(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0143714
(43) 공개일자 2013년12월31일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) *H04W 12/08* (2009.01)
(21) 출원번호 10-2013-7026594
(22) 출원일자(국제) 2012년03월09일
심사청구일자 2013년10월08일
(85) 번역문제출일자 2013년10월08일
(86) 국제출원번호 PCT/US2012/028611
(87) 국제공개번호 WO 2012/122529
국제공개일자 2012년09월13일
(30) 우선권주장
13/213,401 2011년08월19일 미국(US)
61/450,956 2011년03월09일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
팔라니고운데르 아난드
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775
타이드만 에드워드 조지
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775
나시엘스키 존 월라스
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인코리아나

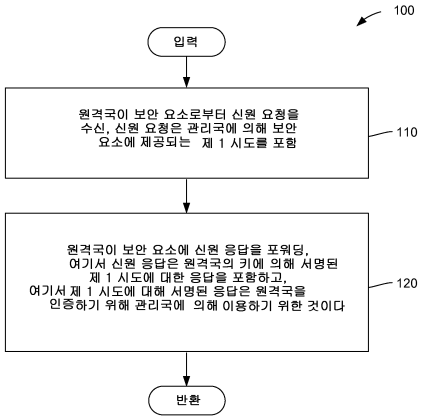
전체 청구항 수 : 총 40 항

(54) 발명의 명칭 **보안 요소를 이용하는 원격국의 인증 방법**

(57) 요 약

보안 요소를 이용하는 관리국에 의한 원격국의 인증 방법이 개시된다. 그 방법에서, 원격국은 보안 요소로부터 신원 요청을 수신한다. 신원 요청은 관리국에 의해 보안 요소에 제공되는 제 1 시도를 포함한다. 원격국은 보안 요소에 신원 응답을 포워딩한다. 신원 응답은 원격국의 키에 의해 서명된 제 1 시도에 대한 응답을 포함하고, 제 1 시도에 대한 서명된 응답은 원격국을 인증하기 위해 관리국에 의해 이용된다.

대 표 도 - 도1



특허청구의 범위

청구항 1

보안 요소를 이용하는 관리국에 의한 원격국의 인증 방법으로서,

상기 원격국이 상기 보안 요소로부터 신원 요청을 수신하는 단계로서, 상기 신원 요청은 상기 관리국에 의해 상기 보안 요소에 제공되는 제 1 시도를 포함하는, 상기 원격국이 상기 보안 요소로부터 신원 요청을 수신하는 단계; 및

상기 원격국이 상기 보안 요소에 신원 응답을 포워딩하는 단계로서, 상기 신원 응답은 상기 원격국의 키에 의해 서명된 상기 제 1 시도에 대한 응답을 포함하고, 상기 제 1 시도에 대한 서명된 상기 응답은 상기 원격국을 인증하기 위해 상기 관리국에 의해 이용하기 위한 것인, 상기 원격국이 상기 보안 요소에 신원 응답을 포워딩하는 단계를 포함하는, 원격국의 인증 방법.

청구항 2

제 1 항에 있어서,

상기 보안 요소는 상기 원격국에 내장되는 스마트카드인, 원격국의 인증 방법.

청구항 3

제 1 항에 있어서,

상기 보안 요소는 상기 원격국으로부터 제거가능한 스마트카드인, 원격국의 인증 방법.

청구항 4

제 1 항에 있어서,

상기 보안 요소는 상기 원격국 내에 구비된 신뢰 프로세서 모듈 (Trusted Processor Module) 인, 원격국의 인증 방법.

청구항 5

제 1 항에 있어서,

상기 원격국은 무선 모바일 디바이스인, 원격국의 인증 방법.

청구항 6

제 1 항에 있어서,

상기 원격국의 키는 상기 관리국이 이용가능한 공개 키에 대응하는 개인 키인, 원격국의 인증 방법.

청구항 7

제 6 항에 있어서,

상기 신원 응답은 상기 공개 키를 포함하는 인증서를 포함하는, 원격국의 인증 방법.

청구항 8

제 1 항에 있어서,

상기 원격국의 키는 상기 관리국에 의해 공유되는 비밀 키인, 원격국의 인증 방법.

청구항 9

제 1 항에 있어서,

상기 신원 응답은 상기 원격국에 고유한 신원 값을 포함하는, 원격국의 인증 방법.

청구항 10

제 1 항에 있어서,

상기 제 1 시도는 제 1 넌스 (nonce) 인, 원격국의 인증 방법.

청구항 11

제 1 항에 있어서,

상기 신원 응답은 상기 관리국을 인증할 시에 이용하기 위해 상기 원격국에 의해 생성된 제 2 시도를 포함하는, 원격국의 인증 방법.

청구항 12

보안 요소로부터 신원 요청을 수신하기 위한 수단으로서, 상기 신원 요청은 관리국에 의해 상기 보안 요소에 제공되는 제 1 시도를 포함하는, 상기 보안 요소로부터 신원 요청을 수신하기 위한 수단; 및

상기 보안 요소에 신원 응답을 포워딩하기 위한 수단으로서, 상기 신원 응답은 상기 원격국의 키에 의해 서명된 상기 제 1 시도에 대한 응답을 포함하고, 상기 제 1 시도에 대한 서명된 상기 응답은 상기 원격국을 인증하기 위해 상기 관리국에 의해 이용하기 위한 것인, 상기 보안 요소에 신원 응답을 포워딩하기 위한 수단을 포함하는, 원격국.

청구항 13

제 12 항에 있어서,

상기 보안 요소는 상기 원격국에 내장되는 스마트카드인, 원격국.

청구항 14

제 12 항에 있어서,

상기 보안 요소는 상기 원격국으로부터 제거가능한 스마트카드인, 원격국.

