(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년06월07일
(11) 등록번호 10-0961087
(24) 등록일자 2010년05월26일

(51) Int. Cl.
H04L 9/08 (2006.01)
(21) 출원번호 10-2007-7020727
(22) 출원일자(국제출원일자) 2006년02월10일
심사청구일자 2007년09월10일
(85) 번역문제출일자 2007년09월10일
(65) 공개번호 10-2007-0102749
(43) 공개일자 2007년10월19일
(86) 국제출원번호 PCT/US2006/004901
(87) 국제공개번호 WO 2006/086721
국제공개일자 2006년08월17일
(30) 우선권주장
60/652,063 2005년02월11일 미국(US)
(56) 선행기술조사문헌
KR1020050057474 A
전체 청구항 수 : 총 40 항

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
패돈 마이클
오스트레일리아 2155 뉴 사우스 웨일즈 켈리빌 아민 웨이 31
로즈 그레고리 고든
미국 92117 캘리포니아주 샌디에고 노스 스타 드라이브 3234
(뒷면에 계속)
(74) 대리인
특허법인코리아나

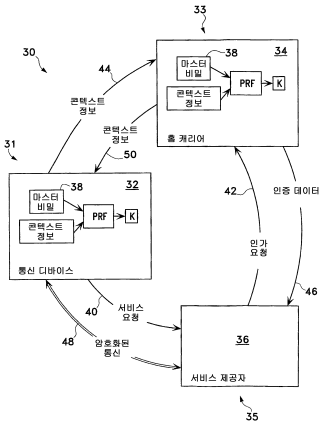
심사관 : 유선중

(54) 콘텍스트 한정된 공유 비밀

(57) 요 약

2 개의 통신 엔터티가 보안된 또는 비밀의 통신 세션을 가지려는 통신 시스템에서는, 우선 신뢰 관계가 확립될 것이 요구된다. 신뢰 관계는, 콘텍스트 정보로부터 차례로 생성되는 공유 비밀의 결정에 기초한다. 콘텍스트 정보는 통신 세션을 둘러싼 환경으로부터 유도된다. 예를 들어, 콘텍스트 정보는 토폴로지 정보, 시간 기반 정보 및 거래 정보를 포함할 수 있다. 공유 비밀은 자체 생성될 수도 있고, 제 3 자로부터 수신될 수도 있다. 두 경우 모두에서, 공유 비밀은 통신 엔터티들 간에 사용되는 임의의 암호화된 프로토콜을 위한 키 재료로서 사용될 수도 있다.

대 표 도 - 도1



(72) 발명자

셈플 제임스

영국 에스더블유7 5엔유 런던 그레이터 런던 퀸스 게이트 플레이스7 넘버4

호크스 필립 마이클

오스트레일리아 2131 뉴 사우스 웨일즈 애쉬필드 녹레이드스트리트 18-20 넘버30

특허청구의 범위

청구항 1

통신 엔터티와의 신뢰 관계를 확립하는 방법으로서,

마스터 비밀을 제공하는 단계;

상기 마스터 비밀 및 소정의 콘텍스트 정보에 기초하여 공유 비밀을 생성하는 단계; 및

상기 공유 비밀에 기초하여 상기 신뢰 관계를 확립하는 단계를 포함하는, 신뢰 관계 확립 방법.

청구항 2

제 1 항에 있어서,

상기 콘텍스트 정보에 토폴로지 정보를 제공하는 단계를 더 포함하는, 신뢰 관계 확립 방법.

청구항 3

제 1 항에 있어서,

상기 콘텍스트 정보에 시간 기반 정보를 제공하는 단계를 더 포함하는, 신뢰 관계 확립 방법.

청구항 4

제 1 항에 있어서,

상기 콘텍스트 정보에 거래 정보를 제공하는 단계를 더 포함하는, 신뢰 관계 확립 방법.

청구항 5

제 1 항에 있어서,

상기 콘텍스트 정보를 또 다른 통신 엔터티로부터 수신하는 단계를 더 포함하는, 신뢰 관계 확립 방법.

청구항 6

제 1 항에 있어서,

상기 공유 비밀을 키 재료로서 사용하여 상기 통신 엔터티와 암호로 통신하는 단계를 더 포함하는, 신뢰 관계 확립 방법.

청구항 7

2 개 이상의 통신 엔터티와의 신뢰 관계를 중재하는 방법으로서,

마스터 비밀을 제공하는 단계;

상기 마스터 비밀 및 소정의 콘텍스트 정보에 기초하여 공유 비밀을 생성하는 단계; 및

상기 공유 비밀에 기초하여 인증 정보를 상기 통신 엔터티 중 하나에 제공하는 단계를 포함하는, 신뢰 관계 중재 방법.

청구항 8

제 7 항에 있어서,

상기 콘텍스트 정보에 토폴로지 정보를 제공하는 단계를 더 포함하는, 신뢰 관계 중재 방법.

청구항 9

제 7 항에 있어서,

상기 콘텍스트 정보에 시간 기반 정보를 제공하는 단계를 더 포함하는, 신뢰 관계 중재 방법.

청구항 10

제 7 항에 있어서,

상기 콘텍스트 정보에 거래 정보를 제공하는 단계를 더 포함하는, 신뢰 관계 중재 방법.

청구항 11

제 7 항에 있어서,

상기 콘텍스트 정보를 상기 통신 엔터티 중 또 다른 엔터티로부터 수신하는 단계를 더 포함하는, 신뢰 관계 중재 방법.

청구항 12

제 7 항에 있어서,

상기 공유 비밀에 기초하여 인증 정보를 상기 통신 엔터티 중 하나에 제공하는 단계는 상기 인증 정보 내의 상기 공유 비밀을 상기 통신 엔터티 중 하나에 제공하는 단계를 포함하는, 신뢰 관계 중재 방법.

청구항 13

통신 엔터티와의 신뢰 관계를 확립하는 장치로서,

마스터 비밀을 제공하는 수단;

상기 마스터 비밀 및 소정의 콘텍스트 정보에 기초하여 공유 비밀을 생성하는 수단; 및

상기 공유 비밀에 기초하여 상기 신뢰 관계를 확립하는 수단을 구비하는, 신뢰 관계 확립 장치.

청구항 14

제 13 항에 있어서,

상기 콘텍스트 정보에 토폴로지 정보를 제공하는 수단을 더 구비하는, 신뢰 관계 확립 장치.

청구항 15

제 13 항에 있어서,

상기 콘텍스트 정보에 시간 기반 정보를 제공하는 수단을 더 구비하는, 신뢰 관계 확립 장치.

청구항 16

제 13 항에 있어서,

상기 콘텍스트 정보에 거래 정보를 제공하는 수단을 더 구비하는, 신뢰 관계 확립 장치.

청구항 17

제 13 항에 있어서,

상기 콘텍스트 정보를 또 다른 통신 엔터티로부터 수신하는 수단을 더 구비하는, 신뢰 관계 확립 장치.

청구항 18

제 13 항에 있어서,

상기 공유 비밀을 키 재료로서 사용하여 상기 통신 엔터티와 암호로 통신하는 수단을 더 구비하는, 신뢰 관계 확립 장치.

