения;

b) определяют, имеет ли приложение ассоциированную цифровую подпись, причем определение содержит этап, на котором считывают файл объявления, ассоциированный с приложением, и устанавливают, является ли объявление подписанным с использованием подписи автора и сертификата;

c) если обнаруживают действительную цифровую подпись ассоциированную с приложением, то исполняют приложение с помощью процессора, ассоциированного с мультимедийным проигрывателем, для синхронного управления графикой, аудио и видео мультимедийными объектами в ответ на пользовательский ввод, причем результатом исполнения приложения является получение приложением доступа к источнику на локальном накопителе в мультимедийном проигрывателе и к сетевому ресурсу;

d) если не обнаруживают действительную цифровую подпись, ассоциированную с приложением, то исполняют приложение с помощью процессора, ассоциированного с мультимедийным проигрывателем, для синхронного управления графикой, аудио и видео мультимедийными объектами в ответ на события пользовательского ввода, однако запрещают исполняемому приложению доступ к источнику на локальном накопителе в мультимедийном проигрывателе и к сетевому ресурсу;

e) принимают еще одно приложение;

f) определяют, имеет ли другое приложение ассоциированную цифровую подпись; и

g) если не обнаруживают действительную цифровую подпись, ассоциированную с упомянутым приложением, или действительную цифровую подпись, ассоциированную с упомянутым другим приложением, запрещают обоим приложениям доступ к источнику на локальном накопителе в мультимедийном проигрывателе и к сетевому ресурсу;

h) если обнаруживают действительную цифровую подпись, ассоциированную с упомянутым приложением, и действительную цифровую подпись, ассоциированную с упомянутым другим приложением, разрешают обоим приложениям доступ к источнику на локальном накопителе в мультимедийном проигрывателе и к сетевому

ресурсу.

2. Способ по п.1, дополнительно содержащий этап, на котором, если обнаруживают действительную цифровую подпись, ассоциированную с приложением, то разрешают исполняемому приложению доступ к вводу/выводу файлов и интерфейсу прикладного программирования (API) безопасности и диагностики мультимедийного проигрывателя.

3. Способ по п.1, в котором приложение содержит архив, в котором помещен файл объявления и, по меньшей мере, один файл ресурсов, и в котором файл объявления представляет собой первый файл в архиве.

4. Способ по п.3, в котором архив имеет такой формат, что архив может подвергаться эффективной потоковой обработке.

5. Способ по п.1, в котором, если обнаруживают действительную цифровую подпись, ассоциированную с приложением, то приложение включает в себя подписанный корневой сертификат, список отмены содержимого или идентификатор автора.

6. Способ по п.1, в котором источник на локальном накопителе представляет собой директорию, сопоставленную с идентификатором автора.

7. Способ по п.1, в котором этап, на котором, если не обнаруживают действительную цифровую подпись, ассоциированную с приложением, запрещают исполняемому приложению доступ к источнику на локальном накопителе в мультимедийном проигрывателе, содержит запрещение доступа к вводу/выводу файлов и API безопасности и диагностики.

8. Способ по п.1, дополнительно содержащий этап, на котором, если не обнаруживают действительную цифровую подпись, ассоциированную с приложением, тогда разрешают доступ к использованию языка разметки и использованию объектов, содержащих расширяемый язык разметки гипертекста (XML) без функции ввода/вывода, глобализацию, функции рисования и функции пользовательского ввода.

9. Способ по п.1, дополнительно содержащий этап, на котором, если не обнаруживают действительную цифровую подпись, ассоциированную с приложением, и приложение принимают с оптического диска, тогда запускают приложение только с оптического диска.

10. Способ по п.1, в котором этап приема приложения содержит прием приложения через мультимедийный диск, читаемый мультимедийным проигрывателем.

