(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년11월18일
(11) 등록번호 10-2180481
(24) 등록일자 2020년11월12일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) *H04L 29/06* (2006.01)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 67/16 (2013.01)
H04L 63/123 (2013.01)
(21) 출원번호 10-2019-0087100
(22) 출원일자 2019년07월18일
심사청구일자 2019년07월18일
(65) 공개번호 10-2020-0127812
(43) 공개일자 2020년11월11일
(30) 우선권주장
1020190052385 2019년05월03일 대한민국(KR)
(56) 선행기술조사문헌
MSG MCP 008-2018 V1.0, "Approved minutes 12th meeting ad hoc multi-stakeholder group on Mobile Contactless SEPA Cards Interoperability Implementation Guidelines" (2018.02.23.)
(뒷면에 계속)
전체 청구항 수 : 총 16 항

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
구종희
경기도 수원시 영통구 삼성로 129 (매탄동)
이덕기
경기도 수원시 영통구 삼성로 129 (매탄동)
(뒷면에 계속)
(74) 대리인
리앤목특허법인

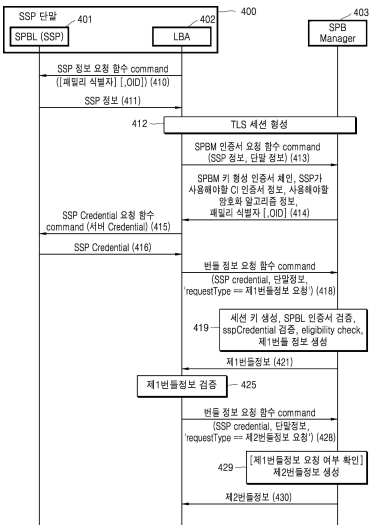
심사관 : 장상배

(54) 발명의 명칭 **번들 정보를 제공하는 방법 및 장치**

(57) 요 약

본 개시는 번들 정보를 제공하는 방법 및 장치에 관한 것이다. 본 개시의 일 실시예에 따른 SSP 단말은 번들의 식별자 및 메타데이터를 포함하는 제 1 번들 정보의 요청을 SPB 서버에 전송하고, 요청에 따라, SPB 서버로부터 수신된 제 1 번들 정보의 유효성을 검증하며, 제 1 번들 정보가 유효한 것으로 검증됨에 따라, 번들에 관한 암호화된 데이터를 포함하는 제 2 번들 정보의 요청을 SPB 서버에 전송하고, 제 2 번들 정보의 요청을 기초로 SSP 단말이 제 1 번들 정보를 요청한 단말임이 확인됨에 따라, SPB 서버로부터 상기 제 2 번들 정보를 수신할 수 있다.

대 표 도 - 도4a



(52) CPC특허분류
H04L 63/166 (2013.01)
H04L 67/2804 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/321 (2013.01)
H04L 9/3247 (2013.01)
H04L 9/3265 (2013.01)
(72) 발명자
윤강진
경기도 수원시 영통구 삼성로 129 (매탄동)
임태형
경기도 수원시 영통구 삼성로 129 (매탄동)

(56) 선행기술조사문헌
US20170222991 A1
US20170048251 A1
WO2018021897 A1
US20190074983 A1

명 세 서

청구범위

청구항 1

단말이 번들 정보를 제공하는 방법에 있어서,

SSP(smart secure platform) 크리덴셜(credential)을 획득하는 단계;

상기 획득한 SSP 크리덴셜 및 번들 정보에 대한 요청 유형을 포함하는 요청 명령을 서버에 전송하는 단계; 및

상기 서버에서 상기 SSP 크리덴셜이 검증된 경우, 상기 요청 유형에 기초하여 제1 번들 정보 또는 제2 번들 정보를 상기 서버로부터 수신하는 단계;를 포함하고,

상기 제1 번들 정보는 상기 제2 번들 정보에 대한 SPB (secondary platform bundle) 메타 데이터를 포함하는, 방법.

청구항 2

제 1 항에 있어서,

상기 수신하는 단계는, 상기 요청 유형이 제1 유형으로 결정된 경우, 상기 서버로부터 상기 제2 번들 정보를 수신하는 단계;를 포함하는, 방법.

청구항 3

제 1 항에 있어서,

상기 수신하는 단계는,

상기 요청 유형이 제2 유형으로 결정된 경우, 상기 서버로부터 상기 제1 번들 정보를 수신하는 단계;

상기 수신된 제1 번들 정보를 검증하는 단계;

상기 제2 번들 정보에 대한 요청 명령을 상기 서버로 전송하는 단계; 및

상기 제2 번들 정보에 대한 요청 명령의 요청 유형이 제3 유형으로 결정되고, 상기 제2 번들 정보에 대한 요청 명령이 상기 SSP 크리덴셜에 기초하여 상기 서버에서 검증된 경우, 상기 서버로부터 상기 제2 번들 정보를 수신하는 단계;를 포함하는, 방법.

청구항 4

제 1 항에 있어서,

상기 SPB 메타 데이터는 패밀리 식별자에 대응하는 관리자 특수 데이터(custodian specific data)의 세트를 포함하는 방법.

청구항 5

삭제

청구항 6

서버가 번들 정보를 제공하는 방법에 있어서,

단말의 SSP(smart secure platform) 크리덴셜(credential) 및 번들 정보에 대한 요청 유형을 포함하는 요청 명령을 상기 단말로부터 수신하는 단계;

상기 요청 명령으로부터 상기 번들 정보에 대한 요청 유형을 식별하는 단계; 및

상기 SSP 크리덴셜이 검증된 경우, 상기 식별된 요청 유형에 기초하여 제1 번들 정보 또는 제2 번들 정보를 상

기 단말에 전송하는 단계;를 포함하고,

상기 제1 번들 정보는 상기 제2 번들 정보에 대한 SPB (secondary platform bundle) 메타 데이터를 포함하는, 방법.

청구항 7

제 6 항에 있어서,

상기 요청 유형이 제1 유형으로 결정된 경우, 상기 제2 번들 정보를 전송하는 단계;를 더 포함하는, 방법.

청구항 8

제 6 항에 있어서,

상기 전송하는 단계는,

상기 요청 유형이 제2 유형으로 결정된 경우, 상기 제1 번들 정보를 상기 단말로 전송하는 단계;

상기 전송된 제1 번들 정보가 상기 단말에서 검증됨에 기초하여, 상기 제2 번들 정보에 대한 요청 명령을 상기 단말로부터 수신하는 단계;

상기 제2 번들 정보에 대한 요청 명령의 요청 유형이 제3 유형으로 결정된 경우, 상기 제2 번들 정보에 대한 요청 명령을 상기 SSP 크리덴셜에 기초하여 검증하는 단계; 및

상기 제2 번들 정보에 대한 요청 명령이 검증된 경우, 상기 제2 번들 정보를 단말로 전송하는 단계;를 포함하는, 방법.

청구항 9

제 6 항에 있어서,

상기 SPB 메타 데이터는 패밀리 식별자에 대응하는 관리자 특수 데이터(custodian specific data)의 세트를 포함하는 방법.

청구항 10

삭제

청구항 11

단말에 있어서,

송수신부; 및

적어도 하나의 프로세서를 포함하고,

상기 적어도 하나의 프로세서는,

SSP(smart secure platform) 크리덴셜(credential)을 획득하고,

상기 송수신부를 통해, 상기 획득한 SSP 크리덴셜 및 번들 정보에 대한 요청 유형을 포함하는 요청 명령을 서버로 전송하며,

상기 서버에서 상기 SSP 크리덴셜이 검증된 경우, 상기 송수신부를 통해, 상기 요청 유형에 기초하여 제1 번들 정보 또는 제2 번들 정보를 상기 서버로부터 수신하고,

상기 제1 번들 정보는 상기 제2 번들 정보에 대한 SPB (secondary platform bundle) 메타 데이터를 포함하는, 단말.

청구항 12

제 11 항에 있어서,

상기 적어도 하나의 프로세서는, 상기 요청 유형이 제1 유형으로 결정된 경우, 상기 송수신부를 통해 상기 서버

로부터 상기 제2 번들 정보를 수신하는, 단말.

청구항 13

제 11 항에 있어서, 상기 적어도 하나의 프로세서는,

상기 요청 유형이 제2 유형으로 결정된 경우, 상기 송수신부를 통해 상기 서버로부터 상기 제1 번들 정보를 수신하고,

상기 수신된 제1 번들 정보를 검증하며,

상기 송수신부를 통해 상기 제2 번들 정보에 대한 요청 명령을 상기 서버로 전송하고,

상기 제2 번들 정보에 대한 요청 명령의 요청 유형이 제3 유형으로 결정되고, 상기 제2 번들 정보에 대한 요청 명령이 상기 SSP 크리덴셜에 기초하여 상기 서버에서 검증된 경우, 상기 송수신부를 통해 상기 서버로부터 상기 제2 번들 정보를 수신하는, 단말.

청구항 14

제 11 항에 있어서,

상기 SPB 메타 데이터는 패밀리 식별자에 대응하는 관리자 특수 데이터(custodian specific data)의 세트를 포함하는, 단말.

청구항 15

삭제

청구항 16

서버에 있어서,

송수신부; 및

적어도 하나의 프로세서를 포함하고,

상기 적어도 하나의 프로세서는,

상기 송수신부를 통해, 단말의 SSP(smart secure platform) 크리덴셜(credential) 및 번들 정보에 대한 요청 유형을 포함하는 요청 명령을 상기 단말로부터 수신하고,

상기 요청 명령으로부터 상기 번들 정보에 대한 요청 유형을 식별하며,

상기 SSP 크리덴셜이 검증된 경우, 상기 송수신부를 통해, 상기 식별된 요청 유형에 기초하여 제1 번들 정보 또는 제2 번들 정보를 상기 단말로 전송하고,

상기 제1 번들 정보는 상기 제2 번들 정보에 대한 SPB (secondary platform bundle) 메타 데이터를 포함하는, 서버.

청구항 17

제 16 항에 있어서, 상기 적어도 하나의 프로세서는,

상기 요청 유형이 제1 유형으로 결정된 경우, 상기 송수신부를 통해 상기 제2 번들 정보를 전송하는, 서버.

청구항 18

제 16 항에 있어서, 상기 적어도 하나의 프로세서는,

상기 요청 유형이 제2 유형으로 결정된 경우, 상기 송수신부를 통해, 상기 제1 번들 정보를 상기 단말로 전송하고,

상기 전송된 제1 번들 정보가 상기 단말에서 검증됨에 기초하여, 상기 송수신부를 통해, 상기 제2 번들 정보에 대한 요청 명령을 상기 단말로부터 수신하며,

상기 제2 번들 정보에 대한 요청 명령의 요청 유형이 제3 유형으로 결정된 경우, 상기 제2 번들 정보에 대한 요청 명령을 상기 SSP 크리덴셜에 기초하여 검증하고,

상기 제2 번들 정보에 대한 요청 명령이 검증된 경우, 상기 송수신부를 통해, 상기 제2 번들 정보를 상기 단말로 전송하는, 서버.

청구항 19

제 16 항에 있어서,

상기 SPB 메타 데이터는 패밀리 식별자에 대응하는 관리자 특수 데이터(custodian specific data)의 세트를 포함하는, 서버.

청구항 20

삭제

발명의 설명

기 술 분 야

[0001] 본 개시는 번들 정보를 제공하는 방법 및 장치에 관한 것으로, 보다 구체적으로, SPB 서버의 번들 정보 생성 방법과 SSP 번들 다운로드 절차에서 SSP 단말이 번들 정보를 요청하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 4G 통신 시스템 상용화 이후 증가 추세에 있는 무선 데이터 트래픽 수요를 충족시키기 위해, 개선된 5G 통신 시스템 또는 pre-5G 통신 시스템을 개발하기 위한 노력이 이루어지고 있다. 이러한 이유로, 5G 통신 시스템 또는 pre-5G 통신 시스템은 4G 네트워크 이후(Beyond 4G Network) 통신 시스템 또는 LTE 시스템 이후(Post LTE) 이후의 시스템이라 불리어지고 있다. 높은 데이터 전송률을 달성하기 위해, 5G 통신 시스템은 초고주파(mmWave) 대역(예를 들어, 60기가(60GHz) 대역과 같은)에서의 구현이 고려되고 있다. 초고주파 대역에서의 전파의 경로손실 완화 및 전파의 전달 거리를 증가시키기 위해, 5G 통신 시스템에서는 빔포밍(beamforming), 거대 배열 다중입출력(massive MIMO), 전차원 다중입출력(full dimensional MIMO, FD-MIMO), 어레이 안테나(array antenna), 아날로그 빔형성(analog beam-forming), 및 대규모 안테나(large scale antenna) 기술들이 논의되고 있다. 또한 시스템의 네트워크 개선을 위해, 5G 통신 시스템에서는 진화된 소형 셀, 개선된 소형 셀(advanced small cell), 클라우드 무선 액세스 네트워크(cloud radio access network: cloud RAN), 초고밀도 네트워크(ultra-dense network), 기기 간 통신(Device to Device communication: D2D), 무선 백홀(wireless backhaul), 이동 네트워크(moving network), 협력 통신(cooperative communication), CoMP(Coordinated Multi-Points), 및 수신 간섭제거(interference cancellation) 등의 기술 개발이 이루어지고 있다. 이 밖에도, 5G 시스템에서는 진보된 코딩 변조(Advanced Coding Modulation: ACM) 방식인 FQAM(Hybrid FSK and QAM Modulation) 및 SWSC(Sliding Window Superposition Coding)과, 진보된 접속 기술인 FBMC(Filter Bank Multi Carrier), NOMA(non-orthogonal multiple access), 및 SCMA(sparse code multiple access) 등이 개발되고 있다.

[0003] 한편, 인터넷은 인간이 정보를 생성하고 소비하는 인간 중심의 연결 망에서, 사물 등 분산된 구성 요소들 간에 정보를 주고 받아 처리하는 IoT(Internet of Things, 사물인터넷) 망으로 진화하고 있다. 클라우드 서버 등과의 연결을 통한 빅데이터(Big data) 처리 기술 등이 IoT 기술에 결합된 IoE(Internet of Everything) 기술도 대두되고 있다. IoT를 구현하기 위해서, 센싱 기술, 유무선 통신 및 네트워크 인프라, 서비스 인터페이스 기술, 및 보안 기술과 같은 기술 요소 들이 요구되어, 최근에는 사물간의 연결을 위한 센서 네트워크(sensor network), 사물 통신(Machine to Machine, M2M), MTC(Machine Type Communication) 등의 기술이 연구되고 있다. IoT 환경에서는 연결된 사물들에서 생성된 데이터를 수집, 분석하여 인간의 삶에 새로운 가치를 창출하는 지능형 IT(Internet Technology) 서비스가 제공될 수 있다. IoT는 기존의 IT(information technology) 기술과 다양한 산업 간의 융합 및 복합을 통하여 스마트홈, 스마트 빌딩, 스마트 시티, 스마트 카 혹은 커넥티드 카, 스마트 그리드, 헬스 케어, 스마트 가전, 첨단의료서비스 등의 분야에 응용될 수 있다.

[0004] 이에, 5G 통신 시스템을 IoT 망에 적용하기 위한 다양한 시도들이 이루어지고 있다. 예를 들어, 센서 네트워크(sensor network), 사물 통신(Machine to Machine, M2M), MTC(Machine Type Communication) 등의 기술이 5G 통신 기술이 빔 포밍, MIMO, 및 어레이 안테나 등의 기법에 의해 구현되고 있는 것이다. 앞서 설명한 빅데이터

처리 기술로써 클라우드 무선 액세스 네트워크(cloud RAN)가 적용되는 것도 5G 기술과 IoT 기술 융합의 일 예라고 할 수 있을 것이다. 상술한 것과 이동통신 시스템의 발전에 따라 다양한 서비스를 제공할 수 있게 됨으로써, 이러한 서비스들을 효과적으로 제공하기 위한 방안이 요구되고 있다.

발명의 내용

해결하려는 과제

[0005] 본 개시의 일 실시예에 따르면, 서비스 제공자(Service Provider) 또는 번들 관리 서버 (SPB Manager)가 SSP 번들의 제1 번들 정보와 제2 번들 정보를 생성하는 방법을 제공할 수 있다.

[0006] 또한, 본 개시에 개시된 실시 예에서는 본 개시로 인하여 SSP 단말이 번들 다운로드를 시도할 때, 제1 번들 정보 및 제 2 번들 정보를 요청하는 절차와 방법을 제공할 수 있다.

과제의 해결 수단

[0007] 일 실시예에 따른 SSP 단말이 번들 정보를 제공하는 방법은, 번들의 식별자 및 메타데이터를 포함하는 제 1 번들 정보의 요청을 SPB 서버에 전송하는 단계; 요청에 따라, SPB 서버로부터 수신된 제 1 번들 정보의 유효성을 검증하는 단계; 제 1 번들 정보가 유효한 것으로 검증됨에 따라, 번들에 관한 암호화된 데이터를 포함하는 제 2 번들 정보의 요청을 SPB 서버에 전송하는 단계; 및

[0008] 제 2 번들 정보의 요청을 기초로 SSP 단말이 제 1 번들 정보를 요청한 단말임이 확인됨에 따라, SPB 서버로부터 상기 제 2 번들 정보를 수신하는 단계를 포함할 수 있다.

[0009] 일 실시예에 따른 SSP 단말이 번들 정보를 제공하는 방법에 있어서, 제 1 번들 정보의 요청 및 제 2 번들 정보의 요청은 각각 SSP 크리덴셜(credential)을 포함하며, 제 2 번들 정보의 요청에 포함된 SSP 크리덴셜이 제 1 번들 정보의 요청에 포함된 SSP 크리덴셜과 대응되는지 여부에 기초하여, SSP 단말이 제 1 번들 정보를 요청한 단말임이 확인될 수 있다.

[0010] 일 실시예에 따른 SSP 단말이 번들 정보를 제공하는 방법은, SPB 서버로부터 제 1 번들 정보 및 식별값을 수신하는 단계; 수신된 식별값을 기반으로 생성된 서명값을 제 2 번들 정보의 요청과 함께 SPB 서버에 전송하는 단계를 더 포함하고, 서명값을 기초로, SSP 단말이 제 1 번들 정보를 요청한 단말임이 확인될 수 있다.

[0011] 일 실시예에 따른 SSP 단말이 번들 정보를 제공하는 방법은, 수신된 식별값을 SPBL에 전송하는 단계; SPBL로부터 식별값을 기초로 생성된 서명값을 수신하는 단계를 더 포함할 수 있다.

[0012] 일 실시예에 따른 SSP 단말이 번들 정보를 제공하는 방법은, SPB 서버로부터 식별값을 수신하는 단계; 및 수신된 식별값을 기초로 서명값을 생성하는 단계를 더 포함하고, 제 1 번들 정보의 요청은, 서명값이 생성됨에 따라, SSP 단말로부터 SPB 서버로 전송될 수 있다.

[0013] 일 실시예에 따른 SSP 단말이 번들 정보를 제공하는 방법은, SPBL 서명용 인증서를 기반으로 서명된 서명값을 획득하는 단계를 더 포함하고, SPB 서버로부터 전송되는 제 2 번들 정보의 요청은, 획득된 서명값을 포함하고, 제 2 번들 정보는, SPB 서버에서 검증된 SPBL 서명용 인증서를 기반으로 서명값이 검증됨에 따라, SPB 서버로부터 수신될 수 있다.

[0014] 일 실시예에 따른 SSP 단말이 번들 정보를 제공하는 방법에 있어서, 제 1 번들 정보의 요청과 상기 제 2 번들 정보의 요청은 각각 서로 다른 종류의 번들 정보 요청 함수 커맨드로 구성될 수 있다. 또한, 제 1 번들 정보 요청 후 제 2 번들 정보를 요청하는 커맨드는, 제 1 번들 정보 요청없이 바로 제 2 번들 정보를 요청하는 커맨드와 구분되어 정의될 수 있다.

[0015] 일 실시예에 따른 SPB 서버가 번들 정보를 제공하는 방법은, 번들의 식별자 및 메타데이터를 포함하는 제 1 번들 정보의 요청을 SSP 단말로부터 수신하는 단계; 요청에 따라, 제 1 번들 정보를 SSP 단말에 전송하는 단계; 번들에 관한 암호화된 데이터를 포함하는 제 2 번들 정보의 요청을 SSP 단말로부터 수신하는 단계; 및 제 2 번들 정보의 요청을 기초로 SSP 단말이 제 1 번들 정보를 요청한 단말임이 확인됨에 따라, 제 2 번들 정보를 SSP 단말에 전송하는 단계를 포함할 수 있다.

[0016] 일 실시예에 따른 SPB 서버가 번들 정보를 제공하는 방법은, 제 2 번들 정보의 요청에 포함된 SSP 크리덴셜(credential)이 제 1 번들 정보의 요청에 포함된 SSP 크리덴셜에 대응되는지 여부를 판단하는 단계를 더 포함하

고, 판단 결과를 기초로, 제 2 번들 정보의 요청을 전송한 단말이 제 1 번들 정보의 요청을 전송한 단말인지 여부가 확인될 수 있다.

[0017] 일 실시예에 따른 SPB 서버가 번들 정보를 제공하는 방법은, SSP 단말에 제 1 번들 정보 및 식별값을 전송하는 단계; 수신된 식별값을 기반으로 생성된 서명값을 제 2 번들 정보의 요청과 함께 SSP 단말로부터 수신하는 단계; 및 서명값을 기초로, SSP 단말이 제 1 번들 정보를 요청한 단말임을 확인하는 단계를 더 포함할 수 있다.

[0018] 일 실시예에 따른 SPB 서버가 번들 정보를 제공하는 방법은, SSP 단말에 식별값을 전송하는 단계; 및 식별값의 전송 이후 수신된 제 1 번들 정보의 요청에 따라, 제 1 번들 정보를 생성하는 단계를 더 포함할 수 있다.

[0019] 일 실시예에 따른 SPB 서버가 번들 정보를 제공하는 방법은, 제 2 번들 정보의 요청에 포함된 서명값을 SPBL 서명용 인증서를 기반으로 검증하는 단계; 및 서명값이 검증됨에 따라, 제 2 번들 정보를 생성하는 단계를 더 포함할 수 있다.

[0020] 일 실시예에 따른 번들 정보를 제공하는 SSP 단말은, 메모리; 송수신부; 및 적어도 하나의 프로세서를 포함하고, 적어도 하나의 프로세서는, 번들의 식별자 및 메타데이터를 포함하는 제 1 번들 정보의 요청을 SPB 서버에 전송하도록 송수신부를 제어하고, 요청에 따라, SPB 서버로부터 수신된 제 1 번들 정보의 유효성을 검증하며, 제 1 번들 정보가 유효한 것으로 검증됨에 따라, 번들에 관한 암호화된 데이터를 포함하는 제 2 번들 정보의 요청을 SPB 서버에 전송하고, 제 2 번들 정보의 요청을 기초로 SSP 단말이 제 1 번들 정보를 요청한 단말임이 확인됨에 따라, SPB 서버로부터 제 2 번들 정보를 수신하도록 송수신부를 제어할 수 있다.

[0021] 일 실시예에 따른 번들 정보를 제공하는 SPB 서버는, 메모리; 송수신부; 및 적어도 하나의 프로세서를 포함하고, 적어도 하나의 프로세서는, 번들의 식별자 및 메타데이터를 포함하는 제 1 번들 정보의 요청을 SSP 단말로부터 수신하고, 요청에 따라, 제 1 번들 정보를 SSP 단말에 전송하며, 번들에 관한 암호화된 데이터를 포함하는 제 2 번들 정보의 요청을 SSP 단말로부터 수신하고, 제 2 번들 정보의 요청을 기초로 SSP 단말이 제 1 번들 정보를 요청한 단말임이 확인됨에 따라, 제 2 번들 정보를 SSP 단말에 전송하도록 송수신부를 제어할 수 있다.

발명의 효과

[0022] 본 개시에 따르면 SSP 단말은 SSP 번들의 다운로드 절차에서 암호화되지 않은 제1 번들 정보를 먼저 수신할 수 있다.

[0023] 본 개시의 SSP 제1 번들 정보 구조에 따르면, 제1 번들 정보는 특정 패밀리 식별자를 가지는 번들에 대해서 공통적으로 사용될 수 있는 패밀리-특수 메타데이타를 가질 수 있으며, 특정 패밀리 식별자에 대해서 복수 개의 관리 기관이 존재할 때, 각각의 관리 기관이 패밀리-특수 메타데이타 이외에 추가로 정의하고자 하는 설정값, 파라미터, 기능을 관리 기관-메타데이타에 포함하여 정의할 수 있다.

