(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2013 년 7 월 4 일 (04.07.2013)

WIPO | PCT

(10) 국제공개번호
WO 2013/100419 A1

(51) 국제특허분류:
G06F 21/00 (2006.01) *G06F 21/22* (2006.01)
G06F 21/20 (2006.01)

(21) 국제출원번호: PCT/KR2012/010323

(22) 국제출원일: 2012 년 11 월 30 일 (30.11.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
61/581,858 2011 년 12 월 30 일 (30.12.2011) US

(71) 출원인: **에스케이씨앤씨 주식회사 (SK C&C CO., LTD.)** [KR/KR]; 463-844 경기도 성남시 분당구 정자동 25-1 번지 SK u- Tower, Gyeonggi-do (KR).

(72) 발명자: **권용성 (KWON, Yong Sung)**; 30004 조지아주 알파레타 3307 디어 런 서클, Georgia (US). **주케빈 (ZHU, Kevin)**; 30068 조지아주 매리에타 3021 캔턴 파인즈 플레이스, Georgia (US).

(74) 대리인: **한지나 (HAN, Gee Na)** 등; 135-854 서울시 강남구 도곡동 517-18 경빈빌딩 6 층, Seoul (KR).

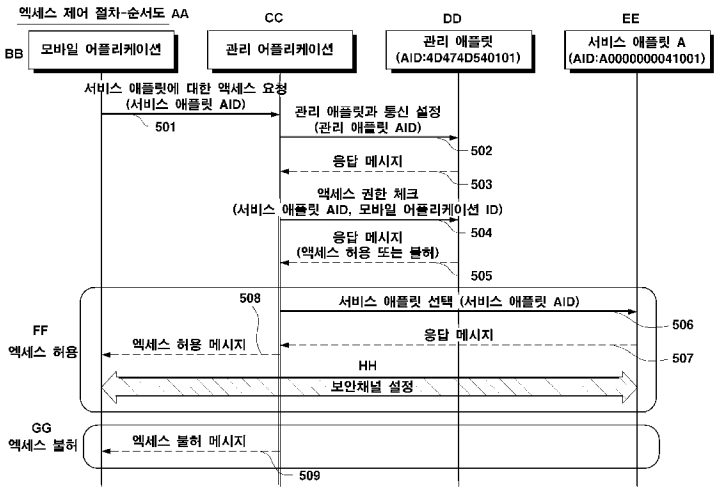
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[다음 쪽 계속]

(54) **Title**: SYSTEM AND METHOD FOR CONTROLLING APPLET ACCESS

(54) **발명의 명칭** : 애플릿 액세스 제어 시스템 및 방법



AA ... Access control process-flowchart
BB ... Mobile application
CC ... Managing application
DD ... Managing applet
EE ... Service applet A
501 ... Access request for service application (service applet AID)
502 ... Set communication with the managing applet (managing applet AID)
503 ... Response message
504 ... Check access authorization (service applet AID, mobile application ID)
505 ... Response message (access granted or denied)
506 ... Select a service applet (service applet (AID)
507 ... Response message
FF ... Access granted
GG ... Access denied
508 ... Access granted message
HH ... Set a secure channel
509 ... Access denied message

(57) **Abstract**: Provided are a system and method for controlling applet access. The method for controlling applet access according to one embodiment of the present invention uses a managing program to control access by an application to an applet for which access has been requested when the application makes a request to the program for access to the applet stored in an SE. Thus, an application that does not have authorization is prevented from accessing an applet, and a high level of security can be maintained for the information contained in the applet.

(57) **요약서**: 애플릿 액세스 제어 시스템 및 방법이 제공된다. 본 발명의 실시예에 따른 애플릿 액세스 제어 방법은, 어플리케이션이 SE 에 저장된 애플릿에 대한 액세스를 관리 프로그램에 요청하면, 관리 프로그램이 액세스 요청된 애플릿에 대한 어플리케이션의 액세스를 제어한다. 이에 의해, 권한 없는 어플리케이션이 애플릿에 액세스하는 것을 제한할 수 있게 되어, 애플릿에 수록된 정보들에 대한 높은 보안성을 유지할 수 있다.

WO 2013/100419 A1

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

명세서

발명의 명칭: 애플릿 액세스 제어 시스템 및 방법

기술분야

[1] 본 발명은 SE(Secure Element)에서 애플릿에 대한 액세스를 제어하기 위한 시스템 및 방법에 관한 것이다.

배경기술

[2] 일반적으로, 모바일 단말은 내부 메모리와 SE를 포함하고 있다. 이때, SE는 하나 이상이 될 수 있다. 내부 메모리는 어플리케이션 뿐만 아니라 모바일 단말과 관련된 데이터를 저장하기 위해 사용된다. 하지만, 보안이 요구되는 정보는 안전한 저장을 위해 SE에 저장한다. SE에 저장된 정보는 보안상의 요구로 인해 액세스가 제한적이다. SE에 저장된 정보는 신용카드, 개인 정보, 금융 정보 등과 관련된 정보를 포함할 수 있다.

[3] SE에 저장되는 정보들의 보안이 요구되는 민감한 정보들이므로, SE의 절도 또는 분실은 정보 유출이나 금융 사고 등을 발생시킬 수 있다. 또한, 멀웨어(malware)가 모바일 단말 소유자의 인증 또는 승인 없이 SE에 저장된 정보에 액세스하여 악용할 우려가 있다.

발명의 상세한 설명

기술적 과제

[4] 본 발명의 실시예들은 SE에 저장된 정보에 대한 액세스를 제어/제한하기 위한 시스템 및 방법을 제공함에 있다

과제 해결 수단

[5] 본 발명의 일 실시예에 따른 모바일 단말은, SE에 저장된 애플릿에 대한 액세스를 요청하는 어플리케이션, 애플릿에 대한 액세스를 관리하는 관리 애플릿과 통신하는 관리 어플리케이션 및 보안정보(보안이 요구되는 정보)가 수록된 애플릿을 포함한다.

[6] 본 발명의 일 실시예에 따른 SE 액세스 보호 방법은, 어플리케이션이 SE에 저장되어 있는 애플릿에 대한 액세스를 요청하는 단계, 관리 어플리케이션이 관리 애플릿과의 통신을 설정하는 단계, 액세스 요청된 애플릿에 대한 액세스 권한을 어플리케이션이 가지고 있는지 관리 애플릿이 판단하는 단계 및 요청한 애플릿에 대한 액세스 권한을 어플리케이션이 가지고 있는 것으로 판단되면, 액세스 요청에 대한 응답으로 애플릿에 대한 액세스를 허용하는 단계를 포함한다.

[7] 본 발명의 일 실시예에 따른 SE 보안 연결 설정방법은, SE에 저장된 애플릿에 대한 액세스를 요청하는 단계, SE에 저장되어 있는 관리 애플릿과 통신하는 단계, 애플릿에 대한 액세스 가능 여부를 판단하는 단계 및 애플릿과 연결을 설정하는 단계를 포함한다.

[8] 본 발명의 일 실시예에 따른 애플릿 액세스 제어 방법은, 어플리케이션이, SE에 저장된 애플릿에 대한 액세스를 관리 프로그램에 요청하는 단계; 및 상기 관리 프로그램이, 액세스 요청된 애플릿에 대한 상기 어플리케이션의 액세스를 제어하는 단계;를 포함한다.

[9] 그리고, 상기 어플리케이션은, 메모리에 설치되어 있고, 상기 관리 프로그램은, 상기 메모리에 설치된 관리 어플리케이션과 상기 SE에 설치된 관리 애플릿을 포함하고, 상기 제어단계는, 상기 관리 어플리케이션과 상기 관리 애플릿 간의 인터랙션에 의해 수행될 수 있다.

[10] 또한, 상기 요청단계는, 상기 어플리케이션이, 상기 애플릿에 대한 액세스를 상기 관리 어플리케이션에 요청하고, 상기 제어단계는, 상기 관리 어플리케이션이, 상기 관리 애플릿과 통신을 설정하는 단계; 상기 관리 어플리케이션이, 상기 어플리케이션의 액세스 요청을 상기 관리 애플릿에 전달하는 단계; 및 상기 관리 애플릿이, 액세스 요청된 애플릿에 대한 액세스 권한이 상기 어플리케이션에 있는지 판단하는 단계;를 더 포함할 수 있다.

