AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00467	12/6/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
Headwater Research LLC	Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,143,976	9/22/2015	Headwater Research LLC
2	9,277,433	3/1/2016	Headwater Research LLC
3	9,609,544	3/28/2017	Headwater Research LLC
4	10,237,773	3/19/2019	Headwater Research LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

GOOGLE EXHIBIT 1002

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00467	12/6/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
Headwater Research LLC	Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	9,143,976	9/22/2015	Headwater Research LLC
2	9,277,433	3/1/2016	Headwater Research LLC
3	9,609,544	3/28/2017	Headwater Research LLC
4	10,237,773	3/19/2019	Headwater Research LLC
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

Accordingly, all claims and causes of action asserted by Plaintiff against the Defendants in the above-captioned case are DISMISSED WITHOUT PREJUDICE

CLERK	(BY) DEPUTY CLERK	DATE
David A. O'Toole	ch	3/24/23

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

Trials@uspto.gov
571-272-7822

Paper 17
Dated: October 8, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
Petitioner,

v.

HEADWATER RESEARCH LLC,
Patent Owner.

IPR2023-01360
Patent 9,609,544 B2

Before ROBERT J. WEINSCHENK, GARTH D. BAER, and RUSSELL E. CASS, *Administrative Patent Judges*.

CASS, *Administrative Patent Judge*.

TERMINATION
Due to Settlement After Institution of Trial
35 U.S.C. § 317; 37 C.F.R. § 42.74

I. INTRODUCTION

With the Board's authorization, Petitioner and Patent Owner (collectively referred to as "the Parties") filed a Joint Motion to Terminate the above-identified proceeding due to settlement. Paper 15 ("Joint Motion"). In support of the Joint Motion, the Parties filed a Settlement Agreement (Ex. 1027 ("Settlement Agreement")), as well as a Joint Request to Treat Exhibit 1027 as Business Confidential Information (Paper 16 ("Joint Request")) pursuant to 35 U.S.C. § 317(b) and 37 C.F.R. § 42.74.

II. DISCUSSION

In the Joint Motion, the Parties represent that they "have reached a settlement that addresses this proceeding," that they "have concurrently filed the Settlement Agreement as Exhibit 1027," and that "there are no other agreements, oral or written, between the Parties made in connection with, or in contemplation of, the termination of the proceeding." Joint Motion 3. The Parties further represent that their settlement resolves "all the disputes in this proceeding and as to the patent at issue," and that they jointly stipulated to a dismissal with prejudice of Patent Owner's claims in the related litigation. *Id* at 4.

Under 35 U.S.C. § 317(a), "[a]n inter partes review instituted under this chapter shall be terminated with respect to any petitioner upon the joint request of the petitioner and the patent owner, unless the Office has decided the merits of the proceeding before the request for termination is filed." Section 35 U.S.C. § 317(a) also provides that if no petitioner remains in the *inter partes* review, the Office may terminate the review.

We instituted a trial on the above-identified proceeding on April 1, 2024. Paper 7. We have not yet decided the merits of the proceeding, and a

final written decision has not been entered. Notwithstanding that the proceeding has moved beyond the preliminary stage, the Parties have shown adequately that the termination of the proceeding is appropriate. Under these circumstances, we determine that good cause exists to terminate the proceeding with respect to the Parties.

After reviewing the Settlement Agreement between Petitioner and Patent Owner, we find that the Settlement Agreement contains confidential business information regarding the terms of settlement. We determine that good cause exists to treat the Settlement Agreement between Petitioner and Patent Owner as business confidential information pursuant to 35 U.S.C. § 317(b) and 37 C.F.R. § 42.74(c).

In the Joint Request, the Parties indicate that the Settlement Agreement requires that its terms "are to be maintained as confidential by the Parties and, subject to certain exceptions, may not be disclosed to any third parties without the express written consent of the non-disclosing party." Joint Request 1. We note that we have no procedure for obtaining express written consent of either party prior to disclosure, and our regulations do not require us to do so. We decline to issue an order regarding consent upon receiving Settlement Agreement access requests.

This Order does not constitute a final written decision pursuant to 35 U.S.C. § 318(a).

III. ORDER

Accordingly, for the reasons discussed above, it is:

ORDERED that the Joint Motion to Terminate (Paper 15) is *granted*, and IPR2023-01360 is *terminated* with respect to Petitioner and Patent Owner pursuant to 35 U.S.C. § 317(a) and 37 C.F.R. § 42.72; and

FURTHER ORDERED that the Joint Request to Treat Exhibit 1027 as Business Confidential Information (Paper 16) is *granted*, and the Settlement Agreement (Ex. 1027) shall be kept separate from the file of Patent 9,609,544, and made available only to Federal Government agencies on written request, or to any person on a showing of good cause, pursuant to 35 U.S.C. § 317(b) and 37 C.F.R. § 42.74(c).

FOR PETITIONER:

W. Karl Renner
Jeremy Monaldo
Ryan Chowdhury
Jennifer Huang
FISH & RICHARDSON P.C.
axf-ptab@fr.com
jjm@fr.com
rchowdhury@fr.com
jjh@fr.com

FOR PATENT OWNER:

Reza Mirzaie
Dale Chang
Amy Hayden
James Milkey
Neil Rubin
Philip Wang
RUSS AUGUST & KABAT
rmirzaie@raklaw.com
dchang@raklaw.com
ahayden@raklaw.com
jmilkey@raklaw.com
nrubin@raklaw.com
pwang@raklaw.com

Trials@uspto.gov
571-272-7822

Paper 7
Entered: April 1, 2024

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.,
Petitioner,

v.

HEADWATER RESEARCH LLC.,
Patent Owner.

IPR2023-01360
Patent 9,609,544 B2

Before ROBERT J. WEINSCHENK, GARTH D. BAER, and RUSSELL E. CASS, *Administrative Patent Judges.*

CASS, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Samsung Electronics Co., LTD. ("Petitioner") filed a Petition requesting an *inter partes* review of claims 1–23 (the "challenged claims") of U.S. Patent No. 9,609,544 B2 (Ex. 1001, "the '544 patent"). Paper 2, 1 ("Pet."). Headwater Research LLC ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

An *inter partes* review may not be instituted unless it is determined that "the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314 (2018); *see also* 37 C.F.R § 42.4(a) (2021) ("The Board institutes the trial on behalf of the Director."). The reasonable likelihood standard is "a higher standard than mere notice pleading," but "lower than the 'preponderance' standard to prevail in a final written decision." *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential).

For the reasons provided below and based on the record before us, we determine that Petitioner has demonstrated a reasonable likelihood that it would prevail in showing the unpatentability of at least one of the challenged claims. Accordingly, we institute an *inter partes* review on all grounds set forth in the Petition.

B. Real Parties in Interest

Petitioner states that the real parties in interest are Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. Pet. 85.

Patent Owner states that Headwater Research LLC is the real party in interest. Paper 4, 1.

C. Related Proceedings

The parties indicate that the '544 patent is the subject of the following district court case: *Headwater Research LLC v. Samsung Electronics Co., Ltd.*, No. 2:22-cv-00422 (E.D. Tex.). Pet. 85; Paper 4, 2.

D. The '544 Patent (Ex. 1001)

The '544 patent relates to "device-assisted services for protecting network capacity." Ex. 1001, code (56). More specifically, the '544 patent explains, the device can manage capacity increases by "apply[ing] a service usage control policy for the network service usage activities to protect network capacity (e.g., reduce network capacity demand)." *Id.* at 13:66–14:2. The device can "assign[] a priority to a network service usage activity and control[] traffic associated with the network services usage activity based on the assigned priority" and provide a "differentiated and dynamic background services classification . . . as a function of network availability state and/or network busy state." *Id.* at 14:25–32. The service usage control policy assists "in network access control of network service usage activities (e.g., deferring some or all of the network capacity demand from these source activities)." *Id.*

The device associates "the network service usage activity with a network service usage control policy" based on factors such as "a network busy state," "a time of day," "application behavior," "a power state of device, a device usage state, a time based criteria, availability of alternative networks, and a set of policy rules." Ex. 1001, 89:15–23. When a policy

applies to an access request, the device can apply various "well known traffic control techniques." *Id.* at 15:48–50.

E. Illustrative Claims

Of challenged claims 1–23, claim 1 is independent. For purposes of the issues raised at this stage of the proceeding, claim 1 is illustrative and is reproduced below.

> [1.1] A wireless end-user device, comprising:
>
> [1.2] a wireless modem to communicate data for network service usage activities between the device and a wireless network;
>
> [1.3] a processor that executes instructions to
>
> associate network service usage activity, on behalf of a first device application, and that occurs when the first device application is not in the foreground of user interaction, with a network service usage control policy,
>
> [1.4] set an application state indicating whether the first device application, associated with a particular network service usage activity, is in the foreground of user interaction, and
>
> [1.5] dynamically determine whether to apply the network service usage control policy to the particular network service usage activity, based on the application state and based on a power control state; and
>
> [1.6] a memory coupled to the processor to provide the processor with instructions.

Ex. 1001, 108:19–37 (indents and bracketed paragraph identifiers added).

F. Applied References

Petitioner relies upon the following references:

> Rao, US 2006/0039354 A1, published Feb. 23, 2006 (Ex. 1005, "Rao");

Araujo, US 2009/0217065 A1, published Aug. 27, 2009 (Ex. 1006, "Araujo");

Freund, US 5,987,611, issued Nov. 16, 1999 (Ex. 1007, "Freund");

Singh, US 8,381,127 B2, issued Feb. 19, 2013 (Ex. 1008, "Singh");

Montemurro, US 2009/0207817 A1, published Aug. 20, 2009 (Ex. 1009, "Montemurro");

Wright, US 2006/0039364 A1, published Feb. 23, 2006 (Ex. 1010, "Wright").

Pet. i, 2. Petitioner also submits the Declaration of Dr. Kevin Butler (Ex. 1003).

G. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims 1–23 of the '544 patent based on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 2, 4–8, 12–16, 18, 20, 22, 23	103	Rao, Araujo
2, 17, 19–21	103	Rao, Araujo, Freund
3	103	Rao, Araujo, Singh
11	103	Rao, Araujo, Montemurro
9, 10, 13, 18	103	Rao, Araujo, Wright

Pet. 1.

II. DISCUSSION

A. Claim Construction

A claim "shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under

35 U.S.C. § 282(b)." 37 C.F.R. § 42.100(b). At this stage of the proceeding, neither party presents any claim terms for construction. Pet. 2–3; Prelim. Resp. 3. Based on the present record, we determine that it is not necessary to provide an express interpretation of any claim terms at this time. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1374 (Fed. Cir. 2019) ("The Board is required to construe 'only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

B. Principles of Law

A claim is unpatentable under 35 U.S.C. § 103 if "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, objective evidence of non-obviousness.[1] *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we must also "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a

[1] At this stage of the proceeding, Patent Owner has not presented objective evidence of non-obviousness.

combination of prior art elements would have produced a predictable result weighs in the ultimate determination of obviousness. *Id.* at 416–417.

In an *inter partes* review, the petitioner must show with particularity why each challenged claim is unpatentable. *Harmonic, Inc. v. Avid Technology, Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016); 37 C.F.R. § 42.104(b) (2020). The burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

We analyze the challenges presented in the Petition in accordance with the above-stated principles.

C. Level of Ordinary Skill in the Art

Petitioner introduces the testimony of Dr. Butler that a person of ordinary skill in the art would have had "(1) at least a bachelor's degree in computer science, electrical engineering, or a related field, and (2) three to five years of experience with networking, power consumption of networked computing devices, and/or wireless communication systems." Pet. 5, n.1; Ex. 1003 ¶ 17. Dr. Butler further states that "[m]ore education, e.g., a doctorate in an academic area emphasizing electrical engineering, computer engineering, computer science, or a related technical field, would compensate for fewer years of work experience." *Id.* Patent Owner states that "[f]or the purposes of this preliminary response," it "does not challenge that definition." Prelim. Resp. 3.

For purposes of this Decision, we adopt the assessment of the level of ordinary skill in the art proposed by Petitioner and Dr. Butler and not disputed by Patent Owner as reasonable and consistent with the prior art.

See Okajima v Bourdeau, 261 F.3d 1350, 1355 (Fed. Cir 2001) (the prior art may reflect an appropriate level of skill in the art).

D. Ground 1A:[2] Asserted Obviousness of Claims 1, 2, 4–10, 12–16, 18, 20, 22, and 23 Based on Rao in view of Araujo

Petitioner contends that claims 1, 2, 4–10, 12–16, 18, 20, 22, and 23 would have been obvious over Rao in view of Araujo. Pet. 6–50. Patent Owner disagrees, arguing that Petitioner has failed to establish that these claims would have been obvious based on Rao and Araujo. Prelim. Resp. 3–12.

1. Overview of Rao (Ex. 1005)

Rao is directed to "a remote access architecture for providing peer-to-peer communications and remote access connectivity." Ex. 1005, code (57). The system is shown in Rao's Figure 1A, reproduced below.

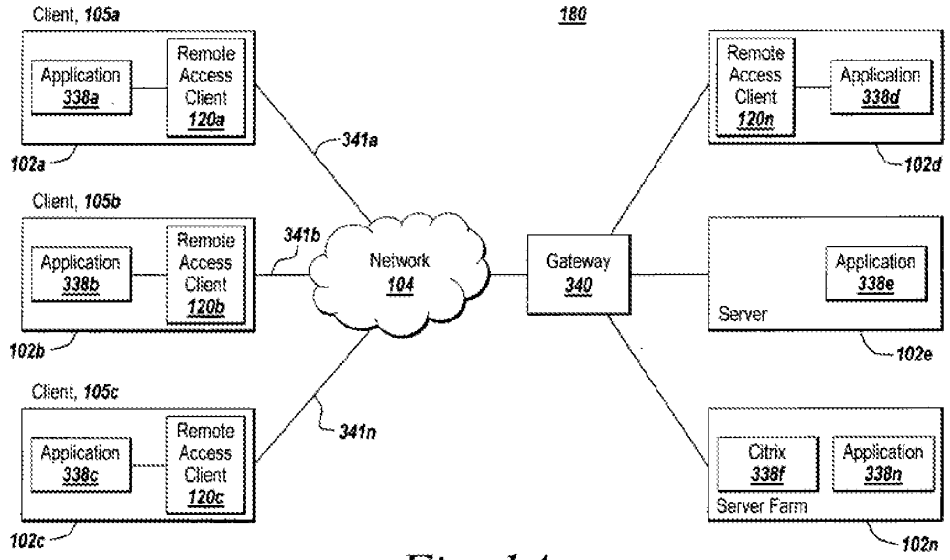


Fig. 1A

[2] Here, and elsewhere in the Decision, the identification of the grounds using designations such as "Ground 1A" and "Ground 1B" refers to the designation of the grounds as presented in the Petition.

Rao's Figure 1A is a block diagram of an embodiment of Rao's system operating via a gateway in a network environment. Ex. 1005 ¶ 60, Fig. 1A. As shown in Figure 1A, Rao's system includes clients 105 (e.g., computing devices 102a–102c) that communicate over network 104 to other devices, such as servers, server farms, and peer computing devices. *Id.* ¶¶ 86–96.

Rao addresses inefficient use of network resources when network communications between devices are "processed in the order generated by the activity of a user and applications of the client." Ex. 1005 ¶ 3. According to Rao, this is not "always desirable" because, for example, network packets for background applications may be processed ahead of network packets for foreground applications, resulting in applications suffering from increased latency and reduced quality of voice communication. *Id.* Rao addresses these inefficiencies by using a prioritization scheme that "provide[s] application-aware, client-specific prioritization of packet traffic." *Id.* As Rao explains, this scheme is achieved by augmenting client 105 as shown in Rao's Figure 1C, reproduced below.

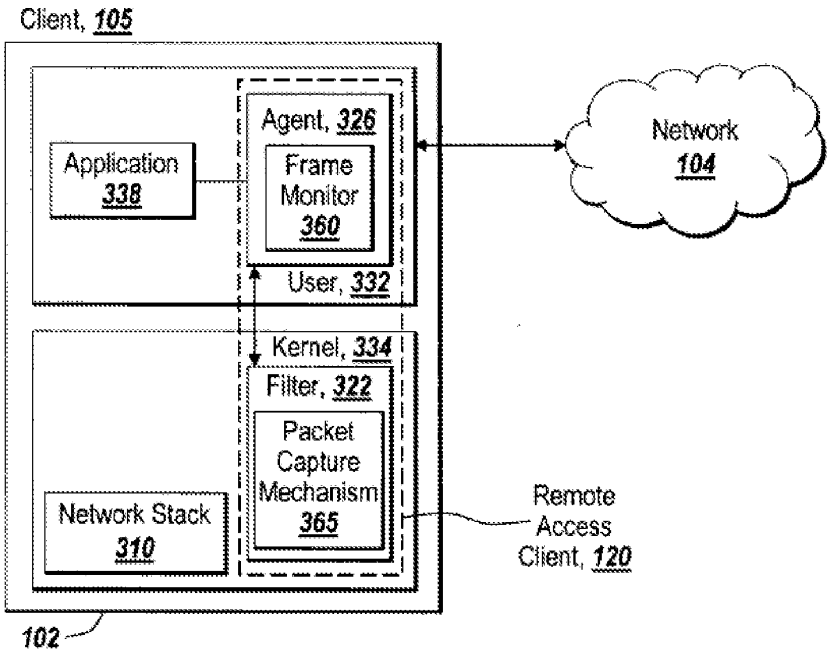


Fig. 1C

Rao's Figure 1C is a block diagram depicting an embodiment of client 105 that has been augmented with remote access client 120 for network communications.

As shown in Figure 1C, Rao's client 105 includes remote access client (RAC) 120 that interacts with application 338 and network stack 310. Ex. 1005 ¶¶ 89, 98–101. RAC 120 includes filter 322 that uses a "filtering table . . . to determine what action to take against packets," including "ensur[ing] that unwanted packets are discarded," "deny[ing] access to particular protocols," and/or "preventing unauthorized access from remote computers by discarding packets to specified destination addresses." *Id.* ¶ 102. RAC 120 can also include agent 326 with frame monitor 360 that "include[s] policies and logic for applying a policy to a received packet,"

and "transmit[s] a packet to a gateway 340 responsive to a policy-based determination made by the frame monitor 360." *Id.* ¶ 108.

Rao also explains that its RAC "provides for the intelligent and client-centric prioritization of application network communications on a client based on the type and/or priority of an application." Ex. 1005 ¶ 179. To perform prioritization, Rao's system may "apply a policy to determine a condition of the client 105, or endpoint, at the time of transmission of the packet," and "frame monitor 360 may identify an application 338 that generated the packet" and "make a policy-based determination to transmit the packet to the gateway 340 responsive to the identified application 338." *Id.* ¶ 109. Additionally, Rao discloses that policies can be specified, for example, by "type of application," type of "protocols used by the applications," or "whether an application is running in the foreground or the background of the client 105." *Id.* ¶ 182. Rao explains that "[o]ne ordinarily skilled in the art will recognize and appreciate the multitude of ways to define client-side application priorities." *Id.*

2. Overview of Araujo (Ex. 1006)

Araujo is directed to the management of a machine's power by using a power-management policy. Ex. 1006, code (57). When a program "makes a request that involves use of one of the machine's power-consuming devices, the policy may take into account factors such as the program's status" indicating "the program's relative level of justification to consume power." *Id.* For example, "some programs may have a 'VIP' status that allows them to consume power in situations where other programs would not be permitted to consume power." *Id.* ¶ 27. Araujo's system includes a power manager 110 that controls the respective power states of devices and "may

cause devices to be turned off, or into a lower power state, based on factors such as timers, the amount of battery power remaining, or any other factor." *Id.* ¶ 22. Such factors are evaluated by Araujo's power management runtime 120 that "may implement policies that determine when, and under what circumstances", power manager 110 is to turn devices 104–108 on or off, or is to place those devices in a different power state." *Id.*

In addition, "[a] component may intercept a request to use a device before the request reaches the driver, and may deflect requests that, if carried out, are not consistent with [the] power usage policy." Ex. 1005, code (57). This may be carried out using "[r]equest deflector component 602" interposed "between program 112 and driver 116." *Id.* ¶ 50. "When request deflector component 602 detects that a request . . . has been made, it interacts with power management runtime 120 to determine what the ambient policy (e.g., power use policy 266) says about whether the request may be carried out at the expense of power use." *Id.* If the request may be carried out under the power policy, "request deflector component 602 passes the request along to driver 116;" otherwise request deflector component 602 "may permanently or temporarily deflect the request from reaching driver 116." *Id.*

3. Analysis of Independent Claim 1

a) [1.1]: "[a] wireless end-user device, comprising:"

Petitioner argues that, to the extent the preamble is limiting, Rao renders it obvious. Pet. 19. Petitioner asserts that Rao teaches a client that is a wireless end-user device such as a "mobile telephone" or "other form of computing or telecommunications device that is capable of communication." *Id.* at 19–20 (citing Ex. 1005 ¶¶ 86, 130; Ex. 1003 ¶ 85). According to

Petitioner, one of ordinary skill "would have known that a wireless telephone is a wireless end-user device." *Id.* at 20 (citing Ex. 1003 ¶ 85).

Patent Owner does not present arguments regarding the preamble. *See* Prelim. Resp. 3–12.

We determine that, on the record before us, Petitioner's cited evidence sufficiently supports its contentions regarding the preamble.[3]

b) [1.2]: "a wireless modem to communicate data for network service usage activities between the device and a wireless network;"

Petitioner argues that Rao teaches a computing device with a network interface that can include a "wireless network adapter," "modem," or "any other device suitable for interfacing the computing device 102 to any type of network capable of communication." Pet. 21 (emphasis omitted) (citing Ex. 1005 ¶ 125). Petitioner also asserts that Rao "teaches that the network interface of its device 'interface[s] to . . . wireless connections.'" *Id.* "Moreover," according to Petitioner, "Rao's device may be implemented as a 'smart phone,'" which one of ordinary skill "would have understood and found obvious includes a wireless modem." *Id.* (citing Ex. 1005 ¶ 198; Ex. 1003 ¶ 87).

Patent Owner does not present arguments directed to this limitation. *See* Prelim. Resp. 3–12.

We determine that, on the record before us, Petitioner's cited evidence sufficiently supports its contentions regarding this limitation.

[3] Because we are persuaded that Petitioner has sufficiently shown that Rao teaches the subject matter recited in the preamble, we need not decide whether the preamble is limiting for purposes of this Decision.

c) *[1.3]: "a processor that executes instructions to associate network service usage activity, on behalf of a first device application, and that occurs when the first device application is not in the foreground of user interaction, with a network service usage control policy,"*

Petitioner argues that Figure 1D of Rao shows a processor (CPU 121) that executes instructions, and discloses that each computing device 102 includes a central processing unit 102 and main memory 104. Pet. 21–22 (citing Ex. 1005 ¶ 118, Fig. 1D). According to Petitioner, one of ordinary skill would have understood that the processor executes instructions. *Id.* at 22 (citing Ex. 1005 ¶ 119; Ex. 1003 ¶ 91).

Petitioner argues that Rao also teaches applying policies when network service usage activity of a first device application occurs when the first device application is not in the foreground of user interaction. Pet. 22 (citing Ex. 1005 ¶ 182; Ex. 1003 ¶ 92). Petitioner points to Rao's disclosure that "policies 520 define prioritization based on whether an application is running in the foreground or the background of the client 105," and argues that one of ordinary skill "would have understood and found obvious that reference to applications 'not in the foreground' includes, for example, applications in the background and thereby are subject to policies 520." *Id.* at 22–23 (citing Ex. 1005 ¶ 182; Ex. 1003 ¶ 92).

Petitioner further argues that Rao "teaches associating network service usage activity of an application with a network service usage control policy." Pet. 23 (citing Ex. 1005 ¶¶ 182–187; Ex. 1003 ¶ 93). For example, Petitioner asserts, "Rao teaches policies 'for specifying client-side prioritization of network communication related to **applications**," and that the remote access client "'determines the association of network packets with applications' to 'determine priorities and apply any priority based

policies' and 'can associate network traffic with applications' by any suitable mechanisms." *Id.* (citing Ex. 1005 ¶ 187). According to Petitioner, one of ordinary skill "would have known that, since Rao's policies can define prioritization based on whether an application is running in the foreground or background of the client, the RAC determines the association of network packets with applications to determine priorities, then applies priority-based policies." *Id.* (citing Ex. 1003 ¶ 94). Thus, Petitioner contends, the combination "renders obvious associating network service usage activity, on behalf of a first application, and that occurs when the first application is not in the foreground of user interaction, with a network service usage control policy." *Id.* at 23–24 (citing Ex. 1005 ¶¶ 182, 187; Ex. 1003 ¶ 94).

Patent Owner does not present arguments directed to this limitation. *See* Prelim. Resp. 3–12.

We determine that, on the record before us, Petitioner's cited evidence sufficiently supports its contentions regarding this limitation.

d) [1.4]: "set an application state indicating whether the first device application, associated with a particular network service usage activity, is in the foreground of user interaction, and"

Petitioner argues that Rao teaches applying policies, which one of ordinary skill would have understood to involve or make obvious setting an application state. Pet. 24 (citing Ex. 1003 ¶ 96). For example, Petitioner asserts, "Rao explains that policies 'define prioritization based on **whether an application is running in the foreground or the background** of the client 105'" and that characteristics of the application, such as whether it runs in the foreground or background, can "indicate priority for a network

packet of the application." *Id.* (citing Ex. 1005 ¶¶ 182, 189). In this example, according to Petitioner, one of ordinary skill "would have understood and found obvious that applying a policy to prioritize network packets for [an] application involves setting an application's state (e.g., foreground, background) to permit the evaluation of policies that rely on the application state." *Id.* (citing Ex. 1003 ¶ 96). Additionally, Petitioner contends, "Rao's policies 'may be specified conditionally' based on application state," and one of ordinary skill "would have similarly understood and found obvious that policy depends on application state ('is running'), and thus, use of the policy includes setting an application state so the policy may be applied." *Id.* at 24–25 (citing Ex. 1003 ¶ 96).

Furthermore, Petitioner argues, Rao teaches "packet interception techniques," which one of ordinary skill "would have understood and found obvious to include associating applications with network service activities." Pet. 25 (citing Ex. 1003 ¶ 97). According to Petitioner, "Rao's client intercepts packets 'associated with an application' and 'a priority for the intercepted and queued network packet is determined based on the type and/or priority of the application.'" *Id.* (citing Ex. 1005 ¶ 184). One of ordinary skill, Petitioner contends, would have recognized that, in the proposed combination, "intercepted packets are examples of network service activities, and thus, the interception of packets that are then prioritized based on application state indicates that applications (which have application states, e.g., foreground, background) are associated with network service activities." *Id.* (citing Ex. 1003 ¶ 97).

Patent Owner does not present arguments directed to this limitation. *See* Prelim. Resp. 3–12.

We determine that, on the record before us, Petitioner's cited evidence sufficiently supports its contentions regarding this limitation.

> e) *[1.5]: "dynamically determine whether to apply the network service usage control policy to the particular network service usage activity, based on the application state and based on a power control state; and*

Petitioner argues that the combination of Rao and Araujo renders this limitation obvious. Pet. 25. More specifically, Petitioner asserts, "Rao teaches policy evaluation based on application state, such that prioritization [is] based on whether an application is running in the foreground or the background." *Id.* (citing Ex. 1005 ¶ 182). According to Petitioner, one of ordinary skill "would have recognized 'foreground' and 'background' as examples of application states." *Id.* at 25–26 (citing Ex. 1003 ¶ 182).

Petitioner also contends that "Araujo teaches that 'devices may have various power states' such as on, off and a processor's clock speed and 'a justification to change a device from one power state to another may be based on at least one other factor other than the mere fact that a request to use the device has been made.'" *Id.* at 26 (citing Ex. 1006 ¶¶ 4, 25). And, Petitioner argues, "Araujo further teaches that the 'current power state of a device may be a factor in determining whether the power state will be changed.'" *Id.* (citing Ex. 1006 ¶ 28). According to Petitioner, one of ordinary skill "would have recognized that Araujo's disclosure that the 'power state of a device' is a power control state and a 'factor in determining whether the power state will be changed' renders obvious that the power control state is used to determine whether to apply a policy regulating network service usage." *Id.* (citing Ex. 1003 ¶ 100).

Turning to motivation to combine, Petitioner argues that one of ordinary skill would have found it obvious to combine Rao's remote access client (RAC) with Aruajo's power manager and power management runtime (collectively referred to as a "power policy manager" or "PPM") and request deflector component in order "to provide a client that better uses energy and 'strikes a balance between providing functionality and maintaining longevity of the charge.'" Pet. 14 (citing Ex. 1006 ¶ 1; Ex. 1003 ¶ 75). Specifically, Petitioner asserts that one of ordinary skill would have perceived opportunities for improving Rao's policy management capabilities "to impart additional advantages, such as optimizing power use," and "would have recognized the importance of power management at least because, in mobile devices, applications cannot execute without sufficient power." *Id.* at 15 (citing Ex. 1003 ¶ 77; Ex. 1006 ¶ 1). Consequently, according to Petitioner, one of ordinary skill "would have looked to policy-based power management, such as taught in Araujo, to serve as one of Rao's 'multitude of ways to define client-side application priorities.'" *Id.* (citing Ex. 1005 ¶ 182; Ex. 1003 ¶ 78). The resulting Rao-Araujo combination, Petitioner explains, "would both manage power according to the PPM techniques of Araujo and manage network use according to both Rao's and Araujo's techniques." *Id.* (citing Ex. 1003 ¶ 78).

As to the proposed combination itself, Petitioner argues that one of ordinary skill "would have incorporated Araujo's PPM and reflector components in Rao's RAC," such that "[t]he enhanced RAC" would "evaluate power-management policies (per Araujo) and network prioritization policies (per Rao and Araujo)." Pet. 15 (citing Ex. 1003 ¶ 79). "For example," Petitioner asserts, the Rao-Araujo combination "would have

determined whether an application has a 'relative level of justification to consume power,' which includes determining whether the application is running in the foreground or background." *Id.* at 15–16 (citing Ex. 1005 ¶ 182; Ex. 1006, code (57); Ex. 1003 ¶ 79). Additionally, according to Petitioner, one of ordinary skill "would have understood and found obvious that policy enforcement" in the proposed combination "may be based on application state (foreground/background) and power state (battery/plugged-in)." *Id.* at 16 (Ex. 1005 ¶ 182; Ex. 1006 ¶¶ 4, 11).

Petitioner also argues that, because Araujo's request is "interposed between the program and the device driver" and Rao's filter "may include a packet capturing mechanism 365, and the filter 322 and/or packet capturing mechanism 365 may comprise a network driver," the Rao-Araujo device's request deflector "would reside in the filter interposed between the other packet capture components and network device driver that provides traffic to the network stack." Pet. 18. Additionally, Petitioner contends that one of ordinary skill would have had a reasonable expectation of success in making the combination because doing would "would have required only routine programming knowledge well within the skill" of a person of ordinary skill in the art at the relevant time. *Id.* at 16–18 (citing Ex. 1003 ¶¶ 81, 83).

Petitioner also provides four examples of how the combined Rao-Araujo device would operate. These examples are as follows.

> Example 1: When the application transmitting packets is in the foreground, giving it VIP status, and the power state indicates the battery is above a threshold level, the device would permit transmission and place the packets in a high-priority queue.
>
> Example 2: When the application transmitting packets is in the background (not having VIP status) and the battery is above a threshold level, the device would permit the transmission and place the packets in a lower-priority queue.

> Example 3: When the application transmitting packets is in the foreground and the battery is below a threshold level, the device would place the packets in a high-priority queue but hold the transmission until a more favorable power state existed.
>
> Example 4: When the application transmitting packets is in the background and the power level is low, the request deflector prevents the request from being passed to the device driver, not queuing the packet and further conserving power.

Pet. 16–17 (citing Ex. 1006 ¶ 22; Ex. 1003 ¶ 80). Petitioner explains that these are examples of the "multitude of ways to define client-side application priorities" referred to by Rao. *Id.* at 17 (citing Ex. 1005 ¶ 182; Ex. 1003 ¶ 80).

Patent Owner responds that the Petition "fails to establish the obviousness of the combination" of Rao and Araujo. Prelim. Resp. 5. In doing so, Patent Owner focuses on Petitioner's Example 3, arguing that "[t]he Petition identifies no plausible benefit or other motivation to place packets 'in a high priority queue . . . until a more favorable power state existed' at some indeterminate future time period, even though the Petition acknowledges that this proposed queuing has the disadvantage of passing the transmission request to the device driver and consuming additional power (during a period of time when the battery power of the device is *already* low)." *Id.* at 5–7 (citing Pet. 17). For example, Patent Owner argues, "in a mobile device with a low battery, the system will not know *when* the device will be plugged in such that 'a more favorable power state' will exist," and thus "the amount of time packets would need to be queued would be entirely indeterminate and would often be on the order of hours." *Id.* at 7. According to Patent Owner, "queuing packets would require consumption by the network driver, which would need to (i) convert data for transmission by the application into packets suitable for transmission over the network

and (ii) remain powered on to preserve and store the network packets in the high-priority queue." *Id.* at 7–8 (citing Pet. 17).

Patent Owner provides a couple of additional arguments as to why Petitioner's proposed combination would be undesirable. First, Patent Owner offers up the example of a trusted application on a smartphone that starts uploading HDR videos, and then is moved to the background. Prelim. Resp. 8. According to Patent Owner, those videos would be processed into tens or hundreds of thousands of network packets, which would be queued until some future point in time, thus consuming CPU and memory battery power and capacity. *Id.* at 8–9. Furthermore, Patent Owner contends, if the user deletes the videos or turns off the device, or the device runs out of battery power before the conditions are met for transmitting the stored network packets, all of the stored packets would be lost. *Id.* at 9.

Patent Owner also argues that queuing but not transmitting packets would interfere with application flow because the application would not be informed that its data for transmission was not actually transmitted over the network, causing the application to continue attempting to transmit data over the network, wasting CPU, memory, and battery resources. Prelim. Resp. 9–10. According to Patent Owner, the application would also need to keep track of what data had been queued and re-request transmission of any packets that ultimately timed out. *Id.* at 10. Patent Owner also contends that the Petition admits that queuing the packet is less power efficient than simply not queuing the packet at all. *Id.* at 11 (citing Pet. 17). These inefficiencies, Patent Owner argues, could be avoided "by simply ***not*** taking the application state into account" and "not queuing any network packets for transmission when the battery is low." *Id.*

Based on the present record, we determine that Petitioner has made a sufficient showing as to this limitation for purposes of institution. In this regard, Petitioner has introduced sufficient evidence at this stage of the proceeding that one of ordinary skill would have been motivated to combine Rao and Araujo as Petitioner proposes. This evidence includes the testimony of Dr. Butler that one of ordinary skill "would have found it obvious to combine a Remote Access Client as taught by Rao with a PPM and request deflector as taught by Araujo to provide a client that better 'use[s] the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.'" Ex. 1003 ¶ 75. It also includes Dr. Butler's testimony that, in implementing Rao's filtering, prioritization, and queuing functionality, one of ordinary skill "would have perceived opportunities for improving the policy management capabilities already present in Rao to impart additional advantages, such as optimizing power use," and would have known that "mobile devices use techniques for optimizing the use of constrained resources, including network bandwidth and battery power." *Id.* ¶ 77. Dr. Butler further explains that one of ordinary skill "would have recognized the importance of power management at least because, in mobile devices, applications cannot execute without sufficient power." *Id.* Additionally, Dr. Butler testifies that, for these reasons, one of ordinary skill "would have looked to policy-based power management such as taught in Araujo to serve as one of Rao's 'multitude of ways to define client-side application priorities,'" to create a device that "would both manage power according to the PPM techniques of Araujo and manage network use according to the techniques of both Rao and Araujo." *Id.* ¶ 78. And, Dr. Butler explains, based on Rao and Araujo, one of

ordinary skill "would have understood and found obvious that policy enforcement" in the Rao-Araujo combination "may be based on application state (foreground, background) and power state (battery/plugged-in). *Id.* ¶ 80. We determine that this testimony is reasonable and credible based on the record presently before us, and is unrebutted by countervailing evidence from Patent Owner.

