



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
61/252,151	10/15/2009		220	RALEP025+		

CONFIRMATION NO. 9965

21912
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

FILING RECEIPT



OC000000038650283

Date Mailed: 11/10/2009

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Gregory G. Raleigh, Woodside, CA;

Power of Attorney:

Michael Schallop--44319

If Required, Foreign Filing License Granted: 11/06/2009

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 61/252,151**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international

patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and

Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

Doc Code: **TR.PROV**

Document Description: Provisional Cover Sheet (SB16)

PTO/SB/16 (04-07)

Approved for use through 06/30/2010 OMB 0851-0032

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name	Middle Name	Family Name	City	State	Country i
Gregory	G.	Raleigh	Woodside	CA	US

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.

Add

Title of Invention	SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES
Attorney Docket Number (if applicable)	RALEP025+

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number ☐ Firm or Individual Name

Customer Number 21912

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Entity Status

Applicant claims small entity status under 37 CFR 1.27

☐ Yes, applicant qualifies for small entity status under 37 CFR 1.27☒ No**Warning**

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Michael J. Schallop/			Date (YYYY-MM-DD)	2009-10-15
First Name	Michael	Last Name	Schallop	Registration Number (If appropriate)	44319

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that : (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to a n other federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICE

CROSS REFERENCE TO OTHER APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 61/206,354 (Attorney Docket No. RALEP001+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed January 28, 2009, U.S. Provisional Patent Application No. 61/206,944 (Attorney Docket No. RALEP002+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 4, 2009, U.S. Provisional Patent Application No. 61/207,393 (Attorney Docket No. RALEP003+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed February 10, 2009, U.S. Provisional Patent Application No. 61/207,739 (Attorney Docket No. RALEP004+) entitled SERVICES POLICY COMMUNICATION SYSTEM AND METHOD filed on February 13, 2009, U.S. Provisional Patent Application No. 61/270,353 (Attorney Docket No. RALEP022+) entitled DEVICE ASSISTED CDR CREATION, AGGREGATION, MEDIATION AND BILLING filed on July 6, 2009, U.S. Provisional Patent Application No. 61/275,208 (Attorney Docket No. RALEP023+) entitled ADAPTIVE AMBIENT SERVICES filed on August 25, 2009, and U.S. Provisional Patent Application No. 61/237,753 (Attorney Docket No. RALEP024+) entitled ADAPTIVE AMBIENT SERVICES filed on August 28, 2009, which are incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

[0002] With the advent of mass market digital communications, applications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), DOCSIS, DSL, and Wi-Fi (Wireless Fidelity) becoming user capacity constrained. In the wireless case, although network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum and cell splitting being

deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand.

[0003] Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user compared to wireless, wire line user service consumption habits are trending toward very high bandwidth applications and content that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Various embodiments of the invention are disclosed in the following detailed description and the accompanying drawings.

[0005] **Figure 1** illustrates a secure execution environment for device assisted services in accordance with some embodiments.

[0006] **Figure 2** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0007] **Figure 3** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0008] **Figure 4** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0009] **Figure 5** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0010] **Figure 6** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0011] **Figure 7** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0012] **Figure 8** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0013] **Figure 9** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0014] **Figure 10** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

[0015] **Figure 11** illustrates another secure execution environment for device assisted services in accordance with some embodiments.

DETAILED DESCRIPTION

[0016] The invention can be implemented in numerous ways, including as a process; an apparatus; a system; a composition of matter; a computer program product embodied on a computer readable storage medium; and/or a processor, such as a processor configured to
5 execute instructions stored on and/or provided by a memory coupled to the processor. In this specification, these implementations, or any other form that the invention may take, may be referred to as techniques. In general, the order of the steps of disclosed processes may be altered within the scope of the invention. Unless stated otherwise, a component such as a processor or a memory described as being configured to perform a task may be implemented as a general
10 component that is temporarily configured to perform the task at a given time or a specific component that is manufactured to perform the task. As used herein, the term ‘processor’ refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.

[0017] A detailed description of one or more embodiments of the invention is provided
15 below along with accompanying figures that illustrate the principles of the invention. The invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The scope of the invention is limited only by the claims and the invention encompasses numerous alternatives, modifications and equivalents. Numerous specific details are set forth in the following description in order to provide a thorough understanding of the
20 invention. These details are provided for the purpose of example and the invention may be practiced according to the claims without some or all of these specific details. For the purpose of clarity, technical material that is known in the technical fields related to the invention has not been described in detail so that the invention is not unnecessarily obscured.

[0018] In some embodiments, security techniques for device assisted services are
25 provided. In some embodiments, secure service measurement and/or control execution partition are provided. In some embodiments, a secure execution environment for device assisted services is provided. In some embodiments, a secure stack is provided. In some embodiments, a secure memory is provided. In some embodiments, a secure modem is provided (e.g., providing a secure communication link between the modem/modem driver and a service processor and/or

agent on the device). In some embodiments, one or more secure monitoring points are provided. In some embodiments, one or more secure monitoring points with verification are provided (e.g., a secured monitoring point can be provided in the modem, which communicates securely to a secured execution environment in the CPU/processor, which can then verify such measures). In some embodiments, a secure bus is provided. In some embodiments, a secure execution environment in the CPU/processor is provided. In some embodiments, secure access to a secure execution environment(s) is provided (e.g., securing communication from a bottom of the stack, such as modem drivers, which require credentials to access the bus as controlled by a service processor or secure agent on the device, and in which the traffic on the bus is encrypted). In some embodiments, various secure execution environments are provided using various hardware partition techniques (e.g., secure memory, secure modems, secure memory partition(s) in the CPU/processor), as described herein.

[0019] In some embodiments, device assisted services (DAS) provide for one or more of device based service usage measurement, service usage policy implementation, service usage accounting, service usage control and any of the other functions described in various embodiments that assist, replace, and/or augment network based functions. For example, various DAS embodiments perform one or more of the following: facilitate and control activation to one or more access service networks; measure access and/or service usage on one or more access networks; control access and/or service usage on one or more access networks; account for different types of service usage on one or more access networks; implement quality of service (QOS) controls, collect and report QOS traffic demand, aggregate multiple device QOS demand reports to assess a measure of overall network QOS demand, and/or facilitate QOS resource allocation; and/or facilitate roaming between access networks. There are many more functions and embodiments for DAS as described with respect to various embodiments.

[0020] In some embodiments, various program elements that perform the functions to implement various DAS embodiments are referred to herein as DAS agents or device assisted service agents, or in some embodiments, more specific terms are used to be more descriptive in specific examples. In some embodiments, device assisted service agent functions include service measurements and/or service measure recording and/or service measure reporting (e.g., to the service controller, the device, the user or other device agents) and/or service measure

synchronization (e.g., between device and network). In some embodiments, device assisted service agent functions include service usage controls and/or service usage control policy settings. In some embodiments, service usage controls include one or more of network authorization, network authentication, network admission, access control, service usage activity classification, allowing or disallowing one or more service usage activity and traffic shaping for one or more service usage activity.

[0021] In some embodiments, device assisted service agent functions include one or more of the following: reporting service usage to QOS control elements in the network, receiving QOS assignment from the network, reporting QOS assignments to the network and/or communicating with QOS service reservation elements in the network. In some embodiments, device assisted service agent functions include one or more of implementing QOS service controls on the device based on one or more of the following criteria: fair queuing of service usage activities, differentiated QOS based on an assigned QOS hierarchy of service usage activities, service usage activity QOS assignments from the network for one or more service usage activities, service usage activity policy directives from the network for one or more service usage activities.

[0022] In some embodiments, a service control link is used for communication between the device assisted service agents and the service controller. In some embodiments, the service control link is a secure link (e.g., encrypted communication link).

[0023] In some embodiments, the device assisted service agent functions include device assisted service system communication, measuring and/or recording and/or reporting and/or synchronizing service measures, observing communicating information for service control integrity, communicating information for service control policy instructions and/or settings, or updating device assisted software and/or agent settings.

[0024] In some embodiments, device assisted service on the device includes the following: service measurements, service controls, user interface and usage reporting, user policy options, accept policy instructions, protected execution partition provided to prevent hacking, malware, errors, and other security techniques. In some embodiments, device assisted service on the server includes the following: set policy, set configurations, install/update agents,

check usage versus policy, check proper operation of agents, synch usage from network to device, and other verification techniques. For example, when errors in policy enforcement are detected, servers can perform actions to either further observe, quarantine, or suspend the device.

[0025] In some embodiments, a control server/control service network element receives service measures from the device. In some embodiments, the control server/control service network element receives service measures from the network. In some embodiments, the control server/control service network element sets policies and manages service across multiple networks (e.g., while one modem is shown in various figures, multiple modems can be employed for multiple networks with consistent service usage measures, service controls, QOS controls, UI, user preferences, user usage reporting, and other settings/controls across different networks).

[0026] In some embodiments, traffic type refers to one or more of best effort network traffic, real-time traffic (e.g., live voice, live video, etc.), streaming traffic, multi-cast traffic, uni-cast traffic, point to point traffic, file types, traffic associated with an application, real time traffic, traffic with an assigned priority, traffic without an assigned priority, traffic for a certain network.

[0027] In some embodiments, service usage activity refers to a usage of service by a device. In some embodiments, service usage activity can be one or more of connection to an access network, connection to certain destinations, URLs or addresses on a network, connection to the network by one or more applications, transmission of certain types of traffic , a type of transaction based service, a type of advertising based services or a combination of one or more of an application type, a network destination/address/URL, a traffic type, or a transaction type.

[0028] In some embodiments, protection of the device assisted service agents to protect the programs that perform the device assisted agent functions is provided with a protected execution partition on the CPU, APU or another hardware based processor. For example, such hardware protected execution capabilities in the CPU, APU or other processor can be combined in some embodiments with either OS software functions or other native mode software functions to create secure program execution partitions as described herein. In some embodiments, the term host is used to refer to the hardware and firmware and/or software system that executes the

device applications and networking stack. In some embodiments, some of the device assisted service agents are implemented in a modem execution partition.