[0024] 본 개시의 SSP 제1 번들 정보 구조에 따르면, 특정 관리 기관이 동일한 패밀리 식별자를 관리하는 다른 관리 기관들이 정의한 관리 기관-메타데이타를 사용하여 번들의 제1 번들 정보를 구성할 수 있다.

[0025] 본 개시의 번들 요청 절차에 따르면, SSP 단말이 제1 번들 정보를 요청한 뒤 제2 번들 정보를 요청할 때, SPB Manager가 중복으로 수행하는 동작이나 불필요한 동작을 최소화 할 수 있다.

[0026] 본 개시의 번들 요청 절차에 따르면, SSP 단말이 제1 번들 정보를 요청한 뒤 제2 번들 정보를 요청할 때, SPB Manager가 SSP 단말이 제1 번들 정보를 수신하였음을 효율적이면서도 보안적으로 안전하게 수행할 수 있다.

도면의 간단한 설명

[0027] 도 1은 SSP 단말의 내부 구성요소와 구성요소 간 인터페이스를 나타내는 도면이다.

도 2는 본 개시의 일 실시예에 따른, SSP 단말이 번들을 다운로드 하기 위한 단말 내부 및 외부의 구성요소를 설명하기 위한 도면이다.

도 3은 SPB Manager가 LBA에 전달하는 제1 번들 정보의 구조를 도시한 도면이다.

도 4a는 본 개시의 일 실시예에 따른, SSP 단말이 SPB Manager에 제1 번들 정보와 제2 번들 정보를 요청하는 방법을 설명하기 위한 흐름도이다.

도 4b는 본 개시의 일부 실시 예에 따른, SSP 단말이 SPB Manager에 제1 번들 정보를 별도 요청하지 않고 제2

번들 정보를 요청하는 방법을 설명하기 위한 흐름도이다.

도 5는 본 개시의 일 실시 예에 따른 SSP 단말이 SPB Manager로부터 제1 번들 정보를 수신한 후, 제2 번들 정보를 요청하는 과정을 설명하기 위한 도면이다.

도 6은 본 개시의 일 실시예에 따른 SSP 단말이 SPB Manager로부터 제1 번들 정보를 수신한 후, 제2 번들 정보를 요청하는 과정을 설명하기 위한 도면이다.

도 7은 본 개시의 일 실시예에 따른 SSP 단말이 SPB Manager로부터 제1 번들 정보를 수신한 후, 제2 번들 정보를 요청하는 과정을 도시한 도면이다.

도 8은 본 개시의 일 실시예에 따른 SSP 단말이 SPB Manager로부터 제1 번들 정보를 수신한 후, 제2 번들 정보를 요청하는 과정을 설명하기 위한 도면이다.

도 9은 본 개시의 일 실시예에 따른 SSP 단말이 SPB Manager로부터 제1 번들 정보를 수신한 후, 제2 번들 정보를 요청하는 과정을 설명하기 위한 도면이다.

도 10은 번들 다운로드 절차 중 SPB Manager가 번들 정보 요청 함수 커맨드(command)를 수신했을 때의 SPB Manager 동작을 설명하기 위한 흐름도이다.

도 11은 일 실시예에 따른 SSP 단말의 동작을 설명하기 위한 흐름도이다.

도 12는 일 실시예에 따른 SPB 서버의 동작을 설명하기 위한 흐름도이다.

도 13은 일 실시예에 따른 SSP 단말(1300)의 블록도이다.

도 14는 일 실시예에 따른 SPB 서버의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0028] 이하, 본 개시의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0029] 실시 예를 설명함에 있어서 본 개시가 속하는 기술 분야에 익히 알려져 있고 본 개시와 직접적으로 관련이 없는 기술 내용에 대해서는 설명을 생략한다. 이는 불필요한 설명을 생략함으로써 본 개시의 요지를 흐리지 않고 더욱 명확히 전달하기 위함이다.

[0030] 마찬가지 이유로 첨부 도면에 있어서 일부 구성요소는 과장되거나 생략되거나 개략적으로 도시되었다. 또한, 각 구성요소의 크기는 실제 크기를 전적으로 반영하는 것이 아니다. 각 도면에서 동일한 또는 대응하는 구성요소에는 동일한 참조 번호를 부여하였다.

[0031] 본 개시의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 개시는 이하에서 개시되는 실시 예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시 예들은 본 개시가 완전하도록 하고, 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 개시의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 개시는 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0032] 이 때, 처리 흐름도 도면들의 각 블록과 흐름도 도면들의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수 있음을 이해할 수 있을 것이다. 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 흐름도 블록(들)에서 설명된 기능들을 수행하는 수단을 생성한다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 흐름도 블록(들)에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 흐름도 블록(들)에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0033] 또한, 각 블록은 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 실행 예들에서는 블록들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 블록들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0034] 이 때, 본 실시 예에서 사용되는 '~부'라는 용어는 소프트웨어 또는 FPGA 또는 ASIC과 같은 하드웨어 구성요소를 의미하며, '~부'는 어떤 역할들을 수행한다. 그렇지만 '~부'는 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. '~부'는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 '~부'는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들, 및 변수들을 포함한다. 구성요소들과 '~부'들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 '~부'들로 결합되거나 추가적인 구성요소들과 '~부'들로 더 분리될 수 있다. 뿐만 아니라, 구성요소들 및 '~부'들은 디바이스 또는 보안 멀티미디어카드 내의 하나 또는 그 이상의 CPU들을 재생시키도록 구현될 수도 있다.

[0035] 이하의 설명에서 사용되는 특정 용어들은 본 개시의 이해를 돕기 위해서 제공된 것이며, 이러한 특정 용어의 사용은 본 개시의 기술적 사상을 벗어나지 않는 범위에서 다른 형태로 변경될 수 있다.

[0036] SE(Secure Element)는 보안 정보(예: 이동통신망 접속 키, 신분증/여권 등의 사용자 신원확인 정보, 신용카드 정보, 암호화 키 등)를 저장하고, 저장된 보안 정보를 이용하는 제어 모듈(예: USIM 등의 망 접속 제어 모듈, 암호화 모듈, 키 생성 모듈 등)을 탑재하고 운영할 수 있는 단일 칩으로 구성된 보안 모듈을 의미한다. SE는 다양한 전자 장치(예: 스마트폰, 태블릿, 웨어러블 장치, 자동차, IoT 장치 등)에 사용될 수 있으며, 보안 정보와 제어 모듈을 통해 보안 서비스(예: 이통통신 망 접속, 결제, 사용자 인증 등)를 제공할 수 있다.

[0037] SE는 UICC(Universal Integrated Circuit Card), eSE (Embedded Secure Element), UICC와 eSE가 통합된 형태인 SSP(Smart Secure Platform)등으로 나뉠 수 있으며, 전자 장치에 연결 또는 설치되는 형태에 따라 탈착식(Removable), 고정식(Embedded), 그리고 특정 소자 또는 SoC(system on chip)에 통합되는 통합식(Integrated)으로 세분화 될 수 있다.

[0038] UICC(Universal Integrated Circuit Card)는 이동 통신 단말기 등에 삽입하여 사용하는 스마트카드(smart card)이고 UICC 카드라고도 부른다. UICC에는 이동통신사업자의 망에 접속하기 위한 접속 제어 모듈이 포함될 수 있다. 접속 제어 모듈의 예로는 USIM(Universal Subscriber Identity Module), SIM(Subscriber Identity Module), ISIM(IP Multimedia Service Identity Module) 등이 있다. USIM이 포함된 UICC를 통상 USIM 카드라고 부르기도 한다. 마찬가지로 SIM 모듈이 포함된 UICC를 통상적으로 SIM카드라고 부르기도 한다.

[0039] 한편, SIM 모듈은 UICC 제조시 탑재되거나 사용자가 원하는 시점에 사용하고자 하는 이동통신 서비스의 SIM 모듈을 UICC 카드에 다운로드 받을 수 있다. UICC 카드는 또한 복수개의 SIM 모듈을 다운로드 받아서 설치하고 그 중의 적어도 한 개의 SIM 모듈을 선택하여 사용할 수 있다. 이러한 UICC 카드는 단말에 고정하거나 고정하지 않을 수 있다. 단말에 고정하여 사용하는 UICC를 eUICC(embedded UICC)라고 하며, 특히 단말의 통신 프로세서(Communication Processor), 어플리케이션 프로세서(Application Processor) 또는 이 두 프로세서가 통합된 단일 프로세서 구조를 포함하는 System-On-Chip(SoC)에 내장된 UICC를 iUICC(Integrated UICC)라고 칭하기도 한다. 통상적으로 eUICC와 iUICC는 단말에 고정하여 사용하고, 원격으로 SIM 모듈을 다운로드 받아서 선택할 수 있는 UICC 카드를 의미할 수 있다.

[0040] 본 개시에서는 원격으로 SIM 모듈을 다운로드 받아 선택할 수 있는 UICC 카드를 eUICC 또는 iUICC로 통칭한다. 즉 원격으로 SIM 모듈을 다운로드 받아 선택할 수 있는 UICC 카드 중 단말에 고정하거나 고정하지 않는 UICC 카드를 통칭하여 eUICC 또는 iUICC로 사용한다. 또한 다운로드 받는 SIM 모듈정보를 통칭하여 eUICC 프로파일 또는 iUICC 프로파일, 또는 더 간단히 프로파일 이라는 용어로 사용한다.

[0041] eSE(Embedded Secure Element)는 전자 장치에 고정하여 사용하는 고정식 SE를 의미한다. eSE는 통상적으로 단말 제조사의 요청에 의해 제조사 전용으로 제조되며, 운영체제와 프레임워크를 포함하여 제조될 수 있다. eSE는 원격으로 애플릿 형태의 서비스 제어 모듈을 다운받아 설치하고 전자지갑, 티켓팅, 전자여권, 디지털키 등과 같은 다양한 보안 서비스 용도로 사용될 수 있다. 본 개시에서는 원격으로 서비스 제어 모듈을 다운로드 받아 설치할

수 있는 전자 장치에 부착된 단일 칩 형태의 SE를 eSE로 통칭한다.

[0042] 스마트 보안 장치 (SSP, Smart Secure Platform)는 UICC와 eSE의 기능을 단일 칩에서 통합 지원이 가능한 것으로, 간단히 SSP라 칭할 수 있다. SSP는 탈착식(rSSP, Removable SSP), 고정식(eSSP, Embedded SSP) 그리고 SoC에 내장된 통합식(iSSP, Integrated SSP)로 구분될 수 있다. SSP는 하나의 프라이머리 플랫폼(PP, Primary Platform)과 PP상에서 동작하는 적어도 하나 이상의 세컨더리 플랫폼 번들(SPB, Secondary Platform Bundle)로 구성될 수 있다. 프라이머리 플랫폼은 하드웨어 플랫폼과 low level Operating System(LLOS) 중 적어도 하나를 포함할 수 있고, 세컨더리 플랫폼 번들은 High-level Operating System(HLOS) 및 HLOS 위에서 구동되는 애플리케이션 중 적어도 하나를 포함할 수 있다. 세컨더리 플랫폼 번들은 SPB 또는 번들이라고 불리기도 한다.

[0043] 번들은 PP가 제공하는 Primary Platform Interface (PPI)를 통해 PP의 중앙처리장치, 메모리 등을 자원에 접근하고 이를 통해 PP상에서 구동될 수 있다. 번들은 SIM(Subscriber Identification Module), USIM(Universal SIM), ISIM(IP Multimedia SIM)등의 통신 어플리케이션이 탑재될 수 있으며, 전자지갑, 티켓팅, 전자여권, 디지털 키 등과 같은 다양한 응용 어플리케이션이 탑재될 수 있다.

[0044] SSP는 원격에서 다운로드 되고 설치되는 번들에 따라서 상기 기술된 UICC 또는 eSE 용도로 사용될 수 있으며, 복수개의 번들을 단일 SSP에 설치하고 동시에 운영하여 UICC와 eSE의 용도를 혼용할 수 있다. 즉, 프로파일을 포함하는 번들이 동작하는 경우 SSP는 이동통신사업자의 망에 접속하기 위한 UICC 용도로 사용 될 수 있다. 해당 UICC 번들은 상기 eUICC 또는 iUICC와 같이 적어도 하나 이상의 프로파일을 원격에서 번들 내로 다운로드 받고, 이 중 적어도 하나를 선택하여 동작할 수 있다. 또한, SSP상에서 전자지갑, 티켓팅, 전자여권 또는 디지털 키 등의 서비스를 제공할 수 있는 응용 어플리케이션을 탑재한 서비스 제어 모듈을 포함하는 번들이 동작하는 경우 SSP는 상기 eSE의 용도로 사용될 수 있다. 다수의 서비스 제어 모듈은 하나의 번들에 통합되어 설치되고 동작하거나, 각기 독립적인 번들로 설치되고 동작할 수 있다.

[0045] 이하에서는 본 개시에서 사용되는 용어에 대해서 더 자세히 설명한다.

[0046] 본 개시에서 SSP는 UICC와 eSE의 기능을 단일 칩에서 통합 지원할 수 있고, 탈착식(rSSP, Removable SSP), 고정식(eSSP, Embedded SSP) 그리고 SoC에 내장된 통합식(iSSP, Integrated SSP)로 구분 될 수 있는 칩 형태의 보안 모듈이다. SSP는 OTA(Over The Air)기술을 이용하여 번들을 외부의 번들 관리 서버(Secondary Platform Bundle Manager, SPB Manager)로부터 다운받아 설치할 수 있다.

[0047] 본 개시에서 SSP에 OTA 기술을 이용하여 번들을 다운받아 설치하는 방법은 단말에 삽입 및 탈거가 가능한 착탈식 SSP(rSSP), 단말에 설치되는 고정식 SSP(eSSP), 단말에 설치되는 SoC내부에 포함되는 통합식 SSP(iSSP)에 동일하게 적용될 수 있다.

[0048] 본 개시에서 용어 UICC는 SIM과 혼용될 수 있고, 용어 eUICC는 eSIM과 혼용될 수 있다.

[0049] 본 개시에서 세컨더리 플랫폼 번들(SPB, Secondary Platform Bundle) 은 SSP의 프라이머리 플랫폼(PP, Primary Platform) 상에서 PP의 리소스를 사용하여 구동되는 것으로 예를 들면 UICC 번들은 기존 UICC 내에 저장되는 어플리케이션, 파일시스템, 인증키 값 등과 이들이 동작하는 운영체체(HLOS)를 소프트웨어 형태로 패키징 한 것을 의미할 수 있다. 본 개시에서 세컨더리 플랫폼 번들은 번들이라고 지칭될 수 있다.

[0050] 본 개시에서 USIM Profile(USIM Profile)은 프로파일 (profile) 과 동일한 의미 또는 프로파일 내 USIM 어플리케이션에 포함된 정보를 소프트웨어 형태로 패키징 한 것을 의미할 수 있다.

[0051] 본 개시에서 단말 또는 외부 서버가 번들을 활성화(enable)하는 동작은, 해당 프로파일의 상태를 활성화 상태(enabled)로 변경하여 단말이 해당 번들이 제공하는 서비스(예: 통신사업자를 통해 통신서비스, 신용카드 결제 서비스, 사용자 인증 서비스 등)를 받을 수 있도록 설정하는 동작을 의미할 수 있다. 활성화 상태의 번들은 "활성화된 번들 (enabled Bundle)"로 표현될 수 있다. 활성화 상태의 번들은 SSP 내부 또는 외부의 저장공간에 암호화된 상태로 저장되어 있을 수 있다.

[0052] 본 개시에서 활성화된 번들은 번들 외부 입력(예: 사용자 입력, 푸쉬, 단말 내 어플리케이션의 요청, 통신 사업자의 인증 요청, PP 관리 메시지 등) 또는 번들 내부의 동작(예: 타이머, Polling)에 따라 구동 상태(Active)로 변경될 수 있다. 구동 상태의 번들은 SSP 내부 또는 외부의 저장공간에서 SSP 내부의 구동 메모리에 로딩되고 SSP 내부의 보안 제어 장치 (Secure CPU)를 이용하여 보안 정보를 처리하고 단말에 보안 서비스를 제공할 수 있다.

[0053] 본 개시에서 단말 또는 외부 서버가 번들을 비활성화(disable)하는 동작은, 해당 번들의 상태를 비활성화 상태

(disabled)로 변경하여 단말이 해당 번들이 제공하는 서비스를 받을 수 없도록 설정하는 동작을 의미할 수 있다. 비활성화 상태의 프로파일은 "비활성화된 번들(disabled Bundle)"로 표현될 수 있다. 활성화 상태의 번들은 SSP 내부 또는 외부의 저장공간에 암호화된 상태로 저장되어 있을 수 있다.

[0054] 본 개시에서 번들 관리서버는 서비스 제공자(Service Provider) 또는 다른 번들 관리서버의 요청에 의해 번들을 생성하거나, 생성된 번들을 암호화 하거나, 번들 원격관리 명령어를 생성하거나, 생성된 번들 원격관리 명령어를 암호화하는 기능을 제공할 수 있다. 상기 기능을 제공하는 번들 관리서버는 SPB Manager (Secondary Platform Bundle Manager), RBM(Remote Bundle Manager), IDS(Image Delivery Server), SM-DP(Subscription Manager Data Preparation), SM-DP+(Subscription Manager Data Preparation plus), 관리자 번들 서버, Managing SM-DP+(Managing Subscription Manager Data Preparation plus), 번들 암호화 서버, 번들 생성서버, 번들 제공자(Bundle Provisioner, BP), 번들 공급자(Bundle Provider), BPC holder(Bundle Provisioning Credentials holder) 중 적어도 하나로 표현될 수 있다.

[0055] 본 개시에서 번들 관리서버는 SSP에서 번들을 다운로드, 설치 또는 업데이트하고 번들의 상태를 원격 관리하기 위한 키 및 인증서의 설정을 관리하는 역할을 수행할 수 있다. 상기 기능을 제공하는 번들 관리 서버는 SPB Manager(Secondary Platform Bundle Manager), RBM(Remote Bundle Manager), IDS(Image Delivery Server), SM-SR(Subscription Manager Secure Routing), SM-SR+(Subscription Manager Secure Routing Plus), off-card entity of eUICC Profile Manager 또는 PMC holder(Profile Management Credentials holder), EM(eUICC Manager) 중 적어도 하나로 표현될 수 있다.

[0056] 본 개시에서 개통중개서버는 SPB Manager (Secondary Platform Bundle Manager), RBM(Remote Bundle Manager), SPBDS(Secondary Platform Bundle Discovery Sever), BDS(Bundle Discovery Sever), SM-DS(Subscription Manager Discovery Service), DS(Discovery Service), 근원개통중개서버(Root SM-DS), 대체개통중개서버(Alternative SM-DS) 중 적어도 하나로 표현될 수 있다. 개통중개서버는 하나 이상의 번들 관리서버 내지 개통중개서버로부터 이벤트 등록 요청(Register Event Request, Event Register Request)을 수신할 수 있다. 또한, 하나 이상의 개통중개서버가 복합적으로 사용될 수 있으며, 이 경우 제1 개통중개서버는 번들 관리서버뿐만 아니라 제2 개통중개서버로부터 이벤트 등록 요청을 수신할 수도 있다. 본 개시에서 개통중개서버의 기능은 번들 관리서버에 통합될 수 있다.

[0057] 본 개시에서 사용하는 용어 '단말'은 이동국(MS), 사용자 장비(UE; User Equipment), 사용자 터미널(UT; User Terminal), 무선 터미널, 액세스 터미널(AT), 터미널, 가입자 유닛(Subscriber Unit), 가입자 스테이션(SS; Subscriber Station), 무선 기기(wireless device), 무선 통신 디바이스, 무선 송수신 유닛(WTRU; Wireless Transmit/Receive Unit), 이동 노드, 모바일 또는 다른 용어들로서 지칭될 수 있다. 단말의 다양한 실시 예들은 셀룰러 전화기, 무선 통신 기능을 가지는 스마트 폰, 무선 통신 기능을 가지는 개인 휴대용 단말기(PDA), 무선 모뎀, 무선 통신 기능을 가지는 휴대용 컴퓨터, 무선 통신 기능을 가지는 디지털 카메라와 같은 촬영장치, 무선 통신 기능을 가지는 게이밍 장치, 무선 통신 기능을 가지는 음악저장 및 재생 가전제품, 무선 인터넷 접속 및 브라우징이 가능한 인터넷 가전제품뿐만 아니라 그러한 기능들의 조합들을 통합하고 있는 휴대형 유닛 또는 단말기들을 포함할 수 있다. 또한, 단말은 M2M(Machine to Machine) 단말, MTC(Machine Type Communication) 단말/디바이스를 포함할 수 있으나, 이에 한정되는 것은 아니다. 본 개시에서 단말은 전자장치라 지칭될 수도 있다.본 개시에서 전자장치에는 번들을 다운로드 하여 설치 가능한 SSP가 내장될 수 있다. SSP가 전자장치에 내장되지 않은 경우, 물리적으로 전자장치와 분리된 SSP는 전자장치에 삽입되어 전자장치와 연결될 수 있다. 예를 들어, SSP는 카드 형태로 전자장치에 삽입될 수 있다. 전자 장치는 단말을 포함할 수 있고, 이때, 단말은 번들을 다운로드하여 설치 가능한 SSP를 포함하는 단말일 수 있다. 단말에 SSP는 내장될 수 있을 뿐만 아니라, 단말과 SSP가 분리된 경우 SSP는 단말에 삽입될 수 있고, 단말에 삽입되어 단말과 연결될 수 있다.

[0058] 본 개시에서 단말 또는 전자장치는 SSP를 제어하도록 단말 또는 전자장치 내에 설치된 소프트웨어 또는 애플리케이션인 Local Bundle Assistant(LBA) 또는 Local Bundle Manager(LBM)를 포함할 수 있다. LBA 애플리케이션은 SSP에 번들을 다운로드하거나 설치된 번들의 활성화, 비활성화, 삭제 명령을 SSP에 전달할 수 있다.

[0059] 본 개시에서 단말 또는 전자장치는 eUICC를 제어하도록 단말 또는 전자장치 내에 설치된 소프트웨어 또는 애플리케이션인 Local Profile Assistant (LPA)를 포함할 수 있다. LPA는 Local Bundle Assistant (LBA)에 포함되어 구현될 수 있거나 LBA와 별도 애플리케이션으로 단말에 존재할 수 있다. 상기 LPA는 SSP를 내장한 단말의 eSIM 번들을 제어할 수 있는 소프트웨어 또는 애플리케이션 일 수 있다.

[0060] 본 개시에서 번들 식별자는 번들 패밀리 식별자(SPB Family Identifier), 번들 Matching ID, 이벤트 식별자

(Event ID)와 매칭되는 인자로 지칭될 수 있다. 번들 식별자(SPB ID)는 각 번들의 고유 식별자를 나타낼 수 있다. 번들 패밀리 식별자(SPB Family Identifier)는 번들의 종류(예: 이동통신사 망 접속을 위한 텔레콤 번들)의 종류를 구분하는 식별자를 나타낼 수 있다. 번들 구분자는 번들 관리서버에서 번들을 색인할 수 있는 값으로 사용될 수 있다. 본 개시에서 SSP 식별자(SSP ID)는, 단말에 내장된 SSP의 고유 식별자일 수 있고, sspID로 지칭될 수 있다. 또한 본 개시의 실시 예에서와 같이 단말과 SSP 칩이 분리되지 않을 경우에는 단말 ID일 수 있다. 또한, SSP 내의 특정한 번들 식별자(SPB ID)를 지칭할 수도 있다. 좀더 자세히는 SSP에서 다른 번들을 설치하고 활성화, 비활성화, 삭제를 관리하는 관리 번들 또는 로더(SPBL, Secondary Platform Bundle Loader)의 번들 식별자를 지칭 할 수도 있다. SSP는 복수개의 SSP 식별자를 가질 수 도 있으며, 복수개의 SSP 식별자는 고유한 단일의 SSP 식별자로부터 유도된 값일 수 있다. SSP 내부의 Primary Platform은 고유의 식별자를 가질 수 있으며 이를 Primary Platform 식별자라고 할 수 있다. SSP 식별자는 Primary Platform 식별자일 수 있다.

[0061] 본 개시에서 로더(SPBL, Secondary Platform Bundle Loader)는 SSP에서 다른 번들을 설치하고 활성화, 비활성화, 삭제를 관리하는 관리 번들을 지칭할 수 있다. 단말의 LBA 또는 원격의 서버는 로더를 통해 특정 번들을 설치, 활성화, 비활성화, 삭제할 수 있다. 본 개시에서 로더는 SSP로도 지칭될 수 있다.

