(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년06월30일
(11) 등록번호 10-1635244
(24) 등록일자 2016년06월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
H04W 12/06 (2009.01)
(21) 출원번호 10-2011-7025792
(22) 출원일자(국제) 2010년04월23일
심사청구일자 2015년03월23일
(85) 번역문제출일자 2011년10월28일
(65) 공개번호 10-2012-0007520
(43) 공개일자 2012년01월20일
(86) 국제출원번호 PCT/US2010/032303
(87) 국제공개번호 WO 2010/126800
국제공개일자 2010년11월04일
(30) 우선권주장
12/432,773 2009년04월30일 미국(US)
(56) 선행기술조사문헌
KR1020080034052 A*
US20050086496 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
크란츠 앤톤 더블유
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
파란데커 에이미
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
(뒷면에 계속)
(74) 대리인
제일특허법인

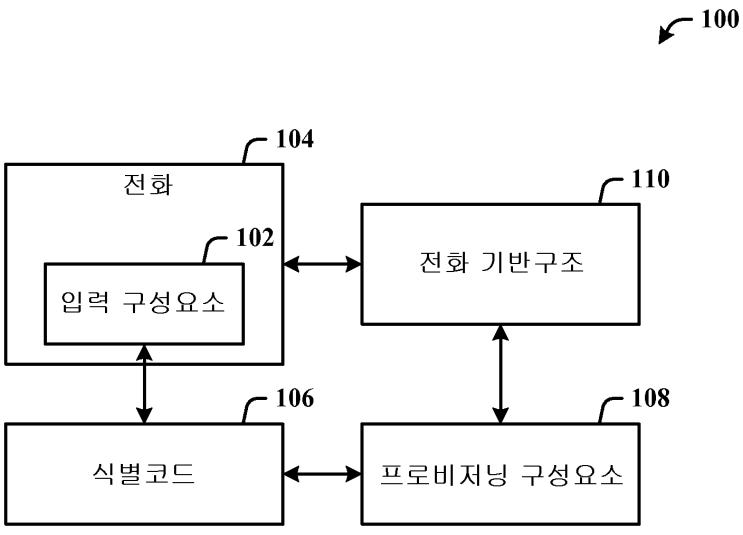
전체 청구항 수 : 총 20 항 심사관 : 양종필

(54) 발명의 명칭 **실시간 통신을 위한 사용자-기반 인증**

(57) 요 약

사용자가 네트워크 관리 사전구성없이 새 위치에 전화를 설정할 수 있도록 해주는 통신 시스템용 구조를 개시한다. 입력 컴포넌트(예를 들면 키패드)는 번호 내선 및 PIN을 수신한다. 내선은 사용자의 전화 내선이고, PIN은 관리상 배정될 수 있다. 로케이션 컴포넌트는 내선에 기초하여 기업 통신 서버의 위치 정보를 전화로 설정한다. 전화는 위치 정보를 사용하여 메시지를 기업 통신 서버로 송신한다. 등록 컴포넌트는 번호 내선에 기초하여 기업 통신 서버에 전화를 등록한다. 전화 주소는 전화로 반환된다. 인증 컴포넌트는 PIN에 기초하여 전화를 인증한다. 인증시에, 내선은 전화로 배정되고, 전화 통신은 그 위치로부터 송신 및 수신될 수 있다.

대 표 도



(72) 발명자

아이델만 바딤

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

나라야난 산카란

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

쿠마 나멘드라

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

세스 사친

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

명 세 서

청구범위

청구항 1

전화 번호 및 숫자로 된 개인 식별 번호(personal identification number: PIN)의 사용자 입력을 가능하게 하는 전화의 입력 컴포넌트와,

상기 전화 번호 및 숫자로 된 PIN을 수신하여 사용자이름 및 인증서를 검색하고 상기 사용자이름 및 인증서에 기초하여 상기 전화를 전화 기반구조(telephony infrastructure)에 설정하기 위한 설정 컴포넌트(provisioning component)와,

상기 입력 컴포넌트 및 상기 설정 컴포넌트 중 적어도 하나와 연관된 컴퓨터 실행가능 명령어들을 실행하는 마이크로프로세서

를 포함하는 컴퓨터로 구현된 통신 시스템.

청구항 2

제1항에 있어서,

상기 설정 컴포넌트는 SIP URI(session initiation protocol uniform resource identifier)를 상기 전화에 할당하고, 상기 SIP URI 및 PIN에 기초하여 상기 전화 기반구조에 액세스하는

컴퓨터로 구현된 통신 시스템.

청구항 3

제1항에 있어서,

상기 전화 번호 및 숫자로 된 PIN에 기초하여 상기 전화 기반구조에 대해 상기 전화를 인증하기 위한 인증 컴포넌트

를 더 포함하는 컴퓨터로 구현된 통신 시스템.

청구항 4

제1항에 있어서,

상기 전화 기반구조는 IP(Internet protocol) 전화 음성 메시지를 처리하기 위한 기업 메시징 서버(enterprise messaging server)를 더 포함하는

컴퓨터로 구현된 통신 시스템.

청구항 5

제1항에 있어서,

상기 전화 기반구조의 IP 주소 또는 도메인 이름(domain name) 중 적어도 하나를 상기 전화에 제공하기 위한 로케이션 컴포넌트(location component)를 더 포함하는 컴퓨터로 구현된 통신 시스템.

청구항 6

제1항에 있어서,

상기 전화 번호 및 숫자로 된 PIN은 전체 전화 번호(full phone number) 및 내선 번호(extension number) 중 하나와 PIN을 포함하는

컴퓨터로 구현된 통신 시스템.

청구항 7

숫자로 된 사용자 식별자 및 PIN을 전화로부터 입력하는 입력 컴포넌트와,

기업 통신 서버의 위치 정보를 내선에 기초하여 상기 전화에 제공하는 로케이션 컴포넌트와,

상기 숫자로 된 사용자 식별자와 연관된 상기 전화의 전화 주소를 설정하는 설정 컴포넌트와,

상기 PIN에 기초하여 상기 전화를 인증하는 인증 컴포넌트와,

상기 기업 통신 서버로부터의 인증서를 후속 인증에 사용되도록 상기 전화에 전송하는 인증서 컴포넌트와,

상기 입력 컴포넌트, 상기 로케이션 컴포넌트, 상기 설정 컴포넌트, 상기 인증 컴포넌트 및 상기 인증서 컴포넌트 중 적어도 하나와 연관된 컴퓨터 실행가능 명령어들을 실행하는 마이크로프로세서

를 포함하는 컴퓨터로 구현된 통신 시스템.

청구항 8

제7항에 있어서,

상기 기업 통신 서버는 IP 전화를 위한 IP 서버를 더 포함하는

컴퓨터로 구현된 통신 시스템.

청구항 9

제7항에 있어서,

상기 전화 주소는 SIP 메시지를 상기 기업 통신 서버에 전송하기 위한 SIP URI를 포함하는

컴퓨터로 구현된 통신 시스템.

청구항 10

제7항에 있어서,

상기 숫자로 된 사용자 식별자는 개인 전화 번호 및 내선 중 하나와 네트워크 신원(identity)의 속성이고, 상기 PIN은 사전에 할당되는

컴퓨터로 구현된 통신 시스템.

청구항 11

제7항에 있어서,

상기 로케이션 컴포넌트는 상기 기업 통신 서버의 IP 주소 및 전체 주소 도메인 이름(fully qualified domain name: FQDN)을 상기 전화에 리턴(return)하기 위한 동적 호스트 구성 서버를 더 포함하는

컴퓨터로 구현된 통신 시스템.

청구항 12

제7항에 있어서,

상기 기업 통신 서버는 SIP URI 및 상기 PIN을 사용하여 상기 전화를 인증하는

컴퓨터로 구현된 통신 시스템.

청구항 13

머신 판독가능한 명령어들을 실행하는 컴퓨터 시스템에 의해 수행되는, 컴퓨터로 구현된 통신 방법으로서,

숫자로 된 사용자 식별자와 PIN을 사용자로부터 전화를 통해 입력받는 단계와,

기업 통신 서버의 위치 정보를 내선에 기초하여 상기 전화에 제공하는 단계와,

상기 사용자 식별자와 연관된 상기 전화의 전화 주소를 설정하는 단계와,

상기 PIN을 사용하여 상기 기업 통신 서버에 대해 사용자의 전화를 인증하는 단계와,

상기 사용자 식별자 및 상기 PIN에 기초하여 상기 전화에 인증서를 발행하는 단계와,

상기 인증서를 사용하여 상기 기업 통신 서버에 상기 전화를 등록하는 단계

를 포함하는 컴퓨터로 구현된 통신 방법.

청구항 14

제13항에 있어서,

상기 인증서로부터 공개키를 송신하여 데이터베이스에 저장함으로써 상기 전화를 설정하는 단계를 더 포함하는 컴퓨터로 구현된 통신 방법.

청구항 15

제13항에 있어서,

상기 사용자 식별자와 상기 PIN에 기초하여 상기 전화에 사용자 SIP URI를 송신하는 단계를 더 포함하는 컴퓨터로 구현된 통신 방법.

청구항 16

제13항에 있어서,

인증서 웹서비스 주소와 레지스트라(registrar) FQDN을 상기 전화로 송신하는 단계를 더 포함하는 컴퓨터로 구현된 통신 방법.

청구항 17

제13항에 있어서,

상기 전화를 사용하여 인증서 설정 웹서비스(certificate provisioning web service)를 발견하고(discovering), 인증서 체인(certification chain)을 다운로드하기 위하여 상기 웹서비스에 연결되는 단계를 더 포함하는 컴퓨터로 구현된 통신 방법.

청구항 18

제17항에 있어서,

상기 전화로부터 상기 인증서 설정 웹서비스로 인증서 서명 요청을 생성 및 제출하는 단계를 더 포함하는 컴퓨터로 구현된 통신 방법.

청구항 19

제13항에 있어서,

통신 서버에 의해 상기 인증서를 서명하는 단계를 더 포함하는 컴퓨터로 구현된 통신 방법.

청구항 20

제13항에 있어서,

상기 전화를 등록하는 단계 이후에, 상기 전화에 대한 모든 후속의 등록을 위해,

SIP 메시지를 레지스트라 FQDN으로 송신하는 단계와,

상기 인증서를 인증하는 단계와,

상기 인증서 및 인증서 파라미터에 기초하여 상기 전화를 허가하는 단계

를 더 포함하는 컴퓨터로 구현된 통신 방법.

발명의 설명

배 경 기 술

[0001] 통신 매체에서 융합(convergence)의 경우, 음성, 비디오, 인스턴트 메시징(instant messaging) 및 회의(conferencing)를 포함한 각종 상이한 모드의 통신이 단일 사용자 신원(user identity) 위주로 통합될 수 있다. 컴퓨터상에서 실행중인 통신 애플리케이션은 사용자에 의해 컴퓨터의 로그온시 사용되는 동일 신원을 사용할 수 있다. 사용자 신원은 전형적으로 로그인 사용자명과 패스워드(password)의 조합이며, 이들 로그인 사용자 이름과 패스워드의 각각은 전형적으로 컴퓨터 키보드로 입력되는 영숫자 문자열을 포함할 수 있다.

[0002] 또한 IP(Internet protocol) 전화와 같은 장치는 컴퓨터와 동일한 네트워크로 연결될 수 있고, 따라서 전형적으로 로그인을 위한 사용자 신원과 동일한 사용자명/패스워드 조합을 사용할 수 있다. 특정 위치에 IP 전화를 처음 설정(provisioning) 하는 경우에(예를 들면 새 사무실 배정시), 사용자는 네트워크로 설정될 수 있도록 전화를 위한 사용자 신원을 직접 입력한다. 그러나 IP 전화는 컴퓨터 키보드를 포함하지 않고, 오히려 예를 들어 12 키 숫자 키패드를 포함한다. 사용자가 전화 키패드를 사용하여 사용자명과 패스워드에 대응한 등가의 문자 코드를 입력하는 일은 번거롭고 오류가 발생하기 쉬운 과정일 수 있다.

[0003] 설정(provisioning)을 위한 다른 접근방안이 알려져 있다. 예를 들면 전화의 물리적 특성인 IP 전화 장치의 MAC(media access control) 주소와 같은 것을 사용하는 것과 같이 하드웨어 특정적 정보를 사용할 수 있다. 장치의 MAC 주소는 네트워크에서 특정 전화선으로 배정된다. 그러나 설정이 쉽지 않으며, MAC 주소와 사용자의 전화 내선(telephone extension)을 상호관련시키기 위해 전형적으로 관리자 또는 다른 전화 지원(telephony support)을 요구한다. 이것은 특히 사용자가 하나의 물리적 위치로부터 다른 물리적 위치로 빈번히 이동하는 기업(enterprises)에서 사용자 설정의 비용을 증가시킨다. 게다가 이 접근 방안에서, IP 전화 장치 그 자체는 사용자 신원을 포함하지 않고, 따라서 장치 신원을 사용자 신원으로 연결시키는데 별개의 데이터베이스를 필요로 하므로, 배치 비용을 더 증가시킨다.

발명의 내용

과제의 해결 수단

[0004] 다음은 여기에 기술된 일부 신규 실시예에 대한 기본적인 이해를 위해 간단한 요약을 제공한다. 이 요약은 광범위한 개요가 아니며, 주요/중대한 요소를 확인하거나 또는 이의 범주를 상술하려는 것이 아니다. 단지 차후에 제공되는 보다 상세한 설명에 대한 서두로서 간단한 형태로 일부 개념을 제공하려는 것이다.