[0029] **Figure 1** illustrates a secure execution environment (e.g., for a communications device) for device assisted services in accordance with some embodiments. The device execution environments include program elements for a communications device that utilizes the modem subsystems #1 through #N to connect to one or more of the access networks #1 through #N. In some embodiments, a communications device includes multiple program execution partitions. As shown, three execution partitions are provided: an application execution partition where application programs execute, kernel execution partition where the lower level drivers and basic low level OS programs execute, protected device assisted service execution partition (also referred to as protected DAS partition) where in some embodiments some or all of the device assisted service agents and/or functions execute, and modem execution partition where the modem program elements execute and in some embodiments some of the device assisted service agents and/or functions execute. Each of these execution partitions are optimized for different software functions, each providing programs with the basic physical memory, data memory, CPU or APU or modem processor execution resources, high level and/or low level OS, memory management, file storage, I/O device resources (e.g., UI, peripherals, etc.), network communications stack, other device resources, etc. that are required for operation of the programs. The collection of these hardware and software resources for the CPU or APU are sometimes referred to herein with the term host. As shown, Figure 1 illustrates an application execution partition and a kernel execution partition, which are shown as separate partitions within the device execution environments. For example, this separation is based on the manner in which “kernel programs” (e.g., drivers and network stack, etc.) are commonly supported as compared to “application programs” (e.g., browsers, word processors, user interfaces, etc.) within the context of several different popular operating systems (OS) (e.g., Windows, UNIX, Linux, MAC OS, certain mobile device OS, certain embedded device OS, etc.). In some embodiments, this functional separation is not required, and, in some embodiments, other functional separations are supported.

[0030] As shown in Figure 1, protected device assisted service agents such as the protected DAS partition device assisted service agents execute in the protected DAS partition

while unprotected device assisted service agents and/or OS networking stack elements and applications execute outside of the secure device assisted service execution partition, such as the application partition device assisted service agents and the OS networking stack and/or kernel partition device assisted service agents. For example, the protected DAS partition can make it more difficult for a hacker, malware or system errors to compromise, attack or modify the device assisted service measurements, service policy implementation or service usage control operations on the device. In some embodiments, the protected DAS partition need not support open access to all programs and OS elements so it can be easier to protect.

[0031] In some embodiments, the protected DAS partition is a protected execution partition on the main device that is supported by certain configurations in the host (or possibly a separate hardware security function). For example, this protected execution partition can be used to provide added service measurement integrity and/or service control integrity for a device assisted service enabled device. In some embodiments, as discussed herein, the OS also performs a role in establishing the protected execution partition for secure operation of device assisted services, and, in some embodiments, this role is performed by native software or firmware operating on secure hardware elements.

[0032] In some embodiments, the DAS agents responsible for maintaining service control integrity execute in the protected DAS partition. For example, the protected DAS partition device assisted service agents can include one or more of the following: one or more service usage measurement functions; some or all of the device networking stack functions that are monitored and/or controlled by the device assisted services system; device drivers that interface to an OS networking stack to observe or manipulate stack traffic; access control integrity functions; service policy control functions; service UI functions; application identification functions and/or functions to classify service usage activities by combinations of application, address/URL and/or traffic type; modem bus driver functions; and/or modem data encryption functions to prevent other unauthorized programs from bypassing the device assisted service measurements and/or controls by directly accessing the modem around the stack. In some embodiments, the system designer or a given set of design criteria determine which of the various described device assisted agent functions should be executed in protected DAS partition to strengthen the service control integrity for the system.

[0033] In some embodiments, the device operating system provides for the protected DAS partition in addition to conventional security features available in the operating system. In some embodiments, the protected DAS partition provides an execution partition with increased program execution protection in which service measurement and/or service control programs (agents) can execute in a mode that provides for higher access control integrity (proper service usage reporting and/or service measurement and/or service control system operation with increased protection from attacks, errors, malware, etc.). In some embodiments, a hardware assisted secure execution partition provides for increased program execution protection for device assisted service agent functions.

[0034] In some embodiments, a service control link is used for communication between the device assisted service agents and the service controller. In some embodiments, the service control link is a secure link (e.g., an encrypted communications link). As discussed at length elsewhere, in some embodiments an encrypted secure control link can be implemented over the higher layers of the network stack (e.g., TCP, HTTP, TLS, etc.), and, in some embodiments, the encrypted link can be implemented over lower layers in the network stack such as the IP layer or the access network layers (e.g., the WWAN device management channels or signaling layers). In some embodiments, service control link security is provided at least in part by encrypting link traffic between the device and the service controller. In some embodiments, service control link security is provided at least in part by running the service control link device side program agents in the protected DAS partition. In some embodiments, service control link security is achieved at least in part by restricting access to the service control link to certain device assisted service agents that are allowed to communicate with the service controller. In some embodiments, the agents that are allowed to communicate with the service control link do so with encrypted communications. In some embodiments, the encrypted communications is accomplished with a secure inter-agent communication bus on the device. In some embodiments, the only mechanism for modifying the configuration of the operation, execution code, execution instructions and/or settings of certain device assisted service processor agents executing in the protected DAS partition is through the service control link. In some embodiments, the only mechanism for modifying any program elements executing inside the protected DAS partition is through the service control link so that only the service controller may modify the operation or service policy

settings for the agents located in the service measurement and/or service control execution partition.

[0035] As shown, various server functions within the service controller are provided. In some embodiments, the service history server collects service usage measures from one or more of the device DAS agents and/or from various sources of potential network based service usage data bases such as the access network service usage (e.g., carrier CDR system), private network service usage (e.g., MVNO or enterprise network service usage accounting system) or billing, mediation service usage log, reconciliation (e.g., service provider billing or mediation system). In some embodiments, an access control integrity server is used to compare various access control verification checks to ensure that the device assisted service agents have not been compromised. The various embodiments used in the access control integrity server to perform these integrity checks are discussed at length elsewhere. Some embodiments include comparing device based service usage measures versus the service usage that should result if the desired service policy were properly implemented, comparing device based service usage measures versus the service usage that should result if the desired service policy were properly implemented with device based service usage measures that are executing in the protected DAS partition and/or the modem execution partition, comparing network based service usage measures versus the service usage that should result if the desired service policy were properly implemented, and comparing network based service usage measures with device based service usage measures. Additional access control integrity server embodiments are discussed at length elsewhere. In some embodiments, the policy control server stores the policy settings for the various service plans that can be implemented on the device, and communicates the appropriate policy settings to the appropriate device DAS agents. Various policy control server embodiments are discussed at length elsewhere.

[0036] In some embodiments, the service controller has secure access to service measures, service control settings, software images, software security state etc., for example, by virtue of the hardware enhanced execution partition and the secure channel into the protected DAS partition. For example, the secure channel can be encrypted employing keys that are public/private or point to point private. Other link security also can be implemented as discussed elsewhere. Servers can ensure that the link remains authenticated and information is validated.

For example, the service controller can perform one or more of the following verification techniques: compare the monitored service usage versus the policy, compare the monitored service usage versus other service usage measures and/or combined with various other network service measures. Additional service controller functions and embodiments are discussed at
5 length elsewhere.

[0037] In some embodiments, the protected device assisted service execution partition includes a host service control link as shown in Figure 1 that works in combination with a network service control link to send and receive secure messages between the service controller and the host. In some embodiments, the protected DAS partition only accepts new program
10 images from the service controller and not from local programs or disks. In some embodiments, the protected DAS partition cannot communicate with other application and/or kernel programs. In some embodiments, the protected DAS partition can also communicate with other application and/or kernel programs but only to gather information or to set settings. In some embodiments, the protected DAS partition can also communicate with other application and/or kernel programs
15 but only through a restricted encrypted communication bus that restricts outside program access to protected programs or agent functions, and can also restrict the agents inside of the protected partition from accepting unauthorized information or code modifications from programs outside the protected partition. Various other security techniques can be provided for the DAS execution environments as will be apparent to one of ordinary skill in the art in view of the embodiments
20 described herein.

[0038] In some embodiments, the protected DAS partition is created by employing CPU or APU hardware security features in addition to or in alternative to other software security features that can be provided by the operating system and/or other software. In some embodiments, the host hardware security features are provided with the operating system secure
25 kernel operating modes. In some embodiments, the host hardware security features used for secure device assisted service execution partition operation are independent of the operating system kernel (e.g., implemented in secure program partitions in a separate secure program area not directly controlled by the OS and/or software that does not have access to the partitions).

[0039] In some embodiments, the hardware security features that support the protected DAS partition include preventing other elements on the device from writing and/or reading certain memory areas reserved for device assisted service agents and/or control link functions. In some embodiments, this memory protection function is accomplished by locating the memory in a secure hardware partition that cannot be accessed by unauthorized device program elements (e.g., a separate bank of isolated memory space within the host CPU). In some embodiments, this memory protection function includes encrypting traffic to and from memory so that only authorized device program elements possess the counterpart encryption capability to access the memory. In some embodiments, the mechanism to access device assisted service agent memory and/or certain data elements is restricted to authorized device assisted service agents and/or the service controller via the service control link so that unauthorized program elements on the device cannot alter the device assisted service agent code and/or operation.

[0040] In some embodiments, the hardware security features that support the protected DAS partition includes preventing unauthorized elements on the device from accessing the protected storage and/or file storage ("protected storage" - e.g., disk storage, non-volatile memory, embedded non-volatile memory such as NVRAM, flash or NVROM, securely embedded non-volatile memory, etc.) that is used to store the device assisted service agent programs. In some embodiments, this protected file storage is maintained within the secure hardware partitions that also execute one or more of the device assisted service agents so that only authorized device assisted service agents have access to the storage locations. In some embodiments, the images that are stored in such protected file storage must be properly encrypted and signed for a boot loader to authorize loading the device assisted service agent programs into execution memory, and in some embodiments if the images are not properly signed then an access control integrity error is generated and/or the program is not loaded. In some embodiments, such properly signed DAS images can only be obtained from the service controller. In some embodiments, such DAS images can only be loaded into protected file storage by the service controller. In some embodiments, the hardware security features that prevent unauthorized elements on the device from accessing the protected file storage include encrypting all traffic to and from the secure storage so that only authorized device program elements possess the counterpart encryption capability to access the storage. In some embodiments, the means to re-program device assisted service agent program store is restricted

to the service controller via the service control link so that unauthorized program elements on the device may not alter the device assisted service agent code and/or operation.

[0041] In some embodiments, the hardware security features that protect device assisted service agent storage include a protected DAS partition in which an access control integrity agent function is isolated from other device program elements, and a secure service control link is also isolated in a similar manner, and the access control integrity agent scans the execution memory, data memory and/or file storage used by one or more device assisted services agents to measure and/or control services. In some embodiments, the purpose of the scan is to detect changes to the device assisted service agent code and/or data. In some embodiments, the purpose of the scan is to detect other unauthorized program elements or data that may be present in reserved or protected areas used for device assisted service agent execution. In some embodiments, reports of such scan audits are reported over the service control link to the service controller for further processing by use of cloud based resources to identify access control integrity violations. In some embodiments, the access control integrity agent functions include one or more of hashing other device assisted security agents, querying other device assisted security agents, observing the operation of other device assisted security agents or monitoring service measures and then either evaluating the results locally on the device to determine if they are within pre-defined allowable parameters or sending at least some of the results to the service controller for further analysis via the service control link. In some embodiments, the scan audits are compared with earlier versions of the scans to compare code configuration or operational characteristics. In some embodiments, the scan audits are compared against known data bases for the code or operational characteristics that should be present in the DAS agents.

