



(51) International Patent Classification:

H04L 29/06 (2006.01) H04M 7/00 (2006.01)

H04L 29/08 (2006.01)

(21) International Application Number:

PCT/US2020/035002

(22) International Filing Date:

28 May 2020 (28.05.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16/453,952 26 June 2019 (26.06.2019) US

(71) Applicant: **ORACLE INTERNATIONAL CORPORATION** [US/US]; 500 Oracle Parkway, Mail Stop 50P7, Redwood Shores, CA 94065 (US).

(72) Inventors: **ZHANG, Shuquan**; Building No. 24, Zhongguancun Software Park, Beijing, 100193 (CN). **Ji, Weigan**; No. 26 Zibahebeili, Chaoyang District, Beijing, 100028 (CN). **MELO, Michael, David**; 24 Birch Road, Framingham, MA 01701 (US). **COCO, Frank**; 6 Zion Hill Road, Salem, NH 03079 (US).

(74) Agent: **HUNT, Gregory, A.**; Jenkins, Wilson, Taylor & Hunt, P.A., 3015 Carrington Mill Boulevard, Suite 550, Morrisville, NC 27560 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) Title: METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR ESTABLISHING A COMMUNICATION SESSION BETWEEN A PUBLIC SWITCHED TELEPHONE NETWORK (PSTN) ENDPOINT AND A WEB REAL TIME COMMUNICATIONS (WEBRTC) ENDPOINT

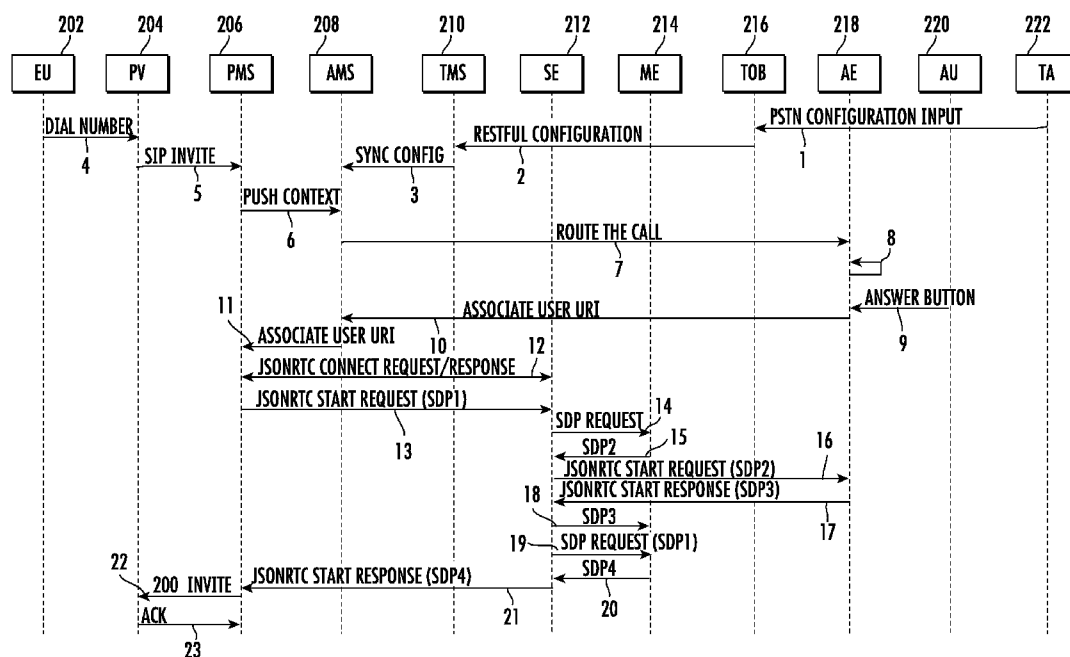


FIG. 2

(57) Abstract: A method for establishing a communication session between a public switched telephone network (PSTN) endpoint and a Web real time communications (WebRTC) endpoint includes receiving, by a PSTN microservice (MS), a session initiation protocol (SIP) based signaling message from a PSTN endpoint and acquiring, by the PSTN MS, endpoint context attribute information from the SIP based signaling message. The method further includes generating, by the PSTN MS, a WebRTC based signaling message that includes an address identifier of an associate endpoint (AE) that is associated with the context attribute information and transmitting, by the PSTN MS, the WebRTC based signaling message to the AE to initiate a call session between the PSTN endpoint and the AE.

SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

DESCRIPTION

METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR
ESTABLISHING A COMMUNICATION SESSION BETWEEN A PUBLIC
SWITCHED TELEPHONE NETWORK (PSTN) ENDPOINT AND A WEB
5 REAL TIME COMMUNICATIONS (WEBRTC) ENDPOINT

PRIORITY CLAIM

This application claims the priority benefit of U.S. Patent Application
Serial No. 16/453,952, filed June 26, 2019, the disclosure of which is
10 incorporated herein by reference in its entirety.

TECHNICAL FIELD

The subject matter described herein relates to enabling real time
communications between public switched telephone network (PSTN) users
15 and Web real time communications (WebRTC) users. More particularly, the
subject matter described herein relates to methods, systems, and computer
readable media for establishing a communication session between a PSTN
endpoint and a WebRTC endpoint.

20

BACKGROUND

Presently, web-based applications and instant messaging clients are
frequently used to communicate media and messages over the Internet.
Likewise, PSTN phone based telecommunications are commonly employed
to establish voice-based call sessions. Notably, each of these different
25 network systems normally requires that all supported endpoints establish a
connection to a call center or server using a common protocols, a common
software client, and the like. In instances where communication between a
WebRTC endpoint and a PSTN-based endpoint is desired, problems can arise
due to incompatible signaling protocols and/or the inability of the different
30 terminal device to reliably share endpoint information. In particular, it is
important for a WebRTC application to have knowledge of some particular
details of the endpoint with which the application is communicating. Further,
additional technical challenges can develop when WebRTC endpoints attempt

to interwork with PSTN endpoints, since a WebRTC based system largely enables the communication of real time media using secure real time protocol (SRTP), which is not used by PSTN endpoints or systems.

Accordingly, there exists a need for methods, systems, and computer
5 readable media for establishing a communication session between a PSTN endpoint and a WebRTC endpoint.

SUMMARY

The subject matter described herein includes a methods, systems, and
10 computer readable media for establishing a communication session between a PSTN endpoint and a WebRTC endpoint. One method includes receiving, by a PSTN microservice (MS), a session initiation protocol (SIP) based signaling message from a PSTN endpoint and acquiring, by the PSTN MS, endpoint context attribute information from the SIP based signaling message.
15 The method further includes generating, by the PSTN MS, a WebRTC based signaling message that includes an address identifier of an associate endpoint (AE) that is associated with the context attribute information and transmitting, by the PSTN MS, the WebRTC based signaling message to the AE to initiate a call session between the PSTN endpoint and the AE.