[0005] 그를 위하여, 사용자가 관리자로부터의 추가 전화 지원이 필요없이 새 위치에 IP 전화를 설정할 수 있는 구조를 개시한다. 사용자는 번호 사용자 식별자(예를 들면 전체 전화번호, 내선 번호 등)를 배정받고, 통신 시스템에서 사용자를 식별하기 위한 번호 PIN(personal identification number)을 제공받는다. 사용자 식별자 및 PIN의 입력시에 시스템이 사용자명, 서버에 의해 발행된 인증서(certificate)를 조사하도록, 사용자 식별자 및 PIN은 사용자 신원과 관련된다. 그러면, 전화는 인증서를 사용하여 후속하여 기업 통신 서버(enterprise communications server)를 인증하고 로그온한다.

[0006] 통신 시스템은 사용자 내선(user extension) 및 PIN을 입력하기 위한 전화 키패드일 수 전화의 입력 컴포넌트를 포함한다. 통신 시스템은 전화로부터 사용자 식별자 및 PIN을 수신한다. 전화는 내선 및 PIN에 기초하여 전화 기반구조로 설정된다. 설정은 기업 통신 서버에 전화를 등록하고, 사용자 식별자에 기초하여 전화 주소를 전화를 송신하는 것을 포함할 수 있다. 전화는 PIN에 기초하여 기업 통신 서버로 인증된다.

[0007] 이 대신에, PIN은 서버로 인증하는데 사용될 수 있는 다른 크리덴셜(credentials)을 등록시키는데 사용될 수 있다. 이런 식으로, 전화 설정은 서비스 도메인의 명시를 필요로 하지 않고 전화 서비스의 자동 발견(automatic discovery)을 가능하게 하기 위하여 사용자 신원과 연결된다. 컴퓨터로 로그온하는데 사용되는 크리덴셜은 새 위치에서 사용자를 인증하고, 관리자로부터의 사전구성없이 사용자로/로부터 콜(calls)을 경로배정(route)하는데 사용된다. 사용자가 번호 사용자 식별자와 PIN을 입력할 때, 네트워크 서버는 관련된 사용자를 동적으로 조사하고, 사용자에 의해 사용되는 전화를 결정하고, 사용자에게 사용자 신원을 반환한다. 그 후에, 전화는 내선과 PIN에 기초하여 사용자를 인증하거나, 또는 사용자 신원을 사용하여 사용자를 위해 크리덴셜을 등록한다. 그러면, 예를 들어 새 사용자가 동일 위치에서 전화를 설정하거나, 또는 상이한 위치에서 다수의 전화를 설정할 때까지, 사용자는 그 위치에서 전화를 사용할 수 있다.

[0008] 그러나 다른 실시예에서, 전화는 일단 확인되고 서명된 인증서를 제공받을 수 있고, 초기 연결 설정 과정후에 후속한 모든 연결에 대한 전화 인증을 위해 사용될 수 있다.

[0009] 상기 및 관련 목적을 성취하기 위해, 다음의 설명 및 첨부 도면과 관련하여 소정 실례 양상을 여기에 기술된다. 이들 양상은 여기에 개시된 원리가 실행될 수 있는 다양한 방식을 나타내고, 모든 양상과 이의 등가물은 청구 주제의 범주내에 포함된다. 다른 이점과 신규 특징은 도면과 함께 고려시에 다음의 상세한 설명으로부터 명백해질 것이다.

도면의 간단한 설명

[0010] 도 1은 통신을 수행하기 위한 컴퓨터 구현 시스템을 도시하는 도면.

도 2는 실시간 통신을 수행하기 위한 등록 및 인증을 포함한 시스템을 도시하는 도면.

도 3은 실시간 통신에서 사용자 기반 인증을 수행하기 위한 시스템에 사용될 수 있는 추가 컴포넌트를 도시하는 도면.

도 4는 사용자 기반 인증을 수행하기 위한 시스템의 다른 실시예를 도시하는 도면.

도 5는 사용자 기반 인증을 수행하기 위한 시스템의 추가 엔티티를 도시하는 도면.

도 6은 사용자 기반 인증을 수행하기 위한 시스템의 구현을 도시하는 도면.

도 7은 사용자 기반 인증을 수행하기 위한 시스템의 데이터 및 메시지 흐름도.

도 8은 사용자 기반 인증을 수행하기 위한 시스템 구현의 데이터 및 메시지 흐름도.

도 9는 실시간 통신에서 사용자 기반 인증의 방법을 도시하는 도면.

도 10은 사용자 기반 인증 방법의 다른 양상을 도시하는 도면.

도 11은 사용자 기반 인증 방법의 또 다른 양상을 도시하는 도면.

도 12는 인증서를 사용하는 통신 방법을 도시하는 도면.

도 13은 인증서를 사용하는 도 12의 통신 방법의 추가 양상을 도시하는 도면.

도 14는 인증서를 사용하는 도 12의 통신 방법의 추가 양상을 도시하는 도면.

도 15는 개시된 구조에 따라서 실시간 통신으로 사용자 기반 인증을 제공하기 위해 동작가능한 컴퓨팅 시스템의 블록도.

도 16은 사용자 기반 인증을 제공하기 위해 동작가능한 예시적인 컴퓨팅 환경을 도시하는 도면.

발명을 실시하기 위한 구체적인 내용

[0011] 개시된 통신 구조는 사용자에게 네트워크 관리자 사전구성없이 새로운 또는 기존 위치에 전화를 설정할 수 있도록 해준다. 번호 사용자 식별자(예를 들면 전화번호 또는 내선)와 PIN(personal identification number)은 전화 키패드를 통해 입력된다. 기업 통신 서버의 위치 정보는 내선에 기초하여 전화로 제공된다. 위치 정보는 FQDN(fully qualified domain name)과 IP 주소를 포함할 수 있다. 위치 정보는 DHCP를 통해 자동적으로 제공될 수 있고, 사용자에 의한 번호 및 PIN 입력을 필요로 하지 않는다. 전화는 위치 정보를 사용하여 기업 통신 서버로 메시지를 송신한다.

[0012] 전화는 번호 사용자 식별자에 기초하여 기업 통신 서버와 함께 등록된다. 이 대신에, 서버는 전화가 통신 서버에 의해 확인될 수 있는 크리덴셜 등록에 사용하는 사용자 신원을 검색하기 위해 PIN을 사용할 수 있다. 전화에 뿐만 아니라, 전술한 접근방안은 비디오 단말기, 전자 화이트보드, 룸기반 회의 시스템 등으로 확장될 수 있다. 전화 주소(예를 들면 SIP URI, Tel URI)가 전화로 반환된다. 전화는 PIN에 기초하여 인증된다. 인증시, 실시간 전화 통신이 송신되어, 그 위치로부터 수신 및 송신될 수 있다.

[0013] 기업 통신 서버는 IP 서버일 수 있고, 전화 주소는 기업 통신 서버로 SIP 메시지를 송신하기 위한 SIP(session initiation protocol) URI(uniform resource identifier)(예를 들면 nobody@nowhere-domain.com)일 수 있다.

또한 전화 주소는 전화 URI일 수 있다(예를 들면 111-222-3333@nowhere-domain.com). 번호 사용자 식별자는 사용자의 개인 전화번호 또는 내선, 그리고 사용자의 네트워크 신원의 속성일 수 있다. PIN은 예를 들어 네트워크 관리자 또는 다른 엔티티에 의해 사용자에게 사전배정될 수 있다.

[0014] 기업 통신 서버의 IP 주소와 DNS(domain name system) 레코드를 전화로 반환하기 위해 DHCP(dynamic host configuration protocol) 서버를 제공한다. DHCP 서버는 DHCP 서버의 소정 기능을 수행할 수 있고 DHCP 응답시에 그의 위치(FQDN과 IP 주소)를 반환할 수 있는 기업 통신 서버의 위치를 반환하도록 구성될 필요가 없다. 기업 통신 서버는 PIN을 가진 전화 주소를 참조하기 위해 인증을 수행할 수 있다.

[0015] 이제 도면을 참조하면, 동일한 참조번호는 도면에 걸쳐 동일 요소를 참조하기 위해 사용된다. 다음 서술에서 설명을 위하여, 철저한 이해를 제공하기 위해 다수의 특정한 상세사항을 설명한다. 그러나 신규 실시예는 이들 특정 상세사항없이 실행될 수 있다. 다른 경우, 설명을 용이하게 하기 위하여 잘 알려진 구조 및 장치를 블록도에 도시한다. 본 발명은 청구 주제의 사상 및 범주내에 있는 모든 변경, 등가물 및 대안을 포함하려고 한다.

[0016] 도 1은 개시된 구조에 따라서 실시간 통신을 위한 사용자 기반 인증을 수행하기 위한 컴퓨터로 구현된 시스템(100)을 도시한다. 전화(104)의 입력 컴포넌트(102)는 식별 코드(identification code)(106)를 입력하는데 사용된다. 입력 컴포넌트(102)는 숫자 0-9와 또한 다른 문자와 기호 * 및 #에 대응한 키뿐만 아니라 키를 위한 멀티기능 능력을 가진 멀티디지트(예를 들면 3x4) 전화 번호 키패드일 수 있는데, 이로 제한되지는 않는다. 임의 적당한 키패드 또는 영숫자 입력 시스템이 개시된 실시예를 벗어나지 않고서도 사용될 수 있다는 것을 알아야 한다. 식별 코드는 내선 번호 및/또는 PIN일 수 있고, 여기서 내선 번호는 사용자가 호출받을 수 있는 기업 구조내 사용자의 전화 내선이다. PIN은 네트워크 관리 구성 동안에 사용자에게 처음 배정된 숫자열(numeric string)일 수 있다. 사용자는 보안을 위하여 PIN을 변경할 수 있다.

[0017] 또한 시스템(100)은 식별 코드(106)를 수신하고, 식별 코드(106)에 기초하여 전화 기반구조(110)로 전화(104)를 설정하기 위한 설정 컴포넌트(108)를 포함한다. 설정 컴포넌트(108)는 식별 코드(106)에 기초하여 사용자 신원을 액세스하고, 사용자 내선이 기업내 특정 전화(유선 또는 무선)로 배정될 수 있도록 등록 및 인증을 자동으로 수행한다. 이런 식으로, 설정 컴포넌트(108)는 사용자가 전화(104)를 설정할 수 있게 하고, 이로써 네트워크 관리의 개입없이 전화 기반구조(110)를 통해 통신할 수 있게 한다.

[0018] 도 2는 실시간 통신을 수행하기 위한 등록 및 인증을 포함한 시스템(200)을 도시한다. 설정 컴포넌트(108)는 SIP URI(202)를 전화(104)로 배정한다. SIP URI(202)와 식별 코드(106)에 기초하여 전화 기반구조(110)를 액세스한다. 인증 컴포넌트(204)는 식별 코드(106)에 기초하여 전화 기반구조(110)로 전화(104)를 인증한다.

[0019] 도 3은 실시간 통신에서 사용자 기반 인증을 수행하기 위한 시스템(100)에 사용될 수 있는 추가 컴포넌트(300)를 도시한다. 전화 기반구조(110)는 IP 전화 메시지(304)를 처리하기 위해 기업 통신 서버(302)를 포함할 수 있다. 로케이션 컴포넌트(location component)(306)는 기업 통신 서버(302)의 도메인명 또는 IP 주소(308)를 전화(104)로 제공한다.

[0020] 도 4는 사용자 기반 인증을 수행하기 위한 시스템(400)의 다른 실시예를 도시한다. 입력 컴포넌트(102)는 전화(104)를 통해 번호 사용자 식별자(402)(예를 들면 전화번호 또는 내선)와 PIN(404)을 입력 및 수신하기 위해 사용된다. 입력 컴포넌트(102)는 예를 들어 전화(104)의 멀티버튼 키패드일 수 있지만, 또한 임의 적당한 입력 인터페이스를 사용할 수 있다는 것을 알아야 한다. 사용자 식별자(402)는 사용자의 개인 전화 내선일 수 있고, 기업 전화 기반구조내에 사용되는 바와 같이 사용자의 네트워크 신원의 속성이다. 또한 사용자 식별자(402)는 사용자가 도달할 수 있는 전화 기반구조내 위치를 정의하는데 사용될 수 있다.

[0021] 도 4에 도시된 바와 같이, PIN(404)은 사용자에게 사전배정될 수 있는 사용자와 관련된 개별화된 번호 코드이다. 사용자 또는 관리자는 예를 들어 보안을 향상시키고, 그리고/또는 사용자로 하여금 기억하기에 보다 적당한 상이한 수를 선택할 수 있도록 해주기 위하여 PIN(404)을 변경할 수 있다. 시스템(400)은 사용자 식별자(402) 및 PIN(404)을 사용자의 네트워크 신원과 연관시키는데, 이는 네트워크를 통해 사용자를 식별하고 로그인시키는데 사용되는 사용자명/인증서 조합일 수 있다.

[0022] 또한 도 4에 도시된 바와 같이, 로케이션 컴포넌트(306)는 사용자의 네트워크(예를 들면 서브넷)에 기초하여 기업 통신 서버(302)의 위치 정보를 전화(104)로 제공한다. 이런 식으로, 전화(104)는 기업 통신 서버(302)의 주소를 얻어 전화(104)로부터의 후속한 음성 통신에 지시한다.

[0023] 전화(104)의 현 물리적 위치에 대한 네트워크 전화 회선이 내선(402)에 의해 지명된 사용자의 특정 전화번호와

관련될 수 있도록, 설정 컴포넌트(108)는 전화(104)로 전화 주소를 반환한다.