청구항 19

2 개 이상의 통신 엔터티와의 신뢰 관계를 중재하는 장치로서,

마스터 비밀을 제공하는 수단;

상기 마스터 비밀 및 소정의 콘텍스트 정보에 기초하여 공유 비밀을 생성하는 수단; 및

상기 공유 비밀에 기초하여 인증 정보를 상기 통신 엔터티 중 하나에 제공하는 수단을 구비하는, 신뢰 관계 중재 장치.

청구항 20

제 19 항에 있어서,

상기 콘텍스트 정보에 토폴로지 정보를 제공하는 수단을 더 구비하는, 신뢰 관계 중재 장치.

청구항 21

제 19 항에 있어서,

상기 콘텍스트 정보에 시간 기반 정보를 제공하는 수단을 더 구비하는, 신뢰 관계 중재 장치.

청구항 22

제 19 항에 있어서,

상기 콘텍스트 정보에 거래 정보를 제공하는 수단을 더 구비하는, 신뢰 관계 중재 장치.

청구항 23

제 19 항에 있어서,

상기 콘텍스트 정보를 상기 통신 엔티티 중 또 다른 엔티티로부터 수신하는 수단을 더 구비하는, 신뢰 관계 중재 장치.

청구항 24

제 19 항에 있어서,

상기 인증 정보 내의 상기 공유 비밀을 상기 통신 엔터티 중 하나에 제공하는 수단을 더 구비하는, 신뢰 관계 중재 장치.

청구항 25

통신 엔터티와의 신뢰 관계를 확립하는 장치로서,

마스터 비밀을 제공하는 컴퓨터 판독가능 명령, 상기 마스터 비밀 및 소정의 콘텍스트 정보에 기초하여 공유 비밀을 생성하는 컴퓨터 판독가능 명령 및 상기 공유 비밀에 기초하여 상기 신뢰 관계를 확립하는 컴퓨터 판독가능 명령을 포함하는 메모리 유닛, 및

상기 컴퓨터 판독가능 명령들을 처리하기 위해 상기 메모리 유닛에 결합되는 프로세서 회로를 구비하는, 신뢰 관계 확립 장치.

청구항 26

제 25 항에 있어서,

상기 메모리 유닛은, 상기 콘텍스트 정보에 토폴로지 정보를 제공하는 컴퓨터 판독가능 명령을 더 포함하는, 신뢰 관계 확립 장치.

청구항 27

제 25 항에 있어서,

상기 메모리 유닛은, 상기 콘텍스트 정보에 시간 기반 정보를 제공하는 컴퓨터 판독가능 명령을 더 포함하는, 신뢰 관계 확립 장치.

청구항 28

제 25 항에 있어서,

상기 메모리 유닛은, 상기 콘텍스트 정보에 거래 정보를 제공하는 컴퓨터 판독가능 명령을 더 포함하는, 신뢰 관계 확립 장치.

청구항 29

제 25 항에 있어서,

상기 메모리 유닛은, 상기 콘텍스트 정보를 또 다른 통신 엔터티로부터 수신하는 컴퓨터 판독가능 명령을 더 포함하는, 신뢰 관계 확립 장치.

청구항 30

제 25 항에 있어서,

상기 메모리 유닛은, 상기 공유 비밀을 사용하여 상기 통신 엔터티와 암호로 통신하는 컴퓨터 판독가능 명령을 더 포함하는, 신뢰 관계 확립 장치.

청구항 31

2 이상의 통신 엔터티와의 신뢰 관계를 중재하는 장치로서,

마스터 비밀을 제공하는 컴퓨터 판독가능 명령, 상기 마스터 비밀 및 소정의 콘텍스트 정보에 기초하여 공유 비밀을 생성하는 컴퓨터 판독가능 명령 및 상기 공유 비밀에 기초하여 상기 통신 엔터티 중 하나에 인증 정보를 제공하는 컴퓨터 판독가능 명령을 포함하는 메모리 유닛, 및

상기 컴퓨터 판독가능 명령들을 처리하기 위해 상기 메모리 유닛에 결합되는 프로세서 회로를 구비하는, 신뢰 관계 중재 장치.

청구항 32

제 31 항에 있어서,

상기 메모리 유닛은, 상기 콘텍스트 정보에 토폴로지 정보를 제공하는 컴퓨터 판독가능 명령을 더 포함하는, 신뢰 관계 중재 장치.

청구항 33

제 31 항에 있어서,

상기 메모리 유닛은, 상기 콘텍스트 정보에 시간 기반 정보를 제공하는 컴퓨터 판독가능 명령을 더 포함하는, 신뢰 관계 중재 장치.

청구항 34

제 31 항에 있어서,

상기 메모리 유닛은, 상기 콘텍스트 정보에 거래 정보를 제공하는 컴퓨터 판독가능 명령을 더 포함하는, 신뢰 관계 중재 장치.

청구항 35

제 31 항에 있어서,

상기 메모리 유닛은, 상기 콘텍스트 정보를 상기 통신 엔터티 중 또 다른 엔터티로부터 수신하는 컴퓨터 판독가능 명령을 더 포함하는, 신뢰 관계 중재 장치.

청구항 36

제 31 항에 있어서,

상기 메모리 유닛은, 상기 인증 정보 내의 상기 공유 비밀을 상기 통신 엔터티 중 하나에 제공하는 컴퓨터 판독가능 명령을 더 포함하는, 신뢰 관계 중재 장치.

청구항 37

마스터 비밀을 제공하는 컴퓨터 판독가능 명령;

상기 마스터 비밀 및 소정의 콘텍스트 정보에 기초하여 공유 비밀을 생성하는 컴퓨터 판독가능 명령; 및

상기 공유 비밀에 기초하여 신뢰 관계를 확립하는 컴퓨터 판독가능 명령을 포함하는, 컴퓨터 판독가능 매체.

청구항 38

제 37 항에 있어서,

상기 콘텍스트 정보는 토폴로지 정보, 시간 기반 정보 및 거래 정보로 구성된 그룹으로부터 선택된 정보를 포함하는, 컴퓨터 판독가능 매체.

청구항 39

마스터 비밀을 제공하는 컴퓨터 판독가능 명령;

상기 마스터 비밀 및 소정의 콘텍스트 정보에 기초하여 공유 비밀을 생성하는 컴퓨터 판독가능 명령; 및

상기 공유 비밀에 기초하여 인증 정보를 통신 엔터티들 중 하나에 제공하는 컴퓨터 판독가능 명령을 포함하는, 컴퓨터 판독가능 매체.

청구항 40

제 39 항에 있어서,

상기 콘텍스트 정보는, 토폴로지 정보, 시간 기반 정보 및 거래 정보로 구성된 그룹으로부터 선택된 정보를 포함하는, 컴퓨터 판독가능 매체.

명 세 서

[0001] **35 U.S.C §119 하의 우선권 주장**

[0002] 본 특허 출원은 2005년 2월 11일 출원되고 본 양수인에게 양도되었으며 본 명세서에 참조로 명백하게 통합된, 발명의 명칭이 "Context Limited Secret Key" 인 미국 가출원 제 60/652,063 호에 대해 우선권을 주장한다.

[0003] **배경**

[0004] **I. 기술분야**

[0005] 본 발명은 일반적으로 통신에 관한 것이고, 더 상세하게는, 콘텍스트 한정 정보로부터 생성된 공유 비밀을 사용하는 보안 및 비밀 (private) 통신에 관한 것이다.

