(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
H04N 7/173
H04N 7/167
H04L 29/06

(11) 공개번호 10-2005-0061545
(43) 공개일자 2005년06월22일

(21) 출원번호 10-2005-7006709
(22) 출원일자 2005년04월18일
번역문 제출일자 2005년04월18일
(86) 국제출원번호 PCT/IB2003/004608
국제출원일자 2003년10월17일
(87) 국제공개번호 WO 2004/036870
국제공개일자 2004년04월29일

(30) 우선권주장 02257275.4 2002년10월18일 유럽특허청(EPO)(EP)

(71) 출원인 코닌클리케 필립스 일렉트로닉스 엔.브이.
네델란드왕국, 아인드호펜, 그로네보드스베그 1

(72) 발명자 반 덴 휴벨, 세바스찬, 에이.,에프.,에이.
네덜란드 엔엘-5656 아아 아인드호벤 프로프. 호스틀란 6 내
애쉴리, 알렉시스, 에스.,알.
네덜란드 엔엘-5656 아아 아인드호벤 프로프. 호스틀란 6 내

(74) 대리인 정상구
신현문
이범래

심사청구 : 없음

(54) TV-애니타임의 메타데이터 보호를 위한 방법 및 시스템

명세서

기술분야

본 발명은 데이터 조각들(data fragments)의 세트가 서명(signature)에 의해 보호되는 데이터 무결성 인증(data integrity authentication) 및 데이터 보호를 제공하는 방법에 관한 것이다.

본 발명은 또한 데이터 조각들을 수신하고 처리하도록 배열되며, 데이터 조각들의 세트가 서명에 의해 보호될 수 있는 데이터 무결성 인증 및 데이터 보호를 제공하기 위한 시스템에 관한 것이다.

본 발명은 또한 데이터 조각들을 처리하도록 배열되며, 데이터 조각들의 세트를 보호하는 서명을 생성하도록 배열된 데이터 무결성 인증 및 데이터 보호를 제공하기 위한 서명 디바이스에 관한 것이다.

본 발명은 또한 데이터 조각들을 처리하도록 배열되며, 데이터 조각들의 세트를 보호하기 위한 서명을 검증하도록 배열된 데이터 무결성 인증 및 데이터 보호를 검증하기 위한 검증 디바이스에 관한 것이다.

본 발명은 또한 데이터 조각들의 세트가 서명에 의해 보호되는 데이터 조각들을 포함하는 신호에 관한 것이다.

본 발명은 또한 이러한 방법을 구현하기 위한 컴퓨터 프로그램 제품에 관한 것이다.

배경기술

채널들에서 사용가능한 프로그래밍 콘텐트의 다양성과 함께, 텔레비전 시청자들에게 사용가능한 이러한 채널들의 수가 증가함에 따라, 텔레비전 시청자들이 관심있는 텔레비전 프로그램들을 식별하는 것은 점점 도전이 되고 있다. 역사적으로,

텔레비전 시청자들은 인쇄된 텔레비전 프로그램 가이드들을 분석함으로써 관심있는 텔레비전 프로그램들을 식별한다. 텔레비전 프로그램들의 수가 증가함에 따라, 이러한 인쇄된 가이드들을 사용하여 원하는 텔레비전 프로그램들을 효율적으로 식별하는 것이 점점 어려워지고 있다.

보다 최근에, 텔레비전 프로그램 가이드들은 전자 포맷으로 사용가능하게 되었으며, 종종 이는 전자 프로그램 가이드(Electronic Program Guide; EPG)들로 불린다. 인쇄된 텔레비전 프로그램 가이드들과 같이, EPG들은 사용가능한 콘텐트의 개요들을 제공하고, 이는 사용자에 의해 간단히 읽어질 수 있다. 콘텐트라는 일반적인 용어는 전형적으로 음악, 노래들, 영화들, 텔레비전 프로그램들, 그림들 등과 같은 것들을 포함할 수 있으나, 또한 개인적인 장면들, MPEG-4 객체들 등을 나타낼 수 있다.

EPG는 개인적인 콘텐트 아이템들을 동반하는 메타데이터로부터 개요를 수집한다. 콘텐트 아이템들에 대한 메타데이터는 다양한 소스들로부터 사용가능하다. 메타데이터는 방송 스트림(예를 들면, MPEG-2 테이블들)으로 포함될 수 있거나 또는 외부 데이터베이스들로부터 다운로드될 수 있다. 예를 들면, 텔레비전 수신기 또는 개인 디지털 기록기(Personal Digital Recorder; PDR)에 인터넷 연결이 제공될 수 있으며, 이는 디바이스가 월드 와이드 웹(World Wide Web)을 통하여 사용가능한 메타데이터에 액세스하게 한다.

이러한 메타데이터는 일반적으로 타이틀, 작가, 장르 등과 같은 정보를 포함하며, 고유한 콘텐트 참조 식별자(Content Reference Identifier; CRID)를 또한 포함할 수 있고, 이는 때때로 콘텐트 참조 식별자로도 불린다. CRID를 사용하여, 각각의 개별적인 콘텐트 아이템은 고유하게 식별될 수 있다. 또한, CRID를 사용하여 다른 정보가 데이터베이스로부터 검색될 수 있다. 예를 들면, 방송 시간 및 장소가 아직 공지되지 않았다고 하더라도, 사용자는 그가 EPG로부터 보길 원하는 콘텐트 아이템을 선택할 수 있다. CRID를 사용하여, 그후 시스템은, 이러한 정보가 사용가능하게 될 때, 콘텐트 아이템의 방송 시간 및 장소를 검색할 수 있다.

CRID는 콘텐트의 방송 전송들로 제한되지 않는다. 이는 또한 인터넷 상의 위치, 또는 임의의 다른 소스를 참조할 수 있다. 콘텐트 분석의 목적은 콘텐트의 특정 아이템의 특정 인스턴스의 획득을 허용하는 것이다. 예를 들면, 사용자는 텔레비전 시리즈의 에피소드를 기록하길 원할 수 있지만, 그는 그 에피소드가 사용가능하게 될 때 및 장소를 알 필요는 없게 된다. 그는 이후 CRID에 의해 에피소드 또는 시리즈에 대한 참조를 입력하기 위해 그의 개인적인 디지털 기록기(PDR) 또는 유사한 디바이스를 사용할 수 있다. CRID는 전체적인 시리즈 또는 그의 개별적인 에피소드를 나타낼 수 있다는 것을 인지하라.

콘텐트 아이템에 대하여 수신된 CRID를 가지면, PDR은 콘텐트 아이템의 위치를 얻고자 시도한다. 이러한 정보는 로케이터(locator)로 불리며, 이는 콘텐트 아이템이 방송될 날짜, 시간 및 채널을 포함한다. 그러나, 사용자는 이를 알아야 할 필요가 없다. PDR이 콘텐트 아이템의 로케이터를 한번 얻으면, PDR은 규정된 날짜 및 시간을 대기하고, 이후 규정된 채널에서 그가 방송됨에 따라 에피소드를 기록한다. 물론, 로케이터가 인터넷 상의 위치를 나타내면, PDR은 그가 사용 가능한 순간에 지시된 위치로부터 콘텐트를 간단히 검색할 수 있다.

TV-애니타임 표준화 기구는 표준화된 콘텐트 참조 ID를 제공한다. TV-Anytime Forum, www.tv-anytime.org, Specification Series:S-4, on Content Referencing(Normative), Document SP004V11, 14 April 2001, later version SP004V12, 28 June 2002, ETSI TS 102 822-4를 참조하라. 이러한 문서는, CRID가 CRID를 생성한 기구를 나타내는 <authority> 필드를 포함하는 것을 규정한다. 인증은 또한 CRID가 로케이터들 또는 다른 CRID들로 분석되도록 하는 기능을 제공할 것이다. 로케이터는 콘텐트의 시간 및 공간에서의 위치들에 대한 이름이다. CRID는 또한 "RFC2396, Uniform Resource Identifiers(URI):Generic Syntax"에 주어진 바와 같은 표준화 리소스 식별자들(Uniform Resource Identifiers;URIs)의 정의를 따르는 자유 포맷 문자열인 <data> 필드를 포함한다. 이러한 문자열은 <authority> 필드에 의해 주어진 인증에 의미를 부여해야 한다.