[0042] In some embodiments, an access control integrity agent, or a new version of the access control integrity agent can be downloaded by the service controller over the secure service control link. This provides for a real time assessment of device service control security state as discussed above in the event that corruption of the secure device assisted service agents has occurred. In some embodiments, the access control integrity agent that is downloaded can have a different configuration and/or operation than any agent previously loaded onto the device so that it is difficult or impossible for a hacker or malware to spoof the operation of the agent in a short period of time. By requiring the agent to report security assessments back to the server in a

period of time that is typically less than what is required to spoof the agent, the agent will either report back an accurate assessment of device status or will be blocked by a hacker or malware, and both of these conditions provide the information required to take action if the device assisted services system has been compromised.

5 **[0043]** In some embodiments, the protected DAS partition and/or the modem execution partition can be used to securely store some or all of the device credentials that are used for one or more of device group association (as discussed at length elsewhere), activation (as discussed at length elsewhere), authorization to the access network and/or the DAS network (as discussed at length elsewhere), service level (as discussed elsewhere) , and service usage accounting and/or
10 billing (as discussed elsewhere).

[0044] In some embodiments, the modem subsystem also includes DAS elements that strengthen the access control integrity of the DAS system. As shown in Figure 1, one or more modems can include in some embodiments DAS agent functions labeled modem partition DAS agents .

15 **[0045]** Example embodiments for DAS agent functions that execute in the modem execution partition include modem encryption and modem service measures. In other embodiments discussed elsewhere, the modem execution partition can also include higher level DAS agent functions such as stack traffic classification, stack manipulation, access control and/or traffic control. As also discussed elsewhere, the modem execution partition, for example,
20 can also include a full service processor (discussed elsewhere) that is fully capable of managing all aspects of service usage measurement and/or service control. It should now be apparent to one of ordinary skill in the art that the modem execution partition can employ a number of the service security embodiments described in the context of the protected DAS partition, for example, to enhance the service integrity of the DAS system. For example, the DAS agents on
25 the modem can be stored in an encrypted and signed format on NV memory on the modem that is only accessible by the network service control link or by a local secure control link from the protected DAS partition to the modem execution partition, etc. As shown in Figure 1, a separate secure modem control channel that is distinct from the host secure control channel is provided. This separate modem control channel can either be implemented over the higher network layers

of the device or over the lower access network layer so that special access to access network resources is required to even connect to the modem DAS agents thus further enhancing security.

5 [0046] In some embodiments, the protected DAS partition provides for performing the DAS agent functions required for parental controls, enterprise WWAN management controls or roaming controls and/or usage reporting in the protected execution space. With the DAS embodiments described herein and elsewhere it will now be apparent to one of ordinary skill in the art how to implement such protected controls for these application scenarios.

10 [0047] In some embodiments, a protected DAS partition provides for performing a virtual machine on top of a secure machine. The device application OS that is accessible by software that can be installed without special permissions can be isolated from the secure hardware and/or OS that is running under the VM. Using these techniques, malware can be “cocooned in” on the VM OS rather than “walled out” as discussed with respect to other embodiments described herein.

15 [0048] In some embodiments, communication between program elements outside of the protected DAS partition to DAS agents inside the protected DAS partition is controlled by a secure encrypted channel. In some embodiments, only programs that have access to communicate with DAS agents are allowed to do so, and, in some embodiments, even these outside programs are not allowed to modify the DAS agent configuration, only to report information and/or receive information.

20 [0049] As discussed elsewhere, various embodiments can be used to connect to multiple access networks through multiple modems, with each modem potentially being associated with a different set of DAS service policies corresponding to the different types of access networks supported. In embodiments such as 3G/4G modems, WWAN/WLAN modems, and various other multiple modem embodiments, the multiple modems can also be provided on the same multi-mode modem subsystem rather than on different modem subsystems.

25

[0050] In some embodiments, the various techniques and embodiments described herein can be readily applied to intermediate networking devices discussed elsewhere. In some embodiments, intermediate networking devices include but are not limited to WWAN/WLAN

bridges, routers and gateways, cell phones with WWAN/WLAN or WWAN/Bluetooth, WWAN/LAN or WWAN/WPAN capabilities, femto cells, back up cards for wired access routers, etc.

[0051] **Figure 2** illustrates another secure execution environment for device assisted

5 services in accordance with some embodiments. In particular, Figure 2 illustrates an embodiment in which DAS agents do not actually replace the OS network stack elements, but instead one or more DAS agents are comprised of device driver programs that interface into the network stack and pass traffic information or actual traffic back and forth with the stack. These device driver interface constructs are labeled OS driver framework and interface as shown in
10 Figure 2. Example OS system constructs that provide for this type of architecture for DAS agents include Windows NDIS and/or TDI drivers, Windows Filter Platform, Berkeley Packet Filter, ipfw (Unix, Linux, MAC OS), etc. While these OS stack options are not secure in themselves, if the drivers that interface them are secured as illustrated in Figure 2 by executing them in the protected DAS partition, then higher overall access control integrity levels can be
15 achieved. As shown in Figure 2, the service measurement and/or policy control drivers represent the DAS drivers that interface to the OS stack device driver interface constructs labeled OS driver framework and interface. In some embodiments, service access control integrity is further enhanced by placing additional measurement points outside of the network stack, so that, for example, if the network stack service usage reporting is hacked or compromised, there is a
20 secure back up service measure located on the device and/or in the network (e.g., as shown with the modem agent labeled service measure in Figure 2). For example, the service measure, encryption, and/or modem bus functions shown in Figure 2 can be executed in a protected partition.

[0052] **Figure 3** illustrates another secure execution environment for device assisted

25 services in accordance with some embodiments. As shown, some stack elements are executed in the kernel execution partition and some stack elements are executed in the protected DAS execution partition. In some embodiments, the DAS agents are directly monitoring and/or controlling stack traffic by intercepting it and imposing additional traffic measurement and/or filtering. Some examples of such techniques are discussed at length elsewhere. As shown, the
30 network stack elements are the OS stack elements that reside in the kernel execution partition

and the protected DAS network stack elements are the stack elements that reside in protected DAS execution partition. Since some or potentially all of the stack network traffic processing resides in protected DAS execution, a high level of service control integrity may be obtained. For example, the modem bus driver can be executed in the protected DAS execution partition so that unauthorized programs may be blocked from accessing the access network through the modem.

[0053] In some embodiments, the entire stack is executed in the protected DAS execution partition with only a stack API executing in kernel execution partition. Other embodiments involve implementing the bare minimum in the protected DAS execution partition required to secure a service measure that can be used to confirm the integrity of the service policy implementation (as illustrated with respect to other embodiments). As will now be apparent to one of ordinary skill in the art, various combinations of stack processing functions can be implemented in a secure host execution partition to strengthen the service measurement and/or service control integrity of the DAS system.

[0054] In some embodiments, the stack elements implemented in the protected DAS execution partition can include stack API, sockets layer, TCP, UDP, service measurements at one or more points in the stack, IP layer processing, VPN/IPSEC, PPP, access control, traffic classification, traffic queuing, traffic routing, traffic QOS, traffic demand reporting to QOS allocation servers, traffic statistics reporting to the QOS servers, traffic QOS reservation requests including by traffic type or app type or service priority to the servers, traffic throttling, traffic statistics gathering, traffic QOS priority identification, modem drivers, modem data encryption, etc.

[0055] In some embodiments, the above mentioned service control mechanisms are controlled by policy commands received over the service control link from the servers. In some embodiments, the device also reports usage measures to servers. In some embodiments, the device also reports QOS demand to the servers and/or accepts QOS instructions from the servers. In some embodiments, the device reports traffic statistics, projected traffic demand, application usage, projected QOS demand may all be reported to the servers for the purpose of provisioning the right amount of data bandwidth and traffic priority to the device, and the servers aggregate

such reports from many different devices to project needed allocations across the entire network and make global bearer channel level or base station level decisions bearer channel allocation and bearer channel QOS allocation decisions, which may also be tied into a bearer channel provisioning, or bearer channel QOS provisioning apparatus located in the access network.

5 **[0056]** As illustrated and discussed elsewhere, additional security measures can be added in some embodiments to augment the secure service partitioning, including, for example, access control integrity checks. As also illustrated and discussed elsewhere, in addition to the service control policy instructions that can be received from the servers, an intermediate policy control agent may be present to make additional higher level decisions on how instantaneous policy
10 should be implemented.

[0057] As shown in Figure 3, the modem control link provides a link from local connection to the host service control link, which in turn connects through the host secure channel to the service controller. This configuration can also be encrypted and, in some embodiments, is an alternative to the direct connection from the modem service control link to
15 the network service control link as shown in the previous figures.

[0058] As shown in Figure 3, the final stack elements that feed a modem bus driver is located in the protected DAS execution partition (illustrated as a solid line in Figure 3), or, in some embodiments, can be located in the kernel execution partition (illustrated as a dashed line in Figure 3). The final stack elements feed the modem subsystem. In some embodiments, the
20 modem subsystem includes an encrypted link so that the stack elements in the protected DAS execution partition can communicate with the modem but other SW programs or HW cannot, for example, thereby preventing the service measures and/or controls from being inappropriately bypassed. The modem subsystem, for example, can include its own the protected execution partition. The modem protected execution partition, for example, can also include a service
25 measure to increase service control integrity verification as depicted by service measure. The modem service measure can be included in protected execution partition that can only be accessed by the service controller by way of the modem local channel, or the modem service measure can only be accessed by another DAS agent in protected execution partition. In some embodiments, the modem local channel is implemented as a secure channel (e.g., an encrypted

communication channel between the modem service control link and the host service control link). As discussed herein, the modem driver can reside in protected service execution environment, or the modem traffic can be encrypted within service execution environment. For example, the encryption settings can be controlled by various secure control servers.