11. Мультимедийная система воспроизведения для приложений, содержащих инструкции для синхронного управления графикой, аудио и видео мультимедийными объектами в ответ на пользовательский ввод, причем упомянутые инструкции не обеспечивают при их исполнении реализацию политики безопасности для упомянутого приложения, при этом система содержит

сетевой ресурс;

источник на локальном накопителе;

устройство, предназначенное для приема по меньшей мере первого приложения;

процессор, предназначенный для определения имеет ли какое-либо из принятых приложений ассоциированную цифровую подпись, причем,

если принимают только первое приложение и если обнаруживают действительную цифровую подпись, ассоциированную с первым приложением, то исполняют первое приложение с помощью процессора, ассоциированного с мультимедийным проигрывателем, для синхронного управления графикой, аудио и видео мультимедийными объектами в ответ на события пользовательского ввода, причем

результатом исполнения первого приложения является получение приложением доступа к источнику на локальном накопителе в мультимедийном проигрывателе и к сетевому ресурсу;

если принимают только первое приложение и если не обнаруживают действительную цифровую подпись, ассоциированную с первым приложением, то исполняют первое приложение с помощью процессора, ассоциированного с мультимедийным проигрывателем, для синхронного управления графикой, аудио и видео мультимедийными объектами в ответ на события пользовательского ввода, однако запрещают исполняемому первому приложению доступ к источнику на локальном накопителе в мультимедийном проигрывателе и к сетевому ресурсу;

если обнаруживают действительную цифровую подпись, ассоциированную с первым приложением, и действительную цифровую подпись, ассоциированную со вторым приложением, причем упомянутое обнаружение содержит этап, на котором считывают файл объявления, ассоциированный с приложением и устанавливают, является ли объявление подписанным с использованием подписи автора и сертификата, то исполняют первое приложение и второе приложение с помощью процессора для синхронного управления графикой, аудио и видео мультимедийными объектами в ответ на события пользовательского ввода, и разрешают обоим приложениям доступ к источнику на локальном накопителе в мультимедийном проигрывателе и к сетевому ресурсу;

если не обнаруживают действительную цифровую подпись, ассоциированную с первым приложением, или действительную цифровую подпись, ассоциированную со вторым приложением, то исполняют первое приложение и второе приложение с помощью процессора для синхронного управления графикой, аудио и видео мультимедийными объектами в ответ на события пользовательского ввода, однако запрещают доступ к источнику на локальном накопителе в мультимедийном проигрывателе и к сетевому ресурсу.

12. Система по п.11, в которой процессор определяет, имеет ли приложение ассоциированную цифровую подпись, путем считывания файла объявления, ассоциированного с приложением, и определения, является ли объявление подписанным с использованием подписи автора и сертификата.

13. Система по п.12, в которой приложение содержит архив, который содержит файл объявления и, по меньшей мере, один файл ресурсов, и в котором файл объявления представляет собой первый файл в архиве.

14. Система по п.11, в которой, если состояние подписи представляет собой "подписано", тогда приложение включает в себя подписанный корневой сертификат, список отмены содержимого или идентификатор автора.