CRID는 위치 분석을 위해 사용되며, 이는 CRID를 다른 CRID(들) 또는 로케이터들로 번역하는 프로세스로서 정의될 수 있다. 예를 들면, 전체적인 TV 시리즈에 대한 CRID는 그 시리즈의 개별적인 에피소드들에 대한 CRID들의 시리즈로 번역될 수 있다. 위치 분석은 기록 디바이스(전형적으로 개인 디지털 기록기 또는 PDR)에서 또는 원격적으로 수행될 수 있다. 분석 제공자는 위치 분석을 수행한다. 분석 제공자들은 식별되고 위치 지정될 사용자 분석 인증 기록(Resolving Authority Record; RAR)들을 사용한다. RAR은 CRID들을 생성하는 기구에 대응하는 적어도 하나의 <authority> 필드를 포함한다.

RAR은 또한 URL과 분석 제공자 이름을 포함한다. URL은 분석 정보가 발견될 수 있는 위치를 나타낸다. 분석 제공자 이름은, 위치 분석을 제공하는 기구의 이름을 포함한다. 이러한 RAR들은 PDR들에 사용될 수 있다.

TV-애니타임 정보 및 서비스들은 귀중한 것이므로, 이러한 정보의 보호가 중요하다. 보호는 소스 인증의 발행과 스푸핑(spoofing)을 포함하며; 데이터의 무결성은 보호되는 것이다. TVA 데이터가 소스로부터 수신될 때, 수신기는, 데이터가 예상된 소스로부터 실제로 왔는가 및 제 3 자에 의해 변경되지 않았는가를 검사하고자 원할 수 있다.

이를 시도하는 제 3 자에 대해서는 보상이 있다. 제 3 자가 메타데이터 또는 CRID 테이블을 변결할 수 있다면, 이는 이후 PDR가 광고들, 예고편들 또는 다른 콘텐트를 포함하는 것으로 의도된 다른 정보를 기록할 수 있도록 한다. 이는 또한 사용자에 대해 매우 불쾌한 것이며, 시스템에 대하여 사용자가 가지는 신뢰를 낮출 것이다. 따라서 PDR은 콘텐트가 신뢰된 소스로부터 온 것인지 여부를 검사하길 원할 것이다. 데이터가 상이한 채널들을 사용하여 분배되더라도 하나의 소스로부터 시작되었다는 것이 인증될 수 있다면, PDR은, 동일한 콘텐트의 다중 소스들에 직면하였을 때, 선택하는데 이를 이용할 수 있을 것이다. 이것의 예로 어떠한 BBC 쇼의 데이터가 BBC에 의해 생성된 것으로 인증될 수 있을 때, 이는 이러한 정보가 옳다는 가능성을 상승시킨다.

TV-애니타임 데이터 및 메타데이터의 소스는 항상 데이터의 생성자는 아니다. 소스는 상이한 소스들로부터 정보를 모으고 그룹핑(grouping)하는 서비스 제공자일 수 있다. 누가 데이터를 생성하였는지 및 데이터가 변경되었는지를 검사하는 것은 유용할 수 있다. 이러한 경우에, 수신되는 데이터는 상이한 소스들에 의해 제공된 부분들을 가질 것이다.

데이터 무결성의 보호에 대한 표준 암호 방법은 암호 기술들을 사용하여 데이터에 서명(sign)하는 것이다. 모든 TVA 메타데이터가 XML로 표현됨에 따라, 서명들이 동일한 데이터 구조에서 운반되는 것을 허용하는 표현 서명들의 운반 중간 방식(transport neutral way)은 TVA 방식의 서명들을 포함할 것이며, 명백한 선택은 xmldsig일 것이다 ("RFC3275,(Extensible Markup Language) XML-Sginature Syntax and Processing"). 그러나, 이러한 표준은 XML 분석 트리의 모든 노드에 대한 XPath 표현의 평가를 정의하기 위해 XPath 데이터 모델("XML Path Language(XPath) Version 1.0, W3C recommendation, J.Clar, S.DeRose, October 1999, http://www.w3.org/TR/1999/REC-xpath-19991116")을 사용하며, 이는 효율적으로 구현하기에 어려울 수 있는 변환이다.

이러한 문제를 극복하기 위한 시도가 효율적인 문서 서브세팅의 개발을 용이하게 하기 위한 XML 서명 변환을 정의하는 "XML-signature XPath Filter"(W3C recommendation, latest revision 8 November 2002, http://www.w3.org/TR/xmldsig-filter)에 기술되었다. 그러나, 이러한 추천은 W3C 콘소시엄에 의해 채택되지 않았다.

이러한 논의로부터, 서비스 제공자들 및 박스 제조자들이 메타데이터에 대한 효율적인 무결성 검사 메카니즘들을 사용하는 것은 고무적인 것이라는 것은 명백하다.

발명의 상세한 설명

본 발명의 목적은, 상이한 소스들로부터 시작하는 데이터 조각들의 보호를 가능하게 하고 많은 인증자들에 의해 데이터 조각들의 보호를 가능하게 하는, 데이터 조각들을 효율적으로 보호하도록 메타데이터 무결성 및 소스 인증을 제공하는 것이다. 이는 데이터가 (분석) 제공자 및 클라이언트 사이에서 운송되는 동안 데이터가 변경되었는지에 대한 검증를 허용할 것이다. 또한 이는 데이터의 후속 저장 및 처리 동안 데이터가 변경되었는지에 대한 검증를 허용할 것이다.

본 발명의 목적은 세트의 각 데이터 조각이 그 자신의 고유한 식별자를 포함하고, 서명은 세트의 데이터 조각들의 각각의 고유한 식별자들에 대한 참조들을 포함하는 것을 특징으로 하는 본 발명에 따른 방법에 의해 성취된다. 본 발명은, 서명들이 개별적으로 제공되고, 고유한 식별자들에 대한 참조가 어떠한 데이터 조각들이 서명에 의해 커버되는지를 나타낼 시스템을 설명한다. 적어도 하나의 식별자는 데이터 조각들과 서명 사이의 링킹을 가능하게 하도록 고유하게 데이터 조각을 식별한다. 이는 그 데이터 조각의 식별을 위해 각각의 데이터 조각으로 부가된 (선택적인) 필드를 제공함으로써 행해진다. 기존의 필드는, 모든 데이터 조각들이 각 데이터 조각을 고유하게 식별하는 이러한 필드를 가지고 있을 때 사용될 수 있다. 그렇지 않으면, 특별한 서명 식별자가 선택적인 필드로서 각 데이터 조각으로 부가될 수 있다. 이러한 필드가 존재할 때, 이것이 데이터 내에 있는 데이터 조각 인스턴스의 고유한 식별자일 수 있다. 서명은, 데이터 조각들의 이러한 세트들은 개별적인 데이터 조각들 대신 서명되도록 많은 데이터 조각들을 참조할 수 있다. 이는 보다 효율적인 다른 장점을 갖는다.

본 발명에 따른 방법의 실시예가 청구항 2에 설명된다. 분배동안, 데이터가 수동으로 변화될 때, 하나 이상의 집단이 그들의 서명을 동일한 데이터 조각에 적용할 수 있다. 이러한 서명들은 데이터 조각들의 상이한 서브세트들, 즉, 전체적으로 분리된 서브세트들, 부분적으로 오버랩핑하는 서브세트들, 또는 동일한 서브세트들에 적용할 수 있다.

본 발명에 따른 방법의 실시예가 청구항 3에 설명된다. 장점은 단지 해시들만이 서명을 계산하거나 변화시키는데 필요하다는 것이다. 이는 특히 동일한 데이터 조각들이 많은 서명들에서 사용될 때 유익하다(계산 시간의 감소).

본 발명에 따른 방법의 실시예가 청구항 4에 설명된다. XML은 표준화된 방법으로 데이터 조각들의 식별을 가능하게 하는 개별적인 데이터 조각들을 명백하게 분리한다. 데이터 조각들은 하나 이상의 XML 문서들로 모아질 수 있다.

본 발명에 따른 방법의 실시예가 청구항 5에 설명된다. 상술된 바와 같이, TV-애니타임 메타데이터는 메타데이터의 비인증된 조작으로부터의 보호가 필요하다. 따라서 본 발명은 TV-애니타임 환경에서 유익하게 적용될 수 있다.