청구항 15

제 12 항에 있어서,

상기 보안 요소는 상기 원격국 내에 구비된 신뢰 프로세서 모듈 (Trusted Processor Module) 인, 원격국.

청구항 16

제 12 항에 있어서,

상기 원격국은 무선 모바일 디바이스인, 원격국.

청구항 17

제 12 항에 있어서,

상기 원격국의 키는 상기 관리국이 이용가능한 공개 키에 대응하는 개인 키인, 원격국.

청구항 18

제 17 항에 있어서,

상기 신원 응답은 상기 공개 키를 포함하는 인증서를 포함하는, 원격국.

청구항 19

제 12 항에 있어서,

상기 원격국의 키는 상기 관리국에 의해 공유되는 비밀 키인, 원격국.

청구항 20

제 12 항에 있어서,

상기 신원 응답은 상기 원격국에 고유한 신원 값을 포함하는, 원격국.

청구항 21

제 12 항에 있어서,

상기 제 1 시도는 제 1 넌스 (nonce) 인, 원격국.

청구항 22

제 12 항에 있어서,

상기 신원 응답은 상기 관리국을 인증할 시에 이용하기 위해 상기 원격국에 의해 생성된 제 2 시도를 포함하는, 원격국.

청구항 23

원격국으로서,

보안 요소로부터 신원 요청을 수신하고, 상기 보안 요소에 신원 응답을 포워딩하도록 구성되는 프로세서; 및

상기 원격국의 키를 저장하도록 구성되는 메모리를 포함하고,

상기 신원 요청은 관리국에 의해 상기 보안 요소에 제공되는 제 1 시도를 포함하며,

상기 신원 응답은 상기 원격국의 키에 의해 서명된 상기 제 1 시도에 대한 응답을 포함하고, 상기 제 1 시도에 대한 서명된 상기 응답은 상기 원격국을 인증하기 위해 상기 관리국에 의해 이용하기 위한 것인, 원격국

청구항 24

제 23 항에 있어서,

상기 보안 요소는 상기 원격국에 내장되는 스마트카드인, 원격국.

청구항 25

제 23 항에 있어서,

상기 보안 요소는 상기 원격국으로부터 제거가능한 스마트카드인, 원격국.

청구항 26

제 23 항에 있어서,

상기 보안 요소는 상기 원격국 내에 구비된 신뢰 프로세서 모듈 (Trusted Processor Module) 인, 원격국.

청구항 27

제 23 항에 있어서,

상기 원격국은 무선 모바일 디바이스인, 원격국.

청구항 28

제 23 항에 있어서,

상기 원격국의 키는 상기 관리국이 이용가능한 공개 키에 대응하는 개인 키인, 원격국.

청구항 29

제 28 항에 있어서,

상기 신원 응답은 상기 공개 키를 포함하는 인증서를 포함하는, 원격국.

청구항 30

제 23 항에 있어서,

상기 원격국의 키는 상기 관리국에 의해 공유되는 비밀 키인, 원격국.

청구항 31

제 23 항에 있어서,

상기 신원 응답은 상기 원격국에 고유한 신원 값을 포함하는, 원격국.

청구항 32

제 23 항에 있어서,

상기 제 1 시도는 제 1 넌스 (nonce) 인, 원격국.

청구항 33

제 23 항에 있어서,

상기 신원 응답은 상기 관리국을 인증할 시에 이용하기 위해 상기 원격국에 의해 생성된 제 2 시도를 포함하는, 원격국.

청구항 34

컴퓨터 판독가능 매체를 포함하는 컴퓨터 프로그램 제품으로서,

상기 컴퓨터 판독가능 매체는,

컴퓨터로 하여금 보안 요소로부터 신원 요청을 수신하도록 하기 위한 코드로서, 상기 신원 요청은 상기 관리국에 의해 상기 보안 요소에 제공되는 제 1 시도를 포함하는, 상기 컴퓨터로 하여금 보안 요소로부터 신원 요청을 수신하도록 하기 위한 코드; 및

컴퓨터로 하여금 상기 보안 요소에 신원 응답을 포워딩하도록 하기 위한 코드로서, 상기 신원 응답은 상기 컴퓨터와 연관된 키에 의해 서명된 상기 제 1 시도에 대한 응답을 포함하고, 상기 제 1 시도에 대한 서명된 상기 응답은 상기 컴퓨터를 인증하기 위해 상기 관리국에 의해 이용하기 위한 것인, 상기 컴퓨터로 하여금 상기 보안 요소에 신원 응답을 포워딩하도록 하기 위한 코드를 포함하는, 컴퓨터 판독가능 매체를 포함하는 컴퓨터 프로그램 제품.

청구항 35

제 34 항에 있어서,

상기 보안 요소는 스마트카드인, 컴퓨터 판독가능 매체를 포함하는 컴퓨터 프로그램 제품.

청구항 36

제 34 항에 있어서,

상기 보안 요소는 제거가능한 스마트카드인, 컴퓨터 판독가능 매체를 포함하는 컴퓨터 프로그램 제품.

청구항 37

제 34 항에 있어서,

상기 보안 요소는 신뢰 프로세서 모듈 (Trusted Processor Module) 인, 컴퓨터 판독가능 매체를 포함하는 컴퓨터 프로그램 제품.

청구항 38

제 34 항에 있어서,

상기 키는 상기 관리국이 이용가능한 공개 키에 대응하는 개인 키인, 컴퓨터 판독가능 매체를 포함하는 컴퓨터 프로그램 제품.

청구항 39

제 34 항에 있어서,

상기 키는 상기 관리국에 의해 공유되는 비밀 키인, 컴퓨터 판독가능 매체를 포함하는 컴퓨터 프로그램 제품.