[0024] 도 4에 더 도시된 바와 같이, 인증 컴포넌트(204)는 PIN(404)에 기초하여 전화(104)를 인증한다. 인증 컴포넌트(204)는 PIN(404)와 관련된 사용자명/패스워드 신원 크리덴셜에 대해 PIN(404)을 조사한다. 인증 컴포넌트(204)는 특정 내선(402)에서 전화(104)를 사용하는 사용자가 사실상 내선(402)으로 배정된 올바른 사용자인지를 확인하기 위해 PIN(404)을 사용한다. 인증시에, 사용자는 내선(402)에서 전화(104)상에서 전화 메시지를 송신 및 수신할 수 있다. 다른 실시예에서, 기업 통신 서버(302)는 사용자를 위해 인증서를 요청할 수 있고, 그 후에 인증서를 반환할 수 있다.

[0025] 도 4에 더 도시된 바와 같이, 인증서를 기업 통신 서버(302)로부터 전화(104)로 송신하기 위한 인증 서비스(406)를 제공한다. 인증서는 후속한 인증에 사용된다. 기업 통신 서버(302)는 전화 주소(예를 들면 SIP URI 또는 전화 URI)와 함께 전화로 환송하기 위한 인증서를 생성한다. 인증서는 번호 내선(402)과 PIN(404)을 사용한 인증 후에 전화(104)로 발행되고, 후속된 인증은 이 인증서를 사용한다.

[0026] 전술한 방식에서, 전화(404)는 시동(startup)시에 단일 시간에 설정될 수 있다. 사용자 PIN이 만료되거나 또는 로그인 정보가 임의 방식으로 변경된다면, 설정을 갱신할 수 있다. 따라서 시스템(400)은 기반구조로 연결하기 위해 전화(104)를 부트스트래핑(bootstrapping)할 수 있다.

[0027] 도 5는 사용자 기반 인증을 수행하기 위한 시스템의 추가 엔티티(500)를 도시한다. 기업 통신 서버(302)는 IP 전화를 위한 IP 서버(502)일 수 있다. 이런 식으로, 전화(104)는 내부 기업 네트워크내 사용되는 IP 전화 네트워크의 일부일 수 있다. 전화 주소는 IP 서버(502)로 SIP 메시지를 송신하기 위한 SIP URI(504)를 포함할 수 있다. 로케이션 컴포넌트(306)는 IP 서버(502)의 IP 주소(508) 및 FQDN(510)을 전화(104)로 반환하기 위해 DHCP(dynamic host configuration protocol) 서버(506) 기반구조를 포함할 수 있다.

[0028] 도 5에 도시된 바와 같이, 기업 통신 서버(302)는 사용자 PIN에 기초하여 사용자를 인증하고 인증 메시지를 IP 서버(502)로 환송하기 위해 인증하기 위한 인증 기능을 제공할 수 있다. 도 4의 시스템(400)은 사용자로 하여금 기업 네트워크 내부의 전화(104)를 설정할 수 있도록 해준다. 따라서 기업 네트워크의 IP 서버(502)가 도메인을 자동적으로 인식할 수 있으므로, 전화(104)를 통해 도메인을 액세스할 필요가 없다.

[0029] 도 6은 사용자 기반 인증을 수행하기 위한 시스템(600)의 일반적인 구현을 도시한다. 시스템(600)은 사용자 또는 관리자가 전화상에 사용자 PIN을 입력할 수 있도록 해주어, 사용자 신원으로 전화를 설정한다. 시스템(600)은 IP 서버일 수 있는 기업 통신 서버(302)로 연결된 IP 전화(602)를 사용하여 PIN 인증을 가능하게 한다.

[0030] 도 6에 도시된 바와 같이, IP 전화(602)는 숫자 키패드를 포함할 수 있다. 전화(602)를 설정하기 위해, 사용자는 키패드를 통해 관련된 내선과 공동 PIN을 입력한다. PIN은 관리자에 의해 제공되며, 사용자에 의해 변경될 수 있다. PIN은 네트워크상에서 다중 메시징 서비스를 액세스하기 위해 통합 메시징 PIN과 같은 적당한 임의 개인 코드일 수 있다. 내선은 사용자 신원의 속성이다.

[0031] 내선과 PIN을 입력시에, 전화(602)는 DHCP 서버(506)로부터 IP 주소를 요청한다. DHCP 서버(506)는 기업 통신 서버(302)의 위치를 알려주는 IP 주소 및 DNS 레코드를 전화(602)로 반환한다. 위치 정보를 수신시에, IP 전화(602)는 기업 통신 서버(302)로 사용자 내선 및 PIN을 포함한 http://request의 형태인 등록 요청을 송신한다.

[0032] 기업 통신 서버(302)는 내선에 기초하여 사용자의 신원(604)(예를 들면 SIP URI 또는 전화 URI)을 액세스한다. 기업 통신 서버(302)는 사용자 인증 요청에서 신원(604)을 기업 통신 서버(302)로 송신한다. 기업 통신 서버(302)는 사용자 PIN에 기초하여 사용자를 인증하고, 신원(604)을 전화로 송신하고, 또한 추가적으로 인증서(606)를 환송한다. 기업 통신 서버(302)는 SIP URI와 함께 IP 전화(602)로 응답을 환송한다. 전화(602)는 신원(604)(예를 들면 SIP URI 또는 Tel URI)를 얻은 후에, 신원(604)과 인증서(606)를 포함한 SIP 등록 요청을 기업 통신 서버(302)로 송신한다. 시스템(600)은 IP 전화 음성 메시지를 처리하기 위해 메시징 서버(608)를 더 포함한다.

[0033] 도 7은 사용자 기반 인증을 수행하기 위한 시스템의 데이터 및 메시지 흐름도(700)를 도시한다. 흐름도(700)는 PIN 기반 인증을 사용하여 어떻게 설정 및 인증을 하는 지를 보여준다. 흐름도(700)는 IP 전화(702), 기업 서버(704), DHCP 서버(706) 및 인증 서버(708) 간의 통신을 도시한다. 단계(710)에서, 전화(702)는 통신 네트워크로 연결시에 DHCP 서버(706)로부터 IP 주소를 요청한다. 단계(712)에서, 사용자가 DNS 발견(DNS discovery)을 위해 도메인명을 제공할 필요가 없도록, DHCP 서버(706)는 기업 서버(704)의 위치를 IP 전화(702)로 반환

한다. 이 대신에, 위치가 기업 서버(704) 그 자체에 의해 반환될 수 있다.

[0034] 단계(714)에서, 사용자는 IP 전화(702)를 통해 관련된 내선 및 PIN을 입력한다. 이 조합은 기업 서버(704)로 사용자를 고유하게 식별한다. 단계(716)에서, 내선 및 PIN은 설정 시퀀스 일부로서 http://message에 포함된 기업 서버(704)로 송신된다. 단계(718)에서, 기업 서버(704)는 사용자 SIP URI를 검색하기 위해 내선을 사용한다. 이것은 기업 서버(704)상에 로컬 데이터베이스에서 사용자 내선을 액세스함으로써, 또는 인증 서버(708)로 요청을 송신함으로써 성취될 수 있다.

[0035] 단계(720)에서 기업 서버(704)는 인증 서버(708)로부터 사용자의 인증을 요청하고, 단계(722)에서 인증 서버(708)는 PIN을 사용하여 사용자를 인증한다. 단계(724)에서, 기업 서버(704)는 설정 응답의 일부로서 IP 전화(702)로 SIP URI를 반환한다. 단계(726)에서, IP 전화(702)는 인증서를 사용하여 사용자를 인증하는 기업 서버(704)로 SIP 등록을 송신한다. 단계(728)에서, 기업 서버(704)는 대역내 설정을 IP 전화(702)로 송신한다. 단계(730)에서, IP 전화(702)는 후속하여 SIP URI를 사용하여 SIP 메시지를 DHCP 서버(706)로 송신한다.

[0036] 네트워크 도메인을 검색하기 위해 임의 라인 내선을 사용하기 보다는 전술한 양상에 부가적으로, 시스템은 전체 전화번호를 포함하도록 내선될 수 있다. 외부 IP 전화망은 사용자로 하여금 나라 코드, 구역 코드, 로컬 교환 및 특정 내선을 포함한 전체 전화번호를 입력함으로써 전화를 설정할 수 있도록 구성될 수 있다. 이 정보는 그 번호 관련된 권한있는 도메인(authoritative domain)을 검색할 수 있는 네트워크로 사용자를 식별하기 위해 PIN과 함께 입력될 수 있다. 이런 식으로, 사용자는 IP 전화를 구매하고, 이를 플러그인하고, 번호를 입력하고, 사용자의 집에 전화를 배선할 전화 또는 캐이블 기술자없이 설정될 수 있다.

[0037] 전술한 양상에 부가적으로, 사용자가 수행한 설정은 또한 셀폰으로 확장될 수 있다. GSM(global system for mobile communications)하에서 동작하는 셀폰의 경우, 네트워크 관리자는 사용자가 수행한 설정을 가능하게 하기 위해 셀폰으로 삽입시킬 수 있는 사전제공된 SIM(subscriber identity module)을 사용자에게 준다. CDMA(code division multiple access) 시스템과 동작하는 셀폰의 경우, 네트워크는 전화를 처음 파워업시에 사용자에게 촉구한다. 사용자는 전화를 설정하기 위해 셀폰 번호와 PIN을 입력할 수 있다.

[0038] 전술한 바와 같이, DHCP 서버는 추진될 수 있는 다수의 구성가능한 옵션을 제공한다. DHCP 서버는 DHCP 서버로 연결된 임의 엔드포인트로 FQDN을 반환하는 "옵션 120"을 포함한다. 옵션(120)은 전화로 도메인을 송신하기 위해 여기에 사용된다. 그러면 전화는 SRV(service) 질의를 사용하여, 서버를 찾아낸다. 예를 들면 "nobody.com"과 같은 FQDN의 경우, DHCP 서버는 그 FQDN을 위한 서브서버의 IP 주소를 자동으로 발견할 수 있다. FQDN을 검색시에, 정보는 등록 동안에 전화에 의해 기업 서버로 제공된다.

[0039] 도 8은 사용자 기반 인증을 수행하기 위한 시스템의 데이터 및 메시지 흐름도(800)를 도시한다. 흐름도(800)는 IP 전화(802), DHCP 서버/레지스트라((804)(여기서 레지스트라(registrar)는 기업 통신 서버의 일부임), 인증서 설정 웹서비스(806) 및 사용자 서비스 컴포넌트(808) 간의 통신을 도시한다. IP 전화(802)는 내부 네트워크상에 "부트스트랩(bootstrap)"될 수 있다. 사용자에게 기업 최상위 인증서 또는 체인을 가지지 않는 "클린(clean)" 전화(802)를 설정한다. 전화(802)는 사용자의 SIP URI를 가지지 않는다. 그러나 전화(802)는 운영체제와 함께 포함된 공인 인증기관 최상위 인증서 집합을 포함한다. 단계(810)에서, 사용자는 전화(802)로 내선 또는 전화번호와 PIN을 입력한다. 단계(812)에서, 전화(802)는 DHCP 서버/레지스트라(804)로 메시지를 통해 네트워크 인증서 설정 웹서비스(806)를 발견한다(예를 들면 DHCP 옵션 43, 120). DHCP 서버/레지스트라(804)는 DHCP 질의에 응답하는 기업 통신 서버일 수 있다. 단계(814)에서, 레지스트라(804)는 SIP 레지스트라 FQDN으로써 옵션(120)에, 인증서 설정 웹서비스(806)의 URI로써 옵션(43)에 응답한다.

[0040] DHCP 서버/레지스트라(804)로 위장(spoofing)하여 불량 서버로 사용자를 향하게 하는 악의적 사용자와 관련된 위협을 경감시키기 위하여, 단계(816)에서 전화(802)는 사용자에게 네트워크 레지스트라(804)와 인증서 설정 웹서비스(806)의 접미사를 확인하도록 촉구할 수 있다. 단계(818)에서, 전화(802)는 DHCP 옵션(43)을 통해 얻은 인증서 웹서비스 URL로 연결된다. 단계(820)에서, 인증서 체인은 인증서 설정 웹서비스(802)로부터 다운로드된다. 단계(822)에서, 전화(802)는 보안 서버를 통해 인증서 설정 웹서비스(806)로 연결되고, 여기서 사용자는 내선 또는 전화번호와 PIN을 제출한다. 단계(824)에서, 웹서비스(806)는 사용자의 SIP URI를 조사하고, PIN을 확인하고, 그리고 전화(802)로 SIP URI를 설정한다.

[0041] 단계(826)에서, 전화(802)는 웹서비스로 제출하기 위해 인증서 서명 요청을 생성한다. 단계(828)에서, 웹서비스는 적절한 만기, SN/SAN(subject name/subject alternate name) 등을 스탬핑(stamp)하고, (웹서비스 개인키와 함께 서명된) 네트워크 서명 인증서를 발행한다. 단계(830)에서, 전화(802)는 네트워크 서명된 인증서에서

공개키(public key)를 웹서비스로 제출한다. 단계(832)에서, 공개키는 사용자 서비스 데이터베이스에 저장된다. 사용자 서비스는 기업 통신 서버의 백엔드 데이터베이스이다. 단계(834)에서, OK 메시지가 전화(802)로 반환된다. 이로써 설정 프로세스를 완료한다.

[0042] 일단 사용자의 SIP URI와 네트워크 서명 인증서가 전화로 설정되면, 후술되는 후속 단계만이 레지스트라(804, registrar)와 웹서비스(806)에 대한 액세스를 위해 후속한 로그온동안에 반복된다. 단계(836)에서, 전화(802)는 SIP 메시지를 TLS(transport layer securty)를 통해 레지스트라 FQDN으로 송신한다. 단계(838)에서, 전화(802)의 SIP URI와 인증서가 레지스트라(804)로 송신된다. 단계(840)에서, 레지스트라(804)는 인증 메시지를 전화(802)로 송신한다. 단계(842)에서, 레지스트라(804)는 사용자 서비스 컴포넌트(808)로 전화(802)를 인증한다. 단계(844)에서, 전화(802)는 인증서 및 매개변수를 가진 SIP URI를 허가로서 등록한다. 단계(846)에서, 전화(802)는 OK 메시지를 수신하고, 그 후에 사용자는 SIP 채널을 통해 이용가능한 모든 기능을 사용할 수 있다.