[0062] 본 개시에서 이벤트(Event)는 번들 다운로드(Bundle Download), 또는 원격 번들 관리(Remote Bundle Management), 또는 기타 번들이나 SSP의 관리/처리 명령어를 통칭하는 용어일 수 있다. 이벤트(Event)는 원격 Bundle 제공 동작(Remote Bundle Provisioning Operation, 또는 RBP 동작, 또는 RBP Operation) 또는 이벤트 기록(Event Record)으로 명명될 수 있으며, 각 이벤트(Event)는 그에 대응하는 이벤트 식별자(Event Identifier, Event ID, EventID) 또는 매칭 식별자(Matching Identifier, Matching ID, MatchingID)와, 해당 이벤트가 저장된 번들 관리서버 또는 개통중개서버의 주소(FQDN, IP Address, 또는 URL) 또는 각 서버 식별자를 적어도 하나 이상 포함하는 데이터로 지칭될 수 있다. 번들 다운로드(Bundle Download)는 번들 설치(Bundle Installation)와 혼용될 수 있다. 또한, 이벤트 종류(Event Type)는 특정 이벤트가 번들 다운로드인지 원격 번들 관리(예를 들어, 삭제, 활성화, 비활성화, 교체, 업데이트 등)인지 또는 기타 번들이나 SSP 관리/처리 명령인지를 나타내는 용어로 사용될 수 있으며, 동작 종류(Operation Type 또는 OperationType), 동작 분류(Operation Class 또는 OperationClass), 이벤트 요청 종류(Event Request Type), 이벤트 분류(Event Class), 이벤트 요청 분류(Event Request Class) 등으로 명명될 수 있다.

[0063] 본 개시에서 로컬 번들 관리(Local Bundle Management, LBM)는 번들 로컬관리(Bundle Local Management), 로컬관리(Local Management), 로컬관리 명령(Local Management Command), 로컬 명령(Local Command), 로컬 번들 관리 패키지(LBM Package), 번들 로컬 관리 패키지(Bundle Local Management Package), 로컬관리 패키지(Local Management Package), 로컬관리 명령 패키지(Local Management Command Package), 로컬명령 패키지(Local Command Package)로 명명될 수 있다. LBM은 단말에 설치된 소프트웨어 등을 통해 특정 번들의 상태(Enabled, Disabled, Deleted)를 변경하거나, 특정 번들의 내용(예를 들면, 번들의 별칭(Bundle Nickname), 또는 번들 메타데이타(Bundle Metadata) 등)을 변경(update)하는 용도로 사용될 수 있다. LBM은 하나 이상의 로컬관리명령을 포함할 수도 있으며, 이 경우 각 로컬관리명령의 대상이 되는 번들은 로컬관리명령마다 서로 같거나 다를 수 있다.

[0064] 본 개시에서 목표 번들(target Bundle)은 로컬관리명령 내지 원격관리명령의 대상이 되는 번들을 지칭하는 용어로 사용될 수 있다.

[0065] 본 개시에서 서비스 제공자(Service Provider)는 번들 관리서버에 요구사항을 발행하여 번들 생성을 요청하고, 해당 번들을 통해 단말에 서비스를 제공하는 사업체를 나타낼 수 있다. 예를 들면, 통신 어플리케이션이 탑재된 번들 통해 통신망 접속 서비스를 제공하는 통신사업자(Mobile Operator)를 나타낼 수 있으며, 통신사업자의 사업지원시스템(Business Supporting System, BSS), 운영지원시스템(Operational Supporting System, OSS), POS 단말(Point of Sale Terminal), 그리고 기타 IT 시스템을 모두 통칭할 수 있다. 또한, 본 개시에서 서비스 제공자는 특정 사업체를 하나만 표현하는데 한정되지 않고, 하나 이상의 사업체의 그룹 또는 연합체(association 또는 consortium) 내지 해당 그룹 또는 연합체를 대표하는 대행사(representative)를 지칭하는 용어로 사용될 수도 있다.

[0066] 또한, 본 개시에서 서비스 제공자는 사업자(Operator 또는 OP 또는 Op.), 번들 소유자(Bundle Owner, BO), 이미지 소유자(Image Owner, IO) 등으로 명명될 수 있으며, 각 서비스 제공자는 이름 그리고/또는 고유 식별자(Object Identifier, OID)를 적어도 하나 이상 설정하거나 할당 받을 수 있다. 만일 서비스 제공자가 하나 이상의 사업체의 그룹 또는 연합체 또는 대행사를 지칭하는 경우, 임의의 그룹 또는 연합체 또는 대행사의 이름 또

는 고유 식별자는 해당 그룹 또는 연합체에 소속한 모든 사업체 내지 해당 대행사와 협력하는 모든 사업체가 공유하는 이름 또는 고유 식별자일 수 있다.

[0067] 본 개시에서 NAA는 네트워크 접속 어플리케이션(Network Access Application) 응용프로그램으로, UICC에 저장되어 망에 접속하기 위한 USIM 또는 ISIM과 같은 응용프로그램일 수 있다. NAA는 망접속 모듈일 수 있다.

[0068] 본 개시에서 텔레콤 번들(Telecom Bundle)은 적어도 하나의 NAA를 탑재하거나, 원격에서 적어도 하나의 NAA 다운로드 하고 설치할 수 있는 기능을 탑재하고 있는 번들 일 수 있다. 본 개시에서 텔레콤 번들은 이를 지칭하는 텔레콤 번들 식별자를 포함할 수 있다.

[0069] 본 개시에서 eSIM 번들 (eSIM Bundle)은 내부에 eUICC OS가 구동되어 eUICC와 같은 기능을 하여 단말에 profile을 받을 수 있는 번들 일 수 있다. 본 개시에서 eSIM 번들은 이를 지칭하는 텔레콤 번들 식별자를 포함할 수 있다.

[0070] 본 개시에서 eSIM 활성화 코드는 eSIM 단말 또는 SSP 단말에 프로파일을 다운로드 하기 위한 소정의 정보로서, eSIM Activation Code 라 명명될 수 있다. eSIM Activation Code는 프로파일을 다운로드 받기 위해 접속해야 하는 SM-DP+ 주소 또는 SM-DP+ 주소를 알려줄 수 있는 SM-DS 서버의 주소를 포함할 수 있으며, SM-DP+에 특정 프로파일의 매칭 식별자로 사용할 수 있는 Activation Code Token 값을 포함할 수 있다. eSIM Activation Code가 QR코드 형태로 입력된 경우, QR 코드에 담기는 데이터의 prefix로 'LPA:' 가 붙을 수 있다.

[0071] 본 개시에서 SSP 활성화 코드는 SSP 단말에 번들을 다운로드 하기 위한 소정의 정보로서, SSP Activation Code 라 명명될 수 있다. 단말 사용자는 SSP 활성화 코드를 SSP 단말의 LBA 애플리케이션에 입력하여 번들 다운로드 절차를 시작할 수 있다. SSP 활성화 코드는 eSIM 활성화 코드를 포함할 수 있다.

[0072] 본 개시에서 활성화 코드는 SSP 활성화 코드와 eSIM 활성화 코드를 통칭할 수 있다. 일반적으로 본 개시에서 활성화 코드는 SSP 활성화 코드 또는 eSIM 활성화 코드임을 판단하기 전 임의의 활성화 코드일 수 있으며, 단말에 입력되었을 때 단말에 의해 SSP 활성화 코드 또는 eSIM 활성화 코드 중 하나로 해석될 수 있다. SSP 활성화 코드에 eSIM 활성화 코드가 포함되어 있는 경우, 단말은 번들 다운로드와 profile 다운로드를 선택적으로 수행할 수 있다.

[0073] 본 개시에서 LBA가 호출하는 함수 (function)는 LBA와 SPB Manager 간의 인터페이스(interface)인 Si2 인터페이스(Si2 interface)와 LBA와 Secondary Platform Bundle Loader와의 인터페이스인 Si3 인터페이스 (Si3 interface)에서 수행되는 함수일 수 있다. LBA는 특정 함수를 통해 SPB Manager나 Secondary Platform Bundle Loader에게 파라미터 (parameter)를 전달할 수 있다. 특정 함수 호출을 통해 LBA에서 전달되는 파라미터들을 해당 함수의 함수 명령어, 함수 커맨드 (function command), 또는 커맨드 (command) 라고 지칭할 수 있다. 함수 커맨드를 받은 SPB Manager나 Secondary Platform Bundle Loader는 함수 커맨드에 따라 특정 동작 (operation)을 수행 후, 함수 커맨드에 대한 응답 (response)을 할 수 있다. 응답(response)은 파라미터들을 포함할 수 있다. Si3 인터페이스 (Si3 interface)에서 전달되는 함수 커맨드(command)와 이에 대한 동작 (operation), 함수 커맨드에 대한 응답 (response)는 여러 개의 함수 커맨드와 이에 대한 동작, 하위 함수 커맨드에 대한 응답으로 구성될 수 있다.

[0074] Si2 인터페이스를 통한 함수 커맨드 전달은 HTTP (Hypertext Transfer Protocol)를 사용할 수 있다. 특히 Si2 인터페이스를 통한 함수 커맨드 전달은 HTTP (Hypertext Transfer Protocol)의 HTTP POST 요청 메시지를 통해 수행될 수 있으며, HTTP POST 요청 메시지의 바디 (body) 부분에 커맨드를 포함시켜 전달될 수 있다.

[0075] 본 개시에서 관리 기관 오브젝트 식별자 (object identifier)는 특정 패밀리 식별자를 관리하는 기관의 오브젝트 식별자를 나타낼 수 있다. 특정 패밀리 식별자에 대해서 관리 기관이 여러 개가 있을 수 있으며, 각각의 기관은 오브젝트 식별자를 가질 수 있다. SSP 단말과 서비스 제공자, 번들 관리 서버는 관리 기관 오브젝트 식별자를 통해서 다운로드를 포함한 번들 관리를 하고자 하는 번들의 관리 주체가 어떤 기관인지 알 수 있다. 또한, 관리 기관 오브젝트 식별자를 통해 해당 번들을 통해서 제공하고자 하는 서비스가 어떤 관리 주체에 의해서 관리되는 서비스인지 파악할 수 있다.

[0076] 본 개시에서 SSP 정보는 제1 SSP 정보와 제2 SSP 정보를 통칭할 수 있다. 제1 SSP 정보는 SSP와 관련된 정보이며 암호화되지 않은 데이타일 수 있다. 제1 SSP 정보는 LBA와 SPB Manager가 특별한 암호 복호화 과정 없이 해석할 수 있다. 제2 SSP 정보는 SSP와 관련된 정보를 암호화한 데이타일 수 있다.

[0077] 본 개시에서 제1 번들 정보는 메타 데이타 (metadata), 번들 메타데이타 (bundle metadata), 세컨더리 플랫폼

번들의 메타데이타 (Secondary Platform Bundle's metadata) 일 수 있다. 제1 번들 정보는 서비스 제공자(service provider) 또는 번들 관리 서버 (SPB Manager)가 SSP 단말에게 다운로드 할 번들에 대해서 SSP 단말의 LBA가 읽을 수 있는 암호화되지 않은 정보를 포함할 수 있다. 제1 번들 정보를 기반으로 SSP 단말의 LBA는 해당 번들의 제2 번들 정보를 받기 전 사용자의 동의를 받거나, 번들 설치 후 운용/관리에 대해서 사용자의 동의, 의도를 요구하는지 여부를 확인할 수 있다. 제1 번들 정보는 번들 설치 전 LBA가 사용자에게 번들의 기본 정보를 보여주는데 사용될 수 있다. 제1 번들 정보는 번들 설치 후 로더(Secondary Platform Bundle Loader, SPBL, Loader)가 관리할 수 있고, 서비스 제공자(Service Provider), 번들 관리 서버(SPB Manager) 등에 의해서 업데이트 될 수 있다.

[0078] 본 개시에서 암호화된 제2 번들 정보는 바운드된 세컨더리 플랫폼 번들 이미지 (bound Secondary Platform Bundle image), 바운드 된 번들 (bound Bundle, bounde Secondary Platform Bundle) 암호화된 세컨더리 플랫폼 번들 이미지 (encrypted Secondary Platform Bundle image), 암호화된 번들 (encrypted Bundle, encrypted Secondary Platform Bundle)일 수 있다. 제2 번들 정보는 제1 번들 정보를 포함할 수 있다. 제 2 번들 정보는 번들 설치에 필요한 정보를 담고 있으며 SSP는 제2 번들 정보로부터 추출한 데이터를 이용하여 번들을 SSP에 설치할 수 있다 제2 번들 정보의 일부는 SSP와 SPB Manager가 생성한 세션 키로 암호화되어 있을 수 있다.

[0079] 본 개시에서 번들 정보 요청 함수는 SSP 단말이 설치하고자 하는 번들의 제1 번들 정보와 제2 번들 정보를 요청하는 함수일 수 있다. 번들의 제1 번들 정보와 제2 번들 정보를 요청하는 동작은 SPB Manager에 번들 정보 요청 함수 커맨드를 전송함으로써 이루어질 수 있다. 번들 정보 요청 함수 커맨드는 SSP 단말이 SPB Manager에게 Si2 인터페이스를 통해서 전달할 수 있다. SSP 단말은 SSP의 인증서, SSP 정보, SSP의 기능(capability)을 포함하는 SSP Credential와 단말 정보를 SPB Manager에 전달하여 제1 번들 정보 또는 제2 번들 정보를 요청할 수 있다. 번들 정보 요청 함수는 커맨드에 포함된 구분자 또는 식별자를 이용하여 구별될 수 있다. 또한, 다른 예에 따라, 번들 정보 요청 함수를 위한 서로 다른 커맨드를 정의함으로써 이를 구별할 수도 있다.

[0080] 그리고, 본 개시를 설명함에 있어서, 관련된 공지기능 또는 구성에 대한 구체적인 설명이 본 개시의 요지를 불필요하게 흐릴 수 있다고 판단된 경우, 그 상세한 설명은 생략한다.

[0081] 특히, 본 개시에서는 다음의 실시 예를 포함한다.

[0082] - SPB Manager가 SSP 번들의 제1 번들 정보를 구성하는 방법

[0083] - SPB Manager가 SSP 단말이 전달한 SSP 정보와 단말 정보를 기반으로 제1 번들 정보를 구성하는 방법

[0084] - SSP 단말이 SPB Manager가 SSP 제1 번들 정보를 구성하는데 사용할 SSP 정보와 단말 정보를 구성하는 방법

[0085] - SSP 단말이 SPB Manager가 SSP 제1 번들 정보를 구성하는데 사용할 SSP 정보와 단말 정보를 패밀리 식별자와 패밀리 식별자를 관리하는 관리 기관의 오브젝트 식별자(object identifier)가 정의한 SSP 정보와 단말 정보를 포함하여 구성하는 방법

[0086] - SSP 단말이 SPB Manager에게 다운로드 받을 번들의 제1 번들 정보를 먼저 요청하는 방법

[0087] - SSP 단말이 SPB Manager에게 제1 번들 정보를 요청하여 전송받은 다음 제2 번들 정보를 요청하는 방법

[0088] - SSP 단말이 SPB Manager에게 제1 번들 정보를 요청하여 전송받은 다음 제2 번들 정보를 요청할 때, SPB Manager가 이전에 제1 번들 정보를 전송한 SSP 단말인지를 확인하는 방법

[0089] - SSP 단말이 SPB Manager에게 제1 번들 정보를 요청하여 전송받은 다음 제2 번들 정보를 요청할 때, SPB Manager가 전달한 challenge값에 대한 서명을 검증함으로써 SPB Manager가 이전에 제1 번들 정보를 전송한 SSP 단말인지를 확인하는 방법

[0090] - SSP 단말이 SPB Manager에게 제1 번들 정보를 요청하여 전송받은 다음 제2 번들 정보를 요청할 때, SSP 단말이 생성한 세션 식별자 (session identifier, transaction identifier)에 대한 서명을 검증함으로써 SPB Manager가 이전에 제1 번들 정보를 전송한 SSP 단말인지를 확인하는 방법

[0091] 이하에서는 SSP 단말의 번들 다운로드 절차 중 제1 번들 정보를 먼저 요청하고 SSP 단말이 메타데이터를 검증한 후 번들을 요청하는 방법과 관련된 다양한 실시 예를 도면을 통해서 구체적으로 설명한다.

[0092] 도 1은 SSP 단말의 내부 구성요소와 구성요소 간 인터페이스를 나타내는 도면이다.

[0093] 도 1에 따르면, SSP 단말(101)은 크게 단말 소프트웨어인 Local bundle Assistant(LBA, 111)와 SSP(131)로 구

성될 수 있다. 또한, SSP 단말(101)은 다른 단말, 기지국, 서버 등과 신호를 송수신하기 위한 송수신부 및 상기 SSP 단말(101)의 전반적인 동작을 제어하는 제어부를 포함할 수 있다. 제어부는 본 개시의 다양한 실시 예에 따른 SSP 단말의 동작을 제어할 수 있다. 상기 제어부는 적어도 하나의 프로세서를 포함할 수 있다. 제어부는 LBA(111)를 통하여 SSP(131)을 제어할 수 있다.

[0094] SSP(131)은 Secondary Platform Bundle(SPB, 번들), Primary Platform(135)과 Primary Platform Interface(134)으로 구성될 수 있다. SPB Loader(로더, 132)와 eSIM Bundle(133)은 번들의 일종이다. LBA(111)와 로더(132)는 제1 인터페이스(122)을 통해서 패킷을 주고받으며, 제1 인터페이스를 통해서 LBA(111)는 다음을 수행할 수 있다. 제1 인터페이스 (122)는 Si3 인터페이스라 불릴 수 있다.

[0095] - 제1 SSP 정보 획득, SSP Credential 획득, 서버 Credential 전송

[0096] - SSP에 설치할 번들 데이터를 로더에 전송

[0097] - SSP에 설치된 번들의 관리 (활성화, 비활성화, 삭제 등)

[0098] 도 2는 본 개시의 일 실시예에 따른, SSP 단말이 번들을 다운로드 하기 위한 단말 내부 및 외부의 구성요소를 설명하기 위한 도면이다.

[0099] 단말(203)은 도 1의 SSP 단말(101)에 대응될 수 있다. LBA(204)는 도 1의 LBA(111)에 대응될 수 있다. SPB Loader(206)은 도 1의 SPB Loader(132) 에 대응될 수 있다. Bundle(207)은 세컨더리 플랫폼 번들(SPB, Secondary Platform Bundle)일 수 있다. 단말(203), LBA(204), SPB loader(206)에 대한 설명은 도 1의 실시예를 참고한다.

[0100] 도 2에 따르면, 사용자(200)는 서비스 가입 과정(210)에서 사용자(200)가 제공하는 서비스(예: 이동통신망을 통한 데이터 서비스 등)를 선택하고 가입할 수 있다. 이때, 사용자(200)는 서비스 제공자(201)가 제공하는 서비스의 이용을 위해 번들을 설치할 단말(203)에 설치된 SSP(205)의 식별자(SSP ID)를 서비스 제공자(201)에게 선택적으로 전달할 수 있다. 일부 실시예에 따르면, 도 2의 서비스 가입 과정(210)에서 사용자(200)는 서비스 가입 후 서비스 제공자(201)로부터 사용자(200)의 단말에 번들을 설치할 수 있는 SSP Activation Code를 QR code 형태로 제공받을 수 있다. 일부 실시 예에 따르면 사용자(200)가 텔레콤 서비스에 가입한 후 제공받는 SSP Activation Code에는 텔레콤 번들을 다운로드 받을 수 있는 정보와 함께 텔레콤 번들 대신 eSIM profile을 다운로드 받을 수 있는 eSIM Activation Code가 같이 포함될 수 있다.

[0101] Bundle제작 요구사항 전달 과정(211)에서 서비스 제공자(201)와 SPB Manager(202)는 번들 다운로드 준비 절차를 수행할 수 있다. Bundle제작 요구사항 전달 과정(211)에서 서비스 제공자(201)는 SPB Manager(202)에 번들이 설치될 SSP(205)의 식별자(SSP ID)를 선택적으로 전달할 수 있으며, 가입자가 선택한 서비스를 제공할 수 있는 특정 번들 식별자(SPB ID), 번들 패밀리 식별자(SPB Family ID) 중 적어도 하나를 SPB Manager(202)에 전달할 수 있다. Bundle제작 요구사항 전달 과정(211)에서 SPB Manager(202)는 전달된 특정 번들 식별자를 가지는 번들 또는 번들 패밀리 식별자를 가지는 번들 중 하나를 선택할 수 있으며, 선택된 번들의 식별자를 서비스 제공자(201)에게 전달 할 수 있다. Bundle제작 요구사항 전달 과정(211)에서 서비스 제공자(201) 또는 SPB Manager(202)는 선택된 번들을 구분할 수 있는 번들 Matching ID를 신규로 생성할 수 있다. 번들을 구분할 수 있는 번들 Matching ID는 CODE_M 이라 불릴 수 있다. 또한 SPB Manager(202)는 전달된 SSP 식별자(SSP ID)와 선택된 번들을 연결하여 관리할 수 도 있다. Bundle제작 요구사항 전달 과정(211)에서 SPB Manager(202)는 선택된 번들을 다운로드 할 수 있는 번들 관리서버 주소 (SPB Manager Address)를 서비스 제공자(201)에 전달할 수 있다. 이 때, 번들 관리서버 주소는 준비된 번들이 저장된 특정 또는 임의의 번들 관리서버의 주소 일 수 있으며, 준비된 번들의 다운로드 정보(서버 주소 등)를 저장하고 획득할 수 있는 다른 번들 관리서버의 주소일 수 있다. Bundle제작 요구사항 전달 과정(211)에서 서비스 제공자(201)가 텔레콤 번들에 대한 준비를 SPB Manager(202)에 요청할 때, 해당 텔레콤 번들과 매칭되는 eSIM profile에 대한 정보를 같이 제공할 수 있다.

[0102] Bundle제작 요구사항 전달 과정(211) 중 일부가 서비스 가입 과정(210)보다 선행되었을 경우, 서비스 가입 과정(210)에서 서비스 제공자(201)는 사용자(200)에게 준비된 번들 다운로드 정보를 전달할 수 있다. 번들 다운로드 정보로는 번들이 준비된 번들 관리서버 주소(SPB Manager Address), 준비된 번들의 번들 Matching ID, 준비된 번들의 번들 패밀리 식별자(family identifier)중 적어도 하나가 선택적으로 전달될 수 있다.

[0103] 도 2를 참조하면, 다운로드할 번들 정보 입력 과정(231) 에서 단말(203)의 LBA(204)로 번들 다운로드 정보가 전달될 수 있다. 번들 다운로드 정보는 LBA(204)가 접속할 번들 관리서버의 주소(SPB Manager Address), 상기 Bundle제작 요구사항 전달 과정(211)에서 준비된 번들의 번들 구분자, 준비된 번들의 번들 패밀리 식별자 중 적

어도 하나를 포함할 수 있다. 번들 구분자는 Bundle제작 요구사항 전달 과정(211)에서 생성된 번들 Matching ID, 또는 번들 Event ID 중 적어도 하나를 포함할 수 있다. 또한, 번들 구분자는 준비된 번들의 번들 패밀리 식별자를 포함할 수 있다. 번들 Event ID는 Bundle제작 요구사항 전달 과정(211)에서 준비된 번들의 번들 Matching ID와 번들 관리서버의 주소 중 적어도 하나를 포함할 수 있다. 사용자(200)는 번들 다운로드 정보를 LBA(204)로 SSP Activation Code를 입력(예: QR코드 스캐닝, 직접 문자 입력 등)하여, 번들 다운로드 정보를 LBA(204)에 입력할 수 있다. 또한, 번들 다운로드 정보는 정보 제공서버(도시되지 않음)를 통해 푸쉬입력을 이용하여 LBA(204)에 입력될 수 있다. 또한, 미리 단말(203)에 설정된 정보 제공서버(도시되지 않음)로 LBA(204)가 접속하여 번들 다운로드 정보를 수신할 수 있다.

[0104] SPB Manager(202)에서 SSP(205)로의 번들 다운로드는 SPB Manager(202)와 LBA(204) 사이의 인터페이스(221)와 LBA(204)와 SPB Loader(206) 사이의 인터페이스(222)에서 이루어지는 함수와 동작으로 구현될 수 있다. 상기 LBA(204)와 SPB Loader(206) 사이의 인터페이스(222)는 도 1의 제1 인터페이스(122) 에 대응될 수 있다. 상기 LBA(204)와 SPB Loader(206) 사이의 인터페이스(222)는 Si3 인터페이스라 불릴 수 있다.