[0006] **II. 배경기술**

[0007] 보안 또는 비밀로 의도되는 통신에서는 공유 비밀의 사용이 통상적이다. 통상적인 공유 비밀 방식에서는, 통신하는 엔터티들에만 알려진 공동 비밀이 공유되고, 이러한 비밀은 통신하는 엔터티들에 의해 신뢰되어, 신뢰 관계를 확립한다. 공유 비밀이 없는 자는 신뢰 관계로부터 배제된다.

[0008] 공유 비밀은 영속적일 수도 있고 일시적일 수도 있다. 일시적인 공유 비밀은 한정된 기간동안 통신을 보호하기 위해 사용될 수 있다. 예를 들어, 일시적인 공유 비밀은 일회용 거래에만 양호할 수 있다.

[0009] 고도의 보안성을 제공하기 위해, 영속적 비밀로부터 일시적 비밀이 유도되는 경우가 매우 많다. 이러한 구조에서는 일시적 비밀이 신뢰 관계를 확립하기 위한 기본으로서 사용된다. 예를 들어, 상대방과 신뢰 관계를 확립하기를 원하는 자는, 상대방과의 암호화된 통신을 위한 키 재료로서 상대방과 공유되는 일시적 비밀을 사용할 수도 있다.

[0010] 때로는 마스터 비밀로 지칭되는 영속적 비밀에 있어서, 비제한적으로 공유되는 경우는 거의 없다. 예를 들어, 이동 통신 설정에서는, 마스터 비밀이 가입자 유닛과 가입자의 홈 캐리어 사이에서만 공유된다. 가입자

유닛이 제 3 자로부터 보안된 통신을 통해 서비스를 요청하는 경우, 가입자 유닛은 마스터 비밀로부터 일시적 비밀을 생성한다. 또한 그와 동시에, 가입자 유닛은 공유된 마스터 비밀로부터 동일한 일시적 비밀을 교대로 생성하는 홈 캐리어에 요청을 전송한다. 또한, 일시적 비밀은 가입자와 제 3 자간의 신뢰 관계의 기초를 형성한다. 예를 들어, 가입자 유닛 및 홈 캐리어 모두는 다른 것들 중 그 일시적 비밀로부터 서비스 제공자에게 사용가능하게 된 암호화 키를 생성할 수도 있다. 가입자 유닛과 서비스 제공자간의 암호화된 통신은 그후에 변경될 수 있다.

[0011] 마스터 비밀로부터 일시적 비밀을 유도하는 근거는 마스터 비밀의 누설 가능성을 감소시키기 위함이다. 마스터 비밀로부터 일시적 비밀의 유도는 가입자 유닛과 홈 캐리어 사이에서 몇몇 미리 구성된 알고리즘에 기초할 수 있다.

[0012] 전술한 보안 모델은, 임의의 유도된 비밀에 접근할 수도 있는 임의의 제 3 자가 유도된 비밀의 기밀성을 보호하려 할 것이라는 가정에 기초한다. 예를 들어, 제 3 자가 유도된 비밀을 또 다른 자에게 누설하면, 그 제 3 자로부터 서비스를 구매할 때의 신뢰도는 심각하게 위협될 것이다. 이러한 경우, 그 제 3 자는, 비밀 누설의 법적 결과를 언급하지 않더라도 사업을 유지하는 엔터티로서 심각하게 영향받을 것이다.

[0013] 그러나, 공유 비밀을 비밀로 유지하려는 경제적 동기 또는 윤리적 고려 모두를 갖지 않는 자가 일부 존재할 수도 있다. 예를 들어, 유도된 비밀이 가입자로서 설정된 사기꾼에게 전달되면, 사기꾼은 그 유도된 비밀을 사용하여 합법적 가입자로 가장하고, 자신에게는 접속불가였을 서비스로의 액세스를 획득할 수 있다. 이러한 상황이 악화되면, 그 불법적 액세스로부터 추가적인 민감한 정보가 더 누설될 수 있다. 더 심각한 결과가 없다 하더라도, 사기꾼이 자신을 서비스 제공자로 설정할 수도 있다.

[0014] 따라서, 유도된 비밀의 누설 및 악용을 방지하기 위해 더 보안된 통신 방식을 제공할 필요가 있다.

[0015] **요약**

[0016] 2 개의 통신 엔터티가 비밀의 또는 보안된 통신 세션을 가질려는 통신 시스템에서는, 우선 신뢰 관계가 확립될 필요가 있다. 신뢰 관계는, 마스터 비밀 및 선택된 콘텍스트 정보로부터 생성된 공유 비밀의 결정에 기초한다. 콘텍스트 정보는 통신 세션을 둘러싼 환경으로부터 유도될 수 있다. 공유 비밀은 각각의 통신 엔터티에 의해 자체 생성될 수도 있다. 또는, 엔터티가 공유 비밀을 직접 유도할만큼 충분한 정보를 보유하지 않은 경우, 공유 비밀은 제 3 자로부터 수신될 수도 있다. 공유 비밀은, 통신 엔터티들간의 보안된 통신을 인증 및 확립하는데 사용되는 암호화된 프로토콜을 위한 키 재료로서 사용될 수 있다.

[0017] 예시적인 실시형태에서는, 하나의 통신 엔티티로서의 가입자 유닛이 또 다른 통신 엔터티로서의 서비스 제공자로부터 서비스를 요구한다. 가입자 유닛은, 미리 저장된 마스터 비밀, 및 토폴로지 정보, 시간 기반 정보 및 거래 정보를 포함하지만 이에 한정되지는 않는 소정의 콘텍스트 정보에 기초하여 자체로 공유 비밀을 생성한다. 마스터 비밀을 보유하지 않은 서비스 제공자는 또 다른 엔터티로부터 공유 비밀을 획득한다. 그 후, 서비스 제공자 및 가입자 유닛은 공유 비밀의 공동 인식을 사용하여 신뢰 관계를 확립한다. 이 예에서, 다른 엔터티는 가입자 유닛의 홈 캐리어이다. 공유 비밀을 서비스 제공자에게 전송하기 전에, 홈 캐리어는 가입자 유닛과 실질적으로 동일한 방식으로 공유 비밀을 생성한다. 또한, 홈 캐리어로부터 서비스 제공자로의 공유 비밀의 전송은 미리 동의된 보호 메커니즘을 통해 보호될 수도 있다.

[0018] 전술한 방식으로 동작하면, 생성된 공유 비밀은 불법적으로 복제되거나 악용될 가능성이 거의 없다.

[0019] 이러한 특성 및 이점과 다른 특성 및 이점은 다음의 상세한 설명 및 첨부한 도면으로부터 당업자에게 자명할 것이고, 첨부한 도면에서 유사한 부호는 유사한 부분을 나타낸다.

[0020] **도면의 간단한 설명**

[0021] 도 1 은 본 발명의 일반적 실시형태를 나타내는 단순화된 개략도이다.

[0022] 도 2a 는, 먼저 통신 세션에 대한 신뢰 관계를 확립하려는 통신 엔터티에 관련된 단계를 도시하는 일 실시형태에 따른 흐름도이다.

[0023] 도 2b 는 신뢰 관계의 확립을 용이하게 하는 중간적 엔터티에 관련된 단계를 도시하는, 도 2a 의 실시형태에 따른 흐름도이다.

