

(authenticity)

ID

가 ,

/

/

/

/

가

1

[0001] environment)

(integrity certification and verification)

(a content consumption e

[0002]

가

가 가

(Intellectual Property Rights Management: IPRM),

(Digital Property Rights Management: DPRM),

(Intellectual Property Management: IPM

), (Digital Rights Management: DRM),

(Rights Management: RM)

(Ele

ctronic Copyright Management: ECM)

[0003]

가

/

(behaviors)

(applications)

(public key infrastructure: PKI)

가

[0004]

PKI

(many-to-many relationship)

(scale)가

[0005]

(behaviors)

(embedding),

(distribution)

(usage)

[0006]

, 가

(interception routine)

" (alien)"

(Attorney Docket No.)가 111325 000002

가

[0007]

(system components)

가

[0008]

[0009]

[0010]

[0011]

[0012]

[0013]

[0014]

[0015]

[0016]

[0017]

[0018]

[0019]

[0020]

[0021]

, PDA , DVD
(distributed network enabled phones),

" (trust)"
(profile)
가

(CDs),

(authentication information)

(protected content)

(identifica

tion: ID)가,

[0019] tected version)

[0020]

[0021]

ID (embedded)

ID
 [0022] , . , . , .
 [0023] 가 , / / /
 [0024]
 [0025]
 [0026] 1 1 (functional overvi
 ew)
 [0027] 2 1
 [0028] 3
 [0029] 4
 [0030] 5 (environment stack)
 [0031] 6
 [0032] 7 (workflow)
 [0033] 8
 [0034] 9
 [0035] 10 (dynamic tampering)
 [0036] 11
 [0037] 12 /
 [0038] 13
 [0039] 14 (integrity authenticator)
 [0040]
 , /
 가
 가
 [0041] 1 (100
) (200), / (300), (400), /
 (500), (260) (270)
 [0042] (500) / (500) /
 (300) / (400) / (400)
 0) / (200) / 가 (50
 (20) (200) (300)
 (400) (400) (50)
 [0043] (400) (300) (400)
 (400) / 가
 / 가

[0044] / (400) (300) , , (300) ID(10) ID(10) 가 (400) 가

[0045] 가 (300) (20) (200) (400) (20) 가 (200) (270) 가 가 (260) / 가 (20) (500) (200) , / (200) (260) (200) (authenticity) 가 (200) (50) (50) (400) (protected content)(10) 가 (unprotected) (400) 00) (100) (300), (400), (500) [0046] 2 (100) (200), (300), / (400), (500) [0047] (300) (310), (320), (330), (340) (300) (CD) CD 가 (200) (210), (220), (230), (240), (250), (260), (270), (280), (290) (295) (200) [0048] (optionally) 가 (optionally) ID ID (optionally) 가 (200) [0049] (400) (410), (420), (430), (440), (450) (460) 가 (500) (510), (520), (530), (540), (550), (560) (300) 가 가 가 가 (500) (500) (500)가 (200) [0051] (500) (300) 가 (500) (300) 가

[0053] / (500) 가
 / (500) 가 . /
 / (500) (300) /

[0054] (100) (5)
 (100) (5)
 (400), (500) (300),
 (multiple instances) (200)

[0055] / (500) /

[0056] (300) (400)
 (400) (300) (400)
 (330) (310) (320)
 (340) (300)

[0057] (400) (300) 가 가
 ID 가 가

[0058] , 가 / / 가,

[0059] , 가 ID (400) (4)
 30) (410) (420) (440)

[0060] (300) (260)
 (20) (260) , (

230) (210) (220) (300)

[0061] (200) (260) (500) (

270) (260) / (500)

(270) 가 (300)

[0062] (300) (260) (

(200) , (210) (220) 가 (

270)

[0063] (200) (200) 가
 (integrity authenticator) 가
 (400) / (450) (dedicated device)
 2 ID
 (200) / (250)
 / ID (260)
 / (hash) (hash value)
 / / 가