청구항 40

제 34 항에 있어서,

상기 제 1 시도는 제 1 넌스 (nonce) 인, 컴퓨터 판독가능 매체를 포함하는 컴퓨터 프로그램 제품.

명 세 서

기 술 분 야

[0001] **관련 출원의 상호 참조**

[0002] 본 출원은, 본원에 참조로 포함된 출원인, 2011 년 3 월 9 일에 출원된, 미국 가출원 제 61/450,956 호의 혜택을 주장한다.

[0003] **기술분야**

[0004] 본 발명은 일반적으로 원격국의 인증에 관한 것이다.

배 경 기 술

[0005] 원격국은 무선 네트워크 오퍼레이터에 의해 제공되는 사용자 서비스들을 호스팅할 수도 있다. GSM, UMTS, LTE 및 cdma2000 시스템들에서, 사용자 서비스들은 스마트 카드를 이용하여 가능하게 될 수도 있다. 스마트 카드의 예는 범용 집적 회로 카드 (Universal Integrated Circuit Card; UICC) 일 수도 있다. UICC 는 제거가능하여, UICC 가 다른 기지국 또는 디바이스로 이동되는 것을 허용할 수도 있다. 무선 네트워크 오퍼레이터는 과도한 비용 없이 호스팅 원격국을 인증하길 원할 수도 있다.

발명의 내용

해결하려는 과제

[0006] 따라서, 원격국을 인증하기 위한 효과적인 기법에 대한 필요성이 있다.

과제의 해결 수단

[0007] 본 발명의 일 양상은 보안 요소를 이용하는 관리국에 의한 원격국의 인증 방법에 있을 수도 있다. 그 방법에서, 원격국은 보안 요소로부터 신원 요청을 수신한다. 신원 요청은 관리국에 의해 보안 요소에 제공되는 제 1 시도 (challenge) 를 포함한다. 원격국은 보안 요소에 신원 응답을 포워딩한다. 신원 응답은 원격국의 키에 의해 서명된 제 1 시도에 대한 응답을 포함한다. 제 1 시도에 대한 서명된 응답은 원격국을 인증하기 위해 관리국에 의해 이용된다.

[0008] 본 발명의 좀더 세부적인 양상들에서, 보안 요소는 원격국에 내장되는 스마트카드, 원격국으로부터 제거가능한 스마트카드, 또는 원격국 내에 구비된 신뢰 프로세서 모듈 (Trusted Processor Module) 일 수도 있다. 원격국은 무선 모바일 디바이스일 수도 있다. 원격국의 키는 관리국이 이용가능한 공개 키에 대응하는 개인 키일 수도 있고, 신원 응답은 공개 키를 포함하는 인증서를 포함할 수도 있다. 대안으로, 원격국의 키는 관리국에 의해 공유되는 비밀 키일 수도 있다. 신원 응답은 원격국에 고유한 신원 값을 포함할 수도 있다. 제 1 시도는 제 1 넌스 (nonce) 일 수도 있다. 또한, 신원 응답은 관리국을 인증하는데 이용하기 위해 원격

국에 의해 생성된 제 2 시도를 포함할 수도 있다.

[0009] 본 발명의 다른 양상은, 보안 요소로부터 신원 요청을 수신하기 위한 수단 (신원 요청은 관리국에 의해 보안 요소에 제공되는 제 1 시도를 포함한다), 및 보안 요소에 신원 응답을 포워딩하기 위한 수단을 포함할 수도 있는 원격국에 있을 수도 있는데, 여기서 신원 응답은 원격국의 키에 의해 서명된 제 1 시도에 대한 응답을 포함하고, 여기서 제 1 시도에 대한 서명된 응답은 원격국을 인증하기 위해 관리국에 의해 이용된다.

[0010] 본 발명의 다른 양상은, 보안 요소로부터 신원 요청을 수신하고 (신원 요청은 관리국에 의해 보안 요소에 제공되는 제 1 시도를 포함한다), 보안 요소에 신원 응답을 포워딩하도록 구성되는 프로세서 (여기서 신원 응답은 원격국의 키에 의해 서명된 제 1 시도에 대한 응답을 포함하고, 여기서 제 1 시도에 대한 서명된 응답은 원격국을 인증하기 위해 관리국에 의해 이용된다); 및 원격국의 키를 저장하도록 구성되는 메모리를 포함할 수도 있는 원격국에 있을 수도 있다.

[0011] 본 발명의 다른 양상은, 컴퓨터로 하여금 보안 요소로부터 신원 요청을 수신하도록 하는 코드 (신원 요청은 관리국에 의해 보안 요소에 제공되는 제 1 시도를 포함한다); 및 컴퓨터로 하여금 보안 요소에 신원 응답을 포워딩하도록 하는 코드를 포함하는, 컴퓨터 판독가능 저장 매체를 포함하는, 컴퓨터 프로그램 제품에 있을 수도 있는데, 여기서 신원 응답은 컴퓨터와 연관된 키에 의해 서명된 제 1 시도에 대한 응답을 포함하고, 여기서 제 1 시도에 대한 서명된 응답은 컴퓨터를 인증하기 위해 관리국에 의해 이용된다.

도면의 간단한 설명

[0012] 도 1 은, 본 발명에 따른, 보안 요소를 이용하는 관리국에 의한 원격국의 인증 방법의 플로우 다이어그램이다.

도 2 는 보안 요소를 이용하는 관리국에 의한 원격국의 인증에 대한 호 흐름의 플로우 다이어그램이다.

도 3 은 프로세서 및 메모리를 포함하는 컴퓨터의 블록 다이어그램이다.

도 4 는 무선 통신 시스템의 일 예의 블록 다이어그램이다.