[0105] 도 3은 SPB Manager가 LBA에 전달하는 제1 번들 정보의 구조를 도시한 도면이다.

[0106] 제1 번들 정보 객체(301)는 제1 번들 정보 기본 필드(310), 패밀리-특수 메타데이타(320), 관리 기관-특수 메타데이타(331, 332)를 포함할 수 있다. 제1 번들 정보 객체(301)는 복수 개의 관리 기관-특수 메타데이타를 포함할 수 있다.

[0107] 제1 번들 정보 기본 필드(310)는 번들 식별자 (311), 번들 패밀리 식별자(312), 관리 기관 오브젝트 식별자(313)를 포함할 수 있다. 번들 식별자(311)는 제1 번들 정보에 상응하는 세컨더리 플랫폼 번들 (Secondary Platform Bundle)의 식별자 (identifier)일 수 있다. 번들 패밀리 식별자(312)는 제1 번들 정보에 상응하는 세컨더리 플랫폼 번들이 속하는 패밀리 식별자일 수 있다. 관리 기관 오브젝트 식별자(313)는 제1 번들 정보에 상응하는 세컨더리 플랫폼 번들의 패밀리 식별자를 관리하는 기관의 오브젝트 식별자 (object identifier)일 수 있다. 제1 번들 정보 기본 필드(310)는 복수 개의 관리 기관 오브젝트 식별자(313)를 포함할 수 있다. 제1 번들 정보 기본 필드(310)가 복수 개의 관리 기관 오브젝트 식별자(313)를 포함하는 경우, 선호도에 따라서 복수 개의 관리 기관 오브젝트 식별자(313)가 나열되거나 복수 개의 관리 기관 오브젝트 식별자(313) 중 가장 선호하는 관리 기관 오브젝트 식별자가 지정될 수 있다. 제1 번들 정보 기본 필드(310)는 SSP 단말의 SPB Loader(로더)(206)가 번들 설치 절차에 사용한 로더의 인증서와 SPB Manager의 인증서가 올바르게 사용되었는지를 검증하는 용도로 사용할 수 있다.

[0108] 도 3의 패밀리-특수 메타데이타(320)는 번들 패밀리 식별자(312)를 포함할 수 있다. 패밀리-특수 메타데이타(320)는 해당 패밀리 식별자를 가지는 번들에 대해 공통적으로 적용할 수 있는 설정, 파라미터, 기능을 포함할 수 있다.

[0109] 도 3의 관리 기관-특수 메타데이타(331, 332)는 관리 기관 오브젝트 식별자를 포함할 수 있다. 관리 기관-특수 메타데이타에 포함되는 관리 기관 오브젝트 식별자는 제1 번들 정보 기본 필드(310)에 포함되는 관리 기관 오브젝트 식별자(313)와 다른 값을 가질 수 있다. 예를 들어, 제1 번들 정보(301)에서 관리 기관 오브젝트 식별자(313)가 제1 관리 기관일때, 제1 번들 정보(301)은 제1 관리 기관과 동일한 패밀리 식별자를 관리하는 제2 관리 기관이 정의한 관리 기관-특수 메타데이타 포함할 수 있다. 제1 번들 정보(301)는 관리 기관-특수 메타데이타를 포함하지 않을 수도 있다.

[0110] 도 3의 제1 번들 정보 예제(301a)는 제1 번들 정보 객체(301)의 구조를 따르는 일부 실시 예이다. 제1 번들 정보 예제(301a)의 제1 번들 정보 기본 필드(310a)는 '1234-5678-aa'의 값을 가지는 번들 식별자 (311a), 텔레콤 패밀리의 패밀리 식별자 값을 가지는 번들 패밀리 식별자(312a), 기관1의 오브젝트 식별자를 가지는 관리 기관 오브젝트 식별자(313a)를 포함할 수 있다.

[0111] 제1 번들 정보 예제(301a)는 패밀리-특수 메타데이타(320a)를 포함할 수 있으며, 패밀리-특수 메타데이타(320a)는 번들 패밀리 식별자 (312a)와 같은 값을 포함할 수 있다. 패밀리-특수 메타데이타(320a)는 번들 패밀리 식별자 (312a)를 가지는 번들에 공통적으로 적용할 수 있는 설정, 파라미터, 기능을 포함할 수 있다. 특히, 제1 번들 정보 예제 (301a)의 번들 패밀리 식별자 (312a)는 텔레콤 패밀리의 패밀리 식별자이므로, 패밀리-특수 메타데이타(320a)는 텔레콤 패밀리의 패밀리 식별자를 포함하며, 텔레콤 패밀리 번들에 공통적으로 적용할 수 있는 설정, 파라미터, 기능을 포함할 수 있다.

[0112] 제1 번들 정보 예제(301a)는 번들 패밀리 식별자(310a)를 관리하는 기관(들) 각각이 정의하는 관리 기관-특수

메타데이타 (331a, 332a)를 포함할 수 있다. 관리 기관-특수 메타데이타(331a, 332a)는 관리 기관의 오브젝트 식별자와 기관이 정의하는 설정, 파라미터, 기능을 포함할 수 있다. 패밀리-특수 메타데이타(320a)는 제1 번들 정보 기본 필드(310a)의 번들 패밀리 식별자(312a)에 대해서 정의되어야 한다. 관리-기관 특수 메타데이타(331a, 332a)는 번들 패밀리 식별자(312a)에 대해서 정의되어야 하지만 반드시 제1 번들 정보 기본 필드(310a)에 포함된 관리 기관 오브젝트 식별자 (313a)를 포함할 필요는 없다.

[0113] 일부 실시 예에 따라 제1 번들 정보는 제1 번들 정보 객체2(302)와 같이 복수 개의 패밀리-특수 메타데이타(320, 321)를 포함할 수 있다. 제1 번들 정보 객체(302)는 도면에 표시되어 있지는 않지만 복수 개의 관리 기관-특수 메타데이타(332)를 포함할 수 도 있다. 제1 번들 정보 예제2(302a)는 복수 개의 패밀리-특수 메타데이타를 포함하는 제1 번들 정보의 예제이다. 제1 번들 정보 예제2(302a)는 제1 번들 정보 예제(302)와 동일하게 패밀리 식별자(312a)는 텔레콤 패밀리의 패밀리 식별자이며, 관리 기관의 오브젝트 식별자(313a)는 기관1의 오브젝트 식별자를 가진다. 제1 번들 정보 예제2(302a)는 두 개의 패밀리-특수 메타데이타(320a, 321a)를 포함하여 패밀리-특수 메타데이타1(320a)은 제1 번들 정보 예제2(302a)의 제1 번들 정보 기본 필드(310a)의 번들 패밀리 식별자(312a)를 포함할 수 있다. 또한, 패밀리-특수 메타데이타1(320a)은 번들 패밀리 식별자(312a)에 적용되는 데이터를 포함할 수 있다. 패밀리-특수 메타데이타2(321a)는 번들 패밀리 식별자(312a)와 다른 패밀리 식별자를 포함할 수 있다. 패밀리-특수 메타데이타2(321a)는 번들 패밀리 식별자(312a)와 다른 값을 포함할 수 있으며, 다른 패밀리 식별자를 위한 데이터를 포함할 수 있다. 패밀리-특수 메타데이타2(321a)는 제1 번들 정보 예제2(302a)의 번들 패밀리 식별자(312a)를 위한 데이터는 아니지만, SSP 단말과 SSP가 필요에 따라서 사용할 수도 있다.

[0114] 도 4a는 본 개시의 일 실시예에 따른, SSP 단말이 SPB Manager에 제1 번들 정보와 제2 번들 정보를 요청하는 방법을 설명하기 위한 흐름도이다.

[0115] 단계 410에서 SSP 단말(400)의 LBA(402)는 SSP 내의 로더(SPB Loader, 401)에게 SSP에의 번들 설치를 위해서 SSP정보 요청을 하는 함수를 보낸다. SSP 정보 요청 함수 command는 설치하고자 하는 번들의 패밀리 식별자를 포함할 수 있다. SSP 정보 요청 함수 command는 또한, 설치하고자 하는 번들의 패밀리 식별자를 관리하는 기관의 Object Identifier를 포함할 수 있다.

[0116] 단계 411에서, 로더(401)는 SSP 정보 요청 함수 command를 수신하면 제1 SSP 정보를 생성하여 LBA(402)에게 전달할 수 있다. 제1 SSP 정보에는 로더(401)와 SPB Manager(403)가 사용해야 할 인증서 CI 정보 리스트, bundle 다운로드 절차에 사용될 암호 알고리즘의 identifier 리스트, 세션 키 형성을 위한 키 교환 알고리즘의 식별자(identifier) 리스트가 포함될 수 있다. 제1 SSP 정보는 특정 패밀리 식별자와 특정 패밀리 식별자를 관리하는 특정 관리 기관의 관리 기관 오브젝트 식별자(Object Identifier)를 가지는 bundle을 다운로드하기 위해서 로더와 SPB Manager(403) 가 사용해야 할 인증서의 CI 정보 리스트, 암호 알고리즘의 identifier 리스트, 키 교환 알고리즘의 identifier 리스트가 포함될 수 있다. 제1 SSP 정보에는 SSP 버전의 정보가 포함될 수 있다.

[0117] 또한, 도 4a에서 단계 410과 단계 411 간에, 로더(401)는 LBA(402)에 단계 410가 완료되었음을 알릴 수 있으며, LBA(402)는 로더(401)에 단계 411의 수행을 요청하는 커맨드를 전달할 수 있다.

[0118] 단계 412에서 LBA(402)는 번들 다운로드를 요청할 SPB Manager(403) 와 Transport Layer Security(TLS) 세션을 형성할 수 있다.

[0119] 단계 413에서 LBA(402)는 SPB Manager(403)에게 SPBM 인증서 요청 함수를 호출한다. 함수 호출 시, LBA(402)는 단계411에서 로더(401)로부터 받은 제1 SSP 정보와 제1 단말 정보를 SPBM 인증서 요청 함수 command에 포함하여 SPB Manager(403)에게 전달할 수 있다. 단말 정보는 LBA (402)의 버전, 패밀리 식별자 별로 정의된 단말 정보, 특정 패밀리 식별자를 관리하는 기관 별로 정의된 단말 정보를 포함하여 하나를 포함하도록 구성될 수 있다.

[0120] 단계 413에서 SPBM 인증서 요청 함수를 호출받은 SPB Manager(403)는 다음의 동작 중 적어도 하나를 수행할 수 있다.

[0121] - Eligibility check 수행: LBA와 SPBL의 버전을 확인하여 SPB Manager가 지원 가능한 SSP 단말인지 확인할 수 있다.

[0122] - 번들의 패밀리 식별자를 선택할 수 있다.

[0123] - 번들의 패밀리 식별자를 관리하는 관리 기관의 오브젝트 식별자 (Object Identifier)를 선택할 수 있다.

[0124] - SPBM 키 생성 인증서(CERT.SPBM.KA)와 이를 검증할 인증서 체인을 선택할 수 있다.

[0125] - SSP가 사용해야할 인증서의 CI 정보를 선택할 수 있다.

[0126] - SSP가 데이터 암호를 위해 사용해야 할 암호 알고리즘의 정보를 선택할 수 있다.

[0127] 단계 414에서 SPB Manager(403)는 SPBM 키 형성 인증서와 인증서 체인, SSP가 사용해야 할 인증서의 CI 정보, SSP가 사용해야 할 암호화 알고리즘 정보, 번들의 패밀리 식별자 중 적어도 하나를 포함하여 응답할 수 있다. SPB Manager(403)는 또한 패밀리 식별자를 관리하는 기관의 Object identifier를 포함하여 응답할 수도 있다.

[0128] 단계 415에 따라 SPB Manager(403)의 응답을 받은 LBA(402)는 로더(401)에 SSP Credential 요청 함수를 호출할 수 있다. LBA(402)는 SSP Credential 요청 함수 호출 시, 함수 command에 서버 Credential을 포함하여 전달할 수 있다.서버 Credential은 다음 중 적어도 하나를 포함할 수 있다.

[0129] - 번들 코드매칭 정보 (Matching ID, CODE_M)

[0130] - 번들 패밀리 식별자

[0131] - SPBM 키 생성 인증서(CERT.SPBM.KA)와 이를 검증할 인증서 체인

[0132] - SSP가 사용해야 할 서명용 인증서의 CI 정보

[0133] - SSP가 사용해야 할 암호 알고리즘 정보

[0134] 또한, 전술한 정보들 이외에도 서버 Credential은 번들 코드매칭 보조 정보 (challenge_S)를 선택적으로 포함할 수 있다.

[0135] SSP Credential 요청 함수 command를 수신한 로더(401)는 수신한 서버 Credential을 기반으로 SSP Credential을 생성할 수 있다. SSP Credential 생성 동작은 다음을 포함할 수 있다.

[0136] - SPBM 키 생성 인증서(CERT.SPBM.KA)의 검증

[0137] - SSP가 사용해야할 인증서의 CI 정보에 따른 SPBL 서명용 인증서 선택

[0138] - SPBL ephemeral key pair 생성

[0139] - session ID로 사용될 수 있는 ID_TRANSAC 생성

[0140] - SPBM 키 생성 인증서에 포함되어 있는 공개키와 SPBL ephemeral key의 비밀키 (eSK.SPBL.KA)로 제1 세션 키 (session key 1) 생성

[0141] - SPBL ephemeral key를 포함하는 sspImageSessionToken 생성 및 sspImageSessionToken을 SPBL 서명용 인증서 (CERT.SPBL.DS)에 대응하는 비밀키 (SK.SPBL.DS)로 서명한 sspImageSessionTokenSignature 생성

[0142] - 제2 SSP 정보 생성. 제2 SSP 정보는 Primary Platform 식별자 (Primary Platform Identifier)를 포함할 수 있다. 제2 SSP 정보는 다운로드 받을 패밀리 식별자를 위해 정의된 SSP 정보와 패밀리 식별자를 관리하는 기관별 정의된 SSP 정보를 포함할 수 있다. 제2 SSP 정보는 다운로드 받고자 하는 번들의 패밀리 식별자에 대하여 해당 패밀리 식별자를 통한 bundle 또는 service를 관리하는 기관 또는 패밀리 식별자를 관리하는 관리 기관 (organization, custodian) 들이 각자 정의한 관리 기관-특수 SSP 정보 (Organization-specific SSP information)를 포함할 수 있다. 제2 SSP 정보는 복수개의 관리 기관-특수 SSP 정보를 포함할 수 있다. 제2 SSP 정보는 다운로드 받고자 하는 번들의 패밀리 식별자에 대해서 관리 기관들이 공통적으로 사용 가능한 패밀리-특수 SSP 정보 (family-specific SSP information)을 포함할 수 있다. 패밀리-특수 SSP 정보 (family-specific SSP information)는 하나의 패밀리 식별자를 포함할 수 있으며, 해당 패밀리 식별자에 대해서 단말에 탑재된 SSP가 지원하고 있는 관리 기관들의 리스트를 포함할 수 있다. SSP가 지원하고 있는 관리 기관들의 리스트는 해당 패밀리 식별자에 대해서 SSP가 지원하는 관리 기관들의 오브젝트 식별자 (object identifier)의 리스트일 수 있다. SSP가 어떤 관리 기관을 지원한다라는 말은 해당 관리 기관이 정의하는 SSP 설정값, 파라미터, 번들의 운용/관리 등에 대해서 SSP가 그 의미를 해석할 수 있고 지원 가능 여부를 판단할 수 있음을 의미할 수 있다.

[0143] - 번들 코드매칭 정보(Matching ID, CODE_M), 번들 코드매칭 보조 정보 (challenge_S), 상기 생성된 제2 SSP 정보를 포함하는 sspToken 생성 및 sspToken에 대해서 SPBL 서명용 인증서(CERT.SPBL.DS)에 대응하는 비밀키 (private key)로 서명한 sspTokenSignature 생성

[0144] - 상기 생성된 제1 세션 키로 SPBL 서명용 인증서(CERT.SPBL.DS)와 SspToken, SspTokenSignature를 암호화하여 제1 암호화 정보(M-SSP)와 제1 무결성 검증(integrity check) 정보(H-SSP) 생성 상기 생성된 SspToken과 SspTokenSignature는 SPBL 서명용 인증서와 별도로 암호화 되어 제2 암호화된 정보(M-SSP2)와 제2 무결성 검증(integrity check) 정보(M-SSP2)를 생성할 수 있다.

[0145] - SPBL 서명용 인증서를 SPB Manager가 검증하기 위해 사용할 인증서 체인, 상기 생성된 sspImageSeesionToken, 상기 생성된 sspImageSessionTokenSignature, 상기 생성된 sspToken, 상기 생성된 sspTokenSignature, 상기 생성된 제1 암호화 정보 (M-SSP), 상기 생성된 제1 무결성 검증 정보 (H-SSP)를 포함하는 SSP 크리덴셜 (Credential) 생성. SSP 크리덴셜은 상기 생성된 제2 암호화 정보(M-SSP2)와 제2 무결성 검증 정보(H-SSP2)를 포함할 수도 있다.

[0146] 단계 416에서 로더(401)는 SSP Credential 요청 함수에 대한 응답으로 LBA(402)에게 생성한 SSP Credential을 전송할 수 있다. 만일, SSP Credential의 생성 과정 중 어떤 동작에서 에러가 발생한 경우에는 에러 메시지로 응답하고 절차를 종료할 수 있다.

[0147] 또한, 도 4a에서 단계 415과 단계 416 간에, 로더(401)는 LBA(402)에 단계 415가 완료되었음을 알릴 수 있으며, LBA(402)는 로더(401)에 단계 416의 수행을 요청하는 커맨드를 전달할 수 있다.

[0148] 단계 418에서, LBA(402)는 로더(401)로부터 SSP Credential을 전달받음에 따라, SPB Manager(403)에 번들 정보 요청 함수를 호출할 수 있다. LBA(402)가 번들 정보 요청 함수를 호출 시, SPB Manager(403)에 다음을 포함하는 번들 정보 요청 함수 커맨드를 전달할 수 있다.

[0149] - 상기 로더(401)로부터 전달 받은 SSP Credential

[0150] - 단말 정보. 단말 정보는 LBA의 버전, 패밀리 식별자에 대해서 정의된 패밀리-특수 단말 정보, 특정 패밀리 식별자를 관리하는 기관이 정의한 관리 기관-특수 단말 정보를 포함할 수 있다. 패밀리 특수-단말 정보는 패밀리 식별자를 포함할 수 있으며, 포함된 패밀리 식별자에 대한 단말 정보임을 나타낼 수 있다. 패밀리 특수-단말 정보는 해당되는 패밀리 식별자와 관련된 정보, 파라미터, 설정값, 기능을 포함할 수 있다. 패밀리 특수-단말 정보는 SSP 단말이 지원하는 관리 기관들의 리스트를 포함할 수 있다. SSP 단말이 지원하는 관리 기관들의 리스트는 해당 패밀리 식별자에 대해서 SSP 단말이 지원하는 관리 기관들의 오브젝트 식별자 (object identifier)의 리스트일 수 있다. SSP 단말이 어떤 관리 기관을 지원하고 있다라는 말은 해당 관리 기관이 정의하는 단말 정보, 단말 설정값, 파라미터, 단말 기능에 대해서 SSP 단말이 그 의미를 해석할 수 있고 지원 가능 여부를 판단할 수 있음을 의미할 수 있다.

[0151] - SSP 단말이 SPB Manager (403)에게 요청하는 정보를 나타내는 requestType.

[0152] requestType은 SSP에 제2 번들 정보를 요청하는 Type-A, 제1 번들 정보만 요청하는 Type-B, 제1 번들 정보 요청 후 제2 번들 정보를 요청하는 Type-C 을 포함하는 여러 Type중 하나로 표현될 수 있다. requestType을 사용하여 상기 언급된 동작 외에 다른 동작을 정의하여 Type-D. Type-E 등을 사용하여 동작을 확장할 수 있다. requestType을 통해 Type을 구분하는 방법으로써, 가장 기본이 되는 동작의 Type을 의미하기 위해 requestType을 보내지 않는 경우도 가능하다. 예를 들어 Type-A의 동작이 기본 동작인 경우, SPB Manager(403)는 번들 정보 요청 함수 command에 requestType이 없는 경우는 Type-A로 인지하고, requestType이 있는 경우는 해당 값에 따라서 다른 동작을 수행할 수도 있다. 또한, request Type과 관련된 정보를 번들 정보 요청 함수 커맨드 내에 포함하지 않고, 특정 Type에 대응되는 특수한 번들 정보 요청 함수 커맨드를 정의하여 Type을 구분할 수 있다.

[0153] LBA(402)가 번들 정보 요청 함수를 호출 시, 번들 정보 요청 함수 command의 requestType이 Type-A (제2 번들 정보를 요청하는 type) 또는 Type-B (제1 번들 정보 만 요청하는 type) 을 포함하는 type 중 하나를 가지는 경우는 단계 418에 대응될 수 있다. 또한, request Type에 관한 정보를 포함하지는 않지만 Type-A와 Type-B에 대응하는 특수한 번들 정보 요청 command를 보내는 경우도 단계 418에 대응될 수 있다. 도 4a의 단계 418은 requestType이 Type-B (제1 번들 정보만 요청하는 type) 인 경우를 도시한다.

[0154] 단계 419에서 SPB Manager(403)는 LBA(402)로부터 SSP Credential, 단말 정보, Type-A 또는 Type-B를 가지는 requestType을 전달받음에 따라, 전달 받은 SSP Credential과 단말 정보를 기반으로 다음과 같은 동작 중 적어도 하나를 수행할 수 있다. 또한, 단계 419에서 requestType을 포함하지는 않지만 Type-A 또는 Type-B에 해당하는 특수한 번들 요청 함수 command를 수신하는 경우 또한 다음과 같은 동작 중 적어도 하나를 수행할 수 있다.

[0155] - requestType이 Type-A 또는 Type-B 인지 확인, 또는 번들 요청 함수 command가 Type-A 또는 Type-B에 대응

하는 것인지 확인

[0156] - 제2 SSP 정보를 기반으로 SPB Manager(403)가 보유 중인 번들이 SSP 단말(400)과 호환되는지 여부 판단

[0157] - SPBL ephemeral key의 공개키 (ePK.SPBL.KA)와 SPBM 키 생성 인증서의 공개키(public key)인 ePK.SPBM.KA와 쌍을 이루는 개인키(private kye)인 eSK.SPBM.KA를 이용하여 제 1 세션 키 (session key 1) 생성

[0158] - 제 1 세션 키를 사용하여 M-SSP 복호화.

[0159] - M-SSP를 복호화 하여 얻은 SPBL 서명용 인증서와 SSP credential 내의 SPBL 인증서 체인을 검증. 인증서 검증은 단계 413에서 전송한 SSP가 사용해야할 인증서의 CI 정보를 활용하여 검증할 수 있다.

[0160] - M-SSP를 복호화 하여 얻은 sspToken과 이것의 서명인 sspToken을 SPBL 인증서로 검증

[0161] - sspImageSessionToken과 이것의 서명인 sspImageSessionTokenSignature를 SPBL 인증서로 검증

[0162] - sspImageSessionToken 내의 ID_TRANSAC 값을 보관

[0163] - 상기 sspToken에 존재하는 CODE_M에 해당하는 번들을 보유중인 지 판단

[0164] - 상기 sspToken에 존재하는 CODE_M에 해당하는 번들이 SSP 단말에 설치 가능한 지 판단. 해당 판단은 제2 SSP 정보에 포함된 Primary Platform Identifier, 다운로드 받을 패밀리 식별자를 위해 정의된 패밀리-특수 SSP 정보와 패밀리 식별자를 관리하는 기관 별 정의된 관리 기관-특수 SSP 정보를 기반으로 수행될 수 있다.

[0165] - 상기 CODE_M에 해당하는 번들의 제1 번들 정보를 생성 또는 이미 준비된 제1 번들 정보를 준비할 수 있다.

[0166] 번들의 제1 번들 정보를 생성하는 과정은 다음 과정을 포함할 수 있다.

[0167] - 번들 식별자(도 3의 311)를 설정

[0168] - 번들 패밀리 식별자(도 3의 312)를 설정. 설정되는 패밀리 식별자는 단계 414에서 SPB Manager(403)가 응답에 포함한 패밀리 식별자와 같을 수 있다.