[0064] / (500) (identification and certificatio
 n verification device)(200) (200)

(540) (510), (520) (500)
 (550) (560) (530) ID, , ,

(build number), / ,

[0065] , , / (500)
 (200) (500) (200)
 가 / (500)

[0066] (250) (optionally) (250) / ID
 (260)

[0067] / (500) (250) (540)
 (target) / (260)
 (250)

[0068] (280)
 (optional interaction relationship)가
 가

[0069] 3 ID (200) ID, (optionally) (250) (250)
 (meta information)가 (250)
 ID / ID
 (300) 가

[0070] ID (280) ID

[0071] ID (290) ID ()
 270) ID 가

[0072] (280)
 (295) ID ID

[0073] 4 (280)
 (200)
 (280) ID (2
 (260) (280) ID,
 (optionally), /

[0074] (280) (240)
 (240) (280)

[0075] (270) ID (usage license) (300)
 (optionally) ID (400)
 (sensitive information) /

[0076] (290)
 (270) (295)
 (295)

[0077] (400) (450) (450)

[0078] 5 (top) (400)

[0079] 6 (OS), (OS boot strap),

[0080] (450) / ID (400)
(embedded) (450) 가

[0081] (450) (450)
7-9 (last-in-first-out) " (push)" " (pop)"
(top)

[0082] 가
가 (stacked)

[0083] 10 (Integrity Authenticator: IA)
IA, IA, IA 가
IA IA
가 IA
IA /
(closed system)