[0043] 전화 설정이 완료된 후에, 사용자는 그 전화를 사용자 컴퓨터로 매이게 할 수 있고, 그리고 다른 웹서비스를 인증하기 위하여, 그리고 기업 메시징 서버에 의해 제공된 콜 로그 및 음성 메일과 같은 기능을 얻기 위하여, 전화로 사용자 인증서를 설정할 수 있다. 전술한 프로세스는 예를 들어 사용자 대신에 MAC(move, add, changes) 기술자에 의해 수행될 수 있다. 이 경우, 사용자 인증서 배치는 없다.

[0044] 다음 섹션은 여기에 개시된 실시예를 구현하기 위한 시나리오를 기술한다. 제1 시나리오는 단말 사용자에 의한 내부 데스크 전화 설정과 로그온에 관한 것이다. 전형적인 새 고용인은 인증 크리덴셜을 사용하여 기업 네트워크로 사인온(sign-on)하지 않고 폰을 사용하여 업무지원센터(helpdesk)와 같은 전화번호로 전화를 건다. 예를 들면 사용자가 기업 크리덴셜로써 로그인할 수 없어 업무지원센터로 전화하려고 한다면, 전화를 쉽게 설정 및 사용할 수 있다. 사용자는 기업 네트워크로 인증할 수 없으므로 PIN을 설정 또는 재설정하기 위해 PIN 관리 포털을 액세스하지 못할 수도 있다.

[0045] 관리자는 사용자명, 내선/전화번호 및 SIP URI를 가진 데이터베이스 요소 또는 디렉토리를 설정한다. 또한 관리자는 사용자 메일박스와 네트워크 계정을 설정하고, PIN을 명시하거나 또는 PIN을 "자동생성(auto-generate)"으로 설정한다. 사용자는 전화를 설정하는 방법에 대한 인스트럭션을 가진 종이 및 데스크 전화를 본다. 또한 사용자는 내선/전화번호 및 PIN을 가진 종이를 넘겨 받을 수 있다. 전화가 부팅된 후에, 사용자는 폰 키패드를 사용하여 내선/전화번호 및 PIN을 입력한다. 전화번호는 라인 URI(예를 들면, 미국 내의 사용자를 위한 1-ZZZ-XXX-YYYY, 그리고 인도에서의 사용자를 위한 91-40-XXX-YYYY)에 공개되는 풀 E.164 전화번호일 수 있다. 내선은 라인 URI에서 발행되는 사용자의 내선이다.

[0046] 내선/전화번호 및 PIN의 입력시에, 전화는 네트워크를 발견하고, 네트워크는 내선/전화번호와 PIN을 사용하여 사용자를 확인한다. 네트워크는 SIP URI(예를 들면 user@nowhere-domain.com)을 전화로 공급하고, 사용자를 식별하는 네트워크 서명 인증서(예를 들면 SN=user@nowhere-domain,com)를 전화로 공급한다. 네트워크 서명된 인증서는 네트워크 레지스트라 및 웹서비스로의 인증을 위해 사용된다. 사용자에게 장치 PIN을 생성하도록 촉구한다. 사용자는 전화를 해제(unlock)하는데 사용되는 동일 PIN을 사용하거나 또는 상이한 PIN을 생성할 수 있다.

[0047] 전술한 바와 같이, 사용자는 이제 PSTN(public-switched telephone network) 또는 기업내에 임의 사용자로/로부터 콜을 송신 및 수신하기 위해 전화를 사용할 수 있다. 사용자는 SIP URI, 도메인 및 패스워드를 전화로 입력할 필요가 없다.

[0048] 제2 시나리오는 내부 데스크 전화 설정과 기술자에 의한 로그온에 관한 것이다. 금융 서비스 및 정부와 같은 소정의 수직 산업에서, 전화는 "이동-추가-변경(Move-adds-changes)" 기술자에 의해 이미 배치되고, 단말 사용자가 도착하기 전에 작동가능하게 만들어진다. 예를 들면 새로운 거래자가 금융 서비스 회사에서 무역업무 데스크에 도착할 때, 운용 전화를 기대한다.

[0049] 새 고용인의 경우, 관리자는 고용인 이름, 전화번호 및 SIP URI를 가진 디렉토리를 설정한다. 또한 관리자는 사용자의 메일박스 및 네트워크 계정을 설정할 수 있고, PIN을 "자동생성(auto-generate)"으로 설정하고, 처음 사용자 로그온시에 PIN을 변경해야 함을 명시한다. 기술자는 관리자에 의해 사용자의 전화번호 및 PIN을 이미 설정한 사용자의 업무 데스크에 도달하고, 전화를 부팅하고, 전화 키패드를 사용하여 내선/전화번호 및 PIN을 입력한다. 전화는 네트워크 발견하고, 그 후에 네트워크는 내선/전화번호 및 PIN을 확인한다. 네트워크는 사용자의 SIP URI(예를 들면 user@nowhere-domain.com)을 전화로 설정하고, 사용자를 식별하는 서명된 인증서(예

를 들면 SN=user@nowhere-domain.com)를 전화로 설정한다. 서명된 인증서는 네트워크 레지스트라 및 웹서비스로 인증하기 위해 사용된다. 이제, 사용자는 전화를 사용하여 다른 사용자로/로부터 콜을 송신 및 수신할 수 있다.

[0050] 제3 시나리오는 원격 위치로부터 데스크 전화 로그온에 관한 것이다. 사용자가 홈 오피스(home office)로부터 작업하는 모바일 사용자라고 간주한다. 처음으로 사용자의 전화를 설정하기 위해, 전화는 내부 기업 네트워크로 물리적으로 연결된다. 사용자는 처음으로 전화를 설정하기 위해 회사 본부 또는 지점을 방문할 수 있다. 전화 설정은 전술한 바와 같이 발생한다. 사용자가 홈 오피스로 돌아올 때, SIP URI 및 서명된 인증서(및/또는 사용자 인증서)는 이미 전화로 설정되었다. 클라이언트는 DNS SRV(서비스 레코드)를 사용하여 네트워크 서버(예를 들면 에지 서버)를 발견하고, 에지 서버(edge server)로 연결된다. 사용자는 서명된 인증서(또는 사용자 인증서)를 사용하여 네트워크로 인증하고, 이제 모든 전화 기능을 사용할 수 있다.

[0051] 제4 시나리오는 컴퓨터와 쌍이 되는 데스크 전화 설정에 관한 것이다. 사용자는 홈 오피스에서 작업하는 모바일 사용자를 고려한다. 처음 전화를 설정하기 위해, 사용자는 네트워크 소프트웨어를 실행중인 관련 컴퓨터로 (유선 또는 무선으로) 전화를 연결한다. 전화는 서명된 인증서(또는 사용자 인증서)를 요청하고, 요청에 대한 보안 인증 프로토콜(예를 들면 Kerberos/NTLM-NT LAN 관리자) 크리덴셜을 사용한다. 네트워크는 서명된 인증서(또는 사용자 인증서)를 전화로 설정한다. 또한 네트워크는 SIP URI를 전화로 설정한다. 사용자는 서명된 인증서(또는 사용자 인증서)를 사용하여 네트워크로 인증하고, 이제 모든 전화 기능을 사용할 수 있다.

[0052] 제 5 시나리오는 기업이 방문 사용자를 위한 전용 사무실 또는 데스크를 가지지 않는 상황에서 방문 사용자에 의해 사용될 수 있는 칸막이형 데스크 전화 또는 "핫 데스크(hot desk)"에 관한 것이다. 예를 들면 사용자는 도킹 스테이션 및 전화와 같이 이용가능한 기반구조를 사용할 수 있다. 이 시나리오는 예를 들어 컨설턴트(consultants)가 모바일이고, 원격 오피스로부터 작업하지만 홈 오피스를 자주 방문하는 컨설팅 산업에 일반적인 일이다.

[0053] 예를 들면 모바일 작업자가 로컬 기반구조에 들르고 이를 사용할 수 있는 제한된 수의 사무실을 가진 런던에 있는 기업 지점을 고려한다. 모바일 사용자는 로그온 버튼을 누르고, 내선/전화번호 및 PIN을 확인한다. 전화는 네트워크를 발견하고, 네트워크는 내선/전화번호 및 PIN을 확인한다. 네트워크는 SIP URI를 전화로 설정하고, 사용자를 식별하는 서명된 인증서(예를 들면 SN=user@nowhere-domain.com)를 전화로 설정한다. 서명된 인증서는 네트워크 레지스트라 및 웹서비스 인증을 위해 사용된다. 이제, 사용자는 기업 내, 또는 SIP 신원을 사용하는 로컬 PSTN 네트워크 또는 기업내 임의 사용자로/로부터 콜을 송신 및 수신하기 위해 전화를 사용할 수 있다. 모바일 사용자가 그 위치를 떠날 때, 사용자는 전화를 사용하여 로그아웃(log out)할 수 있거나, 전화가 사전결정된 시간 주기(예를 들면 수 분)후에 자동적으로 로그오프되돌록 구성될 수 있다. 이제, 또 다른 사용자가 런던, 사무실을 방문할 수 있고, 기술된 절차에 따라서 통신 기반구조를 이용할 수 있다.

[0054] 제6 시나리오는 공동구역 전화 설정과 로그온에 관한 것이다. 공동구역 전화는 전형적으로, 로비, 안내실, 회의실, 복도 등과 같은 공동구역에 배치할 수 있는 로우(low)-단말 장치이다. 관리자는 통신 데이터베이스에 공동구역 전화 신원을 생성한다. 관리자는 공동구역 전화번호에 대해 "자동-생성" 또는 PIN을 설정한다. 공동구역 PIN은 사용자 PIN외 독립된 만료 정책을 가지도록 정의될 수 있다. 예를 들면 관리자는 공동구역 전화 PIN을 "절대 만료하지 않도록(never expire)" 설정할 수 있다.

[0055] 그러면, 기술자는 공동구역을 방문하고, 전화를 연결하고, 공동구역 전화를 위한 내선/전화번호 및 PIN을 입력할 수 있다. 전화는 내선/전화번호 및 PIN을 확인하는 네트워크를 발견한다. 그러면, 네트워크는 (전화번호에 의해 식별되는 자원을 기술하는) Tel URI를 전화로 설정하고, Tel URI를 식별하는 서명된 인증서(예를 들면 SN=4257070030@nowhere-domain.com)을 전화로 설정한다. 서명된 인증서는 네트워크 레지스트라 및 웹서비스로 인증을 위해 사용된다. 공동구역 전화는 이제 작동가능하며, (전화 신원- Tel URI을 사용하여) 콜을 송신 및 수신하는데 사용될 수 있다. 공동구역 모드에서, 전화는 임의 사용자 특정 데이터를 가지지 않는다.

[0056] 개시된 구조의 신규 양상을 수행하기 위한 예시적 방법론을 나타내는 흐름도 셋이 여기에 포함된다. 설명을 간략히 하기 위하여, 예를 들어 흐름도의 형태, 또는 흐름도인 여기에 도시된 하나 이상의 방법론은 일련의 액트(acts)로서 도시 및 기술되었지만, 소정의 액트는 그에 따라서 여기에 도시 및 개시된 다른 액트와 상이한 순서로, 및/또는 동시에 발생하므로, 방법론은 액트 순서에 의해 제한되지 않는다는 것을 이해하고 알 것이다. 예를 들어 당해 기술분야에 통상의 지식을 가진 자는 방법론이 이 대신에 상태도에서와 같이 일련의 상호관련 상태 또는 이벤트로서 표현될 수 있다는 것을 이해하고 것이다. 또한 방법론에 도시된 모든 액트가 신규 구현을 위해 필요하지 않을 수 있다.

[0057] 도 9는 실시간 통신에서 사용자 기반 인증의 방법을 도시한다. 단계(900)에서, 전화로부터 번호 내선 및 PIN을 수신한다. 내선은 사용자가 도달할 수 있는 전화 내선일 수 있다. PIN은 사용자에 의해 변경될 수 있는 관리상 배정된 임의 개인 코드일 수 있다. 사용자는 전화상의 숫자 키패드로 내선 및 PIN을 입력할 수 있다. 단계(902)에서, 번호 내선에 기초하여 기업 통신 서버로 전화를 인증한다. 단계(904)에서, 전화 주소를 전화로 송신한다. 단계(906)에서, 전화 주소(예를 들면 SIP URI 또는 전화 URI 및 인증서)에 기초하여 기업 통신 서버로 전화를 등록한다.

[0058] 도 10은 사용자 기반 인증의 방법의 다른 양상을 도시한다. 단계(1000)에서, 전화를 위해 기업 통신 서버의 FQDN 및 IP 주소를 요청한다. 단계(1002)에서, 기업 통신 서버로부터 전화로 SIP URI를 반환한다. 단계(1004)에서, 전화로부터 기업 통신 서버로 HTTP 메시지를 송신한다. 단계(1006)에서, 전화 주소는 SIP URI 또는 전화 URI 중의 하나이다.

[0059] 도 11은 사용자 기반 인증 방법의 추가 양상을 도시한다. 단계(1100)에서, 번호 내선을 사용하여 기업 통신 서버로 요청을 송신함으로써 전화 주소를 검색한다. 단계(1102)에서, 전화 인증을 위해, 기업 통신 서버와 통신하여 기업 디렉토리 서버(corporate directory server)로부터, 또는 통신 서버로부터 직접 전화 주소를 참조한다. 단계(1104)에서, 개인 전화 내선은 번호 내선으로서 설정된다. 개인 전화 내선은 사용자의 네트워크 신원의 속성이다. 단계(1106)에서, PIN은 (예를 들어 네트워크 행정의 일부로서) 사전배정된다.