We also determine that Petitioner has introduced sufficient evidence that one of ordinary skill would have had a reasonable expectation of success in achieving the proposed Rao-Araujo combination. This evidence includes the testimony of Dr. Butler that one of ordinary skill "would have expected success integrating a PPM and deflector components as taught by Araujo into a remote access client as taught by Rao," that "the request deflector (Araujo) and packet capture mechanism (Rao) serve similar functions," and that "[c]ombining such functions would have required only routine programming skill well within the skill set of" a person of ordinary skill. Ex. 1003 ¶¶ 81, 83.

We do not agree with Patent Owner's arguments against institution. First, we do not agree with Patent Owner that deficiencies in Petitioner's Example 3 of the Rao-Araujo device's operation warrant denial of institution. Even if Patent Owner were correct that one of ordinary skill would not have been motivated to include the operation of Example 3 within the programming of the proposed combination, Petitioner has provided sufficient evidence that one of ordinary skill would have been motivated to program the proposed combination in accordance with Examples 1 and 4. Based on the present record, such programming would be sufficient to meet the relevant language of claim 1, which broadly recites that the processor

dynamically determine whether to apply the network service usage control policy "based on the application state and based on a power control state," without specifying particular details of how the application state and power control state are used. The parties may further address the other examples during the trial.

Based on the present record, we also do not agree with Patent Owner's argument that one of ordinary skill would not have been motivated to make the proposed combination based on its example of a smartphone app that starts uploading HDR videos and then is moved to the background. Prelim. Resp. 8. Patent Owner does not introduce evidence that this example would necessarily require queuing "tens of thousands to hundreds of thousands of network packets" until some future point in time, as Patent Owner contends, but rather relies only on attorney argument. *Id.* at 8–9. Moreover, even if the combined device was not ideal for uploading videos in a background app, Petitioner has sufficiently shown on this record that it would have been suitable for other uses, such as prioritizing real time data communications from a foreground application over non-real-time data communication applications in background applications, as Rao explains. Ex. 1005 ¶ 184 ("The client 105, using the techniques of the present invention, may prioritize the real-time data communications of application 338a ahead of other applications, such as non-real-time data communication applications.").

We also do not agree with Patent Owner's argument that a motivation to combine is lacking because queuing but not transmitting packets would interfere with application flow. Prelim. Resp. 9–10. More specifically, Patent Owner argues that application flow would be impeded because (1) the

application would not be informed that its data for transmission was not actually transmitted over the network, causing the application to continue attempting to transmit data over the network, wasting CPU, memory, and battery resources, and (2) the application would also need to keep track of what data had been queued and re-request transmission of any packets that ultimately timed out. *Id.* Based on the present record, it is not clear to us that the proposed combination would be implemented in the manner that Patent Owner contends, particularly because Patent Owner does not support its assertions with expert testimony, but instead relies only on attorney argument. Specifically, Patent Owner has not sufficiently shown why the application could not be informed that its data for transmission was not actually transmitted over the network (so that it would not need to continue to attempt to transmit the same data), or why keeping track of what data had been queued would be a significant problem in the combination.

Consequently, Petitioner has made a sufficient showing that the prior art teaches this limitation for purposes of institution.

f) [1.6]: "a memory coupled to the processor to provide the processor with the instructions.

Petitioner argues that Rao renders this limitation obvious. Pet. 27. For example, Petitioner asserts, Rao's Figure 1D shows a main memory 122, and "further teaches that the processor (CPU) 'is any logic circuitry that responds to and processes instructions fetched from the main memory unit 104' and 'the processor 100 communicates with main memory 104 via a system bus.'" Pet. 27–28 (citing Ex. 1005 ¶¶ 119–120, Fig. 1D). According to Petitioner, one of ordinary skill "would have recognized that Rao's system bus couples the processor to the memory, and the memory provides instructions fetched by the processor." *Id.* at 28 (citing Ex. 1003 ¶ 105).

Patent Owner does not present arguments directed to this limitation. *See* Prelim. Resp. 3–12.

We determine that, on the record before us, Petitioner's cited evidence sufficiently supports its contentions regarding this limitation.

g) Summary for Claim 1

For the foregoing reasons, Petitioner's cited evidence and reasoning demonstrates a reasonable likelihood that Petitioner would prevail in its contentions regarding claim 1.

4. Claims 2, 4–8, 12–16, 18, 20, 22, and 23

Petitioner contends that dependent claims 2, 4–8, 12–16, 18, 20, 22, and 23 are unpatentable over Rao in view of Araujo. Pet. 28–50. Patent Owner relies on its arguments concerning claim 1 for these claims. *See* Prelim. Resp. 3–12. Based on the evidence of record, we determine that Petitioner has demonstrated a reasonable likelihood that claims 2, 4–8, 12–16, 18, 20, 22, and 23 are unpatentable over Rao in view of Araujo.

E. Grounds 1B–1E

In Grounds 1B–1E Petitioner contends that dependent claims 2, 3, 9–11, 13, and 17–21 would have been obvious over various combinations of Rao, Araujo, Freund, Singh, Montemurro, and Wright. Pet. 1, 50–82. Patent Owner relies on its arguments concerning claim 1 for these claims. *See* Prelim. Resp. 3–12. Based on the evidence of record, we determine that Petitioner has demonstrated a reasonable likelihood that claims are unpatentable over the cited prior art.

III. CONCLUSION

After considering the evidence and arguments presented in the current record, we determine that Petitioner has demonstrated a reasonable

likelihood of success in proving that at least one of the challenged claims of the '544 patent is unpatentable. We therefore institute trial on all challenged claims and grounds raised in the Petition.

At this stage of the proceeding, we have not made a final determination as to the patentability of any challenged claim or as to the construction of any claim term. Any final determination will be based on the record developed during trial. We place Patent Owner on express notice that any argument not asserted in a timely-filed Response to the Petition, or in another manner permitted during trial, shall be deemed waived, even if that argument was presented in the Preliminary Response.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–23 of the '544 patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '544 patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

For PETITIONER:

W. Karl Renner
Jeremy J. Monaldo
Ryan Chowdhury
Jennifer J. Huang
FISH & RICHARDSON PC.
axf-ptab@fr.com
jjm@fr.com
rchowdhury@fr.com
jjh@fr.com

For PATENT OWNER:

Reza Mirzaie
Dale Chang
Amy E. Hayden
James A. Milkey
Neil A. Rubin
Philip X. Wang
RUSS AUGUST & KABAT
rmirzaie@raklaw.com
dchang@raklaw.com
ahayden@raklaw.com
jmilkey@raklaw.com
nrubin@raklaw.com
pwang@raklaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 9,609,544 B2
APPLICATION NO. : 14/082040
DATED : March 28, 2017
INVENTOR(S) : Raleigh et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Add to the end of the first paragraph of item (60), page 2, Column 1:
, said application No. 12/695,019 is a continuation-in-part of application No. 12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,771, filed on Mar. 2, 2009, said application No. 12/695,020 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,445 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,451 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,455 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,021 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,980 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010, said application No. 13/134,005, filed on May 25, 2011, is a continuation-in-part of application No. 12/380,759, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,779, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,758, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,768, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,767, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,780 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,755 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,756 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,770 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,772 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,782 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,783 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,757 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,781 filed on Mar. 2, 2009 and a continuation-in-part of application No. 12/380,774 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,771 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,773 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,769 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,777 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,020, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,445, filed on

Signed and Sealed this
Twenty-sixth Day of February, 2019

Andrei Iancu
Director of the United States Patent and Trademark Office

Jan. 27, 2010, and a continuation-in-part of application No. 12/694,451, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,455, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,980, filed on Jan. 28, 2010.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Raleigh et al.	Patent No.: 9,609,544
Serial No.: 14/082,040	Issue Date: March 28, 2017
Filing Date: November 15, 2013	Conf. No.: 1015
Title: Device-Assisted Services for Protecting Network Capacity	

Commissioner for Patents
Office of Patent Publication
ATTN: Certificate of Correction Branch
P.O. Box 1450
Alexandria, VA 22313-1450

MISCELLANEOUS COMMUNICATION REGARDING CERTIFICATE OF CORRECTION

Applicant/Patentee (hereinafter, "Applicant") respectfully requests that the Office issue a Certificate of Correction for U.S. Patent No. 9,609,544 to correct the missing priority claims in "Related U.S. Application Data (60)" section of the patent. The errors being corrected are the Office's errors.

In the published patent, section (60) recites a priority claim that is incomplete. The complete priority claim is accurately reflected in the November 15, 2013 Application Data Sheet. The following information is missing and should be added to the end of the first paragraph of section (60), page 2, col. 1:

, said application No. 12/695,019 is a continuation-in-part of application No.12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No.12/380,771, filed on Mar. 2, 2009, said application No. 12/695,020 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,445 is a continuation-in-part of application No.

12/380,780, filed on Mar. 2, 2009, said application No. 12/694,451 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,455 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,021 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,980 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, and a continuation-in-part of application No. 2/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010, said application No. 13/134,005, filed on May 25, 2011, is a continuation-in-part of application No. 12/380,759, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,779, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,758, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,768, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,767, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,780 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,755 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,756 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,770 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,772 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,782 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,783 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,757 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,781 filed on Mar. 2, 2009 and a continuation-in-part of application No. 12/380,774 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,771 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,773 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,769 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,777 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,020, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,445, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,451, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,455, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,980, filed on Jan. 28, 2010.

CONCLUSION

Applicant respectfully requests issuance of the Certificate of Correction to correct the errors in the priority claim. The Office is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: January 11, 2019 By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703
(903) 201-6212

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: January 11, 2019 By: /Jennifer Smith/
Jennifer Smith

PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
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.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 9,609,544

APPLICATION NO.: 14/082,040

ISSUE DATE : March 28, 2017

INVENTOR(S) : Raleigh et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Add to the end of the first paragraph of section (60), page 2, col. 1:

, said application No. 12/695,019 is a continuation-in-part of application No.12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No.12/380,771, filed on Mar. 2, 2009, said application No. 12/695,020 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,445 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,451 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/694,455 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,021 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, said application No. 12/695,980 is a continuation-in-part of application No. 12/380,780, filed on Mar. 2, 2009, and a continuation-in-part of application No. 2/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010,

[Continued on next page]

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. 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 1.14. This collection is estimated to take 1.0 hour 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. SEND TO: **Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/44 (09-07)
Approved for use through 08/31/2013. OMB 0651-0033
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.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 9,609,544

APPLICATION NO.: 14/082,040

ISSUE DATE : March 28, 2017

INVENTOR(S) : Raleigh et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

[Add to the end of the first paragraph of section (60), page 2, col. 1]:

said application No. 13/134,005, filed on May 25, 2011, is a continuation-in-part of application No. 12/380,759, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,779, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,758, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,778, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,768, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,767, filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,780 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,755 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,756 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,770 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,772 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,782 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,783 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,757 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,781 filed on Mar. 2, 2009 and a continuation-in-part of application No. 12/380,774 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,771 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,773 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,769 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/380,777 filed on Mar. 2, 2009, and a continuation-in-part of application No. 12/695,019, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,020, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,445, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,451, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/694,455, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,021, filed on Jan. 27, 2010, and a continuation-in-part of application No. 12/695,980, filed on Jan. 28, 2010.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. 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 1.14. This collection is estimated to take 1.0 hour 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. SEND TO: **Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Acknowledgement Receipt	
EFS ID:	34833138
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Jennifer Smith
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	11-JAN-2019
Filing Date:	15-NOV-2013
Time Stamp:	15:07:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Certificate of Correction	P032C1_ReqforCoC_RTF.pdf	426483 9cf033ca7d59ac8e55619da695361c82416ffd60	no	5
Warnings:					

Information:	
Total Files Size (in bytes):	426483

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.

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 NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	03/28/2017	9609544	RALEP032C1	1015

106963 7590 03/08/2017

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 338 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Headwater Partners I LLC, Redwood Shores, CA;
Gregory G. Raleigh, Woodside, CA;
Alireza Raissinia, Monte Sereno, CA;
James Lavine, Corte Madera, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

Change(s) applied to document, /D.D./ 2/22/2017

	229	7565141		2009-07-21	Macaluso, Anthony G.	
	230	7373179		2008-05-13	Stine, Ted et al.	
	231	7236780		2007-06-26	Benco, David S.	
	232	7039403		2006-05-02	Wong, Gregory A.	
	233	8370477		2013-02-05	Short, Joel E. et al.	
	234	8364806		2013-01-29	Short, Joel E. et al.	
	235	8279067		2012-10-02	BERGER, Thomas R. et al.	
	236	8213296		2012-07-03	SHANNON, Frank M. et al.	
	237	8019868		2011-09-13	RAO, Goutham et al.	
	238	8005988		2011-08-23	MAES, Stephane H.	
	239	7978627		2011-07-12	TAYLOR, William Scott et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.R./

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

106963 7590 02/17/2017

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

NOTIFICATION DATE	DELIVERY MODE
02/17/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent@headwaterllc.com

Corrected Notice of Allowability	Application No. 14/082,040	Applicant(s) RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the February 8, 2017 Information Disclosure Statements*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1,5,8-21 and 24-30*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Applicant cancelled claims 2-4, 6, 7, 22 and 23.

3. Applicant's January 31, 2014; May 22, 2014 and two February 8, 2017 Information Disclosure Statements (IDS's) have been reviewed. Note the attached IDS's.

Allowable Subject Matter

4. Claims 1, 5, 8-21 and 24-30 are allowed.

5. The following is an examiner's statement of reasons for allowance: Applicant's December 1, 2016 Amendment regarding claims 1, 5, 8-21 and 24-30 have been reviewed, along with the above aforementioned IDS's. Claims 1, 5, 8-21 and 24-30 are now allowed as all the cited prior art, either alone or in combination, does not disclose Applicant's inventive claim language.

Claims 1, 5, 8-21 and 24-30 have been reviewed in light of Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014) and are not deemed invalidated by such.

Claims 1, 5, 8-21 and 24-30 are determined to be directed to patent-eligible subject matter and the Examiner does not consider any of the pending claims to be directed to an abstract idea. Even if the Examiner were to identify an abstract idea for any claim, then under a further analysis under Alice all claims would still be found to be patent eligible for the following reasons. The Examiner finds that when all of the elements of each claim are considered individually and as an ordered combination, each claim contains an inventive concept which is directed to an application, a particular application, or a special application, of the identified abstract idea. Further the Examiner finds that issuance of a patent for any claim would not preempt the identified abstract idea, or the field of the identified abstract idea.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW JOSEPH RUDY whose telephone number is (571)272-6789. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Fahd A. Obeid can be reached on 571-270-3324. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit 3687

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6115823	A	2000-09-05	Velasco et al.	
	2	9326173	B2	2016-04-26	Luft, Achim	
	3	7203721	B1	2007-04-10	Ben-Efraim et al.	
	4	7219123	B1	2007-05-15	Fiechter et al.	
	5	7505795	B1	2009-03-17	Lim et al.	
	6	7389412		2008-06-17	Sharma et al.	
	7	7466652		2008-12-16	Lau et al.	
	8	7512131		2009-03-31	Svensson et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7526541		2009-04-28	Roese et al.	
	10	8539544		2013-09-17	Garimella et al.	
	11	9111088		2015-08-18	Ghai et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20090065571	A1	2009-03-12	Jain, Deepak	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J RUDY/	Date Considered	02/10/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6879825	B1	2005-04-12	Daly, Brian Kevin	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050163320	A1	2005-07-28	Brown et al.	
	2	20060114821	A1	2006-06-01	Willey et al.	
	3	20070201502	A1	2007-08-30	Abramson, Nathan	
	4	20080168275	A1	2008-07-10	DeAtley et al.	
	5	20080178300	A1	2008-07-24	Brown et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	6	20090049156	A1	2009-02-19	Aronsson et al.	
	7	20090320110	A1	2009-12-24	NICOLSON et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1289326	EP	A1	2003-03-05	Motorola, Inc.		
	2	2006041989	JP		2006-02-09	Fujitsu Ltd.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J RUDY/	Date Considered	02/10/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	2447
Examiner Name	Raleigh, Gregory G.
Attorney Docket Number	RALEP032C1

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5774532	A	1998-06-30	Gottlieb et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040225898	A	2004-11-11	Frost, D. et al.	
	2	20050079863	A	2005-04-14	Macaluso, Anthony G.	
	3	20060114832	A	2006-06-01	Hamilton et al.	
	4	20060156398	A	2006-07-13	Ross et al.	
	5	20060173959	A	2006-08-03	Mckelvie et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	Raleigh, Gregory G.
	Attorney Docket Number	RALEP032C1

	6	20070033194	A	2007-02-08	Srinivas et al.	
	7	20080070550	A	2008-03-20	Hose, David Alan	
	8	20080201266	A	2008-08-21	Chua et al.	
	9	20100284327	A	2010-11-11	Miklos, Gyorgy	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"Communication Concepts for Mobile Agent Systems," by Joachim Baumann et al.; Inst. Of Parallel and Distributed High-Performance Systems, Univ. of Stuttgart, Germany, pp. 123-135, 1997	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J RUDY/	Date Considered	02/10/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6185576	B1	2001-02-06	Mcintosh, Lowrie	
	2	7320029	B2	2008-01-15	Rinne et al.	
	3	7539132	B2	2009-05-26	Werner et al.	
	4	7805606	B2	2010-09-28	Birger et al.	
	5	8175574	B1	2012-05-08	Panda et al.	
	6	8180881	B2	2012-05-15	Seo et al.	
	7	8191124	B2	2012-05-29	Wynn et al.	
	8	8275415	B2	2012-09-25	Huslak, Nicholas S.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	9	8300575	B2	2012-10-30	Willars, Per	
	10	8315593	B2	2012-11-20	Gallant et al.	
	11	8347378	B2	2013-01-01	Merkin et al.	
	12	8375128	B2	2013-02-12	Tofighbakhsh et al.	
	13	8527410	B2	2013-09-03	Markki et al.	
	14	8539561	B2	2013-09-17	Gupta et al.	
	15	8554876	B2	2013-10-08	Winsor, Gerald W.	
	16	8666395	B2	2014-03-04	Silver, Andrew	
	17	8391834	B2	2013-03-05	Raleigh, Gregory G.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

	1	20110238545		2011-09-29	Fanaian, Nabil Ruh et al.	
	2	20040170191	A	2004-09-02	Guo et al.	
	3	20040203833	A	2004-10-14	Rathunde, Dale F. et al.	
	4	20050186948	A	2005-08-25	Gallagher et al.	
	5	20070147317	A	2007-06-28	Smith et al.	
	6	20080025230	A	2008-01-31	Patel et al.	
	7	20080056273	A	2008-03-06	Pelletier et al.	
	8	20080270212	A	2008-10-30	Blight et al.	
	9	20100030890	A	2010-02-04	Dutta et al.	
	10	20110110309	A	2011-05-12	Bennett, James D.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	2447
	Examiner Name	not yet assigned
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1310401	CN	A	2001-08-29	Wang, Di Xing		☐
	2	2466831	EP	A1	2012-06-20	Openet Telecom Ltd. - Mcnamee et al.		☐
	3	2007133844	WO	A	2007-11-22	Camiant, Inc.		☐
	4	1999027723	WO	A1	1999-06-03	Telefonaktiebolaget LM Ericsson		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	"End to End QoS Solution for Real-time Multimedia Application;" Computer Engineering and Applications, 2007, 43 (4): 155-159, by Tan Zu-guo, Wang Wen-juan; Information and Science School, Zhanjian Normal College, Zhan jiang, Guangdong 524048, China	☐
	2	"ASA/PIX: Allow Split Tunneling for VPN Clients on the ASA Configuration Example," Document ID 70917, January 10, 2008	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J RUDY/	Date Considered	02/10/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

106963 7590 01/31/2017
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Ann Taylor	(Depositor's name)
	(Signature)
February 9, 2017	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

TITLE OF INVENTION: DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	05/01/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	709-224000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 James E. Harris
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Headwater Research LLC
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Tyler TX

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 505876 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date February 9, 2017
Typed or printed name James E. Harris Registration No. 40013

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Electronic Patent Application Fee Transmittal				
Application Number:	14082040			
Filing Date:	15-Nov-2013			
Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY			
First Named Inventor/Applicant Name:	Gregory G. Raleigh			
Filer:	James E. Harris/Ann Taylor			
Attorney Docket Number:	RALEP032C1			
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**480**

Electronic Acknowledgement Receipt	
EFS ID:	28314187
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	09-FEB-2017
Filing Date:	15-NOV-2013
Time Stamp:	15:49:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$480
RAM confirmation Number	021017INTEFSW00002181505876
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	P032C1_IssueFee.pdf	139849 b37dd6057c2b0c203de2a34530aadfbb1c6b9cf6	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30280 80bd9b96d9b3cf463a2cd714296c4c138b1424f4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	170129		

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.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6115823	A	2000-09-05	Velasco et al.	
	2	9326173	B2	2016-04-26	Luft, Achim	
	3	7203721	B1	2007-04-10	Ben-Efraim et al.	
	4	7219123	B1	2007-05-15	Fiechter et al.	
	5	7505795	B1	2009-03-17	Lim et al.	
	6	7389412		2008-06-17	Sharma et al.	
	7	7466652		2008-12-16	Lau et al.	
	8	7512131		2009-03-31	Svensson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	7526541		2009-04-28	Roese et al.	
	10	8539544		2013-09-17	Garimella et al.	
	11	9111088		2015-08-18	Ghai et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20090065571	A1	2009-03-12	Jain, Deepak	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

If you wish to add additional non-patent literature document citation information please click the Add button	Add		
EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2017-02-08
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 the Freedom of Information Act requires disclosure of these record s.

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 another 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 inspections 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.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6879825	B1	2005-04-12	Daly, Brian Kevin	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20050163320	A1	2005-07-28	Brown et al.	
	2	20060114821	A1	2006-06-01	Willey et al.	
	3	20070201502	A1	2007-08-30	Abramson, Nathan	
	4	20080168275	A1	2008-07-10	DeAtley et al.	
	5	20080178300	A1	2008-07-24	Brown et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	6	20090049156	A1	2009-02-19	Aronsson et al.	
	7	20090320110	A1	2009-12-24	NICOLSON et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1289326	EP	A1	2003-03-05	Motorola, Inc.		
	2	2006041989	JP		2006-02-09	Fujitsu Ltd.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

X That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

X The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2017-02-08
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 the Freedom of Information Act requires disclosure of these record s.

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 another 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 inspections 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.

Patent Abstracts of Japan

PUBLICATION NUMBER : 2006041989
PUBLICATION DATE : 09-02-06

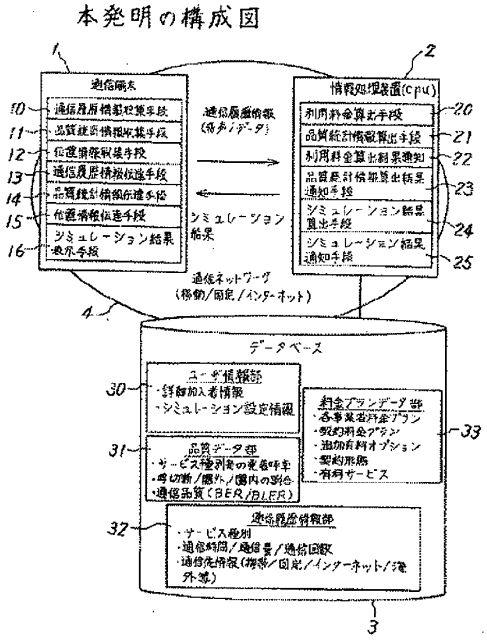
APPLICATION DATE : 28-07-04
APPLICATION NUMBER : 2004219784

APPLICANT : FUJITSU LTD;

INVENTOR : KATAOKA KOSUKE;

INT.CL. : H04M 15/16 (2006.01)

TITLE : CHARGING PLAN NOTIFICATION SYSTEM



ABSTRACT : PROBLEM TO BE SOLVED: To provide a charging plan notification system for calculating the lowest optimum charging plan corresponding to a utilization state of a communication terminal user from charging plans provided by all carriers.

SOLUTION: The charging plan notification system is provided with: a communication terminal for transmitting communication history information concerned with communication; a database 3 for storing the communication history information, all contract information between communication terminal users and communication carriers and all charging plans for communication service provided by all the carriers; and an information processor 2 for calculating utilization charges. The information processor 2 respectively calculates accurate utilization charges in the charging plans provided from respective carriers on the basis of the communication history information of each communication terminal user, the contract information and all the charging plans and notifies the communication terminal user of the calculated results.

COPYRIGHT: (C)2006,JPO&NCIPI

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-41989
(P2006-41989A)
(43)公開日　平成18年2月9日(2006.2.9)

(51)Int.Cl.	F I	テーマコード（参考）
H04M 15/16 (2006.01)	H04M 15/16	5K025

審査請求 未請求　請求項の数 5　OL　（全 15 頁）

(21)出願番号　特願2004-219784 (P2004-219784)
(22)出願日　平成16年7月28日 (2004.7.28)

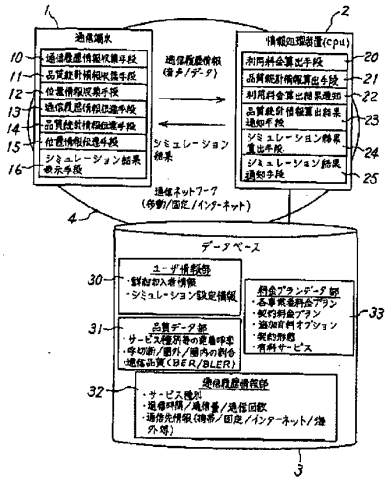
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100083297
弁理士　山谷　晧榮
(74)代理人　100087848
弁理士　小笠原　吉義
(72)発明者　友松　聖詞
東京都品川区南大井６丁目２２番７号　富士通ネットワークソリューションズ株式会社内

最終頁に続く

(54)【発明の名称】料金プラン通知装置

(57)【要約】
【課題】全通信事業者の料金プランの中から通信端末ユーザの利用状態に応じた最も安い最適の料金プランを算出する料金プラン通知装置を提供すること。
【解決手段】このため本発明では、通信に関する通信履歴情報を送信する通信端末１と、通信履歴情報と、通信端末ユーザの通信事業者との全ての契約情報と、全通信事業者が提供する通信サービスの全料金プランとを蓄積しておくデータベース３と、利用料金を算出する情報処理装置２を具備する料金プラン通知装置であって、通信端末ユーザの通信履歴情報と、契約情報と、全料金プランとの情報を利用し、情報処理装置２により各通信事業者が提供している料金プランにおいて、各々正確な利用料金を算出し、通信端末ユーザに通知する。
【選択図】図１

本発明の構成図



BNSDOCID: <JP_____2006041989A__I_>

【特許請求の範囲】
【請求項1】
通信に関する通信履歴情報を送信する通信端末と、
通信履歴情報と、通信端末ユーザの通信事業者との全ての契約情報と、全通信事業者が提供する通信サービスの全料金プランとを蓄積しておくデータベースと、
利用料金を算出する情報処理装置を具備する料金プラン通知装置であって、
通信端末ユーザの通信履歴情報と、契約情報と、全料金プランとの情報を利用し、情報処理装置により各通信事業者が提供している料金プランにおいて、各々正確な利用料金を算出し、通信端末ユーザに通知する料金プラン通知装置。
【請求項2】
前記通信端末は、全通信における発着呼率、通信途中での切断、待受け時における圏内・圏外の割合・データ伝送速度等、全ての品質情報を通信履歴情報、通信端末が取得できる位置情報とをデータベースに送信する伝達手段を持ち、
上記データベースは品質情報を蓄積する蓄積手段を持ち、
上記情報処理装置は、品質情報を基に各通信事業者、エリア、時間帯毎等の統計的な通信サービスの品質情報を算出する算出手段を持ち、通信サービスの品質情報を全料金プランの正確な利用料金と共に通信端末ユーザに通知できる通知手段を具備したことを特徴とする請求項１記載の料金プラン通知装置。
【請求項3】
上記情報処理装置は、予めデータベースに登録されている、通信端末ユーザが通信事業者と契約している料金プラン、追加有料オプション、契約時期、契約形態、有料サービス、全通信事業者が提供している全料金プラン、及び有料オプション、割引情報等の情報を利用して正確な利用料金を算出することを特徴とする請求項１記載の料金プラン通知装置。
【請求項4】
上記情報処理装置は、サービス種別、通信時間、量、回数、通信先、位置情報等の詳細な通信履歴情報を利用して、正確な利用料金を算出することを特徴とする請求項１記載の料金プラン通知装置。
【請求項5】
通信端末ユーザが利用を想定した任意の利用条件をデータベースに設定し、ユーザの要求に応じて情報処理装置は、それらの情報と、データベースに登録してある通信端末ユーザの詳細加入者情報及び料金プランに関連する情報を利用して、各料金プランにおいてシミュレーションし、正確に料金算出し、結果を通信端末ユーザに通知することを特徴とする請求項１記載の料金プラン通知装置。

【発明の詳細な説明】
【技術分野】
【0001】
本発明は、通信端末の利用料金を算出し、通信端末ユーザに通知するサービスを行う料金プランを考慮した料金シミュレーションを実施し、最適な料金プランをユーザおよび事業者に通知する料金プラン通知システムに関する。
【背景技術】
【0002】
従来、携帯電話の如き通信端末では、基本使用料と一定金額の無料通話分の設定や、平日昼間や夜間、土日祝日等通話時間帯毎の通話料割引倍率、パケット料金の割引など様々な割引プランが設定されている。
【0003】
通信事業者は、これらの組み合せによりバリエーションを持たせた料金プランを準備している。
【0004】
ユーザは、あらかじめ１つの料金プランを選択し、そのプランに設定された割引率と実

際の月々の利用料金により算出された金額を契約した通信事業者からの請求により支払う。

【0005】

ユーザが自己の通信に対して最適な料金プランによる通信サービスを受けることができるように、ユーザに対して通話終了毎に、契約された契約料金プランと準備された全ての料金プランとを比較して、得られる最適な料金プランをリアルタイムで通知することが提案されている。

【特許文献1】特開２００１－３６６７３号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

上記従来技術では、ユーザが現在契約している通信事業者が提供しているサービスの中における最適な料金プランの提供であり、他社の通信事業者の提供しているものを含めた料金プランにおける最適なものの提供ではない。

【0007】

したがってユーザが、現在契約している料金システムが自己にとって最適なプランであるかどうかを判断するために、ユーザ自身が月々の利用状態を分析し、検討し、現在の契約通信事業者のみならず他の契約通信事業者の料金プランと比較することが必要である。

【0008】

しかるに各社の料金プランは多様・複雑化しており、ユーザ自らが分析・検討するのは困難である。したがって、各社の料金プランの中からユーザの通信端末の利用状態に応じた、最適の料金プランを提供するサービスが求められている。

【課題を解決するための手段】

【0009】

上記課題を解決するため、本発明では、下記（１）～（５）の料金プラン通知装置を提供する。

【0010】

（１）通信に関する通信履歴情報を送信する通信端末と、通信履歴情報と、通信端末ユーザの通信事業者との全ての契約情報と、全通信事業者が提供する通信サービスの全料金プランとを蓄積しておくデータベースと、利用料金を算出する情報処理装置を具備する料金プラン通知装置であって、通信端末ユーザの通信履歴情報と、契約情報と、全料金プランとの情報を利用し、情報処理装置により各通信事業者が提供している料金プランにおいて、各々正確な利用料金を算出し、通信端末ユーザに通知することを特徴とする料金プラン通知装置。

【0011】

（２）上記（１）の料金プラン通知装置において、前記通信端末は、全通信における発着呼率、通信途中での切断、待受け時における圏内・圏外の割合・データ伝送速度等、全ての品質情報を通信履歴情報、通信端末が取得できる位置情報とをデータベースに送信する伝達手段を持ち、上記データベースは品質情報を蓄積する蓄積手段を持ち、上記情報処理装置は、品質情報を基に各通信事業者、エリア、時間帯毎等の統計的な通信サービスの品質情報を算出する算出手段を持ち、通信サービスの品質情報を全料金プランの正確な利用料金と共に通信端末ユーザに通知できる通知手段を具備したことを特徴とする。

【0012】

（３）上記（１）の料金プラン通知装置において、上記情報処理装置は、予めデータベースに登録されている、通信端末ユーザが通信事業者と契約している料金プラン、追加有料オプション、契約時期、契約形態、有料サービス、全通信事業者が提供している全料金プラン、及び有料オプション、割引情報等の情報を利用して正確な利用料金を算出することを特徴とする。

【0013】

（４）上記（１）の料金プラン通知装置において、上記情報処理装置は、サービス種別

、通信時間、量、回数、通信先、位置情報等の詳細な通信履歴情報を利用して、正確な利用料金を算出することを特徴とする。

【0014】

（５）上記（１）の料金プラン通知装置において、通信端末ユーザが利用を想定した任意の利用条件をデータベースに設定し、ユーザの要求に応じて情報処理装置は、それらの情報と、データベースに登録してある通信端末ユーザの詳細加入者情報及び料金プランに関連する情報を利用して、各料金プランにおいてシミュレーションし、正確に料金算出し、結果を通信端末ユーザに通知することを特徴とする。

【発明の効果】

【0015】

本発明により下記の効果を奏する。

【0016】

（１）通信端末が通信端末ユーザの詳細な通信履歴情報をサービス提供業者の料金プラン通知装置のデータベースに登録し、情報処理装置において、前記データベースに登録された詳細な通信履歴情報と料金プラン情報を使用して、ユーザが契約していない他の通信事業者のプランも含めて全料金プランについて正確な通信料金を算出し、通信端末ユーザに通知するので、通信端末ユーザは前記契約外の通信事業者のプランも含めた一番安い料金プランを正確に知ることができる。

