РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2005 115 106** (13) **A**

(51) МПК[7] **H 04 L 29/06**

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2005115106/09, 17.10.2003**

(30) Приоритет: **18.10.2002 EP 02257275.4**

(43) Дата публикации заявки: **10.10.2005 Бюл. № 28**

(85) Дата перевода заявки PCT на национальную фазу: **18.05.2005**

(86) Заявка PCT:
IB 03/04608 (17.10.2003)

(87) Публикация PCT:
WO 2004/036870 (29.04.2004)

Адрес для переписки:
129010, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Г.Б. Егоровой

(71) Заявитель(и):
КОНИНКЛЕЙКЕ ФИЛИПС ЭЛЕКТРОНИКС Н.В. (NL)

(72) Автор(ы):
ВАН ДЕН ХЕВЕЛ Себастьян А. Ф. А. (NL),
ЭШЛИ Алексис С. Р. (NL)

(74) Патентный поверенный:
Егорова Галина Борисовна

(54) СПОСОБ, СИСТЕМА, УСТРОЙСТВО, СИГНАЛ И ПРОГРАММНЫЙ ПРОДУКТ ДЛЯ ЗАЩИТЫ МЕТАДАННЫХ В TV-ANYTIME

Формула изобретения

1. Способ обеспечения аутентификации целостности данных и защиты данных, согласно которому множество фрагментов данных защищают сигнатурой, отличающийся тем, что каждый фрагмент данных множества содержит свой собственный однозначно определенный идентификатор, сигнатура содержит ссылки на соответствующие однозначно определенные идентификаторы фрагментов данных множества.

2. Способ по п.1, отличающийся тем, что упомянутое множество защищают несколькими сигнатурами, при этом несколько сигнатур могут исходить из разных источников.

3. Способ по п.1, отличающийся тем, что для каждого фрагмента данных формируют хэш-функцию, и хэш-функции фрагментов данных множества используют для вычисления сигнатуры.

4. Способ по п.1, отличающийся тем, что фрагменты данных выражают на языке XML.

5. Способ по п.1, отличающийся тем, что фрагменты данных образуют метаданные TV-Anytime.

6. Способ по п.1, отличающийся тем, что сигнатуру сохраняют согласно стандарту xmldsig.

7. Способ по п.1, отличающийся тем, что множество фрагментов данных определяют функцией преобразования на супермножестве фрагментов данных.

8. Способ по п.1, отличающийся тем, что перед формированием сигнатуры используют функцию каннолизации.

9. Способ по п.1, отличающийся тем, что ссылки также защищены сигнатурой.

RU 2005115106 A

RU 2005115106 A

10. Способ по п.1, отличающийся тем, что вводят по меньшей мере один индексный файл сигнатур.

11. Способ по п.1, отличающийся тем, что однозначно определенный идентификатор в конкретном фрагменте данных начинается с однозначно определенной идентификации организации, которая сформировала определенный фрагмент данных.

12. Способ по п.11, отличающийся тем, что однозначно определенная идентификация представляет собой DNS-имя организации.

13. Способ по п.1, отличающийся тем, что ссылка сопровождается указателем местоположения, который указывает местоположение фрагмента данных, на который ссылается ссылка.

14. Способ по п.13, отличающийся тем, что указатель местоположения указывает маршрут через данные к фрагменту данных, на который делается ссылка.

15. Способ по п.4, отличающийся тем, что сигнатура включена в XML-документе.

16. Способ по п.4, отличающийся тем, что сигнатура находится в XML-документе упаковщика, содержащем исходный XML-документ данных.

17. Способ по п.4, отличающийся тем, что сигнатура находится в отдельном XML-документе, ссылающемся на первоначальный XML-документ данных.

18. Система (20) для обеспечения аутентификации целостности данных и защиты данных, при этом система выполнена с возможностью приема и обработки фрагментов данных, причем множество фрагментов данных могут быть защищены сигнатурой, и система отличается тем, что содержит средство приема и обработки фрагментов данных множества, при этом каждый фрагмент данных идентифицирован однозначно определенным идентификатором, по меньшей мере одно средство для связи сигнатуры с защищаемыми фрагментами данных множества с использованием их однозначно определенных идентификаторов, средство для проверки сигнатуры, связанной с упомянутым множеством, с использованием однозначно определенных идентификаторов защищаемых фрагментов данных, и средство для формирования сигнатуры, которая ссылается на защищаемые фрагменты данных посредством их однозначно определенных идентификаторов.

19. Сигнатурное устройство (13-15) для обеспечения аутентификации целостности данных и защиты данных, причем устройство выполнено с возможностью обработки фрагментов данных и с возможностью формирования сигнатуры для защиты множества фрагментов данных, при этом устройство отличается тем, что оно выполнено с возможностью адресации каждого защищаемого фрагмента данных посредством однозначно определенного идентификатора, включенного во фрагмент данных, и устройство выполнено с возможностью формирования сигнатурной информации, содержащей однозначно определенные идентификаторы для ссылки на фрагменты данных множества.

20. Проверочное устройство (10) для проверки аутентификации целостности данных и защиты данных, причем устройство выполнено с возможностью обработки фрагментов данных и с возможностью проверки сигнатуры для защиты множества фрагментов данных, при этом устройство отличается тем, что оно выполнено с возможностью адресации каждого защищаемого фрагмента данных посредством однозначно определенного идентификатора, включенного во фрагмент данных, и с возможностью проверки сигнатурной информации, содержащей однозначно определенные идентификаторы для ссылки на фрагменты данных множества.

21. Сигнал (11), содержащий фрагменты данных, при этом множество фрагментов данных защищено сигнатурой, отличающийся тем, что каждый фрагмент данных множества содержит свой собственный однозначно определенный идентификатор, и сигнатура содержит ссылки на однозначно определенные идентификаторы фрагментов данных множества.

22. Программный продукт (12) для выполнения способа по п.1.

RU 2005115106 A

RU 2005115106 A