발명을 실시하기 위한 구체적인 내용

[0013] 단어 "예시적인" 은 본원에서 "일 예, 사례, 또는 실례의 역할을 하는" 것을 의미하기 위해 이용된다. "예시적" 으로 본원에서 설명된 임의의 실시형태는 반드시 다른 실시형태들보다 바람직하거나 이로운 것으로 해석되지는 않는다.

[0014] 도 1 및 도 2 를 참조하면, 본 발명의 일 양상은 보안 요소 (230) 를 이용하는 관리국 (220) 에 의한 원격국 (210) 의 인증 방법 (100) 에 있을 수도 있다. 그 방법에서, 원격국은 보안 요소로부터 신원 요청 (REQ ID) 을 수신한다 (단계 110). 신원 요청은 관리국에 의해 보안 요소에 제공되는 제 1 시도 (N1) 를 포함한다. 원격국은 보안 요소에 신원 응답 (ID RES) 을 포워딩한다 (단계 120). 신원 응답은 원격국의 키 (K) 에 의해 서명된 제 1 시도에 대한 응답을 포함한다. 서명된 응답은 원격국을 인증하기 위해 관리국에 의해 이용된다.

[0015] 본 발명의 좀더 세부적인 양상들에서, 보안 요소 (230) 는 원격국 (210) 에 내장되는 스마트카드, 원격국으로부터 제거가능한 스마트카드, 또는 원격국 내에 구비된 신뢰 프로세서 모듈일 수도 있다. 원격국은 무선 디바이스와 같은 모바일 사용자 기기 (user equipment; UE) 를 포함할 수도 있다. 원격국의 키 (K) 는 관리국이 이용가능한 공개 키에 대응하는 개인 키 (K_{PRI}) 일 수도 있고, 신원 응답은 공개 키를 포함하는 인증서 (CERT) 를 포함할 수도 있다. 대안으로, 원격국의 키는 관리국 (220) 에 의해 공유되는 비밀 키 (K_{SH}) 일 수도 있다. 신원 응답은 국제 모바일 기기 식별번호 (International Mobile Equipment Identity; IMEI), 또는 모바일 기기 식별번호 (Mobile Equipment Identity; MEID) 와 같이 원격국에 고유한 신원 값, 또는 원격국을 고유하게 항상 식별하는 임의의 다른 신원을 포함할 수도 있다. 이러한 신원들의 다른 예들은 EUI-48 또는 EUI-64 와 같이 IEEE 에 의해 할당되거나 원격국의 제조자에 의해 할당된 하드웨어 식별자들을 포함할 수도 있으나, 이로 제한되지는 않는다. 제 1 시도 (N1) 는 제 1 넌스일 수도 있다. 또한, 신원 응답은, 관리국을 인증하는데 이용하기 위해 원격국에 의해 생성된, 제 2 넌스와 같은 제 2 시도를 포함할 수도 있다.

[0016] 도 3 을 더 참조하면, 본 발명의 다른 양상은, 보안 요소로부터 신원 요청을 수신하기 위한 수단 (프로세서 (310)) (신원 요청은 관리국에 의해 보안 요소에 제공되는 제 1 시도를 포함한다), 및 보안 요소에 신원 응답을 포워딩하기 위한 수단 (310) 을 포함할 수도 있는 원격국 (210) 에 있을 수도 있는데, 여기서 신원 응답은 원격

국의 키에 의해 서명된 제 1 시도에 대한 응답을 포함하고, 여기서 제 1 시도에 대한 서명된 응답은 원격국을 인증하기 위해 관리국에 의해 이용된다.

[0017] 본 발명의 다른 양상은, 보안 요소로부터 신원 요청을 수신하고 (신원 요청은 관리국에 의해 보안 요소에 제공되는 제 1 시도를 포함한다), 보안 요소에 신원 응답을 포워딩하도록 구성되는 프로세서 (310) (여기서 신원 응답은 원격국의 키에 의해 서명된 제 1 시도에 대한 응답을 포함하고, 여기서 제 1 시도에 대한 서명된 응답은 원격국을 인증하기 위해 관리국에 의해 이용된다); 및 원격국의 키를 저장하도록 구성되는 메모리를 포함할 수도 있는 원격국 (210) 에 있을 수도 있다.

[0018] 본 발명의 다른 양상은, 컴퓨터 (300) 로 하여금 보안 요소로부터 신원 요청을 수신하도록 하는 코드 (신원 요청은 관리국에 의해 보안 요소에 제공되는 제 1 시도를 포함한다); 및 컴퓨터로 하여금 보안 요소에 대한 신원 응답을 포워딩하도록 하는 코드를 포함하는, 비일시적 컴퓨터 판독가능 저장 매체 (320) 를 포함하는, 컴퓨터 프로그램 제품에 있을 수도 있는데, 여기서 신원 응답은 컴퓨터와 연관된 키에 의해 서명된 제 1 시도에 대한 응답을 포함하고, 여기서 제 1 시도에 대한 서명된 응답은 컴퓨터를 인증하기 위해 관리국에 의해 이용된다.

[0019] 원격국 (210) 또는 장치는 프로세서 (310), 메모리 및/또는 디스크 드라이브들과 같은 저장 매체 (320), 보안 모듈 (330), 디스플레이 (340), 키보드 (350) 와 같은 입력 디바이스, 마이크, 스피커(들), 카메라 등을 구비하는 컴퓨터 (300) 를 포함할 수도 있다. 스테이션은 무선 접속부 (360) 를 포함할 수도 있다. 더불어, 스테이션은 또한 USB, 이더넷, 및 유사한 인터페이스들을 포함할 수도 있다.

