(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년09월14일
(11) 등록번호 10-0982166
(24) 등록일자 2010년09월08일

(51) Int. Cl.
H04N 7/16 (2006.01) *H04N 7/167* (2006.01)
(21) 출원번호 10-2004-7018821
(22) 출원일자(국제출원일자) 2003년05월21일
심사청구일자 2008년05월21일
(85) 번역문제출일자 2004년11월22일
(65) 공개번호 10-2004-0111681
(43) 공개일자 2004년12월31일
(86) 국제출원번호 PCT/IB2003/001940
(87) 국제공개번호 WO 2003/098931
국제공개일자 2003년11월27일
(30) 우선권주장
02076998.0 2002년05월22일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
KR1020010050111 A*
US20020157002 A1*
US20020186844 A1*
WO2002009100 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
코닌클리케 필립스 일렉트로닉스 엔.브이.
네델란드왕국, 아인드호펜, 그로네보드스베그 1
(72) 발명자
캄퍼만,프란시스커스,엘.,에이.,제이.
네델란드, 아아 아인트호펜 엔엘-5656, 홀스트란 6
존커,윌렘
네델란드, 아아 아인트호펜 엔엘-5656, 홀스트란 6
(뒷면에 계속)
(74) 대리인
장훈

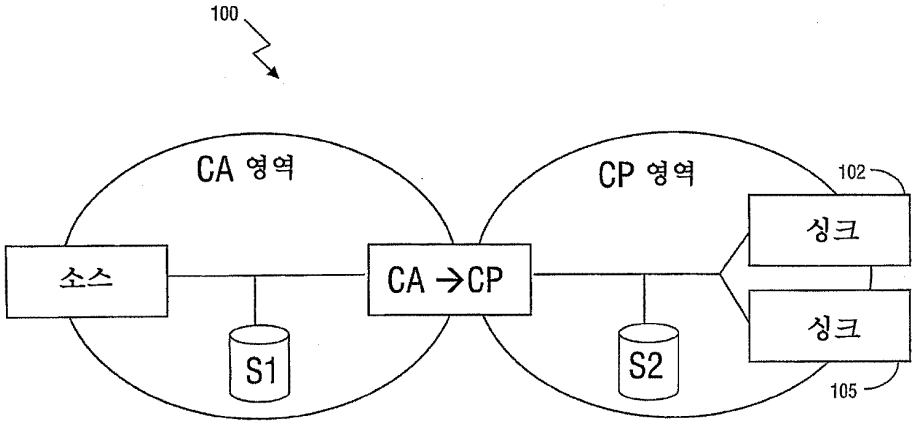
전체 청구항 수 : 총 30 항 심사관 : 조재신

(54) 디지털 권한 관리 방법 및 시스템

(57) 요 약

한 세트의 상호간에 인증되는 디바이스들을 포함하는 도메인에서 콘텐트 아이템에 대한 액세스를 제어하는 방법은, 콘텐트 아이템과 연관된 권한으로부터 도메인에 국한된 하나 이상의 도메인 특정 권한들을 도출하는 단계, 및 도메인 내 디바이스들이 콘텐트 아이템에 대해 액세스하도록 허용하는 단계를 포함한다. 시스템은 한 세트의 상호간에 인증되는 디바이스들을 포함하고, 상기 세트는 도메인을 구성하며, 시스템은 상기 방법을 실행하도록 구성된 중앙 권한 관리자를 포함한다.

대 표 도



(72) 발명자

르느와르,페트루스,제이.

네델란드, 아아 아인트호펜 엔엘-5656, 홀스트란 6

반덴휴벨,세바스찬,에이.,에프.,에이.

네델란드, 아아 아인트호펜 엔엘-5656, 홀스트란 6

특허청구의 범위

청구항 1

도메인의 멤버들인 디바이스들의 세트를 포함하는 상기 도메인에서의 콘텐트 아이템에 대한 액세스를 제어하는 방법으로서, 상기 디바이스들이 상기 콘텐트에 대한 액세스를 관리하는 디지털 권한 관리 시스템을 구현하는, 상기 콘텐트 아이템에 대한 액세스 제어 방법에 있어서,

고유의 도메인 식별자에 의해 도메인을 식별하는 단계로서, 상기 도메인 식별자는 상기 도메인의 모든 디바이스들에 저장되는, 상기 도메인 식별 단계;

상기 도메인에서, 상기 콘텐트 아이템과 연관된 디지털 권한으로부터 하나 이상의 도메인 특정 디지털 권한들을 도출하는 단계로서, 상기 하나 이상의 도메인 특정 디지털 권한들은 상기 디지털 권한 관리 시스템을 통해 상기 도메인에 제한되는, 상기 도메인 특정 디지털 권한들 도출 단계; 및

상기 도메인 내 상기 디바이스들이 상기 콘텐트 아이템에 액세스하도록 허용하는 단계를 포함하는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 2

제 1 항에 있어서,

상기 콘텐트 아이템과 연관된 상기 권한은, 그것이 호환(compliant) 소스로부터 발원된 경우에만 상기 도메인에 임포트(import)되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 3

제 1 항에 있어서,

상기 콘텐트 아이템과 연관된 상기 권한이 상기 도메인으로부터 취소(revoke) 또는 제거되는 경우, 상기 하나 이상의 도메인 특정 권한들이 취소되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 4

제 1 항에 있어서,

상기 콘텐트 아이템은 상기 콘텐트 아이템과 연관된 상기 권한과 함께 착탈식 저장 매체(removable storage medium)상에 저장되며, 상기 착탈식 저장 매체가 1회-생성 복제(one-generation copy)를 허용한다는 것을 나타내는 경우에만 상기 하나 이상의 도메인 특정 권한들이 도출되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 5

제 1 항에 있어서,

상기 콘텐트 아이템은 상기 콘텐트 아이템과 연관된 상기 권한과 함께 착탈식 저장 매체상에 저장되며, 상기 착탈식 저장 매체가 상기 콘텐트 아이템의 단일 복제를 허용한다는 것을 나타내는 경우에만 상기 하나 이상의 도메인 특정 권한들이 도출되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 6

제 1 항에 있어서,

상기 콘텐트 아이템은 상기 콘텐트 아이템과 연관된 상기 권한과 함께 착탈식 저장 매체상에 저장되며, 상기 착탈식 저장 매체가 상기 콘텐트 아이템의 복제를 허용하지 않는다는 것을 나타내는 경우에도 상기 하나 이상의 도메인 특정 권한들이 도출되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 7

제 1 항에 있어서,

상기 콘텐트 아이템은 상기 콘텐트 아이템과 연관된 상기 권한과 함께, 착탈식 저장 매체상에 저장되며, 상기

착탈식 저장 매체가 상기 콘텐트 아이템의 복제를 더 이상 허용하지 않음을 나타내는 경우에도 상기 하나 이상의 도메인 특정 권한들이 도출되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 8

제 1 항에 있어서,

상기 콘텐트 아이템과 연관된 상기 권한은 미리 결정된 횟수만큼 실행될 수 있는 권한이며, 상기 콘텐트 아이템과 연관된 상기 권한으로부터 도출된 도메인 특정한 권한들의 수는 상기 미리 결정된 횟수에 대응하는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 9

제 1 항 또는 제 8 항에 있어서,

상기 콘텐트 아이템과 연관된 상기 권한으로부터 도출된 상기 하나 이상의 도메인 특정 권한들은 미리 결정된 횟수를 실행할 수 있는 권한들인, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 10

제 9 항에 있어서,

상기 하나 이상의 도메인 특정 권한들이 실행될 수 있는 상기 미리 결정된 횟수는 1회인, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 11

제 9 항에 있어서,

상기 하나 이상의 도메인 특정 권한들이 실행될 수 있는 상기 미리 결정된 횟수는 상기 콘텐트 아이템과 연관된 상기 권한에 의해 결정되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 12

제 9 항에 있어서,

상기 하나 이상의 도메인 특정 권한들이 실행될 수 있는 상기 미리 결정된 횟수는 상기 도메인의 특성인, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 13

제 9 항에 있어서,

상기 하나 이상의 도메인 특정 권한들이 실행될 수 있는 상기 미리 결정된 횟수는, 상기 콘텐트 아이템이 상기 도메인에 임포트되는 상기 디바이스의 특성인, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 14

제 1 항에 있어서,

상기 콘텐트 아이템은 자유롭게 복제되는 것이 허용되고, 상기 콘텐트 아이템과 연관된 상기 권한의 단일 표본은 상기 도메인에 존재하도록 허용되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 15

제 1 항에 있어서,

상기 도메인 내 모든 디바이스는 하나 이상의 도메인 식별자들을 갖고, 적어도 하나의 동일한 도메인 식별자를 갖는 다른 디바이스들과만 통신하는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 16

제 15 항에 있어서,

상기 도메인에서의 디바이스에 스스로를 성공적으로 인증시키는 새로운 디바이스는 상기 하나 이상의 도메인 식별자들 중 하나 이상을 수신하는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 17

제 16 항에 있어서,

상기 도메인 내 모든 디바이스는 디바이스 식별자를 갖고, 상기 하나 이상의 도메인 식별자들은 상기 도메인의 멤버들인 디바이스들에 대한 디바이스 식별자들의 리스트를 포함하는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 18

제 16 항에 있어서,

상기 새로운 디바이스는 중앙 제어기 디바이스로부터 상기 하나 이상의 도메인 식별자들 중 상기 하나 이상을 수신하는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 19

제 18 항에 있어서,

상기 새로운 디바이스는 상기 도메인 내 대다수의 상기 디바이스들에 의한 승인 여하에 따라 중앙 제어기 디바이스로부터 상기 하나 이상의 도메인 식별자들 중 상기 하나 이상을 수신하는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 20

제 18 항에 있어서,

상기 하나 이상의 도메인 식별자들은 상기 중앙 제어기 디바이스의 디바이스 식별자를 포함하는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 21

제 15 항에 있어서,

특정 디바이스가 상기 도메인으로부터 이탈 또는 제거될 때, 상기 특정 디바이스에 저장된 상기 하나 이상의 도메인 식별자들을 삭제하는 것을 포함하는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 22

제 1 항에 있어서,

상기 도메인 특정 권한들의 수는 미리 결정된 양으로 제한되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 23

제 1 항에 있어서,

상기 콘텐트 아이템의 재생에 관한 상기 도메인 특정 권한들의 수는 미리 결정된 양으로 제한되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 24

제 22 항 또는 제 23 항에 있어서,

상기 미리 결정된 양은 상기 콘텐트 아이템과 연관된 상기 권한에 의해 결정되는, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 25

제 1 항에 있어서,

상기 디바이스들의 세트는 상호 인증된 디바이스들인, 콘텐트 아이템에 대한 액세스 제어 방법.