[11] 그리고, 상기 제어단계는, 상기 판단단계에서 상기 액세스 권한이 상기 어플리케이션에 있다고 판단되면, 상기 관리 어플리케이션이 액세스 요청된 애플릿에 상기 액세스 요청을 전달하는 단계; 상기 관리 어플리케이션이, 상기 어플리케이션에 액세스 허용 응답을 전송하는 단계; 및 상기 어플리케이션이 상기 액세스 요청된 애플릿과 통신을 설정하는 단계;를 더 포함 할 수 있다.

[12] 또한, 상기 어플리케이션은, 상기 관리 어플리케이션을 통해 액세스 요청된 애플릿과 통신 할 수 있다.

[13] 그리고, 상기 제어단계는, 상기 판단단계에서의 상기 액세스 권한이 상기 어플리케이션에 없다고 판단되면, 상기 관리 어플리케이션이 상기 액세스 요청을 폐기하는 단계; 및 상기 관리 어플리케이션이, 상기 어플리케이션에 액세스 불허 응답을 전송하는 단계;를 더 포함 할 수 있다.

[14] 또한, 상기 어플리케이션은, 상기 관리 애플릿에 액세스할 수 없을 수 있다.

[15] 그리고, 상기 어플리케이션은 지갑 어플리케이션이고, 상기 애플릿은 금융 서비스 애플릿일 수 있다.

[16] 한편, 본 발명의 일 실시예에 따른 모바일 단말은, SE에 저장된 애플릿에 대한 액세스를 관리 프로그램에 요청하는 어플리케이션이 설치된 저장부; 및 상기 어플리케이션 및 액세스 요청된 애플릿에 대한 상기 어플리케이션의 액세스를 제어하는 상기 관리 프로그램을 실행하는 프로세서;를 포함한다.

발명의 효과

[17] 이상 설명한 바와 같이, 본 발명의 실시예들에 따르면, 애플릿에 대한 액세스를 요청한 어플리케이션이 애플릿에 액세스하는 것을 액세스 권한을 기초로 제어할 수 있게 된다. 이에 따라, 권한 없는 어플리케이션이 애플릿에 액세스하는 것을 제한할 수 있게 되어, 애플릿에 수록된 정보들에 대한 높은

보안성을 유지할 수 있다.

[18] 또한, 본 발명의 실시예들에 따르면, 액세스 권한은 SE에 저장하고 관리하여 보안을 더욱 강화할 수 있고, 메모리에 설치된 관리 어플리케이션과 SE에 설치된 관리 애플릿의 인터랙션에 의해 액세스 제어가 수행되므로, 액세스 제어를 악의적으로 조작하는 것이 어렵다.

도면의 간단한 설명

[19] 도 1은 본 발명의 일 실시예에 따른 모바일 단말의 소프트웨어 구성을 도시한 블록도,

[20] 도 2는 본 발명의 일 실시예에 따른 SE 애플릿 액세스 제어 방법에서 액세스 성공 과정을 도시한 흐름도,

[21] 도 3은 본 발명의 일 실시예에 따른 SE 애플릿 액세스 제어 방법에서 액세스 실패 과정을 도시한 흐름도,

[22] 도 4는 본 발명의 일 실시예에 따른 SE 애플릿 액세스 제어 절차를 도시한 흐름도,

[23] 도 5는 본 발명의 일 실시예에 따른 SE 애플릿 액세스 제어 절차를 도시한 순서도, 그리고,

[24] 도 6은 본 발명의 일 실시예에 따른 모바일 단말의 하드웨어 구성을 도시한 블록도이다.

발명의 실시를 위한 최선의 형태

[25] 아래에서 본 발명의 실시예들이 도시된 첨부도면을 참조하여 본 발명에 대하여 더욱 상세하게 설명한다. 그러나, 본 발명은 많은 다른 형태로 실시될 수 있으며, 여기 설명된 실시예들에 한정되는 것으로 해석되어서는 안 된다.

[26] 도 1은 본 발명의 일 실시예에 따른 모바일 단말을 도시한 블록도이다.

[27] 도 1에 도시된 바와 같이, 모바일 단말(100)은 지갑 어플리케이션 A(110), 지갑 어플리케이션 B(120), 지갑 어플리케이션 C(130) (이들을 통칭하는 경우, 지갑 어플리케이션(Wallet Application)으로 지칭함), 관리 어플리케이션(140), SE(Secure Element) 인터페이스(150) 및 SE(160)를 포함한다. 한편, SE(160)는 관리 애플릿(161), 애플릿 A(162), 애플릿 B(163) 및 애플릿 C(164)를 포함한다.

[28] 지갑 어플리케이션은 SE(160) 내에 저장된 애플릿에 대한 액세스를 요청할 수 있다. 지갑 어플리케이션은 ID(entifier) 또는 SP ID(Service Provider IDentification)를 갖는다. 도 1에 도시된 바에 따르면, 지갑 어플리케이션 A(110)의 SP ID는 00000001이고, 지갑 어플리케이션 B(120)의 SP ID는 00000002이며, 지갑 어플리케이션 C(130)의 SP ID는 00000003이다.

[29] 또한, SE(160) 내에 저장된 애플릿도 AID(Applet ID)를 갖는다. 도 1에 도시된 바에 따르면, 애플릿 A(162)의 AID는 00000001이고, 애플릿 B (163) 의 AID는 00000002이며, 애플릿 C(164) 의 AID는 00000003이다.

[30] 모바일 단말 내에 상주하는 어플리케이션(지갑 어플리케이션 A(110), 지갑

어플리케이션 B(120), 지갑 어플리케이션 C(130))은 SE(160)에 저장된 적어도 하나 이상의 애플릿에 대한 액세스 권한을 가질 수 있다.

[31] 구체적으로, 도 1에 도시된 바와 같이, SP ID가 00000001인 지갑 어플리케이션 A(110)는 AID가 00000001인 애플릿 A(162)에 대한 액세스 권한을 갖고, SP ID가 00000002인 지갑 어플리케이션 B(120)는 AID가 00000002인 애플릿 B(163)에 대한 액세스 권한을 갖는다. 한편, SP ID가 00000003인 지갑 어플리케이션 C(130)는 AID가 00000001인 애플릿 A(162), AID가 00000002인 애플릿 B(163) 및 AID가 00000003인 애플릿 C(164)에 대한 액세스 권한을 갖는다.

[32] 어플리케이션은, SE(160)에 저장되어 있는 애플릿들 중, 액세스 권한을 갖는 애플릿에는 액세스할 수 있지만, 액세스 권한을 갖지 않는 애플릿에는 액세스할 수 없다. 예를 들어, 지갑 어플리케이션 A(110)는 애플릿 A(162)에는 액세스할 수 있지만, 애플릿 B(163)에는 액세스할 수 없다.애플릿은 금융 정보, PIN(Personal Identification Number), 암호 코드(Security Code) 등을 수록하고 있을 수 있으며, 이 밖의 다른 정보들을 수록하고 있을 수도 있다.

[33] 사용자가 지갑 어플리케이션 A(110)를 실행한 경우, 지갑 어플리케이션 A(110)는 사용자에게 자신에 연관된 애플릿에 수록된 금융 정보의 일종인 어카운트(Account) 정보를 표시하기 위해, SE(160)에 저장된 애플릿 A(162)에 대한 액세스를 요청할 수 있다. 여기서, 어카운트 정보에는 현재 잔고, 결제예정 내역, 과거 거래내역 등을 포함할 수 있지만, 이에 한정하지 않는다.

[34] 관리 어플리케이션(140)은 SE(160)의 정보 액세스, 모바일 단말에 저장된 어플리케이션의 액세스 관리를 위해, 관리 애플릿(161)과 인터랙션한다. 즉, 도 1에서, 관리 어플리케이션(140)은 SE(160)에 저장된 애플릿에 액세스하고, 지갑 어플리케이션 A(110), 지갑 어플리케이션 B(120) 및 지갑 어플리케이션 C(130) 중 적어도 하나를 관리하게 된다.

[35] 구체적으로, 사용자가 SE(160)에 저장된 애플릿 A(162)에 액세스하기 위해 지갑 어플리케이션 A(110)을 실행한 경우, 관리 어플리케이션(140)은 요청한 지갑 어플리케이션 A가 애플릿 A(162)에 대한 액세스 권한을 가지고 있는지를 판단한다.

[36] 이를 위해, 관리 어플리케이션(140)은 애플릿 액세스를 요청한 어플리케이션의 SP ID를 식별하고, SE 인터페이스(150)를 통해 SE(160)에 상주하는 관리 애플릿(161)과 통신을 설정한다.