20 In one example of the method, the PSTN MS initiates a WebSocket connection with a signaling engine (SE) in response to receiving the SIP based signaling message.

In one example, the method further includes acquiring the endpoint context attribute information including parsing a header section of the SIP
25 based signaling message to obtain origin and/or destination information and call type information that is used to generate the endpoint context attribute information.

In one example of the method, the address identifier of the AE is acquired in response to pushing the endpoint context attribute information to
30 an associate microservice associated with the AE via a representation state transfer (REST) application programming interface (API).

In one example of the method, the PSTN MS sends a join queue request to the AE in response the endpoint context attribute information is pushed via the REST API.

5 In one example of the method, the PSTN MS converts the SIP signaling message to a JavaScript Object Notation (JSON) protocol signaling message that is recognized by the AE.

In one example of the method, the JSON protocol signaling message is a conversation start request message that initiates the call session with the AE.

10 A system for establishing a communication session between a PSTN endpoint and a WebRTC endpoint includes a cloud communication environment (CCE) comprising at least one processor and memory. The system further includes a PSTN MS stored in the memory and when executed by the at least one processor is configured to receive a SIP based signaling
15 message from a PSTN endpoint, acquire endpoint context attribute information from the SIP based signaling message, generate a WebRTC based signaling message that includes an address identifier of an AE that is associated with the context attribute information, and transmit the WebRTC based signaling message to the AE to initiate a call session between the PSTN
20 endpoint and the AE.

In one example of the system, the PSTN MS initiates a WebSocket connection with a signaling engine (SE) in response to receiving the SIP based signaling message.

25 In one example of the system, the PSTN MS is further configured to parse a header section of the SIP based signaling message to obtain origin and/or destination information and call type information that is used to generate the endpoint context attribute information.

In one example of the system, the address identifier of the AE is acquired in response to pushing the endpoint context attribute information to
30 an associate microservice associated with the AE via a REST API.

In one example of the system, the PSTN MS sends a join queue request to the AE in response the endpoint context attribute information is pushed via the REST API.

In one example of the system, the PSTN MS converts the SIP signaling message to a JavaScript Object Notation (JSON) protocol signaling message that is recognized by the AE.

5 In one example of the system, the JSON protocol signaling message is a conversation start request message that initiates the call session with the AE.

The subject matter described herein may be implemented in hardware, software, firmware, or any combination thereof. As such, the terms “function” “node” or “engine” as used herein refer to hardware, which may also include software and/or firmware components, for implementing the feature being described. In one exemplary implementation, the subject matter described herein may be implemented using a non-transitory computer readable medium having stored thereon computer executable instructions that when executed by the processor of a computer control the computer to perform steps. Exemplary computer readable media suitable for implementing the subject matter described herein include non-transitory computer-readable media, such as disk memory devices, chip memory devices, programmable logic devices, and application specific integrated circuits. In addition, a computer readable medium that implements the subject matter described herein may be located on a single device or computing platform or may be distributed across multiple devices or computing platforms.

BRIEF DESCRIPTION OF THE DRAWINGS

25 Figure 1 is a block diagram illustrating an exemplary network for establishing a communication session between a PSTN endpoint and a WebRTC endpoint according to an embodiment of the subject matter described herein;

Figure 2 is a signaling diagram illustrating an exemplary call flow for establishing a communication session between a PSTN endpoint and a WebRTC endpoint according to an embodiment of the subject matter described herein; and

30 Figure 3 is a flow chart illustrating an exemplary process for establishing a communication session between a PSTN endpoint and a

WebRTC endpoint according to an embodiment of the subject matter described herein.

DETAILED DESCRIPTION

5 Methods, systems, and computer readable media for establishing a communication session between a public switched telephone network (PSTN) endpoint and Web real time communications (WebRTC) endpoint are disclosed. In some embodiments, the disclosed subject matter includes an external PSTN endpoint that is permitted to communicate with a web-based
10 associate endpoint (AE). In such instances, a protocol translation is needed to initiate and establish a call or communication session. A host system, such as a cloud communication environment (CCE) utilizes a plurality of microservices (e.g., virtual machines and/or software applications) that are collectively configured to accept an inbound session initiation protocol (SIP)
15 INVITE message from outside the CCE and subsequently translate a SIP INVITE message to a signaling message based on the JavaScript Object Notation (JSON) RTC protocol. By doing so, the receiving AE can promptly accept the incoming call in a seamless manner (e.g., function as if the call originated from another AE). The CCE system is also configured to push
20 related context attribute information pertaining to the sending PSTN endpoint to notify the destination AE that the call signaling message is originating from an endpoint supported in the PSTN system (e.g., "callType: PSTN").

Figure 1 is a block diagram illustrating an exemplary network for establishing a communication session between a PSTN endpoint and a
25 WebRTC endpoint according to an embodiment of the subject matter described herein. For example, Figure 1 depicts a network **100** that includes a PSTN endpoint **102**, a PSTN SIP trunk **104**, a firewall **106**, a load balancer **108**, and a CCE system that comprises at least one external host domain **110** and at least one internal host domain **112**.

30 In some embodiments, PSTN endpoint **102** comprises a mobile device, user equipment, Voice over IP (VoIP) phone, or the like that is capable of communicating over a PSTN network (e.g., PSTN SIP trunk **104**). Notably, endpoint **102** is configured to communicate and establish sessions using SIP

and session description protocol (SDP) signaling messages. In particular, PSTN endpoint **102** may attempt to establish a call session with a WebRTC endpoint, such as AE **114**, by directing a SIP INVITE message toward external host domain **110**. In some embodiments, AE **114** may comprise any WebRTC endpoint, such as a desktop device, a laptop device, a mobile device (e.g., iOS, Android, etc.), or the like.

The SIP INVITE message sent by PSTN endpoint **102** is initially received by a firewall **106** via PSTN SIP trunk **104**. Notably, firewall **106** can provide network address translation (NAT) services of the public facing Internet protocol (IP) network (e.g., 129.146.x.x) for the private network (e.g., 10.0.x.x), which the devices and/or microservices of external host domain **110** are connected. In some embodiments, firewall **106** is a bare metal as a service (BMaaS) firewall.

After successfully passing through firewall **106** (e.g., via a particular port), the SIP INVITE message is received by load balancer **108**. In some embodiments, load balancer **108** is configured to distribute one or more PSTN calls across the host devices and/or microservices of external host domain **110**, which may be configured as a set of back-end servers and/or virtual machines. For example, load balancer **108** is adapted to select one of a plurality of enterprise session Border Controller (ESBC) microservices (e.g., ESBC MS **116**) hosted in the external host domain **110** of the CCE system to process any incoming SIP INVITE messages. In some embodiments, the IP address of load balancer **108** is provisioned in the PSTN SIP trunk **104**. For example, the existing 10.0.x.x private network address can be used to carry the PSTN signaling and media traffic. Because ESBC MS **116** is positioned behind firewall **106**, ESBC MS **116** is configured for NAT traversal such that the SIP and media negotiations reflect the public side IP address of firewall **106**. More specifically, during SIP and media negotiations, the PSTN endpoint **102** will be presented with the BMaaS public facing IP address to reach the ESBC MS **116** in the external host domain **110**.