[0169] - 관리 기관 오브젝트 식별자(310)를 설정. 설정되는 관리 기관 오브젝트 식별자는 단계 414에서 SPB Manager(403)가 응답에 선택적으로 포함한 관리 기관 오브젝트 식별자를 포함할 수 있다..

[0170] - 패밀리-특수 메타데이타(도 3의 320)를 제1 번들 정보에 포함시킴. 패밀리-특수 메타데이타는 상기 설정한 번들 패밀리 식별자를 포함할 수 있다. 패밀리-특수 메타데이타는 상기 설정한 번들 패밀리 식별자에 대해서 정의된 설정값, 파라미터, 번들의 운용/관리와 관련된 정보들을 포함할 수 있다.

[0171] - 관리 기관-특수 메타데이타(도 3의 331)을 제1 번들 정보에 포함시킴. 제1 번들 정보는 복수 개의 관리 기관-특수 메타데이타를 포함할 수도 있다. SPB Manager(403)는 제2 SSP 정보에 포함된 패밀리-특수 SSP 정보와 관리 기관-특수 SSP 정보를 기반으로 관리 기관-특수 메타데이타를 제 1 번들 정보에 포함시킬 수 있다. 예를 들어, SPB Manager(403)는 SSP 단말이 전달한 패밀리-특수 SSP 정보에 포함된 SSP가 지원하는 관리 기관의 리스트에 포함된 관리 기관이 정의한 관리 기관-특수 메타데이타를 제 1 번들 정보에 포함시킬 수 있다. SPB Manager(403)는 SSP 단말이 지원하지 않는 관리 기관이 정의한 관리 기관-특수 메타데이타를 제 1 번들 정보에 포함시킬 수도 있다.

[0172] 단계 419에서, 제1 번들 정보 생성 후 SPB Manager(403)는 제1 번들 정보를 생성했음을 기록하여 관리할 수 있다. SPB Manager(403)는 생성한 제1 번들 정보를 LBA(402)가 전달한 SSP Credential의 전체 또는 일부 정보와 연계하여 관리할 수 있다. 일부 실시 예에 따르면, SPB Manager(403)는 SSP Credential 전체 또는 SSP Credential의 일부 요소, 예를 들면 Transaction Id와 생성한 제1 번들 정보를 연계하여 관리할 수 있다. SPB Manager(403)가 수행하는 해당 기록과 관리는 향후 동일한 단말로부터 제2 번들 정보를 요청하는 번들 정보 요청 함수 command를 수신하였을 때, 단계 429에서 수행하는 동작 중 일부일 수 있는 제1 번들 정보 요청 여부 확인 동작에 번들 정보 요청 함수 command의 SSP credential을 매개로 확인하는 방법에 활용될 수 있다.

[0173] 단계 421에서, SPB Manager(403)는 단계 418의 번들 정보 요청 함수에 대해 제1 번들 정보를 포함하여 응답할 수 있다. 단계 418에서 Type-A에 해당하는 번들 정보 요청함수 command를 수신한 경우 단계 421은 생략될 수 있다.

[0174] 단계 425에서, 제1 번들 정보를 수신한 LBA(402)는 제1 번들 정보 검증 동작을 수행할 수 있다. 제1 번들 정보 검증 동작은 다음 과정을 포함할 수 있다.

[0175] LBA(402)는 수신한 제1 번들 정보에 포함된 패밀리 식별자(도 3의 311)가 유효한 값인지 검증할 수 있다. 패밀리 식별자를 검증하는 방법은, 도 2의 번들 정보 입력 과정(231)에서 LBA가 입력받은 정보를 기반으로 번들 다운로드를 수행하였을 때, LBA가 입력받은 정보에 번들 패밀리 식별자가 있는 경우, 제 1 번들 정보에 포함된 패밀리 식별자와 입력받은 정보에 포함된 패밀리 식별자가 동일한지를 확인하는 절차를 포함할 수 있다. 또한, 패밀리 식별자를 검증하는 방법은 전술한 단계 414에서 SPBM 인증서 요청 함수 커맨드에 대한 응답에 포함된 패밀리 식별자와 제1 번들 정보에 포함된 패밀리 식별자가 동일한지 확인하는 절차를 포함할 수 있다.

[0176] LBA(402)는 수신한 제1 번들 정보에 포함된 관리 기관 오브젝트 식별자(도 3의 313)가 유효한 값인지 검증할 수 있다. 관리 기관 오브젝트 식별자의 유효성을 검증하는 방법은 도 2의 번들 정보 입력 과정(231)에서 LBA가 입력받은 정보를 기반으로 번들 다운로드가 수행되었을 때, LBA가 입력받은 정보에 관리 기관 오브젝트 식별자가 있는 경우, 수신한 제1 번들 정보의 관리 기관 오브젝트 식별자와 값이 같은지 확인하는 절차를 포함할 수 있다. 또한, 관리 기관 오브젝트 식별자의 유효성을 검증하는 방법은, 전술한 단계 414에서 SPBM 인증서 요청 함수 커맨드에 대한 응답에 포함된 관리 기관 오브젝트 식별자와 제1 번들 정보에 포함된 관리 기관 오브젝트 식별자가 동일한지 확인하는 절차를 포함할 수 있다.

[0177] LBA(402)는 수신한 제1 번들 정보에 포함된 패밀리-특수 메타데이타에 포함된 단말 설정, 파라미터, 기능을 확인할 수 있다.

[0178] 단계 428에서, LBA(402)는 번들 정보 요청 함수 command의 requestType이 Type-C (제1 번들 정보 요청 후 제2 번들 정보를 요청하는 type) 인 번들 정보 함수 command를 SPB Manager(403)에 전달할 수 있다. 또한, 단계 428에서 LBA(402)는 requestType을 포함하지는 않지만 Type-C에 대응하는 특수한 번들 요청 함수 command를 SPB Manager(403)에 전달할 수 있다.

[0179] requestType이 Type-C (제1 번들 정보 요청 후 제2 번들 정보를 요청하는 type)인 번들 정보 요청 함수 command를 수신하거나 Type-C에 대응하는 특수한 번들 요청 함수 command를 수신한 SPB Manager(403)는 단계 429를 수행할 수 있다. 단계 429에서, SPB Manager(403)는 제1 번들 정보 요청 여부 확인 과정과 제2 번들 정보 생성 동작을 수행할 수 있다.

[0180] 일부 실시 예에 따라 제1 번들 정보 요청 여부 확인 과정은, 후술할 도 5의 단계 529, 도 6의 단계 629, 도 7의 단계 729, 도 8의 단계 829, 도 9의 단계 929에 서술된 제1 번들 정보 요청 여부 확인 절차일 수 있다.

[0181] 제2 번들 정보 생성 동작은 다음과 같은 동작 중 적어도 하나로 구성될 수 있다.

[0182] - TIME_STAMP를 생성하고 제 1 세션키로 암호화

[0183] - SPBM ephemeral key pair (ePK.SPBM.KA, eSK.SPBM.KA) 생성

[0184] - 상기 SPBM ephemeral private key (eSK.SPBM.KA)와 상기 SSP Credential에서 추출한 ePK.SPBL.KA를 이용하여 제2 세션키 생성

[0185] - 서명용 SPBM 인증서 선택과 인증서 체인 준비

[0186] - SPBM ephemeral public key (ePK.SPBM.KA)와 SSP Credential에 있는 ID_TRANSAC값을 포함한 SPBM token을 생성

[0187] - SPBM token을 서명용 SPBM 인증서에 대응하는 private key로 서명한 SPBM token signature 생성

[0188] - 제2세션키로 Image descriptor, ARP token, Segment Descriptor Structure 등을 암호화

[0189] - 단말에게 전달할 제2 번들 정보를 생성. 제2 번들 정보는 상기 제2 세션키로 암호화된 데이터와 SPBM Token, SPBM Token signature, bundle segment가 포함된 제2 번들 정보를 포함할 수 있다.

[0190] 단계 430에서, SPB Manager(403)는 단계 428의 requestType이 Type-C인 번들 정보 요청 함수 command 또는 Type-C에 대응하는 특수한 번들 정보 요청 함수 command에 대한 응답으로 제2 번들 정보 (bound SPB image)를 LBA(402)에 전달할 수 있다.

[0191] 위 실시 예의 단계 418에서 LBA(402)는 번들 정보 요청 함수 command의 requestType가 Type-A (제2 번들 정보를 요청하는 type)인 번들 정보 요청 함수 또는 Type-A에 대응하는 특수한 번들 요청 함수 command를 호출할 수 있다. 단계 418에서 번들 정보 요청 함수 command의 requestType이 Type-A인 번들 정보 요청 command 또는 Type-A에 대응하는 특수한 번들 요청 함수 command를 수신한 SPB Manager(403)는 다음과 같은 동작을 수행할 수

있다.

[0192] - 단계 419를 수행한다.

[0193] - 단계 429에서 제1 번들 정보 요청 여부 확인 과정은 생략하고, 제2 번들 정보 생성 동작을 수행한다.

[0194] - 단계 430에 따라 SBP Mananger(430)는 제2 번들 정보를 LBA(402)에 전달하여 LBA(402)의 번들 정보 요청 함수 command의 requestType이 Type-A인 번들 정보 요청 함수 command 또는 Type-A에 대응하는 번들 정보 요청 함수 command에 대해 응답할 수 있다.

[0195] 도 4b는 본 개시의 일부 실시 예에 따른, SSP 단말이 SPB Manager에 제1 번들 정보를 별도 요청하지 않고 제2 번들 정보를 요청하는 방법을 설명하기 위한 흐름도이다.

[0196] 도 4b는 도 4의 일부 실시 예일 수 있다. 구체적으로 도 4b는 단계 418에서 SPB Mananger(402)가 Type-A (제2 번들 정보를 요청하는 type) 인 번들 정보 요청 command 또는 Type-A에 대응하는 특수한 번들 정보 요청 함수 command를 수신한 경우, SPB Manager가 제2 번들 정보를 생성하여 LBA(402)에 응답하는 실시 예에 대한 흐름도이다.

[0197] 도 4b에서 단계 410부터 단계 417까지는 도 4a의 단계 410부터 단계 417에 대응될 수 있다. 도 4b에서 단계 418b는 도 4a의 단계 418에서 LBA(402)가 번들 정보 요청 함수를 호출 시, 번들 정보 요청 함수 command에 제2 번들 정보를 요청하는 Type-A를 지칭하는 requestType가 포함되거나, Type-A를 포함하는 제2 번들 정보 요청에 대응되는 특수한 함수 command가 전송되는 일부 실시 예이다. 단계 418b에 따라 Type-A에 상응하는 제2 번들 정보 요청 함수 command를 수신한 SPB Manager(403)는 단계 419를 수행할 수 있다. 상기 단계 419은 도 4a의 단계 419와 대응될 수 있다. 단계 419를 수행 후 SPB Manager(403)는 단계 429b를 수행할 수 있다. 단계 429b는 도 4a의 단계 429의 제2 번들 정보 생성 동작을 수행하는 동작과 대응되는 동작일 수 있다.

[0198] 도 5는 본 개시의 일부 실시 예에 따른 SSP 단말이 SPB Manager로부터 제1 번들 정보를 수신한 후, bundle을 요청하는 과정을 설명하기 위한 도면이다. 도 5는 특히, 도 4를 참조하여 전술한 단계 429에서 제1 번들 정보 요청 여부 확인 절차를 번들 정보 요청 함수 command에 포함된 SSP credential값을 기반으로 수행하는 일 실시예에 관한 것이다.

[0199] 도 5에서 단계 525를 포함한 이전 단계는 도 4에서 전술한 대응되는 각 단계와 동일하게 수행될 수 있다.

[0200] 단계 528에서 LBA(402)는 번들 정보 요청 함수를 command를 SPB manager(403)에 전송할 수 있다. 단계 528에서 LBA(402)는 번들 정보 요청 함수 command에 SSP credential, 단말 정보 (terminal information), 그리고 requestType을 포함시킬 수 있다. 단계 528에서 requestType의 값은 제1 번들 정보를 받은 뒤 제2 번들 정보를 요청하는 것을 의미하는 Type-C를 지칭한다.

[0201] 단계 528의 번들 정보 요청 함수 command를 수신한 SPB Manager(403)는 상기 command를 전송하는 단말이 단계 418에서 번들 정보 요청 함수 command를 보낸 단말과 같은지를 확인하는 절차 (제1 번들 정보 요청 여부 확인 절차)를 수행할 수 있다. 단계 529에서 제1 번들 정보 요청 여부 확인 절차는, 단계 518에서 제1 번들 정보를 요청하기 위해 전달된 command 내에 포함된 SSP credential과 단말 정보와 동일한 SSP credential과 단말 정보가 단계 528의 command에 포함되었는지를 검증하는 것으로 수행될 수 있다.

[0202] 상기 단계 529에서 제1 번들 정보 요청 여부 확인 절차는 단계 528에서 전달된 SSP credential이 단계 518에서 전달된 SSP credential과 같은지 확인하는 과정으로 간소화 될 수도 있다. 상기 단계 529에서 제1 번들 정보 요청 여부 확인 절차는 단계 518에서 전달된 SSP credential과 terminalInfo로 단계 519를 수행하고 단계 521에 따라 단말에게 제1 번들 정보를 성공적으로 전달했는지 여부를 확인하는 절차일 수 있다.

[0203] 상기 단계 529의 제1 번들 정보 요청 여부 확인 절차를 통해 동일 SSP 단말임이 확인이 되면. SPB Manager(403)는 도 4의 단계 429를 참조하여 전술한 제2 번들 정보 생성 동작을 수행할 수 있다. 제2 번들 정보 생성 동작이 성공적으로 수행되면 단계 530에 따라 번들 정보 요청함수 command 에 대한 응답에 제2 번들 정보를 포함시켜 LBA(402)에 전달할 수 있다.

[0204] 도 6은 본 개시의 일 실시예에 따른 SSP 단말이 SPB Manager로부터 제1 번들 정보를 수신한 후, bundle을 요청하는 과정을 설명하기 위한 도면이다. 도 6은 특히 도 4의 단계 429에서 제1 번들 정보 요청 여부 확인 절차를 SPB Manager가 전달한 challenge값에 대한 로더의 서명을 검증하는 것으로 수행하는 실시예에 관한 것이다.

[0205] 도 6에서 단계 619를 포함한 이전 단계는 도 4에서 전술한 대응되는 각 단계와 동일하게 수행될 수 있다.

[0206] 단계 619에서 SPB Manager(403)의 동작이 정상적으로 수행되면, SPB Managner(403)는 단계 621에 따라 번들 정보 요청함수 command에 대한 응답에 제1 번들 정보와 serverChallenge 값을 포함하여 전송할 수 있다. 단계 621에서 SPB Manager(403)가 전송한 응답을 수신한 LBA(402)는 단계 625에 따라 제1 번들 정보를 검증할 수 있다. LBA(402)는 단계 625를 수행한 후 단계 626b에 따라 로더(401)에 서명 요청 함수 command를 전달한다. 서명 요청 함수 command는 단계 621에서 SPB Manager(403)로부터 수신한 serverChallenge를 포함할 수 있다.

[0207] 서명 요청 함수 command를 수신한 로더 (401)는 단계 627에 따라 서명 요청 함수 command에 포함된 serverChallenge값을 기반으로 단계 416에서 SSP Credential에 포함된 로더의 서명용 인증서로 검증 가능한 signedChallenge를 생성하여 LBA(402)에 전달한다. 로더는 로더의 서명용 인증서의 public key와 대응되는 private key로 serverChallenge를 서명하여 signedChallenge를 생성할 수 있다.

[0208] 단계 627에서 로더(401)는 LBA(402)의 서명 요청 함수 command에 대한 응답으로 serverChallenge와 이를 서명한 signedChallenge를 함께 응답에 포함하여 LBA(402)에 전달할 수 있다.

[0209] 단계 627의 로더 (401)로부터 응답을 수신한 LBA(402)는 단계 628에 따라 번들 정보 요청 함수 command를 SPB Manager(403)에게 전달하여 제 2 번들 정보를 요청할 수 있다. 이때 단계 627의 번들 정보 요청 함수 command는 단계 627에서 로더(401)로부터 수신한 signedChallenge를 포함할 수 있다. 번들 정보 요청 함수 command에 signedChallenge가 포함되는 방법으로써 requestType의 값으로 signedChallenge를 사용할 수 있다. serverChallenge는 signedChallenge와 함께 번들 정보 요청 함수 command에 포함되어 전달될 수 있다. 상기 signedChallenge를 requestType의 값으로 사용하는 방법은 Type-C (제1 번들 정보 요청 후 제2 번들 정보를 요청하는 type)를 표시하는 방법 중 하나의 실시 예로 사용될 수 있다.

[0210] 단계 627에서 LBA(402)는 번들 정보 요청 함수 command에 SSP credential과 단말 정보를 포함하지 않을 수도 있다. 이는 SPB Manager가 검증할 수 있는 signedChallenge를 생성할 수 있는 SSP 단말은 오로지 이전에 제1 번들 정보를 요청하기 위해 보낸 번들 정보 요청 함수 command의 응답으로 제1 번들 정보와 serverchallenge를 수신한 SSP 단말이기 때문이다.

[0211] 단계 629에 따라, SPB Manager(403)는 번들 정보 요청 함수 command를 수신하여 command에 포함된 requestType 값을 확인한다. requestType 값이 Type-C (제1 번들 정보 요청 후 제2 번들 정보를 요청하는 type)인 경우, SPB Manager (403)는 제1 번들 정보 요청 여부 확인 절차를 수행할 수 있다. 제1 번들 정보 요청 여부 확인 절차는 SPB Manager(403)가 수신한 command에 포함된 signedChallenge를 검증하는 방법일 수 있다. signedChallenge는 requestType에 포함될 수도 있다. SPB Manager(403)는 번들 정보 요청 함수 command에 포함된 signedChallenge를 단계 619에서 검증한 SPBL (로더)의 인증서에 포함된 public key로 검증할 수 있다. signedChallenge의 검증은 단계 621 에서 SPB Manager(403)이 LBA(002)에 전달한 serverChallenge 값에 대한 서명인지 확인함으로써 검증할 수 있다. 로더의 인증서에 포함된 public key로 signedChallenge가 검증가능하다는 것은 SPB Manager(403)가 보낸 serverChallenge를 SSP credential을 생성했던 로더 (401)가 서명하여 signedChallenge를 생성했다는 것을 입증하는 것이므로, 이러한 절차를 통해 SPB Manager(403)는 번들 정보 요청 함수 command를 전송한 단말이 단계 618에서 제1 번들 정보를 요청한 단말과 같은 단말임을 확인 (제1 번들 정보 요청 여부 확인 절차) 할 수 있다.

[0212] 상기 단계 629의 signedChallenge를 통해 동일 SSP 단말임이 확인이 되면. SPB Manager(403)는 도 4의 단계 629를 참조하여 전술한 제2 번들 정보 생성 동작을 수행할 수 있다. 제2 번들 정보 생성 동작이 성공적으로 수행되면 단계 630에 따라 번들 정보 요청함수 command 에 대한 응답에 제2 번들 정보를 포함시켜 LBA(402)에 전달할 수 있다.

[0213] 도 7은 본 개시의 일실시 예에 따른 SSP 단말이 SPB Manager로부터 제1 번들 정보를 수신한 후, bundle을 요청하는 과정을 도시한 도면이다.

[0214] 도 7은 특히 도 4의 단계 429에서 제1 번들 정보 요청 여부 확인 절차를 SPB Manager가 전달한 challenge값에 대한 로더의 서명을 검증하는 것으로 수행하는 실시 예에 관한 것이다.

[0215] 도 7에서 단계 713을 포함한 이전 단계는 도 4에서 전술한 대응되는 각 단계와 동일하게 수행될 수 있다. 단계 713에서 SPBM 인증서 요청 함수 command를 수신한 SPB Manager(403)는 다음을 수행할 수 있다.

[0216] - Eligibility check 수행: LBA와 SPBL의 버전을 확인하여 지원가능한 SSP 단말인지 확인

[0217] - 번들의 패밀리 식별자 확정

[0218] - (옵션) 번들의 패밀리 식별자를 관리하는 기관의 Object Identifier 확정

[0219] - SPBM 키 생성 인증서(CERT.SPBM.KA)와 이를 검증할 인증서 체인 선택

[0220] - SSP가 사용해야할 인증서의 CI 정보 선택

[0221] - SSP가 데이터 암호를 위해 사용해야 할 암호 알고리즘의 정보 선택

[0222] 단계 713에서 상기 동작을 정상적으로 완료한 SPB Manager(403)은 단계 714에서 SPBM 키 형성 인증서와 인증서 체인, SSP가 사용해야할 인증서의 CI 정보, SSP가 사용해야 할 암호화 알고리즘 정보, 번들의 패밀리 식별자 중 적어도 하나를 포함하여 응답할 수 있다. SPB Manager(403)는 또한 패밀리 식별자를 관리하는 기관의 Object identifier를 포함하여 응답할 수도 있다. 또한, 단계 714에서 SPB Manager(403)는 serverChallenge 값을 생성하고 SPBM 인증서 요청 함수 응답에 이를 포함하여 LBA(402)에 전달할 수 있다. 상기 serverChallenge값은 일반적으로 16 byte 길이를 가지는 octet string이며 SPB Manager(403)가 랜덤으로 생성할 수 있다. 또한, serverChallenge는 다른 길이의 octet string으로도 사용될 수 있다.

[0223] 단계 714에서 SPB Manager(403)의 응답을 받은 LBA(402)는 단계 715에 따라 SSP Credential 요청 함수를 호출하여 SSP Credential 요청 함수 command를 로더 (400)에게 전송할 수 있다. SSP Credential 요청 함수 command는 서버 Credential를 포함할 수 있다. 서버 Credential은 도 4의 단계 415와 동일하게 생성할 수 있다.

[0224] 단계 716에 따라 SSP Credential 요청 함수 command를 수신한 로더 (401)는 수신한 서버 Credential을 기반으로 SSP Credential을 생성할 수 있다. SSP Credential 생성 동작은 도 4의 단계 416에서 SSP Credential 생성 동작과 대응될 수 있다. 단계 716에서 로더(401)는 SSP Credential 요청 함수 command에 포함된 serverChallenge를 서명하여 signedChallenge를 생성할 수 있다. signedChallenge는 SSP Credential에 포함하여 전달하는 SPBL 서명용 인증서의 public key에 대응되는 private key를 이용하여 serverChallenge를 서명함으로써 생성할 수 있다. 단계 716에서 로더(401)는 생성한 SSP Credential과 signedChallenge를 포함하여 SSP Credential 요청 함수 command에 대해 응답할 수 있다.

[0225] 단계 717에 따라 LBA(402)는 단계 716에서 로더(401)로부터 전달받은 signedChallenge 값을 보관할 수 있다. 해당 signedChallenge값은 현재 진행중인 bundle download session에서 LBA(402)가 제1 번들 정보를 먼저 요청하고 수신한 뒤, 제2 번들 정보를 요청할 때, 동일한 SSP 단말임을 입증하는 용도로 사용할 수 있다.

[0226] 도 7의 단계 718, 719, 721은 도 4의 단계 418, 419, 421와 대응될 수 있다.

[0227] 단계 721에서 제1 번들 정보를 SPB Manager(403)로부터 전달받은 LBA(402)는 단계 725에 따라 다음과 같은 동작을 수행할 수 있다.

[0228] - 제1 번들 정보 검증: 해당 동작은 도 4의 단계 425에서 수행하는 제1 번들 정보 검증 동작을 참조할 수 있다.

[0229] - 단계 717에서 보관한 signedChallenge를 사용하여 번들 정보 요청 함수 command를 생성할 수 있다.

[0230] 단계 728에 따라 LBA(402)는 SPB Manager(403)로부터 제2 번들 정보를 다운로드하기 위해 번들 정보 요청 함수 command를 SPB Manager(403)에 전달할 수 있다. 단계 728 에서 번들 정보 요청 함수 command 의 requestType은 Type-C (제1 번들 정보 요청 후 제2 번들 정보를 요청하는 type) 을 의미할 수 있다. 단계 7287에서 LBA(402)는 단계 717에서 보관한 signedChallenge 를 Type-C를 의미하는 requestType의 값으로 사용할 수 있다. 단계 728에서 번들 정보 요청 함수 commmand에 signedChallenge와 serverChallenge가 함께 포함될 수 있다. 단계 728c에서 번들 정보 요청 함수 command에는 SSP credential와 단말 정보가 포함되지 않을 수도 있다.