【0017】

（２）通信端末に、通信履歴情報と共に通話品質に関連する情報をサービス提供業者の料金プラン通知装置のデータベースに送信し、情報処理装置に、データベースに登録されている通信品質に関連する情報を使用して各通信事業者、エリア、時間帯毎等の統計的な通信サービスの品質情報を算出し、通信端末ユーザに通知するので、通信端末ユーザは契約していない通信事業者のつながり易さ、音声品質等の通信品質を含め、全通信事業者の通信品質情報を知る事が出来るので、通信端末ユーザは、一番通信品質の良い通信事業者を選択することができる。

【0018】

（３）通信端末ユーザは、料金プランや契約形態等の詳細な加入者情報、契約情報をサービス提供者の料金プラン通知装置のデータベースに登録し、それらを利用料金算出に使用することにより、利用形態に沿った正確な一番安い利用料金プランを算出することが可能となる。

【0019】

（４）現在の通信端末は音声通話終話単位で表示される通信履歴情報とパケット数情報を確認できるが、これらは各通信事業者の標準的なプランを基にした情報であり必ずしも正確な情報ではなかったが、本発明では通信端末ユーザからの実用的な詳細情報の収集は、通話時間、パケット数だけでなく、通信量、通話回数、接続通話先、データ量、利用回数等通信履歴情報の詳細を用いてデータベースに登録し、それらを利用料金算出に使用できるので、情報処理装置での正確な利用料金算出を可能とする。

【0020】

（５）通信端末ユーザが自分の利用形態を想定した条件をデータベースに登録し、データベースに登録した詳細な加入者情報、各種料金プランを利用することで大雑把な料金シミュレーションではなく、正確なシミュレーションの実現が可能となり、また前月の履歴情報を流用する手段を持たせることで、シミュレーションに必要な情報を前月と同じ状態で算出することができ、ユーザオペレーションを低減させた正確なシミュレーションの実現が可能となる。

【発明を実施するための最良の形態】

【0021】

自己の通信履歴情報を、サービス業者に送信する通信端末と、多数の通信事業者の料金プランと前記通信履歴情報を保持するデータベースと、前記通信履歴情報にもとづき前記多数の通信事業者の料金プランを使用して通信を行ったときの料金を算出する情報処理装

置を設け、前記通信履歴情報にもとづき前記多数の通信事業者の料金プランを使用して通信を行ったときもっとも安いものを前記情報処理装置で算出して、このうちのもっとも安い料金システムを通信端末ユーザに通知する料金プラン通知装置を提供する。これにより、通信端末ユーザは、このサービス業者からの通知により、自己が契約している通信事業者以外の他の通信事業者を含めた全通信事業者の料金プランのうちより、自己に適したもっとも安い料金プランを認識することができる。

【実施例】

【0022】

本発明の実施例１を図１～図３にもとづき説明する。図１は本発明の構成図、図２は本発明の品質統計情報説明図、図３は時間毎の品質統計情報説明図である。

【0023】

図中、１は通信端末、２は情報処理装置、３はデータベース、４は通信ネットワーク、１０は通信履歴情報収集手段、１１は品質統計情報収集手段、１２は位置情報収集手段、１３は通信履歴情報伝達手段、１４は品質統計情報伝達手段、１５は位置情報伝達手段、１６はシミュレーション結果表示手段、２０は利用料金算出手段、２１は品質統計情報算出手段、２２は利用料金算出結果通知手段、２３は品質統計情報算出結果通知手段、２４はシミュレーション結果算出手段、２５はシミュレーション結果通知手段、３０はユーザ情報部、３１は品質データ部、３２は通信履歴情報部、３３は料金プランデータ部である。

【0024】

通信端末１は、ユーザが通信相手と音声やデータを送受信するものであり、例えば携帯端末である。

【0025】

情報処理装置２は、通信端末１から送信された通信履歴情報と、データベース３に保持された多くの通信事業者Ａ、Ｂ、Ｃ・・・の料金プランデータに基づいてシミュレーション演算を行い、そのうちもっとも安いものを送出するものであり、ＣＰＵで構成される。

【0026】

データベース３は通信端末１から送信された通信履歴情報や、多くの通信事業者Ａ、Ｂ、Ｃ、Ｄの料金プランデータが保持されており、外部メモリで構成されている。そしてデータベース３と情報処理装置２はサービス提供業者側の料金プラン通知装置に設置されている。

【0027】

通信ネットワーク４は、移動端末用ネットワーク、固定端末用ネットワーク、インターネットの如き、通信ネットワークである。

【0028】

通信端末１には、通信履歴情報収集手段１０、品質統計情報収集手段１１、位置情報収集手段１２、通信履歴情報伝達手段１３、品質統計情報伝達手段１４、位置情報伝達手段１５、シミュレーション結果表示手段１６等を有する。

【0029】

通信履歴情報収集手段１０は、通信端末１が通信相手に送信した送信データの種別データ量、送信時刻、送信時間、サービス種別等の履歴情報を一定期間保持するものである。

【0030】

品質統計情報収集手段１１は、通信相手から受信したデータの品質を通信相手が使用している通信事業者Ａ、Ｂ、Ｃ・・・毎に、例えば公知の５段階評価し、これを保持するものである。

【0031】

品質情報は、例えば前記受信データの５段階評価の外に、発着呼率、通信途中での切断、圏内・圏外の割合、通信品質（ビットエラーレートＢＥＲ、ブロックエラーレートＢＬＥＲ）、データ伝送レート等である。

【0032】

品質情報の例を図２、図３に示す。図２、図３は、通信事業者Ａ、Ｂ、Ｃ、Ｄの４者における品質統計情報を示すもので、図２（Ａ）は各通信事業者の平均の呼接続率、圏内の割合を示し、図２（Ｂ）は各通信事業者の平均の通信品質を示し、図２（Ｃ）は各通信事業者の平均データ伝送レートを示し、図３は各通信事業者の時間毎の呼接続率、圏内の割合を示す図である。

【0033】

なお図２（Ａ）における呼接続率（平均）Ｍ１と圏内の割合（平均）Ｍ２は下式により算出されるものである。

【0034】

Ｍ１＝（完了呼－不完了呼）／発呼

Ｍ２＝（圏内の時間－圏外の時間）／電源を入れていた時間

図２、図３のデータは、サービス業者に加入している通信事業者Ａ、Ｂ、Ｃ、Ｄを利用しているユーザの通信端末より送信されたデータにもとづく統計情報である。

【0035】

図２（Ａ）に示す如く、呼接続率は通信事業者Ａが約９０％、通信事業者Ｂが約９５％、通信事業者Ｃが約８０％、通信事業者Ｄが約９８％であることを示す。またノイズの少ない安定した状態で通信可能であることを示す圏内の割合は通信事業者Ａが約９５％、通信事業者Ｂが約７６％、通信事業者Ｃが約８５％、通信事業者Ｄが約９７％であることを示す。

【0036】

通信品質は、５段階評価で通信事業者Ａ、Ｂ、Ｄが５、通信事業者Ｃが４であることを示し、平均データ伝送レートは通信事業者Ａが約２５ｋｂｐｓ、通信事業者Ｂが約１７ｋｂｐｓ、通信事業者Ｃが約２３ｋｂｐｓ、通信事業者Ｄが約２４ｋｂｐｓであることを示す。

【0037】

品質情報には通信端末ユーザの住所が記入されているので、サービス装置側では各通信事業者についてこれらの住所を解析することにより例えば通信事業者Ｃが横浜駅周辺では通信品質があまりよくない等の品質統計情報を得ることができ、このような情報をユーザに提供することもできる。

【0038】

位置情報収集手段１２はサービス業者を利用している通信端末ユーザと通信先の通信端末ユーザの位置情報（住所）を収集し、これを保持するものである。

【0039】

通信履歴情報伝達手段１３は、通信履歴情報収集手段１０が収集した通信端末１が行った通信データを、通信ネットワーク４を経由してサービス業者側の情報処理装置２に送出するものである。

【0040】

品質統計情報伝達手段１４は、品質統計情報収集手段１１が収集したデータの品質情報をサービス業者側の情報処理装置２に通信ネットワーク４を経由して送出するものである。

【0041】

位置情報伝達手段１５は、位置情報収集手段１２で収集した、通信端末１と通信した相手端末のユーザの位置情報（住所）を通信ネットワーク４を経由してサービス業者側の情報処理装置２に送出するものである。

【0042】

シミュレーション結果表示手段１６は、情報処理装置２が算出したシミュレーション結果が通信ネットワーク４を経由して通信端末１に伝達されたとき、これを通信端末ユーザに表示する表示手段である。

【0043】

情報処理装置２は、通信端末から送信された通信履歴情報とデータベース４に蓄積され

ている全通信事業者の料金プランを使用して、全通信事業者の各料金プランについて正確な通信料金を算出し、通信端末の要求に応じて算出した通信料金を通信端末に通知したり、通信端末から受信した通信品質情報をデータベースに送信したり、データベースに登録してある通信品質情報を使用し、地域、時間帯通信事業者毎に品質統計情報を算出し通信端末の要求に応じて品質統計情報を通信端末に通知するものである。

【0044】

このため、情報処理装置２には、利用料金算出手段２０、品質統計情報算出手段２１、利用料金算出結果通知手段２２、品質統計情報算出結果通知手段２３、シミュレーション結果算出手段２４、シミュレーション結果通知手段２５等を有する。

【0045】

利用料金算出手段２０は、通信端末１から伝達された音声、データ等の通信履歴情報や、データベース部３に保持された各通信事業者の料金プランを使用して通信端末１のユーザに対する利用料金を算出するものである。

【0046】

品質統計情報算出手段２１は、通信端末１から受信されデータベース３に登録した通信品質情報を使用し、地域、時間帯、通信事業者毎における発着呼率、通信品質情報等を算出し、通信端末１の要求に応じて品質統計情報を通信端末１に通知するものである。

【0047】

利用料金算出結果通知手段２２は、利用料金算出手段２０で算出された全通信事業者の料金プランにもとづく通信料金のうち、もっとも安い料金を通信端末１に通知するものである。

【0048】

シミュレーション結果算出手段２４は、通信端末１のユーザが指定した任意の利用条件にもとづき、各通信事業者の料金プランを使用してもっとも安い利用料金を算出するものである。

【0049】

シミュレーション結果通知手段２５は、このシミュレーション結果算出手段２４から通知されたシミュレーション結果を、シミュレーション要求を行った通信端末に対し通知するものである。

【0050】

データベース３は、通信事業者に対する通信端末の加入者の詳細な契約情報、全通信事業者が提供する各種料金プラン、追加有料オプション情報、割引情報等の全ての課金に関する情報、及び本発明のサービスを制御するための、通信料金の通知回数や通知するタイミング等の設定情報、通信端末が送信した通信履歴情報を蓄積するもので、ユーザ情報部３０、品質データ部３１、通信履歴情報部３２、料金プランデータ部３３等を有し、前記情報処理装置２とともにサービス業者の料金プラン通知装置を構成する。

【0051】

ユーザ情報部３０は、通信端末１の加入者が現在契約している通信業者との詳細な契約情報である詳細加入者情報や、この加入者が料金のシミュレーション演算を求めるシミュレーション設定情報を保持するものである。

【0052】

品質データ部３１は、通信端末より送出されるサービス種別毎の発着呼率、呼切断の割合、圏内と圏外の割合、ビットエラーレート（ＢＥＲ）、ブロックエラーレート（ＢＬＥＲ）等の通信品質を保持するものである。

【0053】

通信履歴情報部３２は、通信端末より伝達された、通信端末が実際に通信を行った結果の情報を保持するもので、サービス種別、通信時間、通信量、通信回数、通信先が携帯端末か、固定端末か、インターネットか、海外か等を示す通信先情報を保持するものである。

【0054】

料金プランデータ部３３は、通信端末が加入しているか否かにかかわらず、全通信事業者の提供する各事業者料金プラン、契約料金プラン、追加有料オプション、契約形態、有料サービス等の課金に関する料金データを保持するものである。これらの料金データは、通信事業者がインターネットで公開したり、通信端末販売業者に郵送したりしているので、容易に入手できるものである。

【0055】

実施例１において、通信端末１は、通信履歴情報収集手段１０が収集したこの通信端末１が実際に通信した通信履歴情報を、通信履歴情報伝達手段１３が電子情報に変換し、移動通信網、固定通信網、インターネットの如き通信ネットワーク４を経由して、サービス業者の料金プラン通知装置を構成する情報処理装置２に送信する。

【0056】

情報処理装置２では、これを受信し、データベース３の通信履歴情報部３２に通信端末毎に、サービス種別、通信時間、通信量、通信回数、通信先情報等に識別して保持する。

【0057】

なお、サービス業者の料金プラン通知装置のデータベース３には、通信端末の加入者の料金プラン、オプション、契約期間等の詳細加入者情報やシミュレーション設定情報がそのユーザ情報部３０に保持され、また各通信事業者の料金プラン、契約料金プラン、追加有料オプション、契約形態、有料サービス等が料金プランデータ部３３に保持されている。

【0058】

したがって、通信端末の加入者が、例えば過去１ヶ月の通信履歴情報にもとづき、全通信事業者の料金プランにしたがって料金算出を求めたとき、情報処理装置２では、利用料金算出手段２０がデータベース３よりこの加入者の通信端末が過去１カ月に実際に通信を行った履歴情報にもとづき、料金プランデータ部３３に保持されている全通信事業者の各料金プランにより料金を算出し、これを利用料金算出結果通知手段２２に伝達する。

【0059】

利用料金算出結果通知手段２２では、この伝達された料金のうちもっとも安いものを選択してこれを通信端末１に送信する。

【0060】

通信端末１ではこれをシミュレーション結果表示手段１６が受信して表示出力し、加入者はこれにより、どの通信事業者の料金プランが自己の過去１ヶ月の通信履歴に対しもっとも安かったか認識し、現在の契約が適切か否かの判定が可能となる。勿論履歴情報は過去１ヶ月ではなく、１週間とか、適宜選択できる。

【0061】

実施例２においては、通信品質情報を算出通知するものである。通信端末１では通信毎の通信品質情報、例えば発着呼率、通信品質、通信時間、位置情報等を品質統計情報収集手段１１が算出し、これを収集する。

【0062】

品質統計情報伝達手段１４はこれらの情報を電子情報に変換し、任意のタイミングで移動通信網、固定通信網、インターネットの如き通信ネットワーク４を経由して、情報処理装置２に送信する。

【0063】

情報処理装置２は、通信端末１から受信した受信品質情報をデータベース３の品質データ部３１に送信し、通信品質情報を蓄積する。

【0064】

そして情報処理装置２は、通信端末１のユーザの要求に応じて、データベース３に登録してある通信品質情報を使用し、その品質統計情報算出手段２１が、地域毎、時間帯毎、通信事業者毎に、各時間帯毎、地域毎、事業者毎における発着呼率、呼切断、圏外・圏内の割合、ＢＥＲ、ＢＬＥＲ等の通信品質情報等を算出し、通信端末１のユーザの要求に応じて品質統計情報算出結果通知手段２３がこの品質統計情報を通信端末１に通知する。通

信端末１はこれをシミュレーション結果表示手段１６で受信してユーザに表示する。通信端末１のユーザは例えば図２、図３に示す如き、各通信事業者のサービス品質情報を取得することにより、通信サービスの品質を比較することができる。

【0065】

実施例３においては、有料オプション、契約期間等の詳細な加入者情報と、全通信事業者の提供する全料金プラン、追加オプション、割引制度情報から料金を比較算出するようにしたものである。

【0066】

データベース３のユーザ情報部３０には、情報処理装置２が通信端末ユーザの利用料金を算出する際に使用する、データベースに登録されている詳細な加入者情報が保持されている。

【0067】

この詳細な加入者情報としては、通信端末ユーザが通信事業者と契約している料金プラン情報すなわち、月額基本料金、無料通話時間、音声・データ・メール（Ｅメール、通信事業者網内向けメール、送受信料）等のサービス種別の通信料、自他国内キャリア、海外キャリア、国内・海外の固定電話、通信電話等の通信先毎の通信料、有料オプション、割引情報、契約期間、個人契約、法人契約（複数回線割引）等の契約形態等が登録されている。

【0068】

有料オプションの代表的なものとしては、通信事業者が提供する、留守番電話サービス、三者通話、海外ローミングサービス、国際通話等、その他ニュース、天気情報等の料金や条件等の詳細情報が登録される。

【0069】

割引情報の代表的なものとしては、家族割引、指定番号割引等の特定番号割引、時間帯割引、年齢・学生割引、長期契約割引、パケット割引の如きサービス種別毎の割引等の詳細情報が登録される。

【0070】

また、データベースの料金プランデータ部３３には、全通信事業者が提供している全料金プラン及び有料オプション、割引情報等の課金対象サービスの全ての詳細情報、条件が登録されており、これらの情報により情報処理装置２の利用料金算出手段２０が、例えば履歴情報に対して正確な利用料金を算出し、通信端末ユーザの契約料金と比較検討することができる。

【0071】

実施例４においては、通信履歴情報の詳細を示す。

【0072】

通信端末１がデータベース３に送信する通信履歴情報には、下記のような通信料金を算出するために必要な詳細情報が含まれている。

【0073】

音声、伝送速度・ＷＥＢアクセス・メール等のデータ、動画等のサービス種別。

【0074】

通信時間、パケット数等の量、回数。

【0075】

通信電話又は固定電話・フリーダイヤル・特定番号・ＵＲＬ・Ｅメール・国内又は海外等の通信先。

【0076】

緯経度等の位置情報。

【0077】

通信端末１は、これらの情報を電子情報に変換し、データベース３に送信する。情報処理装置２ではこれらの情報を利用料金の算出に使用する。

【0078】

BNSDOCID: <JP____2006041989A__I_>

実施例５においては、ユーザの任意の設定により、各料金プランにおいて使用料金をシミュレーション可能とするものである。

【0079】

このために、通信端末にユーザが例えば後述するサービス提供者のホームページより利用方法を想定したシミュレーション条件例えば音声通話時間、メール送受信回数、Ｗｅｂアクセス頻度、データ転送頻度、シミュレーション結果通知項目等を情報処理装置２に送信し、データベース３のユーザ情報部３０にこれらシミュレーション設定情報を登録する。

【0080】

情報処理装置２では、シミュレーション結果算出手段２４がこのシミュレーション条件と、データベース３の料金プランデータ部３３に登録ずみの全通信事業者の料金プランを利用してシミュレーション結果を算出し、シミュレーション結果通知手段２５がそのうちのもっとも安いものを通信端末１に送信し、シミュレーション結果表示手段１６がこれを表示してユーザにシミュレーション結果を知らせることができる。

【0081】

シミュレーション条件としてユーザの設定によるもののみでなく、例えばデータベースに蓄積されている前月の使用明細などの以前の通信履歴情報やデータベース３のユーザ情報部３０に予め用意してある代表的なシミュレーション条件を利用して設定することもできる。

【0082】

以前の通信履歴情報を利用する場合、本発明の料金プラン通知装置を設置するサービス提供者が作成したホームページの入力フォームにこの通信履歴情報を読み込ませるようにしてもよく、定形のファイルに以前の通信履歴情報を入力して通信端末等に送信し、通信端末は以前の通信履歴情報が記載された定形のファイルを編集し、データベースに送信することによっても実現できる。

【0083】

本発明では、通信端末ユーザは任意の利用条件を指定し、各料金プランにおいて通信料金をシミュレーションすることができる。

【0084】

通信端末は、ホームページの利用など公知の手段を使用して任意の利用条件をデータベースに設定する。任意の利用条件は、データベースに蓄積されている以前の通信履歴情報を流用することも可能である。

【0085】

データベースは通信端末から送信されてくる通信履歴情報を蓄積する。

【0086】

情報処理装置は、通信端末ユーザが指定した任意の利用条件、又はデータベースに蓄積されている以前の通信履歴情報、料金プラン、契約情報、割引情報を使用し、通信料金をシミュレーションし、通信端末ユーザに通知することができる。

【0087】

このシミュレーションとは、過去何時間とか特定の日等任意の期間の利用条件を元に、１ヶ月、１年分等の利用料金を全料金プランにおいて試算できる。これにより通信端末ユーザは種々の利用形態における利用料金を知ることができる。

【0088】

本発明では、通信端末ユーザは、情報処理装置で算出した、各料金プランの正確な使用料金、シミュレーション結果、及びサービス種別、通信先、通信時間、回数、情報量等の個別通信毎の料金内訳、品質統計情報等を下記に示す手段で入手することができる。

（１）電子データ：情報処理装置は通信端末ユーザの要求に応じて前記算出情報を、データベースから収集し、データファイル（テキスト、ＨＴＭＬ形式等）に変換して、Ｅメール、データファイルを通信端末ユーザのＥメールアドレスに送信する。また情報処理装置が前記算出情報をホームページに変換し、通信端末ユーザにホームページのアドレスを送

信し、通信端末ユーザはそのホームページのアドレスにアクセスして閲覧することにより前記情報を見ることができる。また情報処理装置が前記算出情報をデータファイルに変換して通信端末ユーザに送信し、通信端末ユーザはそのデータファイルを閲覧することにより前記算出情報を見ることができる。

【0089】

（２）前記以外の手段：情報処理装置は通信端末ユーザの要求に応じて、前記算出情報をデータベースから収集し、音声ガイダンスに変換することで通信端末ユーザに聞かせることができる。またその他に、明細書を作成して郵送したり、オペレータによる対応等により通信端末ユーザは前記算出情報を入手することができる。

【0090】

本発明では、通信端末ユーザは、情報処理装置が行う全ての処理、情報を伝送するタイミングを任意に設定することができる。これにより、通信料が安い時間帯での送信や、日、週、月、年単位等のある期間の通信履歴情報を送信するタイミング、自動又は手動、月に何回等の回数を設定することができる。これにより通信端末は、任意のタイミングで通信履歴情報をデータベースに送信することができる。

【0091】

また通信端末は、利用料金をシミュレーションさせるタイミング、シミュレーション結果を通知するタイミング等の各種タイミングをデータベースに登録することができる。

【0092】

情報処理装置は、前記タイミングで利用料金算出、シミュレーションを行い、通信端末ユーザに利用料金や、シミュレーション結果を通知する。

【0093】

本発明では、通信履歴情報や品質情報及び情報処理装置が送信するデータに優先度をつけることができ、これによりトラフィックを制御することができる。

【0094】

通信端末や情報処理装置では、公知の手段によりそれぞれが送信すべきデータの形式を変換して送信することができる。通信事業者は一般的に許容される伝送遅延を、映像＞音声＞パケットデータ（ＷＥＢアクセス、ファイル転送、Ｅメール等）の順に設定していることが多いので、通信履歴情報や品質情報、使用料金シミュレーション等の通信端末と情報処理装置で送受信する全ての情報を映像のフォーマットに変換して送れば、遅延時間は最小で送信できるが、その分トラフィックを圧迫することになる。反対にパケットデータに変換して送れば、遅延時間は多くなるが、その分トラフィックの隙間を利用して送信できるので、通信ネットワークのトラフィックに負担をあまりかけないようにできる。

【0095】

本発明では、使用料金算出、シミュレーションや品質情報を提供するのに通信費がかかるので、通信端末ユーザは、使用料金算出やシミュレーションに関連する情報を使用料金算出、シミュレーションする際に料金に含むか、含まないかをデータベースに設定することができる。もし「含まない」を選択した場合、情報処理装置は、純粋な通信にかかった使用料金を算出し、通信端末ユーザに送信する。このように通信端末ユーザは、純粋に通信にかかった料金のみを知ることができる。

【0096】

本発明では、通信端末ユーザは、情報処理装置で算出する通信先、通信時間、回数、情報量等の詳細な通信履歴毎の料金、事業者内・事業者間、比較プラン数、通知プラン数等のシミュレーション結果、料金プラン、通信履歴情報、割引情報等のシミュレーション条件の内容を、ユーザが任意に設定できる。

【0097】

これにより使用料金算出、シミュレーションにかかる通信費や情報処理装置がシミュレーションに要する時間を調整できる。

【0098】

通信端末ユーザは、使用料金算出、シミュレーション結果、シミュレーション条件の項

目のうち、任意の項目をデータベースに設定できる。これにより通信端末ユーザはどこまで正確に使用料金を算出するか設定することができる。当然、条件が多ければ通信履歴情報やシミュレーション結果等のデータ量は多くなり、その分通信費、情報処理装置が処理に要する時間は多くなる。

【0099】

情報処理装置は通信端末ユーザがデータベースに設定された条件を使用して使用料金算出、シミュレーションを行い通信端末ユーザに結果を送信する。

【0100】

本発明では、個人情報の秘密を保護するため、通信端末ユーザが送信する通信履歴情報及び情報処理装置において算出する使用料金算出、シミュレーション結果、品質情報等全てを暗号化して送信することができる。例えば通知端末では公知の暗号化機能を有するソフトを使用することができ、また情報処理装置は自身で暗号化機能を持つ。

【0101】

暗号化・復号化手段には一般に使用されている公開鍵暗号方式、秘密暗号方式等の暗号化手段や、ＩＤ、パスワード、電子署名等の認証機能手段が考えられる。

【0102】

暗号化手段を使用する場合は、通信端末のアプリケーションソフトと情報処理装置で同じ暗号化・復号化手段を持つ。また認証機能を使用する場合は、通信端末ユーザはデータベースにＩＤ、パスワード、電子署名等を登録しておき、情報処理装置はそれらの認証情報が一致していることが確認できたら通信端末ユーザからの情報を受信する。

【0103】

また通信端末ユーザは、情報処理装置から送信される認証情報と、予め情報処理装置から入手しておいた認証情報が一致していることが確認できたら、情報処理装置からの情報を受信する。

【0104】

本発明では、通信端末ユーザが設定する任意の使用料金設定を超えた、又は下回っている時に、通信端末ユーザにその旨を通知する機能を持つ。

【0105】

通信端末ユーザは、任意の使用料金と、その設定した使用料金を超えた、又は下回っている時に通知するようデータベースに設定する。情報処理装置はそれらの設定を認識し、通信端末ユーザから送信されてくる通信履歴情報から使用料金を算出し、データベースに設定されている使用料金を超えた、又は下回っている時に、通信端末ユーザに設定金額をいくら上回った、または下回っているかを通知する。

【0106】

本発明では、通信端末ユーザが契約している料金プランにおいて、無料通信料金が設定されている場合、通信端末ユーザに無料通信料金の残高、残り時間、残りパケットを通知する機能を持つ。

【0107】

通信端末ユーザは、データベースに無料通信料金の残高、残り時間、残りパケット数を通知させる時間、ベアラ毎の残高、残り時間、残りパケット数の割合等の内容を設定する。

【0108】

情報処理装置はそれらの設定を認識し、通信端末ユーザから送信されてくる通信履歴情報から使用料金を算出し、通信端末ユーザに、残高、残り時間、残りパケット数を通知する。

【0109】

通信端末ユーザは本発明が提供する、使用料金算出、シミュレーション、品質情報のうち、任意のサービスを選択することができる。

【0110】

通信端末ユーザは、シミュレーション内容、無料通信料金の算出、比較プラン数等デー

BNSDOCID: <JP____2006041989A__I_>

タベースに希望するサービスの種類、シミュレーション回数、品質情報等を受け取る回数、タイミングを設定する。

【0111】

情報処理装置はそれらの設定を認識し、通信端末ユーザから送信してくる通信履歴情報から使用料金、品質情報を算出し、通信端末ユーザの設定した日時に通信端末ユーザが要求した情報を送信する。

【0112】

本発明では、通信端末ユーザの加入者情報は公知のアプリケーションソフトやサービス提供者が作成するホームページを利用することでデータベースに登録、修正することができる。

【0113】

通信端末ユーザは、アプリケーションソフトを使用する場合は、アプリケーションソフトが提供するフォーマットに設定項目を入力し、データベースに送信する。ホームページを使用する場合は、通信端末ユーザが本サービス提供者が提供する加入者情報のホームページにアクセスし、必要事項を記入することで、データベースに通信端末ユーザの加入者情報を登録することができる。修正も同様の手段で可能である。

【0114】

本発明を使用すれば、通信端末ユーザは料金とサービス品質の両面から最適な料金プラン、通信事業者を選択することができる。また通信事業者は各ユーザの使用状況を詳細に把握することができ、適切な料金プランを検討する際に有効なデータや、サービスエリア拡充時に参考になる情報を得ることができる。

【図面の簡単な説明】

【0115】

【図1】本発明の一実施例構成図である。

【図2】本発明の品質統計情報説明図である。

【図3】本発明の時間毎の品質統計情報説明図である。

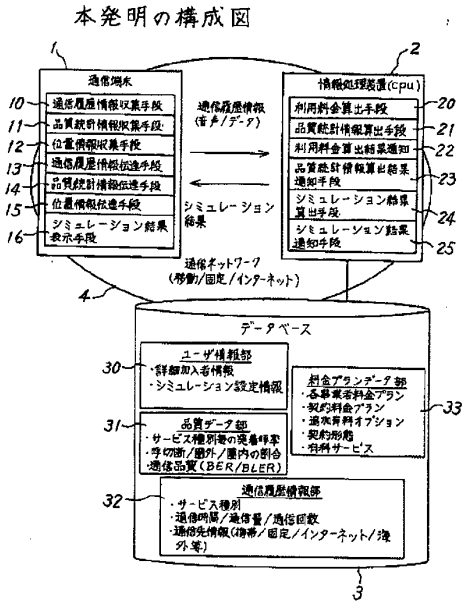
【符号の説明】

【0116】

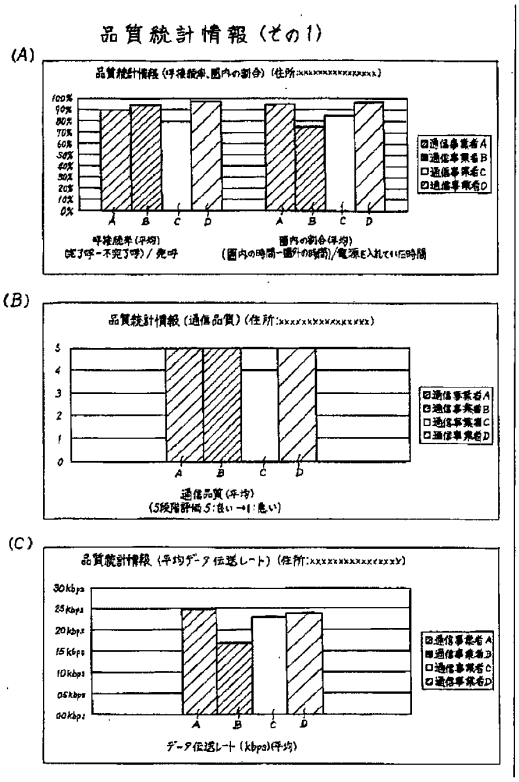
1　通信端末
2　情報処理装置
3　データベース
4　通信ネットワーク

BNSDOCID: <JP_____2006041989A__I_>

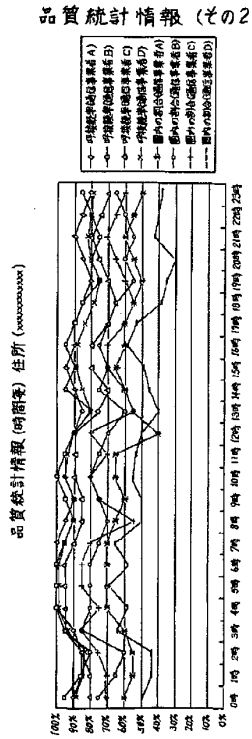
【図1】



【図2】



【図3】



BNSDOCID: <JP_____2006041989A__I_>

(72)発明者　片岡　康祐
東京都品川区南大井６丁目２２番７号　富士通ネットワークソリューションズ株式会社内

Ｆターム(参考) 5K025 AA08　BB06　CC01　JJ02　JJ16　JJ18

BNSDOCID: <JP_____2006041989A__I_>

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 289 326 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.03.2003 Bulletin 2003/10

(51) Int Cl.[7]: **H04Q 7/32**

(21) Application number: **01402259.4**

(22) Date of filing: **30.08.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **MOTOROLA, INC.**
Schaumburg, IL 60196 (US)

(72) Inventors:
- **Deloume, Pascal**
  31170 Tournefeuille (FR)
- **Garani, Pradeep**
  31000 Toulouse (FR)

(74) Representative: **Litchfield, Laura Marie et al**
Motorola European Intellectual Property Operations,
Midpoint - Alencon Link
Basingstoke, Hampshire RG21 7PL (GB)

(54) Method of verifying downloaded software and corresponding device

(57) The present invention relates to ensuring security for software downloads to a device, in which a smart card is used for storage of secure keys and for calculations using the secure keys. The result of the calculations using the smart card are passed to the device for comparison with calculations performed by the device on the downloaded software, to verify the downloaded software. Thus the security of the keys and calculations involving the secure keys are kept secure. Preferably root security keys stored in the smart card can be updated using communication system messaging protocols.

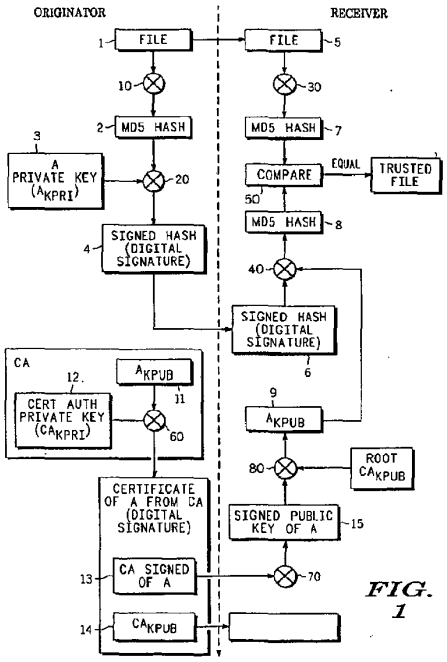


FIG. 1

EP 1 289 326 A1

Printed by Jouve, 75001 PARIS (FR)

BNSDOCID: <EP_____1289326A1_I_>

Description

[0001] The present invention relates to a method of verifying software downloaded from an originator to a device, and to a corresponding device. In particular, the invention relates to download verification in standardised execution environments such as the Mobile Execution Environment (MExE) and Java.

[0002] Increasingly it is becoming desirable for software to be downloaded to a portable device over the air. This allows the device to be upgraded with newly released software or enables new applications to be added to the device as these become available.

[0003] It is desirable that the device checks the authenticity of the downloaded software to determine whether, for example, the downloaded software has indeed been received from a trusted sender. In addition, it is desirable that the downloaded software should be restricted to a given domain, to avoid permission violation for the rest of the device.

[0004] This security can be ensured by keys, which are stored securely in the device such that they cannot be read or tampered with by applications except the security-checking environment. In addition it is desirable to update the keys periodically, and this must be done using a secure method.

[0005] Previously, it has been suggested to implement the security algorithms in software/hardware and then to protect them by hardware control on the processor of the terminal with memory management unit. However, this results in increased cost. In addition, the development of separate security hardware is undesirable.

[0006] The Mobile Execution Environment (MExE), which enables software download, is currently under standardisation. Three class marks are defined in the MexE environment. Class mark 1 relates to devices utilizing the Wireless Application Protocol (WAP); class mark 2 relates to devices, such as personal digital assistants (pda) or laptops using standard edition JAVA™ (J2SE); and class mark 3 relates to small devices, such as mobile telephones, using micro-edition JAVA™ (J2ME).