In some embodiments, external host domain **110** comprises one or more hardware devices that are configured to support and execute ESBC MS **116**, TURN MS **128**, and OHS MS **124**. For example, external host domain

110 may can be implemented in software in combination with hardware and/or firmware. Notably, the subject matter described herein can be implemented in software executed by a processor. In one exemplary implementation, external host domain **110** may include one or more processors, such as a central processing unit (e.g., a single core or multiple processing cores), a microprocessor, a microcontroller, a network processor, an application-specific integrated circuit (ASIC), or the like. External host domain **110** may also include memory. Memory may comprise random access memory (RAM), flash memory, a magnetic disk storage drive, and the like. In some embodiments, memory may be configured to store one or more microservices. In some embodiments, the processor(s) and memory may be managed by a hypervisor to serve as the underlying hardware for supporting virtual machine(s) (VMs) that support the aforementioned microservices **116**, **124**, **128** that are supported in external host domain **110**.

As shown in Figure 1, ESBC MS **116** is configured to receive signaling communications from PSTN SIP trunk **104** via firewall **106** and load balancer **108**. For example, ESBC MS port '5061' can be publicly exposed and adapted to accept SIP over TLS connections. ESBC MS **116** is configured to terminate the PSTN side of the call session and subsequently load balance the SIP INVITE message to a plurality of back end PSTN microservices (e.g., PSTN MS **118**). In some embodiments, ESBC MS **116** is configured to utilize a round-robin load balancing method. In alternate embodiments, ESBC MS **116** can support other types of algorithms or methods to load balance signaling messages directed to AEs as the need arises. After selecting the appropriate PSTN microservice, ESBC MS **116** can establish a secure connection with PSTN MS **118** using transport layer security (TLS), secure sockets layer (SSL), Transmission control protocol (TCP)/IP, or the like.

In some embodiments, EBSC MS **116** is configured to provide the necessary security for the PSTN traffic received by the CCE. For example, ESBC MS **116** may secure the SIP signaling plane by requiring SIP over TLS communication when communicating with a PSTN service provider (e.g., via PSTN SIP trunk **104**). Likewise, ESBC MS **116** can also be configured to secure the media plane by requiring encryption of all media traffic using secure

real-time transport protocol (SRTP). In addition to utilizing SRTP, ESBC MS **116** can provide protection for the exposed media ports against denial of service (DoS), distributed denial of service (DDoS) attacks, and man-in-the-middle attacks. In some embodiments, ESBC MS **116** can run as a kernel-based virtual machine (KVM) instance in the CCE external host domain, not
5 unlike the OHS MS **124** and TURN MS **128**.

In some embodiments, ESBC MS **116** can be used as a public facing service that is configured to negotiate the SIP signaling and media signaling required to establish a PSTN call through the CCE. As indicated above, ESBC
10 MS **116** can be provisioned as a KVM instance on one or more devices/servers in external host domain **110**. The external host domain(s) are deployed behind a BMaaS firewall **106** and load balancer **108**. Firewall **106** provides network address translation (NAT) services for the IP network (129.146.x.x) that is public facing to the private network (10.0.x.x), which the
15 external hosts are connected in external host domain **110**. In some embodiments, External host domain **110** will be provisioned with at least one firewall rule that permits incoming packet traffic originating from the PSTN service provider's SIP port (and a range of media ports) and forwards that traffic to the 10.0.x.x private interface of ESBC MS **116**. Further, a PSTN
20 service provider can be configured with a BMaaS load balancer IP address in order to direct communications toward the CCE. For example, BMaaS load balancer **108** can distribute incoming calls across one or more backend servers (and/or microservices) of external host domain **110**. The existing IP address of the BMaaS load balancer **108** can be provisioned in the PSTN SIP
25 trunk **104** to reach the CCE service. The existing 10.0.x.x private network will be used to carry the PSTN signaling and media traffic.

Because the ESBC MS **116** is behind BMaaS firewall **106**, ESBC MS **116** will be configured for NAT traversal so that the SIP and media negotiations reflect the public side IP address of BMaaS firewall **106**.
30 Specifically, during SIP and media negotiations, PSTN endpoints (e.g., endpoint **102**) will be presented with the BMaaS public facing IP address that can be used to establish contact with the ESBC MS **116**.

For the SIP signaling traffic, ESBC MS **116** can be configured to distribute the load among a plurality of PSTN microservices (e.g., PSTN MS **118**) in the internal host domain **112**. For the media traffic, ESBC MS **116** can forward the packet traffic to a backend media engine (ME) server (e.g., a ME microservice **120**), which will then direct the media traffic to the next hop (e.g., a TURN server and/or microservice **128**) for delivery to the associate endpoint (e.g., AE **114**). It is understood that the existing ME microservices can support a mix of MCU and SFU sessions.

In some embodiments, ESBC MS **116** is configured to perform SIP trunking terminations, TLS and SRTP support, advanced DOS and overload protection, NAT support (e.g., when the ESBC MS is positioned behind a firewall), KVM support, and routing SIP message to a backend set of servers. ESBC MS **116** is further configured to conduct 1:1 optional high availability (HA) support, supports all the relevant PSTN and ME related codecs, and is capable of supporting 12000 signaling sessions, 6000 SRTP sessions, and 2500 transcoded sessions (G.721 <-> G.729).

In some embodiments, the ESBC MS forwards the load balanced SIP INVITE message to a selected/designated PSTN MS **118** that is positioned in the internal host domain **112** of the CCE. In some embodiments, internal host domain **112** may comprise one or more hardware devices that are configured to support and execute tenant MS **105**, associate MS **107**, PSTN MS **118**, ME MS **120**, and SE MS **122**. For example, internal host domain **112** may be implemented in software in combination with hardware and/or firmware. Notably, the subject matter described herein can be implemented in software executed by a processor. In one exemplary implementation, internal host domain **112** may include one or more processors, such as a central processing unit (e.g., a single core or multiple processing cores), a microprocessor, a microcontroller, a network processor, an application-specific integrated circuit (ASIC), or the like. Internal host domain **112** may also include memory. Memory may comprise random access memory (RAM), flash memory, a magnetic disk storage drive, and the like. In some embodiments, memory may be configured to store one or more microservices. In some embodiments, the processor(s) and memory may be

managed by a hypervisor to serve as the underlying hardware for supporting virtual machine(s) (VM) that support the aforementioned microservices **105-107** and **118-122**.