[0060] 도 12는 인증서를 사용하는 통신 방법을 도시한다. 단계(1200)에서, 사용자 식별자 및 PIN을 사용하여 통신 네트워크로 사용자 전화를 인증한다. 단계(1202)에서, 사용자 식별자 및 PIN에 기초하여 전화로 인증서를 발행한다. 단계(1204)에서, 인증서를 사용하여 네트워크로 전화를 등록시킨다.

[0061] 도 13은 인증서를 사용하는 도 12의 통신 방법의 추가 양상을 도시한다. 단계(1300)에서, 사용자 식별자 및 PIN에 기초하여 사용자를 분석한다. 단계(1302)에서, 사용자 식별자 및 PIN에 기초하여 사용자 SIP URI를 전화로 송신한다. 단계(1304)에서, 인증서 웹서비스 구조와 레지스트라 FQDN을 전화로 송신한다. 단계(1306)에서, 전화를 사용하여, 그리고 인증서 체인을 다운로드하기 위해 웹서비스로 연결하여 인증서 설정 웹서비스를 발견한다. 단계(1308)에서, 전화로부터 웹서비스로 인증서 서명 요청을 생성 및 제출한다.

[0062] 도 14는 인증서를 사용하는 도 12의 통신 방법의 추가 양상을 도시한다. 단계(1400)에서, 통신 서버에 의해 인증서를 서명한다. 단계(1402)에서, 초기 등록 후에, 모든 후속한 등록을 위해, 레지스트라 FQDN을 포함한 전송 보안 메시지를 송신한다. 단계(1404)에서, 인증서를 인증한다. 단계(1406)에서, 인증서 및 인증서 매개변수에 기초하여 전화가 허가된다.

[0063] 본 명세서에 사용된 바와 같이, 용어 "컴포넌트"와 "시스템"은 컴퓨터 관련 엔티티, 하드웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어 또는 실행중인 소프트웨어를 언급하려고 한다. 예를 들어 컴포넌트는 프로세서상에서 실행중인 프로세스, 프로세서, 하드 디스크 드라이브, (광학 및/또는 자기 저장매체의) 다중 저장 드라이브, 객체, 실행가능, 실행 스레드, 프로그램, 및/또는 컴퓨터일 수도 있는데, 이로 제한되지는 않는다. 실례로서, 서버상에서 실행중인 애플리케이션과 서버는 컴포넌트일 수 있다. 하나 이상의 컴포넌트는 프로세스 및/또는 실행 스레드내 상주할 수 있고, 컴포넌트는 하나의 컴퓨터상에 국한될 수 있고, 그리고/또는 둘 이상의 컴퓨터들 간에 분산될 수 있다. 단어 "예시적인"은 예, 경우, 또는 실례로서의 기능을 의미하는데 사용될 수 있다. 여기에 기술된 임의 양상 또는 설계가 다른 양상 또는 설계에 비해 반드시 바람직하거나 유리한 것으로 구성될 필요는 없다.

[0064] 이제 도 15를 참조하면, 개시된 구조에 따라서 실시간 통신을 위해 사용자 기반 인증을 설정할 수 있도록 동작가능한 컴퓨팅 시스템(1500)의 블록도를 도시한다. 다양한 양상에 대한 추가 상황(context)을 설정하기 위해, 도 15와 다음의 논의는 다양한 양상을 구현할 수 있는 적절한 컴퓨팅 시스템(1500)의 간단하고 일반적인 설명을 제공하려고 한다. 전술한 설명은 하나 이상의 컴퓨터상에서 실행될 수 있는 컴퓨터 실행가능한 인스트럭션의 일반적 상황이였지만, 당해 기술분야에 통상의 지식을 가진 자는 다른 프로그램 모듈과 조합하여, 그리고/또는 하드웨어와 소프트웨어의 조합으로 구현될 수 있다는 것을 알 것이다.

[0065] 다양한 양상을 구현하기 위한 컴퓨팅 시스템(1500)은 처리 유닛(들)(1504), 시스템 메모리(1506) 및 시스템 버스(1508)를 가진 컴퓨터(1502)를 포함한다. 처리 유닛(들)(1504)은 단일 프로세서, 멀티 프로세서, 단일 코어 유닛 및 멀티 코어 유닛과 같은 상업적으로 사용가능한 다양한 프로세서중의 임의 프로세서일 수 있다. 게다가 당해 기술분야에 통상의 지식을 가진 자는 신규 방법이 미니컴퓨터, 메인프레임 컴퓨터뿐만 아니라 퍼스널 컴퓨터(예를 들면 데스크탑, 랩탑 등), 핸드헬드 컴퓨팅 장치, 마이크로프로세서기반 또는 프로그램가능 가전제품

등을 포함한 다른 컴퓨터 시스템 구성과도 실행될 수 있다는 것을 알 것이며, 위의 예들의 각각은 하나 이상의 관련 장치로 동작가능하게 연결될 수 있다.

[0066] 시스템 메모리(1506)는 VOL(volatile) 메모리(1510)(예를 들면 RAM(random access memory)), NON-VOL(non-volatile memory)(1512)(예를 들면 ROM, EPROM, EEPROM 등)을 포함할 수 있다. BIOS(basic input/output system)은 비휘발성 메모리(1512)에 저장될 수 있고, 그리고 시동과 같은 동안에 컴퓨터(1502)내 컴포넌트들 간에 데이터 및 신호의 통신을 용이하게 하는 기본 루틴을 포함한다. 또한 휘발성 메모리(1510)는 데이터 캐싱을 위한 정적 RAM과 같은 고속 RAM을 포함할 수 있다.

[0067] 시스템 버스(1508)는 메모리 서브시스템(1506)을 포함하지만 이로 제한되지 않는 시스템 컴포넌트를 위한 인터페이스를 처리 유닛(들)(1504)에 제공한다. 시스템 버스(1508)는 각종 상업적으로 이용가능한 버스 구조를 사용하여 (메모리 제어기를 가진 또는 없는) 메모리 버스와 주변 버스(예를 들면 PCI, PCIe, AGp, LPC 등)로 더 상호연결도리 수 있는 몇몇 유형의 버스 구조중의 임의 구조일 수 있다.

[0068] 컴퓨터(1502)는 저장 서브시스템(들)(1514), 그리고 저장 서브시스템(들)(1514)을 시스템 버스(1508) 및 다른 바람직한 컴퓨터 컴포넌트로 인터페이스하기 위한 저장 인터페이스(들)(1516)를 더 포함한다. 저장 서브시스템(들)(1514)은 예를 들어 하드디스크 드라이브(HDD), 자기 플로피 디스크 드라이브(FDD), 및/또는 광 디스크 저장 드라이브(예를 들면 CD-ROM 드라이브, DVD 드라이브)중의 하나 이상을 포함할 수 있다. 저장 인터페이스(들)(1516)는 예를 들어 EIDE, ATA, SATA 및 IEEE 1394와 같은 인터페이스 기술을 포함할 수 있다.

[0069] 하나 이상의 프로그램 및 데이터는 운영체제(1520), 하나 이상의 애플리케이션 프로그램(1522), 다른 프로그램 모듈(1524) 및 프로그램 데이터(1526)를 포함한, 메모리 서브시스템(1506), 분리식 메모리 서브시스템(1518)(예를 들면 플래시 드라이브 폼팩터 기술), 그리고/또는 저장 서브시스템(들)(1514)에 저장될 수 있다. 통상, 프로그램은 특정 작업을 수행하거나 또는 특정한 추상 데이터 유형을 구현하는, 루틴, 방법, 데이터 구조, 다른 소프트웨어 컴포넌트 등을 포함한다. 또한 운영체제(1520), 애플리케이션(1522), 모듈(1524) 및/또는 데이터(1526)의 일부 또는 모두가 예를 들어 휘발성 메모리(1510)과 같은 메모리에 캐싱될 수 있다. 개시된 구조는 상업적으로 이용가능한 다양한 운영체제 또는 (예를 들어 가상 머신과 같은) 운영체제의 조합으로써 구현될 수 있다는 것을 알 것이다.

[0070] 전술한 애플리케이션 프로그램(1522), 프로그램 모듈(1524) 및 프로그램 데이터(1526)는 도 1의 입력 컴포넌트(102), 전화(104), 식별 코드(106), 설정 컴포넌트(108), 그리고 전화 기반구조(110)를 포함한 컴퓨터로 구현된 시스템(100), 도 2의 설정 컴포넌트(108), SIP URI(202) 및 인증 컴포넌트(204)를 포함한 시스템(200), 도 3의 기업 통신 서버(302), 로케이션 컴포넌트(306), IP 주소(308)와 같은 추가 컴포넌트(300)를 포함할 수 있다.

[0071] 전술한 애플리케이션 프로그램(1522), 프로그램 모듈(1524) 및 프로그램 데이터(1526)는 예를 들어 도 4의 입력 컴포넌트(102), 사용자 식별자(402), PIN(404), 인증 서비스(406), 전화(104), 로케이션 컴포넌트(306), 기업 통신 서버(302), 설정 컴포넌트(108), 인증 컴포넌트(204)를 포함한 시스템(400), 도 5의 IP 서버(502), SIP URI(504), DHCP 서버(506), IP 주소(508), FQDN 레코드(510), 기업 통신 서버(302)와 같은 추가 엔티티(500), 도 6의 IP 전화(602), 기업 통신 서버(302) 및 DHCP 서버(506)를 포함한 시스템(600), 도 7 및 도 8의 데이터 및 메시지 흐름도, 도 9내지 도 14의 흐름도에 의해 표현되는 방법을 더 포함할 수 있다.

[0072] 저장 서브시스템(들)(514)과 메모리 서브시스템(1506, 1518)은 데이터, 데이터 구조, 컴퓨터 실행가능 인스트럭션 등을 위한 휘발성 및 비휘발성 저장소로서의 기능을 한다. 컴퓨터 판독가능 매체는 컴퓨터(1502)에 의해 액세스될 수 있으며, 휘발성 및 비휘발성 매체, 분리식 및 비분리식 매체를 포함하는 임의 사용가능한 매체일 수 있다. 컴퓨터(1502)의 경우, 매체는 적당한 임의 디지털 포맷의 데이터 저장소를 수용한다. 당해 기술분야에 통상의 지식을 가진 자는 개시된 구조의 신규 방법을 수행하기 위한 컴퓨터 실행가능한 인스트럭션을 저장하기 위해, 집 드라이브(zip drives) 자기 테잎, 플래시 메모리 카드, 카트리지 등과 같이 다른 유형의 컴퓨터 판독가능 매체를 사용할 수 있다는 것을 알아야 한다.

[0073] 사용자는 키보드 및 마우스와 같은 외부 사용자 입력장치(1528)을 사용하여 컴퓨터(1502), 프로그램 및 데이터와 상호작용할 수 있다. 다른 외부 사용자 입력장치(1528)는 마이크로폰, IR(infrared) 원격 제어부, 조이스틱, 게임패드, 카메라 인식 시스템, 스틸러스 펜, 터치 스크린, 제스처 시스템(예를 들면 눈 움직임, 머리 움직임 등) 등을 포함할 수 있다. 사용자는 터치패드, 마이크로폰, 키보드 등과 같인 온보드 사용자 입력장치(1530)을 사용하여 컴퓨터(1502), 프로그램 및 데이터와 상호작용할 수 있고, 여기서 컴퓨터(1502)는 예를 들어 휴대용 컴퓨터이다. 이들 및 다른 입력장치는 I/O(input/output) 장치 인터페이스(들)(1532)를 통해, 시스

템 버스(1508)를 거쳐 처리 유닛(들)(1504)으로 연결되지만, 병렬 포트, IEEE 1394 시리얼포트, 게임포트, USB 포트, IR 인터페이스 등과 같은 다른 인터페이스에 의해 연결될 수 있다. 또한 I/O 장치 인터페이스(들)(1532)는 사운드 카드 및/또는 온보드 오디오 처리 능력과 같이, 프린터, 오디오 장치, 카메라 장치 등과 같은 출력 주변장치(1534)의 사용을 용이하게한다.

[0074] 하나 이상의 그래픽 인터페이스(들)(1536)(또한 GPU(graphics processing unit)로서 통상 언급됨)는 컴퓨터(1502)와 외부 디스플레이(들)(1538)(예를 들어 LCD, 플라즈마) 및/또는 온보드 디스플레이(1540)(예를 들면 휴대용 컴퓨터) 사이에 그래픽 및 비디오 신호를 제공한다. 또한 그래픽 인터페이스(들)(1536)는 컴퓨터 시스템 보드의 일부로서 제작될 수 있다.

[0075] 컴퓨터(1502)는 하나 이상의 네트워크 및/또는 다른 컴퓨터로 유선/무선 통신 서브시스템(1542)을 통해 논리 연결부를 사용하여 네트워크 환경(예를 들면 IP)에서 동작할 수 있다. 다른 컴퓨터는 워크스테이션, 서버, 라우터(router), 퍼스널 컴퓨터, 마이크로프로세서기반 엔터테인먼트 어플라이언스, 피어 장치(peer device) 또는 다른 공동 네트워크 노드를 포함할 수 있고, 전형적으로 컴퓨터(1502)와 관련하여 기술된 다수 또는 모든 요소를 포함할 수 있다. 논리적 연결부는 LAN(local area network), WAN(wide area network), 핫스팟(hotspot)등으로의 유선/무선 연결성을 포함할 수 있다. LAN 및 WAN 네트워크 환경은 사무실 및 회사에서 흔하며, 이들 모두가 인터넷과 같이 글로벌 통신 네트워크로 연결될 수 있는, 인트라넷과 같은 전사적 컴퓨터 네트워크를 용이하게 한다.