청구항 26

도메인의 멤버들인 디바이스들의 세트를 포함하는 시스템으로서, 상기 디바이스들은 콘텐트에 대한 액세스를 관리하는 디지털 권한 관리 시스템을 실행하고, 상기 세트는 도메인을 구성하는, 상기 시스템에 있어서,

상기 도메인에서,

고유의 도메인 식별자에 의해 도메인을 식별하기 위한 것으로서, 상기 도메인 식별자는 상기 도메인의 모든 디바이스들에 저장되고,

상기 콘텐트 아이템과 연관된 디지털 권한으로부터 하나 이상의 도메인 특정 디지털 권한을 도출하기 위한 것으로서, 상기 하나 이상의 도메인 특정 디지털 권한들이 상기 디지털 권한 관리 시스템을 통해 상기 도메인에 제한되며,

상기 도메인 내의 상기 디바이스들이 상기 콘텐트 아이템에 액세스하도록 허용하기 위한 수단을 포함하는 중앙 권한 관리자를 포함하는, 시스템.

청구항 27

제 26 항에 있어서,

상기 도메인 내 모든 디바이스는 하나 이상의 도메인 식별자들을 갖고, 적어도 하나의 동일한 도메인 식별자를 갖는 다른 디바이스들과만 통신하도록 구성되는, 시스템.

청구항 28

제 27 항에 있어서,

상기 도메인 내 디바이스는 새로운 디바이스를 인증하고, 성공적 인증시 상기 하나 이상의 도메인 식별자들을 상기 새로운 디바이스에 공급하도록 구성되는, 시스템.

청구항 29

제 28 항에 있어서,

상기 새로운 디바이스를 인증하도록 구성된 상기 디바이스는 중앙 제어기 디바이스이고, 상기 하나 이상의 도메인 식별자들은 상기 중앙 제어기 디바이스의 디바이스 식별자를 포함하는, 시스템.

청구항 30

제 26 항에 있어서,

상기 디바이스들의 세트는 상호 인증된 디바이스들인, 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 한 세트의 상호 인증된 디바이스들을 포함하는 도메인에서 콘텐트 아이템에 대한 액세스를 제어하는 방법에 관한 것이다. 본 발명은 또한 한 세트의 상호 인증된 디바이스들을 포함하는 시스템에 관한 것으로, 상기 세트는 도메인(domain)을 구성한다.

배 경 기 술

[0002] 최근에, 콘텐트 보호 시스템들의 양이 빠르게 성장하고 있다. 이들 시스템들 중 일부가 불법 복제에 대해 콘텐트를 보호할 뿐이고, 이외 다른 시스템들은 사용자가 콘텐트에 액세스하는 것을 금지하고 있다. 첫 번째 범주는 복제 보호(CP) 시스템들이라 한다. CP 시스템들은 이러한 유형의 콘텐트 보호가 저렴하게 구현될 것으로 생각되고 콘텐트 제공자와의 양방향 상호작용을 필요로 하지 않기 때문에, 통상적으로 주로 소비자 전자(CE) 디바

이스들에 초점을 맞추어 왔다. 일부 예들로서는 콘텐트 스크램블링 시스템(CSS), DVD ROM 디스크들 및 DTCP의 보호 시스템, IEEE 1394 접속들을 위한 보호 시스템이다.

[0003] 두 번째 범주는 몇 가지 명칭들 하에 알려져 있다. 방송계에서, 이러한 범주의 시스템들은 일반적으로 조건부 액세스(CA) 시스템들로 알려져 있으며, 반면 인터넷계에서 이들은 일반적으로 디지털 권한 관리(DRM) 시스템들로서 알려져 있다.

[0004] 몇몇 유형의 CP 시스템들은 또한 인터페이스하는 CA 또는 DRM 시스템들에 서비스들을 제공할 수 있다. 예들로서는 DVB-CPT 서브-그룹 및 TV-Anytime RMP 그룹에 의해 현재 개발중에 있는 시스템들이다. 목적은 한 세트의 디바이스들이 양방향 접속을 통해 서로를 인증할 수 있는 시스템이다. 이러한 인증에 기초하여, 디바이스들은 서로를 신뢰할 것이며, 이에 따라 그것들은 보호된 콘텐트를 교환할 수 있을 것이다/교환하도록 허용할 것이다. 동반되는 라이센스들은 사용자가 어떤 권한을 갖고 있는지와 콘텐트에 어떤 조작들이 수행되도록 허용되는지를 기술한다. 라이센스는 특정 댁내의 디바이스들 간에만 교환되는 몇몇 일반적인 네트워크 비밀에 의해 보호된다. 이러한 디바이스들의 네트워크를 허가된 도메인(AD: authorized domain)이라 부른다.

[0005] 허가된 도메인의 개념은 콘텐트 소유자들(이들의 저작권에 대한 보호를 원하는) 및 콘텐트 소비자들(콘텐트에 대한 제한되지 않은 사용을 원하는)의 이익을 모두 서비스하기 위한 해결책을 찾고자 하는 것이다. 기본 원리는 콘텐트가 허가된 도메인의 경계를 넘지 않는 한 콘텐트를 비교적 자유롭게 사용할 수 있는 제어된 네트워크 환경을 갖는 것이다. 통상, 허가된 도메인들은 가정 환경 주변의 중앙에 놓여지고, 또한 홈 네트워크라고 칭한다. 물론, 다른 시나리오들이 또한 가능하다. 사용자는 예를 들면 여행 중에 휴대용 텔레비전을 가지고 가서, 호텔 룸에서, 집에 있는 자신의 개인용 비디오 레코더에 저장되어 있는 콘텐트를 액세스하기 위해 이를 사용할 수도 있을 것이다. 휴대용 텔레비전이 홈 네트워크 밖에 있을지라도, 이것은 사용자의 허가된 도메인의 일부이다.

[0006] 홈 네트워크는 몇몇 종류의 네트워크 기술(예를 들면, 이더넷, IEEE 1394, BlueTooth, 802.11b,...)을 사용하여 상호접속되는 디바이스들의 세트로서 정의될 수 있다. 네트워크 기술은 상이한 디바이스들이 통신하도록 할지라도, 이것은 디바이스들이 상호연동하게 하는데 충분하지 않다. 이를 행할 수 있기 위해서, 디바이스들은 네트워크 내 다른 디바이스들에 있는 기능들을 발견하여 어드레스할 수 있도록 요구된다. 이러한 상호운용성(interoperability)은 홈 네트워킹 미들웨어(HN-MW)에 의해 제공된다. 홈 네트워킹 미들웨어의 예들은 Jini, HAVi, UPnP, AVC이다.

[0007] 네트워크 기술 및 HN-MW의 사용은 개개의 디바이스들의 세트를 하나의 거대한 가상 디바이스로서 볼 수 있게 해준다. HN-MW 견지에서, 네트워크는 사용 및 접속될 수 있는 한 세트의 기능들로서 보여질 수 있다. 이러한 시스템은 사용자에게 홈 네트워크 내 어느 곳이든 이로부터 임의의 콘텐트 또는 서비스를 어드레스할 수 있는 능력을 제공한다.

[0008] HN-MW는 두 가지 서비스들을 제공하는 시스템으로서 정의될 수 있다. 이것은 네트워크 내 애플리케이션이 네트워크에서 디바이스들 및 기능들을 찾을 수 있게 한다. 또한, 원격 프로시져 호출들(RPC)과 같은 어떤 종류의 메커니즘은 이들 기능들의 사용 방법을 정의한다.

[0009] NN-MW 견지에서, 안전한 콘텐트를 취급하는 것에 관한 시스템들은 몇 가지 방법들로 나타난다. 네트워크 내 특정 기능들은 보호된 콘텐트에 대한 액세스를 요구한다. 네트워크 내 다른 기능들은 콘텐트 보안을 다루는 네트워크 내 요소들에 의해 사용될 수 있는 기능성을 제공한다. 또한, OPIMA와 같은 보안 프레임워크들은 HN-MW를 사용하여 서로를 찾아 상호운용가능한 방식으로 통신할 수 있다. 물론, 허가된 도메인들은 다른 방법들로 구현될 수 있다.

[0010] 홈 네트워크들에서 DRM의 사용에 대한 보다 광범위한 소개를 위해, F.L.A.J. Kamperman, S.A.F.A. van den Heuvel, M.H. Verberkt, Digital Rights Management in Home Networks, Philips Research, The Netherlands, IBC 2001 conference publication vol. I, 70-77 페이지들을 참조할 수 있다.

[0011] 허가된 도메인들의 개념을 어느 정도 구현하는 다양한 시스템들이 이미 존재한다. 이러한 시스템들의 예들은 SmartRight(Thomson Multimedia), xCP(4C, 주로 IBM), 및 NetDRM (Matshushita)이다.

[0012] SmartRight 시스템은, 특히, 다음의 특성들을 갖는다:

[0013] ·스마트 카드들은 모든 디바이스들에 삽입될 수 있다.

[0014] ·시스템은 이들 스마트 카드들의 인증을 사용한다.

[0015] ·시스템은 공통 네트워크 비밀을 사용한다.

[0016] ·도메인에 부가된 신규 스마트 카드들은 네트워크 비밀을 수신할 것이다.

[0017] ·모든 스마트 카드들은 도메인에서 라이센스들(=권한들)을 열 수 있다.

[0018] xCP 시스템은, 특히, 다음의 특성들을 갖는다:

[0019] ·공통 네트워크 비밀(키 스페이스)을 사용한다.

[0020] ·MKB 구조에 기초한 키 스페이스들

[0021] ·디바이스들이 부가될 때, 키 스페이스들이 병합된다.