[0020] 다시 도 2 를 참조하면, 고수준 호 흐름 (200) 은 관리국 (220) 에 의해 원격국 인증을 호스팅하기 위한 절차들을 도시한다. 보안 요소 (230) 는 원격국 (210) 에 부착되고, 관리국에 대한 주소들을 공급하는 스마트 카드일 수도 있다. 원격국은 보안 저장부 및 실행 환경부 (330), 예를 들어, 3GPP TS 33.320 과 같은 신뢰 환경부 (TrE) 를 갖는 모바일 기기와 같은 호스트 모듈일 수도 있다. 원격국에는 디바이스 신원으로서 IMEI 와 같은 디바이스 자격증명들, 및 안전하게 저장된 디바이스 개인 키나 공유된 비밀 키가 공급될 수도 있다. 디바이스 개인 키에 대응하는 공개 키는 디바이스 개인 키를 이용하여 이루어진 서명을 확인하길 원하는 임의의 사람에게 (예를 들어, 인증서 (CERT) 로부터) 액세스가능할 수도 있다. 이용되는 경우, 공유된 공개 키는, 마찬가지로, 관리국에 의해 안전하게 저장될 것이다. 관리국은 보안 요소에 네트워크 액세스 애플리케이션 (NAA) 들을 제공하는 보안 요소 관리자일 수도 있다. NAA 들은 무선 또는 유선 네트워크들과 같은 액세스 네트워크들로부터 서비스를 획득하는데 이용된다.

[0021] 예를 들어, 보안 요소 (230) 는 배치 전에는 네트워크 오퍼레이터 데이터와 맞춰질 수 없을 수도 있는 스마트카드 (예를 들어, SIM, UICC/eUICC, 또는 R-UIM), 또는 신뢰 프로세서 모듈 (TPM) 일 수도 있다. 스마트카드 또는 TPM 에 네트워크 액세스 자격증명 정보가 제공되기 전에 보증되고/되거나 인증된 호스트 (셀룰러 모듈/모바일 기기) 에 부착되는지를 확인하는 것이 스마트카드 또는 TPM 에 바람직할 수도 있다. 또한, 네트워크 조작자는 스마트카드 또는 TPM 이 여전히 호스트 원격국 (210) 에 부착되어 있는지 여부를 주기적으로 확인하길 원할 수도 있다. 예를 들어, 네트워크 오퍼레이터는, 불법으로 네트워크 액세스를 수신하거나 네트워크 오퍼레이터 또는 정부 관계자에 의한 추적을 피하기 위해, 스마트카드 또는 TPM 과 다른 인증되지 않은 호스트 원격국의 페어링을 방지하길 원할 수도 있다. 스마트카드 또는 TPM 을 이용하는 것은 소정의 전송 액세스 네트워크 (즉, LTE/UMTS, cdma2000, 또는 다른 이러한 무선이나 심지어 유선 액세스 네트워크) 프로토콜들에서의 변화들을 요구하지 않으면서 호스트 원격국의 인증을 허용할 수도 있다.

[0022] 호스트 원격 디바이스의 신원은 디바이스의 개인/공개 키 쌍, 또는 공유된 비밀 키와 연관될 수도 있는 임의의 디바이스 신원일 수도 있다. IMEI 이외에, 다른 예들은 MEID, EUI-64, EUI-48, 또는 임의의 다른 고유의 디바이스 신원을 포함할 수도 있다.

[0023] 관리국 (220) 은 보안 요소 (230) 에 대한 OTA (over-the-air) 관리 플랫폼을 동작시키는 엔티티일 수도 있다. 보안 요소는 ETSI SCP/3GPP 에 의해 명시된 기존의 UICC/SIM 카드 프로토콜들을 이용할 수도 있거나, GlobalPlatform 프로토콜들이나 다른 적합한 프로토콜들을 이용할 수도 있다.

[0024] 호 흐름 (200) 에서, 보안 요소 (230) 는 원격국 (210) 과의 접속을 개방하고, 관리국 (220) 과의 전송 접속을 확립하도록 원격국에 요청할 수도 있다 (단계 250). 보안 요소와 원격국 사이의 접속은 보안 요소와 원격국 사이에 끼어든 공격자로부터의 공격을 방지하도록 안전하게 보호될 수도 있다. 원격국은 관리국과의 전송 접속을 확립하기 위해 전송 시스템 (240) 을 선택한다 (단계 252). 통신 시스템은 무선 광역 액세스 네트워크 WWAN (예를 들어, cdma2000, 또는 GSM/ GPRS/UMTS/LTE 등과 같은 3GPP 액세스 시스템), 무선 근거리 네트워

크 WLAN (예를 들어, IEEE 802.11a/b/g/n 무선 네트워크), 또는 고정 네트워크 (예를 들어, PSTN, xDSL, 케이블, 이더넷, 파이버 등) 에 의해 제공되는 고정 IP 서비스일 수도 있다. 전송 접속은 IP 나 SMS, 또는 임의의 이러한 전송 프로토콜을 이용할 수도 있다. 전송 접속이 확립된다 (단계 254). 보안 요소와 관리국 (220) 은 권한설정 (provisioning) 또는 관리 메시지 교환들을 위한 전송 프로토콜을 통해 안전하게 접속될 수도 있다 (단계 256). 보안 요소와 관리국 사이에 전송되는 메시지들은, 예를 들어, 인증된 HTTPS/TLS 나, 암호화 및/또는 무결성으로 강화된 SMS 를 이용하여 암호화되고 무결성이 보호될 수도 있다.

[0025] 관리국 (220) 은 보안 요소 (230) 에 서명된 호스트 원격국 신원 요청 (REQ ID REQ) 에 대한 요청을 전송한다 (단계 258). 요청은 넌스 (N1) 를 포함한다. 보안 요소는 넌스 (N1) 를 포함하는 서명된 호스트 원격국 신원에 대한 요청을 호스트 원격국 (210) 에 전송한다 (단계 260). 원격국은 원격국의 신원 (예를 들어, 원격국의 IMEI), 넌스, 및 서명을 포함하는 서명된 신원 응답 (ID RES) 을 보안 요소에 반환한다 (단계 262). 서명된 신원 응답은 관리국을 인증하기 위한 시도로서 제 2 넌스 (N2) 를 더 포함할 수도 있다. 서명은 원격국을 인증하기 위해 관리국에 의해 이용된다.