본 발명에 따른 방법의 실시예가 청구항 6에 설명된다. xml로 표현된 데이터에 대한 적절한 선택은 부가된 고유한 식별자들에 대한 참조들을 갖는 서명의 xmldsig 정의를 사용하는 것이다.

본 발명에 따른 방법의 실시예가 청구항 7에 설명된다. 서명될 데이터 조각들은 이러한 서명에 대해 고려되지 않은 데이터 조각들을 제거하는 변환 함수(RFC3275에 따라)의 사용함으로써 접근될 수 있다. 변환 함수는 고유한 식별자를 사용하는 데이터 조각들을 참조한다.

본 발명에 따른 방법의 실시예가 청구항 8에 설명된다. 앞서 언급된 xmldsig 규정에서 설명된 바와 같이, 동일한 텍스트가 상이한 인코딩들을 사용하는 많은 방식들로 코딩될 수 있다. 서명을 계산하기 위하여, 문서의 하나의 정의된 표현이 정의되어야 한다. 이러한 프로세스를 캐놀리제이션(cannolization)이라 부른다. 캐놀리제이션 함수가 사용되는 지시는, 데이터를 먼저 추출할 필요가 없이 서명 값들의 계산을 허용한다.

본 발명에 따른 방법의 실시예가 청구항 9에 설명된다. 참조들에 대한 무결성을 보호하기 위하여, 참조들은 그들 스스로 서명될 데이터에 잠재적으로 또는 명확하게 포함될 수 있다.

본 발명에 따른 방법의 실시예가 청구항 10에 설명된다. 보다 복잡한 탐색 옵션들이 서명 인덱스 파일들을 부가함으로써 제공될 수 있다.

이러한 인덱스 파일은 이후 탐색 옵션을 지지하도록 고유한 식별자를 사용하여 적절한 서명 파일들에 대한 참조들을 링크한다. 이러한 테이블은 서명되는 데이터와 서명들의 리스트 사이에 그룹핑을 제공한다.

본 발명에 따른 방법의 실시예가 청구항 11에 설명된다. 데이터의 이러한 인스턴스들 내에서 동일한 타입의 데이터 조각들 사이에서 식별자가 고유하다는 것을 보장하기 위하여 데이터 조각을 생성하는 것에 대해 신뢰할 수 있는 조직의 고유한 식별을 갖는 고유한 식별자가 출발하는 것을 제안한다. 이는 또한 클라이언트가 어떠한 조직이 데이터를 발행하였는지를 검출하는 것을 허용한다.

본 발명에 따른 방법의 실시예가 청구항 12에 설명된다. DNS 이름은 조직의 고유한 식별에 대하여 쉽고 이해가능한 선택이다.

본 발명에 따른 방법의 실시예가 청구항 13에 설명된다. 고유한 식별자가 데이터 조각을 식별하지만, 이러한 데이터 조각이 모든 데이터 내에서 발견될 수 있는 곳을 정의하지 않는다. 데이터 내의 정확한 데이터 조각의 탐색을 용이하게 하기 위하여, 참조가 바람직하게 또한 위치 지시자에 의해 동반되어야 한다.

본 발명에 따른 방법의 실시예가 청구항 14에 설명된다. 수행은 데이터 조각을 위치시키도록 취해져야 하는 데이터를 통한 경로를 나타낸다.

본 발명에 따른 방법의 실시예가 청구항 15에 설명된다. 데이터 문서 내에 서명 정보를 포함하는 것이 가능하며 효율적이다.

본 발명에 따른 방법의 실시예가 청구항 16에 설명된다. 상이한 방법은 서명 정보 및 서명을 필요로 하는 가능한 일부 다른 요소들을 또한 포함하는 데이터 문서 주위의 랩퍼(wrapper)를 정의하는 것이다. 이러한 경우에, 원래의 데이터는 가능하게는 고유한 식별자들의 손실을 제외하고, 변경들 없이 랩퍼 내에 포함된다. 적절하게 정의된 랩퍼는 부가적인 데이터가 서명된 데이터에 포함되는 것을 허용하도록 확장될 수 있다.

본 발명에 따른 방법의 실시예가 청구항 17에 설명된다. 상이한 방법은 원래의 데이터 문서의 데이터 조각들을 참조하는 서명 정보를 포함하는 개별적인 데이터 문서를 정의하는 것이다. 이러한 방법으로, 원래의 데이터 문서는 가능하게는 고유한 식별자들의 손실을 제외하고, 변경되지 않는다.

본 발명에 따른 시스템은, 상기 세트의 데이터 조각들을 수신하고 처리하기 위한 수단을 포함하며, 각각의 데이터 조각은 고유한 식별자에 의해 식별되며, 상기 시스템은, 그들의 고유한 식별자들을 사용하여 상기 세트의 상기 보호된 데이터 조각들과 서명을 연관시키기 위한 수단, 상기 보호된 데이터 조각들의 상기 고유한 식별자들을 사용하여 상기 세트와 연관된 서명을 검증하기 위한 수단, 그들의 고유한 식별자들에 의해 상기 보호된 데이터 조각들을 참조하는 서명을 생성하기 위한 수단 중 적어도 하나를 더 포함하는 것을 특징으로 한다.

본 발명에 따른 서명 디바이스는, 상기 데이터 조각에 포함된 고유한 식별자에 의해 보호될 각각의 데이터 조각을 어드레싱하도록 배열되고, 상기 디바이스는 상기 세트의 상기 데이터 조각들을 참조하기 위한 상기 고유한 식별자들을 포함하는 서명 정보를 생성하도록 배열되는 것을 특징으로 한다.

본 발명에 따른 검증 디바이스는, 상기 데이터 조각에 포함되는 고유한 식별자에 의해 보호될 각각의 데이터 조각을 어드레싱하도록 배열되고, 상기 디바이스는 상기 세트의 상기 데이터 조각들을 참조하기 위한 상기 고유한 식별자들을 포함하는 서명 정보를 검증하도록 배열되는 것을 특징으로 한다.

본 발명에 따른 신호는, 상기 세트의 각 데이터 조각은 그 자신의 고유한 식별자를 포함하고, 상기 서명은 상기 세트의 상기 데이터 조각들의 상기 고유한 식별자들에 대한 참조들을 포함하는 것을 특징으로 한다.

본 발명은 또한 청구항 1의 방법을 구현하기 위한 컴퓨터 프로그램 제품을 특징으로 한다.

본 발명의 이러한 및 다른 특징들은 개략적인 도면들을 참조하여 예의 방법으로 또한 설명될 것이다.

도면의 간단한 설명

도 1은 콘텐트 분석의 프로세스를 개략적으로 도시하는 도면.

도 2는 TV-애니타임에 의해 정의되는 바와 같은 상이한 조각들을 도시하는 도면.

도 3a, 3b, 및 3c는 고유한 식별자에 관련된 XML 정의들 및 예들을 도시하는 도면.

도 4a, 4b, 및 4c는 서명 정보에 관련된 XML 정의들 및 예들을 도시하는 도면.

도 5는 키 정보에 관련된 XML 정의들 및 예들을 도시하는 도면.

실시예

데이터의 수집 및 처리의 설명에 대하여, 메타데이터의 처리는 TV-애니타임 환경의 개인 디지털 기록기 또는 PDR과 같은 디바이스에 의해 설명될 것이다. 도 1은 콘텐트 분석의 프로세스를 개략적으로 예시한다. PDR(10)은 콘텐트 참조 식별자(CRID)에 의해 식별된 콘텐트 아이템을 기록하도록 명령을 받는다. 콘텐트 아이템을 기록하도록 PDR에 명령하는 것,

또는 다시 말하면 콘텐트 아이템의 기록을 위한 스케줄링은 다양한 방법들로 수행될 수 있다. 현재의 일반적인 방법은, 예를 들면, EPG의 콘텐트 아이템을 선택함으로써, 콘텐트 아이템이 기록될 것임을 사용자가 수동으로 지시하는 것이다. 이하의 PDR의 기능성들의 일부 또는 전체는 또한 텔레비전 수신기들, 셋탑 박스들 또는 개인 컴퓨터들과 같은 하나 이상의 다른 디바이스들로 통합될 수 있다는 것이 쉽게 이해될 것이다. 광학 디스크 또는 고체 상태 메모리와 같은 적절한 포맷에 컴퓨터 판독가능한 명령들을 갖는 컴퓨터 프로그램 제품(12)은, 본 발명을 실행하는 프로그램 명령들을 저장하거나 분배하는데 사용될 수 있다.