[0022] ·또한 새로운 공통 비밀(Media_key)이 이후 발생된다.

[0023] ·모든 라이센스들은 새로운 비밀로 다시 암호화된다.

[0024] ·중앙의 도메인 관리자는 병합이 허용되는지를 결정한다.

[0025] NetDRM 시스템은, 특히, 다음의 특성들을 갖고 있다:

[0026] ·도메인에 디바이스를 등록시키는 중앙 서버. 이 서버는 댁내에 또는 외부 네트워크에 있을 수 있다.

[0027] ·네트워크(도메인) 비밀을 사용한다.

[0028] ·비밀은 댁내에 있을 수도 있을 중앙 서버로부터 분배된다.

[0029] ·라이센스들은 통상 외부 네트워크에 저장되지만, 국부적으로 저장될 수도 있다.

[0030] 가상 사설 네트워크들(VPNs)이 어느 정도 유사하게 고려될 수 있지만, 이들의 목적, 따라서 이들의 구현은 상이하다. 개략적으로, VPN들의 목적은 내부적으로 발생된 콘텐트를 네트워크(통상 네트워크 전체에서 액세스될 수 있는)에서 유지하는 것이라 할 수 있고, 반면에 허가된 도메인들은 외부적으로 발생된 콘텐트(이를테면 구매한 저작권 보호된 콘텐트)를 도메인(통상 도메인 전체에서 액세스될 수 있는)에서 유지하려는 것이다.

발명의 상세한 설명

[0031] 본 발명의 목적은 상호 간에 인증되는 디바이스들의 세트를 포함하는 도메인에서 콘텐트 아이템에의 액세스를 제어하는 방법으로서 콘텐트 및 이 콘텐트에 연관된 권한들의 취급에 관하여 융통성 있는 방법을 제공하는 것이다.

[0032] 이러한 목적은 콘텐트 아이템과 연관된 권한으로부터 도메인에 국한되는 하나 이상의 도메인 특정 권한들을 도출하는 단계, 및 도메인 내 디바이스들이 콘텐트 아이템에 액세스하도록 허용하는 단계를 포함하는 본 발명에 따른 방법으로 달성된다. 바람직하게, 도메인 내 디바이스들은 분권화된 권한 분배 또는 다른 해결책들이 또한 가능할지라도, 도메인 내 중앙 권한 관리자 디바이스로부터 도메인 특정 권한들을 수신한다. 도메인 특정 권한들의 수는 미리 결정된 양으로 제한될 수 있다. 이것은 모든 도메인 특정 권한들에 또는 단지 '재생' 유형의 것들에만 적용할 수도 있다. 이에 의해, 무제한의 복제가 허용되지만 동시 재생을 제한한다.

[0033] 실시예에서, 하나 이상의 도메인 특정 권한들은 콘텐트 아이템과 연관된 권한이 도메인으로부터 취소 또는 제거될 경우 취소된다. 따라서, 콘텐트 아이템과 연관된 유효한 대응하는 권한이 전혀 없다면 도메인 특정 권한들을 실행하는 것은 가능하지 않다.

[0034] 콘텐트 아이템은 이에 연관된 권한과 함께 착탈식 저장 매체(removable storage medium)에 저장될 수도 있다. 이 경우, 하나 이상의 도메인 특정 권한들은 착탈식 저장 매체가 1회 생성 복제(one-generation copy)를 하는 것이 허용된다고 나타낼 경우에만 도출될 수 있을 것이다. 대안적으로, 이들은 착탈식 저장 매체가 콘텐트 아이템의 단일 복제가 허용된다고 나타낼 경우에만 도출된다. 도메인 특정 권한들을 도출하는 이러한 방식은 착탈식 저장 매체에 표시된 허용(권한들)과 일치한다.

[0035] 또 다른 옵션은 착탈식 저장 매체가 콘텐트 아이템의 복제가 허용되지 않거나 더 이상 허용되지 않음을("더 이상 허용불가" 콘텐트라 함) 나타낼지라도 하나 이상의 도메인 특정 권한들을 도출하는 것이다. 이들 옵션들에 의해서, 디스크 상의 권한이 보다 제약적이어도, 도메인 내에서 자유롭게 콤팩트 디스크 또는 디지털 다기능 디

스크와 같은 착탈식 저장 매체 상의 콘텐트를 사용하는 것이 가능해진다. 도메인 특정 권한들이 도메인에 국한되기 때문에, 사용자들이 도메인 밖에서 콘텐트 아이템을 액세스할 수 있는 위험이 없다.

[0036] 일 실시예에서 콘텐트 아이템과 연관된 권한은 미리 결정된 횟수만큼 실행될 수 있는 권한이며, 콘텐트 아이템과 연관된 권한으로부터 도출되는 도메인 특정 권한들의 수는 미리 결정된 수에 대응한다. 이것은 콘텐트에 국한된 권한들(content-bound rights)을 도메인에 국한된 권한들(doamin-bound rights)에 용이하게 매핑시킬 수 있게 한다. 콘텐트 아이템과 연관된 권한으로부터 도출되는 하나 이상의 도메인 특정 권한들은 미리 결정된 횟수, 바람직하게는 1회 사용될 수 있는 권한들일 수도 있을 것이다. 이것은 도메인 특정 권한들의 사용이 매우 제한됨으로써 콘텐트 아이템으로의 액세스에 대해 상당량의 제어를 가능하게 하는 이점이 있다. 또한, 콘텐트 아이템과 연관된 권한이 만료되었거나 또 다른 이유로 무효로 되었어도 도메인 특정 권한이 존재할 수 있다는 문제가 이제 최소화된다.

[0037] 하나 이상의 도메인 특정 권한들이 실행될 수 있는 미리 결정된 횟수는 콘텐트 아이템과 연관된 권한에 의해 표시되거나, 도메인의 특성, 또는 콘텐트 아이템이 도메인에 임포트되는 디바이스의 특성일 수도 있을 것이다. 예를 들면, 미리 결정된 횟수는 도메인의 크기에 비례하거나 또는 반비례할 수도 있을 것이다. 큰 도메인은 콘텐트를 많은 위치들에서 사용할 수 있게 하는 미리 결정된 큰 수를 가질 수 있을 것이고 또는 사용자들이 매우 큰 도메인들을 형성하는 것을 단념시키기 위해 적은 미리 결정된 수일 수도 있다. 미리 결정된 큰 수를 제공하는 임포트 디바이스들은 보다 고가로 판매될 수도 있을 것이다.

[0038] 일 실시예에서, 콘텐트 아이템은 자유롭게 복제되는 것이 허용되고, 콘텐트 아이템과 연관된 권한의 단일 표본(single specimen)이 도메인 내 존재하는 것이 허용된다. 이것은 콘텐트 아이템이 액세스될 수 있는 위치에 대해 큰 융통성을 제공하지만, 허용 범위를 넘어서 사용자들이 권한을 실행하지 못하게 한다.

[0039] 실시예에서, 도메인 내 모든 디바이스는 하나 이상의 도메인 식별자들을 가지며, 단지 적어도 하나의 동일한 도메인 식별자를 가진 다른 디바이스들과 통신한다. 이것은 상호 인증되는 디바이스들의 도메인을 생성하는 대단히 효과적인 방법이다. 모든 도메인에 대해 단일 도메인 식별자가 존재하는 것이 바람직하다. 디바이스는 복수의 도메인들의 멤버가 될 수 있고, 따라서 복수의 도메인 식별자들을 유지한다. 도메인 내에 서브-도메인들이 있을 수도 있을 것이며 이때 디바이스들은 "메인" 도메인에 대한 도메인 식별자와 서브-도메인들에 대한 도메인 식별자들을 소유한다.

[0040] 자신을 도메인 내 디바이스에 성공적으로 인증한 새로운 디바이스는 하나 이상의 도메인 식별자들 중 하나 이상의 것을, 바람직하게는 중앙 제어기 디바이스로부터 수신한다. 이것은 도메인 내 대다수의 디바이스들에 의한 승인 여하에 따라 선택적으로 행해진다. 특정 디바이스가 도메인을 이탈하거나 또는 그로부터 제거될 경우, 그 도메인에 대한 그의 도메인 식별자가 삭제된다.

[0041] 도메인 식별자는 도메인의 멤버들인 디바이스들에 대한 디바이스 식별자의 리스트를 포함할 수 있다. 이 리스트는 쉽게 컴파일링될 수 있고, 따라서 도메인 식별자의 구현이 수월해진다. 도메인 식별자는 중앙 제어기 디바이스의 디바이스 식별자를 포함할 수 있다.

[0042] 콘텐트 아이템과 연관된 권한은 렌더 권한, 수송 권한, 2차적 저작물 권한(derivative work right) 및 유틸리티 권한 중 하나를 포함하는 것이 바람직하다. 이때, 도메인 특정 권한은 렌더 권한, 2차적 저작물 권한 및 유틸리티 권한 중 하나를 포함하는 것이 바람직하다.

[0043] 본 발명의 다른 목적은, 상호 인증된 디바이스들의 세트를 포함하는 시스템을 제공하는 것으로, 상기 세트는 도메인을 구성하며, 상기 시스템은 콘텐트 아이템과 연관된 권한으로부터 하나 이상의 도메인 특정 권한들을 도출하기 위해 배열된 중앙 권한 관리자를 포함하고, 상기 하나 이상의 도메인 특정 권한들은 도메인에 국한되고 도메인 내 디바이스들로 하여금 콘텐트 아이템으로의 액세스를 허용한다.

[0044] 바람직하게, 도메인 내 모든 디바이스는 하나 이상의 도메인 식별자들을 갖고, 적어도 하나의 동일한 도메인 식별자를 갖는 다른 디바이스들과만 통신하도록 구성된다. 이 실시예의 변형에서, 도메인 내 디바이스는 새로운 디바이스를 인증하고 성공적 인증시 새로운 디바이스에 하나 이상의 도메인 식별자들을 공급하도록 구성된다. 새로운 디바이스를 인증하도록 구성되는 디바이스는 중앙 제어기 디바이스일 수도 있을 것이며 이때 하나 이상의 도메인 식별자들은 중앙 제어기 디바이스의 디바이스 식별자를 포함한다.