[0076] 컴퓨터(1502)는 네트워크 환경에 사용될 시에, 유선/무선 네트워크, 유선/무선 프린터, 유선/무선 입력장치(1544)등과 통신하기 위해 유선/무선 통신 서브시스템(1542)(예를 들면 네트워크 인터페이스 어댑터, 온보드 트랜스시버 서브시스템 등)을 통해 네트워크로 연결된다. 컴퓨터(1502)는 모뎀을 포함할 수 있거나, 또는 네트워크를 통해 통신을 설정하기 위한 다른 수단을 가진다. 네트워크 환경에서, 컴퓨터(1502)에 관련된 프로그램 및 데이터는 분산 시스템과 관련있으므로 원격 메모리/저장 장치에 저장될 수 있다. 도시된 네트워크 연결은 예시적이며, 컴퓨터들 간에 통신 링크를 설정하기 위한 다른 수단을 사용할 수 있다는 것을 알 것이다.

[0077] 컴퓨터(1502)는 예를 들어 프린터, 스캐너, 데스크탑 및/또는 휴대용 컴퓨터, PDA(personal digital assistant), 통신 위성, 무선으로 검출가능한 태그, 관련된 위치 또는 임의 설비 피스(예를 들면 키오스크(kiosk), 신문가판대(news stand), 화장실) 및 전화와 무선 통신에서 동작가능하게 배치된 무선 장치와 같은 IEEE 802.xx 패밀리와 같은 무선 기술(예를 들어 IEEE 802.11 OTA(over-the-air) 변조 기법)을 사용하여 유선/무선 장치 또는 엔티티와 통신하도록 동작할 수 있다. 이것은 핫스팟, WiMax 및 블루투스™ 무선 기술을 위해 적어도 Wi-Fi(또는 무선 신뢰도)를 포함한다. 따라서 통신은 적어도 두 장치들 간에 종래 네트워크 또는 간단히 애드혹(ad hoc) 통신과 같은 것을 가진 사전정의된 구조일 수 있다. Wi-Fi 네트워크는 안전하고 신뢰할만하며 신속한 무선 연결을 제공하기 위해 IEEE 802.11x(a, b, g 등)으로 불리는 무선 기술을 사용한다. Wi-Fi 네트워크는 서로, 인터넷으로, (IEEE 802.3 관련 매체 및 기능을 사용하는) 유선 네트워크로 컴퓨터를 연결하는데 사용될 수 있다.

[0078] 또한 도시된 양상은 분산 컴퓨팅 환경에 실행될 수 있고, 여기서 소정 작업은 통신 네트워크를 통해 연결된 원격 처리 장치에 의해 수행된다. 분산 컴퓨터 환경에서, 프로그램 모듈은 로컬 및/또는 원격 저장소 및/또는 메모리 시스템에 위치할 수 있다.

[0079] 이제 도 16을 참조하면, 사용자 기반 인증에 사용될 수 있는 컴퓨팅 환경(1600)의 개략적 블록도를 도시한다. 환경(1600)은 하나 이상의 클라이언트(들)(1602)를 포함한다. 클라이언트(들)(1602)는 하드웨어 및/또는 소프트웨어(예를 들면 스레드, 프로세스, 컴퓨팅 장치)일 수 있다. 클라이언트(들)(1602)는 예를 들어 쿠키(cookie(s)) 및/또는 관련된 상황 정보를 수용할 수 있다.

[0080] 또한 환경(1600)은 하나 이상의 서버(들)(1604)를 포함한다. 또한 서버(들)(1604)는 하드웨어 및/또는 소프트웨어(예를 들어 스레드, 프로세스, 컴퓨팅 장치)일 수 있다. 서버(1604)는 예를 들어 구조를 사용하여 변환을 수행하기 위하여 스레드(threads)를 수용할 수 있다. 클라이언트(1602)와 서버(1604) 간에 가능한 하나의 통신은 둘 이상의 컴퓨터 프로세스들 간에 전송되는데 적합한 데이터 패킷 형태일 수 있다. 데이터 패킷은 예를 들어 쿠키 및/또는 관련된 상황 정보를 포함할 수 있다. 환경(1600)은 클라이언트(들)(1602)와 서버(들)(1604) 사이에 통신을 용이하게 하는데 사용될 수 있는 통신 프레임워크(communication framework)(1606)(예를 들어 인터넷과 같은 글로벌 통신 네트워크)를 포함한다.

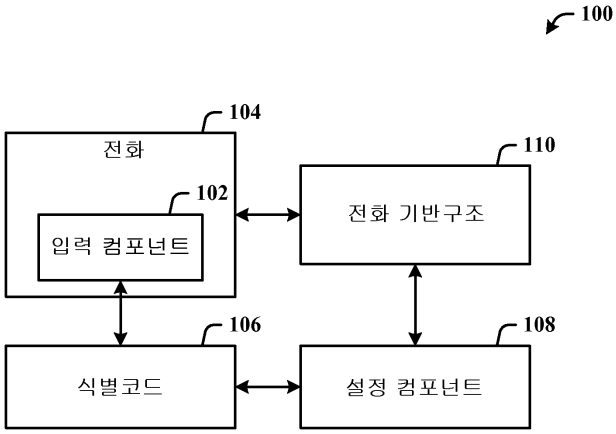
[0081] 통신은 (광섬유를 포함한) 유선 및/또는 무선 기술을 통해 용이해질 수 있다. 클라이언트(들)(1602)는 클라이

언트(들)(1602)로 국한되는 정보(예를 들면 쿠키(들) 및/또는 관련된 상황 정보)를 저장하기 위해 사용될 수 있는 하나 이상의 클라이언트 데이터 저장소(들)(1608)로 동작가능하게 연결된다. 유사하게, 서버(들)(1604)는 서버(1604)로 국한되는 정보를 저장하기 위해 사용가능한 하나 이상의 서버 데이터 저장소(들)(1610)로 동작가능하게 연결된다.

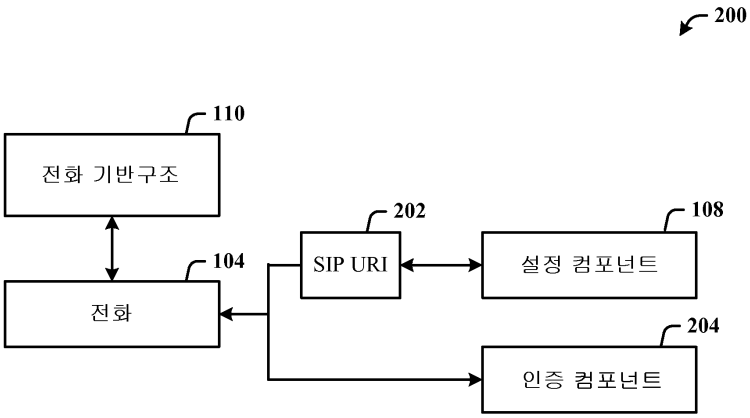
[0082] 전술한 바는 개시된 구조의 예를 포함한다. 물론, 컴포넌트 및/또는 방법론의 모든 인지가능한 조합을 기술하는 것이 불가능하지만, 당해 기술분야에 통상의 지식을 가진 자는 다수의 다른 조합과 치환이 가능하다는 것을 알 수 있다. 따라서 신규의 구조는 첨부된 청구범위의 사상 및 범주내에 있는 모든 이러한 변경, 변형 및 변동을 포함하려 한다. 또한 용어 "포함(includes)"은 상세한 설명 또는 청구범위에 사용되는 한, 이는 청구범위에서 전환어로 사용되는 경우에 용어 "포함하는(comprising)"이 해석되는 바와 같이 용어 "포함하는(comprising)"과 유사한 방식으로 포괄적인 사용을 의도한 것이다.

도면

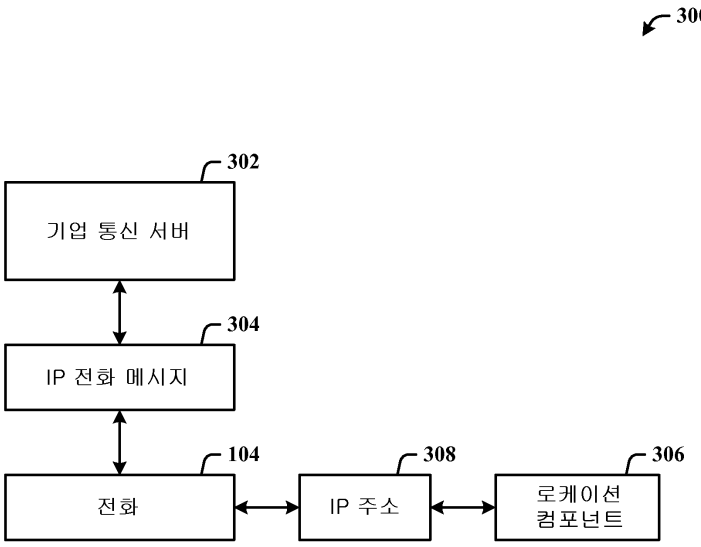
도면1



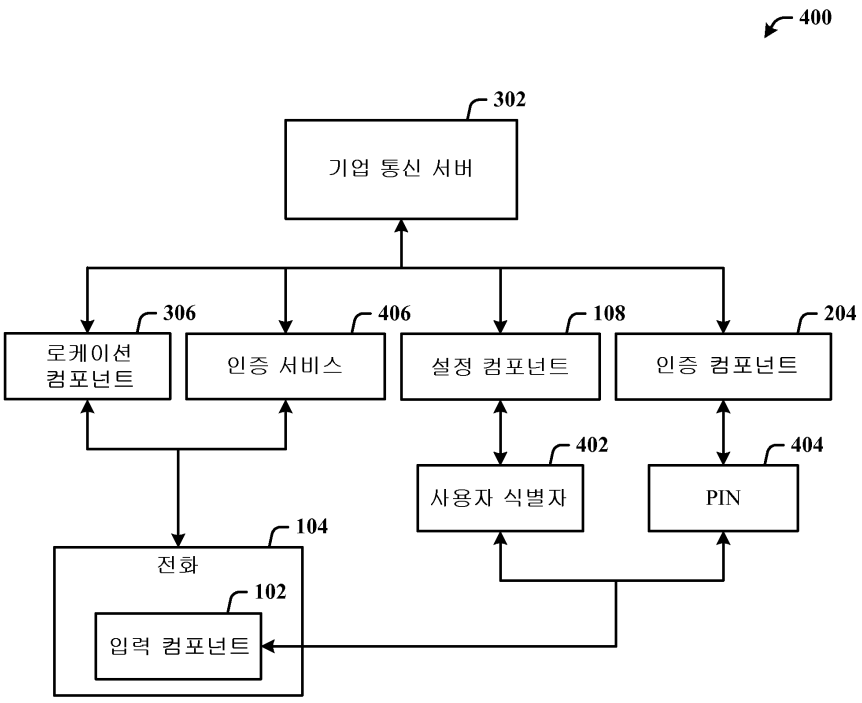
도면2



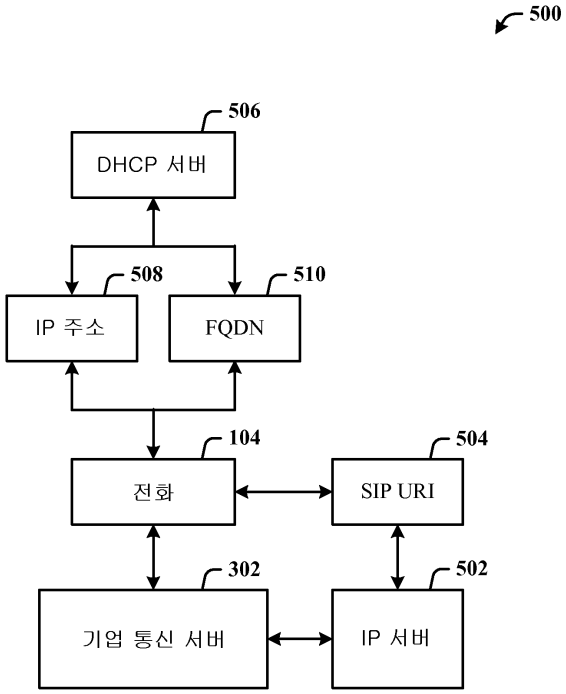
도면3


300
302
기업 통신 서버
304
IP 전화 메시지
104
전화
308
IP 주소
306
로케이션
컴포넌트

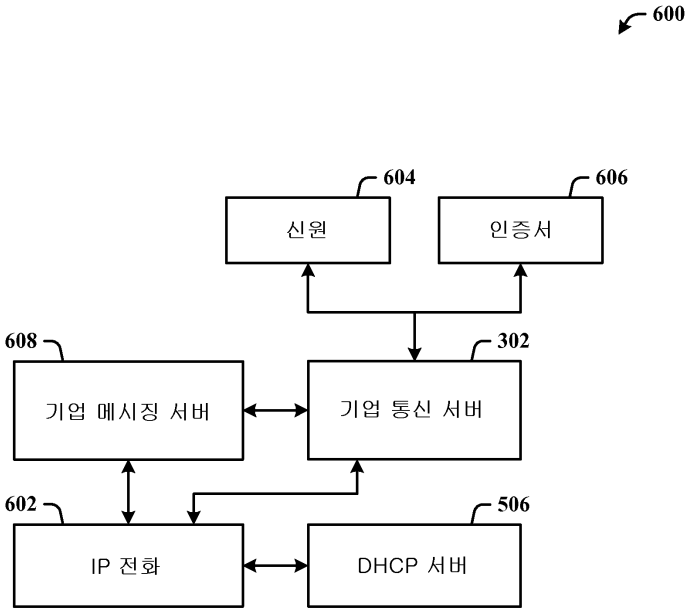
도면4


400
302
기업 통신 서버
306
로케이션
컴포넌트
406
인증 서비스
108
설정 컴포넌트
204
인증 컴포넌트
402
사용자 식별자
404
PIN
104
전화
102
입력 컴포넌트