[37] 이에 대응하여, 관리 애플릿(161)은 액세스 요청된 애플릿에 대한 AID를 식별하며, 액세스 요청된 애플릿의 AID와 액세스 요청한 어플리케이션의 SP ID가 연관(관련)되어 있는지 확인한다. 두 식별자가 서로 연관되어 있는 경우, 관리 애플릿(161)은 '액세스 요청한 어플리케이션'이 '액세스 요청된 애플릿'에 대하여 액세스 권한을 갖는 것으로 판단한다.

[38] 도 2는 본 발명의 일 실시예에 따른 SE 애플릿 액세스 제어 방법에서 액세스 성공 과정을 도시한 흐름도이다.

[39] 단계 201에서, 사용자가 모바일 단말에서 SE에 저장된 애플릿 A에 대한 액세스를 요청하는 지갑 어플리케이션 A을 실행한 것을 상정한다. 이에 따라, 지갑 어플리케이션 A는 관리 어플리케이션을 통해 AID가 00000001인 애플릿에 대한 액세스를 요청하게 된다.

[40] 단계 202에서, 관리 어플리케이션은 SE에 저장된 관리 애플릿과의 통신을 설정한다. 관리 어플리케이션은 모바일 단말에 저장된 어플리케이션(지갑 어플리케이션 A를 포함)의 SP ID를 저장/관리한다고 전술한 바 있다. 도 2에서 지갑 어플리케이션 A의 식별자는 00000001로 도시되어 있다. 또한, 관리 애플릿은 어플리케이션의 액세스 권한과 SE에 저장된 애플릿의 AID를 저장/관리한다고 전술한 바 있다.

[41] 단계 203에서, 어플리케이션의 SP ID와 관련 애플릿의 AID가 연관되어 있는지 판단된다. 판단결과, 액세스 요청한 어플리케이션인 지갑 어플리케이션 A가 액세스 요청된 애플릿인 애플릿 A에 대한 액세스 권한을 가지는 것으로 판단되면, 액세스 요청한 어플리케이션은 액세스 요청된 애플릿에 수록되어 있는 정보에 액세스할 수 있다.

[42] 단계 203을 위해, 먼저 관리 어플리케이션은 액세스 요청한 어플리케이션의 SP ID와 액세스 요청된 애플릿의 AID가 포함된 액세스 요청을 관리 애플릿에 전달한다. 이에, 관리 애플릿은 전달 받은 어플리케이션의 SP ID와 애플릿의 AID를 교차 참조하여 SP ID와 AID가 서로 연관된 것으로 판단된 경우, 액세스 요청한 어플리케이션이 액세스 요청된 애플릿에 수록되어 있는 정보에 액세스할 수 있다고 판단하게 된다.

[43] 도 2에 도시된 바에 따르면, 지갑 어플리케이션 A의 SP ID인 00000001는 애플릿 A의 00000001의 AID와 연관되어 있다. 따라서, 관리 어플리케이션은 지갑 어플리케이션 A가 애플릿 A에 대한 액세스 권한을 가지고 있다고 판단하여 액세스를 허용한다.

[44] 애플릿 A에 대한 액세스가 허용되면, 단계 204에서, 관리 어플리케이션은 액세스 요청을 애플릿 A에 전달하여 애플릿 A를 선택한다. 그리고, 단계 205에서 관리 어플리케이션은 "액세스 허용" 응답을 지갑 어플리케이션 A에 전송한다.

[45] 액세스 요청한 어플리케이션의 SP ID와 액세스 요청된 애플릿의 AID가 매치되지 않으면, 액세스는 거부될 수 있다.

[46] 따라서, 서비스 제공자는 자신이 액세스할 권한이 있는 서비스 애플릿에만 액세스할 수 있으며, 다른 서비스 제공자의 승인되지 않은 정보에 액세스하는 것은 허용되지 않는다. 따라서, 서비스 제공자 자신의 애플릿 정보가 다른 서비스 제공자에게 노출될 가능성이 줄어들기 때문에 보안이 강화될 수 있다.

[47] 도 3은 본 발명의 일 실시예에 따른 SE 애플릿 액세스 제어 방법에서 액세스 실패 과정을 도시한 흐름도이다.

[48] 단계 301에서, 사용자는 모바일 단말에서 SE에 저장된 애플릿 B에 대한 액세스를 요청하는 지갑 어플리케이션 A을 실행한 것을 상정한다. 이에 따라,

지갑 어플리케이션 A는 관리 어플리케이션을 통해 AID가 00000002인 애플릿에 대한 액세스를 요청하게 된다.

[49] 단계 302에서, 관리 어플리케이션은 SE에 저장된 관리 애플릿과의 통신을 설정한다. 관리 어플리케이션은 모바일 단말에 저장된 어플리케이션(지갑 어플리케이션 A를 포함)의 SP ID를 저장/관리한다고 전술한 바 있다. 도 3에서, 지갑 어플리케이션 A의 식별자는 00000001이다. 또한, 관리 애플릿은 SE에 저장된 애플릿(애플릿 B를 포함)의 AID를 저장/관리한다고 전술한 바 있다. 도 2에서, 애플릿 B의 식별자는 00000002이다.

[50] 단계 303에서, 지갑 어플리케이션의 SP ID와 관련 애플릿의 AID가 비교된다. 액세스 요청한 어플리케이션인 지갑 어플리케이션 A이 액세스 요청된 애플릿인 애플릿 B에 대한 액세스 권한을 가지는 것으로 관리 어플리케이션이 판단하면, 액세스 요청한 어플리케이션은 액세스 요청된 애플릿에 수록된 정보를 액세스할 수 있다.

[51] 단계 303를 위해, 먼저 관리 어플리케이션이 액세스 요청한 어플리케이션의 SP ID와 액세스 요청된 애플릿의 AID가 포함된 액세스 요청을 관리 애플릿에 전달하면, 관리 애플릿이 전달 받은 SP ID와 액세스 요청된 애플릿의 AID 정보를 교차 참조하여 SP ID와 ADI가 서로 관련된 것으로 판단된 경우, 액세스 요청한 어플리케이션이 액세스 요청된 애플릿에 수록된 정보에 액세스할 수 있다고 판단하게 된다.

[52] 한편, SP ID와 AID가 서로 연관되지 않는 경우, 액세스 요청한 어플리케이션은 액세스 요청된 애플릿에 수록된 정보에 액세스할 수 없는 것으로 판단하게 된다.

[53] 도 3에 도시된 바와 같이, 지갑 어플리케이션 A의 SP ID인 00000001는, 애플릿 A의 AID인 00000001와 연관되어 있지만, 애플릿 B의 AID인 00000002와는 연관되어 있지 않았다. 따라서, 관리 어플리케이션은 지갑 어플리케이션 A가 애플릿 B에 대한 액세스 권한을 갖지 않은 것으로 판단하고 액세스를 거부한다. 이에, 단계 304에서, 관리 어플리케이션은 “액세스 불허” 응답을 지갑 어플리케이션 A에 전송한다.

[54] 도 4는 본 발명의 일 실시예에 따른 액세스 제어 절차를 도시한 흐름도이다.

[55] 단계 401에서, 모바일 단말에 저장된 지갑 어플리케이션은 모바일 단말의 SE에 저장된 애플릿에 액세스하려고 시도한다. 애플릿은 지갑 어플리케이션과 관련되며 보안이 요구되는 어카운트 정보를 포함할 수 있다.

[56] 또한, 어플리케이션과 애플릿은 각각 SP ID와 AID와 같은 식별자에 의해 식별될 수 있다. 애플릿이 어플리케이션과 연관된 경우, 이들은 연관된 식별자를 가질 수 있다. 예를 들어, 도 1, 도 2, 및 도 3에 도시된 바와 같이 지갑 어플리케이션 A의 SP ID는 00000001이고, 이에 연관된 애플릿 A의 AID는 00000001이다.

[57] 어플리케이션의 SP ID는 관리 어플리케이션에 의해 관리되고, 애플릿의 AID와 그들의 어플리케이션에 대한 연관성은 관리 애플릿에 의해 관리된다.

[58] 단계 402에서, 관리 어플리케이션은 지갑 어플리케이션으로부터 액세스 요청을 수신한다. 단계 403에서, 관리 어플리케이션은 SE에 저장된 관리 애플릿과 통신 연결을 설정한다.

[59] 단계 404 및 405에서, 관리 어플리케이션은 액세스 요청한 어플리케이션이 액세스 요청된 애플릿에 대한 액세스 권한을 갖는지를 판단하기 위해 관리 애플릿에 의해 관리되는 액세스 제어 리스트를 체크한다. 액세스 요청한 어플리케이션의 SP ID가 액세스 요청된 애플릿의 AID와 연관된 경우, 관리 어플리케이션은 액세스 요청한 어플리케이션이 액세스 권한을 갖는 것으로 판단한다.