5 **[0059]** **Figure 4** illustrates another secure execution environment for device assisted services in accordance with some embodiments. In particular, Figure 4 illustrates a direct stack manipulation option performed by the DAS agents in the protected execution partition. The policy implementation agent (discussed at length elsewhere) performs access control and/or traffic shaping according a set of service control policies. The service control policies, for
10 example, can be set by the service controller or by the service controller in coordination with the policy control agent (also discussed at length elsewhere). There is also a protected service measure agent, a modem encryption agent, a modem driver agent, an application identifier agent, an access control integrity agent and a policy control agent all implemented in protected DAS partition, but it will now be apparent to one of ordinary skill in the art that a subset of these
15 functions can be implemented in protected execution partition in various circumstances. Figure 4 also again shows various embodiments that are available for network based service usage measures and interfacing to the mediation and billing systems, and it should be understood that any or all of the embodiments and figures can be employed in the context of carrier networks, MVNOs, private networks, or open networks supporting enterprise IT manger controls, parental
20 controls, multi-network controls or roaming controls.

[0060] **Figure 5** illustrates another secure execution environment for device assisted services in accordance with some embodiments. In particular, Figure 5 illustrates a modem service control link that is connected directly to the service controller via the network service control link (e.g., via a modem secure channel). In some embodiments, a modem control link for
25 DAS is established locally on the device or through an entirely different control channel, which, in some embodiments, provides enhanced security as discussed herein (e.g., it is very difficult to hack a service usage measure or service control that cannot be accessed on the device).

[0061] **Figure 6** illustrates another secure execution environment for device assisted services in accordance with some embodiments. In particular, Figure 6 illustrates a policy

implementation agent that includes the entire networking stack running in protected execution partition and a stack API with an application identifying function in the kernel execution space.

[0062] **Figure 7** illustrates another secure execution environment for device assisted services in accordance with some embodiments. In particular, Figure 7 illustrates DAS agents that do not replace the OS network stack elements, but instead one or more DAS agents are comprised of device driver programs that interface into the network stack and pass traffic information or actual traffic back and forth with the stack. These device driver interface constructs are labeled OS driver framework and interface in Figure 7 as with Figure 2. The main difference between the embodiment in Figure 7 and that in Figure 2 is that a service measure agent, a modem encryption agent, and a modem driver agent are included in the protected DAS partition. For example, this provides for enhanced service control security as discussed elsewhere.

[0063] **Figure 8** illustrates another secure execution environment for device assisted services in accordance with some embodiments. In particular, Figure 8 illustrates a more simplified embodiment that is similar to that of Figure 7. In Figure 8, only an access control integrity agent and a service measure are executed in protected DAS partition. This example embodiment illustrates that provided that at least one protected service measure is provided on the device, then the DAS service control integrity can be very high. For example, if it is not possible to access the program code or control traffic for the service measure agent and the host service control link except through the encrypted control channel from the service controller, then this simplified configuration can be almost as secure as that possible with network based service measures. It will now be apparent to one of ordinary skill in the art that this technique similarly applies to a service measure and control link similarly implemented in a protected modem execution partition. In some embodiments, the access control integrity agent provides additional security, for example, in the event that the protected DAS partition is breached.

[0064] **Figure 9** illustrates another secure execution environment for device assisted services in accordance with some embodiments. In particular, Figure 9 illustrates an embodiment similar to that of Figure 8 except in addition to the service measure being executed in protected DAS partition, a modem encryption agent is also implemented in a protected

partition. For example, this prevents unauthorized software from defeating the service measurements and/or service controls by going around the network stack directly to the modem.

[0065] **Figure 10** illustrates another secure execution environment for device assisted services in accordance with some embodiments. In particular, Figure 10 illustrates an embodiment similar to that of Figure 9 except that there are additional app partition DAS agents executing in application execution partition. For example, this illustrates that some DAS agents can be implemented in application space (e.g., UI agent, policy control agent, etc.) while still maintaining a high level of service measurement and/or control security as long as there are a few key measures and/or controls implemented in protected execution partitions.

[0066] **Figure 11** illustrates another secure execution environment for device assisted services in accordance with some embodiments. In particular, Figure 11 illustrates how the server cloud can be assisted by the on board access control integrity agent to detect tampering with other service measurement and/or control agents, or to protect the service measurement and/or control system from being attacked by malware. As shown, the access control integrity agent executes inside the protected DAS partition. The access control integrity agent performs the various access control integrity check functions described elsewhere, in some embodiments, in coordination with the servers over the secure control channel. In some embodiments, the access control integrity agent can send the service controller information about the other service measurement and/or control agents so that the service controller can determine if the agents are working properly or have been tampered with. Such information can include sections of code, hashes, code segments, code variations from a previous image, code variations from a historical image, responses to queries, checksums, observations of operating behavior or patterns, service usage, policy implementation behavior, etc. In some embodiments, the access control integrity agent can check the operating environment for signs of malware signatures, or may send application and/or driver information or other information about the operating environments to the servers for further processing to detect malware. In some embodiments, the access control integrity agent can perform the basic has operations on protected DAS partition memory, kernel execution partition memory areas, application execution partition memory areas, on disk storage areas or on other file storage areas to detect known malware hashes or signatures, etc., or the

access control integrity agent can send the hashes to the servers for comparison against malware databases.

[0067] In some embodiments, the DAS system is implemented in a manner that is robust to losses in service control link (e.g., coverage outages on a WWAN link or loss of connection on a wired link). In some embodiments, the DAS system to be implemented in a manner that is robust to one or more server elements in the service controller going offline or failing for any reason. The following embodiments facilitate these techniques, as described below.

[0068] In some embodiments, it is advantageous for one or more of the device assisted service agents to maintain a record of the service usage reports and/or other reporting that is provided to the service controller regarding device service control state (e.g., present service plan settings, current service usage policy settings, current user preference settings, current DAS settings, current encrypted control channel and/or local encrypted communication channel key information, current DAS agent status reports, current DAS agent security state reports, current ambient service usage and/or transaction records, current service control integrity threat reports, user status information, device status information, application status information, device location, device QOS state, etc). In addition to such information that exists on the device and is reported to the service controller, additional service information can be derived and recorded in the service controller, such as information received from outside the device and/or analysis of the device reported information (e.g., network based service usage measures, analysis of device service usage, comparison of device reports with other information, analysis of access control integrity agent reports as described elsewhere, information received from roaming networks, information input to the service controller from parental control terminals, enterprise control terminals, virtual service provider control terminals, access network authorization information, service integrity violation level, and many other types of information used to properly measure and/or control the device services). For example, the information reported from the device and received or derived outside the device that is required to adequately define the actions needed from the service controller to maintain proper DAS system operation is sometimes referred to herein as the “device service state”.

[0069] In some embodiments, the service controller functions can be designed so that they are highly scalable and can be executed on a number of hardware and software platforms (e.g., different virtual machines in a server, different servers in a data center, or different servers located in different data centers). In such embodiments the service controller can be designed so that the programs that execute the various service controller server functions can derive all of the information necessary to properly manage the device at any moment in time by knowing past device service state and current service state which adequately define the next set of actions the service controller needs to implement to properly maintain the DAS system operation. By designing the system in this way, if the server that is running the service controller server functions for any given device in question were to go down or become disconnected from the device, then another server could later resume proper operation of the DAS system by assigning another service controller server function to the device and recovering or restoring the necessary past device service state and the necessary current device service state.

[0070] For example, this can be accomplished in some embodiments as described below. The service controller saves the current device service state into a common data base (e.g., which may be centralized or distributed) that is available to all service controller server functions. The device service state is saved each time the device communicates with the service controller, or at regular time intervals, or a combination of both. The device retains its current and past service state reports even after they are reported at least until the service controller sends the device a message confirming that the service controller has saved a given device service state. Once the device receives this save confirmation for a given device state report then it is no longer required to retain that particular device state report once the device has no further use for it. In this manner, if a service controller server function goes down then a save confirmation for one or more reported device states is not transmitted to the device by the service controller, and the device may retain that report. A server load balancer detects that a given service controller server function has gone down, looks up the devices that were being controlled by that service controller server function, finds that the device in question was one of those devices and re-assigns a new service controller server function (either in the same data center or in another data center) to control the device in question. The newly assigned service controller server function then recovers all past device states that were recorded in the service controller data base and are required to properly manage the DAS system, and then asks the device to transmit or re-transmit

all device state reports that were not saved in the service controller data base. Once the device transmits or re-transmits the requested information, the newly assigned service controller function then has the information it needs to properly manage the DAS system, it saves all the reported device state information, and then sends save confirmations to the device so that the
5 device need no longer retain the older service state reports. The newly assigned service controller server function may then resume the DAS system operation with a set of actions that are identical or very similar to the actions that would have been taken by the original service controller server function if it had not gone down. One of ordinary skill in the art will now appreciate that the above techniques can also be used to accommodate temporary losses in the
10 connection between the device and the service controller. For example, such techniques provide for a highly scalable and robust means to implement a distributed service controller across multiple data centers for reliable service redundancy. In some embodiments, the past device service state information is saved in the protected DAS execution partition and/or the modem execution partition, for example, so that it is protected from corruption.

15 **[0071]** Although the foregoing embodiments have been described in some detail for purposes of clarity of understanding, the invention is not limited to the details provided. There are many alternative ways of implementing the invention. The disclosed embodiments are illustrative and not restrictive.

20

SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICE

ABSTRACT OF THE DISCLOSURE

[0072] Security techniques for device assisted services are provided. In some embodiments, secure service measurement and/or control execution partition is provided.