[0045] 본 발명의 이들 및 다른 면들은 도면에 도시한 실시예로부터 명백해질 것이며 이를 참조로 설명한다.

실 시 예

[0050] 도면 전체에 걸쳐, 동일 참조부호는 유사 또는 대응하는 특징들을 지칭한다. 도면에 도시된 특징들 중 일부는 소프트웨어로 전형적으로 구현되며, 이에 따라 소프트웨어 엔티티들, 이를테면 소프트웨어 모듈들 또는 객체들을 나타낸다.

[0051] 시스템 구조

[0052] 도 1은 네트워크(110)를 통해 상호접속된 디바이스들(101-105)을 포함하는 시스템(100)을 개략적으로 도시한 것이다. 이 실시예에서, 시스템(100)은 댁내 네트워크이다. 전형적인 디지털 홈 네트워크는 다수의 디바이스들, 예를 들면, 라디오 수신기, 튜너/디코더, CD 플레이어, 한 쌍의 스피커들, 텔레비전, VCR, 테이프 데크 등을 포함한다. 이들 디바이스들은 통상 하나의 디바이스, 예를 들면 텔레비전이 또 다른 디바이스, 예를 들면 VCR과 같은 디바이스를 제어할 수 있게 상호접속된다. 하나의 디바이스, 예를 들면 튜너/디코더 또는 셋탑 박스(STB)는 통상 다른 디바이스들에 대해 중앙 제어를 제공하는 중앙 디바이스이다.

[0053] 통상 음악, 노래들, 영화들, TV 프로그램들, 화상들, 책들 등과 같은 것들을 포함하고 또한 대화형 서비스들도 포함하는 콘텐트는 댁내 게이트웨이 또는 셋탑 박스(101)를 통해 수신된다. 콘텐트는 또한 다른 소스들, 예를 들면 디스크들과 같은 저장 매체를 통해 또는 휴대용 디바이스들을 사용하여, 홈에 들어갈 수 있을 것이다. 소스는 광대역 케이블 네트워크, 인터넷 접속, 위성 다운링크 등으로의 접속일 수도 있을 것이다. 그러면, 콘텐트는 네트워크(110)를 통해 렌더링을 위한 싱크(sink)에 전송될 수 있다. 싱크는 예를 들면, 텔레비전 디스플레이(102), 휴대용 디스플레이 디바이스(103), 이동 전화(104) 및/또는 오디오 재생 디바이스(105)일 수 있다.

[0054] 콘텐트 아이템을 렌더링하는 정확한 방법은 디바이스의 유형 및 콘텐트의 유형에 종속한다. 예를 들면, 무선 수신기에서, 렌더링은 오디오 신호들을 생성하여 이들을 라우드스피커들에 공급하는 것을 포함한다. 텔레비전 수신기에 대해서, 렌더링은 일반적으로 오디오 및 비디오 신호들을 생성하여 이들을 디스플레이 스크린 및 라우드스피커들에 공급하는 것을 포함한다. 다른 유형들의 콘텐트에 대해서, 유사한 적합한 동작이 취해져야 한다. 렌더링은 이를테면 수신된 신호를 복호화 또는 디스크램블링하고, 오디오 및 비디오 신호들을 동기화하는 등의 동작들을 포함할 수도 있다.

[0055] 셋탑 박스(101), 또는 시스템(100) 내 임의의 다른 디바이스는 수신된 콘텐트를 기록하고 이후에 재생될 수 있게 하는 적절하게 큰 하드 디스크와 같은 저장 매체(S1)를 포함할 수 있다. 저장 매체(S1)는 셋탑 박스(101)가 접속되는 몇몇 종류, 예를 들면 DVD+RW 레코더와 같은 개인 디지털 레코더(PDR)일 수 있을 것이다. 콘텐트는 또한 콤팩트 디스크(CD) 및 디지털 다기능 디스크(DVD)와 같은 캐리어(120)에 저장된 시스템(100)에 넣어질 수 있다.

[0056] 휴대용 디스플레이 디바이스(103) 및 이동 전화(104)는 기지국을 사용하여, 예를 들면 블루투스 또는 IEEE 802.11b를 사용하여 네트워크(110)에 무선으로 접속된다. 다른 디바이스들은 통상의 유선 접속을 사용하여 접속된다. 디바이스들(101-105)이 상호작용하게 하기 위해서, 몇 가지 상호운용성 표준들이 사용가능한데, 이는 상이한 디바이스들이 메시지들 및 정보를 교환하게 하며 서로 제어할 수 있게 한다. 하나의 잘 알려진 표준은 2000년 1월에 공포되고 http://www.havi.org/ 주소로 인터넷에서 이용가능한 홈 오디오/비디오 상호운용성(HAVi) 표준이다. 다른 잘 알려진 표준들은 D2B(domestic digital bus) 표준, IEC 1030에 기술된 통신 프로토콜 및 유니버설 플러그 앤 플레이(http ://www.upnp.org)이다.

[0057] 홈 네트워크에서 디바이스들(101-105)이 콘텐트의 권한없는 복제들을 행하지 않게 보장하는 것이 중요하다. 이를 위해서, 통상 디지털 권한 관리(DRM) 시스템이라 하는 보안 프레임워크가 필요하다. 하나의 이러한 프레임워크에서, 홈 네트워크는 개념적으로는 조건부 액세스(CA) 도메인과 복제 보호(CP) 도메인으로 나뉘어진다. 통상적으로, 싱크는 CP 도메인에 위치한다. 이것은 콘텐트가 싱크에 제공될 때, CP 도메인 내 적소에 복제 보호 방식으로 인하여 콘텐트의 어떠한 권한없는 복제들도 이루어질 수 없게 한다. CP 도메인 내 디바이스들은 임시로 복제들을 만들기 위한 저장 매체를 포함할 수도 있지만, 이러한 복제들은 CP 도메인으로부터 내보내질 수 없다. 이 프레임워크는 본원과 동일 출원인에 의한 유럽 특허출원 01204668.6(대리인 문서 PHNL010880)에 기재되어 있다.

[0058] 선택된 특정의 방식에 관계없이, 보안 프레임워크를 구현하는 댁내 네트워크에서의 모든 디바이스들은 구현 요건들에 따라 그와 같이 행한다. 이러한 프레임워크를 사용하여, 이들 디바이스들은 서로를 인증하여 콘텐트를 안전하게 배포할 수 있다. 콘텐트에 대한 액세스는 보안 시스템에 의해 관리된다. 이것은 보호되지 않은 콘텐트가 권한없는 디바이스들에 자유로이 누출되는 것을 방지하며 신뢰할 수 없는 디바이스들로부터 발원한 데이터

가 시스템에 들어오는 것을 방지한다.

[0059] 도 2는 도 1의 시스템(100)을 CA 도메인과 CP 도메인으로의 개략적 분할을 도시한 것이다. 도 2에서, 시스템(100)은 소스, 싱크 및 두 개의 저장 매체들(S1, S2)을 포함한다. 대부분의 콘텐트는 셋탑 박스(101)(소스)를 통해 CA 도메인에 댁내 네트워크에 넣어진다. 통상, 싱크들, 예를 들면 텔레비전 시스템(102) 및 오디오 재생 디바이스(105)는 CP 도메인에 위치된다. 이것은 콘텐트가 싱크에 제공될 때, CP 도메인 내 적소에 복제 보호 방식으로 인해 콘텐트의 권한없는 복제들이 전혀 행해질 수 없게 한다.

[0060] CA -> CP 게이트웨이는 CA 도메인과 CP 도메인 사이에 제공된다. 이 게이트웨이는 CP 도메인에 콘텐트가 넣어지게 하는 것에 대하여 책임을 진다. 이 프로세스는 콘텐트를 트랜스코딩 및/또는 (재)암호화하는 것과, 콘텐트와 연관된 디지털 권한들을 CP 도메인에서 지원되는 포맷으로 바꾸는 것 등을 요구할 수 있다.

[0061] CP 도메인은 저장 매체(S2)를 포함하고, 이에 콘텐트의 (임시) 복제들이 복제 보호 규칙들에 따라 저장될 수 있다. 이들 복제들은 예를 들면 콘텐트의 시간 시프트된 재생을 위해 사용될 수 있지만, 이들 복제들은 CP 도메인으로부터 쉽게 내보내질 수 없다.

[0062] 디바이스는 이를 CP 도메인 내 이미 있는 또 다른 디바이스에 접속하거나, 이들 디바이스들을 접속하는 버스에 접속함으로써 CP 도메인의 일부가 된다. CP 도메인들의 급격한 변화를 방지하기 위해서, 특정 시간 기간, 예를 들면 1일간 그 특정의 CP 도메인에 있어야 함을 보장함으로써 CP 도메인들을 바꾸는 것을 그만두게 할 수도 있을 것이다.

[0063] 허가된 도메인 기능들 및 설계 원리

[0064] AD의 생성 및 관리에 요구되는 주 기능은 다음을 포함한다:

[0065] - AD 식별(이것은 AD 관리 기능으로서 간주될 수 있다)

[0066] - 디바이스 체크-인(이것은 또한 디바이스 등록이라고 칭할 수 있을 것이다)

[0067] - 디바이스 체크-아웃(이것은 또한 등록 해제라고 칭할 수 있을 것이다.

[0068] - 권한 체크-인

[0069] - 권한 체크-아웃

[0070] - 콘텐트 체크-인

[0071] - 콘텐트 체크-아웃

[0072] - AD 관리:

[0073] ·콘텐트 액세스

[0074] ·도메인에 권한의 저장

[0075] 선택된 일부 설계 원리는 다음과 같다:

[0076] ·AD의 중앙 관리(centralized management)를 하지 않는다.

[0077] ·AD 내 디바이스들의 수와 콘텐트량에 선험적 제약은 없다.

[0078] 다음과 같은 기능상의 요건들이 식별되었다:

[0079] ·도메인 내 콘텐트 액세스에 대한 선험적 제약은 없다.

[0080] ·제어된 콘텐트 및/또는 권한만이 도메인 경계들에서 교환된다.

[0081] ·호환 디바이스들(compliant devices)만이 도메인에 허용된다(비-호환 디바이스들은 고려되지 않는다.)