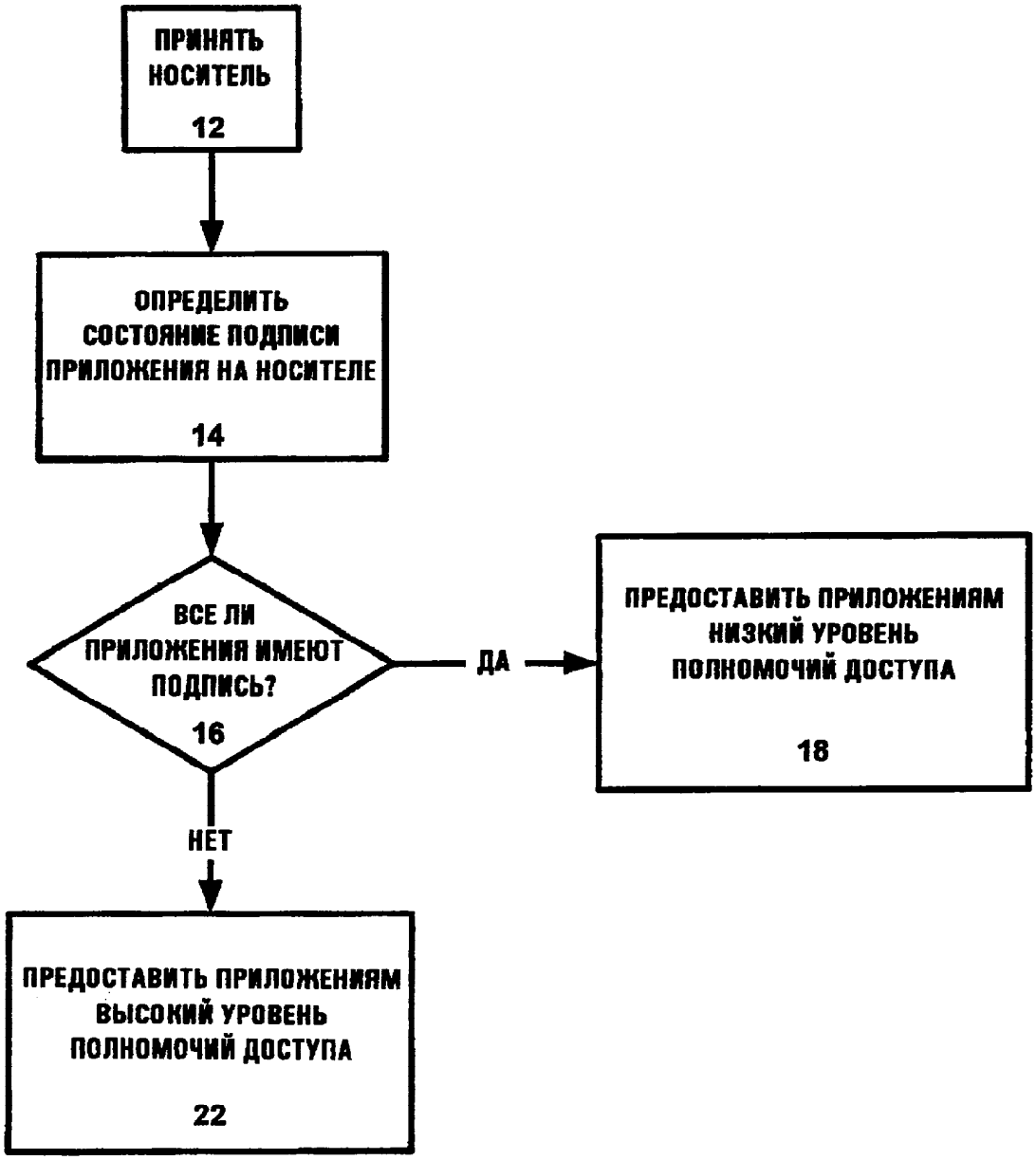
15. Система по п.14, в которой источник на локальном накопителе находится в директории, сопоставленной с идентификатором автора.

16. Система по п.11, в которой, если обнаруживают действительную цифровую подпись, ассоциированную с первым приложением, и действительную цифровую подпись, ассоциированную со вторым приложением, тогда обоим приложениям разрешают доступ к вводу/выводу файлов и к API безопасности и диагностики.

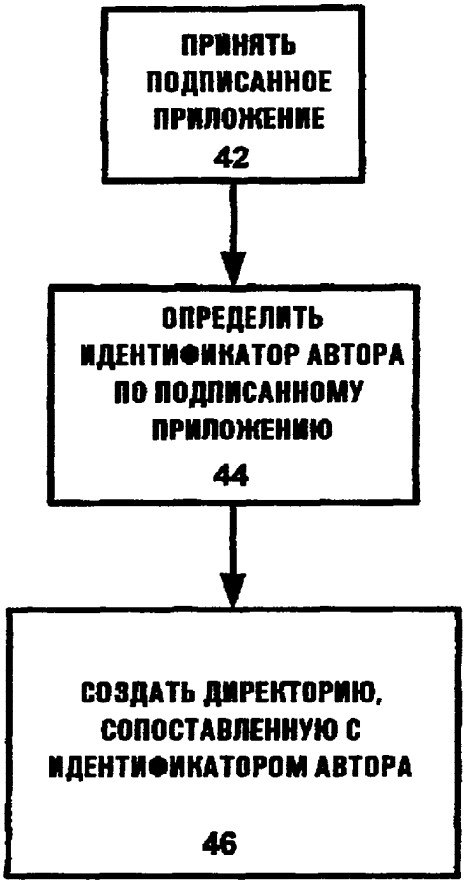
17. Система по п.11, в которой, если не обнаруживают действительную цифровую подпись, ассоциированную с первым приложением, или действительную цифровую подпись, ассоциированную со вторым приложением, тогда для первого и второго приложений