[0007] J2ME is being proposed as an environment for class mark 3 devices in MExE because of its small size, which makes it suitable for environments, such as the mobile communication environment for example, in which the available memory or processing power is limited and the size of files must be limited.

[0008] However, the security model for J2ME requires server-based pre-verification, in which a server inserts basic run-time security information in the software prior to download. The receiving device can then use the run-time security information to check the security of the download and verify the sender.

[0009] It is desirable to increase the security provided for software download, particularly in a MExE class mark 3 environment, so that server-based verification is avoided and software can be downloaded from a greater variety of sources.

[0010] According to a first aspect of the present invention, there is provided a method of verifying software downloaded from an originator to a device adapted to receive, in use, a smart card having at least one secure key stored therein, comprising: receiving software and security information relating to the received software; obtaining in the smart card a first calculation result from the security information using at least one secure key; obtaining in the device a second calculation result from calculations performed on the received software; and comparing in the device first and second calculation results to verify the received software.

[0011] According to a second aspect of the invention, there is provided a device comprising: communication means for receiving software and security information relating to the received software; smart card interface means for passing the security information to a smart card coupled to the smart card interface means and for receiving from the smart card a first calculation result obtained from the security information by the smart card using at least one security key; means for obtaining a second calculation result from calculations performed on the received software; means for comparing first and second calculation results to verify the received software.

[0012] For a better understanding of the present invention, and to show how it may be brought into effect reference will now be made, by way of example to the accompanying drawings in which:

Figure 1 illustrates a known file transfer verification procedure;
Figure 2 shows a communication device;
Figure 3 illustrates a download verification procedure in accordance with the invention;
Figure 4 illustrates message creation for transfer of the root key in accordance with the invention;
Figure 5 illustrates update of the root key in accordance with the invention

[0013] The present invention is described with reference to the use of RSA cryptography. The RSA cryptography algorithm and principle are well known and therefore will not be explained in detail in this document. As will be apparent to a skilled person, other cryptography techniques may also be used in accordance with the invention.

[0014] Figure 1 illustrates a known file transfer verification procedure, for verifying the authenticity of a file transferred from an originator to a receiver. The principle behind this procedure is that in addition to the transfer of the file 1 a second piece of information which is related to both the file 1 and the originator is also transferred between the originator and the receiver, which information enables the receiver to confirm that the file comes from the originator. In addition, the receiver possesses or is passed a third piece of information, which enables

BNSDOCID: <EP_____1289326A1_I_>

the receiver to confirm that the originator can be trusted and that it is therefore safe to execute the downloaded file.

[0015] In the illustrated procedure the originator generates the second piece of information by performing an MD5 hash operation 10 on the file 1 to be transferred to create an MD5 hash result 2. The MD5 hash operation is well known and will not be explained further. The MD5 hash result 2 is uniquely dependent on the file 1 and can be used to verify file 1.

[0016] Next the originator performs an RSA algorithm operation 20 on the MD5 hash result 2 using the private key of the originator (A_{KPRI}) 3 to generate a signed hash (or digital signature) 4. The signed hash 4 thus depends upon the file and is signed as having been originated by A and can therefore act as the second piece of information mentioned above. The file 1 and the signed hash 4 are transferred to the receiver resulting in a received file 5 and a received signed hash 6.

[0017] In order to verify the received file, the receiver independently generates two versions of the MD5 hash result. The first MD5 hash result 7 is generated from the received file 5 using a MD5 hash operation 30, and the second MD5 hash result 8 is obtained from the received signed hash 6 by performing an RSA operation 40 on the received signed hash 6 using the public key of the originator A (A_{Kpub}) 9 held by the receiver. The first MD5 hash result 7 and the second MD5 hash result 8 are compared in a comparison operation 50 and if they are found to be equal, the received file 5 is authenticated and can be executed.

[0018] In order for the above authentication scheme to work, the receiver must have authenticated access to the public key of the originator A (A_{Kpub}). This is achieved in the illustrated procedure through the use of a certification authority. The certification authority is trusted by the receiver, such that received information signed by the certification authority is trusted by the receiver.

[0019] Therefore, as shown the certification authority performs an RSA algorithm operation 60 on the public key of the originator (A_{KPub}) 11 using the private key of the certification authority (CA_{KPRI}) 12 resulting in a signed key 13 of the originator A. The signed key 13 and the certification authority public key (CA_{Kpub}) 14 are transferred to the receiver. As shown, if necessary the signed key 13 undergoes a certificate chain analysis operation 70 to obtain the received signed public key 15 of the originator A.

[0020] A certificate chain analysis operation is required if the certificate authority CA is not known by the receiver. In this case, the certificate authority is requested to provide its public key signed by a further certificate authority using the private key of the further certificate authority. If the further certificate authority is trusted by the receiver, the receiver will be able to use the public key of the further signature authority to verify that the public key of the signed authority has been signed by the private key of the further signature authority. The receiver can then trust the certificate authority and can use the received certificate authority public key. If the further certificate authority is not trusted by the receiver, use must be made of an additional certificate authority.

[0021] The receiver has stored therein a root certification authority public key. The root certification authority is the most trusted by the receiver, and ultimately the stored public key of the root certification authority can be used to verify all other certification authorities in a certificate chain situation.

[0022] The receiver then performs an RSA operation 80 on the resulting signed public key of the originator (A_{KPub}) (15) using the root certification authority public key (Root CA_{KPub}) to obtain the public key of the originator (A_{KPub}) 9. The public key of the originator (A_{KPub}) 9 is then used in the RSA operation 40 as described above.

[0023] The present invention is described below with reference to a communication device, such as a mobile telephone. However, it will be clear to a skilled person that the present invention is also applicable to other devices. An exemplary communication device 200 is now described with reference to Figure 2.

[0024] The communication device 200 shown in Figure 2 comprises a communication interface 210 coupled to an antenna 220 and to a processor 230. The processor 230 and the communication interface 210 are also coupled to volatile memory 240 and to a non-volatile memory 250. A smart card 260 is coupled to a smart card interface 270, which is also coupled to the processor 230. The smart card is equipped with its own processor 280 and memory 290.

[0025] The communication interface 210 comprises the necessary components to convert radio frequency signals for the communication device 200 received by the antenna 220 to digital signals to be stored in volatile memory 240 and/or non-volatile memory 250 and/or to be processed by processor 230, and to convert digital signals from the memories 240 and 250 and/or the processor 230 to radio frequency signals to be transmitted by the antenna 220. Thus communication interface 210 comprises radio frequency transmitter and receiver means and signal processor means, for example.

[0026] The volatile memory 240 and non-volatile memory 250 are used for storing program and other data for operation of the communication device 200.

[0027] The smart card is preferably a subscriber smart card (SIM) holding subscriber information used by the communication device 200, for example a Subscriber Identity Module card as currently used in the Global System for Mobile Communications (GSM system) and in use or proposed for other communication systems. However, it is possible that the smart card 260 may be another type of smart card received in the communication device instead of, or preferably in addition to a SIM card, for example an electronic commerce smart card.

BNSDOCID: <EP_____1289326A1_I_>

[0028] As indicated above, the smart card is equipped with its own processor 280 and memory 290, and is capable of storing information therein and is also capable of carrying out operations or calculations on data received from the processor 230 via smart card interface 270 and of providing data or the results of such calculation to the processor 230 via smart card interface 270.

[0029] The smart card is preferably removably receivable in the communication device, for example by means of the provision of a slot in the housing of the communication device 200.

[0030] It will be appreciated by a skilled person that other components or arrangements of components within the communication device 200 are possible within the scope of the invention.

[0031] The secure download procedure in accordance with the invention will now be described with reference to Figure 3. In Figure 3 operations or data corresponding to operations or data in Figure 1 have been given similar reference numerals.

[0032] Figure 3 illustrates the download of an executable J2ME file in a MExE environment from an originator A to a device such as the communication device 200 described above with reference to Figure 2. As shown in Figure 3, box 3260 represents operations carried out and data stored in the smart card 260 of the communication device 200 shown in Figure 2, and the remaining operation and data storage is carried out in the rest of the communication device 200 shown in Figure 2.

[0033] As illustrated in Figure 2, the smart card 260 has no direct communications capability. Instead, the relevant data received by the communication device is passed by the processor 230 to the smart card 260 for storage therein and operation thereon.

[0034] In the procedure illustrated in Figure 3, the originator A performs an MD5 hash operation 310 on a file 31 to be transferred to create an MD5 hash result 32. As explained above, the MD5 hash result 32 is uniquely dependent on the file 31 and can be used to verify file 31.

[0035] Next the originator A performs an RSA algorithm operation 320 on the MD5 hash result 32 using the private key of the originator (A_{KPRI}) 33 to generate a signed hash 34. The signed hash 34 thus depends upon the file and is signed as having been originated by A and can therefore act as the second piece of information mentioned above. The file 31 and the signed hash 34 are then sent to the communication device 200 resulting in a received file 35 and a received signed hash 36. File 35 is received using antenna 220 and communication interface 210 and is stored by the processor 230 in the volatile memory 240. In contrast, the signed hash 34 is received using antenna 220 and communication interface 210 and is sent by the processor 230 to the smart card 260 via smart card interface 270 and is stored in the smart card memory 290.

[0036] As described above, in order to verify the received file, two versions of the MD5 hash result must be independently generated and compared. The first MD5 hash result 37 is generated by the communication device processor 230 from the received file 35 using a MD5 hash operation 330.

[0037] The second MD5 hash result 38 is obtained by the smart card from the received signed hash 36. The smart card processor 280 performs an RSA operation 340 on the received signed hash 36 stored in the smart card memory 390 using the public key of the originator A (A_{Kpub}) 39 stored in the smart card memory 290, as will be explained later.

[0038] The second MD5 hash result 38 is passed by the smart card processor 280 to the communication device processor 230 and the communication device processor 230 compares the first MD5 hash result 37 and the second MD5 hash result 38, calculated in the smart card 260, in a comparison operation 350. If the first MD5 hash result 37 and the second MD5 hash result 38 are found to be equal, the received file 35 is authenticated and can be executed.

[0039] In this arrangement, the smart card 260 must have authenticated access to the public key of the originator A (A_{Kpub}). This is achieved in the illustrated procedure according to Figure 3 through the use of the root certification authority public key stored in the smart card memory 290. The root certification authority is trusted by the communications device, such that received information signed by the certification authority is trusted.

[0040] In this context, there may be more than one root certification authority. For example in the context of a mobile telephone the manufacturer and/or the operator can act as a root authority. In addition, it is possible to specify one or more trusted third parties as root certification authorities. The public key for each of the root certification authorities (eg the operator public root key (OPRK); the manufacturer public root key (MPRK); and third party public root key (TPRK)) is stored in the smart card of the communication device 200, for example during provisioning of a mobile telephone SIM card.

[0041] In order that the smart card 260 has authenticated access to the public key of the originator A (A_{Kpub}), as shown the root certification authority performs an RSA algorithm operation 360 on the public key of the originator (A_{KPub}) 311 using the private key of the certification authority ($RootCA_{KPRI}$) 312 resulting in a certificate from A 321 signed by the root certification authority. This certificate 321 is sent to the communications device 200, is received using antenna 220 and communication interface 210 and is sent by the processor 230 to the smart card 260 via smart card interface 270 and is stored in the smart card memory 290 as certificate 322.

[0042] The Root certification authority public key ($RootCA_{KPub}$) 332 is already stored in the smart card memory 290, as indicated above. The smart card processor can perform an RSA operation 380 on the received certificate 322 using the Root Certification Authority public key ($RootCA_{KPub}$) 332 to obtain the public

BNSDOCID: <EP_____1289326A1_I_>

key of the originator A (A_{Kpub}) 39. The smart card processor can then use the obtained public key of the originator A (A_{Kpub}) 39 and the received signed hash 36 in RSA operation 340 to obtain the smart card MD5 hash value 38, as outlined above.

[0043] Also shown in Figure 3 is the transfer of the Root Certification Authority public key ($RootCA_{KPub}$) 331 to the communications device for storage in the smart card memory as Root Certification Authority public key ($RootCA_{KPub}$) 332. It is desirable to update the root certification authority keys periodically in a secure manner otherwise the security of the system will be compromised.

[0044] A preferred mechanism for the secure transfer of a Root public key (for example OPRK, MPRK, TPRK) using communication system messaging technology will now be explained with reference to Figures 4 and 5.

[0045] Figure 4 illustrates message creation for transfer of a root key, for example the operator public root key (OPRK), to the smart card 360 in accordance with the invention. In this exemplary arrangement, the update is achieved using a SMS message as provided in the GSM/UMTS systems, although other messaging techniques could be used.

[0046] An RSA operation is performed on the new OPRK 41 with the operator's private root key 42 corresponding to the old OPRK stored in the smart card 360. As mentioned earlier, the old OPRK may have been stored in the smart card 360 during provisioning, or during a previous update of the root key. The resulting signed new operator public root key 44 is included in an SMS message 45 to be sent to the communication device. The SMS message 45 has an SMS header portion 451 and SMS download command 452 in addition to the signed new operator public root key 44. The SMS message in encrypted by the communication system prior to being sent to the communication device.

[0047] Figure 5 illustrates update of the root key in the communication device in accordance with an embodiment of the invention. In this exemplary embodiment of the invention, the SMS message 45 sent by the network 500 to the communication device 200 is passed to the smart card 260. Once the encrypted SMS message 45 is received in the smart card 260, the smart card 260 undertakes an SMS message analysis and memory update procedure 51.

[0048] In the SMS message analysis and memory update procedure 51 the SMS message is initially decrypted and the SMS message is analysed. The download command 452 instructs the smart card 260 that a new OPRK is being sent to the smart card 260. The smart card 260 performs an RSA operation on the received signed new OPRK using the old OPRK already stored in the smart card 260 to verify the identity of the sender. The OPRK stored in the smart card can then be updated using the new value. Preferably a confirmation message 52 is sent from the smart card 260 to the network using the communication interface 210 of the communication device 200.

[0049] Although the update of the operator public root key (OPRK) has been described above, it would be possible to update any root key stored in the smart card in the same way.

[0050] In accordance with an alternative embodiment of the invention, the manufacturer root public key may be stored partially in the smart card memory and partially in the communications device memory. This arrangement is more secure since the communication device then contributes to ensuring the security of download in the manufacturer domain using the manufacturer root public key. This helps to prevent an insecure smart card from changing the manufacturer public root key via download authorization.

[0051] Thus the present invention proposes a solution to ensuring security for software downloads to a device, in which a smart card is used for storage of secure keys and for calculations using the secure keys. The result of the calculations using the smart card are passed to the device for comparison with calculations performed by the device on the downloaded software, to verify the downloaded software.

[0052] Since the secure keys are stored on the smart card and calculations involving the secure keys are performed by the smart card, the security of the secure keys can be ensured. In addition, the result of the calculation performed on the received file by the device is not passed to the smart card.

[0053] As will be apparent to a skilled person, the invention could be implemented in a different form from that shown herein, and so the invention is intended to encompass all arrangements and variations within the scope of the appended claims.

Claims

1. A method of verifying software downloaded from an originator to a device adapted to receive, in use, a smart card having at least one secure key stored therein, comprising:

   receiving software and security information relating to the received software;
   obtaining in the smart card a first calculation result from the security information using at least one secure key;
   obtaining in the device a second calculation result from calculations performed on the received software; and
   comparing in the device first and second calculation results to verify the received software.

2. The method as claimed in claim 1, further comprising the steps of;

   receiving additional signed originator key infor-

BNSDOCID: <EP_____1289326A1_I_>

mation;

obtaining, in the smart card, originator key information from the received signed originator key information using a root security key stored therein; and

obtaining in the smart card the first calculation result from the security information using the originator key information.

3. The method as claimed in claim 2 wherein the root security key stored in the smart card is updated by

receiving a root security key update message containing a new root security key;

verifying the new root security key using the existing root security key stored in the smart card;

storing the new root security key in the smart card.

4. The method as claimed in claim 2 or 3, wherein part of the root security key is stored in the smart card and part of the root security key is stored in the device.

5. The method as claimed in any preceding claim, wherein the smart card is a Subscriber Identity Module (SIM) card

6. A device comprising

communication means for receiving software and security information relating to the received software;

smart card interface means for passing the security information to a smart card coupled to the smart card interface means and for receiving from the smart card a first calculation result obtained from the security information by the smart card using at least one security key;

means for obtaining a second calculation result from calculations performed on the received software;

means for comparing first and second calculation results to verify the received software.

7. The device as claimed in claim 6 wherein

the communications means also receives additional signed originator key information; and

the smart card interface also passes the additional signed originator key information to the smart card, which obtains originator key information from the received signed originator key information using a root security key stored therein; and obtains the first calculation result from the security information using the originator key information.

8. The device as claimed in claim 7 wherein

the communications means also receives a root security key update message containing a new root security key; and

the smart card interface passes the root security key update message to the smart card, which verifies the new root security key using the existing root security key stored in the smart card; and stores the new root security key in the smart card.

9. The device as claimed in claim 7 or 8, wherein the device comprises storage means and part of the root security key is stored in the smart card and part of the root security key is stored in the storage means.

10. The device as claimed in one of claims 6-9, wherein the smart card is a Subscriber Identity Module (SIM) card.

BNSDOCID: <EP_____1289326A1_I_>

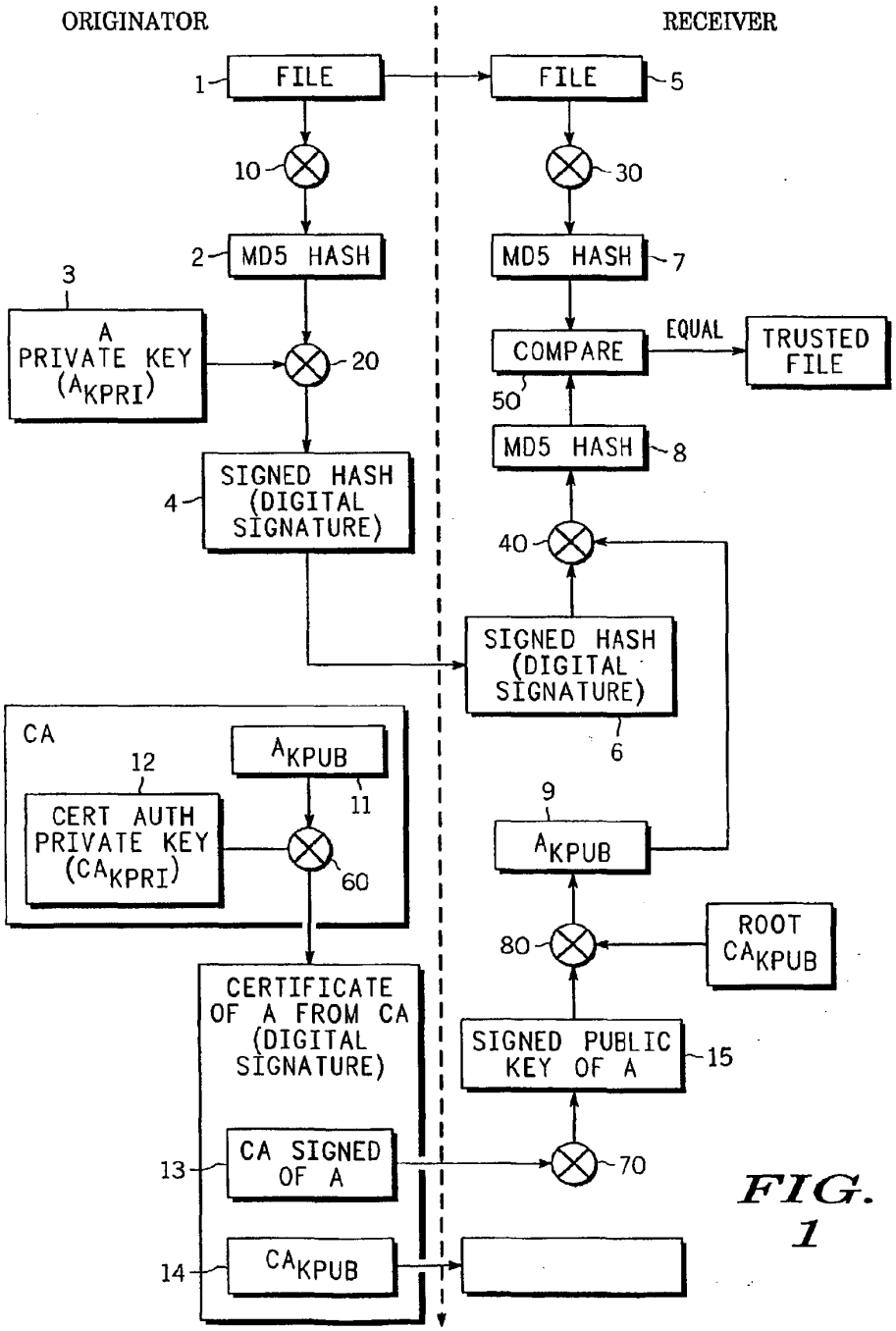


FIG. 1

BNSDOCID: <EP_____1289326A1_I_>

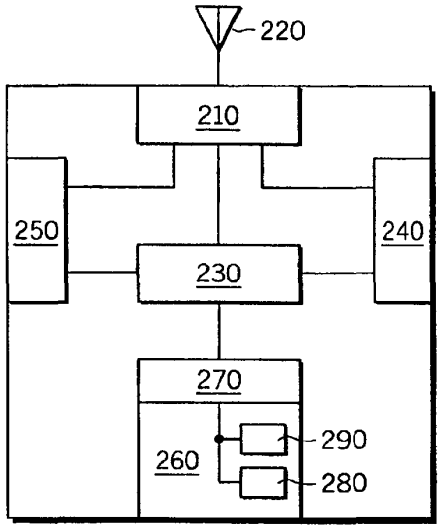


FIG. 2

BNSDOCID: <EP_____1289326A1_I_>

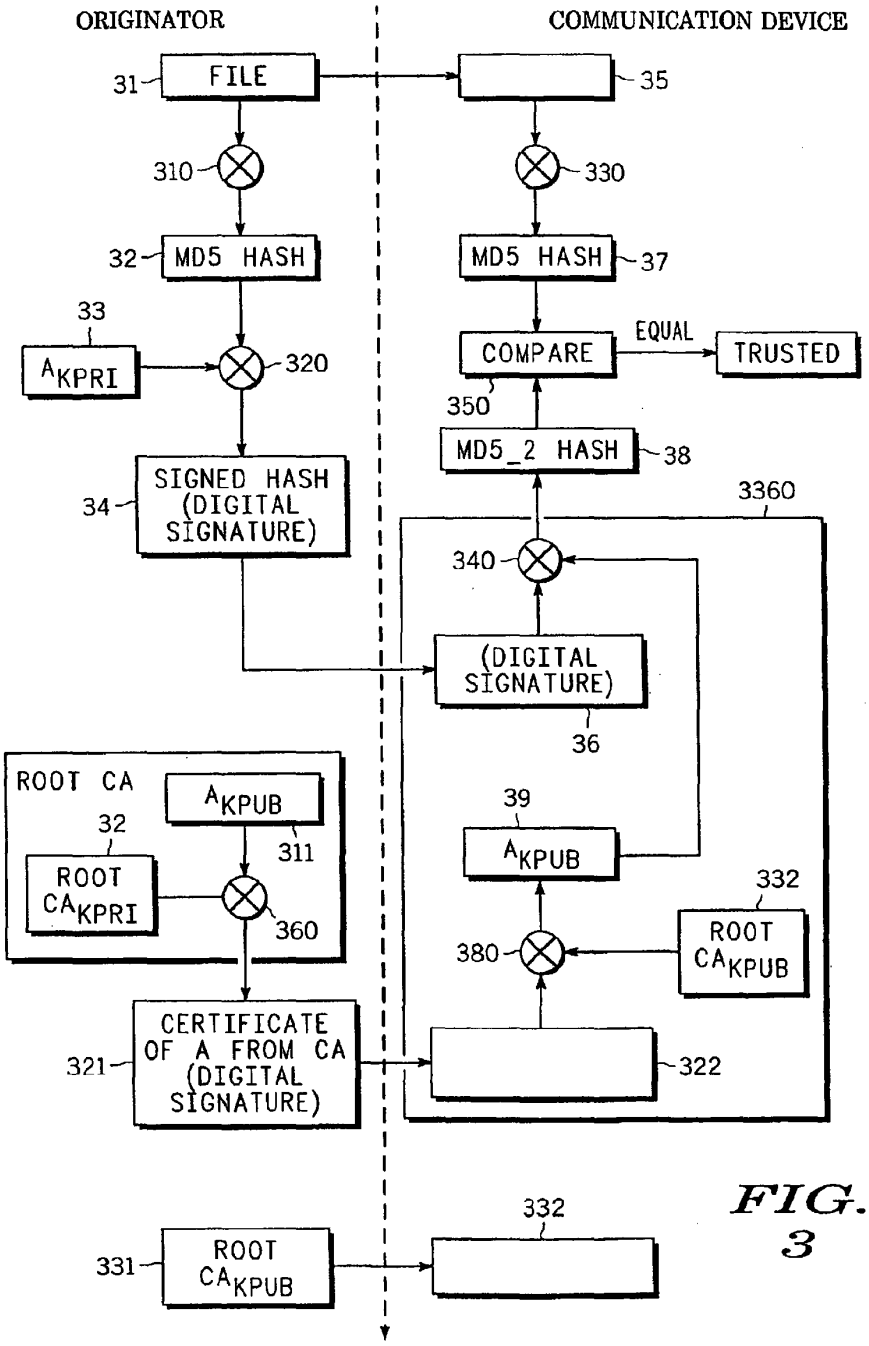


FIG. 3

BNSDOCID: <EP_____1289326A1_I_>

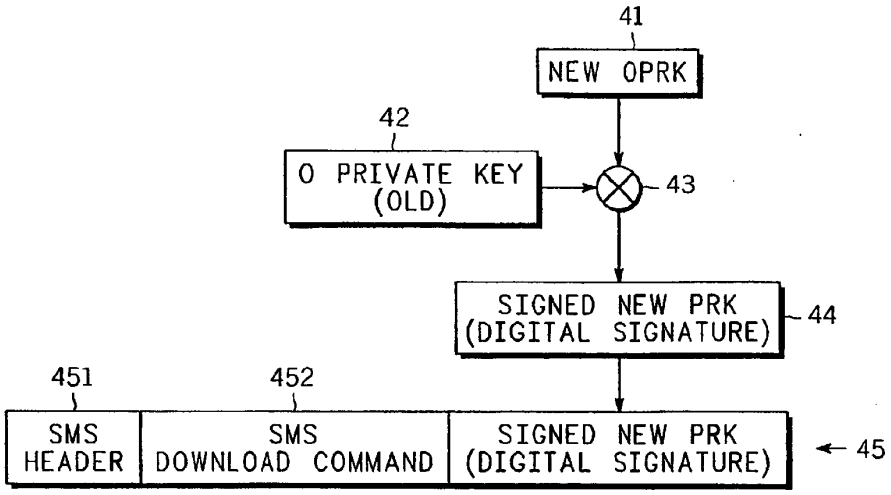
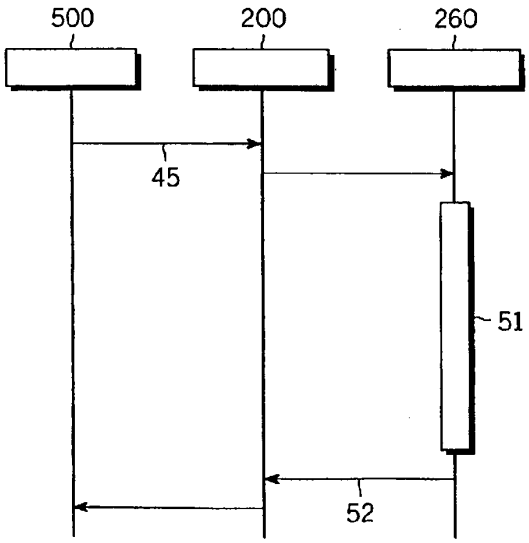


FIG. 4

FIG. 5



BNSDOCID: <EP_____1289326A1_I_>

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 40 2259

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 6 124 799 A (PARKER JOHN PATRICK) 26 September 2000 (2000-09-26) * the whole document *	1-4,6-9	H04Q7/32
X	EP 0 562 890 A (HUTCHISON MICROTEL LIMITED) 29 September 1993 (1993-09-29) * column 4, line 30 - column 5, line 32 *	1,6	
A	EP 1 124 401 A (LUCENT TECHNOLOGIES INC) 16 August 2001 (2001-08-16) * paragraphs '0002!-'0019! * * abstract; claims 1-13 *	2-4,7-9	
A	EP 0 977 452 A (LUCENT TECHNOLOGIES INC) 2 February 2000 (2000-02-02) * the whole document *	2-4,7-9	
A	EP 0 463 384 A (CIT ALCATEL) 2 January 1992 (1992-01-02) * the whole document *	1,6	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	22 February 2002	Coppieters, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP_____1289326A1_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 40 2259

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-02-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6124799 A	26-09-2000	US 5864757 A	26-01-1999
		AU 715488 B2	03-02-2000
		AU 1409997 A	03-07-1997
		CA 2239550 A1	19-06-1997
		EP 0867099 A2	30-09-1998
		JP 11501182 T	26-01-1999
		JP 3080409 B2	28-08-2000
		WO 9722221 A2	19-06-1997
EP 0562890 A	29-09-1993	AT 193965 T	15-06-2000
		DE 69328847 D1	20-07-2000
		DE 69328847 T2	07-12-2000
		EP 0562890 A1	29-09-1993
		ES 2149801 T3	16-11-2000
EP 1124401 A	16-08-2001	AU 1828001 A	16-08-2001
		BR 0100191 A	09-10-2001
		CN 1308472 A	15-08-2001
		EP 1124401 A2	16-08-2001
		JP 2001251292 A	14-09-2001
EP 0977452 A	02-02-2000	US 6243811 B1	05-06-2001
		BR 9902942 A	09-05-2000
		CN 1249588 A	05-04-2000
		EP 0977452 A2	02-02-2000
		JP 2000083017 A	21-03-2000
		TW 428409 B	01-04-2001
EP 0463384 A	02-01-1992	FR 2662878 A1	06-12-1991
		AT 135519 T	15-03-1996
		CA 2043290 A1	01-12-1991
		DE 69117814 D1	18-04-1996
		DE 69117814 T2	25-07-1996
		EP 0463384 A1	02-01-1992
		ES 2084726 T3	16-05-1996
		FI 912548 A	01-12-1991
		JP 3054225 B2	19-06-2000
		JP 4233341 A	21-08-1992
		NO 178597 B	15-01-1996
		US 5303285 A	12-04-1994

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP_____1289326A1_I_>

Electronic Patent Application Fee Transmittal					
Application Number:	14082040				
Filing Date:	15-Nov-2013				
Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY				
First Named Inventor/Applicant Name:	Gregory G. Raleigh				
Filer:	James E. Harris/Ann Taylor				
Attorney Docket Number:	RALEP032C1				
Filed as Small Entity					
Filing Fees for Utility under 35 USC 111(a)					
Description		**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:					
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($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt	
EFS ID:	28303504
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	08-FEB-2017
Filing Date:	15-NOV-2013
Time Stamp:	16:42:56
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$90
RAM confirmation Number	020917INTEFSW00003409505876
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P032C1_IDS1.pdf	1054319 df545a16ff0cfdca7b2df576f47352779352ab6d	no	5
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	P032C1_IDS2.pdf	1054265 198570e13407c6acaebf438f0b56af72fc1ac71a	no	5
Warnings:					
Information:					
3	Foreign Reference	2091.pdf	4030163 9f5a695d3972f432ff9791f8b2ac99ef7cbca74d	no	16
Warnings:					
Information:					
4	Foreign Reference	2092.pdf	2382529 5c57dc228f491cd9301830aad5e4493f4c99b261	no	12
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30661 c7deb7f3a4f4111c4cd28f870c15d1a839ffc674	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	8551937		

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.

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

106963 7590 01/31/2017

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER
RUDY, ANDREW J

ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 01/31/2017

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

TITLE OF INVENTION: DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	05/01/2017

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

106963 7590 01/31/2017
Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

TITLE OF INVENTION: DEVICE-ASSISTED SERVICES FOR PROTECTING NETWORK CAPACITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	05/01/2017

EXAMINER	ART UNIT	CLASS-SUBCLASS
RUDY, ANDREW J	3687	709-224000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
❑ Issue Fee
❑ Publication Fee (No small entity discount permitted)
❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
❑ A check is enclosed.
❑ Payment by credit card. Form PTO-2038 is attached.
❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
❑ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
❑ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
❑ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/082,040	11/15/2013	Gregory G. Raleigh	RALEP032C1	1015

106963 7590 01/31/2017

Headwater Research LLC
1011 Pruitt Place
Tyler, TX 75703

EXAMINER	
RUDY, ANDREW J	

ART UNIT	PAPER NUMBER
3687	

DATE MAILED: 01/31/2017

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. 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 1.14. This collection is estimated to take 12 minutes 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, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. 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.

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 another 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.

Notice of Allowability	Application No. 14/082,040	Applicant(s) RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *December 1, 2016 Amendment*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1,5,8-21 and 24-30*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Applicant cancelled claims 2-4, 6, 7, 22 and 23.

3. Further pertinent references of interest are noted on the attached PTO-892.

4. Applicant's December 1, 2016 Information Disclosure Statement (IDS) has been reviewed. Note the attached IDS.

Allowable Subject Matter

5. Claims 1, 5, 8-21 and 24-30 are allowed.

6. The following is an examiner's statement of reasons for allowance: Applicant's December 1, 2016 Amendment regarding claims 1, 5, 8-21 and 24-30 have been reviewed. Claims 1, 5, 8-21 and 24-30 are now allowed as all the cited prior art, either alone or in combination, does not disclose Applicant's inventive claim language.

Claims 1, 5, 8-21 and 24-30 have been reviewed in light of Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 573 U. S. ___ (2014) and are not deemed invalidated by such.