5 In some embodiments, PSTN MS **118** is configured to handle SIP requests received from outside the CCE (via ESBC MS **116**). As an example, PSTN MS **118** can support a SIP-related call setup method and signaling messages, such as SIP INVITE, UPDATE, ACK, BYE, and CANCEL messages. In some embodiments, PSTN MS **118** can also be configured to implement a SipServlet to handle a SIP INVITE request.

10 After receiving an initial SIP INVITE message, PSTN MS **118** is configured to i) retrieve a tenant key and/or a client identifier based on the target phone number (i.e., called party phone number), ii) generate a JWT token, iii) establish a connection to SE MS **122** via a WebSocket, iii) parse 'from' and 'to' headers of a received SIP INVITE and generate endpoint context attribute information, and iv) push the endpoint context attribute data to an associate MS **107** via a REST API. In some embodiments, associate MS **107** contains a plurality of routing rules that can be used to establish the connection between a PSTN endpoint and a target AE via PSTN MS **118**. Notably, in order to route the PSTN call to the correct associate or correct team (e.g., AE **114**), routing rules need to be initially configured by a tenant administrator on TOB UI **103**. A provisioned routing rule can be based on a target PSTN number, e.g., calls directed to "+01234" will be routed to mceAgent@example.com. Alternatively, the routing rule can also be based on the originating number of PSTN endpoint **102** (e.g., a call from "+64xxx" may be routed to the "NZ support team"). Based on the associate name returned to PSTN MS **118** by the associate MS **107**, PSTN MS **118** can translate or convert the SIP INVITE message to initiate a communication session with a target (e.g., AE) associated with an associate name. As such, this request will be sent to the correct associate or AE. For example, PSTN MS **118** may be further configured to v) send a join queue REST request message after the context attribute information is successfully pushed to the associate MS **107**, and vi) create a conversation inquiry request and send the message to SE MS **122**. After obtaining an inquiry/response, create a

15
20
25
30

conversation start/request message with the related AE information. After obtaining a start/response message, PSTN MS **118** creates a SIP 200 response message for the initial SIP INVITE request sent by the PSTN endpoint **102**. More specifically, when the AE responds with the answer SDP, PSTN MS **118** may generate a SIP 200 message with an answer SDP for the original/initial SIP INVITE request sent by PSTN endpoint **102**.

In some embodiments, PSTN MS **118** receives a SIP CANCEL message before a call is answered and is configured to send a cancel “joinQueue request” to associate MS **107** and may also close the WebSocket with SE MS **122**. PSTN MS **118** then receives the SIP CANCEL message after AE **114** answers, but SIP 200 messages are not delivered to the PSTN client (e.g., PSTN endpoint **102**). In such instances, PSTN MS **118** will send a shutdown message to the SE MS **122** and close the WebSocket.

In some embodiments, AE **114** is configured to communicate via PSTN MS **118** using WebRTC, which is a protocol that enables real-time communication in a hosted browser (as defined in IETF and W3C standards). As indicated above, endpoints that are configured to communicate in WebRTC present some technical challenges in instances where communication with a PSTN endpoint is desired. For example, WebRTC enables the secure communication of real time media using SRTP. However, this protocol is not largely recognized and/or utilized by PSTN networks. In order to address this technical problem, the disclosed subject matter describes a method that provides for a push contextAPI, JavaScript Conversation SDK, and JSON RTC protocol. As such, the disclosed subject matter enables developers to readily construct applications that provide an interworking service for both PSTN users and WebRTC users.

In some embodiments, ESBC MS **116** is configured to negotiate a media session with a PSTN service via PSTN SIP trunk **104** (after the signaling session is initiated). Notably, a range of ESBC media ports can be exposed by ESBC MS **116**. As such, media traffic arriving at the exposed ESBC media ports will be subjected to network address translation (NAT) by firewall **106** to the private IP address of the external host domain **110**. In some embodiments, external host domain **110** will have a firewall rule provisioned

to port forward the range of media ports to the ESBC MS **116**. Once the ESBC MS **116** receives the PSTN media traffic, ESBC MS **116** will forward the media traffic to ME MS **120** for delivery to AE **114**. The media path existing between PSTN SIP trunk **104** and ESBC MS **116** may use SRTP to provide confidentiality, message authentication, and replay protection for the communicated media traffic. In addition to SRTP, ESBC MS **116** can provide security and protection for the publicly exposed ESBC media ports against DOS attacks, DDOS attacks, and man-in-the-middle attacks. However, ESBC MS **116** will not provide any transcoding functionality. Rather, ME MS **120** will be responsible for any transcoding that may be required for the media traffic associated with the established call between PSTN endpoint **102** and AE **114**.

In some embodiments, the disclosed subject matter can be configured to implement a number of security measures. In some embodiments, PSTN MS **118** requires a range or plurality of media ports to be exposed to the public side of the CCE system. Notably, the ME MS does not provide any DOS/DDOS or man-in-the-middle protection of the exposed media ports. As such, it is important for the CCE service to protect these media ports from external attacks. Therefore, the aforementioned ESBC MS **116** is configured to terminate the PSTN SIP trunk as a SIP message enters the CCE. ESBC MS **116** will act as a back-to-back user agent (b2bua) providing security on the public PSTN side and as an interface to PSTN MS **118**, which is positioned in the internal host domain **112** of the CCE. In some embodiments, the ESBC security is achieved by supporting TLS for SIP signaling and supporting SRTP for the media path, as well as protecting against DOS/DDOS and man-in-the-middle attacks. For example, ESBC MS **116** provides protection from possible TCP/TLS message flooding by limiting the number of connections from an endpoint, and by limiting the number of simultaneous TCP/TLS connections to a SIP interface. For example, ESBC MS **116** can use a 'StaticTLS' connection to the PSTN SIP trunk **104**, which means a single TLS connection is established from PSTN service provider to the CCE system. Notably, the signaling of all calls will be designated to use that single TLS connection. Once a call is established, if a SIP signaling event is initiated from the CCE side (e.g., the AE), then it is possible that the CCE system will need to initiate a new TLS

connection back to a PSTN endpoint supported by the PSTN service provider. For example, the connection can be made to the IP:port that was sent by a PSTN service provider in the Contact header of the initial SIP INVITE message. Therefore, a policy mandating a soft limit of TLS connections over the access side SIP interface may be enforced by ESBC MS **116**.