[0082] 다음과 같은 비-기능적 요건들이 식별되었다:

[0083] ·이 해결책은 대부분 오프-라인인 휴대용 디바이스들에 작용해야 한다.

[0084] ·AD에 대한 해결책은 전형적인 DRM 시스템 구조에 따라야 한다. 즉 디지털 권한의 사용은 콘텐트에의 액세스를 제어하기 위한 토대이다.

[0085] 허가된 도메인(AD) 식별

[0086] 허가된 도메인들을 구현할 때 문제들 중 하나는 디바이스가 도메인의 일부인지를 결정할 수 있게 하는 정보 구조를 어떻게 관리할 것인가 하는 것이다. 콘텐트가 도메인 내 디바이스에서 도메인 밖의 디바이스로 쉽게 전송되지 않는 것이 중요하다. 이러한 콘텐트 체크-아웃은 제어된 환경들 하에서 행해져야 하고, 특정 디바이스들로 제한될 수 있다. 예를 들면, DVD+RW 기록기는 DVD 재기록가능 디스크에 콘텐트를 복제하는 것이 허용될 수도 있을 것이나, 도메인 내 개인 비디오 레코더는 이에 내장된 하드 디스크에 저장된 암호화되지 않은 콘텐트를 허가된 도메인 밖의 디바이스가 읽지 못하게 해야 한다. 디바이스가 특정 허가된 도메인의 멤버인지를 결정할 수 있게 하는 여러 가지 방법들을 제공한다. 물론 다른 방법들이 또한 가능하다.

[0087] 제 1 실시예에서, 허가된 도메인은 고유 domain_id에 의해 식별된다. 이어서, 이 식별자는 허가된 도메인의 멤버인 모든 디바이스에 저장된다. 도메인 멤버 디바이스들의 완전한 세트의 개요가 있어야 한다면, 도메인을 구성하는 명확한 device_id의 리스트가 관리될 수 있다. 이 리스트는 허가된 도메인 내 중앙에 저장될 수 있다.

[0088] 이제, 디바이스가 특정 허가된 도메인의 멤버인지를 결정하는 것은 이 특정 도메인에 대한 식별자가 그 디바이스에 저장되어 있는지를 체크함으로써 간단히 행해질 수 있다. 물론, 디바이스는 호환되어야 한다.

[0089] 제 2 실시예에서, 허가된 도메인은 이 도메인을 구성하는 device_id들의 세트에 의해 식별된다. 이러한 device_id들의 세트는 허가된 도메인(또는, 택일적으로는 허가된 도메인 밖에) 내 하나의 지정된 디바이스에 저장된다. 이 해결책에서는 어떠한 명확한 domain_id도 존재하지 않는 것에 유의한다. 그러나, 이 해결책은 덜 실제적인 것으로 보인다. 두 개의 휴대용 디바이스들이 중앙 리스트와의 접속이 없을 때 이들이 통신하기를 원하는 경우, 이들은 다른 것이 AD의 멤버인지를 결정할 수 없다.

[0090] 일 실시예의 변형예에서, device_id들의 세트는 허가된 도메인의 모든 디바이스에 저장된다. 이것은 두 개의 휴대용 디바이스들이 통신하기를 원할 때 일어나는 전술한 문제를 해결하지만, 상당한 관리 복잡도를 야기하고 모든 디바이스들에 비교적 큰 저장 요건을 부과한다.

[0091] 이 실시예의 다른 변형예에서 device_id들의 세트는 허가된 도메인의 다수의 특정의 디바이스들에 저장된다. 이 또한 상당한 관리 복잡도를 야기하며 모든 디바이스들에 비교적 큰 저장 요건을 부과한다.

[0092] 디바이스 체크-인

[0093] 또 다른 중요한 문제는 호환 디바이스를 체크-인하는 방법 및 시기이다. "체크-인" 또는 "등록"은 디바이스를 허가된 도메인의 일부로서 받아들이게 하는 프로세스를 말한다. 악의적 비-호환 디바이스에 기인한 허가된 도메인으로부터의 콘텐트 누출을 방지하기 위해서, 호환 디바이스들만이 받아들여져야 한다. 이 프로세스의 예시적 실시예를 도 3에 흐름도에 나타내었다.

[0094] 체크-인 프로세스는, 단계 301에서, 부가하기를 원하는 호환 디바이스를 허가된 도메인에 이미 있는 또 다른 디바이스에 접속하는 사용자에 의해 개시된다. 이러한 디바이스가 존재한다면 허가된 도메인에 대한 중앙 서버 또는 제어기인 것이 바람직하다. 예를 들면 SmartRight와 같은 다른 시스템들은 부가될 디바이스를 허가된 도메인 내 이미 있는 임의의 디바이스에 접속함으로써 체크-인 프로세스를 개시할 수 있게 허용한다. 물론, "접속한다"라는 것은 케이블들을 사용하여 물리적 접속들을 수립하는 것에 한정하는 것은 아니다. 예를 들면, 블루투스 또는 IEEE 802.11b을 사용한 무선 접속들이 또한 수립될 수 있다.

[0095] 네트워크 접속이 수립된 후에, 다음 단계 302는 접속되는 디바이스에 의해 새로운 디바이스의 인증을 수반한다. 단계 303에서 결정된 바와 같이, 이 인증이 성공적이면, 새로운 디바이스는 단계 304에서 허가된 도메인의 일부가 된다. 그렇지 않다면, 새로운 디바이스는 단계 305에서 거절된다. 예를 들면 단지 한정된 수의 디바이스들만이 허가된 도메인에 허용되는 경우와 같이, 다른 조건들이 체크될 수도 있고, 또 다른 단계는, 이러한 한정된 수를 아직 초과하지 않음을 체크하는 것이 될 것이다.

[0096] 전술한 바와 같이, 중앙 고유 domain_id가 사용되는 경우, 단계 306에서 새로운 디바이스는 중앙 제어기로부터 또는 접속된 디바이스로부터 domain_id를 수신한다. 원한다면, 허가된 도메인 내 임의의 다른 디바이스가 새로운 디바이스에 domain_id를 공급할 수도 있을 것이다. 예를 들면 새로이 부가된 디바이스들에 domain_id들을 배포하는 것이 특정 유형들의 디바이스들에 허용되었음을 지정할 수도 있을 것이다.

[0097] 확장으로서, 새로이 부가된 디바이스는 허가된 도메인 내 임의의 디바이스로부터 domain_id를 얻을 수도 있을 것이지만, 허가된 도메인 내 이미 있는 대다수의 디바이스들이 허용되어야 한다. 따라서, 어떠한 단일의 디바이스(상대방(adversary)에 의해 변경되거나 또는 예를 들면 인증 과정에서 오류가 날 수도 있는)도 다른 디바이스

들을 도메인에 받아들 수 없다.

[0098] 또 다른 실시예에서, 도메인 발원자는 domain_id를 새로이 부가된 디바이스에 전송한다. 이 실시예에서, 모든 호환 디바이스들은 device_id를 저장하고 domain_id를 위한 저장 공간을 갖추고 있다. 도메인 발원자의 domain_id는 자신의 device_id일 것이다. 허가된 도메인에 부가된 임의의 다른 디바이스는 도메인 발원자로부터 domain_id를 수신한다.

[0099] 초기에(공장에서), 디바이스에 대해, domain_id가 device_id에 설정될 것이다. 이어서, 임의의 개개의 디바이스는 1 디바이스 크기를 갖는 AD로서 간주될 수도 있을 것이고, 디바이스는 자동으로 그 AD에 대한 도메인 발원자가 된다. AD가 증대될 때, 발원자의 디바이스는 자신의 device_id를 다른 디바이스들에 domain_id로서 제공할 것이다. 도메인 발원자의 디바이스는 나중에 device_id = domain_id인 디바이스로서 인식될 수 있다. 통상적으로, 발원자 디바이스는 대형의 정적 디바이스, 예를 들면 거실에 있는 텔레비전 세트이고 예를 들면 휴대용 디바이스는 아니다.

[0100] 이러한 두 개의 대형 정적 디바이스들이 하나의 허가된 도메인에서 접속되면, 이들 둘 중 어느 것이 도메인 발원자가 될 것인지를 결정하기 위한 교섭 프로세스(negotiation process)가 필요할 수도 있다. 이러한 교섭 프로세스는 사용자에게 도메인 발원자를 지정할 것을 요청함으로써 구현될 수 있다.

[0101] 이러한 프로토콜로서 사용자가 디바이스를 도메인 발원자에 접속할 것을 요청하므로, 도메인 발원자는 디바이스의 사용자 인터페이스에 이를 나타냄으로써, 예를 들면, 디스플레이 스크린상에 표시자를 보여주고, 특정 LED를 활성화시키는 것 등에 의해 인식될 수 있을 것이다. 사용자는 특별한 안테나 또는 장식적 요소와 같은 물리적 표시, 또는 어떤 다른 방법으로 그 외양을 변경함으로써, 도메인 발원자에 부가시킬 수도 있을 것이다.

[0102] 디바이스는, 디바이스가 호환적이고 댁내에 속할 경우에만 체크-인될 수 있다. 디바이스가 호환적인지 여부는 알려진 (인증) 메커니즘들에 의해 쉽게 체크될 수 있다. 문제들은 디바이스가 댁내에 속하는지를, 즉 어떤 것이든 동일한 도메인의 멤버가 되는 것을 방지하기 위해서, 결정하는 데 있다. 결국, 허가된 도메인들의 원리는 전역에 걸친 무제한의 콘텐트 배포를 허용하는 것이 아니라 소비자들에 의한 콘텐트 취급에 어떤 융통성을 갖게 하기 위해서 도입되었다.

[0103] SmartRight 시스템은 도메인 내 디바이스들의 수에 제한을 부과한다. 이 해결책은 도메인에 속하는 모든 디바이스들이 중앙에 등록되는 경우에 적합하다. 이 해결책에서의 문제는 스케일러블이 좋지 않고 본 설계 원리에 일치하지 않는다는 것이다.

[0104] 또 다른 해결책은 AD 도메인 제어기로부터 콘텐트의 특정 부분을 재생하기 위한 세션들의 수에 대한

제한을 부과하는 것이다. 이 해결책에서의 문제는 오프-라인 휴대용 디바이스들에 매우 적합하지 않고 본 설계 원리에 일치하지 않는다는 것이다. 이 해결책은 본원과 동일 출원인에 의한 유럽 특허출원 번호 02009651.7(대리인 문서 PHNL020372)에 기재되어 있다.