[0024] 도 3a 는 먼저 통신 세션에 대한 신뢰 관계를 확립하려는 통신 엔터티에 관련된 단계를 도시하는 또 다른 실시형태에 따른 흐름도이다.

[0025] 도 3b 는 신뢰 관계의 확립을 용이하게 하는 중간적 엔터티에 관련된 단계를 도시하는, 도 3a 의 실시형태에 따른 흐름도이다.

[0026] 도 4 는 본 발명의 실시형태를 수행하는 하드웨어 구현의 일부를 도시하는 개략도이다.

[0027] **상세한 설명**

[0028] 당업자가 본 발명을 실시하고 이용할 수 있도록 다음의 설명을 제공한다. 다음의 설명에서는 설명의 목적으로 세부사항들을 상세히 설명한다. 통상의 당업자라면 이러한 특정한 세부사항들을 사용하지 않고 본 발명이 실시될 수도 있음을 인식할 것이다. 다른 예에서는, 불필요한 세부사항으로 본 발명의 설명을 모호하게 하지 않기 위해 주지의 구조 및 프로세스는 상술하지 않는다. 따라서, 본 발명은 개시된 실시형태에 한정되는 것이 아니며, 본 명세서에서 개시된 원리 및 특성에 일치하는 최광의 범주에 부합되도록 의도된다.

[0029] 도 1 은 본 발명의 일반적 실시형태의 단순화된 개략도이다. 통신 시스템은 참조 부호 30 에 의해 전체적으로 표시되며, 음성, 데이터, 멀티미디어 또는 그 조합을 전달하는 시스템일 수 있다. 또한, 시스템 (30) 은 다양한 표준 및 프로토콜 하에서 동작될 수 있으며, 그 예로는, cdma2000 (Code Division Multiplex Access 2000), GSM (Global System for Mobile communication), WCDMA (Wideband Code Division Multiple Access) 및 IP (Internet Protocol) 가 있다.

[0030] 명확하고 간결한 설명을 위해, 도 1 에는 3 개의 엔터티, 즉, 제 1 통신 엔터티 (31), 제 2 통신 엔터티 (33) 및 제 3 통신 엔터티 (35) 만 도시되어 있다. 이 예시적인 실시형태에서는, 제 1 엔터티 (31) 가 통신 디바이스 (32) 이다. 제 2 엔티티 (33) 는 홈 캐리어 (34) 이다. 제 3 엔티티 (35) 는 서비스 제공자 (36) 이다.

[0031] 이 예에서는, 통신 디바이스 (32) 가 홈 캐리어 (34) 의 가입자인 것으로 가정한다. 통신 디바이스 (32) 는 유선 디바이스, 예를 들어, 홈 캐리어 (34) 와 동일한 네트워크에 유선 접속된 워크스테이션일 수 있다. 또는, 통신 디바이스 (32) 는 무선 디바이스일 수 있다. 예를 들어, 디바이스 (32) 는 무선 전화기, 무선 컴퓨터 또는 개인 휴대용 정보 단말기 (PDA) 일 수 있다. 이와 같이, 통신 디바이스 (32) 는 홈 캐리어 (34) 와 동일한 네트워크 내에 존재할 수 있다. 또한, 통신 디바이스 (32) 는 홈 캐리어 (34) 의 네트워크 외부에 위치할 수도 있다. 예를 들어, 통신 디바이스 (32) 는 홈 캐리어 (34) 의 네트워크로부터 다른 네트워크로 로밍할 수도 있고, 다른 네트워크에서의 다른 엔터티와 통신할 수도 있다.

[0032] 도 1 을 다시 참조한다. 이 예에서는, 통신 디바이스 (32) 가 서비스 제공자 (36) 로부터 서비스를 요청한다. 요청된 서비스는, 통신 디바이스 (32) 가 홈 캐리어 (34) 의 네트워크 내부에 존재하는 경우 홈 캐리어 (34) 로부터 정규로 요청된 서비스일 수 있다. 또 다른 예로서, 요청된 서비스는 홈 캐리어 (34) 가 아닌 서비스 제공자 (36) 에 의해서만 제공된 서비스일 수 있다. 서비스 제공자 (36) 는 홈 캐리어 (34) 의 네트워크 내부에 존재할 수도 있고 외부에 존재할 수도 있다.

[0033] 보안 및 비밀을 위해, 통신 디바이스 (32) 는 우선 서비스 제공을 위해 서비스 제공자 (36) 의 인가가 보장되는 것을 요구할 수도 있다. 유사하게, 서비스 제공자 (36) 는, 통신 디바이스 (32) 가, 예를 들어, 과금 목적으로 합법적인지 여부의 인식을 요구할 수도 있다. 상이하게 부여되면, 임의의 통신 이전에, 통신 디바이스 (32) 와 서비스 제공자 (36) 사이에 신뢰 관계가 확립될 필요가 있다.

[0034] 본 실시형태에 따르면, 통신 디바이스 (32) 및 홈 캐리어 (34) 는 도 1 에서 참조 부호 38 로 식별되는 마스터 비밀을 공유한다.

[0035] 프로세스를 시작하기 위해, 먼저 통신 디바이스 (32) 는 서비스 요청을 통신 경로 (40) 에 의해 지정된 서비스 제공자 (36) 에 전송한다. 그 후, 신뢰 관계를 확립하는 프로세스가 후속한다.

[0036] 통신 디바이스 (32) 에 있어서는, 먼저 의사 랜덤 함수 (PRF) 를 통해 공유 비밀 K 를 생성한다. PRF 로의 입력에는 다른 것들 중 마스터 비밀 (38) 및 콘텍스트 정보가 포함될 수 있다.

[0037] PRF 의 예로는 해시 기반 메시지 인증 코드 (HMAC), 보안 해시 알고리즘 1 (SHA-1) 또는 그 조합이 있을 수 있다. HMAC 및 SHA-1 모두는 인터넷 엔지니어링 태스크 포스 (IETF) 에 의해 공표된 RFC (Request for Comments) 에서 찾을 수 있다. 더 상세하게는, HMAC 는 1997 년 2 월, "HMAC: Keyed-Hashing for Message Authentication" 라 명명된 RFC 2104 에 설명되어 있다. SHA-1 알고리즘은 2001 년 9월, "U.S. Secure Hash Algorithm 1" 에 정의되어 있다.

[0038] 본 발명의 이 실시형태에 따르면, 통신 세션을 둘러싼 환경으로부터 콘텍스트 정보가 유도될 수 있다.

[0039] 콘텍스트 정보는 토폴로지 기반일 수 있다. 예를 들어, IP 하에서 동작하면, 토폴로지 정보는 도 1 에 도시된 바와 같은 다수의 엔터티 (31, 33 및 35) 의 소스 어드레스 및 수신지 어드레스를 포함할 수 있다. 또한, 전술한 어드레스는 추가적인 레벨의 보안을 위한 어드레스의 블록을 특정하는 네트워크 마스크를 포함할 수 있다. TCP (Transport Control Protocol) 및 UDP (User Datagram Protocol) 하의 통신에 있어서는, 소스 및 수신지 포트가 또한 포함될 수 있다.

[0040] 또한, 콘텍스트 정보는 시간에 관련될 수 있다. 즉, 통신 세션의 환경을 둘러싼 특정한 시간 파라미터가 콘텍스트 정보를 위해 사용될 수 있다. 예를 들어, 콘텍스트 정보는 시작 시간, 종료 시간, 통신 디바이스 (32) 에 의해 서비스 제공자 (36) 로 전송되는 서비스 요청 (40) 의 세션과 같은 특정 통신 세션의 지속기간을 포함할 수 있다.