Furthermore, ESBC MS **116** can be configured to provide security measures for signaling messages. For example, a single port can be opened at firewall **106** and ESBC MS **116** in order to accommodate the receiving of SIP signaling messages. For example, a new port (e.g., 5061) can be opened for SIP over TLS communication. Likewise, a plurality of ports can be opened at firewall **106** and ESBC MS **116** in order to facilitate the accommodating of media traffic. For example, ESBC MS **116** can be installed in external host domain **110** and a range of ports (e.g., UDP ports 49152-60152) can be opened for media traffic (in both firewall **106** and ESBC MS **116**) in the external host domain **110**, such that an external PSTN phone (e.g., endpoint **102**) can communicate with AE **114**. In some embodiments, the media connection established between the PSTN SIP trunk **104** and ESBC MS **116** will be required to use SRTP to provide confidentiality, message authentication, and replay protection for the communicated media traffic.

In some embodiments, ESBC MS **116** is configured to provide signaling and media encryption. For example, the ESBC access side interface to the PSTN service provider (e.g., PSTN SIP trunk **104**) uses TLS to ensure the confidentiality of the SIP signaling layer. Likewise, the ESBC access side media layer uses SRTP to provide confidentiality, message authentication, and replay protection for the media path. In addition to TLS and SRTP, the PSTN service provider is provisioned to only accept calls from the BMaaS public IPs corresponding to the CCE system. Attempts to connect to the PSTN SIP trunk **104** from other non-CCE IPs will be rejected by the PSTN service provider. Similarly, CCE has provisioned security lists that only allow external access to the signaling and media ports from specific PSTN service provider public IPs that are provisioned solely for the CCE service. Access to the signaling/media ports from sources other than the PSTN service provider IP addresses will be rejected by ESBC MS **116**.

In some embodiments, ESBC MS **116** provides further protection internally within the CCE network by only allowing connections from configured 'session-agents'. A 'session-agent' in ESBC terminology is a SIP hop that ESBC MS **116** communicates with, so CCE has one session-agent for the access side (i.e., the external host domain IP address), and one for each supported PSTN MS. The ESBC MS **116** only allows SIP dialogs from these configured session-agents and rejects attempts from all other IPs.

As shown in Figure 1, network **100** further includes a tenant on-boarding (TOB) administrator user interface (UI) **103**. Using this interface, a tenant administrator user can provision and configure PSTN rules for each of a plurality of tenants and/or associate entities (i.e., system subscribers). For example, a tenant administrator can utilize TOB UI **103** (which may be embodied as a browser application hosted and executed by a user computing device) to add context attribute data in a tenant configuration table. The tenant administrator can subsequently configure PSTN rules on TOB UI **103** with the new defined context attribute for one or more tenants or associates. Notably, the context attribute data that is provisioned using TOB UI **103** can be used to configure a PSTN provider/vendor to be able to route PSTN calls to AEs supported by the CCE system. For example, TOB UI **103** can be used to specify an originating PSTN number in a routing rule condition table and specifying an AE as a predefined call destination (e.g., a target phone number). As such, all call signaling messages originating from a particular PSTN endpoint or PSTN vendor can be specifically routed to a particular AE (e.g., a "team").

In some embodiments, the security information configured by the tenant administrator is encrypted before it is stored in a management database. In some embodiments, a DKKey will be used to encrypt the private data. Further, PSTN vendor authentication information will be considered as private information, but tenant subscribed phone numbers can be designated as public information. Further, for cross microservice access, an Auth MS private key is replicated to the PSTN MS domain (e.g., internal host domain **112**), and the private key is used to generate a JWT token for a specific TenantKey/ClientId. Notably, the JWT token is used by PSTN MS **118** to

access the associate MS **107** and SE MS **122**. The use of the JWT token is designated for internal access and no public API is exported.

In some embodiments, the routing rules can be provisioned to one or more tenants by onboarding the rules as RESTful configuration data to a
5 corresponding one or more tenant microservices (TMS) **105**. After receiving the configuration data, TMS **105** can send a synchronization message to one or more related associate microservices (AMS) **107**. AMS **107** can then use the configuration data to specify specific routing rules for PSTN endpoints associated with the subscribed associate MS or tenant MS.

10 Figure 2 is a signaling diagram illustrating an exemplary call flow for establishing a communication session between a PSTN endpoint and a WebRTC endpoint according to an embodiment of the subject matter described herein. As shown in Figure 2, a tenant administrator (TA) **222** utilizes a tenant on-boarding (TOB) user interface **216** to provide a PSTN
15 configuration for each of one or more tenant entities (e.g., see message 1). In some embodiments, tenant administrator **222** is a system user or operator that is responsible for managing the tenants that are subscribed to and support by the CCE system. Notably, tenant administrator **222** can update the configuration data for the tenant entities serviced by the CCE system.

20 In response to the input by tenant administrator **222**, TOB UI **216** is configured to send a signaling message that contains RESTful configuration data (for a tenant entity) to a tenant microservice (TMS) **210** (e.g., see message 2). Tenant MS **210** subsequently provides the received configuration information to an associate MS (AMS) **208** for purposes of synchronization
25 (e.g., see message 3). Accordingly, associate MS **208** is thus provisioned with the PSTN configuration information originally designated by the tenant administrator **222** using TOB UI **216**.

As shown in Figure 2, PSTN endpoint **202** is utilized (e.g., by a user) to dial an access number that may correspond to and/or be mapped to an AE
30 **218** (e.g., see message 4). The dialed number information is received by PSTN vendor **204** (e.g., via a PSTN SIP trunk), which in turn generates a SIP INVITE message (e.g., see message 5) that is directed to the external host domain and/or AE **218**. After traversing a firewall, load balancer, and

designated EBSC MS (see description above and Figure 1), the SIP INVITE message (e.g., see message 6) is received by a PSTN MS (e.g., PSTN MS **206**) that has been selected by the external host network and/or EBSC MS. Notably, PSTN MS **206** extracts endpoint context attribute information from the received SIP INVITE message and provides said data to an associate MS **208** via a push context message.

In some embodiments, associate MS **208** is an agent application initially created by tenant administrator **222** and is responsible for answering calls from PSTN endpoints. In some embodiments, PSTN MS **206** provides the endpoint context attribute information to associate MS **208** using a push context message (e.g., pushContext/getAgentUri message) sent via a REST API (e.g., see message 6). Notably, the endpoint context attribute information can be generated by PSTN MS **206** using information extracted from the header of the received SIP INVITE message. For example, the endpoint context attribute information can include the "From" or "To" information contained in the header of the SIP INVITE message.

In some embodiments, associate MS **208** is responsible for determining which AE should be selected to answer the call request from PSTN endpoint **202**. Upon receiving the push context message (e.g., see message 6), associate MS **208** may be configured to access local routing rules that indicate the AE that is to be designated as the target. As indicated above, the routing rules can designate a target AE based on data contained in the endpoint context attribute information provided by the PSTN MS **206**. In some embodiments, associate MS **208** may cross-reference the endpoint context attribute information with entries in a local routing rules database whose entries include mappings of AE address identifiers with data corresponding to various context attributes.