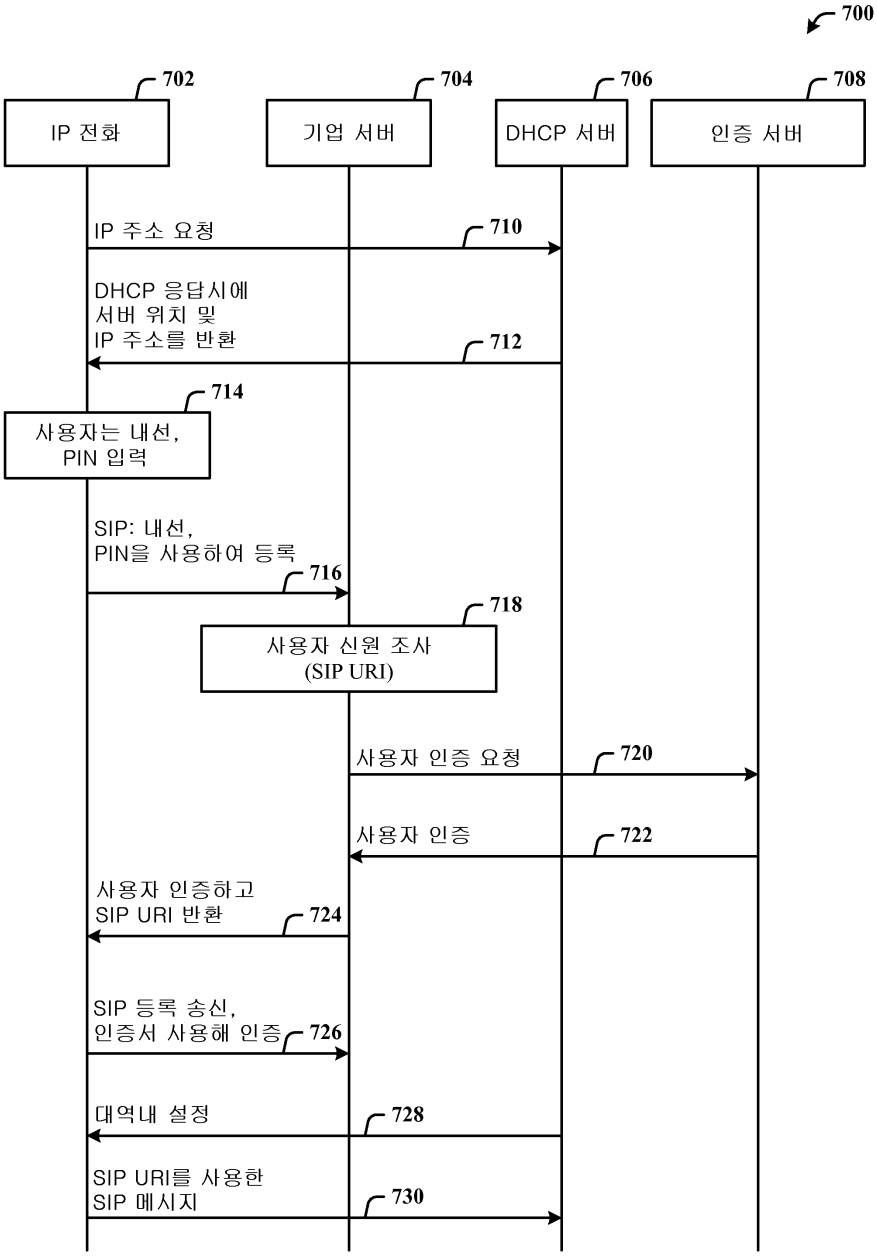
도면5


500
506
DHCP 서버
508
510
IP 주소
FQDN
104
504
전화
SIP URI
302
502
기업 통신 서버
IP 서버

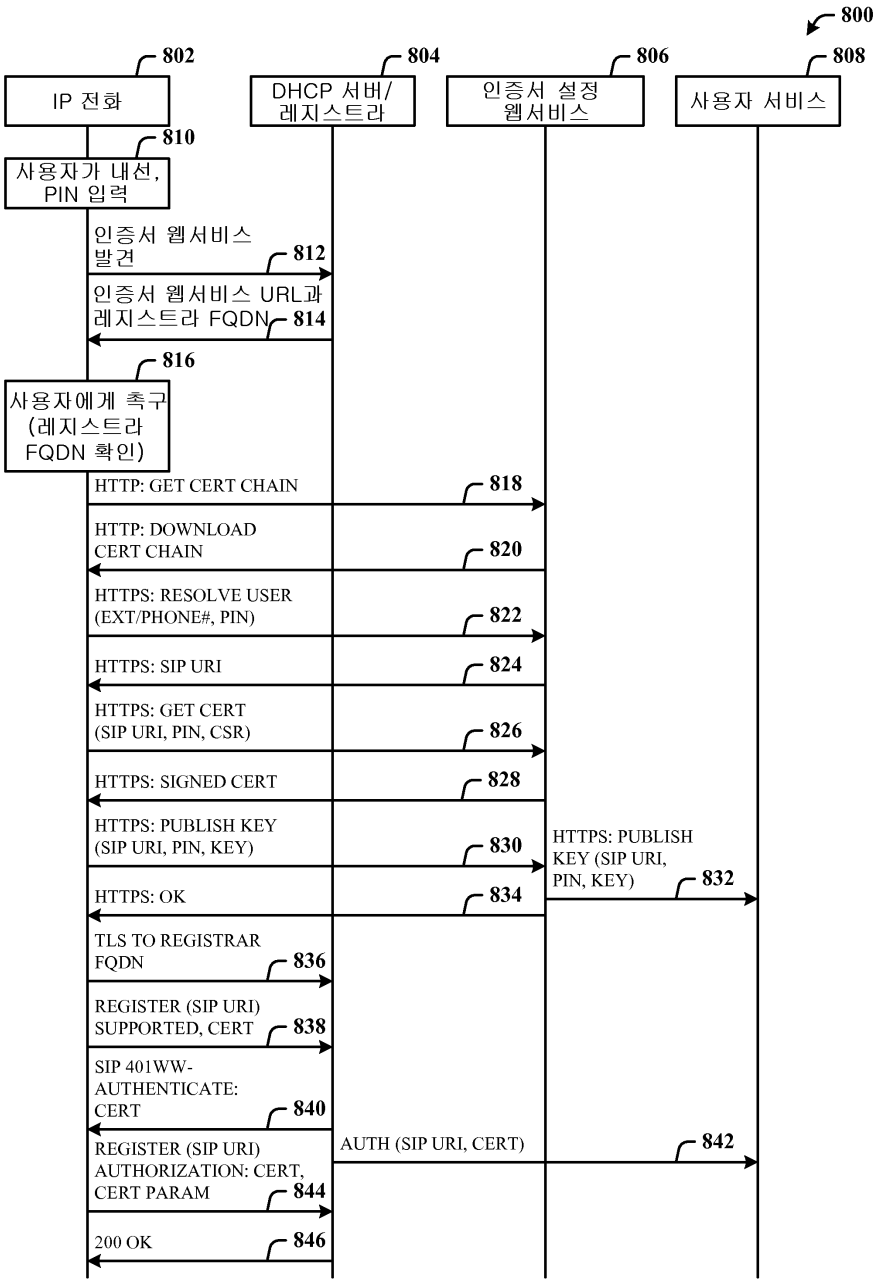
도면6


600
604
606
신원
인증서
608
302
기업 메시징 서버
기업 통신 서버
602
506
IP 전화
DHCP 서버

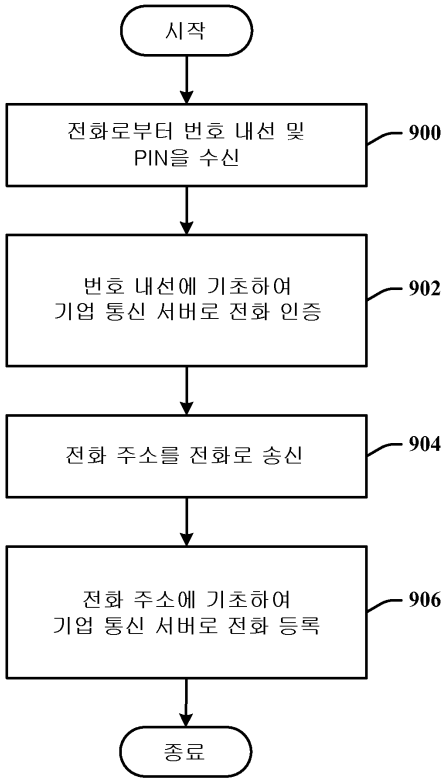
도면7


700
702
IP 전화
704
기업 서버
706
DHCP 서버
708
인증 서버
IP 주소 요청
710
DHCP 응답시에
서버 위치 및
IP 주소를 반환
712
714
사용자는 내선,
PIN 입력
SIP: 내선,
PIN을 사용하여 등록
716
718
사용자 신원 조사
(SIP URI)
사용자 인증 요청
720
사용자 인증
722
사용자 인증하고
SIP URI 반환
724
SIP 등록 송신,
인증서 사용해 인증
726
대역내 설정
728
SIP URI를 사용한
SIP 메시지
730

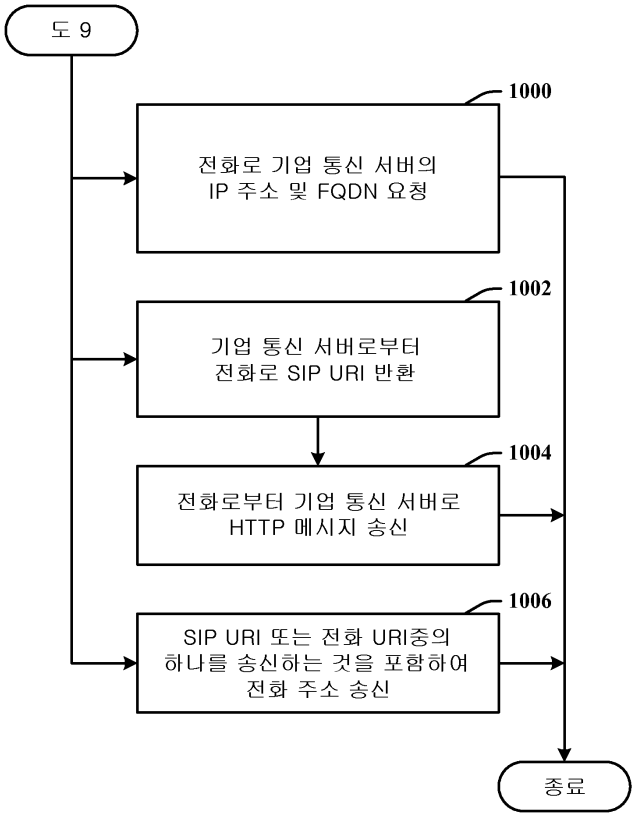
도면8


800
802
IP 전화
804
DHCP 서버/
레지스트라
806
인증서 설정
웹서비스
808
사용자 서비스
810
사용자가 내선,
PIN 입력
인증서 웹서비스
발견
812
인증서 웹서비스 URL과
레지스트라 FQDN
814
816
사용자에게 촉구
(레지스트라
FQDN 확인)
HTTP: GET CERT CHAIN
818
HTTP: DOWNLOAD
CERT CHAIN
820
HTTPS: RESOLVE USER
(EXT/PHONE#, PIN)
822
HTTPS: SIP URI
824
HTTPS: GET CERT
(SIP URI, PIN, CSR)
826
HTTPS: SIGNED CERT
828
HTTPS: PUBLISH KEY
(SIP URI, PIN, KEY)
830
HTTPS: PUBLISH
KEY (SIP URI,
PIN, KEY)
832
HTTPS: OK
834
TLS TO REGISTRAR
FQDN
836
REGISTER (SIP URI)
SUPPORTED, CERT
838
SIP 401WW-
AUTHENTICATE:
CERT
840
AUTH (SIP URI, CERT)
842
REGISTER (SIP URI)
AUTHORIZATION: CERT,
CERT PARAM
844
200 OK
846