Claims 1, 5, 8-21 and 24-30 are determined to be directed to patent-eligible subject matter and the Examiner does not consider any of the pending claims to be directed to an abstract idea. Even if the Examiner were to identify an abstract idea for any claim, then under a further analysis under Alice all claims would still be found to be patent eligible for the following reasons. The Examiner finds that when all of the elements of each claim are considered individually and as an ordered combination, each claim contains an inventive concept which is directed to an application, a particular application, or a special application, of the identified abstract idea. Further the Examiner finds that issuance of a patent for any claim would not preempt the identified abstract idea, or the field of the identified abstract idea.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW JOSEPH RUDY whose telephone number is (571)272-6789. The examiner can normally be reached on Monday thru Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Fahd A. Obeid can be reached on 571-270-3324. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ANDREW JOSEPH RUDY/
Primary Examiner
Art Unit 3687

Notice of References Cited	Application/Control No. 14/082,040	Applicant(s)/Patent Under Reexamination RALEIGH ET AL.	
	Examiner ANDREW JOSEPH RUDY	Art Unit 3687	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6,115,823 A	09-2000	Velasco; Francisco	G06F1/3203	710/16
*	B	US-7,505,795 B1	03-2009	Lim; Vincent Cheekiat	H04W52/0232	340/7.38
*	C	US-9,326,173 B2	04-2016	Luft; Achim	H04W4/00	1/1
*	D	US-2009/0065571 A1	03-2009	Jain; Deepak	G06K19/07739	235/379
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5617539	A	1997-04-01	Ludwig et al.	
	2	6141565	A	2000-10-31	Feuerstein et al.	
	3	6401113	B2	2002-06-04	Lazaridis et al.	
	4	6510152	B1	2003-01-21	Gerszberg et al.	
	5	6535855	B1	2003-03-18	Cahill et al.	
	6	6542500	B1	2003-04-01	Gerszberg et al.	
	7	6546016	B1	2003-04-08	Gerszberg et al.	
	8	6570974	B1	2003-05-27	Gerszberg et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	6601040	B1	2003-07-29	Kolls, H. Brock	
	10	6636721	B2	2003-10-21	Threadgill et al.	
	11	6654786	B1	2003-11-25	Fox et al.	
	12	6690918	B2	2004-02-10	Evans et al.	
	13	6959393	B2	2005-10-25	Hollis et al.	
	14	7082422	B1	2006-07-25	Zirngibl et al.	
	15	7095754	B2	2006-08-22	Benveniste, Mathilde	
	16	7133386	B2	2006-11-07	Holur et al.	
	17	7136361	B2	2006-11-14	Benveniste, Mathilde	
	18	7151764	B1	2006-12-19	Heinonen et al.	
	19	7177919	B1	2007-02-13	Truong et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7191248	B2	2007-03-13	Chattopadhyay et al.	
	21	7272660	B1	2007-09-18	Powers et al.	
	22	7369848	B2	2008-05-06	Jiang, Yue Jun	
	23	7369856	B2	2008-05-06	Ovadia, Shlomo	
	24	7409569	B2	2008-08-05	Illowsky et al.	
	25	7428750	B1	2008-09-23	Dunn et al.	
	26	7440433	B2	2008-10-21	Rink et al.	
	27	7486658	B2	2009-02-03	Kumar, Rajneesh	
	28	7562213	B1	2009-07-14	Timms, Natalie	
	29	7577431	B2	2009-08-18	Jiang, Yue Jun	
	30	7599714	B2	2009-10-06	Kuzminskiy, Alexandr	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	7602746	B2	2009-10-13	Calhoun et al.	
	32	7610047	B2	2009-10-27	Hicks III et al.	
	33	7643411	B2	2010-01-05	Andreasen et al.	
	34	7657920	B2	2010-02-02	Arseneau et al.	
	35	7660419	B1	2010-02-09	Ho, Jin-Meng	
	36	7661124	B2	2010-02-09	Ramanathan et al.	
	37	7664494	B2	2010-02-16	Jiang, Yue Jun	
	38	7719966	B2	2010-05-18	Luft et al.	
	39	7724716	B2	2010-05-25	Fadell, Anthony M.	
	40	7770785	B2	2010-08-10	Jha et al.	
	41	7817983	B2	2010-10-19	Cassett et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	7873001	B2	2011-01-18	Silver, Andrew	
	43	7979069	B2	2011-07-12	Hupp et al.	
	44	8036387	B2	2011-10-11	Kudelski et al.	
	45	8044792	B2	2011-10-25	Orr et al.	
	46	8065365	B2	2011-11-22	Saxena et al.	
	47	8085808	B2	2011-12-27	Brusca et al.	
	48	8125897	B2	2012-02-28	Ray et al.	
	49	8132256	B2	2012-03-06	Bari, Farooq	
	50	8140690	B2	2012-03-20	Ly et al.	
	51	8145194	B2	2012-03-27	Yoshikawa et al.	
	52	8151205	B2	2012-04-03	Follmann et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8191106	B2	2012-05-29	Choyi et al.	
	54	8194549	B2	2012-06-05	Huber et al.	
	55	8194581	B1	2012-06-05	Schroeder et al.	
	56	8195153	B1	2012-06-05	Frencel et al.	
	57	8219134	B2	2012-07-10	Maharajh et al.	
	58	8271025	B2	2012-09-18	Brisebois et al.	
	59	8291439	B2	2012-10-16	Jethi et al.	
	60	8307095	B2	2012-11-06	Clark et al.	
	61	8320902	B2	2012-11-27	Moring et al.	
	62	8325906	B2	2012-12-04	Fullarton et al.	
	63	8340628	B2	2012-12-25	Taylor et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	64	8363799	B2	2013-01-29	Gruchala et al.	
	65	8380247	B2	2013-02-19	Engstrom	
	66	8402165	B2	2013-03-19	Deu-Ngoc et al.	
	67	8412798	B1	2013-04-02	Wang, Frank C.	
	68	8418168	B2	2013-04-09	Tyhurst et al.	
	69	8448015	B2	2013-05-21	Gerhart, David	
	70	8494559	B1	2013-07-23	Malmi	
	71	8503358	B2	2013-08-06	Hanson et al.	
	72	8505073	B2	2013-08-06	Taglienti et al.	
	73	8521775	B1	2013-08-27	Poh et al.	
	74	8531954	B2	2013-09-10	McNaughton et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	75	8538421	B2	2013-09-17	Brisebois et al.	
	76	8543814	B2	2013-09-24	Laitinen et al.	
	77	8600895	B2	2013-12-03	Felsher, David Paul	
	78	8639215	B2	2014-01-28	McGregor et al.	
	79	8670752	B2	2014-03-11	Fan et al.	
	80	8675852	B2	2014-03-18	Maes, Stephane H.	
	81	8700729	B2	2014-04-15	Dua, Robin	
	82	8719397	B2	2014-05-06	Levi et al.	
	83	8731519	B2	2014-05-20	Flynn et al.	
	84	8744339	B2	2014-06-03	Halfmann et al.	
	85	8787249	B2	2014-07-22	Giaretta et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	86	8811338	B2	2014-08-19	Jin et al.	
	87	8819253	B2	2014-08-26	Simeloff et al.	
	88	8837322	B2	2014-09-16	Venkataramanan et al.	
	89	8838686	B2	2014-09-16	Getchius, Jeffery M.	
	90	8838752	B2	2014-09-16	Lor et al.	
	91	8855620	B2	2014-10-07	Sievers et al.	
	92	8862751	B2	2014-10-14	Faccin et al.	
	93	8898748	B2	2014-11-25	Burks et al.	
	94	8908516	B2	2014-12-09	Tzamaloukas et al.	
	95	8943551	B2	2015-01-27	Ganapathy et al.	
	96	8971841	B2	2015-03-03	Menezes et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	97	8971912	B2	2015-03-03	Chou et al.	
	98	8995952	B1	2015-03-31	Baker et al.	
	99	9030934	B2	2015-05-12	Shah et al.	
	100	9032427	B2	2015-05-12	Gallant et al.	
	101	9173090	B2	2015-10-27	Tuchman et al.	
	102	9282460	B2	2016-03-08	Souissi, Slim Salah	
	103	9325737	B2	2016-04-26	Gutowski et al.	
	104	9344557	B2	2016-05-17	Gruchala et al.	
	105	9367680	B2	2016-06-14	Mahaffey et al.	
	106	9413546	B2	2016-08-09	Meier et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020120370	A1	2002-08-29	Parupudi et al.	
	2	20020138599	A1	2002-09-26	Dilman et al.	
	3	20030184793	A1	2003-10-02	Pineau, Richard A.	
	4	20040054779	A1	2004-03-18	Takeshima et al.	
	5	20040176104	A1	2004-09-09	Arcens, Suzanne	
	6	20040225561	A1	2004-11-11	Hertzberg et al.	
	7	20040243680	A1	2004-12-02	Mayer, Georg	
	8	20040267872	A1	2004-12-30	Serdy et al.	
	9	20050091505	A1	2005-04-28	Riley et al.	
	10	20050108075	A1	2005-05-19	Douglis et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	20060099970	A1	2006-05-11	Morgan et al.	
	12	20060182137	A1	2006-08-17	Zhou et al.	
	13	20070130283	A1	2007-06-07	Klein et al.	
	14	20070255797	A1	2007-11-01	Dunn et al.	
	15	20070297378	A1	2007-12-27	Poyhonen et al.	
	16	20080089303	A1	2008-04-17	Wirtanen et al.	
	17	20080096559	A1	2008-04-24	Phillips et al.	
	18	20080279216	A1	2008-11-13	Sharif-Ahmadi et al.	
	19	20080320497	A1	2008-12-25	Tarkoma et al.	
	20	20090006229	A1	2009-01-01	Sweeney et al.	
	21	20090016310	A1	2009-01-15	Rasal, Digambar L.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	22	20090042536	A1	2009-02-12	Bernard et al.	
	23	20090047989	A1	2009-02-19	Harmon et al.	
	24	20090132860	A1	2009-05-21	LIU et al.	
	25	20090217364	A1	2009-08-27	Salmela et al.	
	26	20090307696	A1	2009-12-10	Vals et al.	
	27	20100190469	A1	2010-07-29	Vanderveen et al.	
	28	20120144025	A1	2012-06-07	Melander et al.	
	29	20120166364	A1	2012-06-28	Ahmad et al.	
	30	20130072177	A1	2013-03-21	Ross et al.	
	31	20140241342	A1	2014-08-28	Constantinof, Cristian	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1345154	CN	A	2002-04-17	Datang Microelectronics Tech. Co.		
	2	1545114	EP	A1	2005-06-22	Alcatel		
	3	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		
	4	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		
	5	2005339247A	JP		2005-12-08	Secured Communications		
	6	2006155263A	JP		2006-06-15	NEC Corporation		
	7	2006197137	JP		2006-07-27	NTT Docomo Inc.		
	8	2006344007	JP	A	2006-12-21	Hitachi Ltd.		
	9	2002067616	WO	A1	2002-08-29	Sonera Oyj		
	10	2002093877	WO	A1	2002-11-21	Nokia Corp.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	2003017063	WO	A2	2003-02-27	Apogee Networks		
	12	2003017065	WO	A2	2003-02-27	Apogee Networks		
	13	2005083934	WO	A1	2005-09-09	Research In Motion Ltd.		
	14	2006004784	WO	A1	2006-01-12	Japan Communications Inc.		
	15	2007120310	WO		2007-10-25	Qualcomm Inc.		
	16	2009091295	WO	A1	2009-07-23	Telefonaktiebolaget LM Ericsson		
	17	2011002450	WO	A1	2011-01-06	Alcatel-Lucent USA Inc.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO)," Release 9, Document No. 3GPP TS 24.312, V9.1.0, March 2010	
	2	3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; IP Flow Mobility and seamless WLAN offload; Stage 2," Release 10, Document No. 3GPP TS 23.261, V1.0.0, March 2010	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	3	Ahmed et al., "Multi Access Data Network Connectivity and IP Flow Mobility in Evolved Packet System (EPS)," 2010 IEEE	
	4	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	
	5	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	
	6	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	
	7	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	
	8	Kasper et al., "Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted Computing," Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany; ICACT 2008	
	9	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	
	10	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	
	11	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	
	12	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	
	13	Quintana, David, "Mobile Multitasking," April 14, 2010	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	14	Roy et al., "Energy Management in Mobile Devices with the Cinder Operating System", Stanford University, MIT CSAIL, June 3, 2010	
	15	Windows7 Power Management, published April 2009	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/ANDREW J RUDY/	Date Considered	01/24/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /A.J.R/

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14082040	RALEIGH ET AL.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

CPC							
Symbol						**Type**	**Version**
H04W		28	/	0289		F	2013-01-01
H04W		24	/	00		A	2013-01-01
H04W		36	/	14		A	2013-01-01
H04L		41	/	0893		I	2013-01-01
H04L		41	/	5054		I	2013-01-01
H04L		47	/	803		I	2013-01-01
H04L		47	/	822		I	2013-01-01
H04L		47	/	824		I	2013-01-01
H04L		43	/	0882		I	2013-01-01
H04W		4	/	001		I	2013-01-01
H04W		52	/	0212		I	2013-01-01
H04W		84	/	12		I	2013-01-01
H04L		47	/	20		I	2013-01-01
H04W		28	/	0215		I	2013-01-01
H04W		28	/	12		I	2013-01-01
H04W		84	/	042		A	2013-01-01
H04L		43	/	08		I	2013-01-01
H04L		47	/	12		I	2013-01-01
H04L		47	/	14		I	2013-01-01
H04L		47	/	19		I	2013-01-01
H04L		47	/	801		I	2013-01-01
H04L		47	/	805		I	2013-01-01
H04W		28	/	021		I	2013-01-01
H04W		28	/	0221		I	2013-01-01
H04W		28	/	0268		I	2013-01-01
H04L		41	/	5051		I	2013-01-01
H04L		47	/	808		I	2013-01-01
H04W		28	/	0257		I	2013-01-01
H04L		63	/	10		I	2013-01-01
H04L		63	/	102		I	2013-01-01
H04L		63	/	20		I	2013-01-01

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	23	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	1/26/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	25

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14082040	RALEIGH ET AL.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

H04W		12	/ 08	I	2013-01-01
H04W		48	/ 16	I	2013-01-01
H04W		80	/ 04	I	2013-01-01
H04L		47	/ 2475	I	2013-01-01
H04W		48	/ 04	I	2013-01-01
H04W		52	/ 0264	I	2013-01-01
H04W		24	/ 08	I	2013-01-01
Y02B		60	/ 50	A	2013-01-01
H04L		47	/ 2425	A	2013-01-01
H04W		24	/ 02	I	2013-01-01
H04W		28	/ 0247	I	2013-01-01
H04W		28	/ 20	I	2013-01-01
H04W		48	/ 06	I	2013-01-01
H04L		12	/ 14	I	2013-01-01
H04M		15	/ 30	A	2013-01-01
H04M		15	/ 41	I	2013-01-01
H04M		15	/ 43	I	2013-01-01
H04M		15	/ 44	I	2013-01-01
H04M		15	/ 66	I	2013-01-01
H04M		15	/ 8016	I	2013-01-01
H04M		15	/ 8055	I	2013-01-01
H04M		15	/ 81	I	2013-01-01
H04W		4	/ 26	A	2013-01-01
H04L		41	/ 5006	I	2013-01-01
H04L		41	/ 5022	A	2013-01-01
H04L		41	/ 5029	I	2013-01-01
H04L		12	/ 1492	I	2013-01-01
H04L		12	/ 1496	I	2013-01-01
H04L		41	/ 0896	I	2013-01-01
H04W		28	/ 0284	I	2013-01-01

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 23	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	1/26/2017 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 25

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14082040	RALEIGH ET AL.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

CPC Combination Sets				
Symbol	**Type**	**Set**	**Ranking**	**Version**
/				
/				

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	23	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687	1/26/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	25

U.S. Patent and Trademark Office

Part of Paper No. 20170126

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14082040	RALEIGH ET AL.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
709	224	G	0	6	F	15 / 173 (2006.01.01)						
CROSS REFERENCE(S)		H	0	4	M	3 / 42 (2006.01.01)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											
455	414.1											

NONE (Assistant Examiner)	(Date)	Total Claims Allowed: 23	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	1/26/2017 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 25

U.S. Patent and Trademark Office

Part of Paper No. 20170126

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14082040	RALEIGH ET AL.
	Examiner	**Art Unit**
	ANDREW JOSEPH RUDY	3687

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17												
2	24	18	18												
3	25	19	19												
4	26	20	20												
5	5	21	21												
6	27	22	29												
7	28	23	30												
8	8														
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 23	
/ANDREW JOSEPH RUDY/ Primary Examiner.Art Unit 3687 (Primary Examiner)	1/26/2017 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 25

U.S. Patent and Trademark Office Part of Paper No. 20170126

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination
	14/082,040	RALEIGH ET AL.
	Examiner	Art Unit
	ANDREW JOSEPH RUDY	3687

SEARCHED			
Class	Subclass	Date	Examiner
prior			
search	updated	1/25/2017	AJR
455	405,414.1	1/25/2017	AJR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
709	**224**	**1/26/2017**	**AJR**
455	414.1	1/26/2017	AJR
H04L	29/08072	1/26/2017	AJR
H04I 29/08108		1/26/2017	AJR

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Continuity data reviewed.	1/23/2017	AJR

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/082,040	Filing Date 11/15/2013	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	12/01/2016	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 23	Minus	** 23	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
JASON B. EADDY

This collection of information is required by 37 CFR 1.16. 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 1.14. This collection is estimated to take 12 minutes 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. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Raleigh et al.	Examiner:	Rudy, Andrew J.
Serial No.:	14/082,040	Art Unit:	3687
Filed:	November 15, 2013	Conf. No.:	1015
Title:	Device-Assisted Services for Protecting Network Capacity		

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE

In response to the Office Action dated June 1, 2016, the no-fee deadline for response being September 1, 2016, please amend the above-identified application as follows:

Amendments to the Claims begin on page 2.

Remarks begin on page 7.

AMENDMENTS TO THE CLAIMS

Without prejudice and without surrender of any subject matter, please amend the claims as follows:

1. (Currently Amended) A wireless end-user device ~~system~~, comprising:

a wireless modem to communicate data for network service usage activities between the device and a wireless network;

a processor that executes instructions ~~of a communications device configured~~ to[[:]]

~~monitor a network service usage activity of the communications device in network communication;~~

~~classify the network service usage activity for differential network access control for protecting network capacity; and~~

associate [[the]] network service usage activity, on behalf of a first device application, and that occurs when the first device application is not in the foreground of user interaction, with a network service usage control policy, ~~based on a classification of the network service usage activity to facilitate differential network access control for protecting network capacity~~

set an application state indicating whether the first device application, associated with a particular network service usage activity, is in the foreground of user interaction, and

dynamically determine whether to apply the network service usage control policy to the particular network service usage activity, based on the application state and based on a power control state; and

a memory coupled to the processor ~~and configured~~ to provide the processor with the instructions.

2-4. (Canceled).

5. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

implement the network service usage control policy at least in part via communication with the first device application through ~~differential network access for the network service usage~~

~~activity for protecting network capacity using~~ an emulated network access API that indicates to the first device application that an available wireless network is unavailable when a dynamic determination applies the network service usage control policy to the particular network service usage activity.

6-7. (Canceled).

8. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end-user ~~communications~~ device.

9. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end-user ~~communications~~ device; and

send network busy state information to a service controller, wherein the service controller provides a policy decision point for management for a plurality of wireless end-user ~~communications~~ devices in communication with one or more base stations.

10. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end-user ~~communications~~ device;

send network busy state information to a service controller, wherein the service controller provides a policy decision point for management for a plurality of wireless end-user ~~communications~~ devices in communication with one or more base stations; and

receive router traffic control instructions from the service controller, wherein the service controller provides the router traffic control instructions to assist in dynamically managing network capacity usage for the plurality of wireless end-user ~~communications~~ devices in

communication with the one or more base stations ~~for protecting network capacity of one or more access networks~~.

11. (Currently Amended) The wireless end-user device recited in claim 1, wherein [[the]] dynamically determining whether to apply the network service usage control policy to the particular network service usage activity ~~classifying~~ is further based on a current wireless ~~access~~ network and/or the network service usage control policy is based on a current wireless ~~access~~ network.

12. (Currently Amended) The wireless end-user device recited in claim 1, wherein dynamically determining whether to apply the network service usage control policy to the particular network service usage activity further includes dynamically assigning a network capacity controlled services priority level to the particular network service usage activity based on a network busy state.

13. (Currently Amended) The wireless end-user device recited in claim 1, wherein ~~classifying includes querying a network element for determining a network capacity controlled services classification and/or~~ associating includes querying a network element for determining an association of the first device application with the network service usage control policy.

14. (Currently Amended) The wireless end-user device recited in claim 1, wherein the network service usage control policy includes one or more of the following: block/allow settings, throttle settings, adaptive throttle settings, QoS class settings, packet error rate, jitter and delay settings, queue settings, and tag settings.

15. (Currently Amended) The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters, the filters comprising a first filter specifying applicability of the policy only when the first device application is not in the foreground of user interaction, and a second filter specifying applicability of the policy only in one or more specific power control states.

16. (Currently Amended) The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters implemented as cascading filters.

17. (Currently Amended) The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters using a network busy state and/or a time of day as an index into a traffic control setting.

18. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

differentially control the particular network service usage activity based on the network service usage control policy based on a network busy state~~, wherein the network service usage activity is classified as a network capacity controlled service~~.

19. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

differentially control the particular network service usage activity based on the network service usage control policy based on a user input and/or a current wireless ~~access~~ network~~, wherein the network service usage activity is classified as a network capacity controlled service~~.

20. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

modify or replace a network stack interface of the wireless end-user ~~communications~~ device to provide for intercept or discontinuance of network access messaging for implementing traffic control of the particular network service usage activity ~~for network capacity controlled services for protecting network capacity~~.

21. (Currently Amended) The wireless end-user device ~~system~~ recited in claim 1, wherein the processor executes the instructions further ~~of the communications device is further configured~~ to:

store a network capacity controlled service list, wherein the network capacity controlled service list is periodically updated based on monitored network service usage activities.

22-23. (Canceled).

24. (New) The wireless end-user device of claim 1, wherein the processor executing the instructions determines that the first device application is in the foreground of user interaction when the user of the device is directly interacting with that application or perceiving any benefit from that application.

25. (New) The wireless end-user device of claim 1, wherein the processor executing the instructions determines that the first device application is in the foreground of user interaction based on a state of user interface priority for the application.

26. (New) The wireless end-user device of claim 1, wherein when the network service usage control policy is applied it disallows the particular network service usage activity, and wherein the processor executes the instruction further to, when it is determined that the particular network access request is disallowed, queue that particular network service usage activity until a power state change occurs.

27. (New) The wireless end-user device of claim 1, wherein the processor further executes the instruction to, for at least a second device application or service, allow network service usage activities without regard to the power control state.

28. (New) The wireless end-user device of claim 1, wherein the power control state is a power state of the device.

29. (New) The wireless end-user device of claim 1, wherein the power control state is a power save state of the device.

30. (New) The wireless end-user device of claim 1, wherein the power control state is a power state of the wireless modem.

REMARKS

Claims 1-23 were pending and rejected by the Office Action dated June 1, 2016. Applicant has amended claims 1, 5, and 8-21, canceled claims 2-4, 6-7, and 22-23, and added new claims 24-30. Accordingly, claims 1, 5, 8-21, and 24-30 are active in the application. In view of the amendments to the claims and the following remarks, Applicant respectfully requests reconsideration.

Claim Rejections – 35 U.S.C. § 101

In section 4, the Office Action rejected claims 1-23 under 35 U.S.C. § 101, indicating that the claimed invention is directed towards non-statutory subject matter.

Applicant has extensively reworked the claims to remove potentially abstract language and incorporate further elements from prior dependent claims 6 and 15 and from the specification (see, e.g., paragraphs [00256]-[00257] and [00265]-[00266]) into claim 1. Applicant submits that claim 1 and its dependents are now are within a statutorily permitted subject area, as the current claims are drawn to a device and include limitations that improve the functioning of the device itself. For instance, the device as recited in claim 1 contains features that allow network service usage policies to be directed to the network service usage activity of a particular application based on specific operational states, including the foreground state of the application and the power control state of the device and/or modem. Thus as exemplary but non-limiting enabled improvements to the device, such features allow an embodiment of the device to prevent applications that the user is not interacting with from further depleting an already-low battery, or allow an embodiment of the device to prevent applications that the user is not interacting with from cycling modem power. Applicant respectfully submits that, at least due to the inclusion of such features, the amended claims are directed to statutory subject matter. No new matter has been added.

Claim Rejections – 35 U.S.C. § 103

In section 6, the Office Action rejected claims 1-23 under 35 U.S.C. § 103(a) as being unpatentable over U.S. 8,484,568 to Rados (hereinafter, "Rados"). Applicant respectfully

submits that Rados is not prior art to the current claims. It is Applicant's belief that the claims are each supported no later than May 25, 2010, the filing date of Provisional Patent Application 61/348,022, which is in the chain of priority for the current application. This priority date predates the filing date of Rados. Accordingly, Applicant respectfully requests that the rejection be withdrawn.

CONCLUSION

Applicant respectfully requests entry of these amendments as provided herein. The application is believed to be in condition for allowance, and a Notice of Allowance is hereby respectfully requested. If the Examiner has any questions or needs any additional information, the Examiner is invited to contact the undersigned.

The Commissioner is authorized to charge any fee deficiency or credit any overpayment to Deposit Account 50-5876.

Respectfully submitted,

Date: December 1, 2016 By: /James E. Harris/

James E. Harris
Reg. No. 40,013
Patent Counsel
Headwater Partners I LLC
1011 Pruitt Place
Tyler, TX 75703
(903) 201-6212

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being filed electronically via EFS-Web addressed to the Commissioner for Patents on:

Date: Dec. 1, 2016 By: /Ann Taylor/
Ann Taylor

Electronic Patent Application Fee Transmittal					
Application Number:	14082040				
Filing Date:	15-Nov-2013				
Title of Invention:	Device-Assisted Services for Protecting Network Capacity				
First Named Inventor/Applicant Name:	Gregory G. Raleigh				
Filer:	James E. Harris/Ann Taylor				
Attorney Docket Number:	RALEP032C1				
Filed as Small Entity					
Filing Fees for Utility under 35 USC 111(a)					
Description		**Fee Code**	**Quantity**	**Amount**	**Sub-Total in USD($)**
Basic Filing:					
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($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**790**

Electronic Acknowledgement Receipt	
EFS ID:	27671315
Application Number:	14082040
International Application Number:	
Confirmation Number:	1015
Title of Invention:	Device-Assisted Services for Protecting Network Capacity
First Named Inventor/Applicant Name:	Gregory G. Raleigh
Customer Number:	106963
Filer:	James E. Harris/Ann Taylor
Filer Authorized By:	James E. Harris
Attorney Docket Number:	RALEP032C1
Receipt Date:	01-DEC-2016
Filing Date:	15-NOV-2013
Time Stamp:	18:56:28
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$790
RAM confirmation Number	120216INTEFSW00005609505876
Deposit Account	505876
Authorized User	Ann Taylor
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 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	Information Disclosure Statement (IDS) Form (SB08)	P032C1_IDS.pdf	1059039 953834adfce4a09146cb780c6f5b39a175095d45	no	19
Warnings:					
Information:					
2	Foreign Reference	2074.pdf	7047386 8fcf0ca549f5be7aaa631006e8ff2b73a8defc71	no	40
Warnings:					
Information:					
3	Foreign Reference	2075.pdf	1121298 941f56ab8972334f740a42da0f64323e27525f22	no	46
Warnings:					
Information:					
4	Foreign Reference	2076.pdf	972543 b6cc2b50dfba5f9dafe28939427a6228d7218933	no	39
Warnings:					
Information:					
5	Foreign Reference	2077.pdf	1901018 653916447508 6ad9ab3c492961440050eb14eb60	no	51
Warnings:					
Information:					
6	Foreign Reference	2078.pdf	1128425 34d3158d2965f487838e0079c67c3c6926679a7c	no	38
Warnings:					
Information:					

7	Foreign Reference	2079.pdf	1123981 085b25ad47976d8c5eaa309e384a85cf56ef2e6a	no	3
Warnings:					
Information:					
8	Foreign Reference	2080.pdf	877755 277dd25bee280796f81a1943a6d00e1e91ac213a	no	11
Warnings:					
Information:					
9	Foreign Reference	2081.pdf	975121 23277e1884ea272e116216d6e83b5c822a6a2d58	no	14
Warnings:					
Information:					
10	Foreign Reference	2082.pdf	7497094 1cab9a3e1917138dd03e255717030799796eafc5	no	45
Warnings:					
Information:					
11	Foreign Reference	2083.pdf	782462 2ce1ee70705ca2f54e4571f31517ddc96b1c19c4	no	8
Warnings:					
Information:					
12	Foreign Reference	2084.pdf	1397656 9e6a8957ad2e807f979431120ddbd1741e2acde7	no	57
Warnings:					
Information:					
13	Foreign Reference	2085.pdf	441333 e8defb411cdca2f87d3c0c97eae168e0c2960826	no	19
Warnings:					
Information:					

14	Foreign Reference	2086.pdf	232424 fbefdfe44bda45a08d0dfa2e2b40b5d0f577f976	no	29
Warnings:					
Information:					
15	Foreign Reference	2087.pdf	922375 5370f148f48d4def4ad535f2c2b1762f0ca57119	no	47
Warnings:					
Information:					
16	Foreign Reference	2088.pdf	255944 b4b8ef7ddc1f98c4716aaed35917fdb84c9be0fa	no	18
Warnings:					
Information:					
17	Foreign Reference	2089.pdf	172902 9025822de8f174376f282787af6b3524407be5db	no	13
Warnings:					
Information:					
18	Foreign Reference	2090.pdf	643809 f84e3fb9347dd0d758241de1f737fa384a62bebe	no	38
Warnings:					
Information:					
19	Extension of Time	P032C1_Ext.pdf	163581 8fcbd2e524be36d7274e429cb2e8415f513a43f5	no	2
Warnings:					
Information:					
20		P032C1_OAR.pdf	96821 c8a108013b6da6af953f66f267038f78454caaf3	yes	9
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	

	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	6	
	Applicant Arguments/Remarks Made in an Amendment		7	9	
Warnings:					
Information:					
21	Fee Worksheet (SB06)	fee-info.pdf	32680 ab7d11ad5138a1cc2b59c2406b971432c646b422	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	28845647		

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.