[0026] 개인/공개 키 쌍을 이용하는 경우, 원격국 (210) 은 메시지를 해싱하고, 개인 키를 이용하여 메시지를 암호화한다. 관리국 (220) 은 원격국의 공개 키를 이용해 암호화된 해시를 해독하여 원격국을 인증한다 (단계 266). 수신된 메시지를 재해싱하고 그것을 서명 해시와 비교함으로써 메시지 무결성이 확인된다.

[0027] 공유된 비밀 키를 이용하는 경우, 원격국 (210) 은 공유 키 (MAC = HMAC (공유 키, 메시지)) 를 이용하여 서명 (MAC) 을 생성한다. 관리국 (220) 은 공유 키를 이용하여 서명 (MAC) 을 재생성하고, 그것을 수신된 MAC 와 비교한다 (단계 266). 그 다음에 수신된 신원에 의해 호스트 원격국이 식별된다.

[0028] 호스트 원격국 (210) 의 성공적인 인증 후, 그 다음에, 관리국 (220) 은 보안 요소 (230) 에 NAA 들이나 또는 원격국에 서비스들을 제공하기 위한 다른 자격증명들을 안전하게 공급하고 활성화시킬 수도 있다 (단계 268). 호스트 원격국의 인증이 실패하는 경우, 관리국은 그 원격국을 블랙리스트에 올리고, 그 원격국에 NAA 들, 또는 서비스 제공자로부터 서비스를 획득하기 위해 원격국이 필요로 하는 다른 자격증명들 정보를 공급하지 않는다. 관리국은 또한, 보안 요소 상에 있는 경우, 호스트 원격국에 의한 네트워크 액세스 자격증명 정보의 이용을 불허용하도록 보안 요소에 지시할 수도 있다.

[0029] 관리국 (220) 은 호스트 원격국 인증을 주기적으로 요청할 수도 있다. 예를 들어, 관리국은 진행 중인 관리 세션 중에 인증을 요청할 수도 있다. 대안으로, 관리국은, 호스트 원격국에서의 변화의 검출 시에 (예를 들어, 새로운 디바이스가 쌍을 이루게 됨), 또는 모든 호스트 원격국의 파워 업 시에, 구성된 시간의 끝에서 인증 단계들을 수행하도록 보안 요소 (230) 에 정책을 구성할 수도 있다.

[0030] 도 4 를 참조하면, 무선 원격국 (RS) (402) (또는 UE) 은 무선 통신 시스템 (400) 의 하나 이상의 기지국들 (BS) (404) 과 통신할 수도 있다. RS 는 무선 피어 (peer) 디바이스와 더 쌍을 이룰 수도 있다. 무선 통신 시스템 (400) 은 하나 이상의 기지국 제어기들 (BSC) (406), 및 코어 네트워크 (408) 를 더 포함할 수도 있다. 코어 네트워크는 적합한 백홀들을 통해 인터넷 (410) 및 공중 전화망 (Public Switched Telephone Network; PSTN) (412) 에 접속될 수도 있다. 전형적인 무선 모바일국은 핸드헬드 전화, 또는 랩탑 컴퓨터를 포함할 수도 있다. 무선 통신 시스템 (400) 은 코드 분할 다중 접속 (code division multiple access; CDMA), 시간 분할 다중 접속 (time division multiple access; TDMA), 주파수 분할 다중 접속 (frequency division multiple access; FDMA), 공간 분할 다중 접속 (space division multiple access; SDMA), 편파 분할 다중 접속 (polarization division multiple access; PDMA), 또는 공지된 다른 변조 기법들과 같은 다수의 액세스 기법들 중 임의의 하나를 채용할 수도 있다.

[0031] 당업자라면, 정보 및 신호들이 임의의 다양한 상이한 기술들 및 기법들 중 임의의 것을 이용하여 표현될 수도 있음을 이해할 것이다. 예를 들어, 상기 설명을 통해 참조될 수도 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심볼들, 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 입자들, 광학 필드들 또는 입자들, 또는 이들의 임의의 조합에 의해 표현될 수도 있다.

[0032] 당업자라면, 본원에서 개시된 예시적인 실시형태들과 연계하여 설명된 다양한 예증적인 논리 블록들, 모듈들, 회로들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이들 양자 모두의 조합으로서 구현될 수도 있음을 또한 알 수 있을 것이다. 하드웨어 및 소프트웨어의 이러한 상호교환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들이 그들의 기능성의 관점에서 일반적으로 위에서 설명되었다. 그러한 기능성이 하드웨어 또는 소프트웨어로 구현되는지 여부는 특정 애플리케이션

및 전체 시스템에 부과되는 설계 제약들에 따라 달라진다. 당업자들은 각각의 특정 애플리케이션을 위해 다양한 방식들로 설명된 기능성을 구현할 수도 있으나, 그러한 구현 결정들이 본 발명의 범위로부터 벗어나게 하는 것으로 해석되어서는 안된다.

[0033] 본원에서 개시된 실시형태들과 연계하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 및 회로들은 범용 프로세서, 디지털 신호 프로세서 (digital signal processor; DSP), 주문형 반도체 (application specific integrated circuit; ASIC), 필드 프로그래머블 게이트 어레이 (field programmable gate array; FPGA) 또는 다른 프로그래머블 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본원에서 설명된 기능들을 수행하도록 설계된 것들의 임의의 조합에 의해 구현되거나 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 다르게는, 상기 프로세서는 임의의 종래의 프로세서, 컨트롤러, 마이크로컨트롤러, 또는 상태 머신일 수도 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합, 예를 들어, DSP와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 연계한 하나 이상의 마이크로프로세서들, 또는 임의의 다른 그러한 구성으로 구현될 수도 있다.