[0084] 11 S110 S110 S100 S120 S140
S130

[0085] S140 S150 S160 S170
가 가

[0086] 12 S200 S180 S210 가
S220 가 / / /
S230 / / 가
가 S240

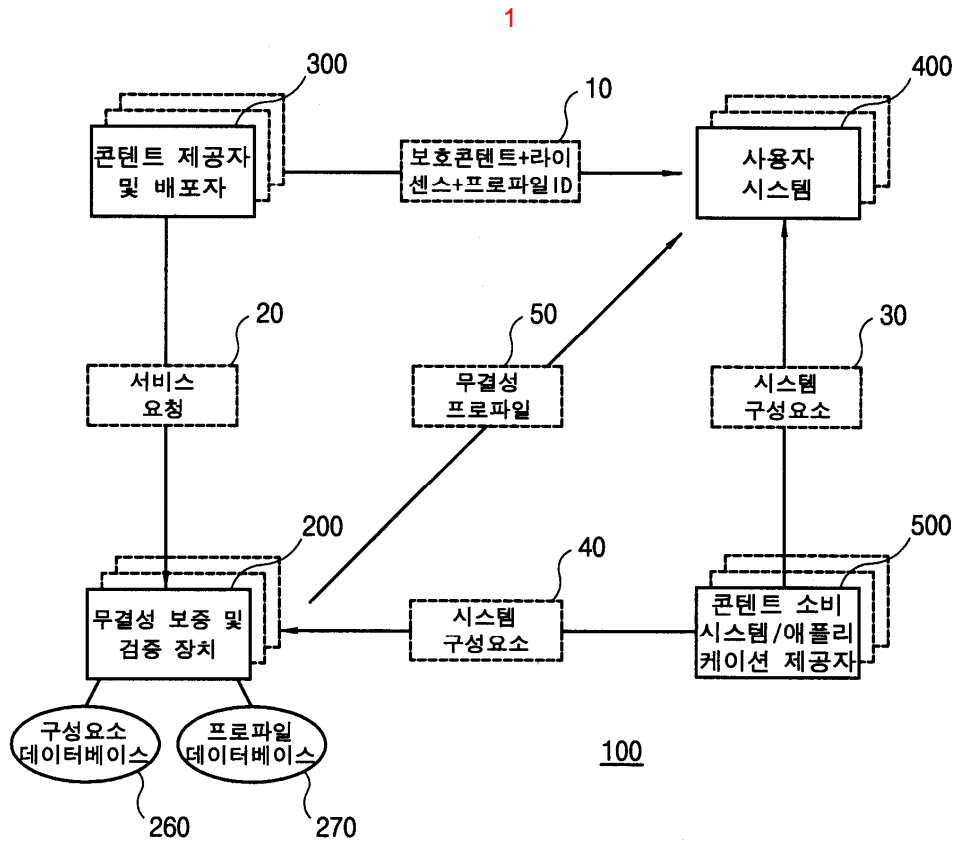
[0087] S240 S250 S260

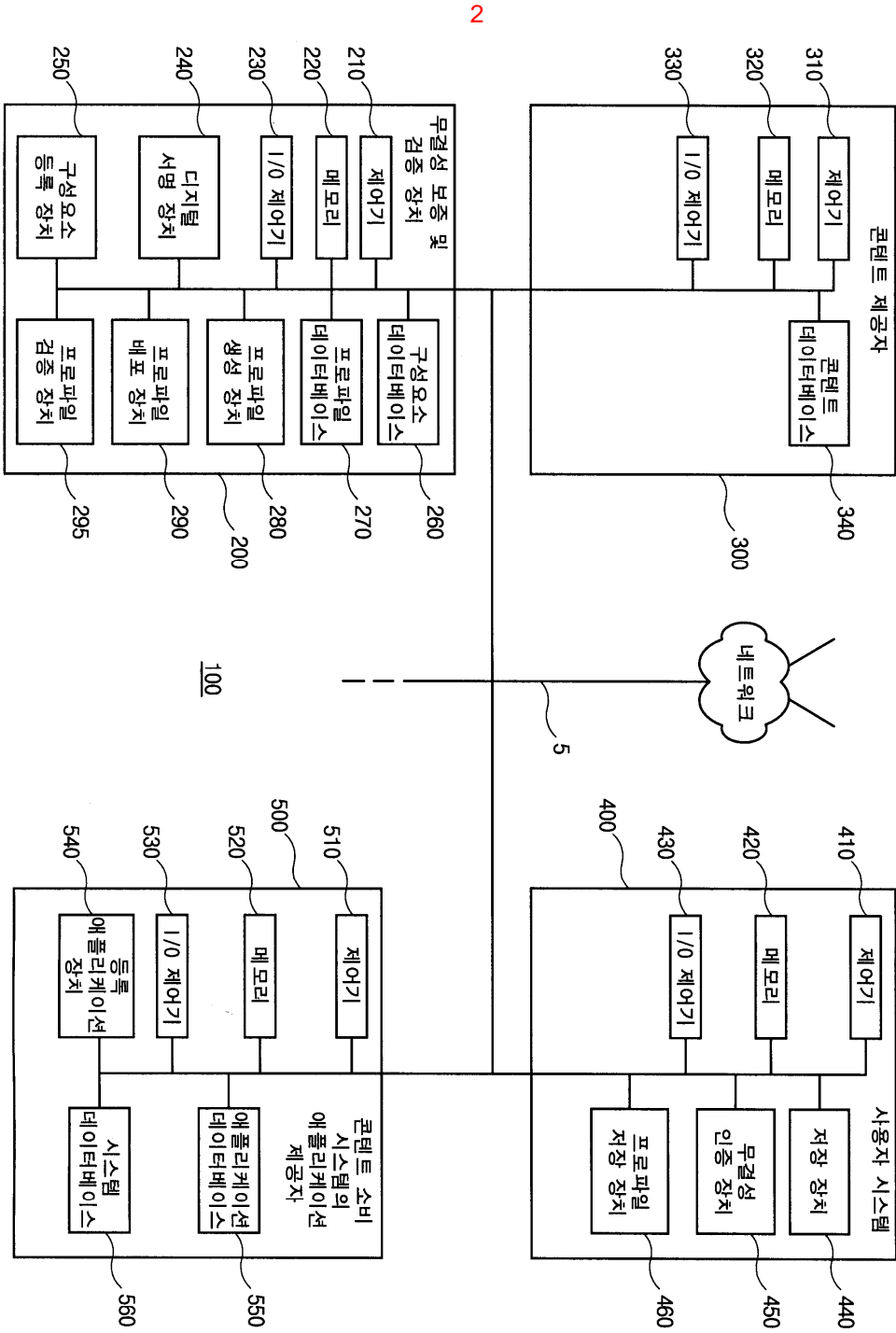
[0088] S270 가
S280
S290 가

[0089] 13 S300 S310 S320 S300
S310 ID S330 S320 /

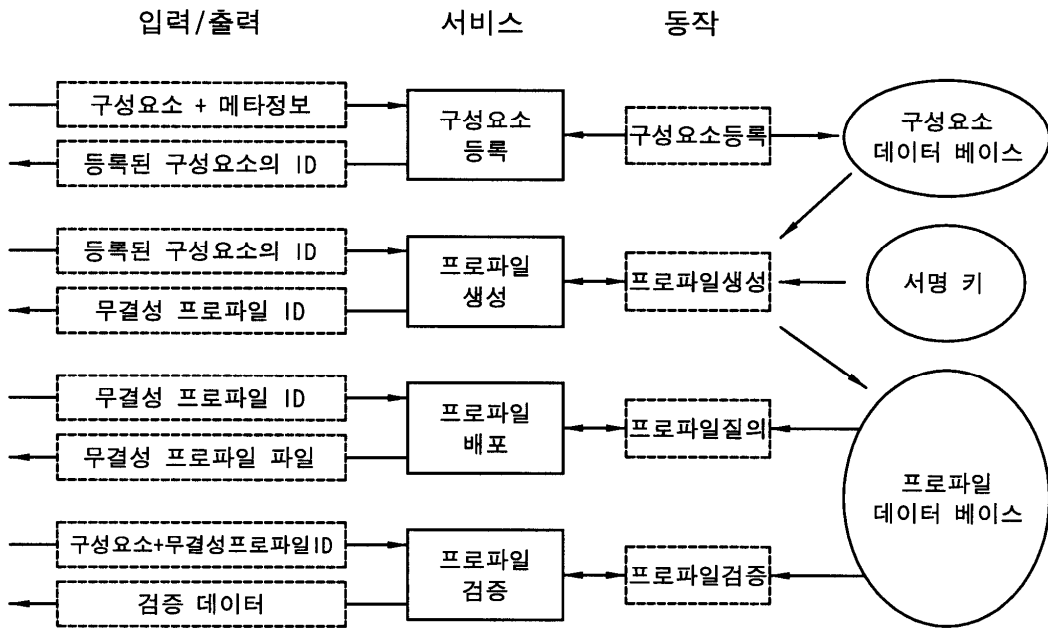
1. (authentication information)
가 (authenticity) (a
uthenticated environment)
2. (identification)
3. (maintain)
4. (specified),
(identification)
(authenticity)
- 5.
6. (identification)
- 7.
- 8.
9. 가
(not authentic) (access) 가
- 10.
11. (authenticated environment) 가 (verifiable information) ;
(access rights)
12. (authentication information)
- 13.
14. 가 (at least one of ena
bling or disabling access to the content)
- 15.

- 15 16. , .
- 15 17. , .
- 18. , .
- 11 19. , , (a tamper resistant environment)
- 11 20. , .
- 20 21. , ,
- 11 22. , , 가 (establishing)
- 23. 가 가 , , (authenticated environment) 가 ; , (access rights) 가 (computer readable medium).
- 23 24. , 가 .
- 25. , .
- 23 26. , 가 가 가
- 23 27. , , 가
- 가 28. , 가
- 27 29. , 가 .
- 30. , .
- 23 31. , 가 .
- 23 32. , 가 .
- 32 33. , 가 .
- 23 34. , , (establishes) 가 .