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14082040
Filing Date	2013-11-15
First Named Inventor	Gregory G. Raleigh
Art Unit	3687
Examiner Name	Rudy, Andrew J.
Attorney Docket Number	RALEP032C1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5617539	A	1997-04-01	Ludwig et al.	
	2	6141565	A	2000-10-31	Feuerstein et al.	
	3	6401113	B2	2002-06-04	Lazaridis et al.	
	4	6510152	B1	2003-01-21	Gerszberg et al.	
	5	6535855	B1	2003-03-18	Cahill et al.	
	6	6542500	B1	2003-04-01	Gerszberg et al.	
	7	6546016	B1	2003-04-08	Gerszberg et al.	
	8	6570974	B1	2003-05-27	Gerszberg et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	9	6601040	B1	2003-07-29	Kolls, H. Brock	
	10	6636721	B2	2003-10-21	Threadgill et al.	
	11	6654786	B1	2003-11-25	Fox et al.	
	12	6690918	B2	2004-02-10	Evans et al.	
	13	6959393	B2	2005-10-25	Hollis et al.	
	14	7082422	B1	2006-07-25	Zirngibl et al.	
	15	7095754	B2	2006-08-22	Benveniste, Mathilde	
	16	7133386	B2	2006-11-07	Holur et al.	
	17	7136361	B2	2006-11-14	Benveniste, Mathilde	
	18	7151764	B1	2006-12-19	Heinonen et al.	
	19	7177919	B1	2007-02-13	Truong et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	20	7191248	B2	2007-03-13	Chattopadhyay et al.	
	21	7272660	B1	2007-09-18	Powers et al.	
	22	7369848	B2	2008-05-06	Jiang, Yue Jun	
	23	7369856	B2	2008-05-06	Ovadia, Shlomo	
	24	7409569	B2	2008-08-05	Illowsky et al.	
	25	7428750	B1	2008-09-23	Dunn et al.	
	26	7440433	B2	2008-10-21	Rink et al.	
	27	7486658	B2	2009-02-03	Kumar, Rajneesh	
	28	7562213	B1	2009-07-14	Timms, Natalie	
	29	7577431	B2	2009-08-18	Jiang, Yue Jun	
	30	7599714	B2	2009-10-06	Kuzminskiy, Alexandr	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	31	7602746	B2	2009-10-13	Calhoun et al.	
	32	7610047	B2	2009-10-27	Hicks III et al.	
	33	7643411	B2	2010-01-05	Andreasen et al.	
	34	7657920	B2	2010-02-02	Arseneau et al.	
	35	7660419	B1	2010-02-09	Ho, Jin-Meng	
	36	7661124	B2	2010-02-09	Ramanathan et al.	
	37	7664494	B2	2010-02-16	Jiang, Yue Jun	
	38	7719966	B2	2010-05-18	Luft et al.	
	39	7724716	B2	2010-05-25	Fadell, Anthony M.	
	40	7770785	B2	2010-08-10	Jha et al.	
	41	7817983	B2	2010-10-19	Cassett et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	42	7873001	B2	2011-01-18	Silver, Andrew	
	43	7979069	B2	2011-07-12	Hupp et al.	
	44	8036387	B2	2011-10-11	Kudelski et al.	
	45	8044792	B2	2011-10-25	Orr et al.	
	46	8065365	B2	2011-11-22	Saxena et al.	
	47	8085808	B2	2011-12-27	Brusca et al.	
	48	8125897	B2	2012-02-28	Ray et al.	
	49	8132256	B2	2012-03-06	Bari, Farooq	
	50	8140690	B2	2012-03-20	Ly et al.	
	51	8145194	B2	2012-03-27	Yoshikawa et al.	
	52	8151205	B2	2012-04-03	Follmann et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	53	8191106	B2	2012-05-29	Choyi et al.	
	54	8194549	B2	2012-06-05	Huber et al.	
	55	8194581	B1	2012-06-05	Schroeder et al.	
	56	8195153	B1	2012-06-05	Frencel et al.	
	57	8219134	B2	2012-07-10	Maharajh et al.	
	58	8271025	B2	2012-09-18	Brisebois et al.	
	59	8291439	B2	2012-10-16	Jethi et al.	
	60	8307095	B2	2012-11-06	Clark et al.	
	61	8320902	B2	2012-11-27	Moring et al.	
	62	8325906	B2	2012-12-04	Fullarton et al.	
	63	8340628	B2	2012-12-25	Taylor et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	64	8363799	B2	2013-01-29	Gruchala et al.	
	65	8380247	B2	2013-02-19	Engstrom	
	66	8402165	B2	2013-03-19	Deu-Ngoc et al.	
	67	8412798	B1	2013-04-02	Wang, Frank C.	
	68	8418168	B2	2013-04-09	Tyhurst et al.	
	69	8448015	B2	2013-05-21	Gerhart, David	
	70	8494559	B1	2013-07-23	Malmi	
	71	8503358	B2	2013-08-06	Hanson et al.	
	72	8505073	B2	2013-08-06	Taglienti et al.	
	73	8521775	B1	2013-08-27	Poh et al.	
	74	8531954	B2	2013-09-10	McNaughton et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	75	8538421	B2	2013-09-17	Brisebois et al.	
	76	8543814	B2	2013-09-24	Laitinen et al.	
	77	8600895	B2	2013-12-03	Felsher, David Paul	
	78	8639215	B2	2014-01-28	McGregor et al.	
	79	8670752	B2	2014-03-11	Fan et al.	
	80	8675852	B2	2014-03-18	Maes, Stephane H.	
	81	8700729	B2	2014-04-15	Dua, Robin	
	82	8719397	B2	2014-05-06	Levi et al.	
	83	8731519	B2	2014-05-20	Flynn et al.	
	84	8744339	B2	2014-06-03	Halfmann et al.	
	85	8787249	B2	2014-07-22	Giaretta et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	86	8811338	B2	2014-08-19	Jin et al.	
	87	8819253	B2	2014-08-26	Simeloff et al.	
	88	8837322	B2	2014-09-16	Venkataramanan et al.	
	89	8838686	B2	2014-09-16	Getchius, Jeffery M.	
	90	8838752	B2	2014-09-16	Lor et al.	
	91	8855620	B2	2014-10-07	Sievers et al.	
	92	8862751	B2	2014-10-14	Faccin et al.	
	93	8898748	B2	2014-11-25	Burks et al.	
	94	8908516	B2	2014-12-09	Tzamaloukas et al.	
	95	8943551	B2	2015-01-27	Ganapathy et al.	
	96	8971841	B2	2015-03-03	Menezes et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	97	8971912	B2	2015-03-03	Chou et al.	
	98	8995952	B1	2015-03-31	Baker et al.	
	99	9030934	B2	2015-05-12	Shah et al.	
	100	9032427	B2	2015-05-12	Gallant et al.	
	101	9173090	B2	2015-10-27	Tuchman et al.	
	102	9282460	B2	2016-03-08	Souissi, Slim Salah	
	103	9325737	B2	2016-04-26	Gutowski et al.	
	104	9344557	B2	2016-05-17	Gruchala et al.	
	105	9367680	B2	2016-06-14	Mahaffey et al.	
	106	9413546	B2	2016-08-09	Meier et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020120370	A1	2002-08-29	Parupudi et al.	
	2	20020138599	A1	2002-09-26	Dilman et al.	
	3	20030184793	A1	2003-10-02	Pineau, Richard A.	
	4	20040054779	A1	2004-03-18	Takeshima et al.	
	5	20040176104	A1	2004-09-09	Arcens, Suzanne	
	6	20040225561	A1	2004-11-11	Hertzberg et al.	
	7	20040243680	A1	2004-12-02	Mayer, Georg	
	8	20040267872	A1	2004-12-30	Serdy et al.	
	9	20050091505	A1	2005-04-28	Riley et al.	
	10	20050108075	A1	2005-05-19	Douglis et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	20060099970	A1	2006-05-11	Morgan et al.	
	12	20060182137	A1	2006-08-17	Zhou et al.	
	13	20070130283	A1	2007-06-07	Klein et al.	
	14	20070255797	A1	2007-11-01	Dunn et al.	
	15	20070297378	A1	2007-12-27	Poyhonen et al.	
	16	20080089303	A1	2008-04-17	Wirtanen et al.	
	17	20080096559	A1	2008-04-24	Phillips et al.	
	18	20080279216	A1	2008-11-13	Sharif-Ahmadi et al.	
	19	20080320497	A1	2008-12-25	Tarkoma et al.	
	20	20090006229	A1	2009-01-01	Sweeney et al.	
	21	20090016310	A1	2009-01-15	Rasal, Digambar L.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	22	20090042536	A1	2009-02-12	Bernard et al.	
	23	20090047989	A1	2009-02-19	Harmon et al.	
	24	20090132860	A1	2009-05-21	LIU et al.	
	25	20090217364	A1	2009-08-27	Salmela et al.	
	26	20090307696	A1	2009-12-10	Vals et al.	
	27	20100190469	A1	2010-07-29	Vanderveen et al.	
	28	20120144025	A1	2012-06-07	Melander et al.	
	29	20120166364	A1	2012-06-28	Ahmad et al.	
	30	20130072177	A1	2013-03-21	Ross et al.	
	31	20140241342	A1	2014-08-28	Constantinof, Cristian	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	1345154	CN	A	2002-04-17	Datang Microelectronics Tech. Co.		
	2	1545114	EP	A1	2005-06-22	Alcatel		
	3	1887732	EP	A1	2008-02-13	Huawei Technologies Co., Ltd.		
	4	2007065	EP	A1	2008-12-24	Huawei Technologies Co., Ltd.		
	5	2005339247A	JP		2005-12-08	Secured Communications		
	6	2006155263A	JP		2006-06-15	NEC Corporation		
	7	2006197137	JP		2006-07-27	NTT Docomo Inc.		
	8	2006344007	JP	A	2006-12-21	Hitachi Ltd.		
	9	2002067616	WO	A1	2002-08-29	Sonera Oyj		
	10	2002093877	WO	A1	2002-11-21	Nokia Corp.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	11	2003017063	WO	A2	2003-02-27	Apogee Networks		
	12	2003017065	WO	A2	2003-02-27	Apogee Networks		
	13	2005083934	WO	A1	2005-09-09	Research In Motion Ltd.		
	14	2006004784	WO	A1	2006-01-12	Japan Communications Inc.		
	15	2007120310	WO		2007-10-25	Qualcomm Inc.		
	16	2009091295	WO	A1	2009-07-23	Telefonaktiebolaget LM Ericsson		
	17	2011002450	WO	A1	2011-01-06	Alcatel-Lucent USA Inc.		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	3rd Generation Partnership Project, "Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO)," Release 9, Document No. 3GPP TS 24.312, V9.1.0, March 2010	
	2	3rd Generation Partnership Project; "Technical Specification Group Services and System Aspects; IP Flow Mobility and seamless WLAN offload; Stage 2," Release 10, Document No. 3GPP TS 23.261, V1.0.0, March 2010	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	3	Ahmed et al., "Multi Access Data Network Connectivity and IP Flow Mobility in Evolved Packet System (EPS)," 2010 IEEE	
	4	Blackberry Mobile Data System, version 4.1, Technical Overview, 2006	
	5	Client Guide for Symantec Endpoint Protection and Symantec Network Access Control, 2007	
	6	Ehnert, "Small application to monitor IP trafic on a Blackberry - 1.01.03 ", March 27, 2008; http://www.ehnert.net/MiniMoni/	
	7	Fujitsu, "Server Push Technology Survey and Bidirectional Communication in HTTP Browser," January 9, 2008 (JP)	
	8	Kasper et al., "Subscriber Authentication in mobile cellular Networks with virtual software SIM Credentials using Trusted Computing," Fraunhofer-Institute for Secure Information Technology SIT, Darmstadt, Germany; ICACT 2008	
	9	Kuntze et al., "Trustworthy content push," Fraunhofer-Institute for Secure Information Technology SIT; Germany; WCNC 2007 proceedings, IEEE	
	10	Muntermann et al., "Potentiale und Sicherheitsanforderungen mobiler Finanzinformationsdienste und deren Systeminfrastrukturen," Chair of Mobile Commerce & Multilateral Security, Goethe Univ. Frankfurt, 2004	
	11	NetLimiter Lite 4.0.19.0; http://www.heise.de/download/netlimiter-lite-3617703.html from vol. 14/2007	
	12	Open Mobile Alliance (OMA), Push Architecture, Candidate Version 2.2; Oct. 2, 2007; OMA-AD-Push-V2_2-20071002-C	
	13	Quintana, David, "Mobile Multitasking," April 14, 2010	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

	14	Roy et al., "Energy Management in Mobile Devices with the Cinder Operating System", Stanford University, MIT CSAIL, June 3, 2010	
	15	Windows7 Power Management, published April 2009	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14082040
	Filing Date	2013-11-15
	First Named Inventor	Gregory G. Raleigh
	Art Unit	3687
	Examiner Name	Rudy, Andrew J.
	Attorney Docket Number	RALEP032C1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/James E. Harris/	Date (YYYY-MM-DD)	2016-12-01
Name/Print	James E. Harris	Registration Number	40013

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1.14. This collection is estimated to take 1 hour 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. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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 the Freedom of Information Act requires disclosure of these record s.

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 another 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 inspections 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.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 July 2009 (23.07.2009)

PCT

(10) International Publication Number
WO 2009/091295 A1

(51) International Patent Classification:
H04Q 7/38 (2006.01) *H04Q 7/32* (2006.01)

(21) International Application Number:
PCT/SE2008/000031

(22) International Filing Date: 15 January 2008 (15.01.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: RUNE, Johan [SE/SE]; Terrängvägen 12, S-181 30 Lidingö (SE).

(74) Agent: MOSSMARK, Anders; Albihns AB, Box 142, S-401 22 Göteborg (SE).

(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, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

(54) Title: PRE-FETCHING OF INPUT DATA FOR ACCESS NETWORK SELECTION

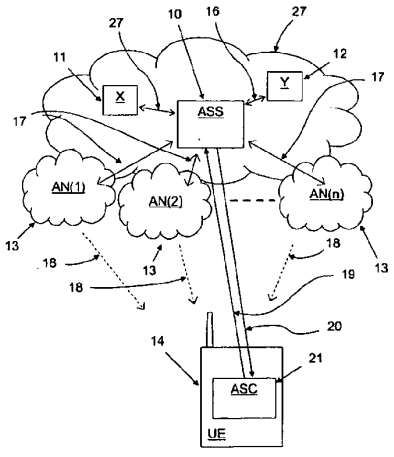


FIG 1

(57) Abstract: The present invention relates to a method, an Access Selection Server and a communication network 27 for network access selection 26. The network comprises an Access Selection Server (ASS) 10, at least one User Equipment (UE) 14, an Access Selection Client (ASC) 21 arranged in the UE 14 and communication nodes 11, 12. The ASS collects 23 access selection parameters used for the selection 26 of access network for the network access for the UE 14 in a multi-access environment. The network access enables a traffic bearer for a traffic flow between an application in the UE 14 and a first node. The ASS 10 forwards 25 the access selection parameters and/or processes 23 the access selection parameters and sends 25 the results of the processed parameters to the UE 14. The parameters forwarded 25 or the results sent 25 by the ASS 21 being access selection information, based on which the ASC 21 performs 26 activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow. What particularly characterizes the invention is that the ASS 10 controls at least the collection or the processing 23 of the access selection parameters, the collection or the processing 23 being performed at least when the UE 14 is disconnected from the communication network 27. Furthermore, the parameters collected or processed 23 when the UE 14 is disconnected from the communication network 27 are forwarded 25 and/or the results of the processed parameters are sent 25 as access selection information by the ASS 10 to the UE 14 when the UE 14 is again connected to the communication network 27.

WO 2009/091295 A1

TITEL

Pre-Fetching of Input Data for Access Network Selection

TECHNICAL FIELD

The present invention relates to a method and a communication system for network access selection and an access selection server in the system enabling said method.

BACKGROUND

Third generation mobile systems (3G), based on WCDMA (Wideband Code Division Multiple Access) radio access technology, are being deployed on a broad scale all around the world. However, as user and operator requirements and expectations will continue to evolve a new phase in the standard specification body called 3rd Generation Partnership Project (3GPP) has started to consider the next major steps in the evolution of the 3G standard. The terminals used in the network are having more functions integrated which means that an increasing number of access types such as e.g. LTE (Long Term Evolution), WiMAX (Worldwide Interoperability for Microwave Access) and WLAN (Wireless Local Area Network) and new services such as Voice over IP (VoIP) or IP-TV are added to the terminal.

In a multi-access environment the multi-interface terminal is often faced with a choice of potential access networks to connect to, either for a new connection or for a potential handover of an existing one or simply for being reachable through after power on.

These access networks may differ in various properties, such as access technology (e.g. 3G or WLAN), available operators (directly or indirectly) and roaming agreements, presence of NATs and/or firewalls, applicable policies (such as codec restrictions), access rate, supported QoS and current load. All these variable parameters make the choice of access network(s) potentially complex. The more data about the available access networks that

the access selection algorithm takes into account, the more sophisticated and accurate (and thus beneficial) the selection can be made.

Some of this information is available through scanning of system information that is broadcast from access points or base stations and that can be received by any terminal (equipped with a matching interface) without any type of prior association, registration, authentication or connection.

However, retrieval of other parts of the information, potentially most of it, requires IP level communication, which in turn implies that the terminal has to go through all the preceding procedures that are needed to establish IP level communication. In for example a WLAN network this means that the terminal first has to associate with the access point at the MAC layer, then in most cases go through the user authentication and authorization procedure, typically using Extensible Authentication Protocol (EAP), and finally request and receive IP configuration data through Dynamic Host Configuration Protocol (DHCP).

It is first after all these procedures that the terminal can retrieve some of the information that may be required to select which of the available access networks that it should connect to. That is, the terminal actually has to connect to an access network in order to retrieve access selection input data. This implies an additional effort, unless the terminal already is connected.

Furthermore, retrieving such information related to a particular access network may be difficult using IP communication via another access network. Instead the terminal may have to connect to the particular concerned access network. The reason is that with the currently proposed techniques for locating an access network's local network profile, in which much of the interesting information is expected to be stored, relies on information conveyed in DHCP option 15 during the DHCP configuration procedure.

The DCHP-related technique is for instance described in the internet-draft "A Framework for Session Initiation Protocol User Agent Profile Delivery",

written by D. Petrie and published October 2006. This document specifies a framework to enable configuration of Session Initiation Protocol (SIP) User Agents in SIP deployments. The framework provides a means to deliver profile data that terminals need to be functional, automatically and with minimal (preferably none) user and administrative intervention. The framework describes how SIP User Agents can discover sources, request profiles and receive notifications related to profile modifications.

Since DHCP relies on subnet broadcasting and hardware addresses, it is only available through the particular access network and not via routers from another access network. As an unfortunate consequence the terminal in practice has to connect to each available access network in order to retrieve the information that serves as input data to the selection of which access network to connect to. Even if workarounds would appear for the limitation of the DHCP-based local network profile retrieval, the terminal would still have to connect to at least one access network in order to retrieve the relevant information from all the available access networks to enable sophisticated access selection.

Consequently, connecting to an access network and establishing IP level communication (with all its preceding procedures) with subsequent information retrieval can be rather time consuming and could consequently make the access selection inconveniently slow. It is even worse if the terminal has to connect not only to one, but to all the available access networks. The problem is the most severe when the terminal is not already connected to an access network and the access selection concerns a new connection.

Previous access selection solutions are either terminal-controlled, network-controlled or a combination of both (or the trivial method: user-controlled access selection). Network-controlled access selection is typically used for controlling handover in cellular networks. More accurately this access selection is network-controlled but terminal-assisted – the network's decision

relies on reports of measured radio signal strengths from neighbouring base stations. In networks based on IETF protocols, relying on Mobile IP for mobility and session continuity, handovers and their associated access selection are typically entirely terminal-controlled. For access selection during the initial connection to a network, before any network connectivity is available, the solutions are inherently terminal-controlled, since no network-based functionality is available.

In one approach to access selection it is proposed to implement so called access awareness functionality (for support and execution of access selection) both in the terminal and in the network. It is implemented as a layer between the application layer and the transport layer (between applications and sockets). The functionality-related signalling is independent (not mixed with other signalling, in particular application control signalling). It assumes simultaneous accesses and applies to individual communication sessions without impact to the service performance. The network-based access awareness functionality is generic and system independent in the sense that it can be applied to Internet based systems as well as cellular systems, such as 3GPP and IP Multimedia Subsystem (IMS).

The applications interface an extended socket mechanism which makes decision about what accesses to use for connection establishment/handover influenced by a set of criteria or descriptions provided by the application at socket creation. The functionality is structured to have a clear separation between the actual decision making process and the actions resulting from access awareness decisions. The access awareness functionality is system wide which means that it is generally distributed between network entities and in particular an end-user terminal and the network side.

The Assumptions/high-level requirements for the functionality includes: support for any application, compatible with any mobility management, support of simultaneous use of different accesses, separated from

applications by an interface and extensible to cover other contexts than the current networking capabilities.

A prime task of the network-based functionality is to assist the terminal-based functionality by collecting network-based information on behalf of the terminal, which is filtered and possibly refined before it is sent to the terminal. The functionality collects events from the system that is needed for access awareness. In this way the terminal and the potentially resource-scarce access link are relieved from some of the potentially demanding information retrieval and processing.

Another potential task of the network-based access awareness functionality is to assist the terminal-based functionality in calculating choices, decisions and/or recommendation in order to offload the terminal of some of this processing, which is expected to be rather intensive. The access awareness assistant performs its tasks on explicit instructions from the terminal or by analyzing contextual information or, possibly in some cases, based on default instructions.

The communication session is per socket basis (individual communication sessions) and a socket request from the application in the terminal triggers the access awareness functionality. The access selection functionality identifies the application from the port numbers in the socket request (and/or possibly other information such as indications of the process originating the socket request) and infers the application's requirements on the communication quality. This, together with policies and other information, such as available accesses and possibly network load, is then used as input data to the access selection decision. The characteristics are provided to the access awareness functionality in the network as "application preferences". These preferences may express what the functionality is allowed to do on behalf of the application and within which limits it may act. For instance, "I need 128 kbps, but could stretch myself down to 64 kbps, but not lower".

The purpose of the network-based access awareness functionality is to let users and applications exploit the fact that accesses and access networks have different characteristics. That is to give applications the necessary tools to exploit differences or give the applications enough support so that they do not need to be aware of the different charactertics. Another purpose is to provide means to adapt to existing or changing conditions. That is, for instance to give recommendations to applications, make applications adapt to changing conditions, adapt communications to changing conditions and trigger mobility management actions. The user benefits can be summarized in increased service quality, reduced interference between applications, convenience and reduced costs. The Access Service Provided (ASP) benefits include more satisfied customers, a mechanism to improve service and a new, potential service offering. Benefits for application and contents providers are higher service penetration and usage take rate, more attractive services and potential for better services.

The 3GPP has also initiated activities to develop access selection functionality (also know as multi access terminal steering) for the evolving 3GPP systems being (or expected to be) deployed in an access network environment of increasing multitude and heterogeneity. The access selection work in 3GPP focuses on packet-switched services and on 3GPP context (access technologies such as EGPRS, WCDMA/HSPA and LTE). It works also for non-3GPP context (WLAN, WiMAX, etc.). The target is a (more or less) network-controlled solution, but there will also be some kind of terminal-based access selection functionality.

The 3GPP access selection provides new functionality in the 3GPP architecture with an Access Selection Discovery and Selection Function (ANDSF), which is separate or part of the Policy and Charging Rules Function (PCRF) in the network. The ANDSF has control of all available accesses for the terminal, current network load, RAT etc. The functionality also comprises an access selection function in the terminal, which based on

request or information from the network based access selection functionality (ANDSF) performs activation/deactivation/modification or changes of access (es). It finally comprises a reference point between the access selection functions in the terminal and the network and potentially new interfaces between the PCRF and the ANDSF and between the Proxy-Call Session Control Function - P-CFCS (application server) and the ANDSF.

An assumption (which is not valid for the initial phase of access selection in a 3GPP context but which is a natural continuation in future phases) is that the terminal may have multiple accesses that may be active in parallel, so called simultaneous multi-access. The ANDSF further gets access information from the access selection function in the terminal and information from the network (load status etc.). The ANDSF will also have session information on all active accesses for the terminal. An IP connection between the access selection function in the terminal and in the network will be established at activation of the default access network. The connection is used to communicate access selection information between the access selection function in the terminal and the ANDSF. The ANDSF will be able to send activation/deactivation/modification/change requests of an access network, or instructions, policies, rules or information as the basis for such decisions to the access selection function in the terminal.

The objectives of the 3GPP access selection are automated access selection, automated network discovery/selection, tariff-dependent access priorities, definition of preferred network and service-dependent priorities. Example of benefits for the operators are network load management, radio management capabilities, automatic access selection for the user, improved resource efficiency and system usage and minimized handover effects. User benefits are enablement to influence the access selection, reduction of energy consumption in the terminal, selection of zone per cost etc.

The choice of access network is consequently complex and time consuming. There are so many parameters to consider, e.g. access technology, available

operators, roaming agreements, presence of NATs, and/or firewalls, applicable policies, access rate, supported QoS, current load etc. The collection of these parameters takes long time. Some of this information is available through scanning of system information that is broadcast from access points or base stations and that can be received without any type of prior association, registration, authentication or connection. However, as described, retrieval of other parts of the information, potentially most of it, requires IP level communication between the terminal and the network. This in turn implies that the terminal has to go through all the preceding procedures that are needed to establish IP level communication. Normally the terminal must connect to each concerned access network in order to retrieve all access selection input data.

In the research community access selection schemes have been developed that rely on functionality in both the terminal and the network, typically with some kind of access awareness assistant or access selection wizard in the network helping the terminal by providing information or recommendations or even making decisions on behalf of the terminal in order to maintain operator control.

However, the network access awareness/access control function acts on explicit instructions from the terminal and/or current contextual information about the terminal's whereabouts and current activities. It is largely dependent on contextual information and/or the explicit instructions from the terminal and remains in a standby mode when the terminal is disconnected from the network. The advanced access selection schemes depend on information that requires IP communication to retrieve – scanning is not enough.

Moreover, gathering a multitude of information from potential access networks over resource scarce and error prone access link is time consuming. The network-based functionality off-loads the terminal-based access awareness/access control functionality, but still needs time to collect

and deliver the information. When the information is needed for an access selection decision, it will often take too long time to collect all the input data to enable a timely access selection decision.

Consequently, due to the time delay and the need for an IP communication, today's solutions do not allow swift, sophisticated access selection.

SUMMARY

The object of the present invention is to remove the above mentioned deficiencies of prior art solutions and to shorten the time for network access selection.

This object is enabled by means of a method for network access selection in a communication network. The network comprises an Access Selection Server (ASS), at least one User Equipment (UE), an Access Selection Client (ASC) arranged in the UE and communication nodes. The ASS collects access selection parameters used for the selection of access network for the network access for the UE in a multi-access environment. The network access enables a traffic bearer for a traffic flow between an application in the UE and a first node. The ASS forwards the access selection parameters and/or processes the access selection parameters and sends the results of the processed parameters to the UE. The parameters forwarded or the results sent by the ASS being access selection information, based on which the ASC performs activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow .

What particularly characterizes the method is that the ASS controls at least the collection or the processing of the access selection parameters, the collection or the processing at least being performed when the UE (14) is disconnected from the communication network. Furthermore, the parameters collected or processed when the UE is disconnected from the communication network are forwarded and/or the results of the processed parameters are

sent as access selection information by the ASS to the UE when the UE is again connected to the communication network.

This object is also enabled by means of an Access Selection Server (ASS) being adapted for network access selection. The ASS is arranged in a communication network further comprising at least one User Equipment (UE), an Access Selection Client (ASC) being arranged in the UE and communication nodes. The ASS is further adapted to collect access selection parameters used for the selection of access network for the network access for the UE in a multi-access environment. The network access enables a traffic bearer for a traffic flow between an application in the UE and a first node. The ASS further is adapted to forward the access selection parameters and/or process the access selection parameters and send the results of the processed parameters to the UE. The parameters forwarded or the results sent by the ASS being access selection information based on which the ASC performs activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow.

What particularly characterizes the ASS is that it is further adapted to control at least the collection or the processing of the access selection parameters. The ASS is further adapted to perform the collection or the processing at least when the UE is disconnected from the communication network. The ASS is further adapted to, when the UE (14) is again connected to the communication network, forward the parameters, collected or processed when the UE is disconnected from the communication network, and/or send the results of the processed parameters, as access selection information to the UE.

This object is finally enabled by means of a communication network for network access selection. The communication network comprises an Access Selection Server (ASS), at least one User Equipment (UE), an Access Selection Client (ASC) being arranged in the UE and communication nodes.

The ASS is adapted to collect access selection parameters used for the selection of access network for the network access for the UE in a multi-access environment. The network access enables a traffic bearer for a traffic flow between an application in the UE and a first node. The ASS further is adapted to forward the access selection parameters and/or process the access selection parameters and send the results of the processed parameters to the UE. The parameters forwarded or the results sent by the ASS being access selection information based on which the ASC performs activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow.

What particularly characterizes the ASS is that it is further adapted to control at least the collection or the processing of the access selection parameters. The ASS is further adapted to perform the collection or the processing at least when the UE is disconnected from the communication network. The ASS is further adapted to, when the UE (14) is again connected to the communication network, forward the parameters, collected or processed when the UE is disconnected from the communication network, and/or send the results of the processed parameters, as access selection information to the UE.

One advantage of the invention is that the solution enables swift, sophisticated access selection that takes data into account that cannot be retrieved from the respective candidate access networks through scanning from the terminal, but which requires established IP communication to retrieve. Another advantage it that it is general enough to be applicable in a variety of access selection solutions, including the ones being worked out in the research community_and in the 3GPP. Further advantages will be described in relation to the embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following text the invention will be described in detail with reference to the attached drawings. These drawings are used for illustration only and do not in any way limit the scope of the invention:

Figure 1 Schematically shows the communication system with the Access Selection functionality according to the present invention.

Figure 2 Schematically shows a flow diagram for the Access Selection functionality.

Figure 3 Shows a signalling diagram for the Access Selection functionality.

DETAILED DESCRIPTION

The invention will now be described in detail with reference to embodiments described in the detailed description and shown in the drawings.

The present invention focus on the problem that existing access selection solutions do not allow swift, sophisticated access selection that takes data into account that cannot be retrieved from the respective candidate access networks through scanning from the terminal. Instead it requires established IP communication to retrieve such data. Such network-based information is either gathered by network-based access selection functionality or by the terminal itself, potentially over a resource restricted and possibly delay prone radio connection. When the information is needed for an advanced access selection decision, it often, or even typically, takes too long to collect or process all the relevant input data to enable a timely access selection decision.

The embodiments refer to a method and a telecommunication system for network access selection, an Access Selection Server and an Access Selection Client, in the system enabling said method. The system, the server

and the client are adapted to perform the method steps as described in the method. It should be understood by a person skilled in the art that the fact that the system and in particular the system parts perform a method step means that it is adapted to perform said step.

The present invention relates to a method for network access selection comprising an Access Selection Server (ASS) 10 being arranged in a communication network 27, at least one User Equipment (UE) 14, an Access Selection Client (ASC) 21 being arranged in the UE and communication nodes 11, 12.

The communication network 27 is illustrated in figure 1. The term "node" is herein used in a general sense. It should be understood that different nodes may be integrated into a single node and that the functions represented/employed by a node could also be realized as separate nodes. The ASS 10 is located in the core network. Where it is located depends on which kind of access selection technology that is used (terminal- or network controlled). Examples of selection technologies are described in the background part. The communication nodes X 11 and Y 12 may for instance be databases, profile servers, Authentication/Authorization and Accounting (AAA) server, Home Subscriber Server (HSS), Session Initiation Protocol (SIP) proxies, Home Agents etc. What kind of nodes which are present depends on in which network/sub-network that the access selection function is located.

The functionality of the ASS 10, on which the invention is based, is illustrated in figure 2. The functionality comprises a learning stage 22 for the behaviour of a control of at least the collecting/receiving or processing of access selection parameters when the UE 14 is disconnected from the communication network 27. It further comprises a step 23 when the collecting/receiving or processing is performed. This is followed by a requesting stage 24 where the UE when being connected to the communication network requests the ASS to send/forward access selection

information. During step 25 the ASS sends/forwards the information and at step 26 the UE (the ASC in the UE) performs the access selection, handover or similar. The collecting/receiving is performed via connections 27, 16 and 17 from the nodes 11 – 12 and the access networks 13. The request is sent via connection 19 and the information is sent/forwarded via connection 20. The functionality will also be described step by step in the following text.

During operation the ASS collects 23 access selection parameters used for the selection 26 of access network for the network access for the UE 14 in a multi-access environment (more than one access network 13). What kind of parameters and how it is used (network or terminal controlled access selection 26) varies, and it should be understood that all kinds of access selection related parameters are included within the term "collected".

In particular, the ASS during operation receives 23, see figure 2, access selection parameters from the nodes 11,12 via the connections 27,16 established using reference points (not described further in this document) corresponding to a certain interfaces. Possible parameters received are e.g. node location information, connection information, disconnection information, network load information, policy-based restrictions and network-based information. The ASS further receives 23 network-based parameters from the different access networks 13 (1, 2 up to n) connected to the core network. This is enabled through a reference point 17. The interfaces referenced 18 – 20 will be described later.

The network access enables a traffic bearer for a traffic flow between an application in the UE 14 and a first node. A first node is for instance a peer node for peer-to-peer communication, e.g. Voice over IP communication, or an application server for client-server communication. The traffic preferably flows via a PDN-GW, which for instance could be a Systems Architecture Evolution (SAE) Gateway (GW)/Home Agent (HA) in a SAE network in a 3GPP domain or an access router. An application could for instance be VoIP or video calls. A first node is the receiver of the traffic flow from the UE.

The traffic bearer may be enabled between the UE 14 and a Packet Data Network Gateway (PDN GW) and the traffic flow between the application in the UE and a first node is then communicated via the PDN GW.

During operation the ASS 10 forwards 25 the access selection parameters and/or processes the access selection parameters and sends 25 the results of the processed parameters to the UE 14 using connection 20, see figure 1-2. The parameters forwarded or the results sent by the ASS are defined as access selection information. Results are network-based filtered and refined information.

From now on reference will be made to the UE 14 including the ASC 21. Since the ASC is included in the UE, the UE is able to perform activities in practise executed by the ASC.

Based on the access selection information, the UE 14, executed by the ASC 21, performs 26 activation of new network access and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow.

Access selection information is for instance instructions to the ASC to select 26 a certain access for the traffic bearer, the instruction being accompanied by for instance Quality of Service and Traffic Flow Template information. As another example the access selection information may be information that serves as input data to an access selection decision in the UE, e.g. rules guiding or directing such an access selection decision or input data in the form of information about the current state of the network(s) or access network(s).

What particularly characterizes the present invention is that the ASS 10 controls at least the collection or the processing 23 of the access selection parameters and that the collection or the processing 23 at least being performed when the UE 14 is disconnected from the communication network 27. The parameters collected or processed when the UE is disconnected

from the communication network are forwarded 25 and/or the results of the processed parameters are sent as access selection information by the ASS to the UE when the UE is again connected to the communication network.

In an access selection functionality it is an important task of the ASS 10 to feed 25 the UE 14 with relevant information collected from network-based sources 11, 12, and 13, which are not accessible through scanning from the UE 14. In addition to offloading the UE from some of the collection and processing 23 of information, the inventive solution proposes an adaptive feature in the ASS that allows it not only to provide the UE with relevant information, but also to prepare such information transfers while the UE is disconnected. This enables access selection 26 decisions that are both fast and sophisticated.

The ASS can collect and/or process 23 access selection parameters from various access networks 13. This is made through the reference point 17. What parameters to at least collect or process and from which access networks are normally determined by contextual information, such as the terminal's current point of connection, concerned applications, policy and profile data, etc. The problem with the known access selection technologies is that the ASS 10 can either itself analyze such contextual information received from the UE 14 or base its parameter collection on explicit instructions from the UE. The ASS is then largely dependent on the UE and remains in a standby mode when the terminal is disconnected from the communication network 27.

According to the characterizing part the present invention this dependency is partly removed by enabling the ASS 10 to maintain meaningful activity even when the UE 14 is disconnected from the communication network 27. During such time periods the ASS controls what parameters it should at least collect or process 23 and from which access networks 13 it should collect or process it. The purpose of collecting or processing parameters even when the UE is disconnected from the communication network is to be able to provide 25 the

ASC 21 in the UE with relevant access selection information without unnecessary delay as soon as the UE connects to the communication network 27 (and/or when requested by the UE). If the ASS has managed to collect or process parameters that actually turn out to be relevant, this method enables fast and sophisticated access selection 26.

According to one embodiment of the present invention the control by the ASS 10, comprising the control of at least the collection or the processing 23 of parameters by the ASS, is based on contextual information, historical records and/or statistics from the records for the communication network 27 location of the UE. An adaptive learning scheme is located in the ASS and controls at least the collection or the processing 23 of parameters. Also the sending and/or forwarding 25 of access selection information are preferably controlled by the adaptive learning scheme in the ASS.

To be able to adapt the control of at least the collection or processing 23 to the UE's history of movements, connections and disconnections the ASS has to be able to detect (and record) these actions from the UE which constitute the input data to the adaptive scheme.

A key component in the present invention is the control of at least the collection or the processing 23 behaviour by the ASS 10 (the adaptive learning scheme). According to the adaptive scheme the ASS continuously records relevant contextual information and learns 22 from historical records as well as statistics extracted from such records. The control behaviour is then continuously modified accordingly. There are different examples what kind of contextual information that the ASS can learn from:

According to a first example the time period between the disconnecting and the following connecting of the UE 14 to the communication network 27 is controlled. If the period exceeds a certain period value, the control of at least the collection or the processing 23 of parameters is at least based on:

1. Contextual information on where in the communication network 27 the UE is most likely to appear when connecting to the communication network, and

2. Which access network or networks the UE can select from when connecting to the communication network 27.

The statistics is based in information about the selectable access network or networks.

The ASS 10 consequently learns 22 where the UE 14 is most likely to "appear" after a significant period of disconnection and which access networks 13 that it then usually has to select between. The word "appear" is here used as a metaphor for connecting to the communication network 27. From the point of view of the ASS the UE is invisible as long as it is disconnected and visible only when it is connected to the communication network. Thus, in this context and with this "terminology" the word "appear" is a rather descriptive term for the event where the UE changes from being invisible to being visible.

Contextual data may take the shape of an access network 13, one or more access points/base stations, one or more cell(s)/zone(s) or even geographical data. The ASS 10 can learn 22 and maintain statistics about multiple such "locations of probable appearance". The knowledge acquired in this way allows the ASS 10 to proactively at least collect or process 23 data that is relevant for access selection 26 during initial connections.

In another example of what kind of contextual information that the ASS 10 can learn 22 from, the control of at least the collection the or processing 23 of parameters is at least based on movement pattern that reoccurs frequently. In this context movement pattern refers to movement between communication network 27 locations.

This means that the ASS 10 learns to which new location the UE 14 is likely to move from a certain current communication network 27 location. A "location" may in this context be an access network 13, an access point(s)/base station(s), one or more cell(s)/zone(s) or a geographical area (e.g. indicating the vicinity of a certain access network, a certain access point/base station or a certain cell/zone). The knowledge learnt 22 in this way allows the ASS to proactively at least collect or process 23 parameters that are relevant for access selection 26 during (potential) handovers. To refine its choice of information sources, the ASS may also take into consideration the currently used application(s).

The acquired knowledge may also be relevant for access selection 26 in a "camping" state, i.e. when the UE 10 is connected/associated with an access network 13, but not actively communicating. Optionally, the ASS 10 may maintain separate statistics on movement patterns for the UE 14 in the "camping" and actively communicating states respectively. An additional option for how to refine the statistics for movement patterns in an actively communicating state (i.e. for the purpose of handovers) is to take the currently used application(s) into account, such that movement pattern statistics per application or application type can be maintained.

In another example of what kind of contextual information that the ASS 10 can learn 22 from the time period between the disconnecting and the following connecting is below a certain period value. The control of at least the collection the or processing 23 of parameters is then at least based on the communication network 27 location where it was last connected.