[60] 액세스 요청한 어플리케이션이 액세스 권한을 갖지 않는 것으로 판단되면, 단계 406에서 관리 어플리케이션은 액세스 불허 응답을 액세스 요청한 어플리케이션에게 회신한다.

[61] 반면, 액세스 요청한 어플리케이션이 액세스 권한을 갖는 것으로 판단되면, 단계 407에서 관리 어플리케이션은 액세스 요청된 애플릿에 액세스 요청을 전달한다.

[62] 단계 408에서, 관리 어플리케이션은 액세스 허용 응답을 액세스 요청한 어플리케이션에 회신한다.

[63] 단계 409에서, 액세스 요청한 어플리케이션과 액세스 요청된 애플릿 간에 보안채널이 설정된다. 따라서, 어플리케이션은 애플릿에 수록된 정보를 액세스할 수 있게 된다.

[64] 도 5는 본 발명의 일 실시예에 따른 액세스 제어 절차를 도시한 순서도이다.

[65] 단계 501에서, 모바일 어플리케이션은 서비스 애플릿 A에 대한 액세스를 위해 관리 어플리케이션에 액세스 요청을 전송한다. 액세스 요청에는 액세스하고자 하는 서비스 애플릿의 AID가 포함된다. 도 5에서 서비스 애플릿 A의 AID는 A0000000041001이다.

[66] 단계 502에서, 관리 어플리케이션은 관리 애플릿과의 통신 설정 요청한다. 관리 어플리케이션은 관리 애플릿의 AID를 이용하여 관리 애플릿을 호출(선택)할 수 있다. 여기서, 관리 애플릿의 AID는 4D474D540101이다.

[67] 단계 503에서, 관리 애플릿은 관리 어플리케이션의 통신 설정 요청을 허락하거나 거부하는 응답 메시지를 전송한다.

[68] 단계 504에서, 관리 애플릿이 관리 어플리케이션과 통신을 설정하면, 관리 애플리케이션은 서비스 애플릿 A에 대한 액세스 요청을 전송한다.

[69] 단계 505에서, 액세스 요청한 모바일 어플리케이션이 서비스 애플릿 A에 대한 액세스 권한이 있는 것으로 관리 애플릿이 판단한 경우, 액세스 허용 메시지가 응답된다.

[70] 모바일 어플리케이션의 SP ID가 서비스 애플릿 A의 AID와 연관된 경우, 모바일 어플리케이션이 서비스 애플릿 A에 대한 액세스 권한을 갖는 것으로 판단된다.

[71] 단계 506에서, 모바일 어플리케이션이 서비스 애플릿 A에 대한 액세스 권한을 갖고 있는 것으로 판단되면, 관리 어플리케이션은 액세스 요청된 서비스 애플릿 A을 선택하여 연결 설정을 요청한다. 단계 507에서, 서비스 애플릿 A는 관리 어플리케이션이 요청한 연결을 설정하거나 또는 거부 응답 메시지를 전송한다. 서비스 애플릿 A가 관리 어플리케이션의 연결 설정 요청을 수용한 경우, 관리 어플리케이션은 연결 정보를 모바일 어플리케이션에게 전달한다. 이후, 모바일 어플리케이션이 서비스 애플릿 A와 연결을 설정하면, 모바일 어플리케이션은 서비스 애플릿 A에 수록된 정보에 액세스할 수 있다.

[72] 반면, 관리 애플릿이 요청한 모바일 어플리케이션이 서비스 애플릿 A에 대한 액세스 권한을 갖지 않는 것으로 관리 애플릿이 판단한 경우, 액세스 불허 메시지가 응답된다.

[73] 액세스 요청한 모바일 어플리케이션이 서비스 애플릿 A에 대한 액세스 권한을 갖지 않는 것으로 판단한 경우, 단계 509에서, 관리 애플릿은 액세스를 거부하고, 액세스 불허 메세지가 관리 어플리케이션에서 모바일 어플리케이션으로 전송된다.

[74] 지금까지, SE의 애플릿에 대한 액세스를 제어/제한하는 방법에 대해 바람직한 실시예들을 들어 상세히 설명하였다.

[75] 위 실시예에서는, 액세스 권한이 없는 애플릿에 대한 액세스 요청을 관리 어플리케이션이 폐기하여, 액세스 요청이 액세스로 전달되지 않도록 함으로서, 액세스 권한 없는 어플리케이션의 애플릿 액세스를 금지한다.

[76] 또한, 메모리와 SE에 각각 설치된 관리 어플리케이션과 관리 애플릿이 관리 프로그램을 구성하여, 상호 간의 인터랙션 으로 애플릿 액세스 제어를 수행하도록 한 것으로 변형이 가능하다. 예를 들어, 관리 애플릿의 기능을 관리 어플리케이션에 흡수시키고 관리 애플릿을 생략하거나, 관리 어플리케이션의 기능을 관리 애플릿에 흡수시키고 관리 어플리케이션을 생략하는 것이 가능하다.

[77] 한편, 위 실시예에서는 지갑 어플리케이션과 어카운트 정보가 수록된 금융 서비스 애플릿을 상정하였는데, 이는 설명의 편의를 위한 예시적인 것에 불과하다. 지갑 어플리케이션 이외의 다른 어플리케이션과 금융 서비스 이외의 다른 서비스를 위한 애플릿의 경우도 본 발명의 기술적 사상이 적용될 수 있다.

[78] 또한, 어플리케이션을 식별하기 위한 SP ID는 다른 종류의 ID로 대체가능함은 물론이다.

[79] 그리고, 애플릿 액세스를 요청한 어플리케이션이 액세스 권한을 보유하였는지에 대한 판단은, 위 실시예들과 같이 관리 애플릿이 수행하여 관리 어플리케이션에 판단결과를 통보할 수 있음은 물론, 관리 어플리케이션이 관리 애플릿에 수록된 연관성 정보를 참고하여 판단하도록 구현하는 것도 가능하다.

[80] 한편, 보안 강화를 위해, 관리 어플리케이션을 제외한 어플리케이션은 관리 애플릿에 액세스할 수 없도록 구현할 수 있다. 더 나아가, 어플리케이션이 관리

어플리케이션을 통해서만 애플릿과 통신하도록 구현하는 것도 가능하다.

[81] 그리고, 보안 강화를 위해, 관리 애플릿에 수록된 어플리케이션과 애플릿의 연관성(도 1 내지 도 3에 도시된 테이블)은 TSM(Trusted Service Manager)에 의해 업데이트되도록 구현함이 바람직하다.

[82] 또한, 관리 어플리케이션은 액세스 불허 횟수가 정해진 상한을 초과하는 어플리케이션에 대해서는, 사용자에게 안내하여 점검을 유도하거나, 모든 애플릿에 대한 액세스를 제한하는 것으로 구현할 수 있다. 이는, 액세스 불허 횟수가 많은 어플리케이션은 멀웨어일 가능성이 있기 때문이다.

[83] 도 6은 본 발명의 일 실시예에 따른 모바일 단말의 하드웨어 구성을 도시한 블록도이다. 도 6에 도시된 바와 같이, 모바일 기기(600)는, 터치 스크린(610), 무선 통신부(620), 프로세서(630), NFC 모듈(Near Field Communication Module)(640), 메모리(650) 및 SE(660)를 구비한다.

[84] 터치 스크린(610)은 시각 정보(위 실시예에서는, 어플리케이션 실행 화면, 어카운트 정보 등) 이 표시되는 디스플레이로 기능하는 한편, 사용자 명령을 입력받기 위한 사용자 입력 수단으로 기능하다.

[85] 무선 통신부(620)는 이동 통신과 무선 네트워킹을 위한 수단이고, NFC 모듈(640)은 POS의 NFC 리더와 통신하여 SE(660)에 설치된 애플릿에 수록된 결제 정보와 그 밖의 서비스 정보를 전달하기 위한 모듈이다.

[86] 메모리(650)는 어플리케이션들과 관리 어플리케이션이 설치되는 저장매체이며, SE(660)는 서비스 애플릿들과 관리 애플릿이 설치되는 저장매체로, UICC(Universal IC Card), e-SE(embedded-SE), SD 카드(Secure Digital Card) 등으로 구현가능하다. SE(660)에는 NFC 모듈(640)이 포함될 수도 있다.