Associate MS **208** subsequently routes the call to a selected destination AE, such as AE **218** (e.g., see message 7). After receiving the call, AE **218** can be configured to display an incoming call alert (e.g., see message 8). Such a call alert can be a visual display and/or audible signal that prompts an associate user **220** (e.g., user of AE **218**) to select an answer button (e.g., see message 9) in order to receive the call and ultimately establish a media

session connection. After the answer button is interfaced/activate by associate user **220**, AE **218** sends a response message, such as an “associateUser URI” message (e.g., see message 10) containing an address identifier of associate user **220**, to associate MS **208**. In some embodiments, the address
5 identifier can be a uniform resource identifier (URI) address that corresponds to the AE **218** and/or associate user **220**.

Accordingly, associate MS **208** forwards the message containing the associate user URI information to PSTN MS **206**, which then begins to establish a WebSocket connection with the signaling engine (SE) MS
10 **212**. For example, PSTN MS **206** generates and sends a Web RTC message, such as a JSON RTC connection request message, to SE **212** to establish the WebSocket connection. After receiving a response from SE **212**, PSTN MS **206** sends a JSON RTC start request message to SE **212**.

After receiving the start request message, SE **212** sends an SDP
15 request message (for AE **218**) to ME MS **214**. ME MS **214** responds with an SDP message, which is used by the endpoint to negotiate the parameters of the media channel, e.g. which codec to transmit the media. The SDP message also prompts SE **212** to send a JSON RTC start request message to AE **218**. AE **218** responds with a JSON RTC response message. In
20 response, SE MS **212** then sends an SDP message to ME MS **214**. After receiving an SDP message from ME MS **214**, SE **212** sends a JSON RTC start response message back to PSTN MS **206** as a reply to the initial JSON start request message. In response, PSTN MS **206** is triggered to communicate a 200 SIP INVITE acknowledge message to PSTN vendor **204**
25 (via a PSTN SIP trunk). PSTN vendor **204** subsequently sends an acknowledgement message to PSTN MS **206** to finalize the media connection between endpoint **202** and AE **218**.

Figure 3 is a flow chart illustrating an exemplary process or method **300** for establishing a communication session between a PSTN endpoint and a
30 WebRTC endpoint according to an embodiment of the subject matter described herein. In some embodiments, method **300** as depicted in Figure 3 is an algorithm stored in memory that when executed by a hardware processor performs one or more of blocks **302-308**.

In block **302**, a SIP based signaling message is received from a PSTN endpoint by a public switched telephone network (PSTN) microservice (MS). In some embodiments, a PSTN receives a SIP INVITE message from the PSTN endpoint device. Notably, the SIP INVITE message may traverse
5 through a firewall, a load balancer, and an ESBC MS (in the external host domain of the CCE) prior to reaching the PSTN MS (in the internal host domain of the CCE system).

In block **304**, endpoint context attribute information is acquired by the PSTN MS from the SIP based signaling message. In some embodiments, the
10 PSTN MS parses the headers of a received SIP INVITE message to extract “to” and “from” data from the signaling message. The PSTN MS pushes the endpoint context attribute information to an associate MS that is provisioned with routing rules. In response to receiving the endpoint context attribute information, the associate MS access a local routing rules database and
15 locates an address identifier that corresponds to the target AE and provides the identifier to the PSTN MS. The address identifier may be a URI corresponding to the target AE.

In block **306**, a Web real-time communications (WebRTC) based signaling message that includes the address identifier of an associate
20 endpoint (AE) that is associated with the endpoint context attribute information is generated by the PSTN MS. In some embodiments, the PSTN MS generates a Web RTC message, such as a JSON RTC message, that requests a communication session with the target AE corresponding to the address identifier.

25 In block **308**, the WebRTC based signaling message is transmitted by the PSTN MS to the AE to initiate a call session between the PSTN endpoint and the AE. In some embodiments, the PSTN MS directs the JSON RTC message to the AE destination to establish the call session between the AE and the sending PSTN endpoint.

30 It will be understood that various details of the presently disclosed subject matter may be changed without departing from the scope of the presently disclosed subject matter. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation.

CLAIMS

What is claimed is:

1. A method comprising:
 - receiving, by a public switched telephone network (PSTN) microservice (MS), a session initiation protocol (SIP) based signaling message from a PSTN endpoint;
 - acquiring, by the PSTN MS, endpoint context attribute information from the SIP based signaling message;
 - generating, by the PSTN MS, a web real time communications (WebRTC) based signaling message that includes an address identifier of an associate endpoint (AE) that is associated with the context attribute information; and
 - transmitting, by the PSTN MS, the WebRTC based signaling message to the AE to initiate a call session between the PSTN endpoint and the AE.
2. The method of claim 1 wherein the PSTN MS initiates a WebSocket connection with a signaling engine (SE) in response to receiving the SIP based signaling message.
3. The method of claim 1 or claim 2 wherein acquiring the endpoint context attribute information includes parsing a header section of the SIP based signaling message to obtain origin and/or destination information and call type information that is used to generate the endpoint context attribute information.
4. The method of any preceding claim wherein the address identifier of the AE is acquired in response to pushing the endpoint context attribute information to an associate microservice associated with the AE via a representation state transfer (REST) application programming interface (API).
5. The method of claim 4 wherein the PSTN MS sends a join queue request to the AE in response the endpoint context attribute information is pushed via the REST API.

6. The method of any preceding claim wherein the PSTN MS converts the SIP signaling message to a JavaScript Object Notation (JSON) protocol signaling message that is recognized by the AE.
7. The method of claim 6 wherein the JSON protocol signaling message is a conversation start request message that initiates the call session with the AE.
8. A system comprising:
 - a cloud communication environment (CCE) comprising at least one processor and memory; and
 - a public switched telephone network (PSTN) microservice (MS) stored in the memory and when executed by the at least one processor is configured to receive a session initiation protocol (SIP) based signaling message from a PSTN endpoint, acquire endpoint context attribute information from the SIP based signaling message, generate a Web real time communications (WebRTC) based signaling message that includes an address identifier of an associate endpoint (AE) that is associated with the context attribute information, and transmit the WebRTC based signaling message to the AE to initiate a call session between the PSTN endpoint and the AE.
9. The system of claim 8 wherein the PSTN MS initiates a WebSocket connection with a signaling engine (SE) in response to receiving the SIP based signaling message.
10. The system of claim 8 or claim 9 wherein the PSTN MS is further configured to parse a header section of the SIP based signaling message to obtain origin and/or destination information and call type information that is used to generate the endpoint context attribute information.
11. The system of any of claims 8 to 10 wherein the address identifier of the AE is acquired in response to pushing the endpoint context attribute information to an associate microservice associated with the AE via a representation state transfer (REST) application programming interface (API).