DEVICE EXECUTION ENVIRONMENTS

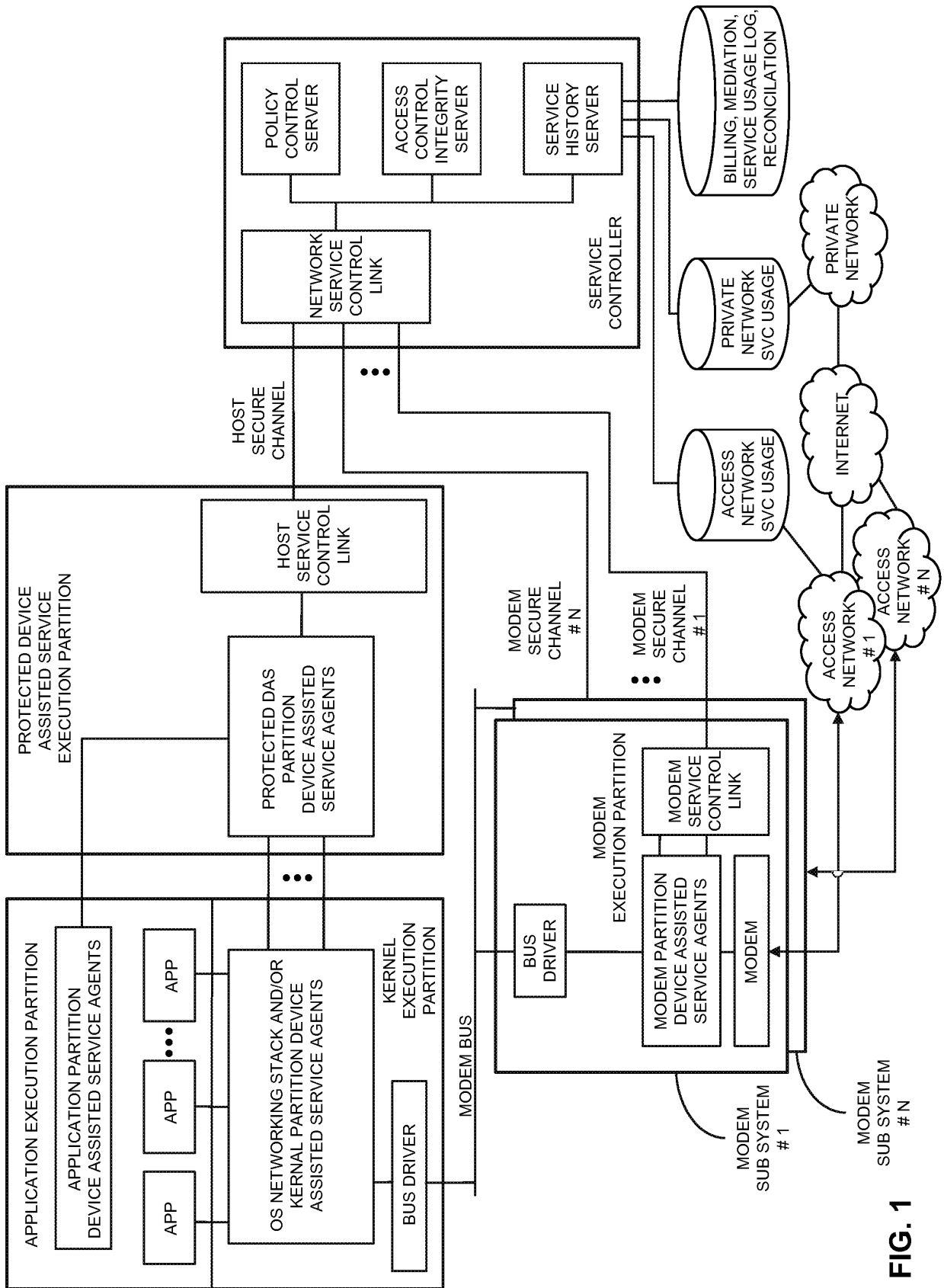


FIG. 1

DEVICE EXECUTION ENVIRONMENTS

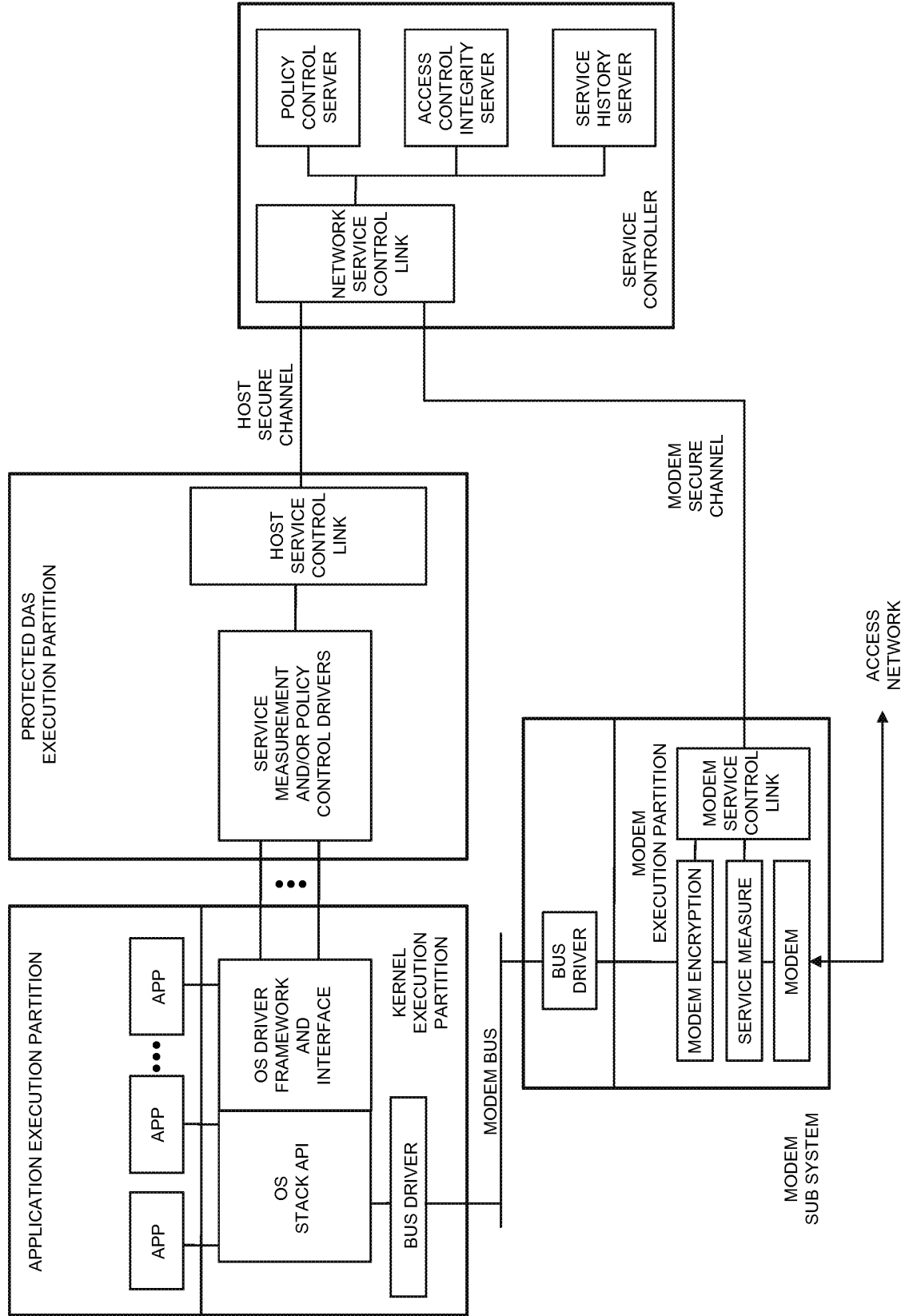


FIG. 2

DEVICE EXECUTION ENVIRONMENTS