[0231] 단계 7297에서 SPB Manager(403)는 번들 정보 요청 함수 command를 수신하고 requestType을 확인할 수 있다. requestType이 Type-C 인 경우, SPB Manager (403)는 제1 번들 요청 여부 확인 절차를 수행할 수 있다. 제1 번들 요청 여부 확인 절차는 번들 정보 요청 함수 command에 포함된 signedChallenge를 검증하는 방법일 수 있다. signedChallenge는 requestType의 값으로 사용되어 Type-C임을 의미할 수도 있다. signedChallenge는 단계 7719에서 검증한 SPBL 서명용 인증서를 사용하여 검증한다. signedChallenge의 검증은 714에서 SPB Manager(403)이 생성한 severChallenge에 대한 SSP의 서명이 signedChallenge가 맞는지를 SPBL 서명용 인증서를 이용하여 검증하는 과정일 수 있다.signedChallenge가 bb14c 단계에서 보낸 serverChallenge에 대한 서명인지를 검증한 다음 SPB Manager(403)는 제2 번들 정보를 생성한다. 제2 번들 정보 생성 동작은 도 4의 단계 429의 제2 번들 정보 생성 동작을 참조할 수 있다. 단계 729에서 signedChallenge검증과 제2 번들 정보 생성을 완료한 SPB Manager(403)는 단계 730에 따라 번들 정보 요청 함수 command에 대한 응답에 제2 번들 정보를 포함시

켜 LBA(402)에 응답할 수 있다.

[0232] 도 8은 본 개시의 일 실시예에 따른 SSP 단말이 SPB Manager로부터 제1 번들 정보를 수신한 후, 제2 번들 정보를 요청하는 과정을 설명하기 위한 도면이다. 도 8은 특히 도 4의 단계 429에서 제1 번들 정보 요청 여부 확인 절차를 SSP Credential에 포함되는 session ID로 사용될 수 있는 ID_TRANSAC 값에 대한 서명을 검증하는 방식으로 수행하는 실시예에 관한 것이다.

[0233] 도 8에서 단계 815를 포함한 이전 단계는 도 4에서 전술한 대응되는 각 단계와 동일하게 수행될 수 있다.

[0234] 단계 816에서 LBA(402)로부터 SSP Credential 요청 함수 command를 받은 로더(401)는 수신한 서버 Credential을 기반으로 SSP Credential을 생성할 수 있다. 단계 816에서 로더(401)는 SSP Credential 생성 과정 중에 생성한 ID_TRANSAC 값을 서명하여 signedIdTransac 을 생성할 수 있다. signedIdTransac 값은 SSP Credential에 포함되는 SPBL 서명용 인증서의 public key에 대응되는 private key를 이용하여 ID_TRANSAC 값을 서명하여 생성할 수 있다. 단계 816에서 로더(401)는 LBA(402)의 SSP Credential 요청 함수 command에 대해 SSP Credential과 signedIdTransac을 포함하여 응답할 수 있다.

[0235] 단계 817에서 LBA(402)는 단계 816에서 로더(401)로부터 받은 응답에 포함된 signedIdTransac을 보관할 수 있다. 해당 signedIdTransac값은 현재 진행중인 bundle download session에서 LBA(402)가 제1 번들 정보를 먼저 요청하고 수신한 뒤, 제2 번들 정보를 요청할 때, 동일한 SSP 단말임을 입증하는 용도로 사용할 수 있다.

[0236] 도 8의 단계 818, 819, 821은 도 4의 단계 418, 419, 421와 대응될 수 있다.

[0237] 단계 821에서 제1 번들 정보를 SPB Manager(403)로부터 전달받은 LBA(402)는 단계 825에 따라 다음과 같은 동작을 수행할 수 있다.

[0238] - 제1 번들 정보 검증: 해당 동작은 도 4의 단계 425에서 수행하는 제1 번들 정보 검증 동작을 참조할 수 있다.

[0239] - 단계 817에서 보관한 signedIdTransac을 사용하여 번들 정보 요청 함수 command를 생성할 수 있다.

[0240] 단계 828에 따라 LBA(402)는 SPB Manager(403)로부터 제2 번들 정보를 다운로드하기 위해 번들 정보 요청 함수 command를 SPB Manager(403)에 전달할 수 있다. 단계 828 에서 번들 정보 요청 함수 command 의 requestType은 Type-C (제1 번들 정보 요청 후 제2 번들 정보를 요청하는 type) 을 의미할 수 있다. 단계 828에서 LBA(402)는 단계 817에서 보관한 signedIdTransac 를 Type-C를 의미하는 requestType의 값으로 사용할 수 있다. 단계 828에서 번들 정보 요청 함수 commmand에 signedIdTransac과 ID_TRANSAC을 함께 포함할 수 있다. 단계 828에서 번들 정보 요청 함수 command에는 SSP credential와 단말 정보가 포함되지 않을 수도 있다.

[0241] 단계 829에서 SPB Manager(403)는 번들 정보 요청 함수 command를 수신하고 requestType을 확인할 수 있다. requestType이 Type-C 인 경우, SPB Manager(403)는 제1 번들 요청 여부 확인 절차를 수행한다. 제1 번들 요청 여부 확인 절차는 번들 정보 요청 함수 command에 포함된 signedIdTransac을 검증하는 방법일 수 있다. signedIdTransac은 requestType의 값으로 사용되어 Type-C임을 의미할 수도 있다. signedIdTransac는 단계 819에서 검증한 SPBL 서명용 인증서를 사용하여 검증한다. signedIdTransac의 검증은 818에서 SPB Manager(403)가 수신한 번들 정보 요청 함수 command에 포함된 ID_TRANSAC에 대한 SSP의 서명이 signedIdTransac이 맞는지를 SPBL 서명용 인증서를 이용하여 검증하는 과정일 수 있다. signedIdTransac이 818 단계에서 받은 ID_TRANSAC에 대한 서명인지를 검증한 다음 SPB Manager(403)는 제2 번들 정보를 생성한다. 제2 번들 정보 생성 동작은 도 4의 단계 429의 제2 번들 정보 생성 동작과 대응될 수 있다. 단계 829에서 signedIdTransac 검증과 제2 번들 정보 생성을 완료한 SPB Manager(403)는 단계 830에 따라 번들 정보 요청 함수 command에 대한 응답에 제2 번들 정보를 포함시켜 LBA(402)에 응답할 수 있다.

[0242] 도 9은 본 개시의 일 실시예에 따른 SSP 단말이 SPB Manager로부터 제1 번들 정보를 수신한 후, 제2 번들 정보를 요청하는 과정을 설명하기 위한 도면이다. 도 9는 특히, 제 1 번들 정보 요청 함수 command와 제 2 번들 정보 요청 함수 command가 각각 별개로 존재하고, 제 2 번들 정보가 제 1 번들 정보 생성 이후에 생성되는 실시예에 관한 것이다.

[0243] 도 9에서 단계 916을 포함한 이전 단계는, 도 4를 참조하여 전술한 각 단계와 대응될 수 있다.

[0244] 단계 918에서, LBA(402)는 제 1 번들 정보 요청 함수 command를 SPB Manager (403)에 전송할 수 있다. 제 1 번들 정보 요청 함수 command는 SSP credential 및 단말 정보를 포함할 수 있으며, 본 command는 제 1 번들 정보를 요청하는 것으로 특정된 것으로 전술한 실시예들과 달리 request type에 관한 정보는 포함되지 않을 수

있다.

[0245] 단계 919, 단계 921 및 단계 925는 도 4를 참조하여 전술한 단계 419, 단계 421 및 단계 425와 대응될 수 있다.

[0246] 단계 928에서, LBA(402)는 제 2 번들 정보 요청 함수 command를 SPB Manager (403)에 전송할 수 있다. 제 2 번들 정보 요청 함수 command는 SSP credential 및 단말 정보를 포함할 수 있으며, 본 command는 제 2 번들 정보를 요청하는 것으로 특정된 것으로 전술한 실시예들과 달리 request type에 관한 정보는 포함되지 않을 수 있다.

[0247] 단계 928에 의해 제2 번들 정보 요청 함수 command를 수신한 SPB Manager는 단계 929를 수행할 수 있다. 단계 929에서 SPB Manager는 제2 번들 정보 요청 함수 command에 포함된 SSP Credential과 단말 정보를 기반으로 제1 번들 정보를 수신한 SSP 단말인지 확인하는 절차를 수행할 수 있다. 단계 929에서 SPB Manager는 단계 919의 동작을 한 번 더 수행할 수 있다.

[0248] 한편, SSP 단말이 단계 918에서 제2 번들 요청 함수 command를 보낸 경우, SPB Manager는 단계 919를 수행 후 단계 921을 생략하고 제 2번들 정보를 생성하는 동작(단계 929)를 수행할 수 있다. 단계 921을 수행하지 않도록 하는 번들 요청 함수 command는 단계 928에서 전달되는 제2 번들 요청 함수 command와 다른 함수 command로 정의될 수 있다.

[0249] 단계 930은, 도 4를 참조하여 전술한 단계 430과 대응될 수 있다.

[0250] 도 10은 번들 다운로드 절차 중 SPB Manager가 번들 정보 요청 함수 커맨드(command)를 수신했을 때의 SPB Manager 동작을 설명하기 위한 흐름도이다.

[0251] 도 10에서의 SPB Manager 동작의 시작은 LBA와 SPB Manager 간의 인터페이스인 Si2 인터페이스를 통해서 함수 커맨드를 수신하는 것을 시작으로 한다. Si2 인터페이스를 통해서 함수 커맨드를 수신한 SPB Manager는 도 1001에 따라서 수신한 함수 커맨드가 번들 또는 제1 번들 정보를 요청하는 커맨드인지를 파악한다. 해당 함수 커맨드는 본 개시에서 번들 정보 요청 함수 커맨드라 명명하며, Si2GetBoundSpbImageCommand, Si2GetBoundSpbImageMetadataCommand 등으로도 불릴 수 있다. 번들 정보 요청 함수 커맨드는 SSP Credential, 단말 정보, requestType을 포함할 수 있다.

[0252] 도 1001에서 수신한 함수 커맨드가 도 4의 단계 418에서 정의한 Type-A (제2 번들 정보를 요청하는 type) 또는 Type-B (제1 번들 정보 만 요청하는 type)를 의미하는 번들 정보 요청 함수 커맨드일 경우 단계 1002에 따라 제1 세션 키 생성, SBPL 서명용 인증서 검증, SSP Credential 검증, 번들 선택, 번들 다운로드를 요청한 SSP 단말이 번들을 다운로드 받을 수 있는지 체크, 메타 데이터 생성을 수행할 수 있다. 단계 1002는 도 4의 단계 419에서 SPB Manager가 수행하는 동작과 대응될 수 있다.

[0253] 단계 1003에 따라 단계 1002를 정상적으로 수행한 SPB Manager는 단계 1004에 따라서 번들 정보 요청 커맨드에 포함된 requestType이 Type-B (제1 번들 정보 만 요청하는 type)인지를 확인할 수 있다. requestType이 Type-B (제1 번들 정보 만 요청하는 type) 인 경우는 단계 1005에 따라 제1 번들 정보를 포함하여 LBA에 응답할 수 있다. 단계 1005에서 SPB Manager는 일부 실시 예에 따라 응답에 제1 번들 정보와 함께 serverChallenge를 포함시킬 수 있다. 단계 1002의 모든 동작을 정상적으로 수행하지 못한 SPB Manager는 단계 1010에 따라 LBA에 대한 응답으로 에러 메시지를 전송할 수 있다.

[0254] 단계 1004에서 번들 정보 요청 커맨드에 포함된 requestType이 Type-A (제2 번들 정보를 요청하는 type) 인 경우, SPB Manager는 도 509에 따라 제2 번들 정보를 생성하고 생성한 제2 번들 정보를 포함하여 LBA에 응답한다. 제2 번들 정보 생성 동작은 도 4의 단계 429의 제2 번들 정보 생성 동작과 대응될 수 있다.

[0255] 단계 1006에서 따라 수신한 함수 커맨드가 도 4의 단계 418에서 정의한 Type-C (제1 번들 정보 요청 후 제2 번들 정보를 요청하는 type)이 포함된 경우, 단계 507에 따라 SPB Manager는 해당 함수 커맨드를 전송한 단말이 이전에 제1 번들 정보를 요청한 단말인지를 검증하는 동작을 수행할 수 있다. 단계 1007의 검증 동작은 다음 중 하나로 수행될 수 있다.

[0256] - 도 5의 단계 529의 제1 번들 정보 요청 여부 확인 절차: 단계 5295에서 전달된 SSP credential가 단계 518에서 전달된 SSP credential과 같은지 확인하는 과정으로 간소화 될 수도 있다.

[0257] - 도 6의 단계 629에서의 signedChallenge 검증: SPB Manager(403)은 수신한 command에 포함된 signedChallenge를 검증한다. signedChallenge는 requestType에 포함될 수도 있다. SPB Manager(403)는 번들

정보 요청 함수 command에 포함된 signedChallenge를 단계 619에서 검증한 SPBL (로더)의 인증서에 포함된 public key로 검증한다. signedChallenge의 검증은 단계 621 에서 SPB Manager(403)이 LBA(002)에 전달한 serverChallenge 값에 대한 서명인지 확인함으로써 검증할 수 있다.

[0258] - 도 7의 단계 729에서의 signedChallenge 검증: signedChallenge는 단계 719에서 검증한 SPBL 서명용 인증서를 사용하여 검증한다. signedChallenge의 검증은 bb14c에서 SPB Manager(403)이 생성한 severChallenge에 대한 SSP의 서명이 signedChallenge가 맞는지를 SPBL 서명용 인증서를 이용하여 검증하는 과정일 수 있다.

[0259] - 도 8의 단계 829의 signedIdTransac 검증: 번들 정보 요청 함수 command에 포함된 signedIdTransac을 검증한다. signedIdTransac은 requestType의 값으로 사용되어 Type-C임을 의미할 수도 있다. signedIdTransac는 단계 819에서 검증한 SPBL 서명용 인증서를 사용하여 검증한다. signedIdTransac의 검증은 bb18에서 SPB Manager(403)가 수신한 번들 정보 요청 함수 command에 포함된 ID_TRANSAC에 대한 SSP의 서명이 signedIdTransac이 맞는지를 SPBL 서명용 인증서를 이용하여 검증하는 과정일 수 있다.

[0260] 단계 1007의 검증 동작을 성공적으로 수행한 SPB Manager는 단계 1009를 수행한다. 단계 1007의 검증 동작이 실패하면 단계 1010에 따라 에러 메시지를 전달할 수 있다.

[0261] 도 11은 일 실시예에 따른 SSP 단말의 동작을 설명하기 위한 흐름도이다.

[0262] 단계 1110에서, SSP 단말은 번들의 식별자 및 메타데이터를 포함하는 제 1 번들 정보의 요청을 SPB 서버에 전송할 수 있다. 단계 1110은 도 4 내지 도 9 각각의 단계 418, 단계 518, 단계 618, 단계 718, 단계 818 및 단계 918과 대응될 수 있다.

[0263] 단계 1120에서, SSP 단말은 요청에 따라 SPB 서버로부터 수신된 제 1 번들 정보의 유효성을 검증할 수 있다. 단계 1120은 도 4 내지 도 9 각각의 단계 425, 단계 525, 단계 625, 단계 725, 단계 825 및 단계 925와 대응될 수 있다.

[0264] 단계 1130에서, SSP 단말은 제 1 번들 정보가 유효한 것으로 검증됨에 따라 번들에 관한 암호화된 데이터를 포함하는 제 2 번들 정보의 요청을 SPB 서버에 전송할 수 있다. 단계 1130은 도 4 내지 도 9 각각의 단계 428, 단계 528, 단계 628, 단계 728, 단계 828 및 단계 928과 대응될 수 있다.

[0265] 단계 1140에서, SSP 단말은 제 2 번들 정보의 요청을 기초로 SSP 단말이 제 1 번들 정보를 요청한 단말임이 확인됨에 따라, SPB 서버로부터 제 2 번들 정보를 수신할 수 있다. 단계 1140은 도 4 내지 도 9 각각의 단계 430, 단계 530, 단계 630, 단계 730, 단계 830 및 단계 930과 대응될 수 있다.

[0266] 도 12는 일 실시예에 따른 SPB 서버의 동작을 설명하기 위한 흐름도이다.

[0267] 단계 1210에서, SPB 서버는 번들의 식별자 및 메타데이터를 포함하는 제 1 번들 정보의 요청을 SSP 단말로부터 수신할 수 있다. 단계 1110은 도 4 내지 도 9 각각의 단계 418, 단계 518, 단계 618, 단계 718, 단계 818 및 단계 918과 대응될 수 있다.

[0268] 단계 1220에서, SPB 서버는 요청에 따라 제 1 번들 정보를 SSP 단말에 전송할 수 있다. 단계 1220은 도 4 내지 도 9 각각의 단계 421, 단계 521, 단계 621, 단계 721, 단계 821 및 단계 921과 대응될 수 있다.

[0269] 단계 1230에서, SPB 서버는 제 1 번들 정보가 유효한 것으로 검증됨에 따라 번들에 관한 암호화된 데이터를 포함하는 제 2 번들 정보의 요청을 SSP 단말로부터 수신할 수 있다. 단계 1130은 도 4 내지 도 9 각각의 단계 428, 단계 528, 단계 628, 단계 728, 단계 828 및 단계 928과 대응될 수 있다.

[0270] 단계 1240에서, SPB 서버는 제 2 번들 정보의 요청을 기초로 SSP 단말이 제 1 번들 정보를 요청한 단말임이 확인됨에 따라, 제 2 번들 정보를 SSP 단말에 전송할 수 있다. 단계 1140은 도 4 내지 도 9 각각의 단계 430, 단계 530, 단계 630, 단계 730, 단계 830 및 단계 930과 대응될 수 있다.

[0271] 도 13은 일 실시예에 따른 SSP 단말의 블록도이다.

[0272] SSP 단말(1300)은 LBA(1310), 프로세서(1320), 송수신부(1330) 및 메모리(1340)를 포함할 수 있다.

[0273] LBA(1310) 및 프로세서(1320)는 도 1 내지 도 9를 참조하여 전술한 LBA 및 SSP와 대응될 수 있으며, 도 13에 도시된 블록도는 일 예일 뿐, LBA가 프로세서 내부에 구성될 수도 있다.

[0274] 송수신부(1330)는 다른 장치, 예를 들어, SPB 서버와 신호를 송수신할 수 있다. 이를 위해, 송수신부 (1330)는 송신되는 신호의 주파수를 상승 변환 및 증폭하는 RF 송신기와, 수신되는 신호를 저 잡음 증폭하고 주파수를 하

강 변환하는 RF 수신기 등으로 구성될 수 있다.

[0275] 메모리(1340)는 SSP 단말에서 송수신하는 신호를 저장할 수 있으며, 전술한 동작들을 수행하는데 필요한 명령어를 저장할 수 있다.

[0276] 도 14는 일 실시예에 따른 SPB 서버(1400)의 블록도이다.

[0277] SPB 서버(1400)는 송수신부(1410), 프로세서(1420) 및 메모리(1430)를 포함할 수 있다.

[0278] 송수신부(1410)는 다른 장치, 예를 들어, SSP 단말과 신호를 송수신할 수 있다. 이를 위해, 송수신부 (1410)는 송신되는 신호의 주파수를 상승 변환 및 증폭하는 RF 송신기와, 수신되는 신호를 저 잡음 증폭하고 주파수를 하강 변환하는 RF 수신기 등으로 구성될 수 있다.

[0279] 프로세서(1420)는 도 1 내지 도 9를 참조하여 전술한 SPB Manager의 동작을 수행하도록, SPB 서버(1400)를 제어할 수 있다.

[0280] 메모리(1430)는 SPB 서버(1400)에서 송수신하는 신호를 저장할 수 있으며, 전술한 동작들을 수행하는데 필요한 명령어를 저장할 수 있다.

[0281] 상술한 본 개시의 구체적인 실시 예들에서, 개시에 포함되는 구성 요소는 제시된 구체적인 실시 예에 따라 단수 또는 복수로 표현되었다. 그러나, 단수 또는 복수의 표현은 설명의 편의를 위해 제시한 상황에 적합하게 선택된 것으로서, 본 개시가 단수 또는 복수의 구성 요소에 제한되는 것은 아니며, 복수로 표현된 구성 요소라 하더라도 단수로 구성되거나, 단수로 표현된 구성 요소라 하더라도 복수로 구성될 수 있다.

[0282] 한편 본 개시의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 개시의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 개시의 범위는 설명된 실시 예에 국한되어 정해져서는 아니 되며 후술하는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

[0283] 본 개시의 다양한 실시 예들 및 이에 사용된 용어들은 본 개시에 기재된 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 해당 실시예의 다양한 변경, 균등물, 및/또는 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 구성요소에 대해서는 유사한 참조 부호가 사용될 수 있다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다. 본 개시에서, "A 또는 B", "A 및/또는 B 중 적어도 하나", "A, B 또는 C" 또는 "A, B 및/또는 C 중 적어도 하나" 등의 표현은 함께 나열된 항목들의 모든 가능한 조합을 포함할 수 있다. "제1", "제2", "첫째" 또는 "둘째" 등의 표현들은 해당 구성요소들을, 순서 또는 중요도에 상관없이 수식할 수 있고, 한 구성요소를 다른 구성요소와 구분하기 위해 사용될 뿐 해당 구성요소들을 한정하지 않는다. 어떤(예: 제1) 구성요소가 다른(예: 제2) 구성요소에 "(기능적으로 또는 통신적으로) 연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 상기 어떤 구성요소가 상기 다른 구성요소에 직접적으로 연결되거나, 다른 구성요소(예: 제3 구성요소)를 통하여 연결될 수 있다.

[0284] 본 개시에서 사용된 용어 "모듈"은 하드웨어, 소프트웨어 또는 펌웨어로 구성된 유닛을 포함하며, 예를 들면, 로직, 논리 블록, 부품, 또는 회로 등의 용어와 상호 호환적으로 사용될 수 있다. 모듈은, 일체로 구성된 부품 또는 하나 또는 그 이상의 기능을 수행하는 최소 단위 또는 그 일부가 될 수 있다. 예를 들면, 모듈은 ASIC(application-specific integrated circuit)으로 구성될 수 있다.

[0285] 본 개시의 다양한 실시 예들은 기기(machine)(예: 컴퓨터)로 읽을 수 있는 저장 매체(machine-readable storage media)(예: 내장 메모리 또는 외장 메모리에 저장된 명령어를 포함하는 소프트웨어(예: 프로그램)로 구현될 수 있다. 기기는, 저장 매체로부터 저장된 명령어를 호출하고, 호출된 명령어에 따라 동작이 가능한 장치로서, 다양한 실시 예들에 따른 단말을 포함할 수 있다. 상기 명령이 프로세서에 의해 실행될 경우, 프로세서가 직접, 또는 상기 프로세서의 제어 하에 다른 구성요소들을 이용하여 상기 명령에 해당하는 기능을 수행할 수 있다. 명령은 컴파일러 또는 인터프리터에 의해 생성 또는 실행되는 코드를 포함할 수 있다.

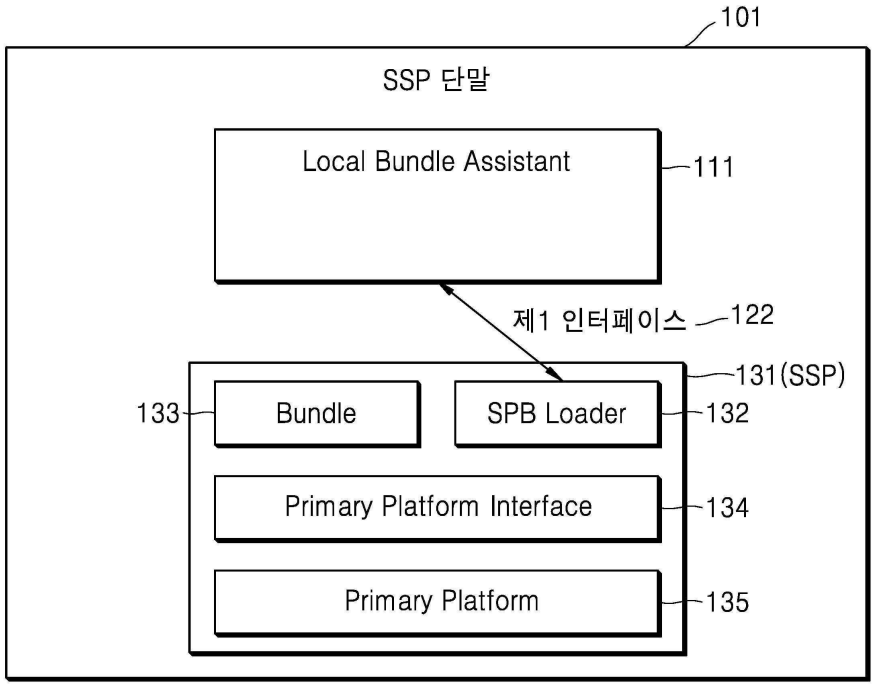
[0286] 기기로 읽을 수 있는 저장매체는, 비일시적(non-transitory) 저장매체의 형태로 제공될 수 있다. 여기서, '비일시적'은 저장매체가 신호(signal)를 포함하지 않으며 실재(tangible)한다는 것을 의미할 뿐 데이터가 저장매체에 반영구적 또는 임시적으로 저장됨을 구분하지 않는다.