[0041] 또한, 콘텍스트 정보는 거래 특정일 수 있다. 다양한 통신 시스템 하에서, 각각의 통신 세션은 임시 (nonce) 또는 거래 식별자로 지칭되는 식별자에 의해 고유하게 식별된다. 또한, 이러한 식별 정보는 콘텍스트 정보로서 사용되고 포함될 수 있다.

[0042] 전술한 바와 같이, 공유 비밀 K 를 생성하기 위해, PRF 로의 입력에는 마스터 비밀 및 콘텍스트 정보가 포함될 수 있다. 수학적으로는,

[0043] $$K = PRF(master\_secret, contextual\_information) \quad (A)$$

[0044] 로 표현될 수 있으며, 여기서, master_secret 는 예를 들어, 전술한 바와 같은 마스터 비밀 (38) 이고, contextual_information 는,

[0045] $$contextual\_information = \cup(server\_address, server\_port, start\_time, end\_time, random\_nonce) \quad (B)$$

[0046] 로 표현될 수 있으며, 여기서 ∪ 는 식 (B) 의 괄호에 포함된 바와 같은 파라미터들의 집합을 나타낸다. 이러한 특정 예에서, server_address 는 서비스 제공자 (36) 의 네트워크 어드레스이고, server_port 는 서비스 제공자 (36) 의 포트 번호이고, start_time 은 통신 디바이스 (32) 가 서비스 요청 (40) 을 서비스 제공자 (36) 에 전송하는 시작 시간이고, end_time 은 전술한 서비스 요청의 종료 시간이다.

[0047] 서비스 제공자 (36) 측에서는, 통신 디바이스 (32) 로부터 서비스 요청의 수신시에, 서비스 제공자 (36) 가 인가를 위해 도 1 에서 통신 경로 (42) 로 식별되는 바와 같이 홈 캐리어 (34) 에 통지한다. 동시에, 자체 시작시에 또는 홈 캐리어 (34) 로부터의 요청시에, 통신 디바이스 (32) 는 통신 경로 (44) 로 식별되는 바와 같이 홈 캐리어 (34) 로 콘텍스트 정보를 전송한다. 콘텍스트 정보 및 미리 저장된 마스터 비밀 (38) 을 사용하여, 홈 캐리어 (34) 는, 전술한 바와 같이 통신 디바이스 (32) 가 고유 비밀 K 를 생성하는 것과 동일한 방식으로 식 (A) 및 (B) 에 따라 공유 비밀 K 를 차례로 생성한다.

[0048] 공유 비밀 K 는 서비스 제공자 (36) 와 통신 디바이스 (32) 사이에서 후속적인 보안 통신을 위한 지원 기반을 제공한다.

[0049] 예를 들어, 보안 및 비밀 통신을 위해, 다양한 암호화된 프로토콜이 서비스 제공자 (36) 와 통신 디바이스 (32) 사이에서 나중에 사용될 수 있다. 각각의 암호화된 프로토콜은 보안 통신 데이터를 암호화하기 위해 암호키 Ke 를 요구할 수도 있다. 암호키 Ke 는 공유 비밀 K 로부터 생성될 수 있다.

[0050] 또 다른 예로서, 적용할 수 있다면, 서비스 제공자 (36) 와 통신 디바이스 (32) 사이에서 교환되는 챌린지 데이터를 생성하는데 공유 비밀 K 가 사용될 수 있다. 챌린지 데이터는 챌린지 메시지 및 기대 응답을 포함할 수도 있다. 기대 응답은 공유 비밀 K 를 인식한 경우 및 챌린지 메시지로부터만 생성될 수 있다. 예를 들어, 도 1 을 참조하면, 서비스 제공자 (36) 가 홈 캐리어 (34) 로부터 공유 비밀 K 를 수신한 경우, 서비스 제공자 (36) 는 챌린지 메시지를 통신 디바이스 (32) 로 전송함으로써 통신 디바이스 (32) 의 인증을 시도할 수도 있다. 통신 디바이스 (32) 는 공유 비밀 K 를 보유한다. 그 후, 통신 디바이스 (32) 는 공유 비밀 K 에 기반하여 기대 메시지를 생성하고, 인증을 위해 기대 메시지를 서비스 제공자 (36) 에 전송한다. 그 후, 서비스 제공자 (36) 는, 통신 디바이스 (32) 로부터 수신된 기대 메시지와, 홈 캐리어 (34) 로부터 이전에 수신되었던 공유 비밀 K 에 기초한 자체 생성 기대 메시지를 비교함으로써 통신 디바이스 (32) 의 인증을 결정할 수도 있다.

[0051] 계속하여 도 1 을 참조한다. 인가를 위한 요청 (42) 에 응답하여, 그리고 나중에 사용될 암호 프로토콜에 따라, 홈 캐리어 (33) 는 인증 데이터를 전송하며, 이 예에서, 인증 데이터에는 통신 경로 (46) 에 의해 식별되는 바와 같이 서비스 제공자 (36) 로의 공유 비밀 K 가 포함된다. 통신 경로 (46) 를 통한 인증 데이터의 송신은 미리 구성된 보안 메커니즘에 의해 보호될 수도 있다.

[0052] 통신 디바이스 (32) 및 서비스 제공자 (36) 가 일단 공유 비밀 K 를 보유하면, 암호로 보안되는 통신을 확립하기 위한 키 재료로서 비밀 K 를 사용할 수 있다. 통신 디바이스 (32) 와 서비스 제공자 (36) 사이의 암호화 통신의 통신 경로는 도 1 에 도시된 바와 같이 참조 부호 48 에 의해 표시된다.

[0053] 전술한 프로세스는 도 2a 및 도 2b 의 흐름도로 요약된다. 도 2a 는 통신 디바이스 (32) 에 의해 실행되는 프로세스 단계를 도시한다. 도 2b 는 홈 캐리어 (34) 에 의해 수행되는 대응 프로세스 단계를 도시한다.

[0054] 전술한 방식으로 동작하면, 공유 비밀 K 가 미인가된 자에게 부적절하게 누설되는 경우에도, 공유 비밀 K 가 원래 생성시킨 정확한 콘텍스트 정보가 성공을 위해 복제되었을 것이기 때문에, 미인가된 자가 합법적 비밀 유지자로 오인되는 비밀 K 의 미인가 사용의 가능성은 실질적으로 감소된다.

[0055] 또는, 통신 디바이스 (32) 가 콘텍스트 정보를 홈 캐리어 (34) 에 전송하게 하는 대신에, 그 역도 가능할 수 있다. 즉, 서비스 제공자 (46) 로부터 인가를 위한 요청의 수신시에, 홈 캐리어 (34) 는 콘텍스트 정보를 통신 디바이스 (32) 에 전송할 수 있다. 예를 들어, 식 (B) 에서 소정의 파라미터 start_time 및 end_time 이 도 1 에 도시된 바와 같이 인가 요청 (42) 의 시작 및 종료시에 각각 설정될 수 있다. 그 후, 통신 디바이스 (32) 는 수신된 콘텍스트 정보를 사용하여 공유 비밀 K 를 생성할 수 있다. 또한, 공유 비밀 K 는 통신 디바이스 (32) 와 서비스 제공자 (36) 사이의 암호화 통신을 위해 사용될 임의의 암호화 프로토콜에 적합한 키 재료로서 사용될 수도 있다. 이 프로세스는 전술한 바와 실질적으로 유사하고 도 3a 및 도 3b 의 흐름도에 요약되어 있다. 도 3a 는 통신 디바이스 (32) 에 의해 실행되는 프로세스 단계를 도시한다. 도 3b 는 홈 캐리어 (34) 에 의해 수행되는 대응 프로세스 단계를 도시한다.