12. The system of claim 11 wherein the PSTN MS sends a join queue request to the AE in response the endpoint context attribute information is pushed via the REST API.
13. The system of any of claims 8 to 12 wherein the PSTN MS converts the SIP signaling message to a JavaScript Object Notation (JSON) protocol signaling message that is recognized by the AE.
14. The system of claim 13 wherein the JSON protocol signaling message is a conversation start request message that initiates the call session with the AE.
15. A non-transitory computer readable medium having stored thereon executable instructions that when executed by a processor of a computer controls the computer to perform steps comprising:
 - receiving, by a public switched telephone network (PSTN) microservice (MS), a session initiation protocol (SIP) based signaling message from a PSTN endpoint;
 - acquiring, by the PSTN MS, endpoint context attribute information from the SIP based signaling message;
 - generating, by the PSTN MS, a Web real time communications (WebRTC) based signaling message that includes an address identifier of an associate endpoint (AE) that is associated with the context attribute information; and
 - transmitting, by the PSTN MS, the WebRTC based signaling message to the AE to initiate a call session between the PSTN endpoint and the AE.
16. The non-transitory computer readable medium of claim 15 wherein the PSTN MS initiates a WebSocket connection with a signaling engine (SE) in response to receiving the SIP based signaling message.
17. The non-transitory computer readable medium of claim 15 or claims 16 wherein acquiring the endpoint context attribute information includes parsing a header section of the SIP based signaling message to obtain origin and/or destination information and call type information that is used to generate the endpoint context attribute information.

18. The non-transitory computer readable medium of any of claims 15 to 17 wherein the address identifier of the AE is acquired in response to pushing the endpoint context attribute information to an associate microservice associated with the AE via a representation state transfer (REST) application programming interface (API).
5
19. The non-transitory computer readable medium of claim 18 wherein the PSTN MS sends a join queue request to the AE in response the endpoint context attribute information is pushed via the REST API.
20. The non-transitory computer readable medium of any of claims 15 to 19 wherein the PSTN MS converts the SIP signaling message to a JavaScript Object Notation (JSON) protocol signaling message that is
10 recognized by the AE.