PDR, 또는 PDR이 접속되는 다른 디바이스는 소비자가 관심을 가질 수 있는 콘텐트 아이템들의 종류들을 결정하도록 준비될 수 있다. 이것은 사용자 프로파일링 또는 추천기 시스템들로 알려져 있다. 소비자가 시청하는 콘텐트 아이템들의 트랙을 보관하고, 이러한 콘텐트 아이템들에 대한 암시적인 및/또는 명시적인 등급 시스템을 사용함으로써, 소비자가 관심을 가질 수 있는 다른 콘텐트 아이템들의 정밀도의 변화 정도들을 예측하는 것이 가능하게 될 수 있다. 이후 소비자에게 흥미있을 것 같은 콘텐트 아이템들을 자동적으로 기록하는 것이 가능하게 될 수 있다. 이러한 콘텐트 아이템들은 이후 PDR에 의해 기록될 수 있다. 사용자 프로파일링을 위한 많은 기술들이 분야에 알려져 있다. PDR이, 특정 콘텐트 아이템은 관심있을 것이라고, 사용자 프로파일링을 사용하여 결정할 때, 기록을 위해 콘텐트 아이템을 스케줄링한다.

콘텐트 아이템을 위한 CRID는 콘텐트 아이템의 자동 기록을 용이하게 하는데 사용된다. CRID는 사용자에 의해 수동으로 입력될 수 있으며, 또는 전자 프로그램 가이드를 통해 콘텐트 아이템을 선택한 결과일 수 있다. 두번째 선택사항은, CRID가 CRID 공급자 엔티티(13)에 의해 EPG에서 사용된 다른 메타데이터와 함께 PDR로 제공된다는 것을 가정한다. 대안적으로, CRID가 사용자 또는 PDR에 의해 알려지지 않았으면, 사용자는, 예를 들면, 메타데이터 데이터베이스에서 콘텐트 아이템의 제목을 사용하여 탐색을 수행하고, 탐색 결과들로부터 원하는 콘텐트 아이템을 선택할 수 있다. CRID는 이후 검색 엔진에 의해 PDR로 공급된다.

CRID를 PDR로 공급하는데는 많은 다른 방법들이 있다. 예를 들면, 영화에 대한 예고편 또는 미리보기는 어떠한 방법(예를 들면, 워터마크)으로 상업적인 콘텐트에 삽입된 CRID로 방송될 수 있다. 사용자는 이후 그의 원격 제어, 텔레비전 또는 PDR 상의 버튼을 누를 수 있다. PDR 또는 텔레비전은 이후 상업적인 콘텐트에서 CRID를 추출한다.

소망된 콘텐트 아이템에 대한 CRID가 한번 알려지면, PDR은 CRID를 입력으로서 사용하여 콘텐트 아이템에 대한 위치 정보를 얻도록 시도한다. 이러한 위치 정보는 항상 사용가능할 필요는 없다. 예를 들면, CRID는 영화 극장들에서 최근 개봉되었던 영화만을 참조할 수 있다. 이러한 영화는 가까운 미래에 텔레비전에서 방송하지 않을 것이고, 따라서 EPG 정보를 사용하여 스케줄링될 수 없다. 이러한 경우에, PDR은 로케이터가 후에 사용가능하게 될 때까지(예를 들면, 영화가 TV 상에서 방송될 1년 후) 로케이터를 얻도록 규칙적으로 시도하여야 한다. CRID는 또한 TV 시리즈를 선호할 수 있으며, 이는 이후 그 시리즈를 개인적인 에피소드들을 위한 다수의 CRID들로 분리된다. 일부 에피소드들에 대해서는 사용가능한 로케이터 정보가 없을 수 있다. 여기서 PDR은 또한 이러한 에피소드들에 대한 로케이터(들)를 얻기 위해 규칙적으로 재시도해야 한다.

CRID를 로케이터 정보로 번역하는 프로세스는 위치 분석으로서 TV-애니타임에 공지된다. 위치 분석은 위치 독립적인 콘텐트 참조(CRID)를 시간(예를 들면, 방송 시스템의 스케줄링된 전송 시간)과 공간(예를 들면, TV 채널, IP 어드레스)에서의 그의 위치로 매핑하는 것을 포함한다. 상술된 바와 같이, 시간과 공간에서의 이러한 위치들은 "로케이터들"로 불린다. 위치 분석의 프로세스는 PDR의 내부에서 일어날 수 있으며, 또는 인터넷 상의 서버와 같은 물리적으로 떨어진 원격 서버를 사용함으로써 일어날 수도 있다.

PDR에 대하여, CRID는, 외부의 도움 없이 위치를 분석할 수 없는 불명료한 정보를 필수적으로 포함한다. CRID들에 대한 로케이터 정보를 제공하는 분석 제공자(Resolution Provider; RP)는 이러한 문제를 해결하도록 제공된다. 일반적으로 많은 RP들이 사용가능하며, PDR은 특정 CRID를 위하여 어떤 RP를 사용해야하는지를 알아야 한다. 종종, 이것은 CRID를 생성한 것과 동일한 기구가다. 인증의 이름은 상술한 바와 같이, <authority> 필드의 CRID에 존재한다. 분석 인증(Resolution Authority; RA)(15)은 TV-애니타임 규정 SP004에 규정된 도메인 이름 분석 프로세스를 사용하여 인터넷 상에서 찾는 것이 가능하다.

각 RA는 위치 분석을 행하기 위하여, 하나 이상이 분석 인증 기록들(RAR)이 PDR에 존재하도록 요구할 것이다. 각 분석 인증 기록은, PDR이 이것이 RAR인 것을 알도록하는 일부 종류의 운송 특정 콘테이너 내부에 위치될 필요가 있을 것이다. 동일한 인증에 대한 많은 기록들의 경우에, PDR은 그들 중 단지 하나만이 사용되도록 선택할 수 있거나, 모두를 차례로 시도할 수 있다. 분석 인증 기록(RAR)은, 콘텐트 참조 분석 정보가 발견될 수 있는 RA들을 식별하는 정보를 포함한다.

RAR을 사용하여, PDR은, 어떤 RP가 특정 CRID를 분석하는데 사용되는지를 결정한다. PDR은 이후 CRID에 의해 수행된 위치에 대한 요청을 문제의 분석 제공자에게 제시한다. 이러한 요청에 응답하여, 분석 제공자는 로케이터 정보를 되돌려준다(이러한 정보는 물론 그 RP에서 사용가능하다는 것을 가정한다). PDR은 이후 콘텐트 소스에 액세스할 수 있으며 콘텐트 아이템을 얻을 수 있다. 콘텐트 아이템은 예를 들면, 그가 다중 시간들에서 방송되거나 다중 제공자들로부터 사용가능할 때, 하나 이상의 로케이터를 가질 수 있다. PDR은 이후 어떤 로케이터가 사용되는지를 선택하거나, 또는 사용자가 선택하도록 촉구할 수 있다.

로케이터 정보가 한번 얻어졌으면, PDR은, 특정 데이터 및 시간에 대하여 대기하고, 이후 특정 채널 상에서 방송되면 에피소드를 기록한다. 물론, 로케이터가 인터넷 등의 위치를 나타내면, PDR은 간단하게 사용가능하게 될 때 지시된 위치로부터 콘텐트를 검색할 수 있다.

어떤 로케이터 정보가 사용가능한 것인가에 대한 콘텐트 아이템들은, 적절한 순간에서 PDR에 의해 기록될 수 있다. 이를 위해, PDR은 충분하게 큰 하드 디스크와 같은 로컬 저장장치, 및/또는 DVD+RW 라이터와 같은 디바이스를 포함할 수 있다. 콘텐트 아이템들이 저장되는 저장장치는 PDR에 대하여 로컬일 필요는 없지만, 하드 디스크와 같은 외부 디바이스이거나 또는 홈 네트워크를 통해 PDR에 접속된 파일 서버일 수 있다. 콘텐트 아이템들이 한번 기록되면, 그들은 그들이 삭제될 때까지 언제나 재생될 수 있다.