[0056] 도 4 는 본 발명의 예시적인 실시형태에 따라 참조 부호 60 으로 지정되는, 도 1 에 도시된 통신 엔터티 (31 및 33) 와 같은 장치의 하드웨어 구현의 일부를 도시한다. 장치 (60) 는, 일부만 언급한다면, 스테이셔너리 컴퓨터, 네트워크 하드웨어의 일부, 랩탑 컴퓨터, PDA 또는 셀룰러 폰과 같이 다양한 형태로 제작 및 통합될 수 있다.

[0057] 장치 (60) 는 다수의 회로를 함께 링크하는 중앙 데이터 버스 (62) 를 포함한다. 회로는 CPU (중앙 처리 장치) 또는 제어기 (64), 수신 회로 (66), 송신 회로 (68) 및 메모리 유닛 (70) 을 포함한다.

[0058] 장치 (60) 가 무선 디바이스의 일부이면, 수신 회로 및 송신 회로 (66 및 68) 는 RF (Radio Frequency) 회로에 접속될 수 있지만 도면에는 도시하지 않았다. 수신 회로 (66) 는 수신된 신호를 데이터 버스 (62) 에 전송하기 전에 처리 및 버퍼링한다. 한편, 송신 회로 (68) 는 데이터 버스 (62) 로부터의 데이터를 디바이스 (60) 로부터 전송하기 전에 처리 및 버퍼링한다. CPU/제어기 (64) 는 데이터 버스 (62) 의 데이터 관리의 기능을 수행하고, 메모리 유닛 (70) 의 명령 콘텐츠를 실행하는 것을 포함하는 일반적 데이터 처리의 기능을 더 수행한다.

[0059] 도 4 에 도시된 바와 같이 개별적으로 배치되는 대신에, 대체예로서, 송신 회로 (68) 및 수신 회로 (66) 는 CPU/제어기 (64) 의 일부일 수 있다.

[0060] 메모리 유닛 (70) 은 참조 부호 72 로 일반적으로 지정된 명령의 세트를 포함한다. 이 실시형태에서, 명령에는, 다른 명령들중, 장치 (60) 에 의해 수행되는 역할에 따라 도 2a, 2b, 3a 및 3b 의 흐름도에 도시되고 설명된 바와 같은 처리 단계가 포함되며, 이러한 단계들은 도 4 에 도시된 바와 같이, "공유 비밀 생성 및 처리 펑션" 으로서 참조 부호 74 에 의해 전체적으로 지정되어 있다. 전술한 바와 같이 PRF 가 펑션 (74) 에 포함될 수 있다.

[0061] 또한, 메모리 유닛 (70) 에는, 임의의 선택된 암호화 프로토콜을 수행하는 암호화 통신 펑션 (76) 이 포함된다. 또한, 동일한 메모리 유닛 (70) 에는, 다른 것들 중 마스터 비밀 (38) 이 저장된다. 펑션 (74, 76) 및 마스터 비밀 (38) 은 상이한 메모리 유닛 (미도시) 로부터, 예를 들어 장치 (60) 의 파워업동안 메모리 유닛 (70) 으로 전송될 수 있다.

[0062] 본 실시형태에서, 메모리 유닛 (70) 은 RAM (Random Access Memory) 회로이다. 예시적인 명령부 (72) 는 소프트웨어 루틴 또는 모듈이다. 전술한 바와 같이, 메모리 유닛 (70) 은 휘발성일 수도 있고 비휘발성일

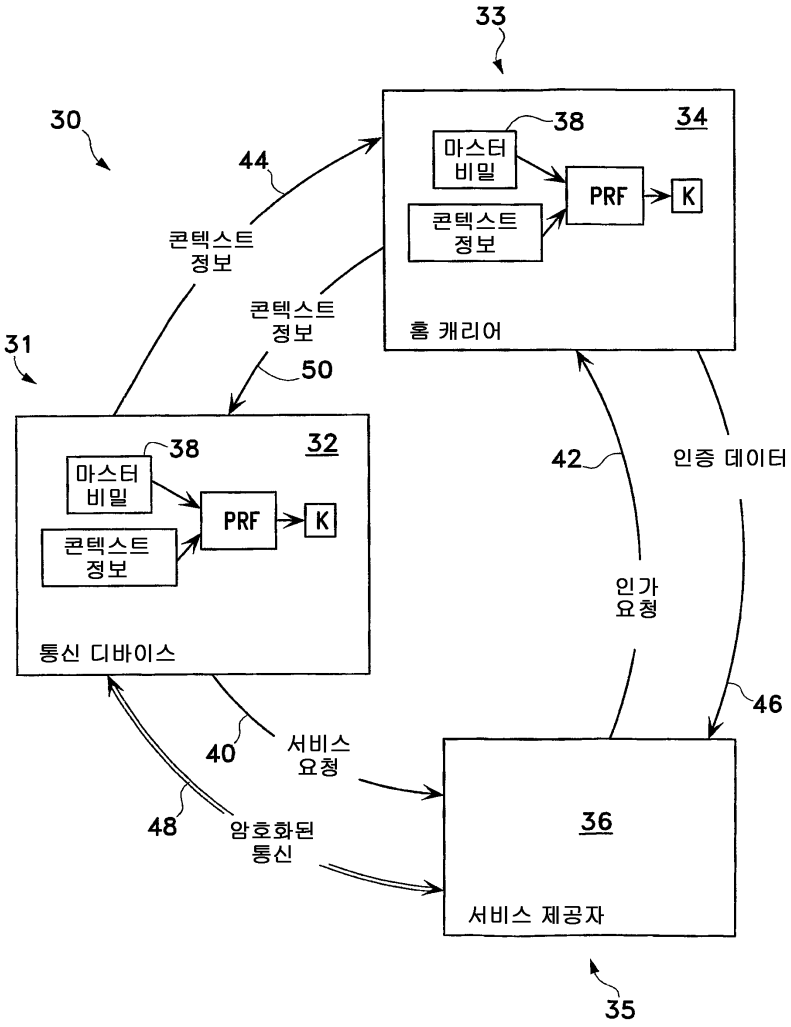
수도 있는 또 다른 메모리 회로 (미도시) 에 고정될 수 있다. 대체예로서, 메모리 유닛 (70) 은, EEPROM (Electrically Erasable Programmable Read Only Memory), EPROM (Electrical Programmable Read Only Memory), ROM (Read Only Memory), ASIC (Application Specific Integrated Circuit), 자기 디스크, 광 디스크 및 주지의 다른 회로와 같은 다른 회로 타입으로 구성될 수 있다.