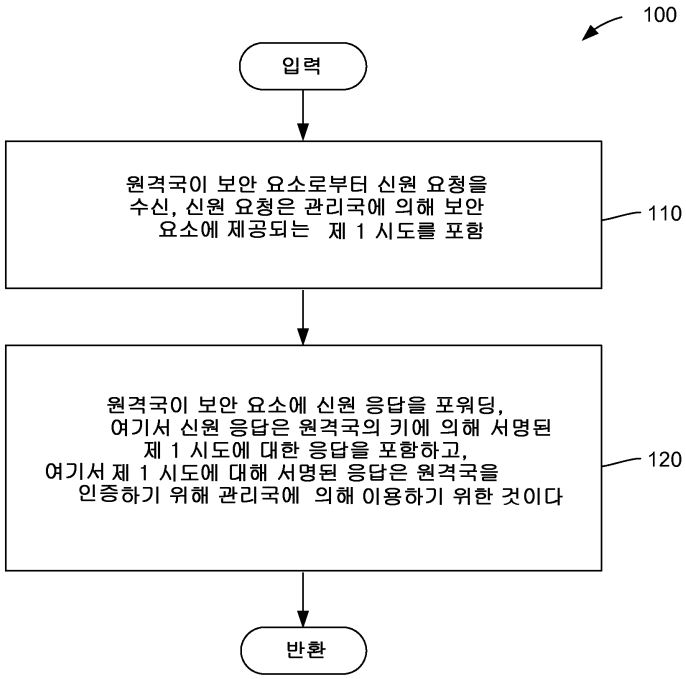
[0034] 본원에서 개시된 실시형태들과 연계하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어에서, 프로세서에 의해 실행되는 소프트웨어 모듈에서, 또는 이들 둘의 조합에서 직접적으로 구현될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 이동식 디스크, CD-ROM, 또는 공지된 임의의 다른 형태의 저장 매체 내에 있을 수도 있다. 일 예시적인 저장 매체는 프로세서에 커플링되어 프로세서가 저장 매체로부터 정보를 판독할 수도 있고 저장 매체에 정보를 기록할 수도 있다. 대안에서, 저장 매체는 프로세서에 통합될 수도 있다. 프로세서와 저장 매체는 ASIC 내에 있을 수도 있다. ASIC 는 사용자 단말기 내에 있을 수도 있다. 대안에서, 프로세서와 저장 매체는 사용자 단말기에서 개별 컴포넌트들로 있을 수도 있다.

[0035] 하나 이상의 예시적인 실시형태들에서, 상술된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 이들의 임의의 조합으로 구현될 수도 있다. 컴퓨터 프로그램 제품으로서 소프트웨어로 구현되는 경우, 상기 기능들은 하나 이상의 명령들 또는 코드로서 컴퓨터 판독가능 매체 상에 저장되거나 또는 전송될 수도 있다. 컴퓨터 판독가능 매체들은 한 장소에서 다른 장소로 컴퓨터 프로그램의 전송을 가능하게 하는 임의의 매체를 포함하여 컴퓨터 저장 매체들 및 통신 매체들 양자를 포함한다. 저장 매체들은 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체들일 수도 있다. 비제한적인 예로서, 이러한 컴퓨터 판독가능 매체들은 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 스토리지, 자기 디스크 스토리지 또는 다른 자기 스토리지 디바이스들, 또는 요구되는 프로그램 코드를 명령들 또는 데이터 구조들의 형태로 이송 또는 저장하기 위해 이용될 수 있으며 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 접속은 컴퓨터 판독가능 매체라고 적절히 칭해진다. 예를 들어, 소프트웨어가 동축 케이블, 광섬유 케이블, 연선, 디지털 가입자 회선 (digital subscriber line; DSL), 또는 적외선, 무선, 및 마이크로파와 같은 무선 기술들을 이용하여 웹사이트, 서버, 또는 다른 원격 소스로부터 송신되는 경우, 동축 케이블, 광섬유 케이블, 연선, DSL, 또는 적외선, 무선, 및 마이크로파와 같은 무선 기술들은 매체의 정의 내에 포함된다. 본원에서 사용된 디스크 (disk) 와 디스크 (disc) 는, 컴팩트 디스크 (CD), 레이저 디스크, 광학 디스크, 디지털 다기능 디스크 (DVD), 플로피디스크, 및 블루레이 디스크를 포함하며, 여기서 디스크 (disk) 들은 통상 자기적으로 데이터를 재생하는 반면, 디스크 (disc) 들은 레이저들을 이용하여 광학적으로 데이터를 재생한다. 위의 조합들도 컴퓨터 판독가능 매체들의 범위 내에 포함되어야 한다.