상기 방법을 사용하여, 콘텐트의 위치를 알고있는 누구나 분석 제공자로서 역할을 할 수 있다. 그러나, 콘텐트 및 서비스 제공자들은, 인증된 분석 제공자들만이 예를 들면, 그들의 평판(ruputation)을 보호할 수 있도록 그들의 콘텐트에 대한 콘텐트 분석을 수행하는 것을 원할 것이다. 반면, 소비자들과 PDR들에 대해서는 CRID 인증 및 분석 제공자를 신뢰하고 믿을 수 있는 것이 중요하므로 그들은 정당한 콘텐트를 얻을 수 있다.

PDR이 디지털 권리 관리(DRM) 시스템에 따라 동작하면, 이후 콘텐트 아이템과 연관된 권리들이 삭제를 요청할 때, 콘텐트 아이템은 삭제될 수 있다. 또한, 일부 콘텐트 아이템들은 아이템 전체를 기록하는 권리, 또는 제한된 시간이나 제한된 횟수에 대해서만 시청을 허용하는 권리만을 가질 수 있다. PDR은 이후 제한이 초과되거나, 다른 액세스를 허용하는 다른 권리들이 얻어질 때까지 콘텐트에 대한 다른 액세스를 거부할 때, 콘텐트 아이템을 삭제하여야 한다. 클라이언트 박스 내에 수신된 콘텐트는 암호화에 의한 전송동안 보호될 수 있다. 콘텐트가 액세스될 수 있기 전에, 콘텐트는 암호 해독되어야 한다. 이러한 프로세스는 DRM 또는 조건부 액세스(CA) 시스템에 의해 제어된다.

TV-애니타임 규정은 두개의 상이한 분배 방법들: 일방성(unidirectional) 및 양방성(bidirectional)을 구별한다. 일방성 상황에서, TV-애니타임 데이터는 적당한 정상 시그널링를 갖는 방송 스트림 내의 다른 스트림이다. 이러한 스트림에 대한 액세스는 스크램블링과 같은 종래의 조건적 액세스 시스템들을 사용하여 보호될 수 있다. 전송 메카니즘에 대해 정의된 일반적인 시그널링 방법들을 사용하여, 조건적인 액세스 시스템이 식별되며, 이러한 스트림과 연관된 조건적 액세스 정보를 나르는 메세지들이 지적된다. 대부분의 디지털 방송 시스템들은 MPEG-2 전송 스트림 포맷(ISO/IEC 13818-1:1996(E), Information technology-Generic coding of moving pictures and associated audio information: Systems, First Edition, 1996-04-15)을 사용한다.

양방성 경우에서, 클라이언트와 서버 사이에 점대점 연결이 생성된다. 이러한 프로세스는 TV-Anytime document SP004v1.2, Specification series S-4 on Content Referencing, Version 1.2, Final Specification, 28 June 2002, ETSI TS 108 822-4에서 설명된다. DRM 시스템은 안전한 채널을 서비스 제공자에게 개방하며, 이러한 채널을 통해 통신을 터널링할 것이다. 이러한 방법으로 인증된 TV-애니타임 클라이언트들 만이 콘텐트에 액세스할 수 있다.

방송 시스템에서 기존의 CRC 메카니즘들이 전송 에러들과 함께 분배되더라도, 계획된 변화들을 검출하고 청구된 소스에 의해 생성된 정보를 인증하기를 여전히 희망한다.

TV-애니타임 데이터의 소스가 항상 데이터의 생성자인 것은 아니다. 소스는 상이한 소스들로부터 정보를 모으고 그룹핑하는 서비스 제공자일 수 있다. 데이터는 또한 상이한 소스들로부터 PDR에 의해 검색될 수 있다. 따라서, 수신되는 데이터는 상이한 소스들에 의해 제공된 부분들을 유지할 것이다. 누가 데이터를 생성하였는지와 데이터가 변화되었는지를 검사하는 것은 유용할 수 있다. 이는 서명들을 사용하여 행해진다.

모든 TVA 메타데이터는 TVA 조각들로 제공된다. TVA에서, 메타데이터 규정에 따라(TV-Anytime document WD647/SP003v1.3 Part A, Specification series S-3 on Metadata:Part A Metadata Schemas, version 1.3, 15 December 2002, ETSI TS 102 822-3), TVA 조각은 "메타데이터의 자기 포함 원자 부분(a self contained atomic portion of the metadata)"이다. 이러한 문서에서, 서명될 수 있는 최소 TVA 메타데이터 요소가 조각임이 가정된다.

본 발명은 조각을 서명로 링크하기 위하여 TV-애니타임 조각을 고유하게 식별하는데 사용되는 라벨(label)의 정의를 포함한다. 이는 각각의 TV-애니타임 조각에 부가되는 선택적인 필드를 제공함으로써 수행된다. 존재할 때, 이러한 고유한 식별자는 메타데이터의 이러한 인스턴스 내의 그러한 조각 인스턴스의 고유한 식별이다. 고유한 식별자는 메타데이터 내의 조각의 쉬운 트레이싱(tracing)을 고려해야 한다. 이는 서명을 계산하는데 필요한 상이한 조각들을 찾기 위해 요구된다.

도 2는 TV-애니타임에 의해 정의된 바와 같은 상이한 조각들을 도시한다. 서명들을 지지하기 위하여, 모든 조각들은 조각의 식별을 위한 선택적인 또는 필수의 고유한 식별자를 갖는다. TV-애니타임 규정 내에서, TVAID로 불리는 필드가 이러한 조각들에서 사용된다. 상기 식별된 메타데이터 규정에 따라 TVAID들은 "메타데이터 설명 내의 고유함을 나타내는데 " 사용된다. 그들이 식별자에 대한 요청을 매칭하는 것으로 보인다고 하여도, 그들은 단지 TVAID의 특별한 타입에 대하여 고유할 뿐이다. 예를 들면, 서비스ID와 세그먼트ID는 특별한 메타데이터 설명 내에서 동일할 수 있다.

고유한 식별자의 개념을 수행하기 위해 몇몇 변화들이 가능할 수 있다.

본 발명의 제 1 변화에서, TVAID는 참조 식별자로서 사용된다. 이는, 서명에 사용된 참조가 콘텍스트(예를 들면 서비스 또는 세그먼트)를 나타낼 때, 고유한 식별자를 제공한다. TVAID는 모든 조각들이 하나를 가질 때(또는 하나가 부가될 때) 사용될 수 있으며, TVAID를 사용하여 조각에 대한 고유한 참조가 TVA 메타데이터의 이러한 인스턴스 내에서 생성될 수 있다는 것이 결정된다.

제 2 변화에서, 특별한 TVA 서명 식별자가 선택적인 필드로서 모든 조각들에 부가된다. TVAID 또는 새로운 식별자 중 하나가 이러한 목적을 위해 정의된다. 메타데이터 내의 동일한 타입의 다른 조각들 사이의 조각을 고유하게 식별하는 각각의 TVA 조각에 부가된 예시적인 식별자에 대한 XML 정의가 도 3a에 도시된다. 각 조각(또는 조각들의 세트)을 참조할 수 있도록 하기 위하여, 모든 TV-애니타임 조각들에 대한 포맷의 예는 도 3b에 도시된 바와 같이 형식적으로 정의된, TVASignatureId 특성을 부가하는 것일 수 있다.

본 발명의 다른 유익한 변화는 조각을 생성하는 것에 대해 응답하는 조직의 DNS 이름(또는 다른 고유한 식별)을 갖는 식별자를 개시함으로써 메타데이터 내의 동일한 타입의 조각들 중에서 식별자가 고유하다는 것을 보장한다. 또한 이것은 클라이언트가 어떠한 조직이 데이터를 생성한 것을 검출하도록 허용할 것이다. MyCompany사에 의해 생성된 조각의 TVASignatureId의 예가 도 3c에 도시된 바와 같이 볼 수 있다.

각각의 개별적인 조각 또는 조각들의 세트를 라벨링하는 것 및 참조들을 사용하여 서명하는 것은, 적절히 선택될 때, 참조가 서명 파일로부터 조각로의 링크를 제공한다는 장점을 갖는다. 또한, 고유한 식별자는 조각(들)과 서명을 포함하는 데이터 사이의 링크를 제공한다.