[0105] 또 다른 해결책은 도메인에서 허가된 도메인 권한 수(예를 들면, 재생 권한, 보다 자세한 것은 다음의 허가된 도메인 권한을 참조)에 제한을 부과한다. 이 방법, 예를 들면 재생 권한은 한 번에 1회만 사용될 수 있다. 이 해결책은 분산적으로 구현될 수 있으므로 본 설계 원리에 들어맞는다. 그러나, 가능한 문제는 복제 관리 방식 내에서 복제 관리 방식을 갖고 있다는 것이다(이 해결책은 바람직하게는 디바이스 등록 방식과 함께 적용되어야 한다).

[0106] 또 다른 실시예에서, 외부 제3자는 디바이스로 하여금 특정 도메인 내에서 작동되게 할 수 있다. 이러한 메시지는 방송 채널, 인터넷을 통해서, 또는 플로피 디스크들, 플래시 카드들, 스마트 카드들 등과 같은 저장 매체를 사용하여 전송될 수 있다. 이것이 유효한 방법이긴 하지만, 구현은 본원에 나타낸 모델과는 매우 상이하므로 더 이상 다루지 않겠다.

[0107] 디바이스 체크-아웃

[0108] 허가된 도메인들의 또 다른 중요한 면은 호환 디바이스를 어떻게 언제 체크-아웃할 것인가 하는 것이다. "체크-아웃" 또는 "등록 해제"는 허가된 도메인의 일부인 디바이스가 허가된 도메인을 탈퇴할 수 있게 하는 프로세스를 말한다. 허가된 도메인이 고유 domain_id에 의해 식별되면, 허가된 도메인 내 디바이스를 체크-아웃하는 것은 디바이스 내 저장된 domain_id를 삭제함으로써 구현될 수 있다.

[0109] 디바이스가 허가된 도메인으로부터 체크-아웃할 때, 사실상, 원래 허가된 도메인과 자체가 허가된 도메인으로서

간주될 수 있는 현 탈퇴한 디바이스인, 두 허가된 도메인들이 존재하게 되는 상황을 갖게 된다. 이때, 이들 두 허가된 도메인들 간에 (XAD) 권한(권한 유형에 대한 설명을 위해 이후 참조)의 분배가 행해져야 한다(체크-아웃된 XAD 권한에 속하는 AD 권한은 예를 들면 취소 메시지를 도메인에 보냄으로써 삭제되어야 한다). 이것은 (사용자에 의해) 제어되는 권한 체크-아웃 및 체크-인에 의해 구현될 것이다.

[0110] 디지털 권한 관리

[0111] 허가된 도메인 내에서의 콘텐트에는 여전히 디지털 권한 관리 규칙들이 요구된다. 콘텐트와 연관된 디지털 권한은 통상적으로 허가된 도메인에 넣어질 때 콘텐트와 함께 수신된다. 예를 들면, 권한은 웹사이트로부터 콘텐트와 함께 다운로드된 라이센스 파일에 있을 수 있거나, 또는 케이블 네트워크를 통해 수신된 MPEG-2 스트림의 일부일 수도 있을 것이다.

[0112] 권한은 또한 별도로 구입할 수 있다. 소비자는 예를 들면 상점에서 DVD 디스크와 같은 캐리어를 구입할 수 있을 것이다. 이 디스크 상의 콘텐트는 예를 들면 콘텐트 소유자의 웹사이트에서 재생 권한을 별도로 구입한 경우에만 재생될 수 있다. 이러한 재생 권한은 시간이 제한될 수도 있을 것이며, 따라서 소비자는 정기적으로 새로운 재생 권한을 구입할 수밖에 없다.

[0113] 권한은 물론 이미 AD 포맷으로 배포될 수 있을지라도 권한은 전유의 포맷들로 배포될 것으로 보인다. 권한은 다른 AD들, 즉, AD 간 통신으로부터 발원할 수도 있다. 이것은 권한을 허가된 도메인 내에서 사용되는 포맷으로 변환하는 것을 필요하게 한다. 이를 "권한 체크-인"이라 한다. 권한 체크-인에 관한 몇 가지 요건은 다음과 같다:

[0114] ·AD에 의해 집행될 수 있는 권한만을 받아들인다.

[0115] ·의무들이 수락될 수 있는 경우에만 권한을 받아들이다(한정된 수의 식별가능한 의무들이 목록을 사용하여 구현을 용이하고 간단하게 하므로 이러한 의무들이 있는 경우만을 고찰할 것이다).

[0116] ·권한에 관계된 콘텐트가 수락될 수 있는 경우에만 권한을 받아들인다(특정 콘텐트, 예를 들면, 성인용 영화들은 어린이들이 있는 가정에서는 수락될 수 없을 수도 있다).

[0117] AD 권한 관리는 3가지 유형의 동작들을 수반하는 것이 바람직하다:

[0118] - AD 권한 식별: 권한이 어떤 도메인에 속하는지를 어떻게 찾을 것인가?

[0119] - AD에 권한을 체크-인: 권한을 도메인에 어떻게 부가할 것인가?

[0120] - AD로부터 권한을 체크-아웃: 권한을 도메인으로부터 어떻게 삭제/이전할 것인가?

[0121] 권한 식별은 상이한 방법들로 동작할 수 있다:

[0122] i. 공통 AD 키는 도메인에서 권한을 암호화할 수 있다. 공통 키를 소유하는 디바이스들만이 권한 내 콘텐트 키를 사용할 수 있다.

[0123] ii. 권한은 AD 식별자를 포함할 수 있다. 호환 디바이스들은 올바른 AD 식별자를 가진 권한만을 "사용"할 것이다.

[0124] iii. 권한은 절대적으로 도메인에 국한된다. 즉 일단 도메인에 들어왔으면 이것은 도메인을 떠날 수 없다. 이것은 디바이스들에 의해서 그리고 보안 인터페이스들 상에서 보호된다.

[0125] 방법 i 및 ii의 이점은 어느 허가된 도메인에 권한이 속해 있는지가 매우 명료하다는 것이다. 그러나, 단점은 도메인 내 디바이스들의 세트에 변화가 발생할 때마다 그리고 권한이 체크-인/아웃될 때, 권한이 변경되어야 한다는 것이다(상이한 식별자/상이한 암호화).

[0126] 권한은 도메인에 호환하고 이의 출처로부터 체크-아웃이 허용되었을 경우에만 체크-인될 수 있다. 권한은 전형적인 출처는 DRM 또는 유료(pay)-TV 시스템일 것이다. 권한 체크-아웃은 권한에 의해 허용되었을 때에만 행해질 수 있다. 권한의 올바른 취급은 권한을 다루는 디바이스들의 호환에 의해 보장된다.

[0127] 본 발명에 따라 디지털 권한을 체크-인하는 프로세스의 예시적인 실시예를 도 4의 흐름도에 나타내었다. 제 1 단계(401)는 권한이 전유의 포맷으로 되어 있는지를 결정하는 것이다. 그러하다면, 다음 단계(402)는 전유 포맷에서 AD 포맷으로 권한을 변환하는 것이다. 변환이 가능하지 않다면, 또 다른 엔티티가 AD에 대한 권한을 변환 또는 해석해야 한다. 이 또한 할 수 없다면 변환이 실패되어 권한은 거절될 것이다.

[0128] AD 포맷으로 디지털 권한을 얻었으면, 다음 단계들(403, 404, 405, 407 및 408)에서는 다음의 여부를 체크한다.

[0129] a) 권한이 합법적인지, 즉, 권한/라이센스 당국에 의해 인가된 것인지(단계 403),

[0130] b) 트랜잭션이 합법적인지, 즉 이 권한을 수신/수락하도록 허용되는지(단계 404),

[0131] c) 권한이 AD에 의해 집행될 수 있는지(단계 405); 그렇지 않다면 권한을 거절 또는 강등시킨다(단계 406).

[0132] d) 의무가 AD 또는 AD 소유자에게 수락가능한지(단계 407),

[0133] e) 권한이 AD가 수락할 콘텐트를 가리키는지(단계 408).

[0134] 이들 모든 체크들이 통과되면, 권한이 AD 내 권한 관리자의 제어하에, 단계 409에서, AD에 부가된다. 이 권한 관리자는 단일의 식별가능한 엔티티가 아닐 수 있지만, 완전히 배포될 수 있다.

[0135] 물론 시스템이 원래 DRM 시스템 내 콘텐트에 관한 권한의 소유를 관리하는 것을 방해하는 것은 아무것도 없다. 따라서, 권한이 강등되었을 때, 사용자는 그래도 원래 DRM 시스템을 사용하여 권한 전부를 이용할 수 있을 것이다.

[0136] 이제 a) 및 b) 항목을 더 논하도록 하겠다. c), d), e) 항목들은 권한들의 내용 및 콘텐트에 더욱 관련된 것이고 허가된 도메인 관리에는 덜 관련된 것이므로 더 자세히 하지는 않겠다.

[0137] a) 하에 경우 II에서, 권한은 1) 권한/라이센스 당국에 의해 또는 또 다른 인가받은 측(또는 디바이스)에 의해 진정성 마크(authenticity mark)를 갖고 있는 경우, 2) 권한이, 승인된/호환 디바이스로부터 발원한 것일 경우엔 합법적인 것으로 간주한다. 이에 대해선 이를 달성하는 기술들이 알려져 있으므로 더 이상 상세히 하지는 않겠다.

[0138] b) 하에 경우 II에서, 먼저, 권한의 서로 다른 출처를 알 필요가 있다. 권한을 얻는 몇몇 예시적인 방법들은,

[0139] i. 권한은 유선 또는 무선 허가된 도메인 인터페이스를 통해 임포트될 수 있다는 것과,

[0140] ii. 권한은 (패키징된) 매체상에 피기백(piggyback)할 수 있다는 것과,

[0141] iii. 권한은 디바이스상에 피기백할 수 있다는 것과,

[0142] iv. 권한은 도메인 자체 내에서 생성될 수 있다는 것이다. 국제특허출원 WO02/065255(대리인 문서 PHNL010113)에는 콘텐트를 임포트할 때 권한을 생성할 수 있는 방법을 기재하고 있다. 몇몇 확장들이 유럽 특허출원 번호 02076209.2(대리인 문서 PHNL020246)에 기재되어 있다.