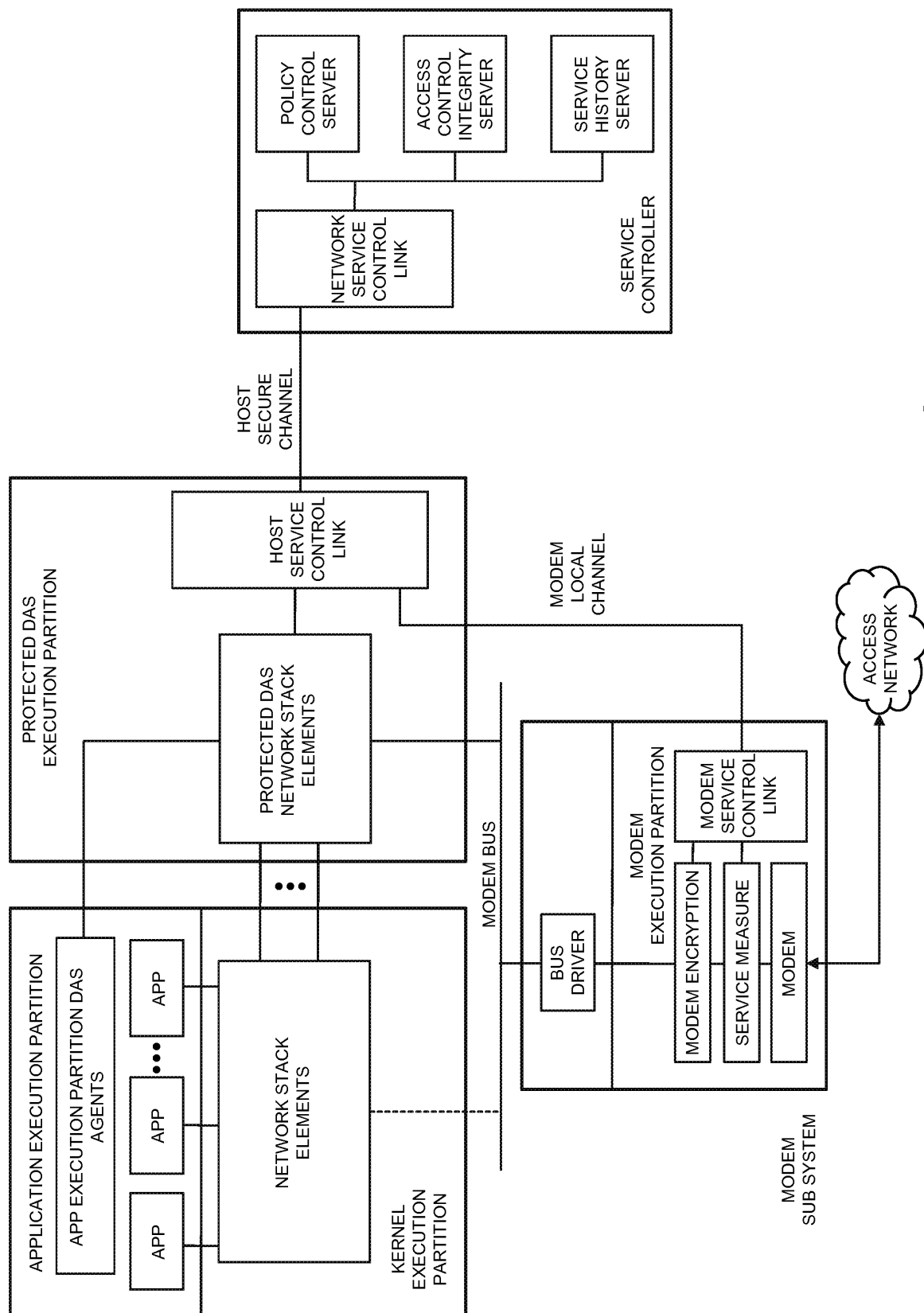


FIG. 3

DEVICE EXECUTION ENVIRONMENTS

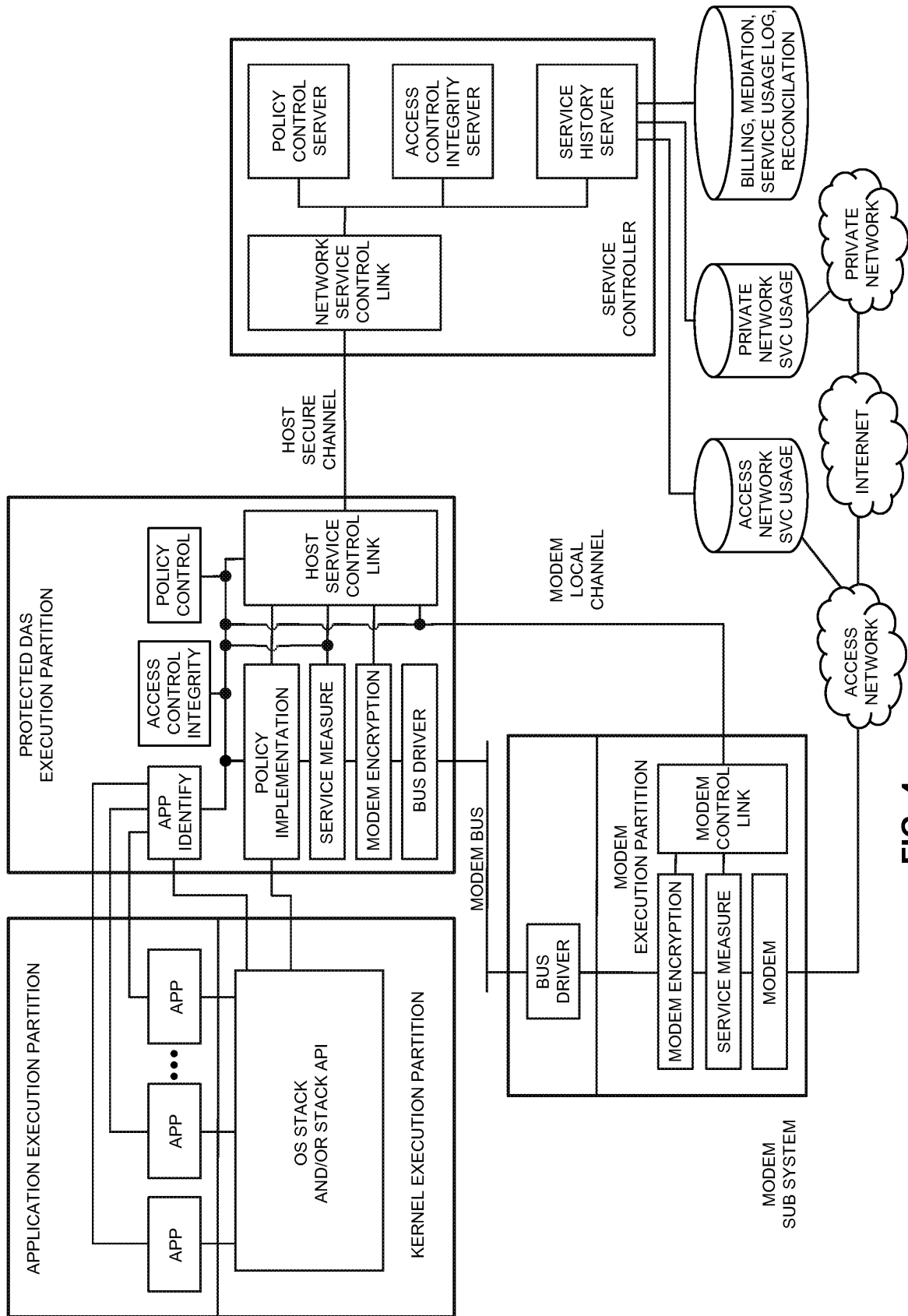


FIG. 4

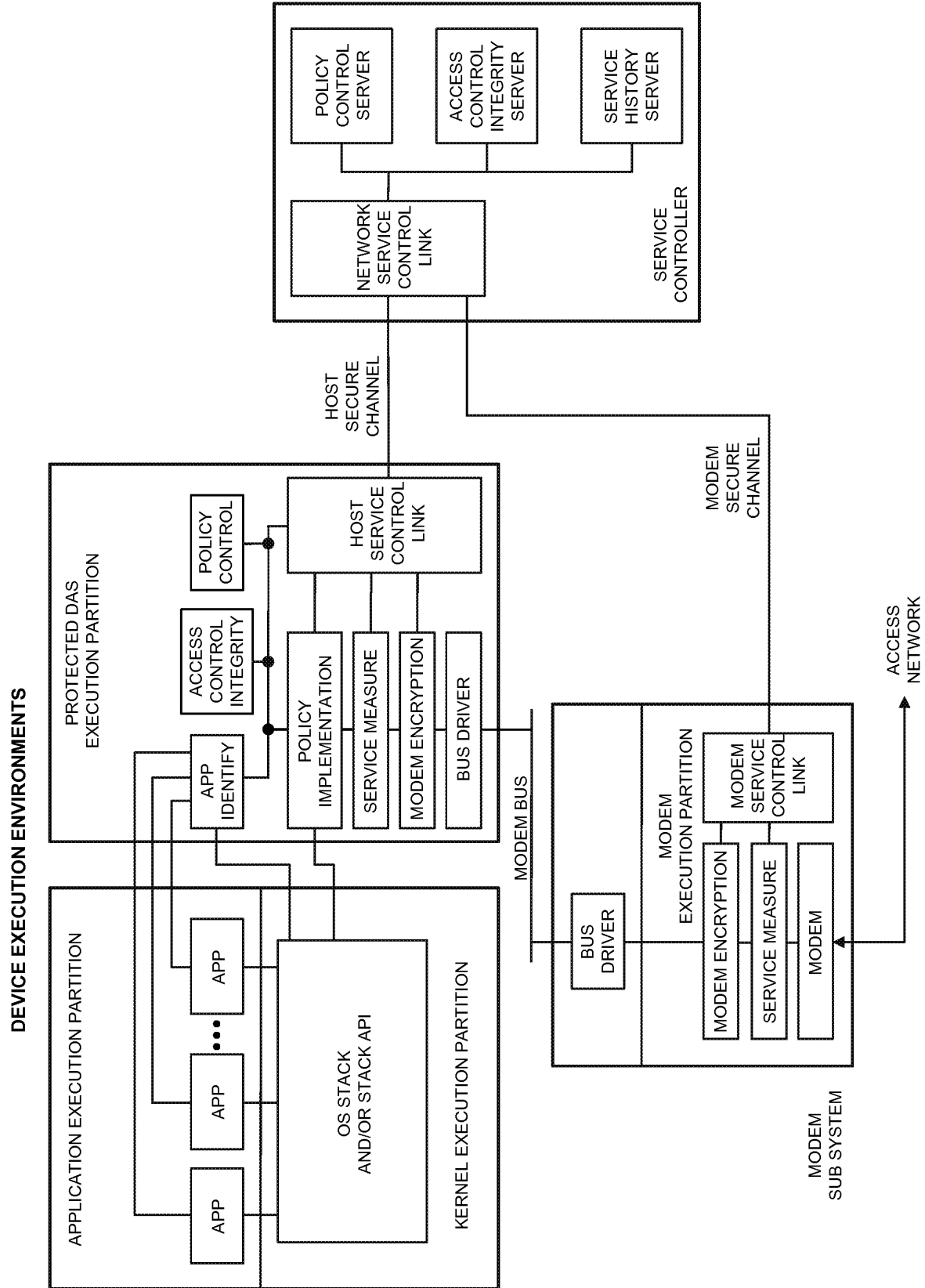
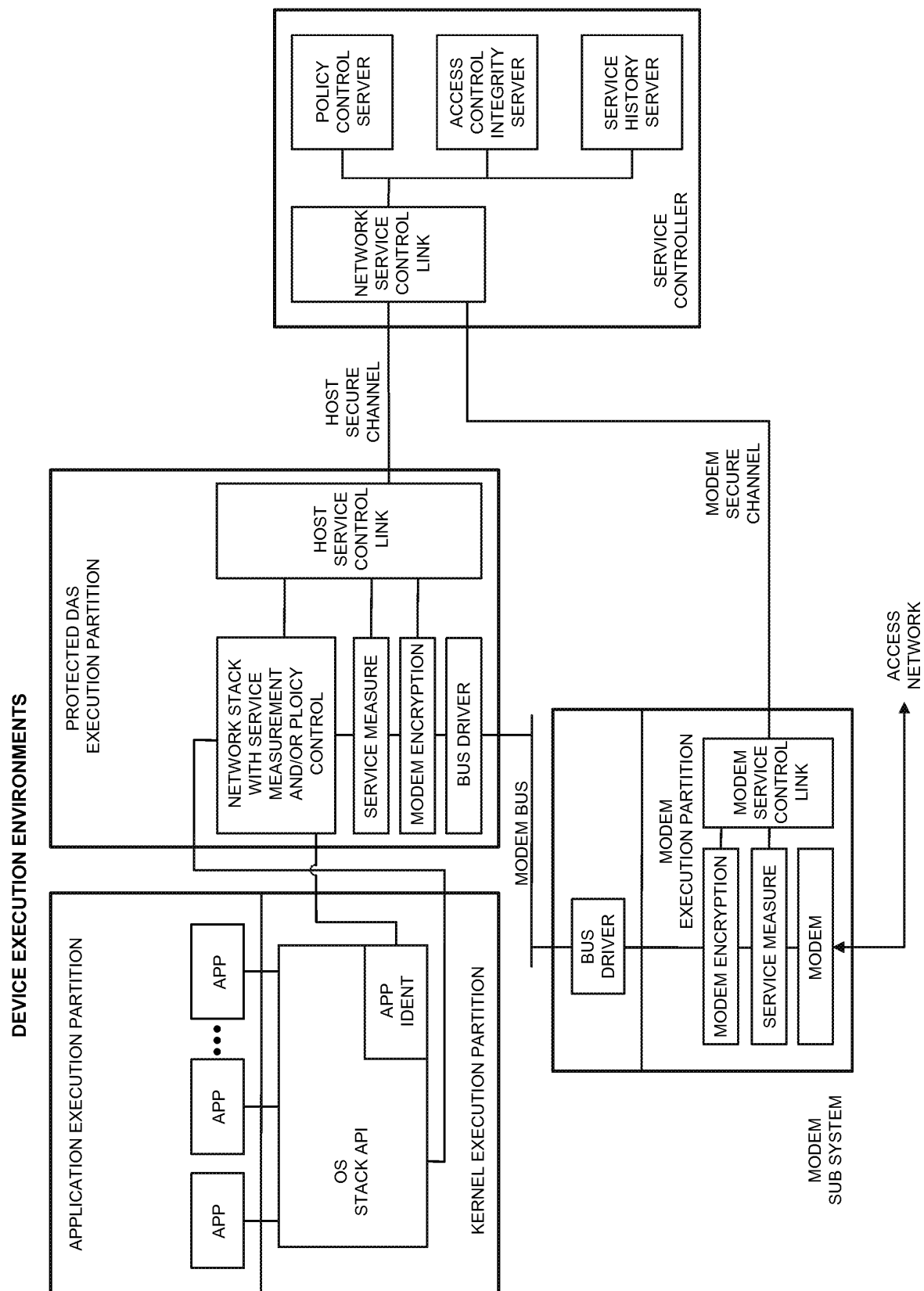