모든 TVA 메타데이터가 xml로 표현됨에 따라, 서명들이 동일한 데이터 구조에서 운반되는 것을 허용하는 표현 서명들의 운반 중간 방식이 TVA 개요에 서명들을 포함할 수 있도록 한다. TV-애니타임 메타데이터는 xml로 표현되며, 적절한 선택은 xmldsig일 수 있지만, 다른 XML기반 서명 스킴들이 물론 정의될 수 있다.

서명은 xmldsig 표준에 따라 저장될 수 있다. 부가적으로, 고유한 식별자에 대한 참조는 조각들이 서명을 계산하는데 사용된다는 것을 나타낸다. 고유한 식별자가 조각을 식별한다고 하여도, 이러한 조각이 모든 TVAMain 내에서 발견될 수 있다는 것은 정의되지 않는다. 메타데이터 내의 정확한 조각의 탐색을 용이하게 하기 위하여, (RFC2396에 따른 URI 포맷에 정의된) 참조는 또한 위치를 바람직하게 나타내야 한다. 따라서 본발명의 확장은, 조각을 위치시키기 위하여 취해져야 하는 메타데이터를 통한 경로를 나타내기 위해 선택적인 위치 지시자를 부가한다.

본 발명에 따라 고유한 식별자를 포함하는 조각 URI의 정의를 따르는 예는 "tva://<path>/<TVASignatureId>"로서 정의될 수 있으며, 여기서 <path>는 조각을 향한 메타데이터의 개시로부터의 경로이며, TVAID는 조각의 식별자이다.

일부 예들은 "tva://TVAMain/aap.org;132423", "tva://TVAMain/ClassificationTable/CSAlias/publisher.com;122314" 및 "tva://TVAMain/ProgramDescription/ProgramLocationTable/Schedule/metwt.org;320984"이다. 제 1 예는 완전한 TVAMain 메타데이터 문서를 서명하는 것이 또한 가능하다는 것을 설명한다. 이러한 경우에, 증명 및 서명 경로들이 없는 모든 TVAMain이 고려되어야 한다.

본 실시예에서 고유한 식별자(TVASignatureId와 같은)가 조각들로 참조하도록 URI들에서 사용되기 때문에, 식별자는 RFC2396에 설명된 바와 같이 URI들에 위치된 포매팅 제한(formatting restriction)들에서 겸용이어야 한다. 또한, URI의 분석들을 용이하게 하기 위하여 TVASignatureId에는 슬래시들("/")이 사용되지 않는다.

TVASignatureTable은 서명된 데이터와 서명들의 리스트 사이에 그룹핑을 제공하며, 이러한 테이블의 예시적인 정의가 도 4a와 4b에 도시된다. 이러한 정의에서, 이러한 테이블의 ContentReferencingTable 및 ResolvingAuthorityRecordTable과 같은 다른 TV-애니타임 메타데이터 문서들을 포함하도록 하는 옵션이 있다. 이는 그들이 한번만 발생할 수 있으며, 테이블과 URI의 그 메타데이터를 위하여 고유한 식별자가 필요하지 않다는 장점을 가진다.

TVASignatureTable은 도 4c에 도시된 바와 같이 정의된다. 0 이상의 서명들이 제공될 수 있다. 데이터가 시스템에서 사용가능하지 않거나, 아직 사용가능하지 않거나, 더이상 사용가능하지 않아짐에 따라, TCASignatureWrapper에서 지시된 데이터에 대해 사용가능한 모든 서명들이 항상 포함되지 않으며, 다양한 서명들에 의해 보호되는 모든 조각들이 항상 제공되지 않는다. 전달 시스템의 수행은 관련 조각들 및 서명이 필요할 때 제공되어야 한다는 것에 주의되어야 할 것이다. 양방향 전달 시스템에서 손실 조각들 또는 손실 서명들이 다운로드될 수 있다.

서명될 필요가 있는 조각들을 정의하는 상이한 방법은, 서명에 대해 고려되지 않는 메타데이터로부터 일부 또는 모든 요소들을 제거하는 변환 함수(RFC3275에 따라)를 정의하는 것에 의한 것이다.

서명을 검사하기 위하여, 서명(들)에 적용된 집단의 대응 공용키가 필요하다. 이러한 키들의 분배가 몇몇 방법들로 수행될 수 있다. 그들은 디바이스에서 하드 코딩될 수 있지만, 새로운 키들이 사용되거나 또는 현재의 키들이 타협될 때 문제들을 일으킴에 따라 키들의 분배의 대부분의 일반적인 방법은 이들을 소위 증명-체인으로 병합시키는 것에 의한다("Applied Cryptography Second Edition:protocols, algorithms, and source code in C, Bruce Schneier, Wiley, 1996"). 따라서 서명들의 데이터에 부가하여 서명을 검사하기 위하여, 서명들을 제공하는 집단들의 증명들이 또한 필요하다. TVASignature는 TVASignature 랩퍼 내의 이러한 증명들의 운반을 지지하기 위하여 하나 이상의 ds:KeyInfo의 포함을 허용한다. 식별자들을 동반하는 KeyInfo 객체들의 리스트를 나타내는 XML 복합 타입이 도 5에 도시된다.

서명로부터 Signatures로부터의 KeyInfoWrapperTable의 KeyInfo 요소들로 참조할 수 있도록 하기 위하여, 참조 URI는 "tva://KeyInfoListTable/<Identifier>"와 같이 정의되며, 여기서 <Identifier>는 KeyInfoWrapperType에 지시된 지시자이다. 따라서 일부 예들이 "tva://KeyInfoListTable/132423", "tva://KeyInfoListTable/435432h" 및 "tva://KeyInfoListTable/MyKeyInfo"이다.

이는 증명들 및 통신 KeyInfo 객체들의 다른 옵션들의 포함을 허용한다. 이는 또한 어떻게 그들이 서명들과 링크되는지를 나타낸다.

(공용) 키들은 또한 X509 증명들을 사용하여 저장될 수 있으며, 여기서 509 증명의 서브젝트 필드는 조직 이름 또는 키 소스를 식별하는 상이한 고유한 식별을 많이 포함할 수 있다. 이는 데이터가 서명된 것을 갖기 위해 청구하는 조직에 의해 실질적으로 서명되도록 하기 위한 부가적인 방법을 제공한다.

서명들은, DSA 또는 RSA 서명 생성 알고리즘들과 같은 적절한 알고리즘을 사용하여 생성될 수 있다.

xmldsig 규정에서 설명된 바와 같이, 텍스트는 많은 방법들로 코딩될 수 있다. 서명을 계산하기 위하여, 문서의 하나의 정의된 표현이 정의되어야 한다. 이러한 프로세스는 캐놀리제이션으로 불린다. TV-애니타임 내에서, BiM은 TV-애니타임 데이터의 2진 인코딩을 위한 2진 사본으로 사용된다. BiM 인코딩이 사용될 때, BiM은 캐놀리제이션 함수로서 지시되어야 한다. 이는 클라이언트가 데이터를 먼저 추출할 필요없이 서명 값들을 계산하는데 BiM 인코딩된 파일들을 사용하는 것을 허용한다. 변환 및 캐놀리제이션 함수는 콘텐트를 프로세싱하는데 사용되어, 고유하고 항상 동일한 바이트들의 세트가 서명이 계산되는 것을 통해 생성된다.

고유한 식별자에 대한 참조들의 무결성을 또한 보호하기 위하여, 그들은 서명될 데이터에 암시적으로 또는 명시적으로 포함될 수 있다. 도 5와 관련하여 상술된 바와 같이, 서명들은 시스템에서 사용된 상이한 테이블들을 보호하는데 또한 사용될 수 있다.

보다 복잡한 탐색 옵션들은, 서명 인덱스 파일들을 부가함으로써 제공될 수 있다. 이러한 인덱스 파일은 적절한 서명 파일들로 고유한 식별자들을 링크할 것이다.

"ISO/IEC 13818-6:1998, Information technology-Generic coding of moving pictures and associated audio information:Extensions for Digital Storage Media Command and Control, 1998" 및 "ETSI TS 102 812 V1.1.1(2001-11), Digital Video Broadcasting(DVB); Multimedia Home Platform(MHP) Specification 1.1, 28 June 2002"에서 설명된 바와 같이, 디지털 서명들은 콘텐트 상의 해시를 계산하고 공용키 암호화를 사용하여 해시를 서명하는 것에 의해 수행될 수 있다.