[0143] 권한의 이들 서로 상이한 출처가 있을 때: 다음의 경우라면 트랜잭션을 합법적인 것으로 간주한다.

[0144] ·당해의 그 권한을 현재의 도메인에 전송하는 것이 허용된다면, 즉 권한이 특정 도메인에 국한되지 않는 경우, 또는

[0145] ·권한이 호환 전송/통신 채널(예를 들면, 보안 인증된 채널(SAC)), 호환 디바이스, 호환 매체, 또는 호환 권한 생성 디바이스(예를 들면, 호환 A/D 변환기)로부터 발원한 경우.

[0146] 위의 항목들이 주어졌을 때, 도메인에 국한되는 권한을 갖고, 그리고 도메인들 간에 이전될 수 있는 권한을 갖게 된다. 따라서, 두 유형들의 권한, XAD 권한(또는 크로스-AD 권한) 및 AD 권한을 도입한다. AD 권한은 하나의 AD에 속한다. XAD 권한은 AD들 간에(허용된다면) 이전될 수 있다.

[0147] 다음 유형의 권한이 인식될 수 있다:

[0148] ·렌더 권한, 예를 들면, 뷰, 재생, 인쇄.

[0149] ·수송 권한, 예를 들면, 복제, 이동, 임대.

[0150] ·파생 작업 권한, 예를 들면, 추출, 삽입, 편집.

[0151] ·유틸리티 권한, 예를 들면, 백업, 캐시, 데이터 무결성

[0152] 다음 속성들은 권한에 첨부될 수 있다:

[0153] ·보수(consideration): 무엇이든 사용자가 보답으로 주어야 할 것.

[0154] ·범위: 길이; 수량, 장소, 등.

[0155] ·사용자 속성들, 가입자들, 나이, 성별, 등.

[0156] AD 권한은 수송 유형의 권한을 제외하고, 임의의 유형의 권한일 수 있다. 즉, AD 권한은 다른 AD들에 대한 수송을 위한 권한이 될 수 없다. AD 내에서 렌더 권한은 예를 들면 복제될 수 있다. XAD 권한은 임의의 유형의 권한일 수 있다. AD 권한은 허가된 도메인 내에서 사용되도록 한 것일 뿐이며 XAD 권한으로부터 도출된다. 초기에 XAD 권한은 권한 소유자로부터 발원한다. XAD 권한이 허가된 도메인으로 체크-인되면, AD 권한은 이로부터 도출될 수 있다. AD 권한은 도메인 내에서 마음대로 증식될 수도 있지만 도메인을 결코 떠날 수는 없다.

[0157] XAD 권한은 도메인간 통신을 제어하는데 사용될 것이다. 용이한 관리의 이유로, XAD 권한의 한 복제만이 허용되는 것이 바람직하다(복제들이 백업 이유로 행해지지 않는다면). 그러나, XAD 권한이 허가된 도메인을 떠난다면, 원래의 도메인에서 도출된 AD 권한은 삭제되어야 한다. 이것은 XAD 권한을 따라 취하는 디바이스로부터 취소 메시지들을 보냄으로써 행해질 수 있다.

[0158] 이제 권한 체크-인을 위한 본 발명의 해결책을 갖게 된다: XAC 권한의 체크인만을 허용하여 그 후 그것들이 호환 전송들이 호환 전송/통신/디바이스/매체/생성기로부터 발원할 경우에만.

[0159] 또한, 이제 권한 체크-아웃을 위한 본 발명의 해결책을 갖게 된다: 도메인으로부터 XAD 권한 체크-아웃만을 허용할 경우에만. 도메인으로부터의 AD 권한의 이출은 금지된다.

[0160] 콘텐트 관리

[0161] 콘텐트는 통상적으로 음악, 노래들, 영화들, TV 프로그램들, 화상들, 책들 등과 같은 것들을 포함하지만, 또한 대화형 서비스들을 포함할 수도 있을 것이다. 세 가지 유형들의 콘텐트들 간에 구별한다:

[0162] ·암호화된 콘텐트(디지털 포맷)

[0163] ·암호화되지 않았으나 워터마크된 콘텐트(이들은 디지털 포맷과 유사하다)

[0164] ·보호되지 않은 콘텐트(이들은 디지털 포맷과 유사함)

[0165] 허가된 도메인에서 디지털 권한은 콘텐트의 사용을 제어한다. 권한이 없으면, 콘텐트는 도메인에서 쓸모가 없다. 따라서, AD에서 디지털 보호된 콘텐트의 체크-인 동작은 본 발명과는 관계가 없으며 더 이상 논하지 않을 것이다.

[0166] 워터마크는 되어 있으나 암호화되지 않은 콘텐트인 경우, 콘텐트 체크-인이 허용되는지와 어떤 조건하에 있는지를 알기 위해서 임포팅 디바이스에 의해 워터마크가 체크되어야 한다. 이 체크-인이 허용된 경우, 콘텐트는 임포트되고 그에 따른 권한이 생성된다. 콘텐트를 임포트한 후에는 이를 보호하기 위해 암호화하는 것이 바람직하다.

[0167] 보호되지 않은 콘텐트의 경우, 콘텐트가 임포트될 것이고 수반하는 권한이 생성될 것이다.

[0168] 대안적인 방법은 일부 권한은 승인되고 일부는 승인되지 않는 것인, 콘텐트에 설정된 제한을 허가된 도메인이 집행하게 하는 것이다. 보호되지 않은 콘텐트(법 또는 라이센스에 의해 어떠한 사용 제약도 검출될 수 없는 콘텐트)의 경우, 이러한 집행 서브-시스템은 필요하지 않다. 따라서 콘텐트는 제약없이 자유롭게 이동할 수 있고 임포트될 필요가 없다.

[0169] 콘텐트 체크-아웃에 관하여, 전형적으로 디지털 포맷 콘텐트가 암호화되고 다른 곳에서(권한 없이) 사용될 수 없음을 안다. 아날로그 포맷으로 콘텐트의 흐름은 어쨌든 보호될 수 없다. 이러한 콘텐트는 물론 워터마크들을 포함할 수 있고, 또는 워터마크들이 아날로그 콘텐트에 부가될 수 있다. 워터마크들을 사용하는 특별한 경우는 항상 복제 불가를 표시하여 아날로그 콘텐트의 재삽입을 방지하는 것이다. 콘텐트 체크-아웃의 문제는 여기서 더 이상 논하지 않겠다.

[0170] 콘텐트 권한이 체크-아웃될 때, 콘텐트는 다시 암호화될 필요가 있을 수 있다. 콘텐트의 보호 및 AD의 집행이 주로 권한을 제어함으로써 행해질 때, 콘텐트는 AD에 넣어지지 않았고, 권한만이 넣어진 것이라 할 수 있다.

[0171] 허가된 도메인 관리

[0172] 콘텐트는 올바른 AD 권한이 사용가능할 경우에만 도메인에 액세스될 수 있다. AD 권한은 전술한 바와 같이, 사용가능한 XAD 권한으로부터 도출된다. AD 권한은 완전한 도메인에서 유효하고, 도메인들 간에 이전이 가능하지

않다. AD 권한은 도메인 내에서 증식하도록 허용될 수 있다. 이것은 권한을 필요로 하는 도메인 내 임의의 디바이스가 권한에 무조건 액세스할 수 있을 것임을 의미한다. 권한은 도메인 내 어느 곳에든 저장될 수 있다. 그러므로 이러한 권한을 찾고 얻기 위한 방법이 제시되어야 한다. 이를 위해 상이한 전략들이 적용될 수 있다. 이들 방법들은 일반적으로 중앙집중된 저장 방법들 및 분권화된 저장 방법들로 나뉘어질 수 있다.

[0173] 권한의 중앙집중된 저장의 경우에는 특정의 권한을 얻기 위해 접촉될 중앙 권한 관리자가 있다. 권한의 분권화된 저장의 경우에는 도메인 내 권한을 찾아 얻기 위해서 분산 탐색 메커니즘이 사용된다. 실제로 권한은 거의/항상 온에 있는 디바이스들에 위치하여 있어야 하는 것과 권한은 대개는 콘텐트와 동일한 디바이스에 저장되는 것에 유의한다.

[0174] 몇몇 (AD) 권한에 대해서, 권한(도메인 내에서), 예를 들면 무제한 재생 권한의 다수의 경우들/복제들을 갖는 것이 수락될 수 있다(그리고 도메인 내 임의의 장소에 저장될 수 있다). 통상, 제약된, 예를 들면 재생 또는 복제 횟수에 대한 어떤 계수 메커니즘을 포함하는 권한은 추가의 조치 없이는 시스템에서 복제될 수 없다. 이 문제의 일부를 해결하는 한 방법은 다수의 "1회 사용 권한"을 생성하는 것이다. "1회 복제"의 경우, 하나의 "복제 권한"이 생성될 것이다. 이 권한은 콘텐트가 또 다른 도메인에 복제될 때 소모(삭제)될 것이다. 권한이 1회 동작을 나타낼 때, 이것은 복제에 대해 보호될 것이지만 도메인 내에선 자유롭게 이동할 수 있다.

[0175] 콘텐트와 함께 권한을 저장하는 것이 이점이 있을 수 있다. 이것은 권한을 찾는 것을 용이하게 할 것이다(콘텐트가 사용가능한 경우, 권한도 또한 사용가능하다). 또 다른 이점은 권한에 필요한 저장 공간이 콘텐트를 저장하는데 사용될 수 있는 저장에 따라 가변될 수 있다는 것이다. 주된 단점은 어떤 종류의 계수 메커니즘으로 권한을 지지하기가 어려워진다는 것이다.