[0287] 본 개시에 개시된 다양한 실시 예들에 따른 방법은 컴퓨터 프로그램 제품(computer program product)에 포함되어 제공될 수 있다. 컴퓨터 프로그램 제품은 상품으로서 판매자 및 구매자 간에 거래될 수 있다. 컴퓨터 프로그

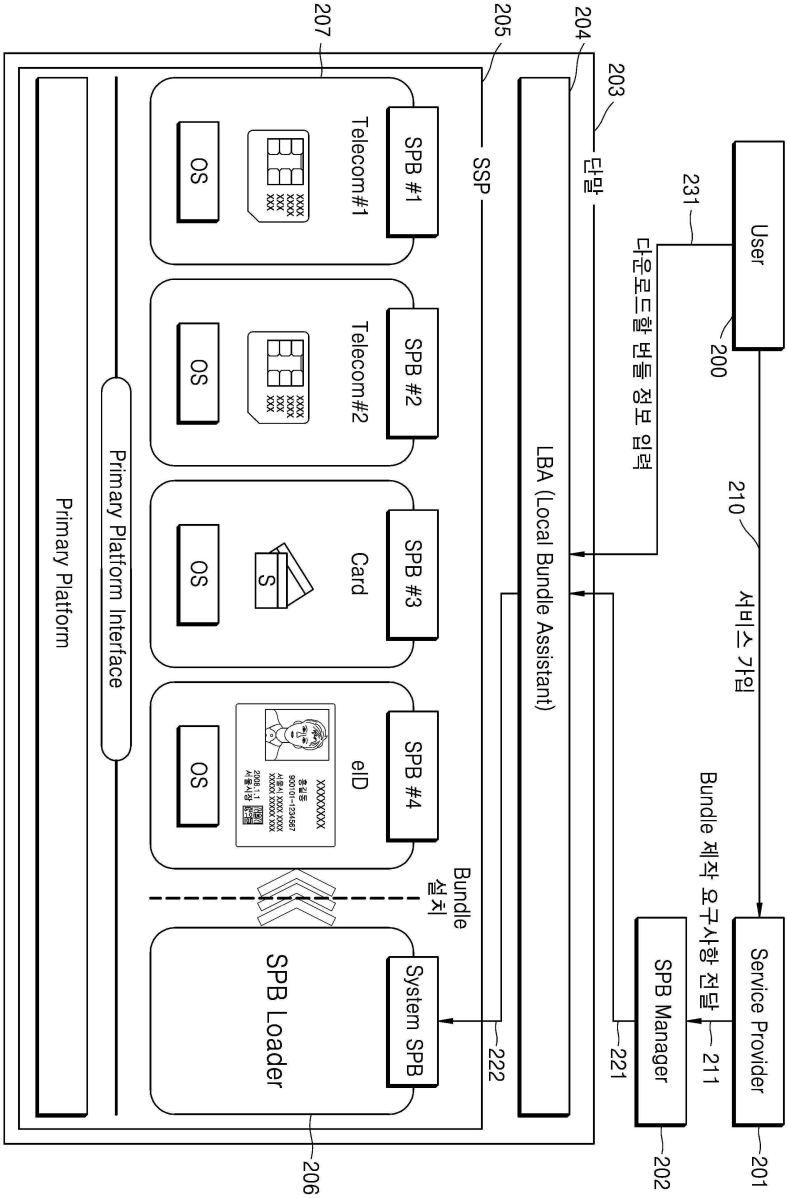
램 제품은 기기로 읽을 수 있는 저장 매체(예: compact disc read only memory (CD-ROM))의 형태로, 또는 어플리케이션 스토어(예: 플레이 스토어TM)를 통해 온라인으로 배포될 수 있다. 온라인 배포의 경우에, 컴퓨터 프로그램 제품의 적어도 일부는 제조사의 서버, 어플리케이션 스토어의 서버, 또는 중계 서버의 메모리와 같은 저장 매체에 적어도 일시 저장되거나, 임시적으로 생성될 수 있다. 다양한 실시 예들에 따른 구성 요소(예: 모듈 또는 프로그램) 각각은 단수 또는 복수의 개체로 구성될 수 있으며, 전술한 해당 서브 구성 요소들 중 일부 서브 구성 요소가 생략되거나, 또는 다른 서브 구성 요소가 다양한 실시 예에 더 포함될 수 있다. 대체적으로 또는 추가적으로, 일부 구성 요소들(예: 모듈 또는 프로그램)은 하나의 개체로 통합되어, 통합되기 이전의 각각의 해당 구성 요소에 의해 수행되는 기능을 동일 또는 유사하게 수행할 수 있다. 다양한 실시 예들에 따른, 모듈, 프로그램 또는 다른 구성 요소에 의해 수행되는 동작들은 순차적, 병렬적, 반복적 또는 휴리스틱하게 실행되거나, 적어도 일부 동작이 다른 순서로 실행되거나, 생략되거나, 또는 다른 동작이 추가될 수 있다.

도면

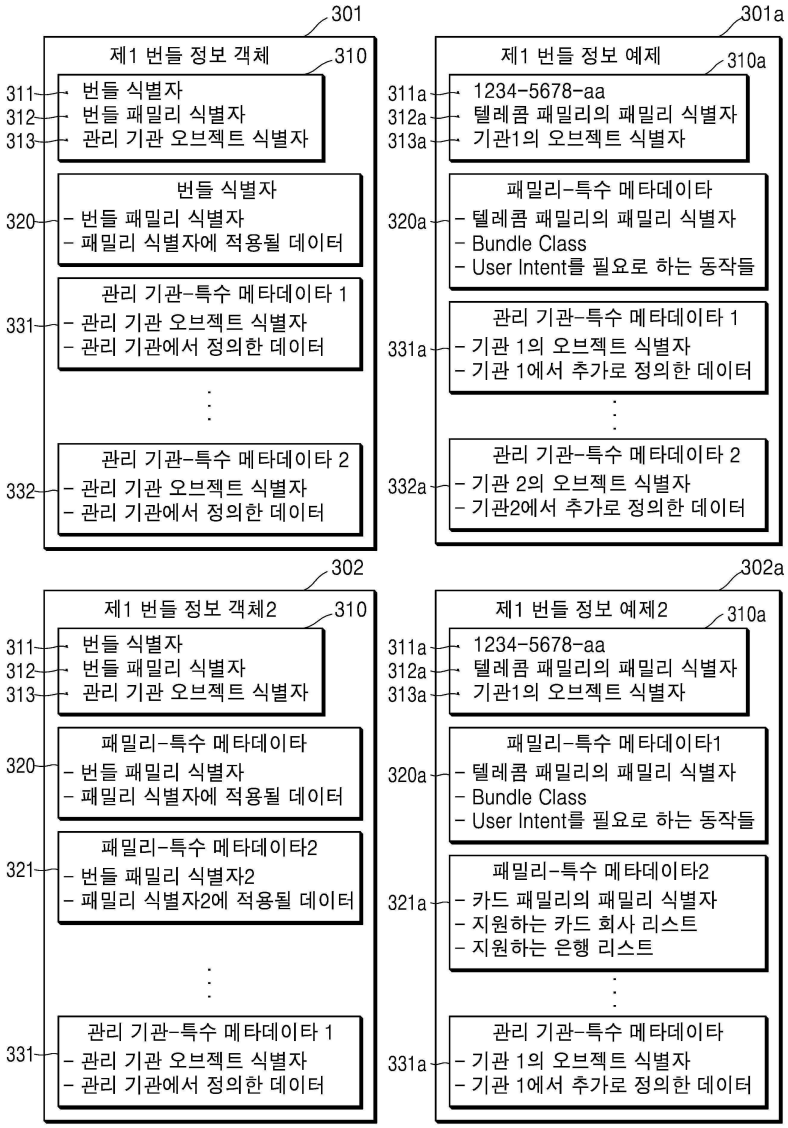
도면1



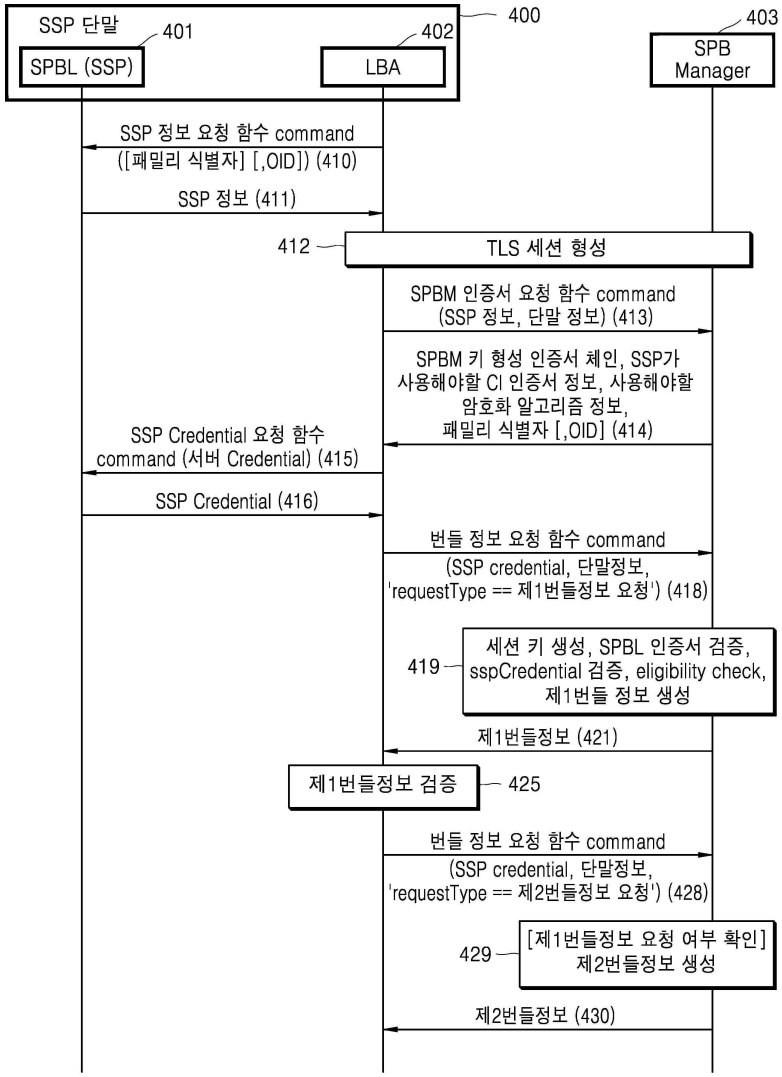
도면2


User
Service Provider
SPB Manager
단말
SSP
LBA (Local Bundle Assistant)
Primary Platform
Primary Platform Interface
SPB #1
SPB #2
SPB #3
SPB #4
System SPB
SPB Loader
Telecom#1
Telecom#2
Card
eID
OS
Bundle 설치
다운로드할 번들 정보 입력
서비스 가입
Bundle 제작 요구사항 전달
200
201
202
203
204
205
206
207
210
211
221
222
231

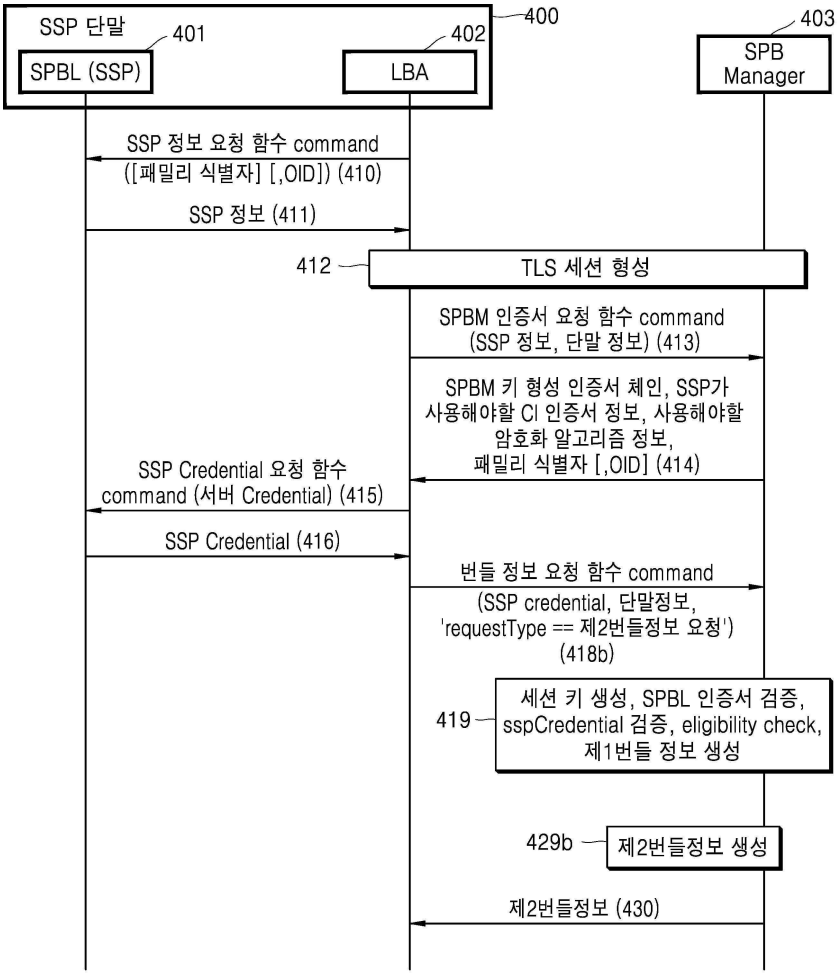
도면3


301
제1 번들 정보 객체
310
311 번들 식별자
312 번들 패밀리 식별자
313 관리 기관 오브젝트 식별자
번들 식별자
320 - 번들 패밀리 식별자
- 패밀리 식별자에 적용될 데이터
관리 기관-특수 메타데이타 1
331 - 관리 기관 오브젝트 식별자
- 관리 기관에서 정의한 데이터
관리 기관-특수 메타데이타 2
332 - 관리 기관 오브젝트 식별자
- 관리 기관에서 정의한 데이터
301a
제1 번들 정보 예제
310a
311a 1234-5678-aa
312a 텔레콤 패밀리의 패밀리 식별자
313a 기관1의 오브젝트 식별자
패밀리-특수 메타데이타
320a - 텔레콤 패밀리의 패밀리 식별자
- Bundle Class
- User Intent를 필요로 하는 동작들
관리 기관-특수 메타데이타 1
331a - 기관 1의 오브젝트 식별자
- 기관 1에서 추가로 정의한 데이터
관리 기관-특수 메타데이타 2
332a - 기관 2의 오브젝트 식별자
- 기관2에서 추가로 정의한 데이터
302
제1 번들 정보 객체2
310
311 번들 식별자
312 번들 패밀리 식별자
313 관리 기관 오브젝트 식별자
패밀리-특수 메타데이타
320 - 번들 패밀리 식별자
- 패밀리 식별자에 적용될 데이터
패밀리-특수 메타데이타2
321 - 번들 패밀리 식별자2
- 패밀리 식별자2에 적용될 데이터
관리 기관-특수 메타데이타 1
331 - 관리 기관 오브젝트 식별자
- 관리 기관에서 정의한 데이터
302a
제1 번들 정보 예제2
310a
311a 1234-5678-aa
312a 텔레콤 패밀리의 패밀리 식별자
313a 기관1의 오브젝트 식별자
패밀리-특수 메타데이타1
320a - 텔레콤 패밀리의 패밀리 식별자
- Bundle Class
- User Intent를 필요로 하는 동작들
패밀리-특수 메타데이타2
321a - 카드 패밀리의 패밀리 식별자
- 지원하는 카드 회사 리스트
- 지원하는 은행 리스트
관리 기관-특수 메타데이타
331a - 기관 1의 오브젝트 식별자
- 기관 1에서 추가로 정의한 데이터

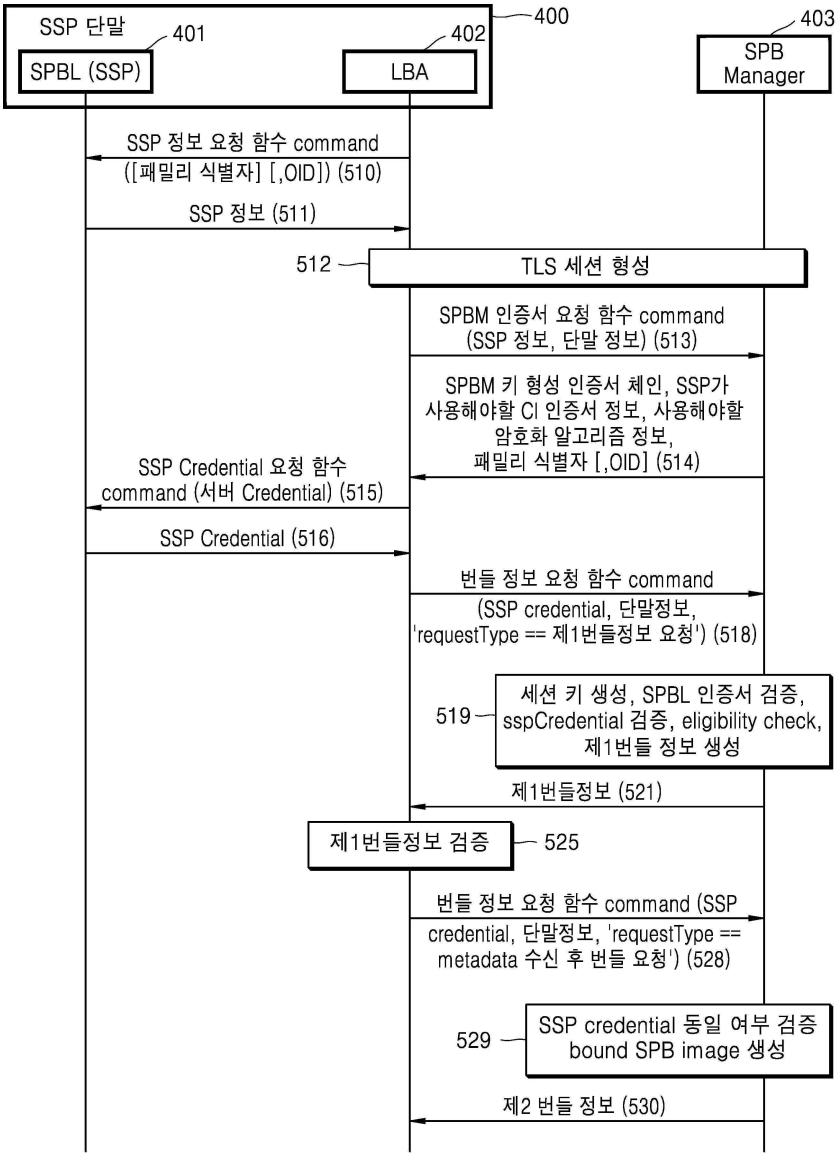
도면4a


SSP 단말
400
401
402
403
SPBL (SSP)
LBA
SPB Manager
SSP 정보 요청 함수 command ([패밀리 식별자] [,OID]) (410)
SSP 정보 (411)
412
TLS 세션 형성
SPBM 인증서 요청 함수 command (SSP 정보, 단말 정보) (413)
SPBM 키 형성 인증서 체인, SSP가 사용해야할 CI 인증서 정보, 사용해야할 암호화 알고리즘 정보, 패밀리 식별자 [,OID] (414)
SSP Credential 요청 함수 command (서버 Credential) (415)
SSP Credential (416)
번들 정보 요청 함수 command (SSP credential, 단말정보, 'requestType == 제1번들정보 요청') (418)
419
세션 키 생성, SPBL 인증서 검증, sspCredential 검증, eligibility check, 제1번들 정보 생성
제1번들정보 (421)
제1번들정보 검증
425
번들 정보 요청 함수 command (SSP credential, 단말정보, 'requestType == 제2번들정보 요청') (428)
429
[제1번들정보 요청 여부 확인] 제2번들정보 생성
제2번들정보 (430)

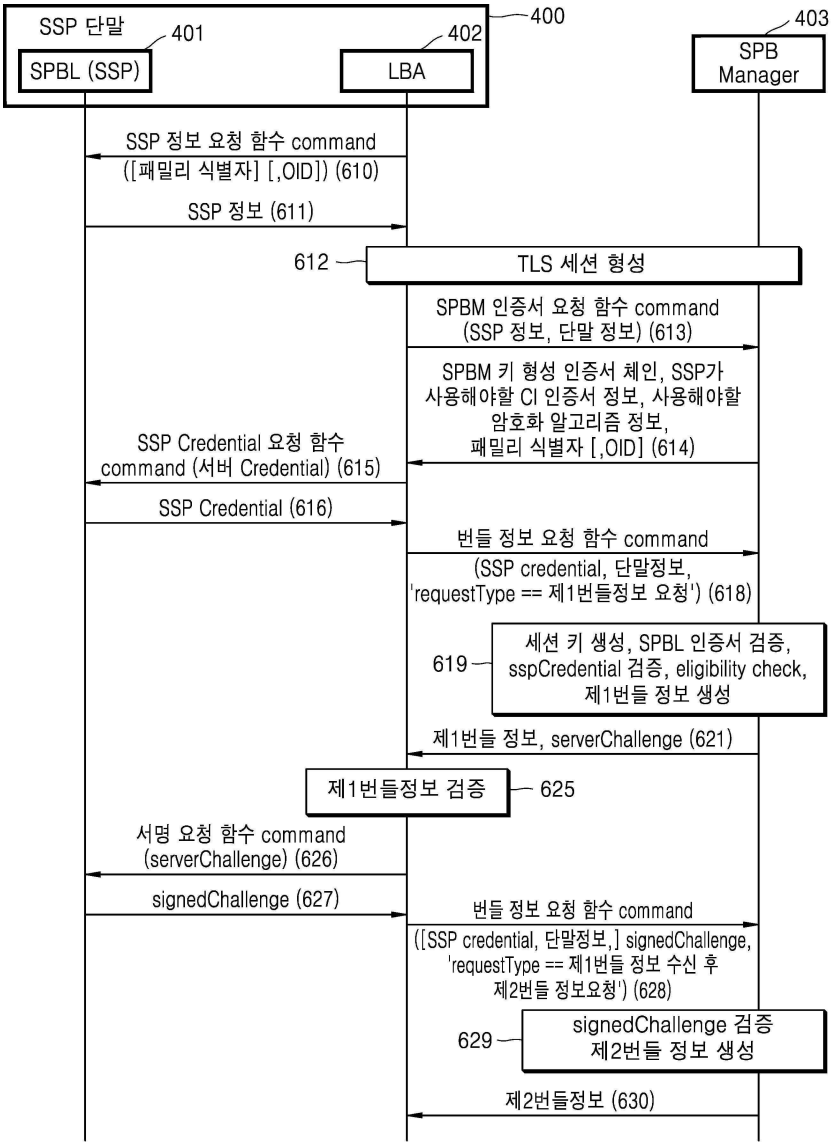
도면4b


SSP 단말
401
SPBL (SSP)
402
LBA
400
403
SPB Manager
SSP 정보 요청 함수 command ([패밀리 식별자] [,OID]) (410)
SSP 정보 (411)
412
TLS 세션 형성
SPBM 인증서 요청 함수 command (SSP 정보, 단말 정보) (413)
SPBM 키 형성 인증서 체인, SSP가 사용해야할 CI 인증서 정보, 사용해야할 암호화 알고리즘 정보, 패밀리 식별자 [,OID] (414)
SSP Credential 요청 함수 command (서버 Credential) (415)
SSP Credential (416)
번들 정보 요청 함수 command (SSP credential, 단말정보, 'requestType == 제2번들정보 요청') (418b)
419
세션 키 생성, SPBL 인증서 검증, sspCredential 검증, eligibility check, 제1번들 정보 생성
429b
제2번들정보 생성
제2번들정보 (430)