서명들의 위치에 관하여 본 발명의 두가지 변화들이 있다.

본 발명의 제 1 변화에서, 메타데이터 개체(TVAMain과 같은)는 서명 조각들로 확장되어, 이는 서명 정보를 포함할 것이다. 이는 서명들이 분배될 때 및 TV-애니타임에 의해 지시되는 바와 같이 일반 분배 시스템 내에서 액세스될 때 유익하다.

본 발명의 제 2 변화에서, 서명들은, 예를 들면, TVAMain 및 가능하게는 서명을 필요로 하는 일부 다른 요소들을 포함하는 랩퍼의 정의에 의해 개별적으로 제공된다. 이는 이것이 현재의 메타데이터 규정을 변화시키지 않을 것이며, 이는 또한 다른 TV-애니타임 문서들(예를 들면, ContentReferencingTable 및 ResolvingAuthorityRecordTable)을 포함하는 것을 허용한다는 점에서 유익하다.

본 발명에 따른 시스템은 단일 또는 다중 조각들을 통한 서명들을 지원한다. 이는 이것이 조각들의 세트를 서명할 수 있도록 하고, 이는 각각의 개별적인 조각을 서명하는 것보다 효율적이라는 장점을 갖는다. 이는 또한 기존의 메타데이터 규정 상에서 변화 레벨을 최소화하면서, 양방향 뿐만 아니라 일방향 분배 시스템에서 겸용할 수 있다는 장점을 갖는다.

상기 실시예들에서 사용된 기준들은 개별적으로 사용될 수 있지만, 이러한 기준들은 또한 보다 나은 보호를 위해, 또는 많은 조짐들에 대한 보호를 위해 제공되도록 조합될 수 있다.

상술된 실시예들은 본 발명을 제한하기 보다 설명하며, 당업자는 첨부된 청구항들의 범위로부터 벗어남이 없이 많은 대안의 실시예들을 설계할 수 있다는 것이 주의되어야 한다.

청구항들에서, 괄호들 사이에 위치된 임의의 참조 기호들은 청구항을 제한하는 것으로 해석되어서는 안된다. "포함하다"라는 단어는 청구항에 기록된 것과 다른 요소들 또는 단계들의 존재를 배제하지 않는다. 요소들 앞의 "하나"라는 단어는 이러한 복수의 요소들의 존재를 배제하지 않는다. 본 발명은 몇몇 별개의 요소들을 포함하는 하드웨어에 의해, 및 적절하게 프로그램된 컴퓨터에 의해 구현될 수 있다.

몇몇 수단을 열거하는 장치 청구항에서, 이들 수단의 몇몇은 하나의 하드웨어 및 하드웨어의 동일 아이템에 의해 구현될 수 있다. 단지 몇몇 수단들이 서로 상이한 종속항들에 기술되는 사실은 이들 수단들의 조합이 장점으로 사용될 수 없다는 것을 나타내지 않는다.

물론, 상기 기술들은 또한 TV-애니타임의 범위 안과 밖 모두에서 사용될 수 있다.

(57) 청구의 범위

청구항 1.

데이터 조각들(data fragments)의 세트가 서명에 의해 보호되는, 데이터 무결성 인증(data integrity authentication) 및 데이터 보호를 제공하는 방법에 있어서,

상기 세트의 각 데이터 조각은 그 자신의 고유한 식별자를 포함하며,

상기 서명은 상기 세트의 상기 데이터 조각들의 상기 각각의 고유한 식별자들에 대한 참조들을 포함하는 것을 특징으로 하는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 2.

제 1 항에 있어서, 상기 세트는 다중 서명들에 의해 보호되고, 상기 다중 서명들은 상이한 소스들로부터 시작(originate)될 수 있는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 3.

제 1 항에 있어서, 각각의 데이터 조각에 대하여 해시(hash)가 생성되고 상기 세트의 상기 데이터 조각들의 상기 해시들은 상기 서명을 계산하는데 사용되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 4.

제 1 항에 있어서, 상기 데이터 조각들은 XML로 표현되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 5.

제 1 항에 있어서, 상기 데이터 조각들은 TV-애니타임(TV-Anytime) 메타데이터를 구성하는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 6.

제 1 항에 있어서, 상기 서명은 xmldsig 표준에 따라 저장되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 7.

제 1 항에 있어서, 데이터 조각들의 상기 세트는 데이터 조각들의 슈퍼세트 상의 변환 함수에 의해 정의되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 8.

제 1 항에 있어서, 캐놀리제이션(cannolization) 함수는 상기 서명 생성 전에 사용되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 9.

제 1 항에 있어서, 상기 참조들은 또한 상기 서명에 의해 보호되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 10.

제 1 항에 있어서, 적어도 하나의 서명 인덱스 파일이 부가되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 11.

제 1 항에 있어서, 특정 데이터 조각의 상기 고유한 식별자는 상기 특정 데이터 조각을 생성시킨 조직(organization)의 고유한 식별로 시작하는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 12.

제 11 항에 있어서, 상기 고유한 식별자는 상기 조직의 DNS 이름인, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 13.

제 1 항에 있어서, 상기 참조는, 상기 참조가 참조하는 상기 데이터 조각의 위치를 나타내는 상기 위치 지시자에 의해 수행되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 14.

제 13 항에 있어서, 상기 위치 지시자는 상기 참조된 데이터 조각으로의 상기 데이터를 통한 경로를 나타내는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 15.

제 4 항에 있어서, 상기 서명은 XML 문서 내에 포함되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 16.

제 4 항에 있어서, 상기 서명은, 상기 원래 XML 데이터 문서를 포함하는 랩퍼(wrapper) XML 문서에 제공되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 17.

제 4 항에 있어서, 상기 서명은, 상기 원래 XML 데이터 문서를 참조하는 개별적인 XML 문서에 제공되는, 데이터 무결성 인증 및 데이터 보호 제공 방법.

청구항 18.

데이터 무결성 인증 및 데이터 보호를 제공하기 위한 시스템(20)으로서,

상기 시스템은 데이터 조각들을 수신하고 처리(handle)하도록 배열되고, 데이터 조각들의 세트는 서명에 의해 보호될 수 있는, 상기 시스템(20)에 있어서,

상기 시스템은 상기 세트의 데이터 조각들을 수신하고 처리하기 위한 수단을 포함하며, 각각의 데이터 조각은 고유한 식별자에 의해 식별되며,

상기 시스템은,

상기 세트의 상기 보호된 데이터 조각들의 고유한 식별자들을 사용하여 상기 세트의 상기 보호된 데이터 조각들과 서명을 연관시키기 위한 수단,

상기 보호된 데이터 조각들의 상기 고유한 식별자들을 사용하여 상기 세트와 연관된 서명을 검증하기 위한 수단,

상기 보호된 데이터 조각들의 고유한 식별자들에 의해 상기 보호된 데이터 조각들을 참조하는 서명을 생성하기 위한 수단 중 적어도 하나를 더 포함하는 것을 특징으로 하는, 데이터 무결성 인증 및 데이터 보호 제공 시스템(20).

청구항 19.

데이터 무결성 인증 및 데이터 보호를 제공하기 위한 서명 디바이스(13-15)로서,

상기 디바이스는 데이터 조각들을 처리하도록 배열되고,

상기 디바이스는 데이터 조각들의 세트를 보호하기 위한 서명을 생성하도록 배열되는, 상기 서명 디바이스에 있어서,

상기 디바이스는 상기 데이터 조각에 포함된 고유한 식별자에 의해 보호될 각각의 데이터 조각을 어드레싱하도록 배열되고,

상기 디바이스는 상기 세트의 상기 데이터 조각들을 참조하기 위한 상기 고유한 식별자들을 포함하는 서명 정보를 생성하도록 배열되는 것을 특징으로 하는, 서명 디바이스.

청구항 20.

데이터 무결성 인증 및 데이터 보호를 검증하기 위한 검증 디바이스(10)로서,

상기 디바이스는 데이터 조각들을 처리하도록 배열되고,

상기 디바이스는 데이터 조각들의 세트를 보호하기 위한 서명을 검증하도록 배열되는, 상기 검증 디바이스에 있어서,

상기 디바이스는 상기 데이터 조각에 포함되는 고유한 식별자에 의해 보호될 각각의 데이터 조각을 어드레싱하도록 배열되고,

상기 디바이스는 상기 세트의 상기 데이터 조각들을 참조하기 위한 상기 고유한 식별자들을 포함하는 서명 정보를 검증하도록 배열되는 것을 특징으로 하는, 검증 디바이스.