[87] 프로세서(630)는, 메모리(650)에 저장/설치된 어플리케이션들과 관리 어플리케이션을이 실행하고, SE(660)에 저장/설치된 서비스 애플릿들과 관리 애플릿을 실행하여, 궁극적으도 도 2 내지 도 5에 도시된 절차들이 모바일 단말(600) 내에서 수행되도록 한다.

[88] 본 발명의 기술적 사상 또는 범주를 벗어남이 없이 본 발명에서 다양한 수정 및 변형실시가 가능한 것은 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명백할 것이다. 따라서, 본 발명이 청구항 및 그들의 균등물의 범주 내에 있다는 것을 전제로 본 발명이 이 발명의 수정 및 변형을 포함하는 것을 의도한다.

청구범위

[청구항 1] 어플리케이션이, SE(Secure Element)에 저장된 애플릿에 대한 액세스를 관리 프로그램에 요청하는 단계; 및
상기 관리 프로그램이, 액세스 요청된 애플릿에 대한 상기 어플리케이션의 액세스를 제어하는 단계;를 포함하는 것을 특징으로 하는 애플릿 액세스 제어 방법.

[청구항 2] 제 1항에 있어서,
상기 어플리케이션은, 메모리에 설치되어 있고,
상기 관리 프로그램은, 상기 메모리에 설치된 관리 어플리케이션과 상기 SE에 설치된 관리 애플릿을 포함하며,
상기 제어단계는,
상기 관리 어플리케이션과 상기 관리 애플릿 간의 인터랙션에 의해 수행되는 것을 특징으로 하는 애플릿 액세스 제어 방법.

[청구항 3] 제 2항에 있어서,
상기 요청단계는,
상기 어플리케이션이, 상기 애플릿에 대한 액세스를 상기 관리 어플리케이션에 요청하고,
상기 제어단계는,
상기 관리 어플리케이션이, 상기 관리 애플릿과 통신을 설정하는 단계;
상기 관리 어플리케이션이, 상기 어플리케이션의 액세스 요청을 상기 관리 애플릿에 전달하는 단계; 및
상기 관리 애플릿이, 액세스 요청된 애플릿에 대한 액세스 권한이 상기 어플리케이션에 있는지 판단하는 단계;를 더 포함하는 것을 특징으로 하는 애플릿 액세스 제어 방법.

[청구항 4] 제 3항에 있어서,
상기 제어단계는,
상기 판단단계에서 상기 액세스 권한이 상기 어플리케이션에 있다고 판단되면, 상기 관리 어플리케이션이 액세스 요청된 애플릿에 상기 액세스 요청을 전달하는 단계;
상기 관리 어플리케이션이, 상기 어플리케이션에 액세스 허용 응답을 전송하는 단계; 및
상기 어플리케이션이 상기 액세스 요청된 애플릿과 통신을 설정하는 단계;를 더 포함하는 것을 특징으로 하는 애플릿 액세스 제어 방법.

[청구항 5] 제 4항에 있어서,
상기 어플리케이션은,

상기 관리 어플리케이션을 통해 액세스 요청된 애플릿과 통신하는 것을 특징으로 하는 애플릿 액세스 제어 방법.

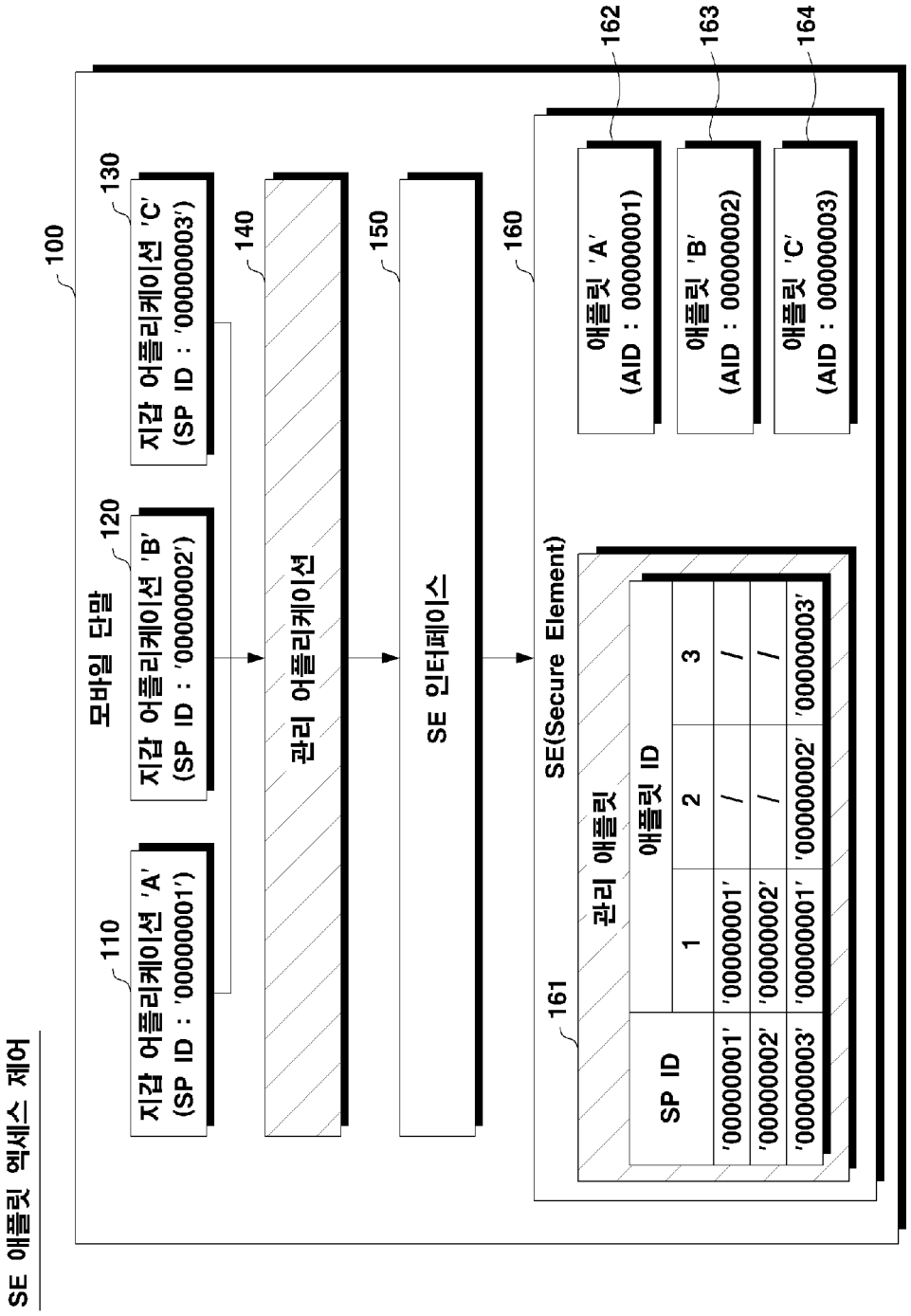
[청구항 6] 제 3항에 있어서,
상기 제어단계는,
상기 판단단계에서의 상기 액세스 권한이 상기 어플리케이션에 없다고 판단되면, 상기 관리 어플리케이션이 상기 액세스 요청을 폐기하는 단계; 및
상기 관리 어플리케이션이, 상기 어플리케이션에 액세스 불허 응답을 전송하는 단계;를 더 포함하는 것을 특징으로 하는 애플릿 액세스 제어 방법.

[청구항 7] 제 1항에 있어서,
상기 어플리케이션은,
상기 관리 애플릿에 액세스할 수 없는 것을 특징으로 하는 애플릿 액세스 제어 방법.