[0063] 전술한 도 2a, 2b, 3a 및 3b 에서 설명되고 도시된 바와 같은 프로세스는 공지된 임의의 컴퓨터 판독가능 매체 상에서 수행되는 컴퓨터 판독가능 명령으로서 코딩될 수 있음을 유의해야 한다. 본 명세서 및 첨부한 청구항에서, 용어 "컴퓨터 판독가능 매체" 는, 도 4 에 도시되고 설명된 CPU/제어기 (64) 와 같은 실행을 위한 임의의 프로세서에 명령을 제공하는데 참여하는 임의의 매체를 지칭한다. 이러한 매체는 저장 타입일 수도 있고, 예를 들어, 도 4 의 메모리 유닛 (70) 의 설명에서 전술한 바와 같이, 휘발성 저장 매체 또는 비휘발성 저장 매체의 형태를 가질 수도 있다. 또한, 이러한 매체는 송신 타입일 수도 있고, 동축 케이블, 구리선, 광 케이블, 및 머신 또는 컴퓨터에 의해 판독가능한 신호를 반송할 수 있는 음향파 또는 전자기파를 전달하는 무선 인터페이스일 수도 있다.

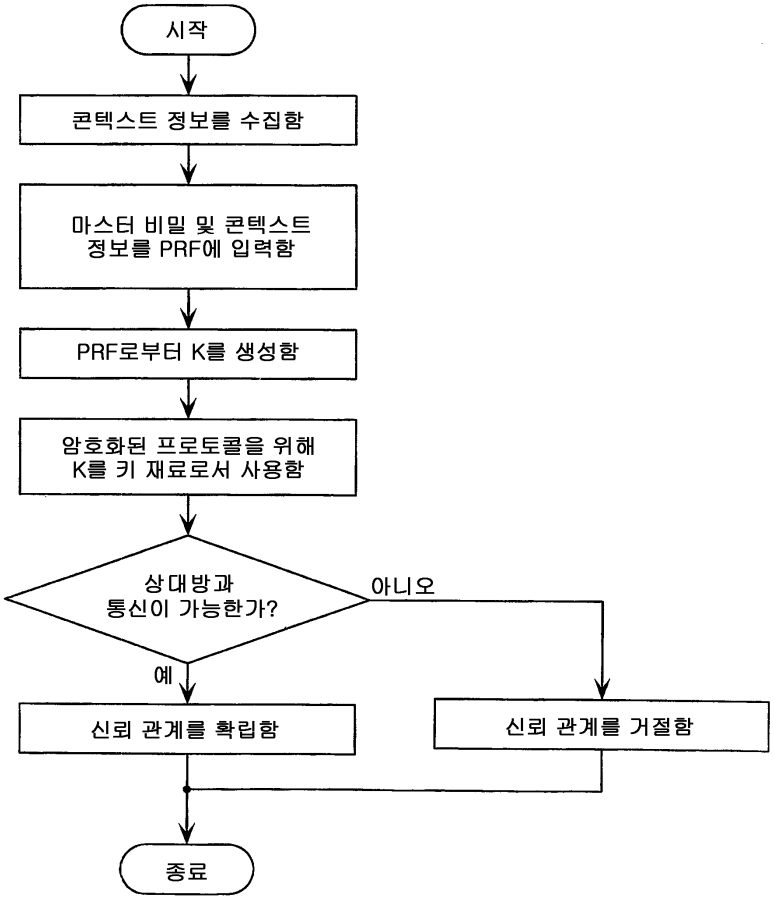
[0064] 마지막으로, 본 실시형태에서 설명한 제 1, 제 2 및 제 3 통신 엔터티 (31, 33 및 35) 는 각각 통신 디바이스 (32), 홈 캐리어 (34) 및 서비스 제공자 (36) 로 설명된다. 본 발명의 범주 내에서 상이한 구성이 가능하다. 예를 들어, 제 1 엔터티 (31) 는, 디바이스 대신에 네트워크 또는 캐리어의 일부인 라우터와 같은 상이한 형태를 가정할 수 있다. 유사하게, 제 2 및 제 3 엔터티 (33 및 35) 또한 전술한 바와 같이 상이한 형태를 가정할 수 있다. 예시적인 실시형태에서, 공유 비밀은 콘텍스트 정보와 함께 마스터 비밀로부터 생성되는 것으로 설명되었다. 또한, 공유 비밀은 전술한 식 (A) 에 리스트된 정보와는 다른 많은 정보로 생성될 수 있다. 예를 들어, GPS (Global Positioning System) 로부터의 좌표 또는 통신 엔터티의 전자 식별과 같은 넌-콘텍스트 정보가 식 (A) 로의 추가적인 입력으로서 기능할 수 있음은 확실하다. 식 (B) 또한 전술한 정보와는 다른 콘텍스트 정보를 포함할 수 있다. 한편, 예시적인 실시형태에서 설명한 바와 같은 모든 콘텍스트 정보가 공유 비밀을 생성하기 위해 포함되어야 하는 것은 아니다. 부분적 정보 또는 선택된 정보만 사용할 수 있다. 예를 들어, 전술한 바와 같이 공유 비밀의 생성을 위한 다양한 토폴로지 정보, 시간 기반 정보 및 거래 정보 대신에, 선택된 토폴로지 정보만 PRF 에 입력되어 공유 비밀에 도달할 수 있다. 또한, 예시적인 실시형태에서는, 통신 디바이스 (32) 및 홈 캐리어 (34) 가 콘텍스트 정보를 수집하는 엔터티로서 설명되었다. 서비스 제공자 (36) 가 콘텍스트 정보 수집의 의무를 수행하고 수집된 정보를 직접 또는 간접적으로 다른 자에게 전송하는 것은 명백하다. 또한, 본 실시형태에 관련하여 설명된 임의의 논리 블록, 회로 및 알고리즘은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 조합에 의해 구현될 수 있다. 당업자는, 본 발명의 범주 및 사상을 벗어나지 않으면서 형태 및 세부사항에서의 이러한 변경 및 또 다른 변경이 이루어질 수도 있음을 이해할 것이다.

도면

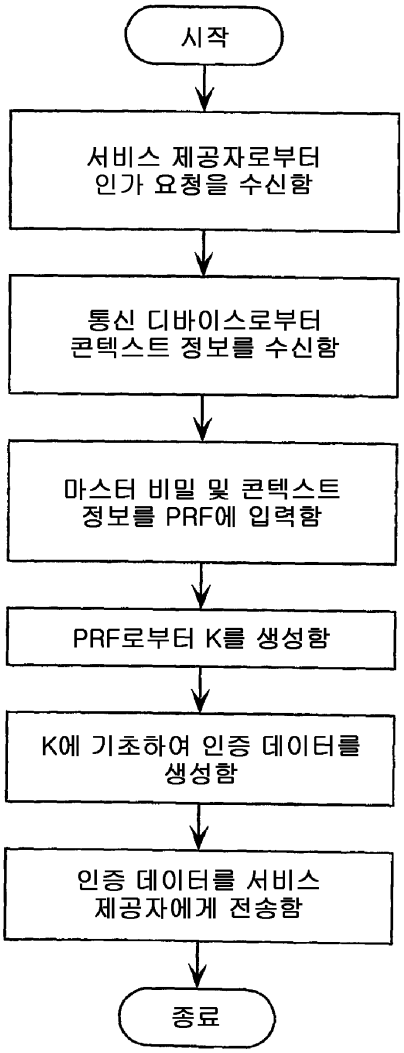
도면1


33
30
44
38
34
마스터 비밀
PRF
K
콘텍스트 정보
콘텍스트 정보
콘텍스트 정보
홈 캐리어
31
50
38
32
마스터 비밀
PRF
K
콘텍스트 정보
통신 디바이스
42
인증 데이터
인가 요청
46
40
서비스 요청
48
암호화된 통신
36
서비스 제공자
35