청구항 21.

데이터 조각들을 포함하는 신호(11)로서, 데이터 조각들의 세트가 서명에 의해 보호되는, 상기 신호에 있어서,

상기 세트의 각 데이터 조각은 그 자신의 고유한 식별자를 포함하고,

상기 서명은 상기 세트의 상기 데이터 조각들의 상기 고유한 식별자들에 대한 참조들을 포함하는 것을 특징으로 하는, 신호.

청구항 22.

제 1 항의 방법을 구현하기 위한 컴퓨터 프로그램 제품(12).

요약

본 발명은 TV-애니타임 메타데이터 무결성(metadata integrity)의 보호를 위한 방법, 시스템, 디바이스 및 신호와, 그에 따라 이러한 보호된 정보를 운반하는 신호에 관한 것이다. 보호는 서명 및 증명 방법을 적용함으로써 획득된다. 선택적으로, 캐놀리제이션(cannolization) 또는 변환 함수의 부가적인 단계가 사용된다. 데이터 조각들은 고유한 식별자로 라벨링될 수 있으므로, 그들은 참조될 수 있고 개별적으로 또는 몇몇 상이한 당사자들에 의한 세트로 분리적으로 서명될 수 있다.

대표도

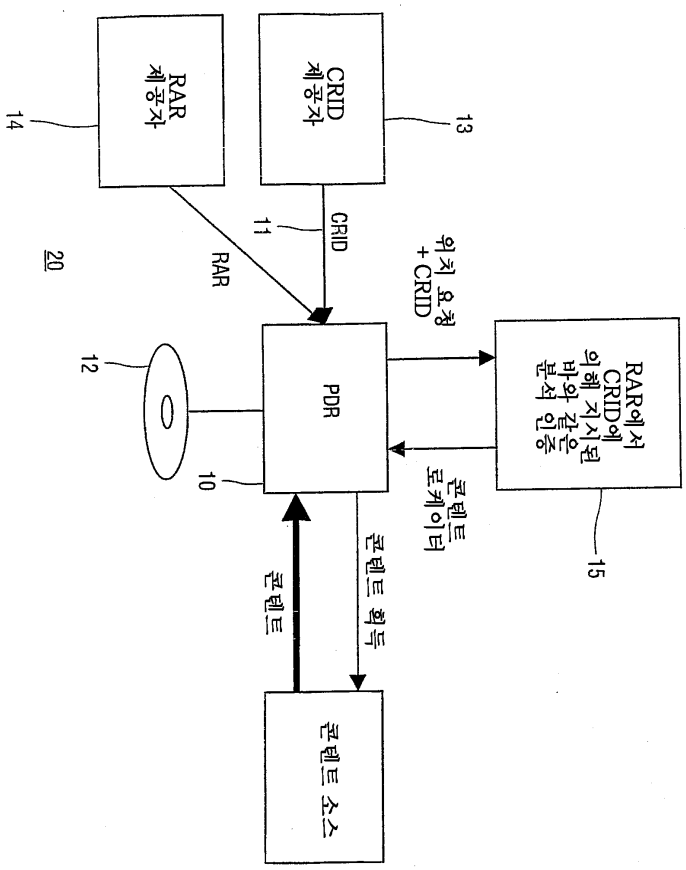
도 1

색인어

TV-애니타임, 메타데이터, 데이터 무결성 인증, 데이터 조각, XML 문서

도면

도면1



도면2

- TVA 메인
  - 분류 테이블
    - CS 별명
    - 분류 방식
  - 프로그램 설명
    - 프로그램 정보 테이블
      - 프로그램 정보
    - 그룹 정보 테이블
      - 그룹 정보
    - 프로그램 위치 테이블
      - 방송 이벤트
      - 스케줄
    - 서비스 정보 테이블
      - 서비스 정보
    - 신용 정보 테이블
      - 개인 이름
      - 조직 이름
    - 프로그램 리뷰 테이블
      - 프로그램 리뷰들
    - 세그먼트 정보 테이블
      - 세그먼트 정보
      - 세그먼트 그룹 정보
    - 수요 프로그램 위치

도면3a

```
<SimpleType name="TVASignatureIdType">
  <restriction base="string">
    <whiteSpace value="collapse"/>
  </restriction>
</simpleType>
```

이름	정의
TVASignatureIdType	메타데이터의 이러한 인스턴스 내의 동일한 타입의 다른 조각들 중에서 이러한 조각을 고유하게 식별하는 각각의 TVA 조각에 선택적 식별자를 부가하는데 사용되는 간단한 타입

도면3b

```
<attribute name="TVASignatureId"
    type="TVASignatureIdType " use="optional">
```

도면3c

```
<TVASignatureId> "MyCompagny.com;1283bshdga7213"
</TVASignatureId>
```

도면4a

```
<element name="TVASignatureWrapper"
    type="TVASignatureWrapperType"/>
<complexType name="TVASignatureWrapperType" >
  <attribute name="TVAMain"
    type="TVAMainType" use="optional"/>
  <attribute name="ContentReferencingTable"
    type= "ContentReferencingTableType" use="optional"/>
  <attribute name="ResolvingAuthorityRecordTable"
    type= "ResolvingAuthorityRecordTableType" use="optional"/>
  <attribute name="SignatureTable"
    type= "TVASignatureTableType" use="required"/>
  <attribute name="KeyInfoTypeTable"
    type= "KeyInfoTableType" use="required"/>

  <attribute name="version" type="integer" use="optional"/>
  <attribute ref="xml:lang" default="en" use="optional"/>
  <attribute name="publisher" type="string" use="optional"/>
  <attribute name="publicationTime" type="dateTime" use="optional"/>
  <attribute name="rightsOwner" type="string" use="optional"/>
  <attribute name="copyrightNotice" type="string" use="optional"/>
</complexType>
```

도면4b

이름	정의
TVA 서명 랩퍼	TV-애너타임 데이터 및 동반한 서명들을 갖는 복잡한 타입
TVA 메인	서명 리스트 내의 서명들에 의해 서명된 조각들을 갖는 TVA 메인 인스턴스
콘텐트 참조 테이블	서명 리스트 내의 서명들에 의해 서명된 콘텐트 참조 테이블
분석 인증 기록 테이블	서명 리스트 내의 서명들에 의해 서명된 분석 인증 기록 테이블
서명 테이블	데이터 요소들의 서명들을 갖는 리스트
키 정보 테이블	키 정보 랩퍼 객체들을 갖는 리스트
버전	설명에서 규정된 버전
xml:lang	설명의 언어를 규정
발행자	설명의 발행자의 이름을 규정
발행 시간	메타데이터 설명이 발행된 시간을 규정
권리 소유자	설명에 대한 권리를 갖는 엔티티를 규정
저작권 고지	설명 문서에 대한 저작권 정보를 규정

도면4c

```
<complexType name="TVASignatureTableType">
  <sequence>
    <element name="Signature"
      type="ds:SignatureType" minOccurs="0"
      maxOccurs="unbounded"/>
  </sequence>
</complexType>
```

이름	정의
서명 테이블 타입	서명들의 리스트를 포함하는 복잡한 타입
서명 리스트	서명 정보 요소들의 리스트

도면5

```
<complexType name="KeyInfoWrapperType">
    attribute name="Identifier" type="string" use="required"/>
    attribute name="KeyInfo" type="tds:KeyInfoType" use="required"/>
</complexType>

<complexType name="KeyInfoTableType">
    <sequence>
        <element name="KeyInfoWrapper"
            type="KeyInfoWrapperType" minOccurs="0"
            maxOccurs="unbounded"/>
    </sequence>
</complexType>
```

이름	정의
키 정보 랩퍼 타입	TVA 메인 내에 기존의 서명들을 포함하는 복잡한 타입
식별자	키 정보 객체의 고유한 식별자
키정보	키 정보
키 정보 리스트 테이블 타입	키 정보 랩퍼들의 리스트
키 정보 랩퍼	식별을 갖는 키 정보