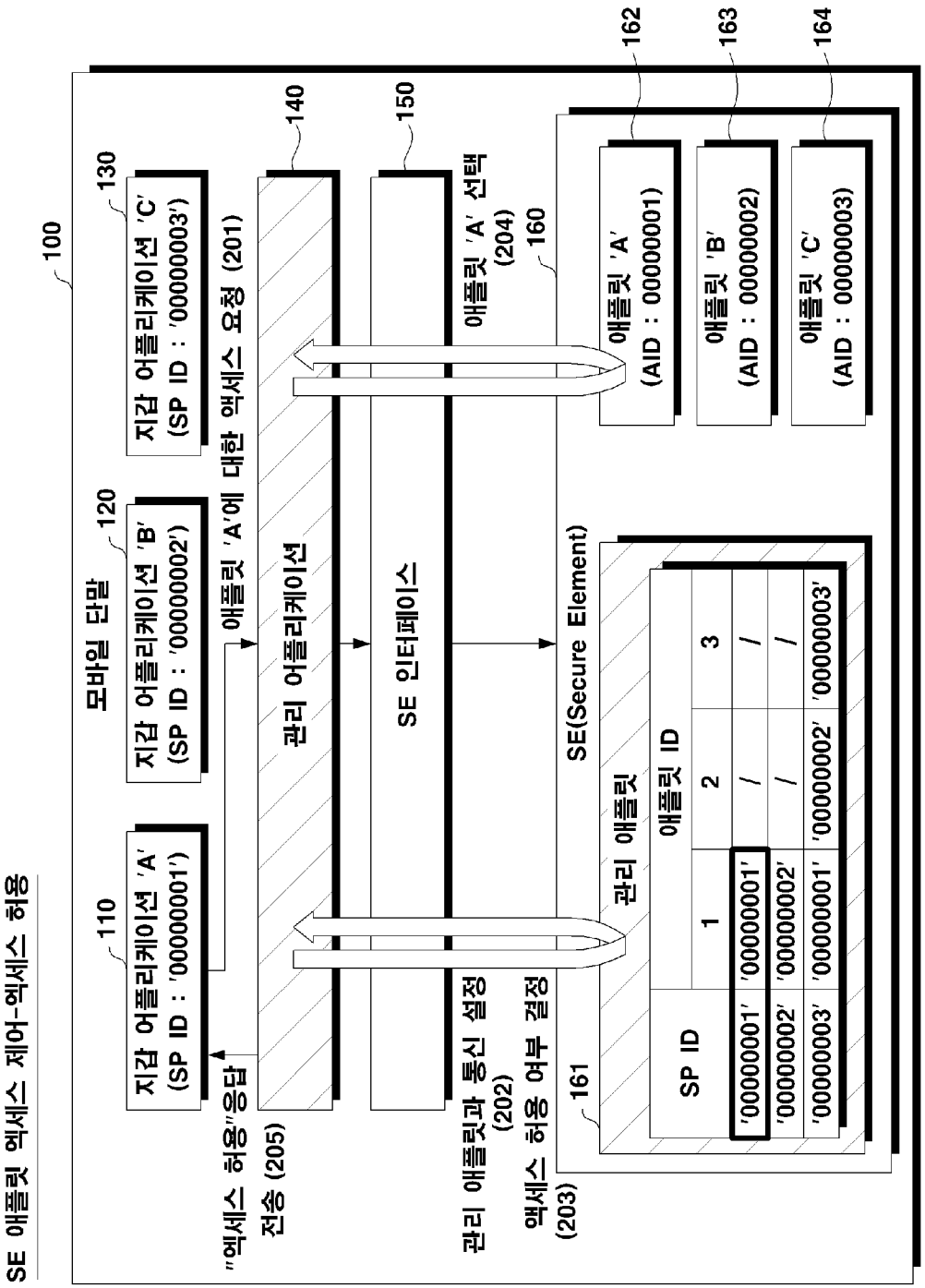
[청구항 8] 제 1항에 있어서,
상기 어플리케이션은 지갑 어플리케이션이고,
상기 애플릿은 금융 서비스 애플릿인 것을 특징으로 하는 애플릿 액세스 제어 방법.

[청구항 9] SE(Secure Element)에 저장된 애플릿에 대한 액세스를 관리 프로그램에 요청하는 어플리케이션이 설치된 저장부; 및
상기 어플리케이션 및 액세스 요청된 애플릿에 대한 상기 어플리케이션의 액세스를 제어하는 상기 관리 프로그램을 실행하는 프로세서;를 포함한하는 것을 특징으로 하는 모바일 단말.

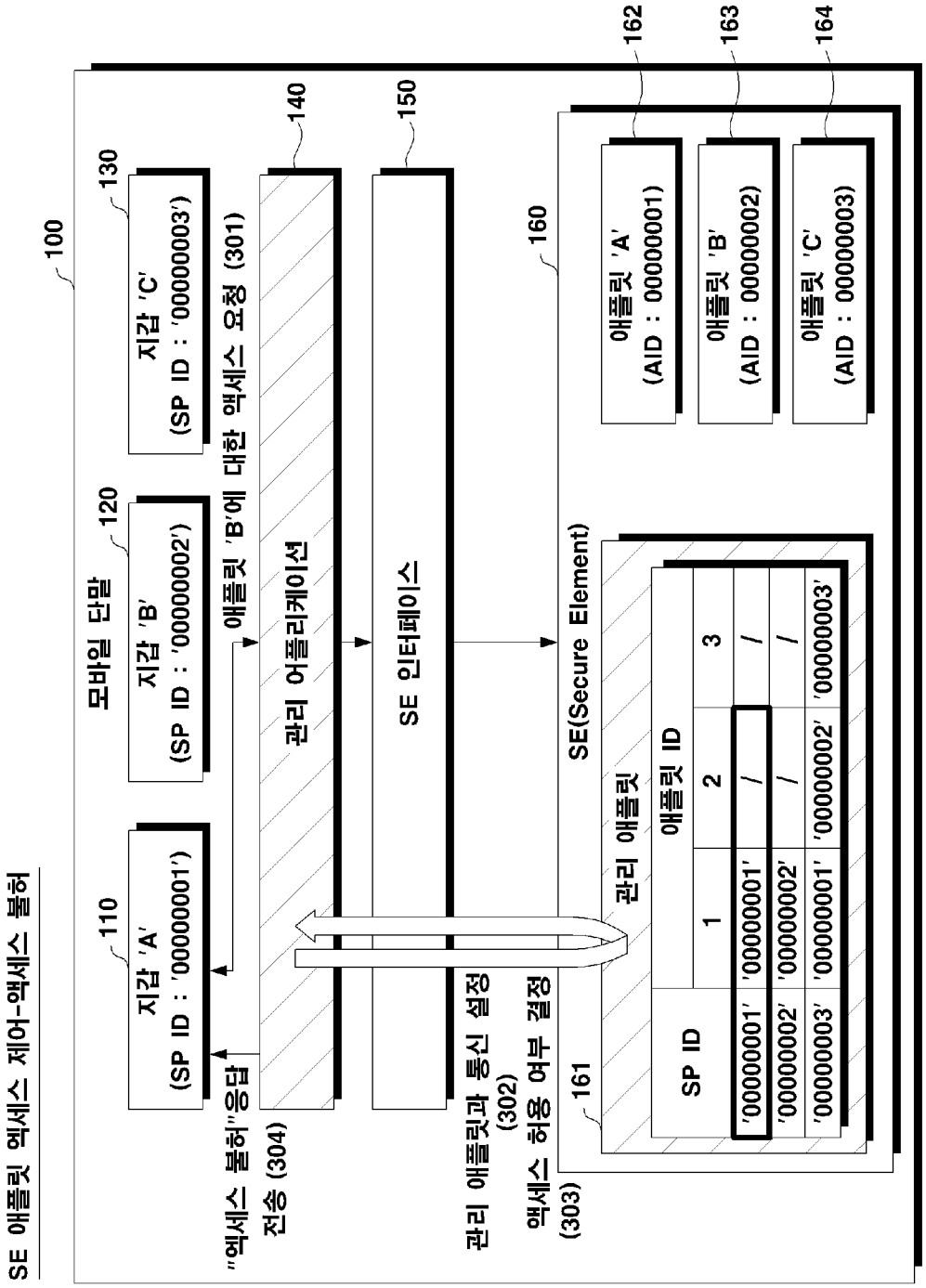
[Fig. 1]


SE 애플릿 엑세스 제어
100
모바일 단말
110
지갑 어플리케이션 'A'
(SP ID : '00000001')
120
지갑 어플리케이션 'B'
(SP ID : '00000002')
130
지갑 어플리케이션 'C'
(SP ID : '00000003')
140
관리 어플리케이션
150
SE 인터페이스
160
SE(Secure Element)
161
관리 애플릿
SP ID
애플릿 ID
1
2
3
'00000001'
'00000001'
/
/
'00000002'
'00000002'
/
/
'00000003'
'00000001'
'00000002'
'00000003'
162
애플릿 'A'
(AID : 00000001)
163
애플릿 'B'
(AID : 00000002)
164
애플릿 'C'
(AID : 00000003)

[Fig. 2]