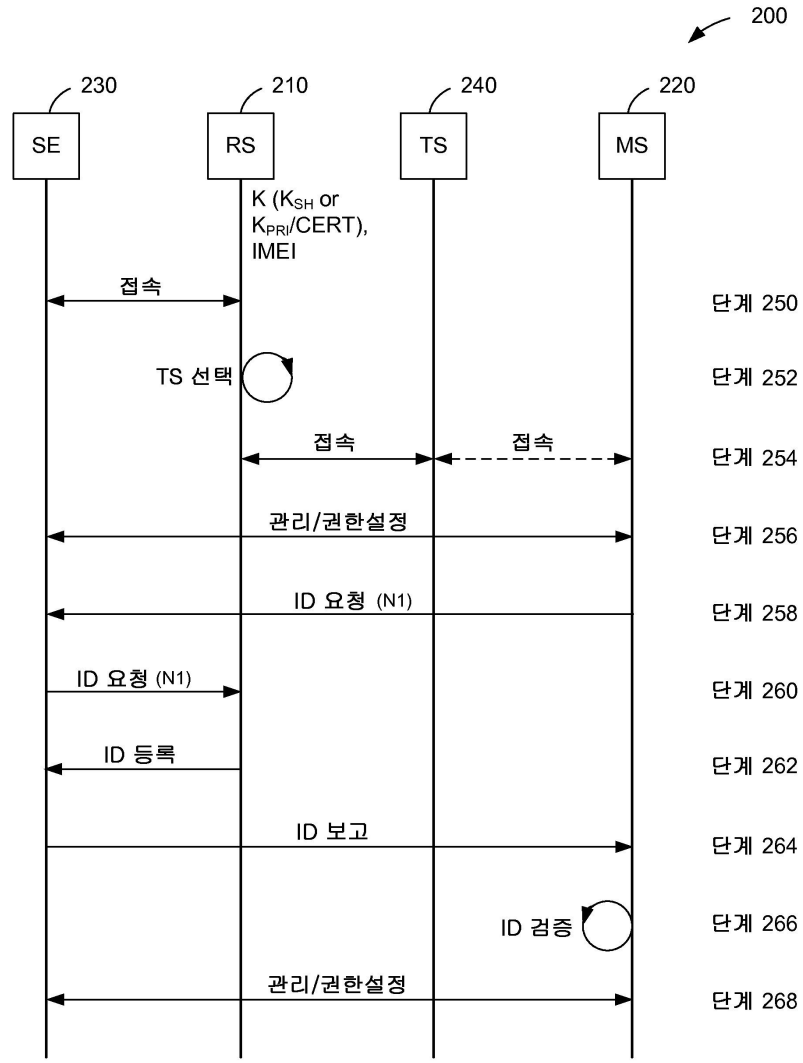
[0036] 개시된 실시형태들의 앞서의 설명은 임의의 당업자가 본 발명을 실시하거나 이용하는 것을 가능하게 하도록 하기 위해 제공된다. 이러한 실시형태들에 대한 다양한 수정예들이 당업자에게는 자명할 것이고, 본원에서 정의된 일반적인 원칙들은 본 발명의 취지와 범위를 벗어나지 않으면서 다른 실시형태들에 적용될 수도 있다. 따라서, 본 발명은 본원에서 보여진 실시형태들로 제한되도록 의도된 것은 아니며 본원에 개시된 원칙들과 신규한 특징들과 일치하는 가장 광의의 범위에 부합되고자 한다.

도면

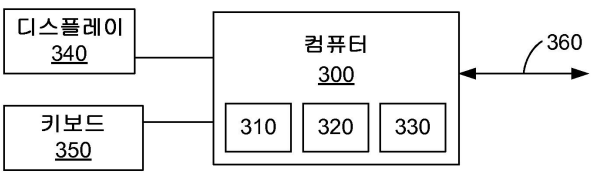
도면1


100
입력
원격국이 보안 요소로부터 신원 요청을 수신, 신원 요청은 관리국에 의해 보안 요소에 제공되는 제 1 시도를 포함
110
원격국이 보안 요소에 신원 응답을 포워딩, 여기서 신원 응답은 원격국의 키에 의해 서명된 제 1 시도에 대한 응답을 포함하고, 여기서 제 1 시도에 대해 서명된 응답은 원격국을 인증하기 위해 관리국에 의해 이용하기 위한 것이다
120
반환

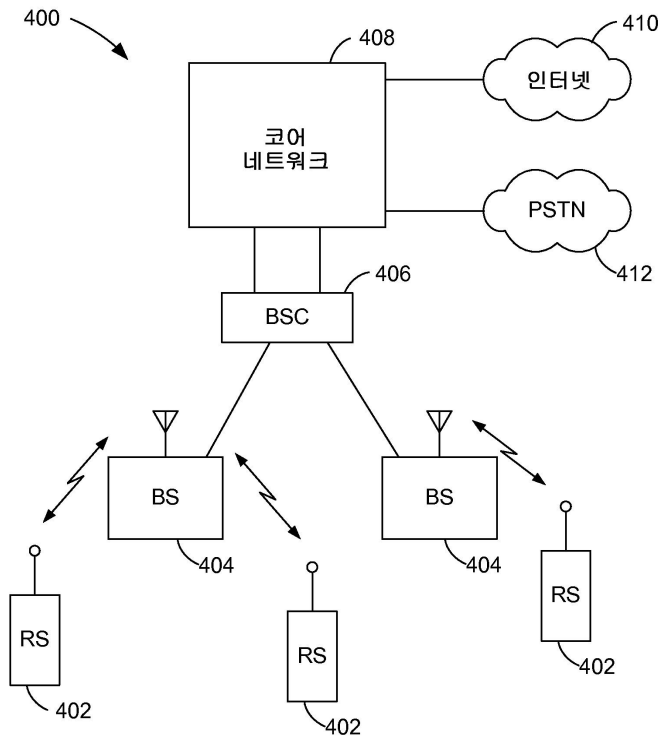
도면2


200
230
SE
210
RS
240
TS
220
MS
K (KSH or KPRI/CERT), IMEI
접속
단계 250
TS 선택
단계 252
접속
접속
단계 254
관리/권한설정
단계 256
ID 요청 (N1)
단계 258
ID 요청 (N1)
단계 260
ID 등록
단계 262
ID 보고
단계 264
ID 검증
단계 266
관리/권한설정
단계 268

도면3


디스플레이
340
키보드
350
컴퓨터
300
310
320
330
360

도면4


400
408
410
인터넷
코어
네트워크
PSTN
412
406
BSC
BS
BS
404
404
RS
RS
RS
402
402
402