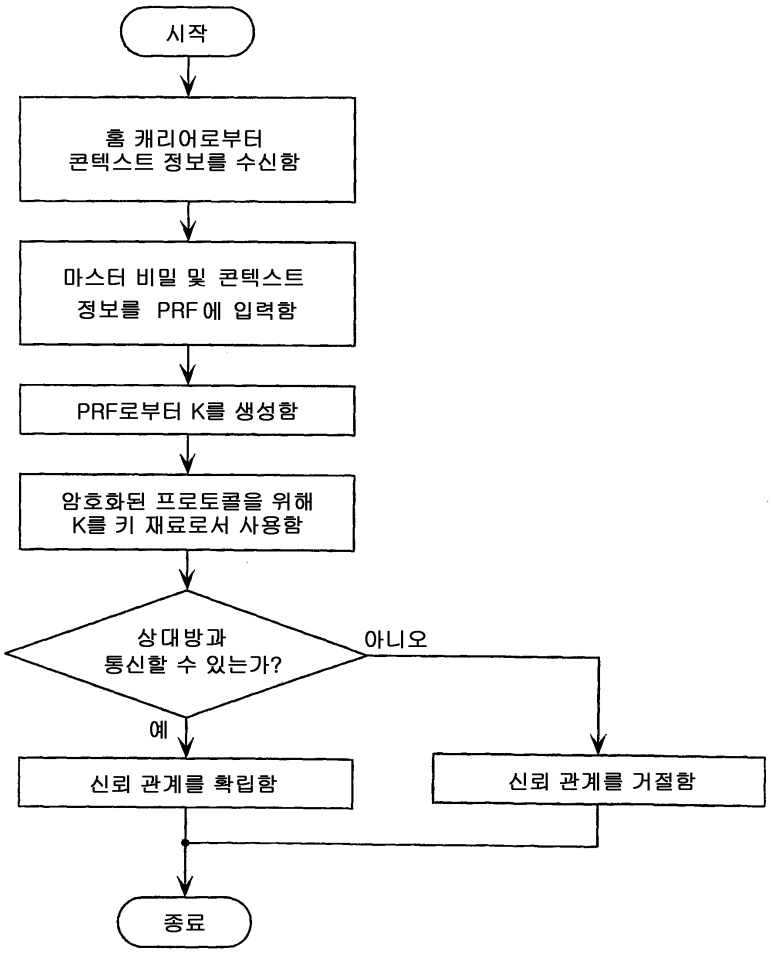
도면2a


시작
콘텍스트 정보를 수집함
마스터 비밀 및 콘텍스트 정보를 PRF에 입력함
PRF로부터 K를 생성함
암호화된 프로토콜을 위해 K를 키 재료로서 사용함
상대방과 통신이 가능한가?
아니오
예
신뢰 관계를 확립함
신뢰 관계를 거절함
종료

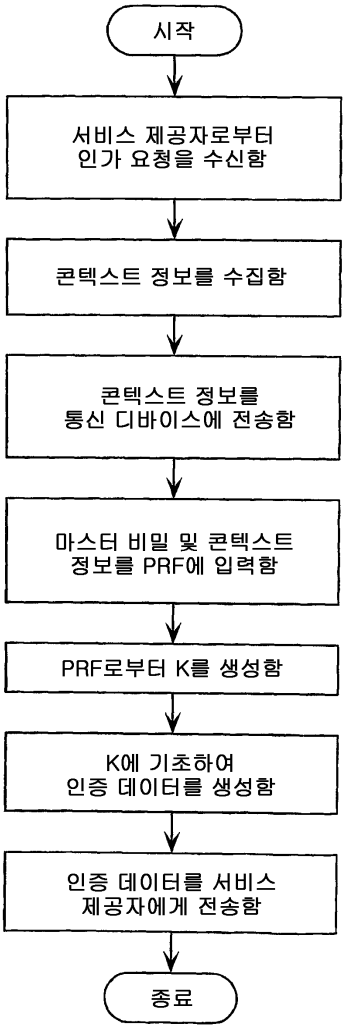
도면2b


시작
서비스 제공자로부터 인가 요청을 수신함
통신 디바이스로부터 콘텍스트 정보를 수신함
마스터 비밀 및 콘텍스트 정보를 PRF에 입력함
PRF로부터 K를 생성함
K에 기초하여 인증 데이터를 생성함
인증 데이터를 서비스 제공자에게 전송함
종료

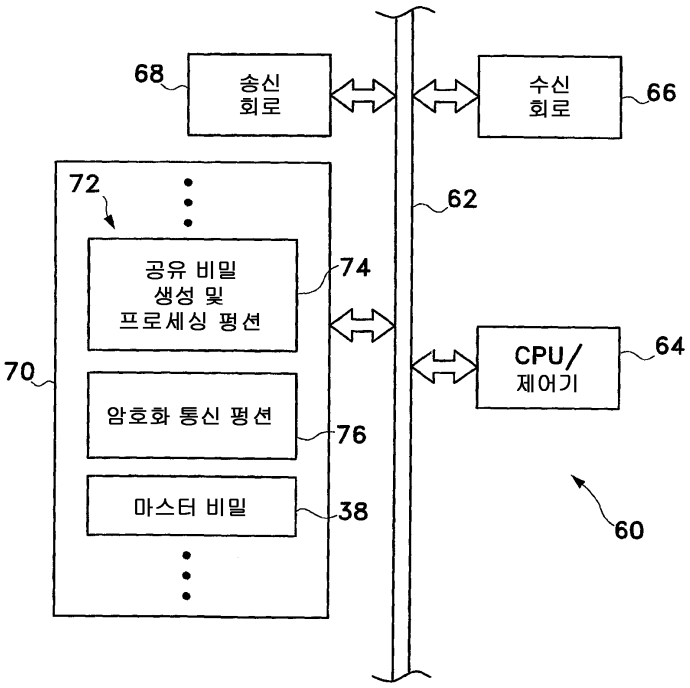
도면3a


시작
홈 캐리어로부터
콘텍스트 정보를 수신함
마스터 비밀 및 콘텍스트
정보를 PRF에 입력함
PRF로부터 K를 생성함
암호화된 프로토콜을 위해
K를 키 재료로서 사용함
상대방과
통신할 수 있는가?
아니오
예
신뢰 관계를 확립함
신뢰 관계를 거절함
종료

도면3b


시작
서비스 제공자로부터 인가 요청을 수신함
콘텍스트 정보를 수집함
콘텍스트 정보를 통신 디바이스에 전송함
마스터 비밀 및 콘텍스트 정보를 PRF에 입력함
PRF로부터 K를 생성함
K에 기초하여 인증 데이터를 생성함
인증 데이터를 서비스 제공자에게 전송함
종료

도면4


68
송신
회로
수신
회로
66
72
62
공유 비밀
생성 및
프로세싱 펑션
74
70
CPU/
제어기
64
암호화 통신 펑션
76
마스터 비밀
38
60