3



4

무결성 프로파일의 구조

무결성 프로파일 식별자
무결성 프로파일의 버전 번호
생성일
생성자
콘텐츠 제공자 이름과 ID
구성요소들의 무결성값(예:해시값) 리스트
구성요소들간의 (임의적인) 상호작용관계
무결성 프로파일의 디지털 서명

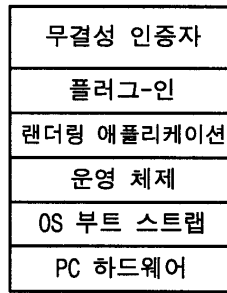
5

일반적인 최종 사용자 시스템 환경 스택

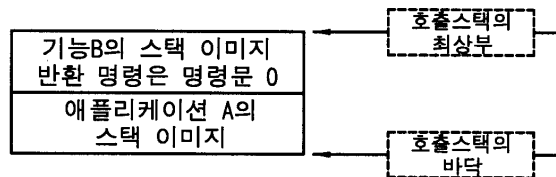
무결성 인증자
시스템 구성요소1
시스템 구성요소2
시스템 구성요소N

6

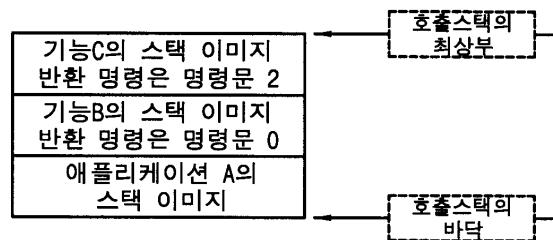
최종 사용자 시스템 환경 스택의 예



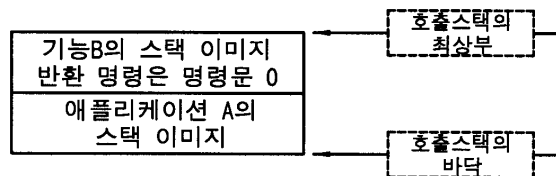
7



8

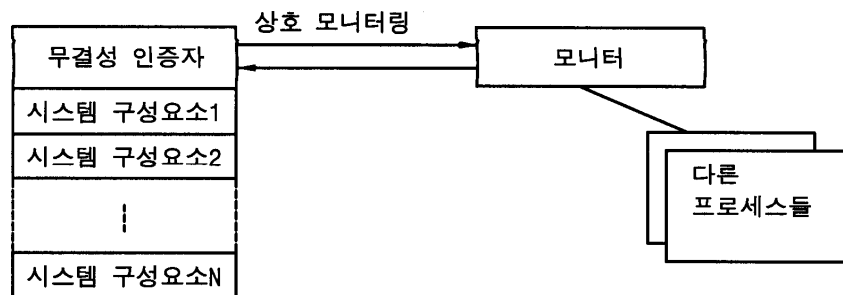


9

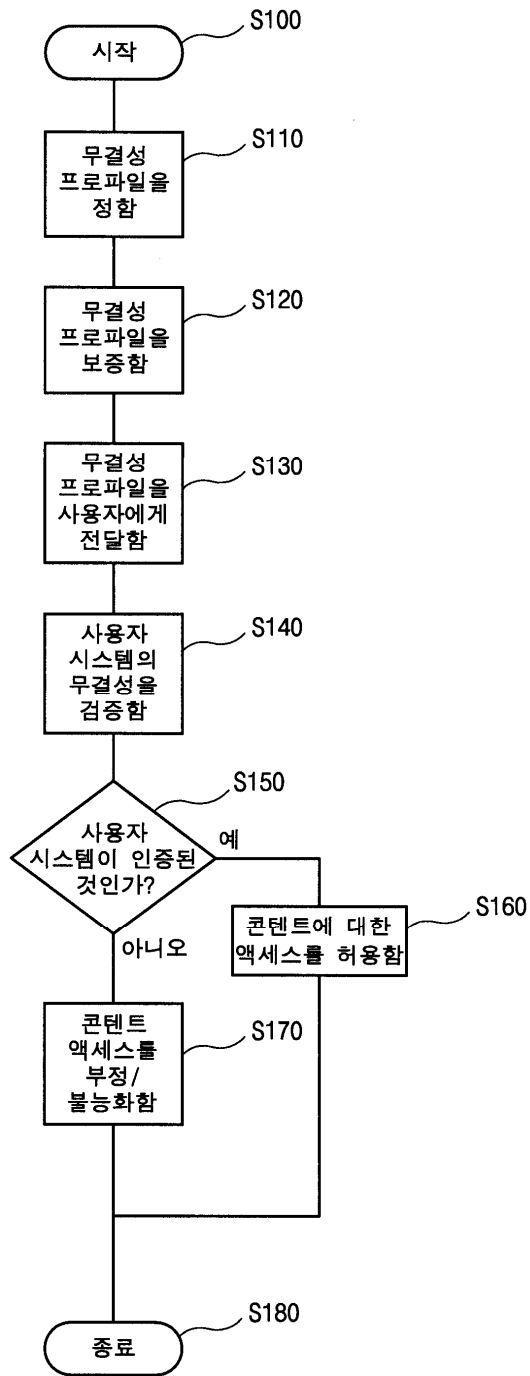


10

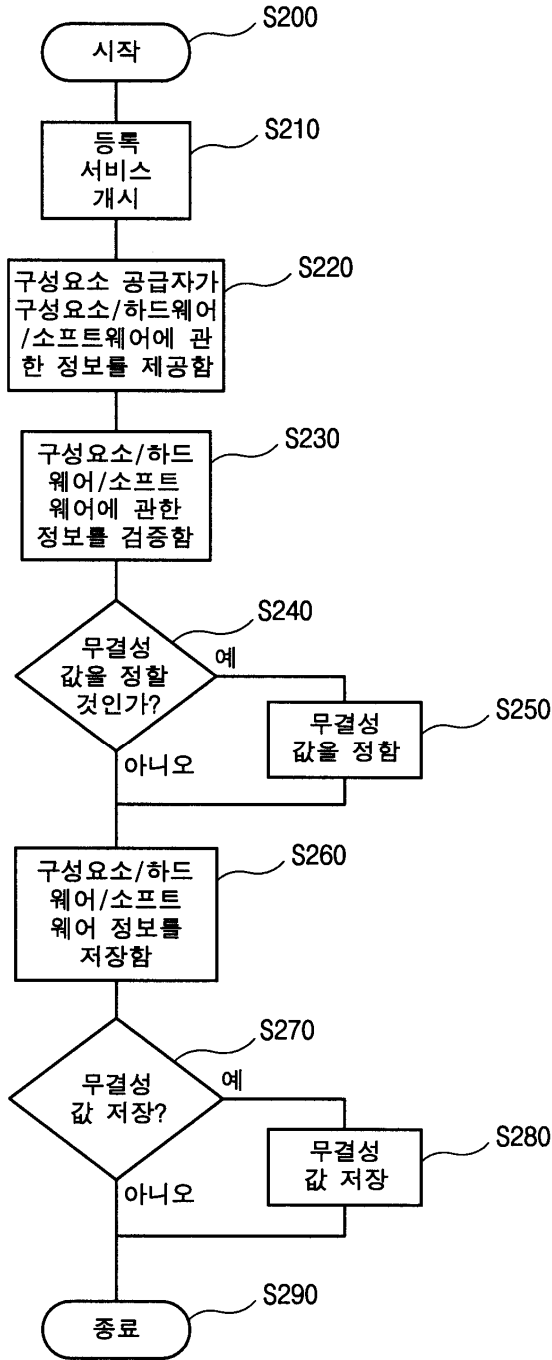
디버깅과 같은, 모니터링을 사용하는 동적인 간섭을 방지하는 것에 의한 실행환경의 보호



11



12



13