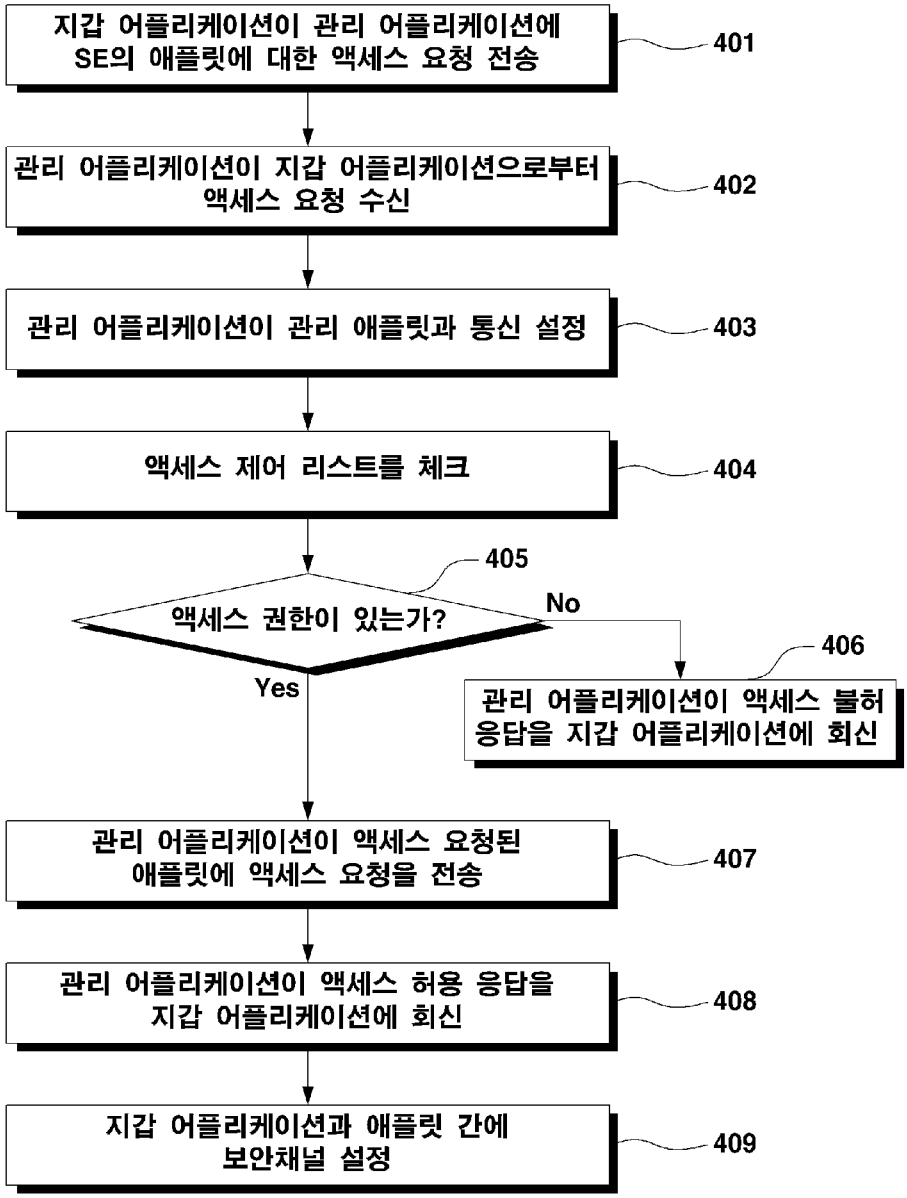

SE 애플릿 엑세스 제어-엑세스 허용
100
모바일 단말
110
지갑 어플리케이션 'A'
(SP ID : '00000001')
120
지갑 어플리케이션 'B'
(SP ID : '00000002')
130
지갑 어플리케이션 'C'
(SP ID : '00000003')
140
관리 어플리케이션
150
SE 인터페이스
160
SE(Secure Element)
161
관리 애플릿
162
애플릿 'A'
(AID : 00000001)
163
애플릿 'B'
(AID : 00000002)
164
애플릿 'C'
(AID : 00000003)
애플릿 'A' 선택
(204)
애플릿 'A'에 대한 엑세스 요청 (201)
"엑세스 허용"응답
전송 (205)
관리 애플릿과 통신 설정
(202)
엑세스 허용 여부 결정
(203)
SP ID
애플릿 ID
1
2
3
'00000001'
'00000001'
/
/
'00000002'
'00000002'
/
/
'00000003'
'00000001'
'00000002'
'00000003'

[Fig. 3]

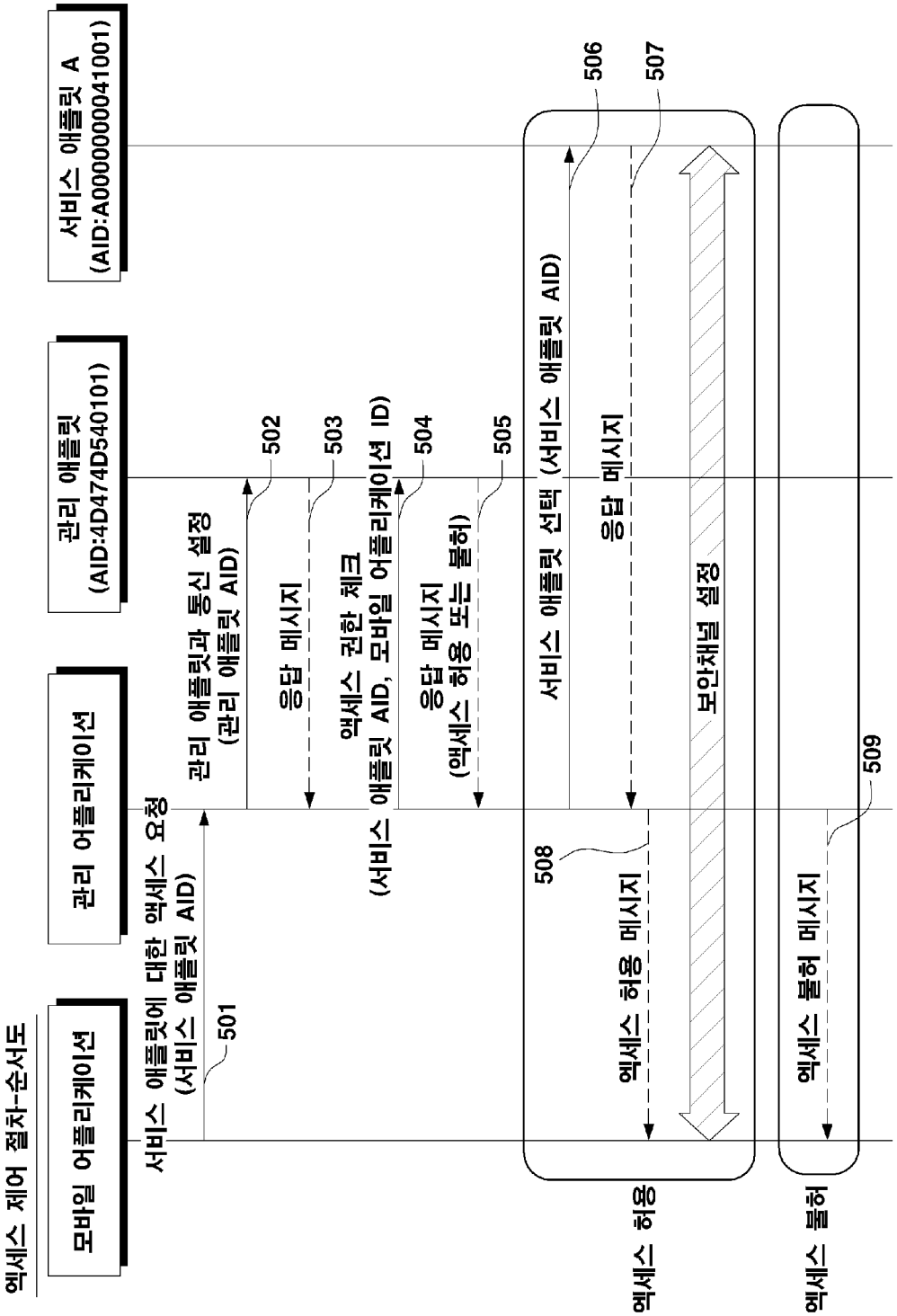

SE 애플릿 엑세스 제어-액세스 불허
100
모바일 단말
110
지갑 'A'
(SP ID : '00000001')
120
지갑 'B'
(SP ID : '00000002')
130
지갑 'C'
(SP ID : '00000003')
"엑세스 불허"응답
전송 (304)
애플릿 'B'에 대한 액세스 요청 (301)
140
관리 어플리케이션
150
SE 인터페이스
관리 애플릿과 통신 설정
(302)
액세스 허용 여부 결정
(303)
160
SE(Secure Element)
161
관리 애플릿
SP ID
애플릿 ID
1
2
3
'00000001'
'00000001'
/
/
'00000002'
'00000002'
/
/
'00000003'
'00000001'
'00000002'
'00000003'
162
애플릿 'A'
(AID : 00000001)
163
애플릿 'B'
(AID : 00000002)
164
애플릿 'C'
(AID : 00000003)