According to this example, the ASS 10 learns 22 where the UE 14 is most likely to "reappear" after a brief (insignificant) period of disconnection based on the location where it was last connected. The word "reappear" is here used in a similar way as "appear". The purpose of the prefix "re" is to distinguish the situation where the UE has been "invisible" for the ASS for a limited period (below a certain period value) of time from the situation where

the UE has been "invisible" for a significant period (exceeds a certain period value) of time. The former case implies that the UE probably has not moved very long from the location where it was last "visible" for the ASS, whereas in the latter case the UE has had ample time to move even to locations far a way from the one where it was last "visible".

For instance, if the UE 14 was last disconnected from the communication network 27 in location α, then the ASS may have learnt 22 that if the UE connects to the communication network again within a certain limited period of time (implying a limited movement), it is likely to do this in location β (which may well be the same as location α). The definition of "location" in this context is the same as above. A more concrete or precise example could be that if a disconnected UE was last connected in cell X of access network A, then the ASS may have learnt that if the UE reconnects to the communication network within a certain limited period of time, then it will usually do this in cell Y in access network A with access networks B and C also within reach.

This means that when the UE 14 disconnects from cell X of access network A then, unless it is a handover, the ASS 10 starts at least collecting or processing 23 relevant parameters from access networks A (with focus on cell Y if applicable), B and C in order to be able to support quick access selection 26 if the UE 14 reappears (reconnects) as expected. However, if it takes too long before the UE reconnects, the ASS starts at least collecting or processing information according to the principles described above for the case where the UE is disconnected from the communication network 27 during a significant period of time, i.e. from the "location(s)" where the UE most commonly appears after a significant period of disconnection. Thus, the knowledge learnt in this way allows the ASS to proactively at least collect or process parameters that are relevant for access selection 26 during connection(s) in certain situations.

In accordance with one alternative of how the ASS 10 receives 23 information about the communication network 27 location of the UE, it gets information about the communication network location of the UE 14 explicitly. This means that the UE informs the ASS of its communication network location whenever it arrives in a location. The explicit information is the most important. The UE informs the ASS of its location with the detail/granularity needed, e.g. access network, cell, zone, access point, domain name, geographical data etc., whenever it arrives in a location (manifested as connection, handover, movement in idle mode or "camping" state). If the UE moves in a mode in which it is not configured for IP communication, IP configuration is required before explicitly informing the ASS of a new location. It may be argued that it is not beneficial to go to such lengths merely to inform the ASS of the new location of the UE, but it is at least a possible option.

In accordance with another alternative of how the ASS 10 receives information about the communication network 27 location of the UE 14, the ASS gets information about the network location of the UE implicitly. This means that the UE contacts the ASS for other purposes than to inform about its communication network location, during which contact the UE reveals its Internet Protocol address to the ASS.

In another alternative of how the ASS 10 receives information about the communication network 27 location of the UE it is also possible that the ASS can retrieve location information from other entities that possess knowledge about the location of a UE, such as a SIP proxy, a Mobile IP Home Agent, a AAA server or a HSS.

Within one embodiment of the present invention the Uniform Resource Identifier (URI) of an access network's local network profile is sent by the UE 14 to the ASS 10 when being connected to the communication network 27. The URI may be delivered to a UE in Dynamic Host Configuration Protocol (DCHP) option 15 during the DCHP configuration procedure. In some cases

it is possible that the relevant information cannot be located without prior information that is only available through scanning 18, see figure 1, or by connecting to a certain access link. One example is this retrieval of a local network profile located through a URI that is delivered in DHCP option 15. Since DHCP relies on link-local mechanisms like broadcast, this URI can only be retrieved by a device connected to the concerned access network. In cases like this, the UE will transfer to the ASS 10 the information that is required to locate certain relevant information, e.g. in the form of a URI for a local network profile or a domain name for information in general.

The UE 14 will do this opportunistically, i.e. any time that the UE has contact with the ASS 10 and concerning any information that may potentially be relevant for the ASS to retrieve. Out of the information of this type that the ASS receives from the UE, it may choose to retain only a selected part that turns out to be useful within a reasonable time. In other words, information of this type that the ASS does not use is eventually timed out and deleted.

Within one embodiment of the present invention the UE 14 subscribes to certain events from the ASS 10. The ASS continuously monitors the information sources that are relevant for the subscribed events and when a criteria for a subscribed event is fulfilled the ASS sends a notification to the UE. Such events may e.g. be changes in policies, Quality of Service support or load. The ASS continuously monitors the information sources that are relevant for the subscribed events and when the criteria for a subscribed event are fulfilled, the ASS sends a notification to the UE.

The sending and/or forwarding 25 of information are preferably controlled by the ASS 10. The access selection information is preferably sent/forwarded to the UE 14 through the interface 20. The access selection information is not available through scanning from the UE.

The notion of the ASS controlling the sending and/or forwarding 25 of information may constitute that the ASS determines which information and/or

which type of information that is appropriate to send/forward to the UE in each particular situation.

The notion of the ASS controlling the sending and/or forwarding 25 of information may also constitute that the access selection information is sent and/or forwarded 25 to the UE when requested by the UE. Such a request is sent when the UE is again connected to the communication network 27. The request may optionally be sent immediately when the UE connects to the communication network. The request is sent via a communication interface 19 between the ASS and the ASC. Figure 2 illustrates this alternative.

Proactively collected 23 parameters (as well as more reactively collected parameters) are typically transferred 25 to the UE 14 on request 24, i.e. the UE retrieves the access selection information from the ASS 10. When an access selection 26 situation arises in the ASC 21 in the UE 14 and the decision requires input data that can beneficially (or only) be collected by the ASS 10, then the UE requests the ASS to at least collect or process the concerned parameters and transfer it as access selection information to the UE.

If the ASS's adaptive, proactive behaviour has been successful and the requested 24 parameters consequently are already at least collected or processed 23, then the ASS can transfer 25 it as access selection information to the UE immediately. Otherwise, the ASS has to collect or process 23 the requested parameters before it can transfer 25 it to the UE. From the UE's point of view these two situations differ only in how quick the UE receives the requested access selection information from the ASS.

There are two major cases of access selection 26 in the context of the UE requesting access selection information from the ASS 10. In one case the UE 14 requests 24 the access selection information from the ASS via anyone of the access networks 13 that the UE is connected to. This for instance relate to access selection 26 for handover of a connection or access selection 26

for a new connection request from an application when the UE is already connected. If the UE is connected to one or more access network(s) when the access selection situation arises, it can use any one of the connected accesses to send its request 24 for access selection information to the ASS.

The other case relates to access selection when the UE is not connected to an access network, e.g. for access/cell selection in idle mode (also known as access selection for "camping") or access selection for a connection (socket) request from an application when the terminal is disconnected/idle.

If the UE 14 is not connected to an access network 13 when the access selection situation arises, it has to connect to one of the available access networks before requesting 24 the information from the ASS. Which one of the available accesses to choose for this communication may be governed by default policies (with information retrieved through scanning as input data, possibly enhanced with old, cached contextual data, such as application usage history and additional information about the discovered access networks). If the access selection 26 is only for idle mode (in the sense that no IP configuration is required) then it may not be considered worthwhile to connect to an access network (going through authentication and IP configuration etc.) merely to be able to retrieve information from the ASS and consequently it is an option to rely only on information that can be retrieved through scanning or from within the terminal in such situations.

The notion of the ASS controlling the sending and/or forwarding 25 of information may finally constitute in that the ASS (10) sends and/or forwards the access selection information to the UE (14) after receiving an indication from another network entity that the UE has connected to one of the available access networks. The ASS consequently transfers access selection information to the UE without a prior request, when it receives an indication from another network entity, e.g. an AAA server that the UE has connected to the communication network 27 (provided that the ASS has a means to appropriately address the UE with this information transfer).

Figure 3 shows a signalling diagram illustrating the Access Selection functionality according to the present invention. When the UE 14 is disconnected D from the communication network 27, the ASS 10 checks 1 historical records, statistics etc. in order to control at least the collection or processing of parameters. The ASS further requests 2 and receives 3 network-based information from the network based entity X 11 and receives 4 unsolicited network-based information from the network-based entity Y 12Y 12. The communication nodes X and Y may for instance be databases, profile servers, Authentication/Authorization and Accounting (AAA) server, Home Subscriber Server (HSS), Session Initiation Protocol (SIP) proxies, Home Agents etc.

When the UE 14 again connects C to for instance access node 1 (AN (1)) 13 it sends 5 location information and a request for access selection information to the ASS. The ASS 10 sends 6 back such information to the ASC 21 in the UE. Then ASC in the UE then processes 7 the access selection information.

Depending on the outcome of the processing 7 by the UE, certain actions 8 are performed. As a possibility the UE connects 8A to access node 2 (AN(2)) 13 and possibly disconnects 8B from AN(1) 13.

It will also be appreciated by a person skilled in the art that various modifications may be made to the above-described embodiments without departing from the scope of the present invention.

CLAIMS

1. A method for network access selection (26) in a communication network (27) comprising an Access Selection Server (ASS) (10), at least one User Equipment (UE) (14), an Access Selection Client (ASC) (21) being arranged in the UE (14) and communication nodes (11,12),

the ASS (10) collecting (23) access selection parameters used for the selection (26) of access network for the network access for the UE (14) in a multi-access environment

the network access enabling a traffic bearer for a traffic flow between an application in the UE (14) and a first node,

the ASS (10) forwarding (25) the access selection parameters and/or processing (23) the access selection parameters and sending (25) the results of the processed parameters to the UE,

the parameters forwarded or the results sent (25) by the ASS (10) being access selection information based on which the ASC (21) performs (26) activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow ,

characterized in that

the ASS (10) controls at least the collection or the processing (23) of the access selection parameters, the collection or the processing (23) at least being performed when the UE (14) is disconnected from the communication network (27),

the parameters collected or processed (23) when the UE (14) is disconnected from the communication network (27) are forwarded (25) and/or the results of the processed parameters are sent as access selection

information by the ASS (10) to the UE (14) when the UE (14) is again connected to the communication network (27).

2. Method according to claim 1 wherein the control by the ASS of at least the collection or the processing (23) of parameters is based on contextual information, historical records and/or statistics from the records for the communication network (27) location of the UE (14).

3. Method according to claim 2 wherein an adaptive learning scheme being located in the ASS (10) controls at least the collection or the processing (23) of parameters.

4. Method according to any of the claims 2 - 3 wherein if the time period between the disconnecting and the following connecting exceeds a certain period value, the control of at least the collection or the processing (23) of parameters is at least based on:

contextual information on where in the communication network (27) the UE (14) is most likely to appear when connecting to the communication network (27), and

which access network or networks the UE can select from when connecting to the communication network (27).

5. Method according to claim 4 wherein the statistics is based in information about the selectable access network or networks (13).

6. Method according to any of the claims 2 – 5 wherein the control of at least the collection or the processing (23) of parameters is at least based on movement patterns that reoccurs frequently, the patterns being movement between communication network (27) locations.

7. Method according to any of the claims 2 - 6 wherein if the time period between the disconnecting and the following connecting is below a certain period value the control of at least the collection or the processing (23) of

parameters is at least based on the communication network (27) location where it was last connected.

8. Method according to any of the claims 2 - 7 wherein the ASS (10) gets information about the communication network (27) location of the UE (14) explicitly, in which the UE (14) informs the ASS (10) of its communication network (27) location whenever it arrives in a location.

9. Method according to any of the claims 2 - 7 wherein the ASS (10) gets information about the communication network (27) location of the UE (14) implicitly, in which the UE (14) contacts the ASS (10) for other purposes than to inform about its communication network (27) location, during which contact the UE (14) reveals its Internet Protocol address to the ASS (10).

10. Method according to any of the preceding claims wherein the access selection information is not available through scanning from the UE (14).

11. Method according to any of the preceding claims wherein a Uniform Resource Identifier (URI) of an access network's local network profile, is sent by the UE (14) to the ASS (10) when being connected to the communication network (27).

12. Method according to any of the preceding claims wherein the UE (14) subscribes to certain events from the ASS (10), the ASS (10) continuously monitoring the information sources that are relevant for the subscribed events and when a criteria for a subscribed event is fulfilled the ASS (10) sends a notification to the UE (14).

13. Method according to any of the preceding claims wherein the access selection information is sent and/or forwarded (25) to the UE when requested (24) by the UE .

14. Method according to any of the preceding claims wherein the UE (14) requests (24) the access selection information from the ASS (10) via any of the access networks (13) that the UE (14) is connected to.

15. Method according to any of the preceding claims wherein the ASS (10) sends and/or forwards the access selection information after receiving an indication from another network entity that the UE has connected to one of the available access networks.

16 Access Selection Server (ASS) (10) being adapted for network access selection (26), the ASS (10) being arranged in a communication network (27) further comprising at least one User Equipment (UE) (14), an Access Selection Client (ASC) (21) being arranged in the UE (14) and communication nodes (11,12),

the ASS (10) further is adapted to collect (23) access selection parameters used for the selection (26) of access network for the network access for the UE (14) in a multi-access environment,

the network access enabling a traffic bearer for a traffic flow between an application in the UE (14) and a first node,

the ASS (10) further is adapted to forward (25) the access selection parameters and/or process (23) the access selection parameters and send (25) the results of the processed parameters to the UE,

the parameters forwarded or the results sent (25) by the ASS (10) being access selection information based on which the ASC (21) performs activation (26) of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow,

characterized in that

the ASS (10) is further adapted to control at least the collection or the processing (23) of the access selection parameters,

the ASS is further adapted to perform the collection or the processing (23) at least when the UE is disconnected from the communication network (27),

the ASS (10) is further adapted to, when the UE (14) is again connected to the communication network (27), forward (25) the parameters, collected or processed (23) when the UE (14) is disconnected from the communication network (27), and/or send the results of the processed parameters, as access selection information to the UE (14).

17. The ASS (10) according to claim 16 wherein the ASS is adapted to perform the control of at least the collection or the processing (23) of parameters on the basis of contextual information, historical records and/or statistics from the records for the communication network (27) location of the UE (14).

18. The ASS (10) according to claim 17 wherein an adaptive learning scheme located in the ASS (10) is adapted to control at least the collection or the processing (23) of parameters.

19. The ASS (10) according to any of the claims 17 - 18 wherein the ASS (10) is adapted to get information about the communication network (27) location of the UE (14) explicitly, in which the UE (14) informs the ASS (10) of its communication network (27) location whenever it arrives in a location.

20. The ASS (10) according to any of the claims 17 – 18 wherein the ASS (10) is adapted to get information about the communication network (27) location of the UE (14) implicitly, in which the UE (14) contacts the ASS (10) for other purposes than to inform about its communication network (27) location, during which contact the UE (14) reveals its Internet Protocol address to the ASS (10).

21. The ASS (10) according to any of the claims 16 – 20 wherein the UE (14) subscribes to certain events from the ASS (10), the ASS (10) is further adapted to continuously monitor the information sources that are relevant for

the subscribed events, and when a criteria for a subscribed event is fulfilled the ASS (10) is further adapted to send a notification to the UE (14).

22. The ASS (10) according to any of the claims 16 - 21 wherein the ASS (10) is further adapted to send and/or forward (25) the access selection information to the UE when requested (24) by the UE .

23. The ASS (10) according to any of the preceding claims wherein the ASS (10) is further adapted to send and/or forward the access selection information after receiving an indication from another network entity that the UE has connected to one of the available access networks.

24. A communication network (27) for network access selection (26), the communication network (27) comprising an Access Selection Server (ASS) (10), at least one User Equipment (UE) (14), an Access Selection Client (ASC) (21) being arranged in the UE (14) and communication nodes (11,12),

the ASS (10) is adapted to collect (23) access selection parameters used for the selection (26) of access network for the network access for the UE (14) in a multi-access environment,

the network access enabling a traffic bearer for a traffic flow between an application in the UE (14) and a first node,

the ASS (10) is further adapted to forward (25) the access selection parameters and/or process (23) the access selection parameters and send (25) the results of the processed parameters to the UE (14),

the parameters forwarded (25) or the results sent (25) by the ASS being access selection information based on which the ASC (21) is adapted to perform (26) activation of new network accesses and/or selection, modification, deactivation or change of existing network accesses in order to enable the traffic flow,

characterized in that

the ASS (10) is further adapted to control at least the collection or the processing (23) of the access selection parameters,

the ASS is further adapted to perform the collection or the processing (23) at least when the UE (14) is disconnected from the communication network (27),

the ASS is further adapted to, when the UE (14) is again connected to the communication network (27), forward (25) the parameters collected or processed (23) when the UE (14) is disconnected from the communication network (27), and/or send the results of the processed parameters, as access selection information to the UE (14).

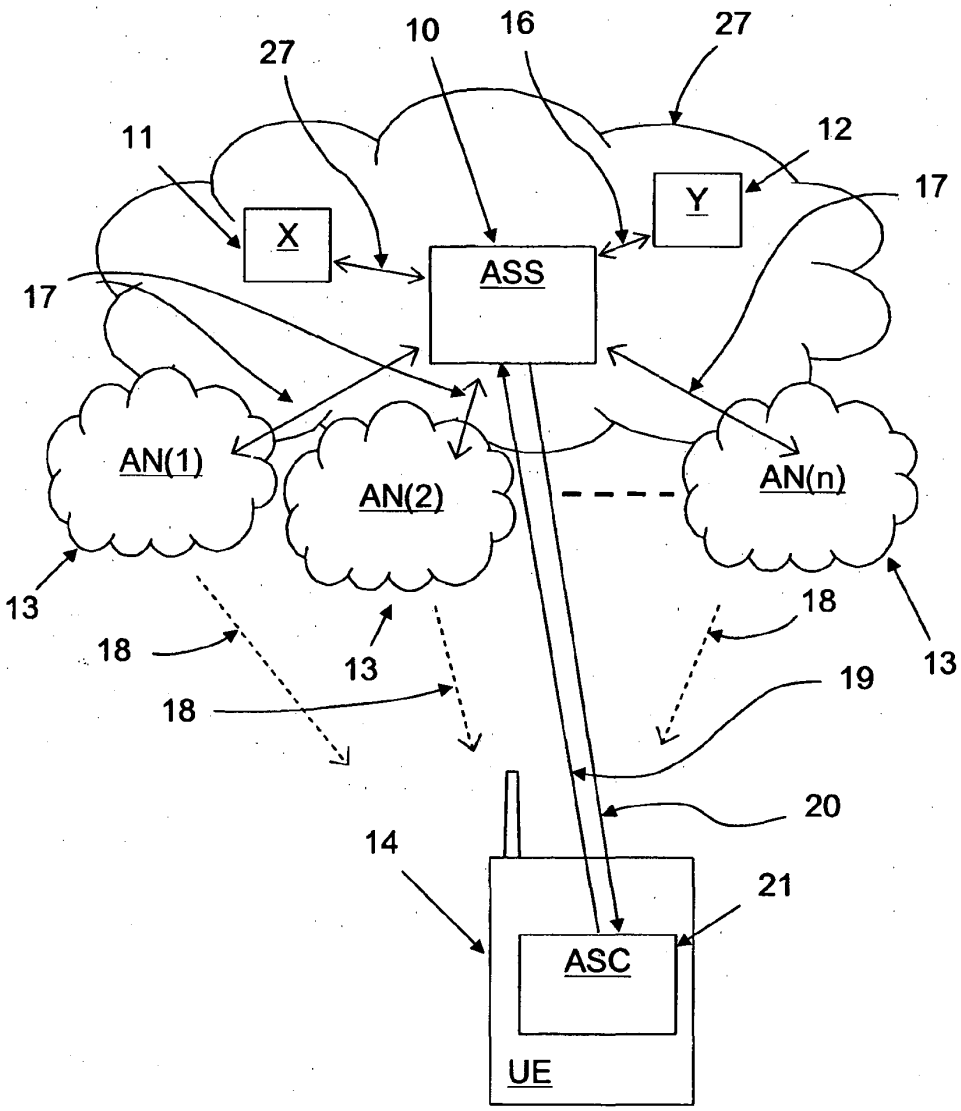

27
10
16
27
11
12
17
X
Y
ASS
17
AN(1)
AN(2)
AN(n)
13
18
13
18
13
18
19
20
14
21
ASC
UE

FIG 1

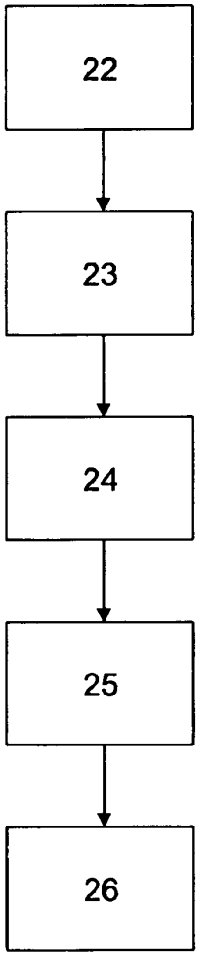


FIG 2

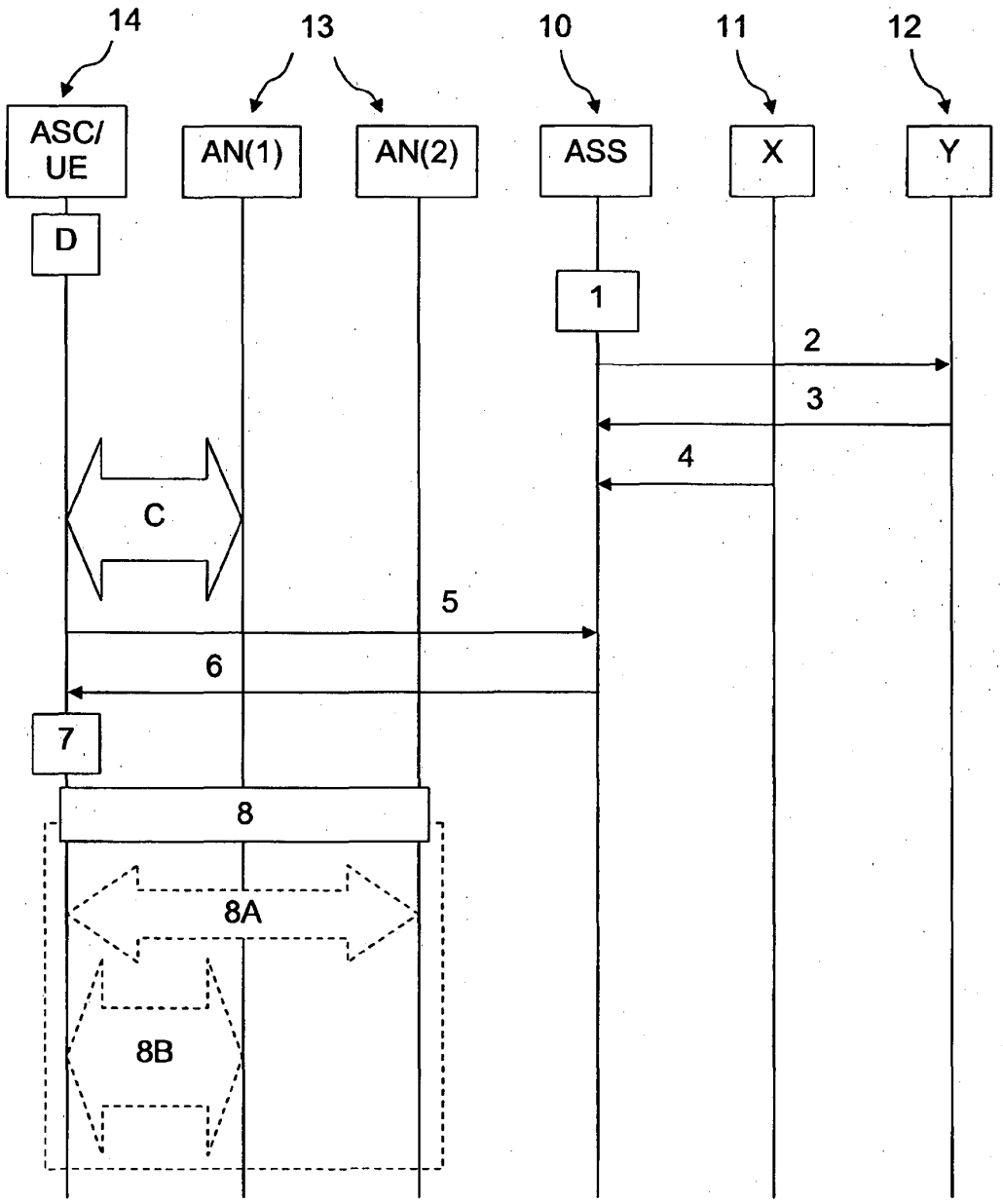


FIG 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/000031

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
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)

IPC: H04Q, H04L

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2005117463 A2 (NOKIA CORP.), 8 December 2005 (08.12.2005), figures 1-5, claims 1-26, paragraphs [0009] - [0041] --	1-24
A	XP005333980, Kaloxylos et al, "A flexible handover mechanism for seamless service continuity in heterogeneous environments", 20060331 ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, NL VOL - 29 NR - 6 PG - 717 - 729 See the whole document --	1-24

[X] Further documents are listed in the continuation of Box C. [X] 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	Date of mailing of the international search report
30 October 2008	06-11-2008
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Elisabet Aselius/PR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2008/000031

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	WO 2008043970 A1 (FRANCE TELECOM), 17 April 2008 (17.04.2008), page 1, line 7 - page 5, line 15, figures 1-4, claims 1-10, abstract ---	1-24
A	US 20040218605 A1 (GUSTAFSSON ET AL), 4 November 2004 (04.11.2004), figures 1-8, claims 1-29, abstract, paragraphs [0013] - [0018] ---	1-24
A	WO 2006103402 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY), 5 October 2006 (05.10.2006), page 1, line 25 - page 2, line 35, figures 1-4, claims 1-13, abstract --- --------	1-24

Form PCT/ISA/210 (continuation of second sheet) (July 2008)

International patent classification (IPC)
H04Q 7/38 (2006.01)
H04Q 7/32 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument(service in Swedish).

Use the application number as username.
The password is **GLZJVOXTPZ.**

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

WO	2005117463	A2	08/12/2005	AU	2005330571	A	07/12/2006
				CN	1957634	A	02/05/2007
				EP	1749419	A	07/02/2007
				JP	2008500756	T	10/01/2008
				US	20080064393	A	13/03/2008
WO	2008043970	A1	17/04/2008	NONE			
US	20040218605	A1	04/11/2004	NONE			
WO	2006103402	A1	05/10/2006	EP	1708526	A	04/10/2006
				EP	1864533	A	12/12/2007

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 November 2002 (21.11.2002)

PCT

(10) International Publication Number
WO 02/093877 A1

(51) International Patent Classification[7]: H04M 1/00, 3/00, 3/42, 11/10, H04B 1/38

(21) International Application Number: PCT/IB02/01550

(22) International Filing Date: 7 May 2002 (07.05.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/854,628 15 May 2001 (15.05.2001) US

(71) Applicants: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI). **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, TX 75039 (US).

(72) Inventors: **NYKÄNEN, Petri**; Lehdokkikatu 3, FIN-37120 Nokia (FI). **PALONIEMI, Jari**; Yliki-imingintie 169, FIN-90900 Kiiminki (FI). **KANGAS, Petri**; Pölkkytie 7A3, FIN-90800 Oulu (FI).

(74) Agent: **HOEL, John**; Morgan & Finnegan, LLP, 345 Park Avenue, New York, NY 10154 (US).

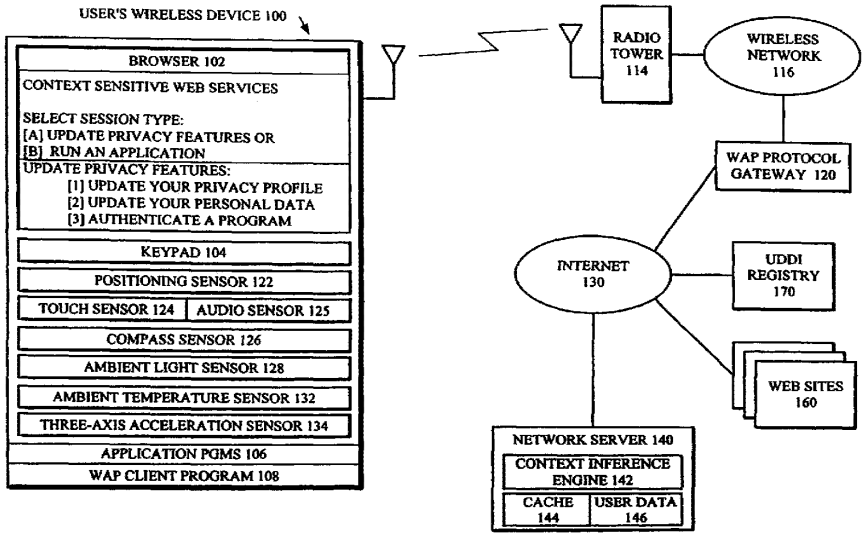
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: CONTEXT SENSITIVE WEB SERVICES



(57) Abstract: The context sensitive web services method enables a mobile phone or wireless device (100) to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment. The method includes the steps of receiving sensor signals (122-134) characterizing a current environment of the wireless device (100); processing the sensor signals with a context inference engine (142); outputting a current context result from the processing by the context inference engine (142); and providing useful information to the user in response to the current context result.

WO 02/093877 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONTEXT SENSITIVE WEB SERVICES

This application claims priority to U.S. Application Serial No. 09/857,628, filed May 15, 2001, entitled, "Context Sensitive Web Services, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of the Invention:

The invention disclosed broadly relates to methods for providing Internet services and more particularly relates to improvements in mobile device accessing of Internet services.

Background Art:

Mobile phones and wireless personal digital assistants (PDAs) are able to access the Internet using the Wireless Application Protocol (WAP). WAP-enabled wireless devices can now access Internet applications such as headline news, exchange rates, sports results, stock quotes, weather forecasts, multilingual phrase dictionaries, personal online calendars, online travel and banking services, or download distinctive ringing tones. Broadband wireless networks make it possible for WAP-enabled wireless devices to exchange multimedia messages that combine conventional text with much richer content types, such as photographs, images, voice clips, and video clips. WAP-enabled wireless devices can be used to pay bills online using the wireless device as a virtual wallet. WAP-enabled wireless devices can deliver useful and informative advertising and transaction services from online merchants. WAP-enabled wireless devices now also provide entertainment services, such as interactive adventure games, quizzes, and chess tournaments.

What is needed is the ability of a mobile phone or wireless PDA to use context inference techniques to sense the mobile user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment. It would be even more useful to offload some of the computationally intensive computing necessary in context inference techniques, from the mobile user's wireless device to a server and to web sites on the Internet. It would be beneficial to maintain a personal

CONFIRMATION COPY

profile of the mobile user's personal preferences in an online server or web site. It would be important to provide the mobile user with the ability to control any access to the user's profile by the online server or web site.

SUMMARY OF THE INVENTION:

The context sensitive web services invention enables a mobile phone or wireless PDA to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment.

One aspect of the invention is a method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment. The method includes the steps of receiving sensor signals characterizing a current environment of the wireless device; processing the sensor signals with a context inference engine; outputting a current context result from the processing by context inference engine; and providing useful information to the user in response to the current context result. The processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device. In another aspect of the invention, the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device. The server can access files from a web server, for selective forwarding to the user's wireless device. A personal profile of the user can be maintained by the server.

A further aspect of the invention provides user control of access by application programs to the user's private data. This can also include providing user control of access by application programs to the user's private data in the server. Still further, this can also include providing user control of access by application programs in a web server, to the user's private data.

Another aspect of the invention is providing the current context result to an application program in response to the user control and receiving the useful information from the application program. The invention enables the user to grant access permission to the application program to access the current context result. This can be performed in

the user's wireless device or in the network server. The network server can carry out the control of access by application programs in web servers, in response to a user privacy profile received from the user's wireless device.

DESCRIPTION OF THE FIGURES:

Figure 1 is a network diagram of the invention, showing an example relationship between the user's Wireless Application Protocol (WAP)-enabled portable wireless device, the WAP protocol gateway to the Internet, the network server, the Universal Description, Discovery and Integration (UDDI) registry, and a plurality of web sites.

Figure 1A shows the user's wireless device with the UPDATE PRIVACY FEATURES: sub-menu of the Context Sensitive Services menu, enabling the user to UPDATE YOUR PRIVACY PROFILE or UPDATE YOUR PERSONAL DATA.

Figure 1B shows the user's wireless device with the UPDATE PRIVACY FEATURES: sub-menu of the Context Sensitive Services menu, enabling the user to AUTHENTICATE A PROGRAM and REGISTER A PROGRAM.

Figures 1C and 1D show the user's wireless device with the RUN AN APPLICATION sub-menu of the Context Sensitive Services menu, enabling the user to RUN AN APPLICATION.

Figure 2 is a functional block diagram of the wireless device 100, showing its various components and programs.

Figure 2A is a functional block diagram of the wireless device 100, the server 140, and the web server 160, and their interaction when exchanging a metadata vector 138 and privacy control data 150.

Figure 3 is a network process flow diagram of the interaction of the wireless device 100, network server 140, and web server 160 when carrying out the determination of the current context of the wireless device 100.

Figure 4 is a functional block diagram of the network server 140, showing the memory storing the application services software programs needed to perform the operations of the invention.

DISCUSSION OF THE PREFERRED EMBODIMENT:

The context sensitive web services invention enables a mobile phone or wireless PDA to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's perceived environment. The invention offloads some of the computationally intensive computing necessary in context inference techniques, from the mobile user's wireless device to a server and to web sites on the Internet. The context sensitive web services invention maintains a personal profile of the mobile user's personal preferences in an online server or web site. The mobile user is provided with the ability to control access by application programs in the wireless device, to the user's private data. The context sensitive web services invention provide the mobile user with the ability to control any access to the user's profile by the online server or web site.

The mobile user's wireless device is equipped with a context inference engine for providing and awareness of the mobile user's context to application programs, including third party applications. Since the processing power and storage capacity is limited in typical wireless devices, the computational load and storage requirements of the context inference engine are distributed to a context inference server capable of processing the context data. The invention enables the mobile user to control which application programs in the wireless device are granted access to the user's private context information. A privacy control block in the wireless device grants or revokes access by application programs to the private context information, based on the mobile user's preferences stored in a privacy profile. The same privacy control and privacy profile is extended to the context inference server, thereby enabling the extension of the user's privacy control to any web server connected to the context inference server. The invention thus enables building an infrastructure for context sensitive applications and services within the wireless device and the server, while providing to the mobile user control over the privacy user's context information.