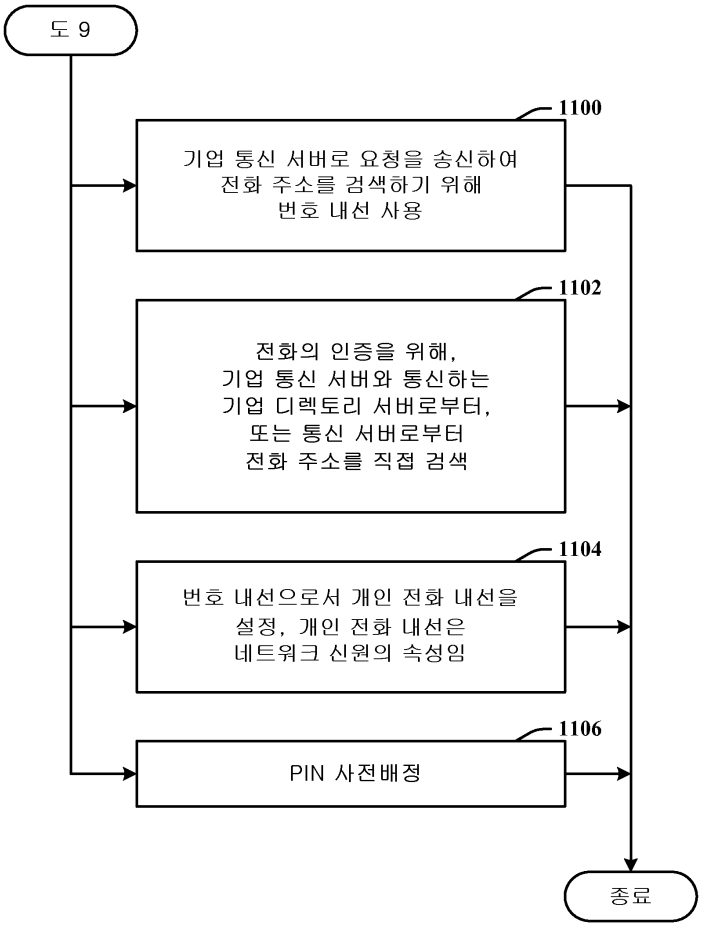
도면9


시작
전화로부터 번호 내선 및 PIN을 수신
900
번호 내선에 기초하여 기업 통신 서버로 전화 인증
902
전화 주소를 전화로 송신
904
전화 주소에 기초하여 기업 통신 서버로 전화 등록
906
종료

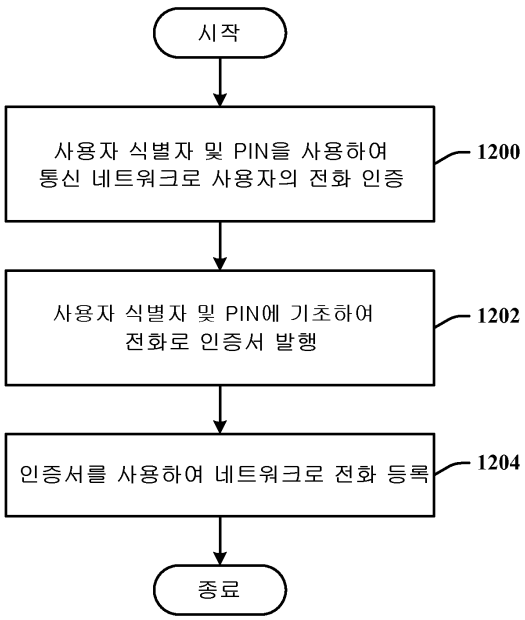
도면10


도 9
1000
전화로 기업 통신 서버의 IP 주소 및 FQDN 요청
1002
기업 통신 서버로부터 전화로 SIP URI 반환
1004
전화로부터 기업 통신 서버로 HTTP 메시지 송신
1006
SIP URI 또는 전화 URI중의 하나를 송신하는 것을 포함하여 전화 주소 송신
종료

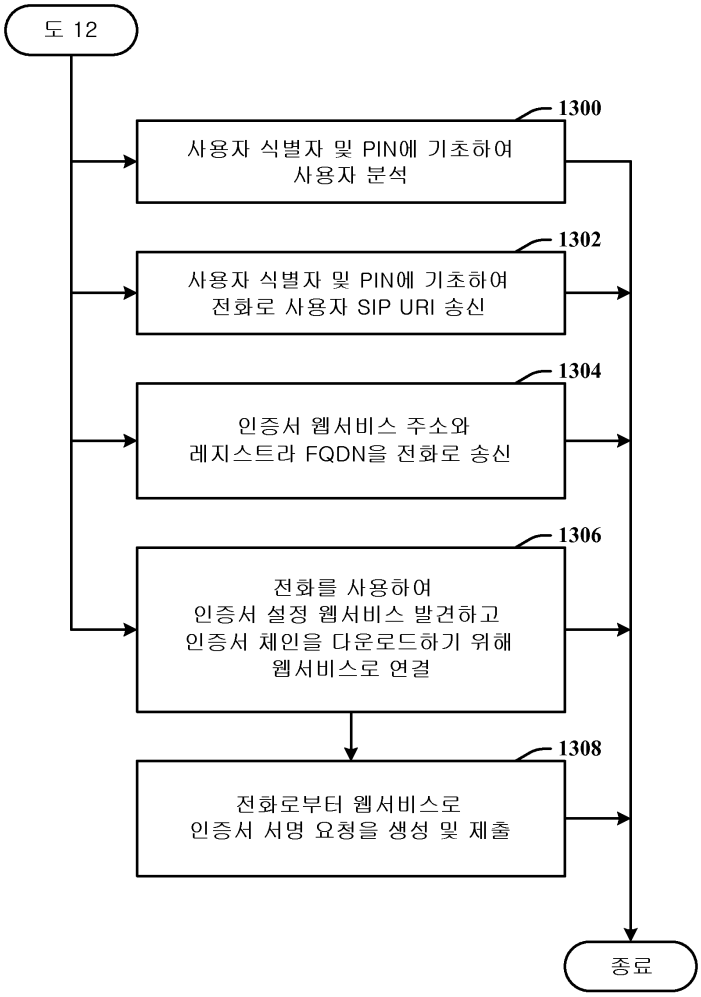
도면11


도 9
1100
기업 통신 서버로 요청을 송신하여
전화 주소를 검색하기 위해
번호 내선 사용
1102
전화의 인증을 위해,
기업 통신 서버와 통신하는
기업 디렉토리 서버로부터,
또는 통신 서버로부터
전화 주소를 직접 검색
1104
번호 내선으로서 개인 전화 내선을
설정, 개인 전화 내선은
네트워크 신원의 속성임
1106
PIN 사전배정
종료

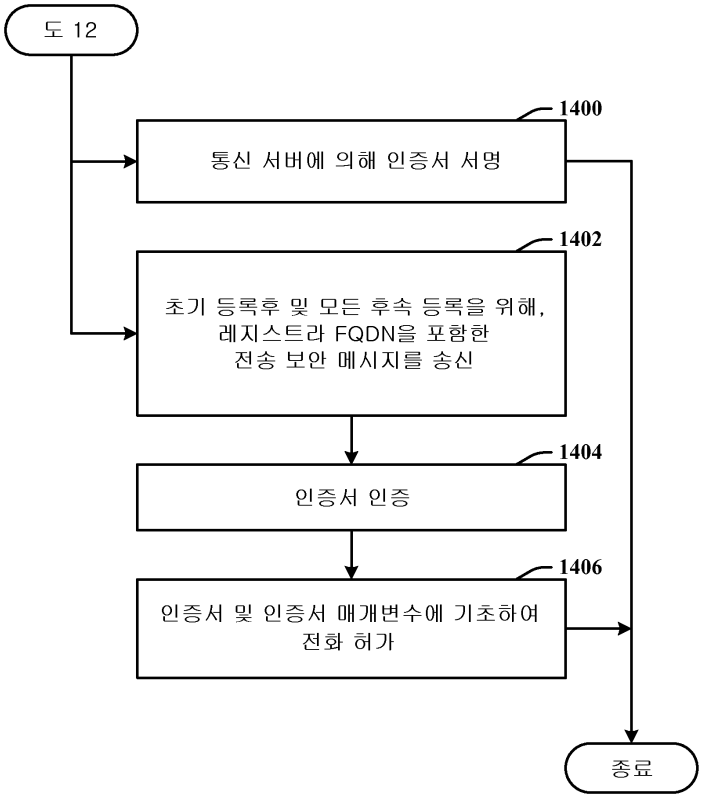
도면12


시작
사용자 식별자 및 PIN을 사용하여
통신 네트워크로 사용자의 전화 인증
1200
사용자 식별자 및 PIN에 기초하여
전화로 인증서 발행
1202
인증서를 사용하여 네트워크로 전화 등록
1204
종료

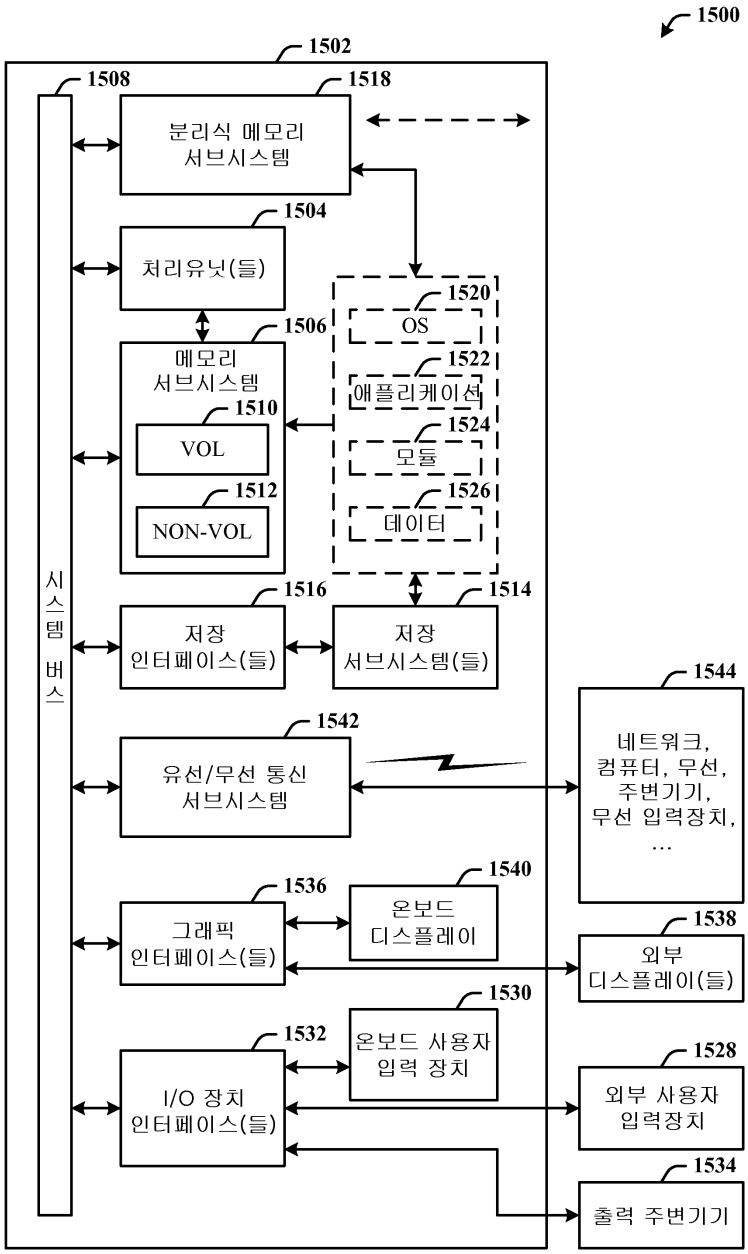
도면13


도 12
1300
사용자 식별자 및 PIN에 기초하여
사용자 분석
1302
사용자 식별자 및 PIN에 기초하여
전화로 사용자 SIP URI 송신
1304
인증서 웹서비스 주소와
레지스트라 FQDN을 전화로 송신
1306
전화를 사용하여
인증서 설정 웹서비스 발견하고
인증서 체인을 다운로드하기 위해
웹서비스로 연결
1308
전화로부터 웹서비스로
인증서 서명 요청을 생성 및 제출
종료

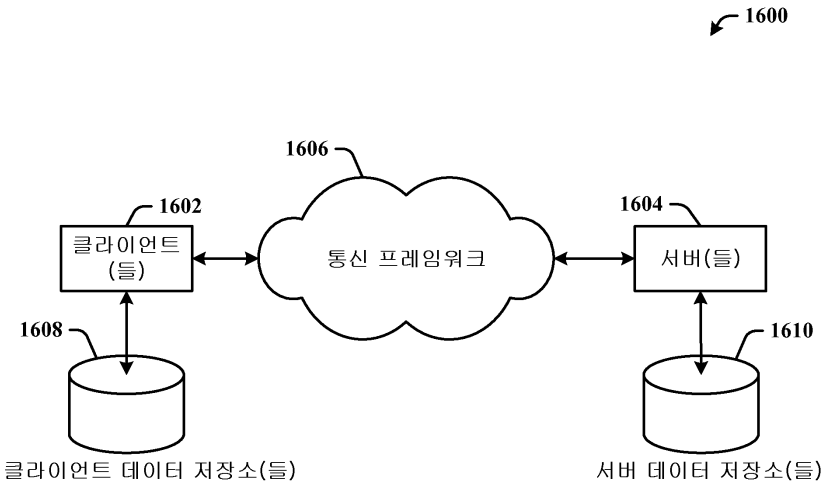
도면14


도 12
1400
통신 서버에 의해 인증서 서명
1402
초기 등록후 및 모든 후속 등록을 위해,
레지스트라 FQDN을 포함한
전송 보안 메시지를 송신
1404
인증서 인증
1406
인증서 및 인증서 매개변수에 기초하여
전화 허가
종료

도면15


1500
1502
1508
1518
분리식 메모리
서브시스템
1504
처리유닛(들)
1520
OS
1506
메모리
서브시스템
1522
애플리케이션
1510
VOL
1524
모듈
1512
NON-VOL
1526
데이터
시스템 버스
1516
저장
인터페이스(들)
1514
저장
서브시스템(들)
1544
네트워크,
컴퓨터, 무선,
주변기기,
무선 입력장치,
…
1542
유선/무선 통신
서브시스템
1540
1536
그래픽
인터페이스(들)
온보드
디스플레이
1538
외부
디스플레이(들)
1530
1532
온보드 사용자
입력 장치
1528
I/O 장치
인터페이스(들)
외부 사용자
입력장치
1534
출력 주변기기

도면16


1600
1606
1602
클라이언트
(들)
통신 프레임워크
1604
서버(들)
1608
1610
클라이언트 데이터 저장소(들)
서버 데이터 저장소(들)