[Fig. 4]

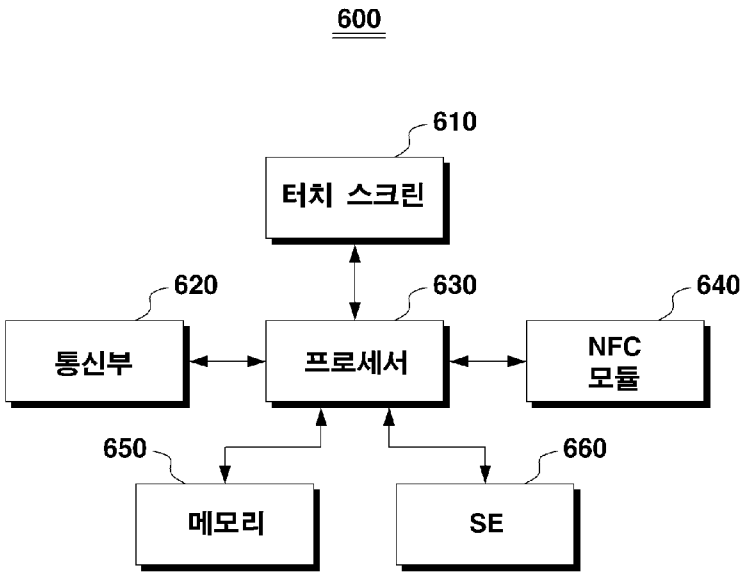
엑세스 제어 절차-흐름도



[Fig. 5]


엑세스 제어 절차-순서도
모바일 어플리케이션
관리 어플리케이션
관리 애플릿 (AID:4D474D540101)
서비스 애플릿 A (AID:A0000000041001)
서비스 애플릿에 대한 액세스 요청 (서비스 애플릿 AID)
501
관리 애플릿과 통신 설정 (관리 애플릿 AID)
502
응답 메시지
503
액세스 권한 체크 (서비스 애플릿 AID, 모바일 어플리케이션 ID)
504
응답 메시지 (액세스 허용 또는 불허)
505
서비스 애플릿 선택 (서비스 애플릿 AID)
506
응답 메시지
507
보안채널 설정
508
엑세스 허용 메시지
509
엑세스 불허 메시지
엑세스 허용
엑세스 불허

[Fig. 6]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2012/010323

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00(2006.01)i, G06F 21/20(2006.01)i, G06F 21/22(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/00; G06F 21/24; H04W 88/02; G06F 21/20; H04L 29/06; G06F 21/02; G06Q 20/32; G06Q 40/02; H04L 12/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: SE(Secure Element), application, applet, access, right

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2005-0114635 A (NOKIA CORPORATION) 06 December 2005 See page 4, lines 12-35; claim 1; and figures 1-3.	1-9
Y	JP 2011-048761 A (NTT DOCOMO, INC.) 10 March 2011 See paragraphs 35-38; abstract; and figure 1.	1-9
A	WO 2011-000690 A1 (THOMSON LICENSING) 06 January 2011 See abstract; and claim 1.	1-9
A	KR 10-2011-0104480 A (VIVOTECH, INC.) 22 September 2011 See paragraphs 43-46; and figure 3b.	1-9
A	KR 10-2011-0120977 A (MOTOROLA MOBILITY LLC) 04 November 2011 See paragraphs 51-54; and figure 6.	1-9

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 FEBRUARY 2013 (15.02.2013)	**18 FEBRUARY 2013 (18.02.2013)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

International application No.
PCT/KR2012/010323

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2005-0114635 A	06.12.2005	EP 1455499 A1	08.09.2004
		EP 1455499 A9	08.12.2004
		EP 1455499 B1	09.09.2009
		JP 04303284 B2	01.05.2009
		JP 2006-519524 A	24.08.2006
		US 2006-0173991 A1	03.08.2006
		US 7395049 B2	01.07.2008
		WO 2004-080027 A1	16.09.2004
JP 2011-048761 A	10.03.2011	CN 102483791 A	30.05.2012
		EP 2472429 A1	04.07.2012
		US 2012-0222136 A1	30.08.2012
		WO 2011-024564 A1	03.03.2011
WO 2011-000690 A1	06.01.2011	CN 102473216 A	23.05.2012
		EP 2270708 A1	05.01.2011
		EP 2449500 A1	09.05.2012
		KR 10-2012-0101292 A	13.09.2012
		US 2012-0110238 A1	03.05.2012
KR 10-2011-0104480 A	22.09.2011	AU 2009-302485 A1	15.04.2010
		AU 2009-302485 A8	15.04.2010
		CN 102257524 A	23.11.2011
		US 2010-0088188 A1	08.04.2010
		WO 2010-042560 A2	15.04.2010
		WO 2010-042560 A3	08.07.2010
KR 10-2011-0120977 A	04.11.2011	CN 102498705 A	13.06.2012
		EP 2412150 A1	01.02.2012
		US 2010-0248710 A1	30.09.2010
		WO 2010-111002 A1	30.09.2010

국 제 조 사 보 고 서

국제출원번호
PCT/KR2012/010323

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/00(2006.01)i, G06F 21/20(2006.01)i, G06F 21/22(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06F 21/00; G06F 21/24; H04W 88/02; G06F 21/20; H04L 29/06; G06F 21/02; G06Q 20/32; G06Q 40/02; H04L 12/22

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: SE(Secure Element), 어플리케이션, 애플릿, 액세스, 권한

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2005-0114635 A (노키아 코포레이션) 2005.12.06 페이지 4, 라인 12-35; 청구항 1; 및 도면 1-3 참조.	1-9
Y	JP 2011-048761 A (NTT DOCOMO, INC.) 2011.03.10 단락 35-38; 요약; 및 도면 1 참조.	1-9
A	WO 2011-000690 A1 (THOMSON LICENSING) 2011.01.06 요약; 및 청구항 1 참조.	1-9
A	KR 10-2011-0104480 A (비보텍, 인코포레이티드) 2011.09.22 단락 43-46; 및 도면 3b 참조.	1-9
A	KR 10-2011-0120977 A (모토로라 모빌리티, 인크.) 2011.11.04 단락 51-54; 및 도면 6 참조	1-9

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2013년 02월 15일 (15.02.2013)	**2013년 02월 18일 (18.02.2013)**

ISA/KR의 명칭 및 우편주소

팩스 번호 82-42-472-7140

심사관

변성철

전화번호 82-42-481-8262

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2012/010323

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2005-0114635 A	2005.12.06	EP 1455499 A1	2004.09.08
		EP 1455499 A9	2004.12.08
		EP 1455499 B1	2009.09.09
		JP 04303284 B2	2009.05.01
		JP 2006-519524 A	2006.08.24
		US 2006-0173991 A1	2006.08.03
		US 7395049 B2	2008.07.01
		WO 2004-080027 A1	2004.09.16
JP 2011-048761 A	2011.03.10	CN 102483791 A	2012.05.30
		EP 2472429 A1	2012.07.04
		US 2012-0222136 A1	2012.08.30
		WO 2011-024564 A1	2011.03.03
WO 2011-000690 A1	2011.01.06	CN 102473216 A	2012.05.23
		EP 2270708 A1	2011.01.05
		EP 2449500 A1	2012.05.09
		KR 10-2012-0101292 A	2012.09.13
		US 2012-0110238 A1	2012.05.03
KR 10-2011-0104480 A	2011.09.22	AU 2009-302485 A1	2010.04.15
		AU 2009-302485 A8	2010.04.15
		CN 102257524 A	2011.11.23
		US 2010-0088188 A1	2010.04.08
		WO 2010-042560 A2	2010.04.15
		WO 2010-042560 A3	2010.07.08
KR 10-2011-0120977 A	2011.11.04	CN 102498705 A	2012.06.13
		EP 2412150 A1	2012.02.01
		US 2010-0248710 A1	2010.09.30
		WO 2010-111002 A1	2010.09.30