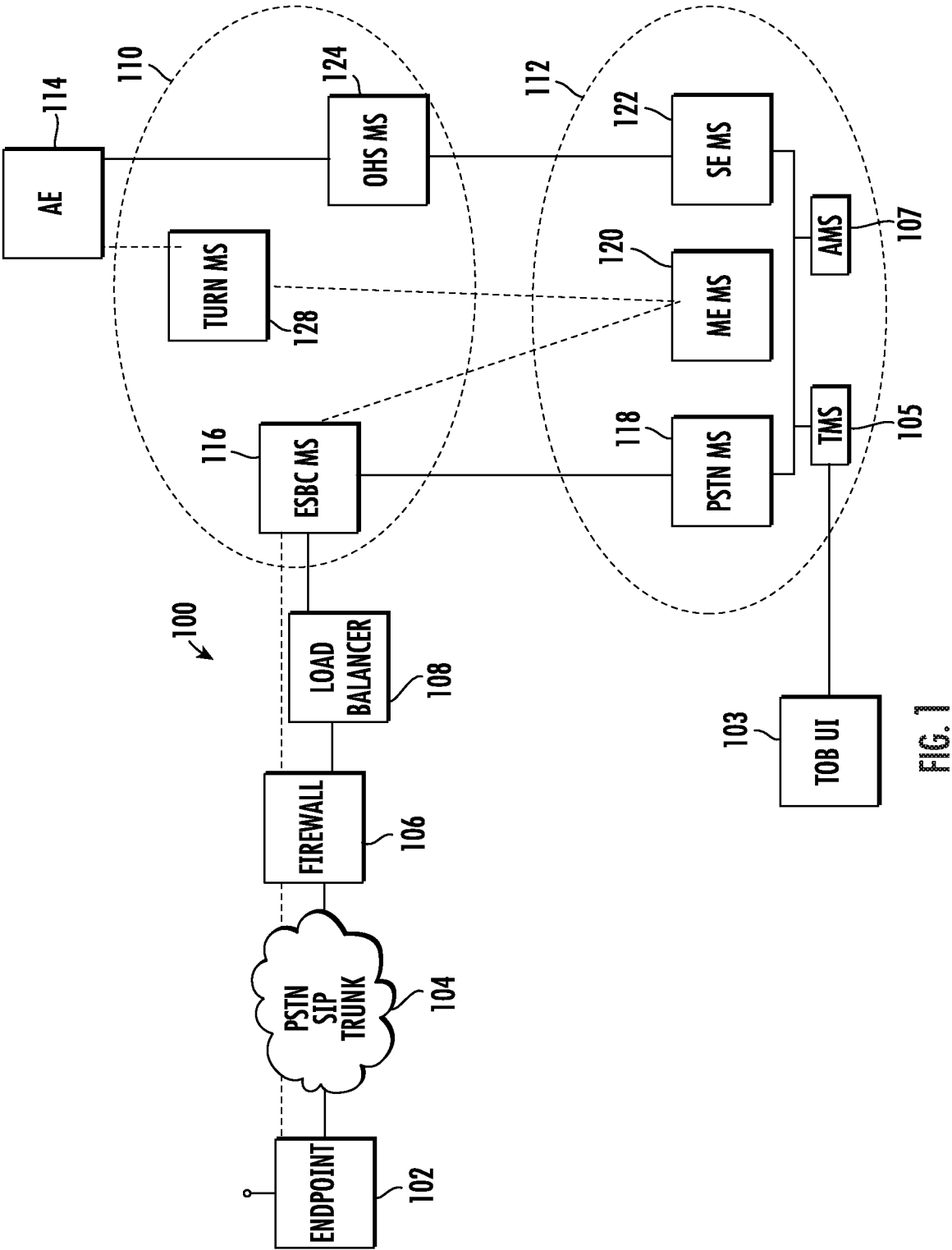


FIG. 1

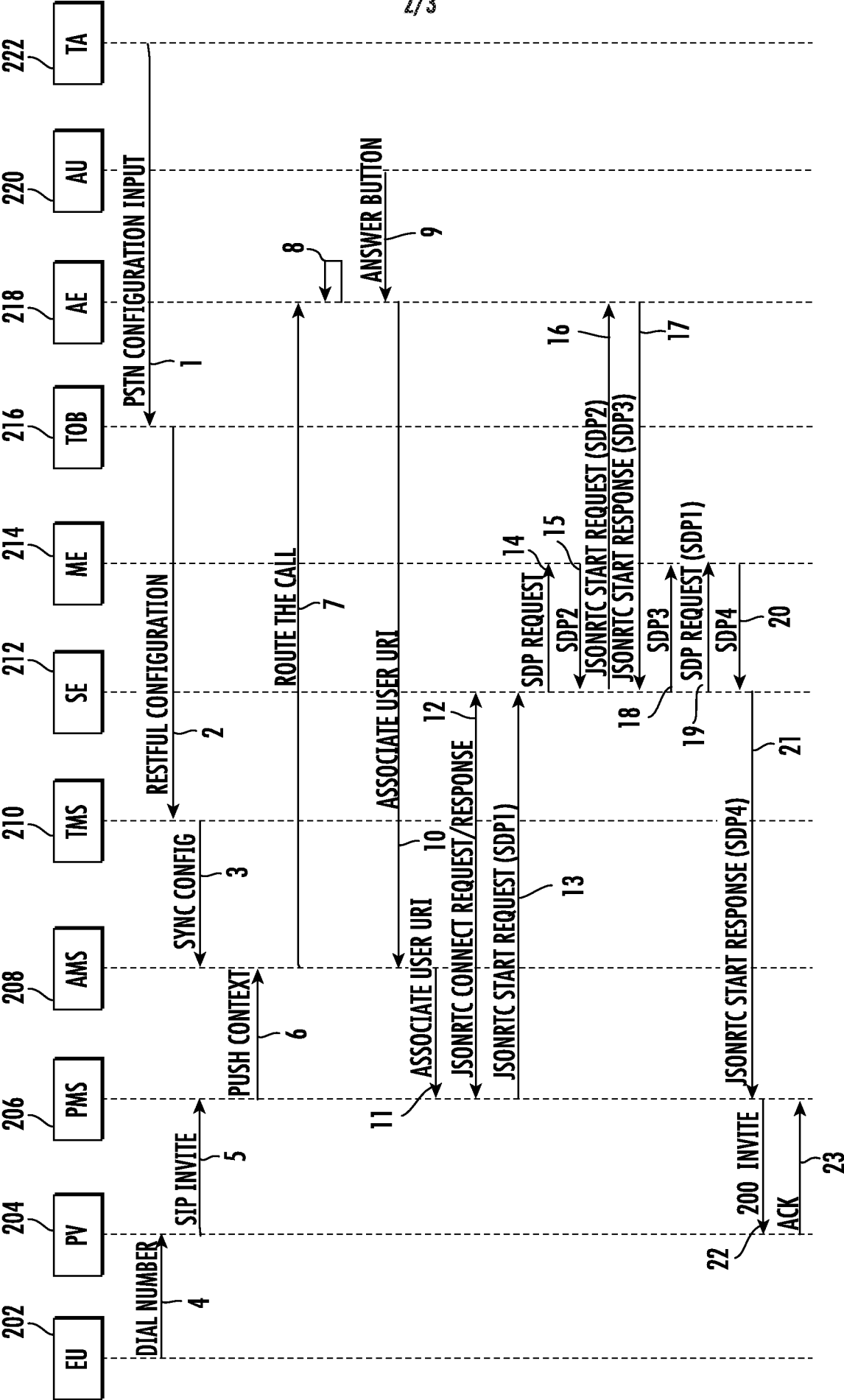


FIG. 2

3/3

300 →

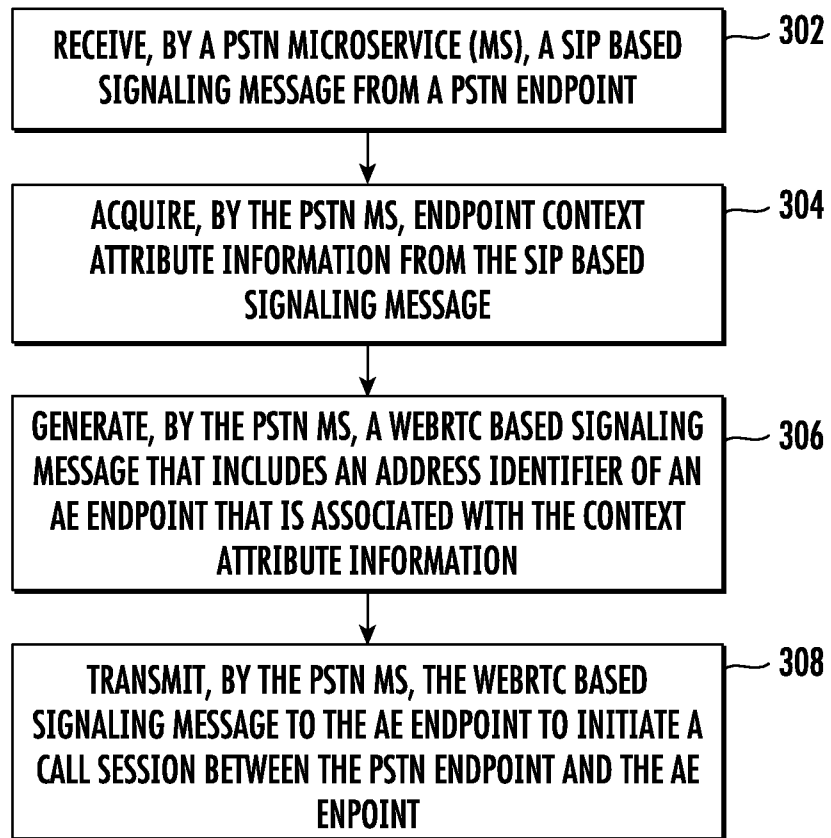


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2020/035002

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06 H04L29/08 H04M7/00
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

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

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2016/156256 A1 (BRITISH TELECOMM [GB]) 6 October 2016 (2016-10-06)	1-3, 8-10, 15-17
Y	page 2 l.16-29, page 3 l. 4-27, from page 7 l.10 to page 9 l. 10; figures 1,2	4-7, 11-14, 18-20
X	----- US 2016/219026 A1 (GANGADHARAN BINOD PANKAJAKSHY [IN] ET AL) 28 July 2016 (2016-07-28)	1,8,15
Y	paragraphs [0009] - [0012], [0018] - [0050]	4-7, 11-14, 18-20
A	----- -/-	2,3,9, 10,16,17



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

13 August 2020

Date of mailing of the international search report

21/08/2020

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Valero, Monica

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2020/035002

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KAPLAN ACME PACKET H: "Requirements for Interworking WebRTC with Current SIP Deployments; draft-kaplan-rtcweb-sip-interworking-requirements-02.txt", REQUIREMENTS FOR INTERWORKING WEBRTC WITH CURRENT SIP DEPLOYMENTS; DRAFT-KAPLAN-RTCWEB-SIP-INTERWORKING-REQUIREMENTS-02.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWI, 22 November 2011 (2011-11-22), pages 1-24, XP015079523, [retrieved on 2011-11-22] Chapters 5 and 6 -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2020/035002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2016156256 A1	06-10-2016	GB 2553230 A WO 2016156256 A1	28-02-2018 06-10-2016
US 2016219026 A1	28-07-2016	NONE	