а) запрещают доступ к вводу/выводу файлов и API безопасности и диагностики; или

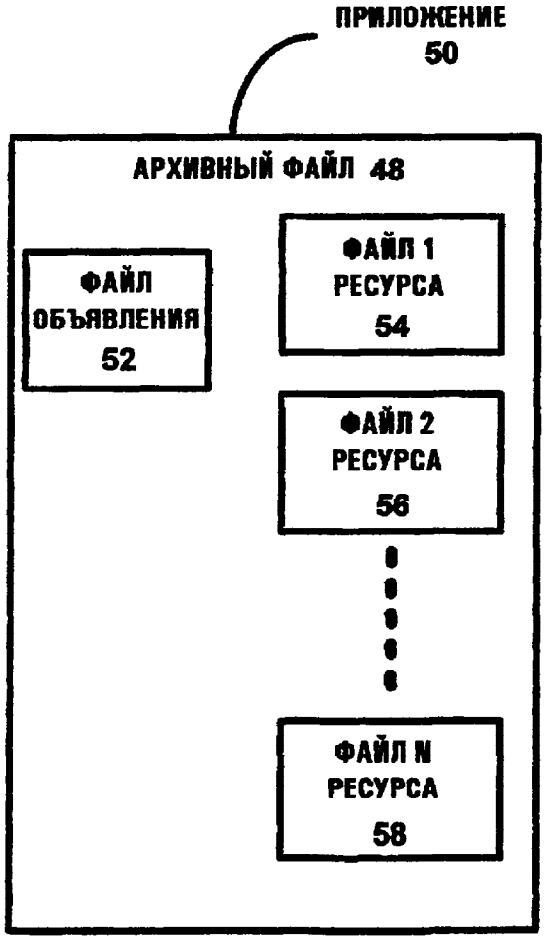
b) разрешают доступ для использования языка разметки и использования объектов, содержащих XML без функции ввода/вывода, глобализацию, функции рисования и операции пользовательского ввода.


ПРИНЯТЬ НОСИТЕЛЬ
12
ОПРЕДЕЛИТЬ СОСТОЯНИЕ ПОДПИСИ ПРИЛОЖЕНИЯ НА НОСИТЕЛЕ
14
ВСЕ ЛИ ПРИЛОЖЕНИЯ ИМЕЮТ ПОДПИСЬ?
16
ДА
ПРЕДОСТАВИТЬ ПРИЛОЖЕНИЯМ НИЗКИЙ УРОВЕНЬ ПОЛНОМОЧИЙ ДОСТУПА
18
НЕТ
ПРЕДОСТАВИТЬ ПРИЛОЖЕНИЯМ ВЫСОКИЙ УРОВЕНЬ ПОЛНОМОЧИЙ ДОСТУПА
22

ФИГ.1


ПРИНЯТЬ ПОДПИСАННОЕ ПРИЛОЖЕНИЕ
42
ОПРЕДЕЛИТЬ ИДЕНТИФИКАТОР АВТОРА ПО ПОДПИСАННОМУ ПРИЛОЖЕНИЮ
44
СОЗДАТЬ ДИРЕКТОРИЮ, СОПОСТАВЛЕННУЮ С ИДЕНТИФИКАТОРОМ АВТОРА
46

ФИГ.3


ПРИЛОЖЕНИЕ
50
АРХИВНЫЙ ФАЙЛ 48
ФАЙЛ ОБЪЯВЛЕНИЯ 52
ФАЙЛ 1 РЕСУРСА 54
ФАЙЛ 2 РЕСУРСА 56
ФАЙЛ N РЕСУРСА 58

ФИГ.4