FIG. 5



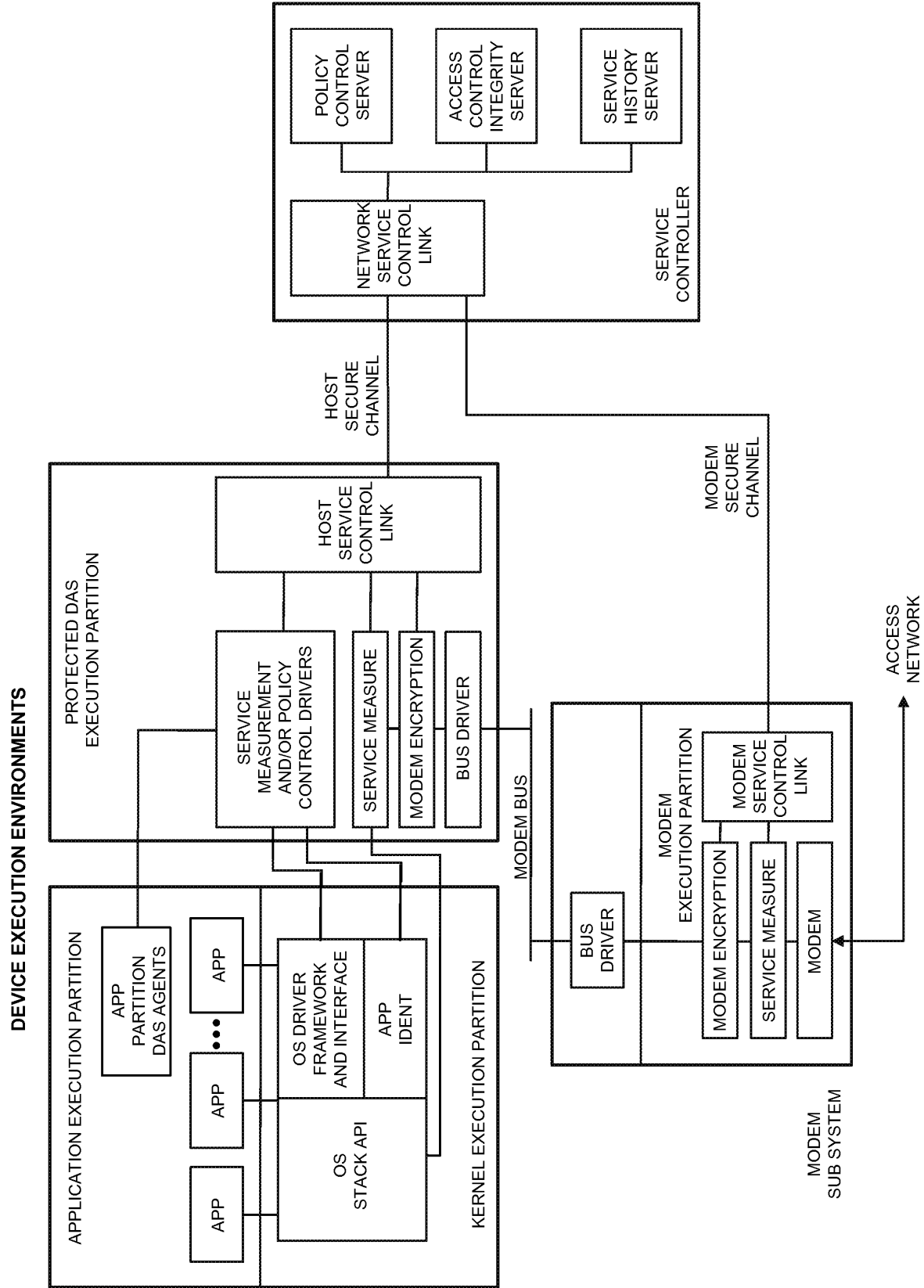


FIG. 7

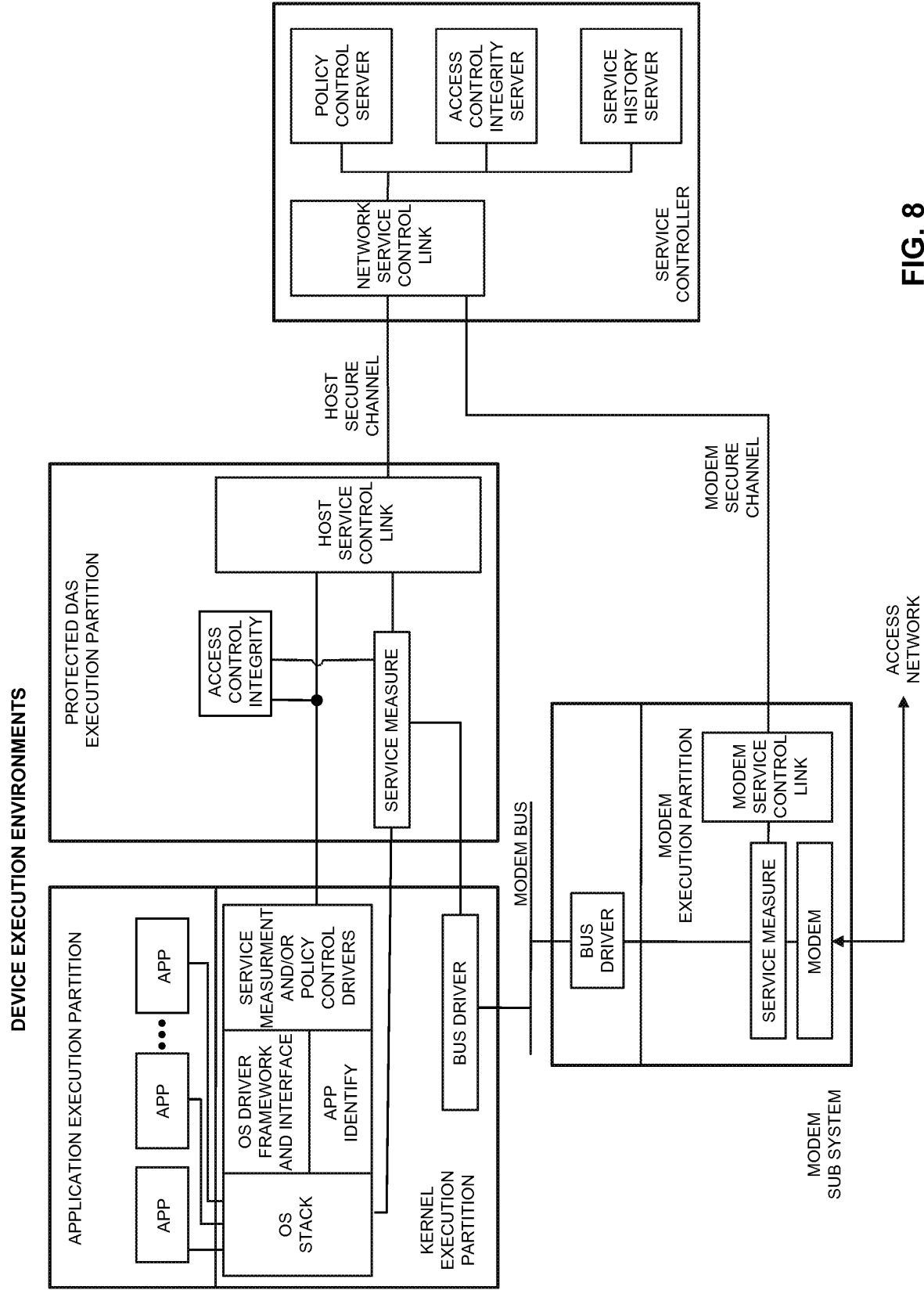


FIG. 8

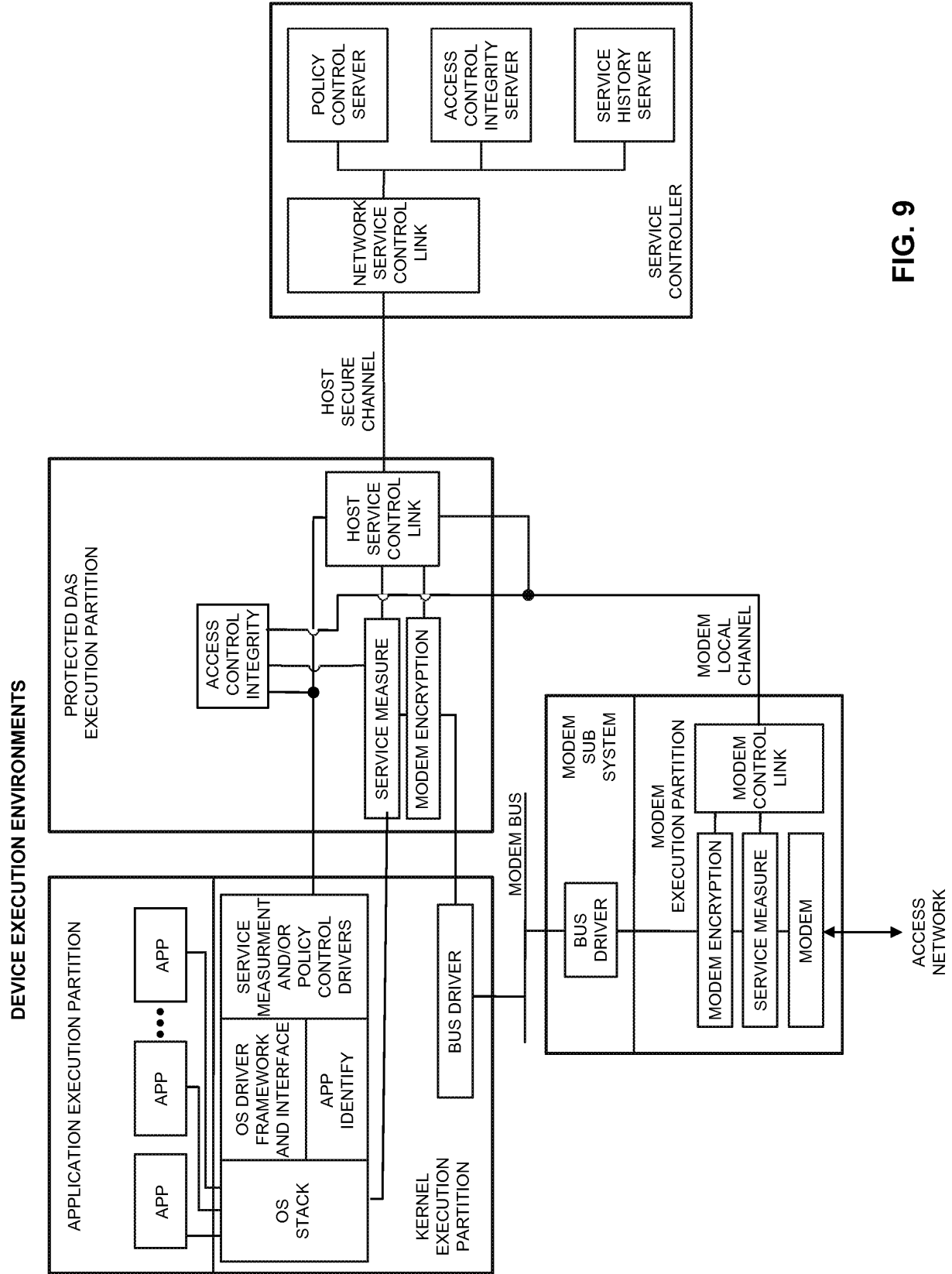


FIG. 9

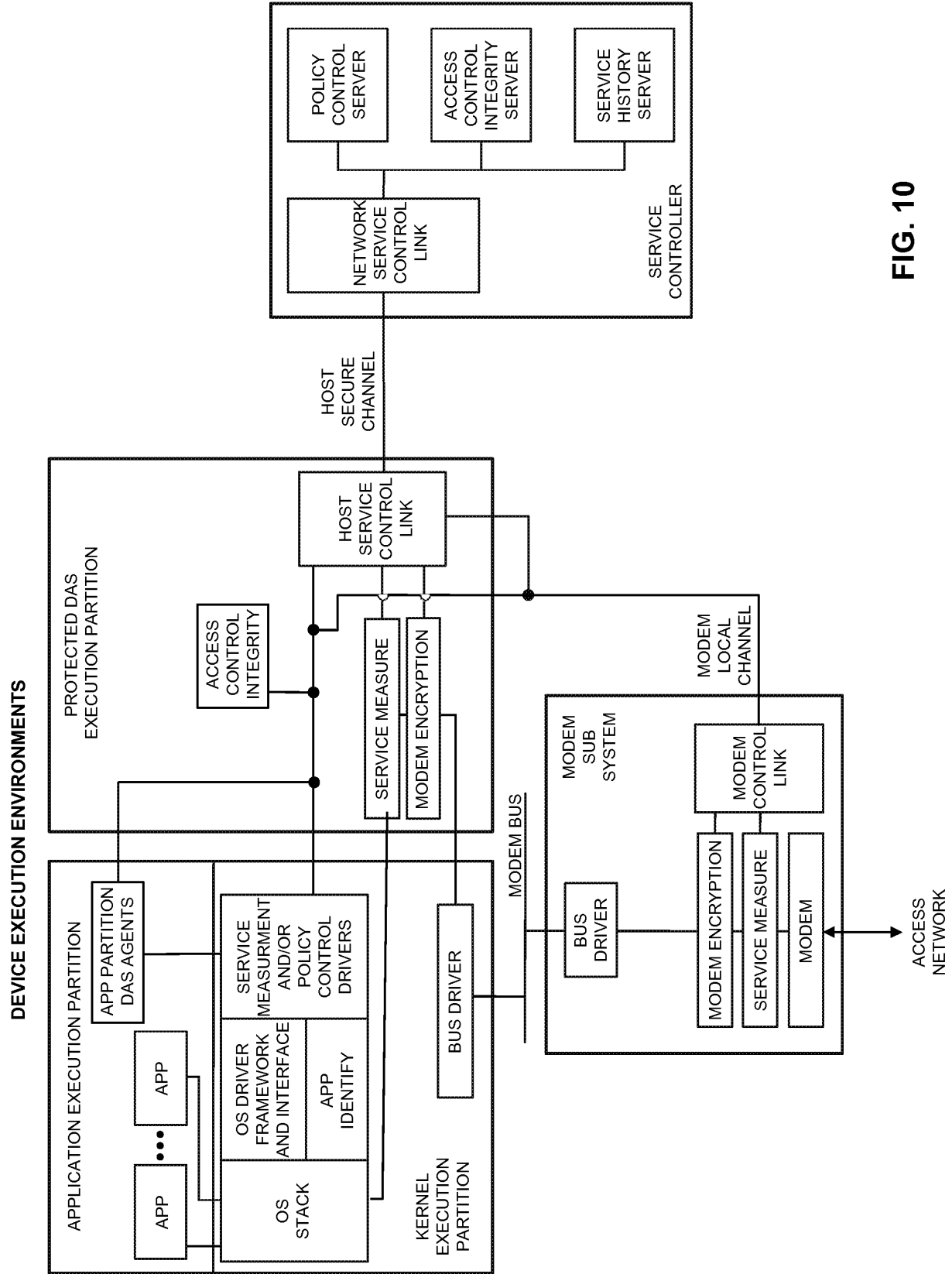


FIG. 10

DEVICE EXECUTION ENVIRONMENTS

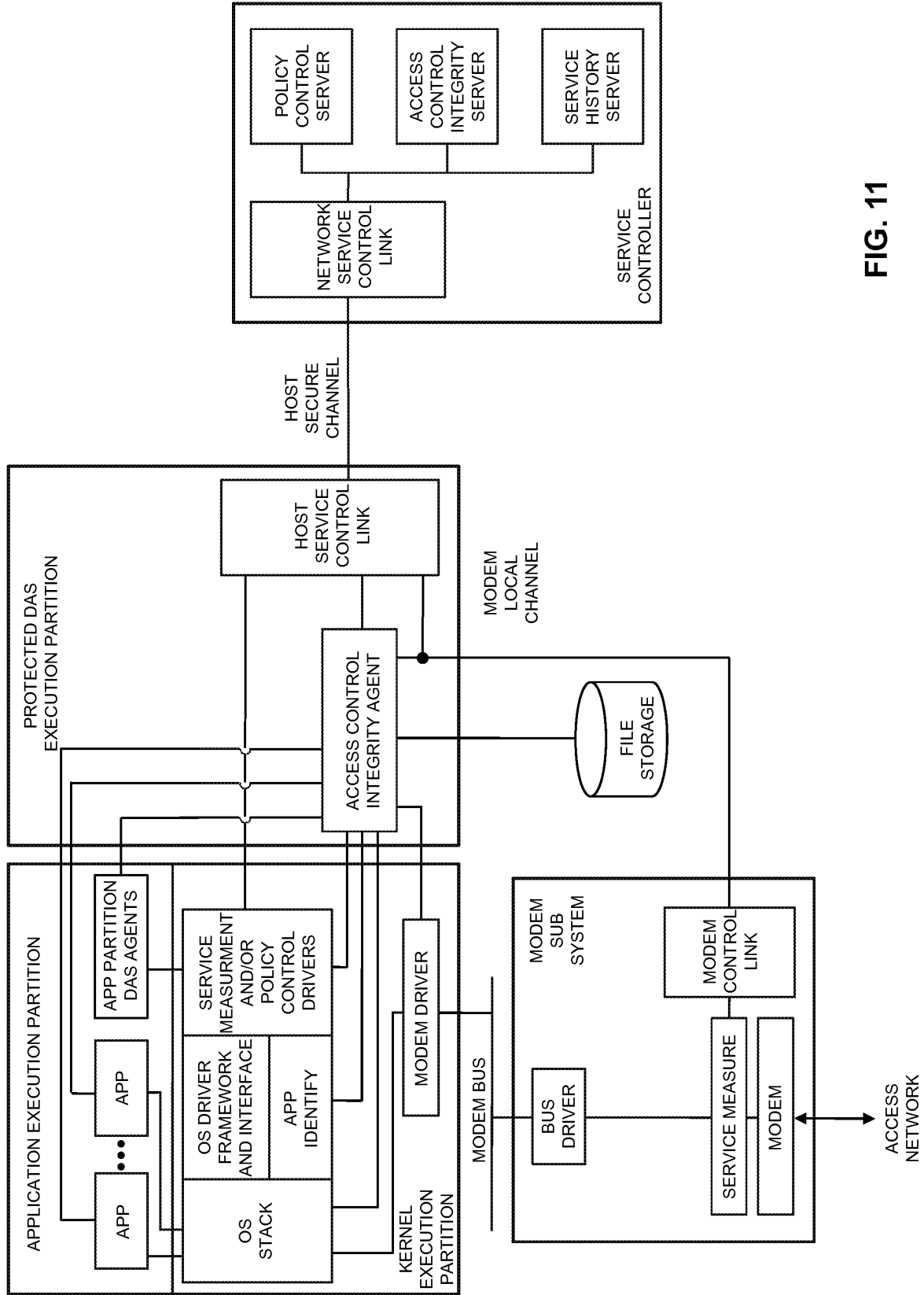


FIG. 11

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES		
First Named Inventor/Applicant Name:		Gregory G. Raleigh		
Filer:		Michael J. Schallop		
Attorney Docket Number:		RALEP025+		
Filed as Large Entity				
Provisional Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Provisional application filing	1005	1	220	220
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				220

Electronic Acknowledgement Receipt	
EFS ID:	6273465
Application Number:	61252151
International Application Number:	
Confirmation Number:	9965
Title of Invention:	SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	21912
Filer:	Michael J. Schallop
Filer Authorized By:	
Attorney Docket Number:	RALEP025+
Receipt Date:	15-OCT-2009
Filing Date:	
Time Stamp:	23:26:18
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$220
RAM confirmation Number	5717
Deposit Account	500685
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Provisional Cover Sheet (SB16)	RALEP025plus_Provisional_Coversheet.pdf	1000055	no	3
			4413619fc6263f9337f6d5cd4f8637cd1afab020		
Warnings:					
Information:					
2		RALEP025plus_APP.pdf	143153	yes	27
			b33b4aa7c8695bb6790a986ddf16e5ba0d5a5b1e		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	26	
	Abstract		27	27	
Warnings:					
Information:					
3	Drawings-only black and white line drawings	RALEP025plus_Figures.pdf	151481	no	11
			9a3e77696d35dba09a3bde4335fc988278ca36f4		
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29286	no	2
			c501720607e561dbbef8ba0a70e82bc09d93e9f1		
Warnings:					
Information:					
Total Files Size (in bytes):			1323975		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.