[0176] 디지털 다기능 디스크들(DVD), 또는 콤팩트 디스크들과 같은 패키징된 매체들은 특별히 언급할 만하다. 패키징된 (ROM) 매체가 1회 복제와 같은 권한을 지지하기 위해 예를 들면 디스크에 계수 메커니즘을 포함하는 것이 가능하지 않다면, 보드 상에 연쇄 복제 관리(XAD 권한의 소스임)을 갖는 것으로 가정한다. 이러한 메커니즘의 예는 국제특허출원 WO02/17316(대리인 문서 PHNL010233)에 기술된 바와 같은 칩-인-디스크 유형의 메커니즘을 사용하여 실현될 수 있다.

[0177] 바람직한 실시예에서, 패키징된 매체는 XAD 권한만을 포함할 수도 있다. 매체가 AD 권한을 포함한다면 대응하는 XAD 권한이 도메인으로부터 제거된 경우 나중에 이들 권한을 삭제하기는 불가능할 수도 있을 것이다. 또한, 소비자들은 패키징된 매체들(예를 들면 DVD+RW)이 어느 곳이든 그리고 임의의 호환 디바이스에서 재생될 것으로 기대한다.

[0178] "더 이상 복제 불가"의 경우, 디스크는 도메인 발원자 디바이스, 즉 device_id = domain_id인 디바이스에서 또는 디스크 판독기에서만 재생(즉, 렌더링)될 것을 요구할 수도 있을 것이다(이에 따라 전체 도메인 내에서 재생될 수 없다). 이것은 원 매체 판매를 고무시킬 수도 있을 것이다. 다른 사용 규칙들이 일련의 복제 관리 비트들의 설정에 따라 가능하다.

[0179] 요약하면, 본 발명의 하나 이상의 다른 실시예들과 각각이 조합될 수 있거나 독자로 놓여질 수 있는 일부 이점이 있는 실시예들은 다음과 같다:

[0180] 1. 도메인 내 디바이스들을 식별하기 위해 디바이스들에서 domain_id들을 사용한다. 이 경우 모든 AD 호환 디바이스들은 domain_id 번호를 저장하기 위한 저장 공간을 구비할 필요가 있다.

[0181] 2. 도메인 크기를 제한하기 위해서, 디바이스는 도메인 발원자 디바이스에 그리고 이 디바이스에 근접하여 있을 때 체크-인 된다.

[0182] 3. 도메인의 크기는 도메인에서 재생 권한의 양을 제한시킴으로써 제한된다.

[0183] 4. AD에 두 유형들의 권한으로서, 도메인들간 이전을 위한 XAD 권한 및 도메인 내 사용을 위한 AD 권한.

[0184] 5. 디바이스를 체크-아웃할 때, 이의 domain_id는 예를 들면 이를 다시 device_id와 같게 함으로써 삭제되고, 디바이스에 있는 AD 권한도 삭제된다. 이것은 디바이스를 체크-아웃함으로써 도메인으로부터 콘텐트를 내보내는 공격을 방지한다.

[0185] 6. XAD 권한을 포함하는 디바이스를 체크-아웃할 때, 대응하는 AD 권한에 대한 취소 메시지가 도메인에 보내지거나, 또는 하트 비트(hart beat)(화이트 리스트) 메커니즘을 사용한다. 이 경우 휴대용 디바이스들(항시 네트워크에 접속되는 것인 아닌)은 일정 간격으로 재개된 AD 권한을 얻을 필요가 있다. 이 메커니즘은 디바이스를

체크-아웃함으로써 도메인에 콘텐트/권한을 남겨놓고 나가려는 공격을 저지한다. 디바이스를 체크-인하고, 이에 콘텐트를 저장하고, 이어서 디바이스를 체크-아웃하여 또 다른 허가된 도메인에 디바이스를 체크-인함으로써 콘텐트를 불법 분배하는 것을 방지한다.

[0186] 7. 원래 패키징된 매체들의 판매를 고무시키고, 매체가 "1회 복제 생성" 허용됨을 나타내는 경우, 패키징된 매체상에 XAD로부터 AD 권한의 도출만을 허용한다. 이것은 "더 이상 복제 불가" XAD 권한으로부터 AD 권한을 도출하는 것이 가능하지 않다는 것과, 매체 상의 콘텐트는 매체가 도메인 내 있을 경우 도메인에서만 재생될 수 있음을 의미한다.

[0187] 8. 한정된 수의 사용 권한은 "1회 권한" 또는 "권한 토큰들"을 생성함으로써 구현된다.

[0188] 전술한 실시예를 본 발명을 한정하는 것이 아니라 예시하는 것이며, 당업자는 첨부된 청구항들의 범위 내에서 많은 대안적 실시예들을 설계할 수 있을 것임에 유의해야 할 것이다. 홈 네트워크를 나타내는 시스템(100)은 물론 허가된 도메인이 유용한 유일한 상황이 아니다.

[0189] 청구항들에서, 괄호 내 참조 부호들은 청구항을 한정하는 것으로 해석되지 않은 것이다. "포함하다"라는 단어는 청구항에 나열된 것들 이외의 요소들 또는 단계들의 존재를 배제하는 것은 아니다. 요소의 단수 표현은 복수의 이러한 요소들의 존재를 배제하는 것이 아니다. 본 발명은 몇 개의 구별되는 요소들을 포함하는 하드웨어에 의해서, 아울러 적합하게 프로그램된 컴퓨터에 의해 구현될 수 있다.

[0190] 몇 개의 수단을 열거한 디바이스 청구항에서, 이들 수단 몇 개는 하나의 동일한 하드웨어로 실현될 수 있다. 특정 조치가 상호 상이한 종속 청구항들에서 인용되어 있다는 단순한 사실은 이들 조치들의 조합이 유리하도록 사용될 수 없다는 것을 나타내는 것은 아니다.

도면의 간단한 설명

[0046] 도 1은 네트워크를 통해 상호 접속된 디바이스들을 포함하는 시스템을 개략적으로 도시한 도면.

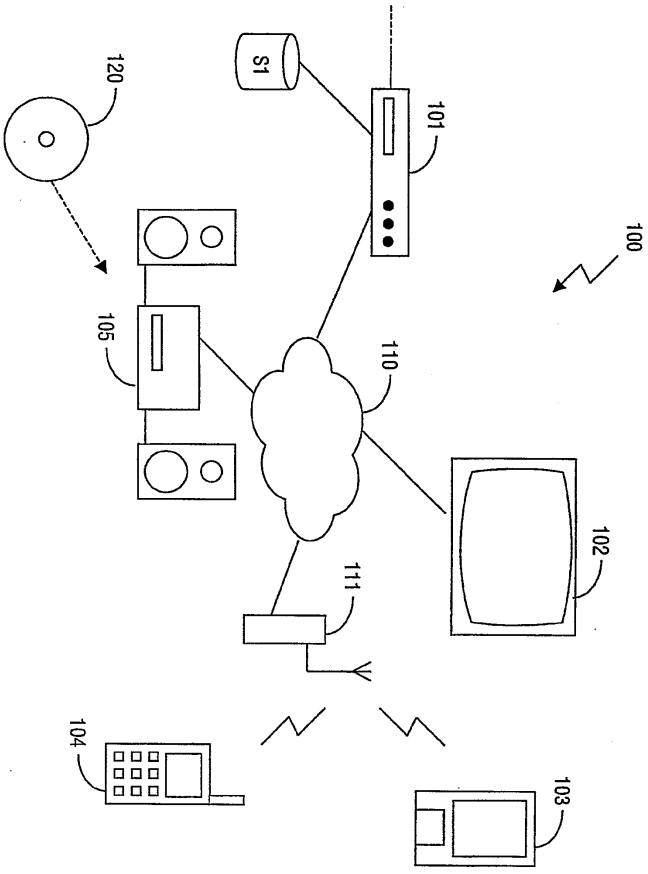
[0047] 도 2는 CA 도메인과 CP 도메인으로 도 1의 시스템(100)의 개략적 분할을 도시한 도면.

[0048] 도 3은 도 2의 CP 도메인에 디바이스 체크-인하는 프로세스의 실시예에 대한 흐름도.

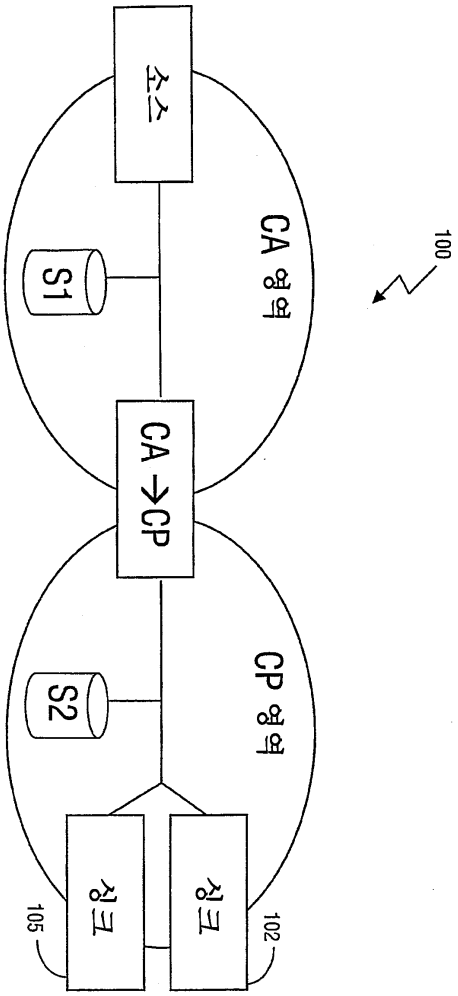
[0049] 도 4는 도 2의 CP 도메인에 디지털 권한들을 체크-인하는 프로세스의 실시예에 대한 흐름도.

도면

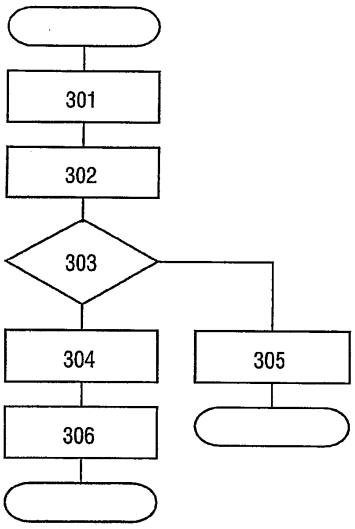
도면1



도면2



도면3



도면4