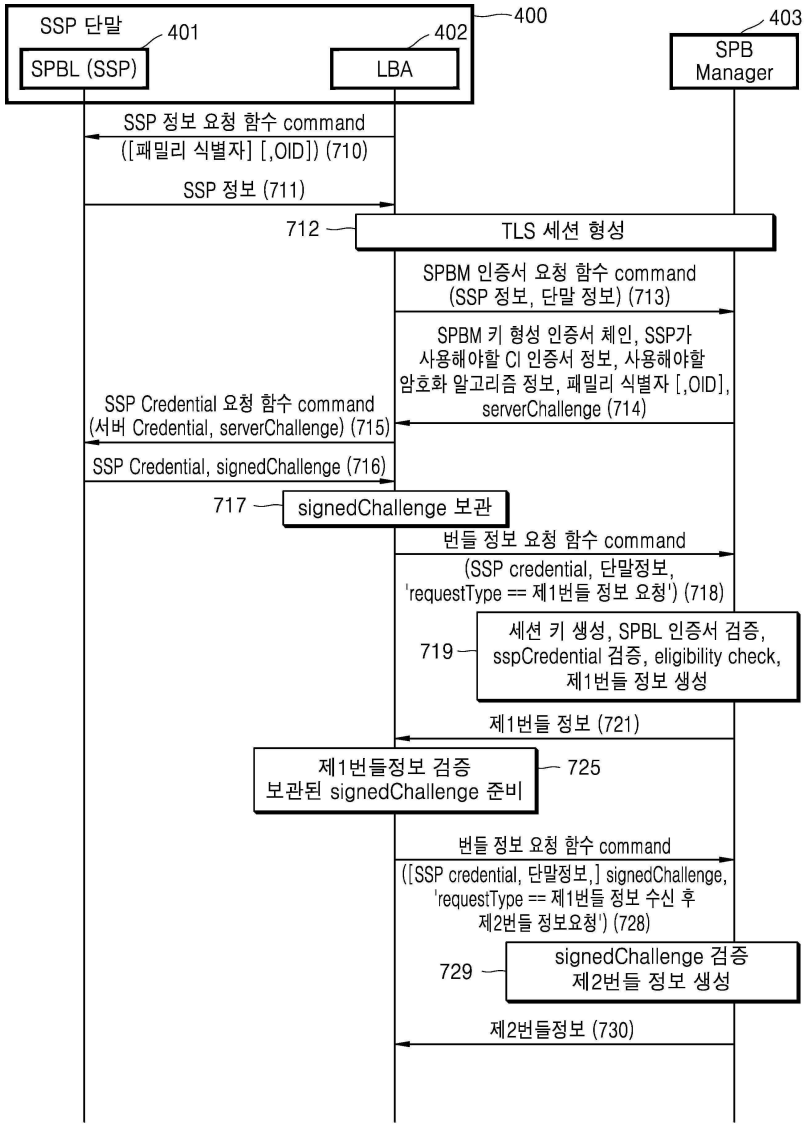
도면5


SSP 단말
401
SPBL (SSP)
402
LBA
400
403
SPB Manager
SSP 정보 요청 함수 command ([패밀리 식별자] [,OID]) (510)
SSP 정보 (511)
512
TLS 세션 형성
SPBM 인증서 요청 함수 command (SSP 정보, 단말 정보) (513)
SPBM 키 형성 인증서 체인, SSP가 사용해야할 CI 인증서 정보, 사용해야할 암호화 알고리즘 정보, 패밀리 식별자 [,OID] (514)
SSP Credential 요청 함수 command (서버 Credential) (515)
SSP Credential (516)
번들 정보 요청 함수 command (SSP credential, 단말정보, 'requestType == 제1번들정보 요청') (518)
519
세션 키 생성, SPBL 인증서 검증, sspCredential 검증, eligibility check, 제1번들 정보 생성
제1번들정보 (521)
제1번들정보 검증
525
번들 정보 요청 함수 command (SSP credential, 단말정보, 'requestType == metadata 수신 후 번들 요청') (528)
529
SSP credential 동일 여부 검증 bound SPB image 생성
제2 번들 정보 (530)

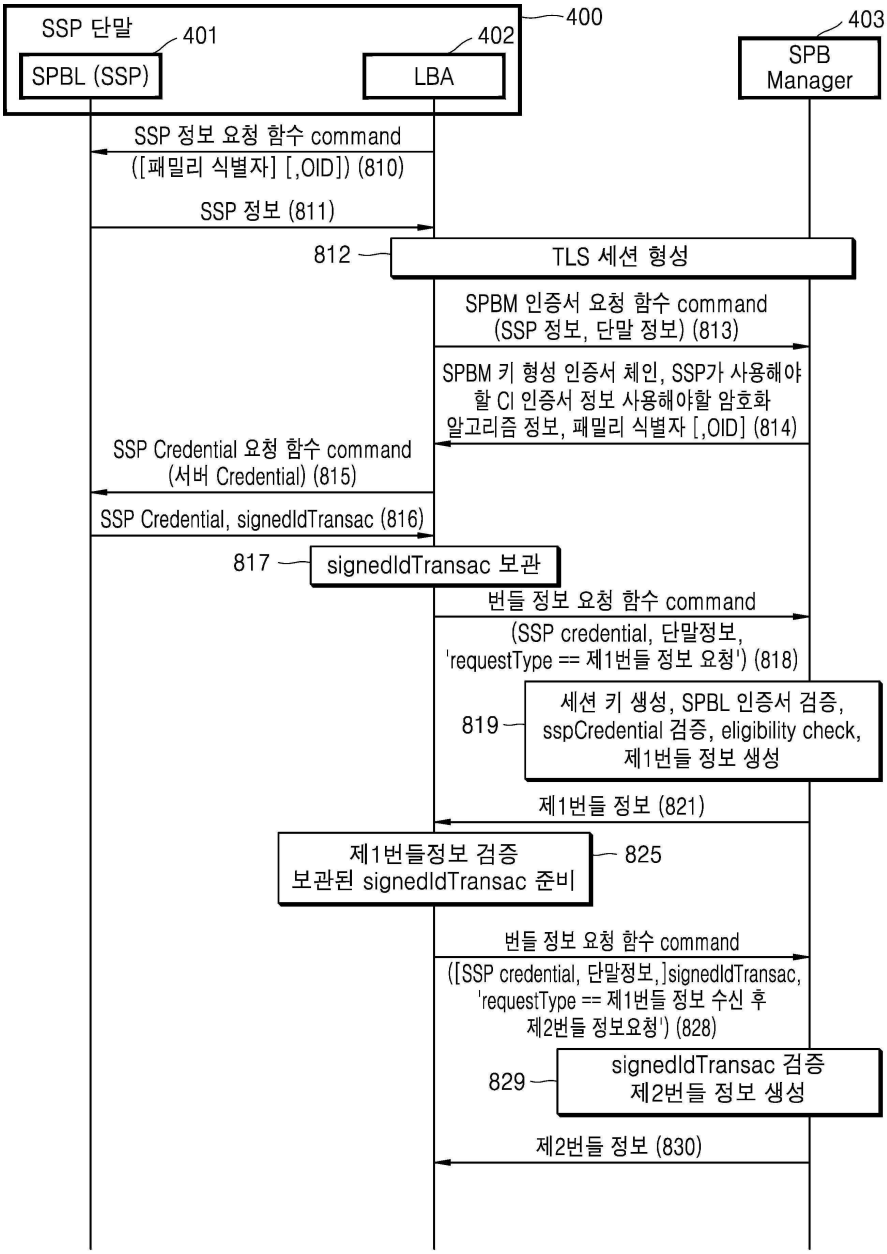
도면6


SSP 단말
401
SPBL (SSP)
402
LBA
400
403
SPB Manager
SSP 정보 요청 함수 command ([패밀리 식별자] [,OID]) (610)
SSP 정보 (611)
612
TLS 세션 형성
SPBM 인증서 요청 함수 command (SSP 정보, 단말 정보) (613)
SPBM 키 형성 인증서 체인, SSP가 사용해야할 CI 인증서 정보, 사용해야할 암호화 알고리즘 정보, 패밀리 식별자 [,OID] (614)
SSP Credential 요청 함수 command (서버 Credential) (615)
SSP Credential (616)
번들 정보 요청 함수 command (SSP credential, 단말정보, 'requestType == 제1번들정보 요청') (618)
619
세션 키 생성, SPBL 인증서 검증, sspCredential 검증, eligibility check, 제1번들 정보 생성
제1번들 정보, serverChallenge (621)
제1번들정보 검증
625
서명 요청 함수 command (serverChallenge) (626)
signedChallenge (627)
번들 정보 요청 함수 command ([SSP credential, 단말정보,] signedChallenge, 'requestType == 제1번들 정보 수신 후 제2번들 정보요청') (628)
629
signedChallenge 검증 제2번들 정보 생성
제2번들정보 (630)

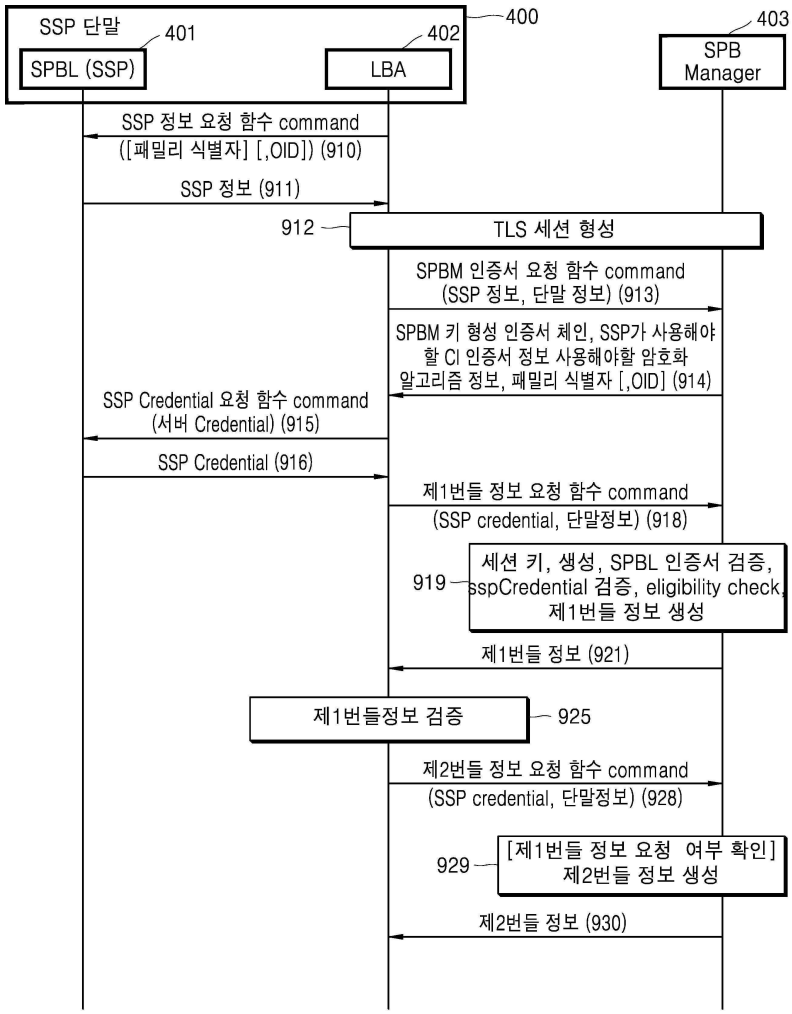
도면7


SSP 단말
400
401
402
403
SPBL (SSP)
LBA
SPB Manager
SSP 정보 요청 함수 command ([패밀리 식별자] [,OID]) (710)
SSP 정보 (711)
712
TLS 세션 형성
SPBM 인증서 요청 함수 command (SSP 정보, 단말 정보) (713)
SPBM 키 형성 인증서 체인, SSP가 사용해야할 CI 인증서 정보, 사용해야할 암호화 알고리즘 정보, 패밀리 식별자 [,OID], serverChallenge (714)
SSP Credential 요청 함수 command (서버 Credential, serverChallenge) (715)
SSP Credential, signedChallenge (716)
717
signedChallenge 보관
번들 정보 요청 함수 command (SSP credential, 단말정보, 'requestType == 제1번들 정보 요청') (718)
719
세션 키 생성, SPBL 인증서 검증, sspCredential 검증, eligibility check, 제1번들 정보 생성
제1번들 정보 (721)
제1번들정보 검증 보관된 signedChallenge 준비
725
번들 정보 요청 함수 command ([SSP credential, 단말정보,] signedChallenge, 'requestType == 제1번들 정보 수신 후 제2번들 정보요청') (728)
729
signedChallenge 검증 제2번들 정보 생성
제2번들정보 (730)

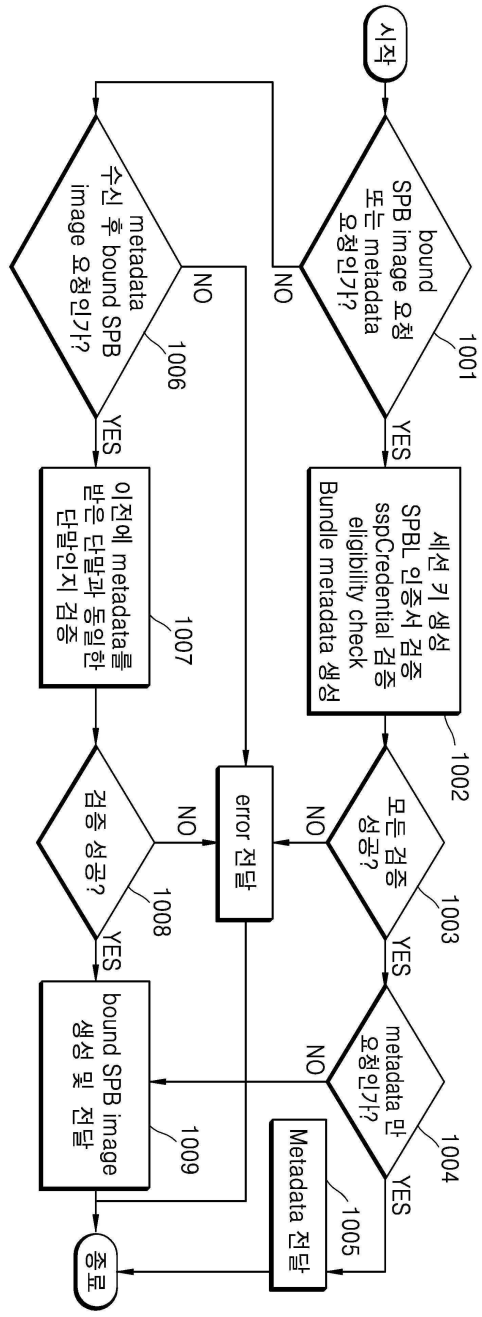
도면8


SSP 단말
401
SPBL (SSP)
402
LBA
400
403
SPB Manager
SSP 정보 요청 함수 command ([패밀리 식별자] [,OID]) (810)
SSP 정보 (811)
812
TLS 세션 형성
SPBM 인증서 요청 함수 command (SSP 정보, 단말 정보) (813)
SPBM 키 형성 인증서 체인, SSP가 사용해야 할 CI 인증서 정보 사용해야할 암호화 알고리즘 정보, 패밀리 식별자 [,OID] (814)
SSP Credential 요청 함수 command (서버 Credential) (815)
SSP Credential, signedIdTransac (816)
817
signedIdTransac 보관
번들 정보 요청 함수 command (SSP credential, 단말정보, 'requestType == 제1번들 정보 요청') (818)
819
세션 키 생성, SPBL 인증서 검증, sspCredential 검증, eligibility check, 제1번들 정보 생성
제1번들 정보 (821)
제1번들정보 검증 보관된 signedIdTransac 준비
825
번들 정보 요청 함수 command ([SSP credential, 단말정보,]signedIdTransac, 'requestType == 제1번들 정보 수신 후 제2번들 정보요청') (828)
829
signedIdTransac 검증 제2번들 정보 생성
제2번들 정보 (830)

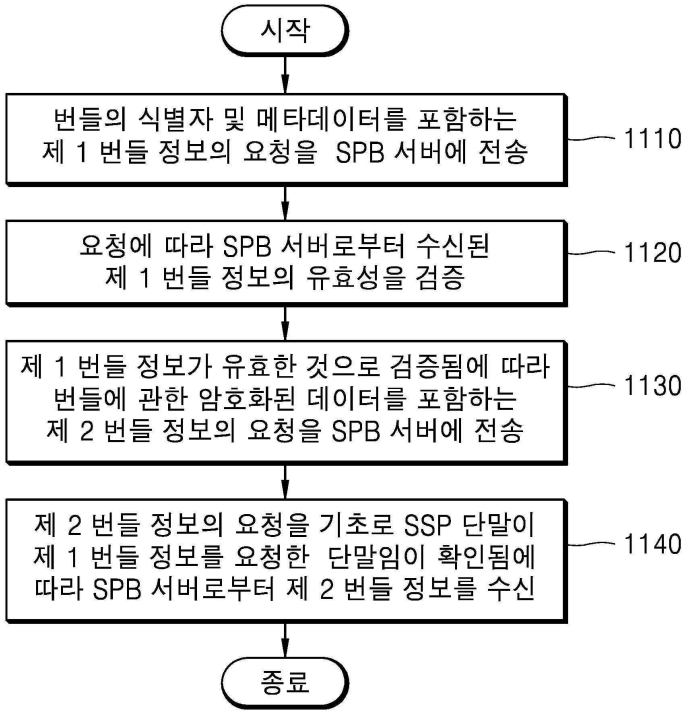
도면9


SSP 단말
400
401
402
403
SPBL (SSP)
LBA
SPB Manager
SSP 정보 요청 함수 command ([패밀리 식별자] [,OID]) (910)
SSP 정보 (911)
912
TLS 세션 형성
SPBM 인증서 요청 함수 command (SSP 정보, 단말 정보) (913)
SPBM 키 형성 인증서 체인, SSP가 사용해야 할 CI 인증서 정보 사용해야할 암호화 알고리즘 정보, 패밀리 식별자 [,OID] (914)
SSP Credential 요청 함수 command (서버 Credential) (915)
SSP Credential (916)
제1번들 정보 요청 함수 command (SSP credential, 단말정보) (918)
919
세션 키, 생성, SPBL 인증서 검증, sspCredential 검증, eligibility check, 제1번들 정보 생성
제1번들 정보 (921)
제1번들정보 검증
925
제2번들 정보 요청 함수 command (SSP credential, 단말정보) (928)
929
[제1번들 정보 요청 여부 확인] 제2번들 정보 생성
제2번들 정보 (930)

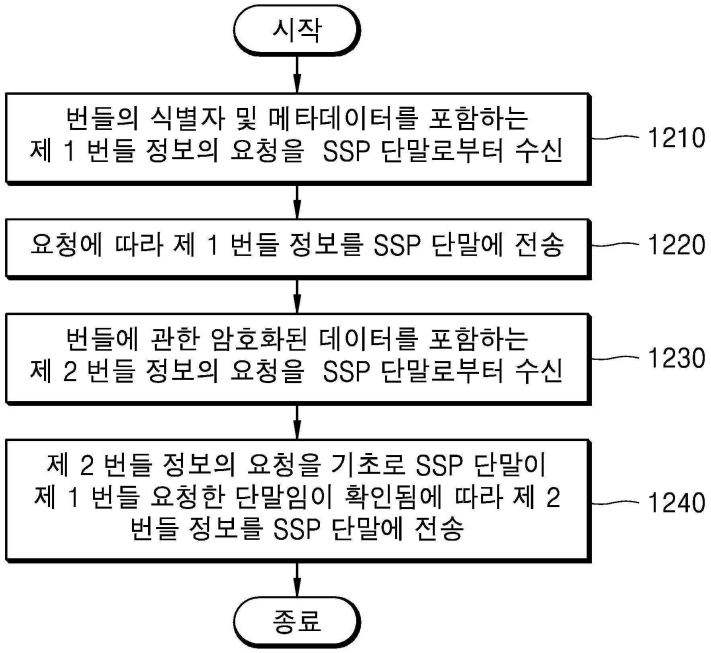
도면10


시작
bound SPB image 요청 또는 metadata 요청인가?
1001
YES
NO
세션 키 생성
SPBL 인증서 검증
sspCredential 검증
eligibility check
Bundle metadata 생성
1002
모든 검증 성공?
1003
YES
NO
metadata 만 요청인가?
1004
YES
NO
Metadata 전달
1005
종료
metadata 수신 후 bound SPB image 요청인가?
1006
YES
NO
이전에 metadata를 받은 단말과 동일한 단말인지 검증
1007
검증 성공?
1008
YES
NO
bound SPB image 생성 및 전달
1009
error 전달

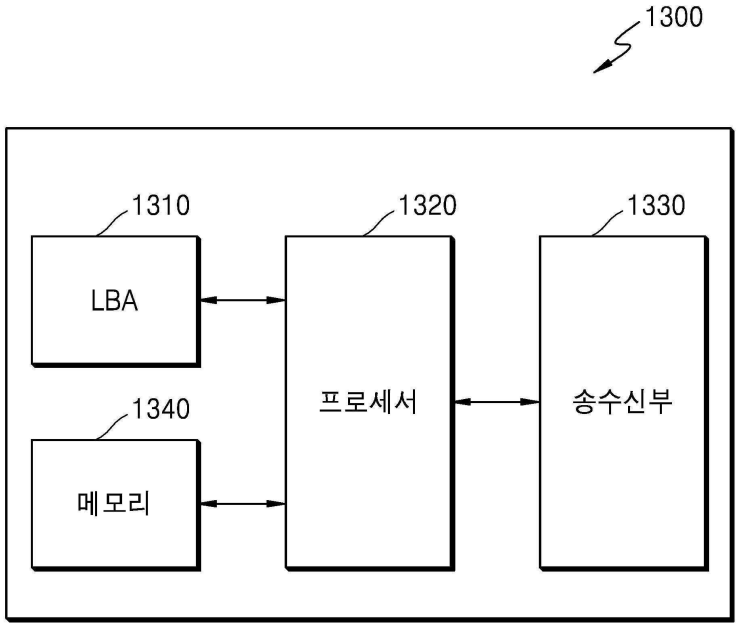
도면11


시작
번들의 식별자 및 메타데이터를 포함하는 제 1 번들 정보의 요청을 SPB 서버에 전송
1110
요청에 따라 SPB 서버로부터 수신된 제 1 번들 정보의 유효성을 검증
1120
제 1 번들 정보가 유효한 것으로 검증됨에 따라 번들에 관한 암호화된 데이터를 포함하는 제 2 번들 정보의 요청을 SPB 서버에 전송
1130
제 2 번들 정보의 요청을 기초로 SSP 단말이 제 1 번들 정보를 요청한 단말임이 확인됨에 따라 SPB 서버로부터 제 2 번들 정보를 수신
1140
종료

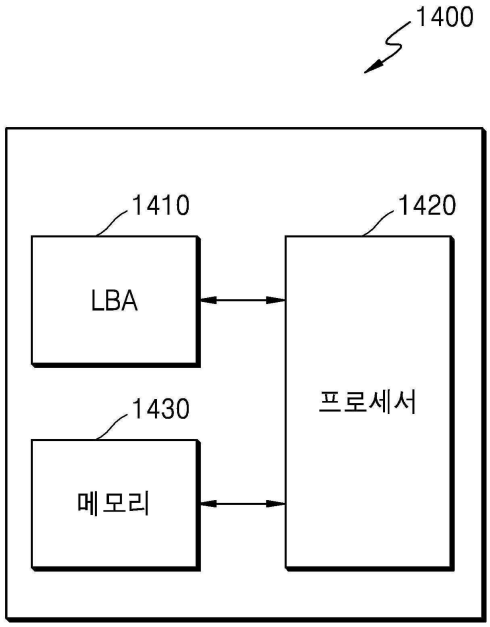
도면12


시작
번들의 식별자 및 메타데이터를 포함하는 제 1 번들 정보의 요청을 SSP 단말로부터 수신
1210
요청에 따라 제 1 번들 정보를 SSP 단말에 전송
1220
번들에 관한 암호화된 데이터를 포함하는 제 2 번들 정보의 요청을 SSP 단말로부터 수신
1230
제 2 번들 정보의 요청을 기초로 SSP 단말이 제 1 번들 요청한 단말임이 확인됨에 따라 제 2 번들 정보를 SSP 단말에 전송
1240
종료

도면13


1300
1310
LBA
1320
프로세서
1330
송수신부
1340
메모리

도면14


1400
1410
LBA
1420
프로세서
1430
메모리