The invention is applied to wireless telephones and wireless personal digital assistants (PDAs) implementing the Wireless Application Protocol (WAP) standard. Figure 1 is a network diagram of an embodiment of the invention, showing an example relationship between the user's Wireless Application Protocol (WAP)-enabled portable wireless device 100, a WAP protocol gateway 120, and the server 140. The user's WAP-enabled portable wireless device 100 can be a wireless mobile phone, pager, two-way

radio, smartphone, personal communicator, or the like. The user's WAP-enabled portable wireless device 100 accesses a small file called a deck which is composed of several smaller pages called cards which are small enough to fit into the display area of the device's microbrowser 102. The small size of the microbrowser 102 and the small file sizes accommodate the low memory constraints of the portable wireless device 100 and the low-bandwidth constraints of a wireless network 116. The cards are written in the Wireless Markup Language (WML) which is specifically devised for small screens and one-hand navigation without a keyboard. The WML language is scaleable from two-line text displays on the microbrowser 102 of a cellular telephone, up through large LCD screens found on smart phones and personal communicators. The cards written in the WML language can include programs written in WMLScript, which is similar to JavaScript, but makes minimal demands on memory and CPU power of the device 100 because it does not contain many of the unnecessary functions found in other scripting languages.

The Nokia WAP Client Version 2.0 is a software product containing the components necessary to implement the WAP client 108 on the wireless device 100. These components include a Wireless Markup Language (WML) Browser, WMLScript engine, Push Subsystem, and Wireless Protocol Stack. The Nokia WAP Client is a source-code product that can port and integrate into wireless devices such as mobile phones and wireless PDAs. Application programs 106 stored in the wireless device 100 interact with the WAP Client 108 to implement a variety of communications applications. Details of the Nokia WAP Client Version 2.0 can be found in the online paper: Nokia WAP Client Version 2.0, Product Overview, Nokia Internet Communications, 2000, www.nokia.com/corporate/wap.

The WAP Client 108 includes the Wireless Public Key infrastructure (PKI) feature, providing the infrastructure and the procedures required for authentication and digital signatures for servers and mobile clients. Wireless PKI is a certificate-based system that utilizes public/private key pairs associated with each party involved in a mobile transaction. Wireless Identity Module (WIM) is a security token feature of the WAP Client 108, which includes security features, such as the public and private keys and service certificates, needed for user authentication and digital signatures. Additionally, it has the ability to perform cryptographic operations to encrypt and decrypt messages.

The wireless device 100 of Figure 1 also has a plurality of sensors for sensing the mobile user's ambient conditions. The sensors shown include POSITIONING SENSOR 122, TOUCH SENSOR 124, AUDIO SENSOR 125, COMPASS SENSOR 126, AMBIENT LIGHT SENSOR 128, AMBIENT TEMPERATURE SENSOR 132, and THREE-AXIS ACCELERATION SENSOR 134. The audio sensor 125 can be a microphone, for example, which can detect speech or environmental sounds. The positioning sensor can be, for example, a GPS receiver integrated in the device. The positioning sensor can also be, for example, a radio beacon triangulation sensor that determines the location of the wireless device by means of a network of radio beacons, base stations, or access points, as is described for example, in Nokia European patent EP 0 767 594 A2, entitled "Mobile Station Positioning System". These sensors provide inputs which are sampled by the wireless device 100 to infer a current context, as will be described below.

The WAP protocol gateway 120 links the Internet 130 and the wireless network 116. The WAP protocol gateway 120 includes the Wireless Public Key infrastructure (PKI) feature to help provide a secure Internet connection to the wireless device 100. The WAP protocol gateway 120 enables the WAP-enabled wireless device 100 to access Internet applications such as headline news, exchange rates, sports results, stock quotes, online travel and banking services, or to download distinctive ringing tones.

The user's WAP-enabled portable wireless device 100 communicates with the radio tower 114 and can exchange messages for distances up to several kilometers. The types of wireless networks 116 supported by the WAP standard include Cellular Digital Packet Data (CDPD), Code-Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), Time Division Multiple Access (TDMA), GPRS, 3G-Broadband, and the like.

The overall process of communication between the user's WAP-enabled wireless device (the client) 100, through the WAP protocol gateway 120, to the server 140 resembles the way Web pages are served on the Internet using the HyperText Transfer Protocol (HTTP) or World Wide Web protocol:

[1] The user presses a phone key on the user's device 100 related to the Uniform Resource Locator (URL) of the server 140.

[2] The user's device 100 sends the URL, via the radio tower 114 and the wireless network 116, to the gateway 120 using WAP protocols.

[3] The gateway 120 translates the WAP request into an HTTP request and sends it over the Internet 130 to the server 140, via Transmission Control Protocol/ Internet Protocol (TCP/IP) interfaces.

[4] The server 140 handles the request just like any other HTTP request received over the Internet. The server 140 either returns a WML deck or a HyperText Markup Language (HTML) page back to the gateway 120 using standard server programs written, for example in Common Gateway Interface (CGI) programs, Java servlets, or the like.

[5] The gateway 120 receives the response from the server 140 on behalf of the user's device 100. If the response is an HTML page, it gets transcoded into WML if necessary. Then the WML and WMLScript coding is encoded into a byte code that is then sent to the user's device 100.

[6] The user's device 100 receives the response in the WML byte code and displays the first card in the deck on the microbrowser 102 to the user.

In Figure 1, the protocol gateway 120 includes a WAP protocol stack organized into five different layers. An application layer is the wireless application environment, which executes portable applications and services. A session layer is the wireless session protocol, which supplies methods for the organized exchange of content between client/server applications. A transaction layer is the wireless transaction protocol, which provides methods for performing reliable transactions. A security layer is the wireless transport layer security, which provides authentication, privacy, and secure connections between applications. The transport layer is the wireless datagram protocol, which shelters the upper layers from the unique requirements of the diverse wireless network protocols, such as CDPD, CDMA, GSM, etc. Additional information about the WAP standard and the WAP protocol stack can be found in the book by Charles Arehart, et al. entitled, "Professional WAP", published by Wrox Press Ltd., 2000 (ISBN 1-861004-04-1).

In Figure 1, the user's portable wireless device 100 includes the microbrowser 102 displays the Context Sensitive Services menu, to enable the user to navigate through the cards being displayed and to select options that are programmed by the application

programs 106. The user's device 100 also includes the WAP client program 108 which has been previously discussed.

The Context Sensitive Services menu displayed by the microbrowser 102 in Figure 1 is rendered by the WAP client program 108 under the control of the application programs 106, which are shown in Figures 2 and 2A. The user can select the session type with Context Sensitive Services menu, either [A] UPDATE PRIVACY FEATURES or [B] RUN AN APPLICATION. If the UPDATE PRIVACY FEATURES session type is selected by the user, the Context Sensitive Services menu of Figure 1 then presents to the user the UPDATE PRIVACY FEATURES sub-menu from which the user can select the following options:

[A] UPDATE PRIVACY FEATURES:
[1] UPDATE YOUR PRIVACY PROFILE
[2] UPDATE YOUR PERSONAL DATA
[3] AUTHENTICATE A PROGRAM

Option [1] of UPDATE YOUR PRIVACY PROFILE, leads to a second sub-menu shown in Figure 1A, which has the following options:

[1] UPDATE YOUR PRIVACY PROFILE
[a] Add a local program to permissions list
[b] Remove a local program from list
[c] Add a server program to permissions list
[d] Remove a server program from list
[e] Add a network program to permissions list
[f] Remove a network program from list.

Option [2] of UPDATE YOUR PERSONAL DATA, leads to a another sub-menu shown in Figure 1A, which has the following options:

[2] UPDATE YOUR PERSONAL DATA
[a] Update server database
[b] Update network database.

Option [3] of AUTHENTICATE A PROGRAM, leads to a another sub-menu shown in Figure 1B, which has the following options:

[3] AUTHENTICATE A PROGRAM
[a] Request program's public key certificate
[b] Verify certificate signatures

[c] Verify validity time
[d] Verify revocation status
[e] Check if certificate authority on trust list
[f] Flag program as authenticated.

The AUTHENTICATE A PROGRAM option calls the privacy control 150 of the wireless device 100 in Figure 2. If an application program A, B, X, or Y has been verified for its acceptability by a trusted authority, then the trusted authority will have issued a digital certificate on a message authentication code (MAC) it has computed for the application program, which can be checked by the privacy control 150. As long as the privacy control 150 trusts the trusted authority issuing the digital certificate, authentication of the application program is straight forward.

Once the mobile user has verified the program's digital certificate and is satisfied that the application program will not subvert the integrity or security of the user's private data, the user can register the program. Registration is the granting by the user of access permission to the program, to access the current context of the user's wireless device and/or to access other portions of the user's private data. There are several levels of permission that can be granted by the user in two categories, [a] when can the accesses take place and [b] what data can be accessed.

Option [4] of REGISTER A PROGRAM, leads to a another sub-menu shown in Figure 1B, which has the following options:

[4] REGISTER A PROGRAM
[a] When can the accesses take place
[b] What data can be accessed

For the first category of [a] when can the accesses take place, the highest level of permission in this category is that access can occur anytime and without notice. The lowest level of permission in this category is that access can only occur at specified times or under specified conditions, and only after notice to the user and specific authorization by the user. For the second category of [b] what data can be accessed, the highest level of permission in this category is to access unlimited datasets in the user's private data, including current context information, personal data entered by the user, the user's Internet usage history data, the user's Internet cookie data, and the user's application program usage data. The lowest level of permission in this category is that access of any data can

only occur after notice to the user and specific authorization by the user. The user can configure any levels of permission in between the highest and lowest and make that the basis for the registration. The user can include the terms of registration in a digital certificate signed by the user and appended to the application program. This registration certificate can be presented by the program to the privacy control 150 prior to a proposed access event, the privacy control 150 to automatically verify the registration status of the program. The registration certificate can be constructed as follows.

The privacy control 150 can compute a message authentication code (MAC) and its own digital signature and append it as a certificate to an acceptable application program A, B, X, or Y. The privacy control 150 can include the terms of registration in the digital certificate. Then when the program requests access to the user's private data, the privacy control 150 can automatically check the MAC and its own digital signature to verify that the program has not been changed and the privacy control 150 can also automatically verify the registration status of the program. This is achieved by the privacy control 150 computing a hash value for the entire application program A, B, X, or Y (or some portion of it) and the terms of registration, and then forming a message authentication code (MAC) from the hash value. The privacy control 150 then uses its PKI private key to digitally sign the message authentication code (MAC). The terms of the registration, the MAC and the privacy control's digital signature are appended to the application program A, B, X, or Y as a registration certificate.

Then, whenever the application program A, B, X, or Y requests access to the user's context data or private data, the privacy control 150 will require the application program to present the registration certificate so that the privacy control 150 can check that the presented MAC compares with a computed MAC and that the presented digital signature is genuine. The privacy control 150 can then automatically grant access permission to the application program, in accordance with the terms of the registration.

Methods to generate and evaluate message authentication codes to insure the integrity of data are described in the book by Stephen Thomas entitled "SSL and TLS", published by John Wiley and Sons, 2000. Two example algorithms for message authentication are RSA's Message Digest (MD5) and the Secure Hash Algorithm (SHA),

both of which are described in the book by Stephen Thomas. Another reference that goes into greater detail in its discussion of data integrity methods is the book by Bruce Schneier entitled "Applied Cryptography - 2nd Edition" published by John Wiley and Sons, 1996. Methods to generate and evaluate digital signatures to insure the source of the digital program are described in the book by Richard E. Smith entitled "Internet Cryptography", published by Addison Wesley, 1997.

What has been described here for the privacy control 150 in the wireless device 100, is equally applicable to the privacy control 164 in the network server 140 of Figure 2A. The privacy control 164 in the network server 140 can compute the message authentication code (MAC) and its own digital signature and append it, with the terms of the registration, as a registration certificate to an acceptable application program in the web server 160. Privacy control 164 has a cached copy 144 of the Privacy Profile 152 of the wireless device 100. This enables automatically processing the privacy check in the network Server 140 for access requests from web server 160. When the application program in the web server 160 requests access to the user's private data in the network server 140 or in the wireless device 100, the privacy control 164 in the network server 140 will require the application program in the web server 160 to present the registration certificate so that it can check the MAC and its own digital signature to verify that the application program has not been changed. The privacy control 164 can then automatically grant access permission to the application program in the web server 160, in accordance with the terms of the registration.

If the [B] RUN AN APPLICATION session type is selected by the user, the Context Sensitive Services menu of Figure 1C then presents to the user the RUN AN APPLICATION sub-menu from which the user can select the following options:

[1] MESSAGING
[a] exchange multimedia messages

[2] MOBILE COMMERCE
[a] personal online calendar
[b] exchange rates
[c] banking services
[d] pay bills online using virtual wallet
[e] useful and informative advertising

[f] online merchant transaction services

The Context Sensitive Services menu of Figure 1D presents to the user the RUN AN APPLICATION sub-menu from which the user can select the following options:

[3] ENTERTAINMENT
[a] headline news
[b] sports results
[c] stock quotes
[d] weather forecasts
[e] multilingual phrase dictionaries
[f] online travel
[g] download distinctive ringing tones
[h] interactive games

The RUN AN APPLICATION option calls one of the application programs A, B, X, or Y of the wireless device 100 in Figure 2.

Figure 2 is a functional block diagram of the wireless device 100, showing its various components and programs. The wireless device 100 has context sensitive applications A, B, X, and Y, either downloaded, or in firmware. The wireless device 100 does not need to utilize external functionality in the network for the initial sampling and digitization of the sensor inputs. The sampled and digitized values of the sensor inputs are POSITIONING METADATA 122', TOUCH METADATA 124', AUDIO METADATA 125', COMPASS METADATA 126', AMBIENT LIGHT METADATA 128', AMBIENT TEMPERATURE METADATA 132', and THREE-AXIS ACCELERATION METADATA 134'. The sampled and digitized values of the sensor inputs are loaded into a metadata vector 138.

Figure 2 shows the memory 202 of the wireless device 100, connected by the bus 204 to the keypad 104, the radio 206, the sensor interface 208, the central processor 210, and the display 212. The memory 202 stores programs which are sequences of executable instructions which, when executed by the processor 210, carry out the methods of the invention. The memory 202 stores the WAP client program 108, the context inference engine 136, the privacy control 150, the privacy profile 152, the context aware API 154, the motion/gesture API 156, the location API 158, and other APIs 162. The context inference engine 136 processes the metadata vector 138 to produce the current context.

Application programs 106 stored in the memory 202 include the application programs A and B which are part of the software system SS1, and the application programs X and Y which are contained in the execution environment "Exec. Env."

If sufficient computational power and storage capacity are available in the wireless device 100, further processing of the metadata vector 138 can take place in the context inference engine 136, toward the objective of producing the result of an inferred current context. However, if at some point in the computation, the context inference engine 136 needs the processing power or storage capacity available at the network server 140, the metadata vector 138 is sent from the wireless device 100 to the context inference engine 142 in the network server 140 of Figure 2A. The context inference engine 142 in the network server 140 can perform the required processing on the metadata vector 138 and then return it to the context inference engine 136 in the wireless device 100 for completion of the an inferred current context result. Alternately, the context inference engine 142 in the network server 140 can complete the required processing and then return the resultant inferred current context to the wireless device 100.

Figure 2 shows the architecture of a wireless device with support for context awareness. The context awareness is built on top of sensory information received from various types of sensors physically located in the handset shown in Figure 1. The sensors shown include POSITIONING SENSOR 122, TOUCH SENSOR 124, AUDIO SENSOR 125, COMPASS SENSOR 126, AMBIENT LIGHT SENSOR 128, AMBIENT TEMPERATURE SENSOR 132, and THREE-AXIS ACCELERATION SENSOR 134. The sensors can also be located in accessory-like phone covers or in a wireless accessory such as a Bluetooth enabled device. The sensors may also be located in the environment such as in the user's rooms or vehicles. Also the time duration of use of a phone and other available information can be used along with sensor data in context awareness services.

Figure 2 shows sensor data received from the sensors 122, 124, 125, 126, 128, 132, and 134 is processed by Context Inference Engine 136. The application programs A, B, X, or Y running in the wireless device 100, may optionally provide application data to the context inference engine 136, along with their request for current context. The context inference engine 136 can optionally process the sensor signals and the application data to

produce the current context. The context inference engine 136 then feeds the current context through various APIs 154, 156, 158, and 162 to application programs A, B, X, and Y. The application programs may register themselves at the Application Programming Interface 154 to receive current context or changes in the context. This enables context sensitivity in the application programs.

Figure 2 shows "native" application programs A and B which are executed in a first software system SS1 of the wireless device 100. The term "Software System" is used here for any environment with execution capability. This first software system may be proprietary or based on a commercially available real-time operating system, such as NOS, ISA, EPOC, JAVA, or WAP. Third party application programs X and are executed within an execution environment. This execution environment may limit the system capabilities available for the application programs, such as access to APIs (fixed, not dynamic behavior).

Figure 2 shows the mobile user's privacy control feature. The privacy control feature enables the user to designate which application programs are granted access to the context awareness APIs 154 to utilize the current context information produced by the context inference engine 136. All requests or registrations by application programs A, B, X, and Y to have access to the Context Inference Engine 136, must first go through the Privacy Control block 150. Privacy Control block 150 uses the user's security data check stored in the Privacy Profile 152 to grant access rights to the requesting application programs. The user controls the granting of access rights by means of the user's security data input by the user through the user interface. The user's security data includes permissions list 155, Public Key Infrastructure (PKI) certificates 157, PKI trusted authority trust list 159, and flags set by the user for those application programs that have been authenticated by the PKI procedures, data set 161. The user can update the user's security data with the UPDATE PRIVACY FEATURES menu displayed by the wireless device 100 shown in Figures 1A and 1B. Access might be granted to an application program based on its digital signature, which is a part of the system applications, or other means known in the art. It is also possible to provide a separate system-wide Privacy User Interface to the privacy control 150, which can be employed by the mobile user to set the privacy policies and to alert the mobile user that an application program is attempting to

register to receive the user's private context awareness information. The privacy control 150 and Privacy Profile 152 enable the mobile user to grant, deny, or revoke access, to grant access for a limited time, or to require an application program to always request registration before the user grants access.

In Figure 2, the Context Inference Engine 136 in the wireless device 100 makes inferences from all the sensor inputs based on where the wireless device is located by the mobile user. For instance the inferred current context of the device 100 may be "IN THE USER'S POCKET", when a certain set of sensors input a specific combination of signals having a specific value range. As an example, the resulting inference of the current context by the Context Interference Engine 136 could be expressed in XML language format as follows:

<Context Inference Engine in Device>

<device placement> pocket </ device placement>

<User Interface state> sleep mode </User Interface state>

< device location> in elevator 5 building 1 floor 2</ device location>

<API active actions> meeting starting on floor 3 room 322 </API active actions>

</Context Inference Engine in Device >

The Context Inference Engine 136 in the wireless device 100 can perform the context inference process with any of several methods. Different input information from the sensors can be weighted according to their relative value of importance appropriate for each environment condition or situation to be analyzed. Each sensor has it's own weight value. Alternatively, the weight values for each sensor for each environment condition can be learned from training sessions using, for example artificial neural networks (ANNs), self-organizing maps (SOMs), decision trees, fuzzy rule-based systems, or model-based systems such as Hidden Markov Modeling (HMM). Combinations of two or more of the alternate methods can be used, depending on the application.

The Context Inference Engine 136 can continuously adapt its weights through adaptive and continuous learning methods, where the user teaches the wireless device 100 new environment conditions and names them. Hidden Markov Modeling (HMM) can be

used, for example, to implement an adaptive and continuous learning method for the Context Inference Engine 136. Alternately, the wireless device 100 can be programmed to spontaneously recognize a changed scene by comparing it with known scenes. The user can teach the wireless device new environmental conditions and name them, using the adaptive and automatic learning capability of neural networks. Adaptive and continuous learning methods are computationally intensive and are appropriate candidates to place on the network server 140, which assists the wireless device 100, as discussed below.

The field of context inference has applied the principles of automated pattern recognition to processing diverse types sensor inputs. Speech recognition has been applied to processing speech signals and handwriting recognition has been applied to processing hand force and accelerometer signals. In the field of robotics, image recognition has been applied to processing digitized still and motion images, mechanical location recognition has been applied to processing laser and sonar range finder signals, and mechanical motion recognition to has been applied to processing inertial, acceleration, and heading signals. In the field of prosthetic devices, touch recognition has been applied to processing tactile sensor signals. In the field of medicine, automated diagnostic programs recognize various pathologies by processing bioelectric field signals, as well as the more traditional pulse, respiration rate, and body temperature signals. These diverse sensor signal recognition processes have the common feature that an initial training stage is conducted where sampled signals are equated with a statistical model for those signals.

The principles of automated pattern recognition for these diverse sensor inputs are exemplified by the techniques for recognizing speech patterns. A common technique used in speech recognition is Hidden Markov Modeling (HMM). The term "Hidden" refers to the probabilistic and not directly observable events which underlie a speech signal. HMM speech recognition systems typically use realizations of phonemes which are statistical models of phonetic segments having parameters that are estimated from a set of training examples. Models of words are made by chaining or linking appropriate statistical models of phonetic segments. The statistical models serve as standards which are to be matched with the unknown voice signals to be recognized.

Recognition of unknown voice signals requires sampling and digitizing the speaker's spoken phonemes. These digitized phonemes are then processed into metadata. The metadata is then compared with the standard statistical models of phonemes. The most likely matches are then the inferred speech recognition result.

Recognition consists of finding the most likely path through the set of word models for the input speech signal. HMM speech recognition decoding systems first need to be trained through an iterative process. The system must be exposed to training examples or words of a particular speaker's voice. A training word is analyzed to generate a framed sequence of acoustic parameters or statistical models. A valid or "good" recognition occurs when the most likely path through the set of word models for the training word results in recognizing the correct training word.

Some useful references discussing the principles of Hidden Markov Models are:

Rabiner, L. R., "A tutorial on hidden Markov models and selected applications in speech recognition", Proceedings of the IEEE, volume 77, number 2, 1989, pages 257-286.

Rabiner, L. R. and Juang, B. H., "An introduction to hidden Markov models", IEEE ASSP Magazine, January 1986, pages 4-15.

Fraser, Andrew M. and Dimitriadis, Alexis, "Forecasting Probability Densities by Using Hidden Markov Models with Mixed States", Time Series Prediction: Forecasting the Future and Understanding the Past, Addison-Wesley, editor Weigend, Andreas S. and Gershenfeld, Neil A., 1994.

Charniak, Eugene, Statistical Language Learning, MIT Press, Cambridge, Massachusetts, 1993.

To illustrate how Hidden Markov Modeling (HMM) can be extended beyond speech recognition, an example is given here for touch recognition. In the training stage for touch recognition, tactile sensor signals are input from touching a tactile transducer to a rough texture, such as for example sandpaper. The tactile sensor signals are transformed into a statistical model of the input signal. The statistical model is stored as a standard in a computer memory under the handle "rough_texture". To expand the range of sensor signals that are included in the model for "rough_texture", several training

sessions can be conducted, each with a different direction or pressure for touching the sandpaper, resulting in several different samples of the statistical model. The set of samples of the statistical model are stored as a standard under the handle "rough_texture". Other training sessions are conducted with a smooth texture, such as glass. The tactile sensor signals input from touching the tactile transducer to the smooth texture are transformed into a statistical model of the input signal and stored as a standard under the handle "smooth_texture". Later, in the recognition mode, an unknown object is touched by the tactile transducer resulting in a sample tactile sensor signal. Recognition of unknown touch signals requires sampling and digitizing the touch transducer's signals. These digitized sensor signals are then processed into metadata. The metadata is then compared with the standard statistical models of "rough_texture" and "smooth_texture". The most likely match is then the inferred touch recognition result.

Combinations of two or more types of sensors can have their signals combined into an input metadata vector that characterizes a composite sampling event. The composite sampling event can be recognized using the principles of Hidden Markov Modeling (HMM). An example composite sampling event can be the state of the health and fatigue of the user of a wireless device 100. For example, a wireless device 100 can be equipped with a tactile transducer which outputs tactile sensor signals in response to the hand force and pulse rate of the user who is gripping the wireless device 100. The wireless device 100 can be equipped with a temperature sensor which outputs body temperature signals in response to the user gripping the wireless device 100. Hidden Markov Modeling (HMM) can be used to recognize a force/temperature input metadata vector that characterizes the combination of the hand force and the temperature sensor signals resulting from a sampling event. A composite sampling event in this example can have an extended duration so that the force sensor can transduce the pulse rate of the user over a period of time.

In the training stage, the tactile sensor signals and the force sensor signals are output while the user is in a condition of good health and resting normally. The tactile sensor signals and the force sensor signals are combined into a force/temperature input metadata vector which is transformed into a statistical model of the input signals. The statistical model is stored as a standard in the computer memory of the wireless device

100 under the handle "good_health_ resting_normally". Other training sessions are conducted with the user in different states of health and fatigue. For example, the user may be training the wireless device 100 while working late at night at the office. The tactile sensor signals and the force sensor signals resulting from holding the wireless device 100, are combined into a force/temperature input metadata vector for the user in the condition of being in good health but fatigued. The force/temperature input metadata vector is transformed into a statistical model of the input signals and stored as a standard under the handle "good_health_ fatigued".

Later, in the recognition mode, as the user holds the wireless device 100, the tactile sensor signals and the force sensor signals are sampled. The Health/Fatigue_State recognition consists of sampling and digitizing the touch transducer's signals. These digitized sensor signals are then processed into a metadata vector. The metadata vector is then compared with the standard statistical models of handle "good_health_ resting_normally" and "good_health_ fatigued". The most likely match is then the inferred touch recognition result.

In accordance with the invention, this recognition result can be used by a health maintenance application program in the wireless device 100, to provide useful and appropriate information to the user. For example, a health maintenance program can process the recognition result, and in response, signal an alarm to the user and provide suggestions for medications to palliate the sensed fatigue. One problem with automatic recognition programs is that they are either relatively large or they call databases that are relatively large in comparison to the memory capacity of the wireless device 100.

Another aspect of the invention is the recognition result can be used by a supplementary application program in a remote server, to provide additional and more detailed useful and appropriate information to the user. For example, the server can access a large database of suggestions for medications to palliate the sensed fatigue of the user. The results of the search of the database can be returned to the wireless device 100. The server can also maintain a personal profile of the user's characteristics and preferences and it can use that profile in automatically formulate its query to the database. For example, the user's drug allergies can be stored in the server's database, to insure that

recommendations are not made that will result in an allergic reaction by the user to the suggested medication.

Figure 2A is a functional block diagram of the wireless device 100, the server 140, and the web server 160, and their interaction when exchanging the metadata vector 138 and the privacy control data 150'. These exchanges are bulk encrypted with a symmetric session key, such as a Data Encryption Standard (DES) key, to protect the privacy of the data. To insure the integrity of the metadata vector 138 and the privacy control data 150', a message authentication code (MAC) can be computed and appended to the data, as described in the above referenced book by Stephen Thomas entitled "SSL and TLS", published by John Wiley and Sons, 2000. To insure that the source of the metadata vector 138 and the privacy control data 150' cannot be repudiated, a digital signature can be appended to the data, as described in the above referenced book by Richard E. Smith entitled "Internet Cryptography", published by Addison Wesley, 1997.

Figure 2A shows the scope of the distributed context awareness implementation. The wireless device 100 has context sensitive applications A, B, X, and Y either downloaded or in firmware. The wireless device 100 may locally preprocess part of the context information in the metadata vector 138 before sending it to the context inference engine 142 in the network server 140 which is capable of processing the data and responding back with the resulting current context. The wireless device 100 may run application programs that require accessing the web service server 160 to provide context sensitive services to the mobile user.

Figure 2A shows how processing of sensor data from the sensors in the wireless device 100, can be distributed between the wireless device and the network server 140. The operation in Figure 2A is as follows:

1. The sensors continuously provide the sensor data to the Context Inference Engine 136 in the wireless device 100.

2. An application program that utilizes the context awareness APIs 154 may request the latest context information, or the application program may be registered to receive any changes to specific context information.

3. The Context Inference Engine 136 securely contacts the Context Inference Engine 142 of the network server 140 and sends the metadata vector 138 to the server 140. Depending on the sensors and the implementation details, Context Inference Engine 136 may preprocess part of the sensor data in the metadata vector 138 prior to sending it. Depending on the sensors and the interval for processing, there may be virtual connection open between Context Inference Engine 136 and Context Inference Engine 142 for frequent data exchanges. Context Inference Engine 142 at the network server 140, has the processing power and memory capacity to handle computationally intensive and/or memory intensive processing of the preprocessed sensor data in the metadata vector 138 to produce the current context result information.

4. Context Inference Engine 142 at the network server 140 may utilize local user information (history information, customer details) stored in the user database 146 for making a more accurate determination of the mobile user's current context.

5. Context Inference Engine 142 at the network server 140 then securely returns the current context awareness information to Context Inference Engine 136 in the wireless device 100.

6. Context Inference Engine 136 in the wireless device 100 then provides the current context awareness information through Context Awareness APIs 154 to the application programs registered for to receive that information.

Figure 2A shows how Web Services in Web Service Server 160 are enabled to receive current context results of the wireless device 100. Web Services Server 160 has a software system for server application program A and an execution environment for server application programs X and Y that are similar to the software system SS1 and execution environment (Exec. Env.) in the wireless device 100 shown in Figure 2. Server Application programs A, X, and Y in Web Service Server 160 may require access through the Context Awareness APIs to provide Web Services with the current context of the wireless device 100.

In Figure 2A, Web Service Server 160 uses the Context Inference Client 176 to contact the Context Inference Server 174 in the network server 140. Context Inference Client 176 may utilize customer database information in database 184 to enhance the context sensitivity capabilities of the web server 160. The contact to the network server

140 is done through a context awareness interface 186 to the Context Inference Server 174 in the network server 140.

Context Inference Server 174 registers the Web Services of the web server 160 through the privacy control 164 of the network server 140 to the Context Inference Engine 142. Privacy control 164 has a cached copy 144 of the Privacy Profile 152 of the wireless device 100. This enables processing of the privacy check in the network Server 140 for access requests from web server 160. The communication between web server 160 and network server 140 is secured using the Internet secure protocols such as HTTPS or SSL. The Context Inference Server 174 can publish its own service as a Web Service to other Web Services on the Internet, in which case the implementation of the interface 186 between web server 160 and network server 140 can be Extensible Markup Language (XML) messages carried in the Simple Object Access Protocol (SOAP) messaging protocol.

The Context inference Engine 142 in the network server 140 will receive processed sensor metadata vector 138 information and possibly some application API information originated from the Context Inference Engine 136 of the wireless device 100. The Context inference Engine 142 of the network server has user database 146 information of the behavior of the user and of the past usage of the wireless device. The Context inference Engine 142 of the network server may also have third party services available (such as instances offering content and/or services) to be offered to potential users. What is offered to the user can also depend on the user profile 144. The nature of the Context inference Engine 136 information of the wireless device 100 that is conveyed to the Context inference Engine 142 of the network can be controlled with the privacy control 150 that is managed by the user of the wireless device 100. The user may thus fully or partly disable the Context inference Engine 142 of the network to control the amount of his/her information that can be used by third party services. The privacy control 150 enables the user to control access by anyone to his/her private information.

The Context inference Engine 136 of the wireless device receives an input from the API interface 154 from the applications A, B, X, or Y located in the wireless device 100. An example would be from a calendar application program indicating that a meeting is starting in 25 minutes time. As another example the calendar application program

indicates that Lisa is having a birthday tomorrow into which you are participating. The Context inference Engine 136 of the wireless device can convey processed result information to the Context inference Engine 142 of the network server. Now in addition to the sensor information, information from the application programs A, B, X, or Y can also be used in the decision making of the Context inference Engine 136 of the wireless device. A combination of the sensor information and information coming from the application programs A, B, X, or Y can be processed by the Context inference Engine 136. The user's behavior or usage patterns can be detected from the sensor and recorded in a the user database, concerning the usage of the application programs. As previously discussed, the processing of this combined information from the sensors and from the application programs can be shared between the Context inference Engine 136 and the Context inference Engine 142. Either the application programs A, B, X, or Y running in the wireless device 100 or the server application programs A, X and Y running in the web server 160, may optionally provide application data to the context inference engine 142 in the network server 140. The context inference engine 142 can optionally process the metadata vector 138 and the application data to produce the current context.

The information transfer from the Context inference Engine 136 of the wireless device to the Context inference Engine 142 of the network server can be done in alternative ways. The system can be managed so that the current consumption and transfer capacity between the wireless device 100 and the network server 140 is taken into account. The context information does not always have to be collected so frequently that it would have to be periodically transferred to the network side 140 every few seconds. Depending on the application, the timing window applied to information transfer from the Context inference Engine 136 of the wireless device 100 to the Context inference Engine 142 of the server 140 can vary from seconds to minutes. If there were no event change or condition change in the environment of the wireless device 100, there would be no need to transfer information to the Context inference Engine 142 of the server 140. Additionally information can be temporarily stored in a buffer in the wireless device 100, which can then transferred less frequently to the network Context inference Engine 142. Packet based GPRS and UMTS can support the less frequent information transfer rates. Also, it is advantageous to send the network Context inference Engine 142 information

from the wireless device 100 as an attachment, immediately subsequent to other signaling made to in the network direction from the wireless device 100, thus saving the radio transmitter of the wireless device 100 from having to be switched on again for transferring the Context inference Engine 136 information separately to the network server 140.

Returning to Figure 1, the relationship is shown between the network server 140, the Universal Description, Discovery and Integration (UDDI) registry 170, and a plurality of web site servers 160. UDDI is a defacto standard for an Internet-based registry. The UDDI registry 170 enables the network server 140 to discover new web sites for services and businesses on the Internet. Once such services and businesses are identified by the UDDI registry 170 to the network server 140, then the server 140 must apply the mobile user's cached privacy profile 144 in Figure 2A, in order to prevent unauthorized access of the user's private data by application programs on the newly discovered web sites.

Figure 3 is a network process flow diagram of the interaction of the wireless device 100 I the first column, network server 140 in the middle column, and web server 160 in the right column, when they carry out the determination of the current context of the wireless device 100. The process begins with the wireless device 100 in step 302:

Step 302: PRIVACY CONTROL 150 IN WIRELESS DEVICE 100 SENDS UPDATED PRIVACY PROFILE TO NETWORK SERVER 140.

Then the network server 140 continues with step 304:

Step 304: NETWORK SERVER 140 UPDATES CACHED PRIVACY PROFILE 144.

The wireless device 100 continues with the following steps 306, 308, and 310:

Step 306: SENSORS CONTINUOUSLY PROVIDE SENSOR DATA TO CONTEXT INFERENCE ENGINE 136 IN WIRELESS DEVICE 100.

Step 308: APPLICATION PROGRAM THAT USES CONTEXT AWARENESS API 154 REQUESTS LATEST CONTEXT INFORMATION.

Step 310: CONTEXT INFERENCE ENGINE 136 CONTACTS CONTEXT INFERENCE ENGINE 142 OF THE NETWORK SERVER 140 AND SENDS THE METADATA VECTOR 138 TO SERVER 140.

Then the network server 140 continues with steps 312 and 314:

Step 312: CONTEXT INFERENCE ENGINE 142 AT NETWORK SERVER 140 USES LOCAL USER INFORMATION STORED IN USER DATABASE 146 TO MAKE A MORE ACCURATE DETERMINATION OF THE MOBILE USER'S CURRENT CONTEXT.

Step 314: NETWORK SERVER 140 REQUESTS DATA FROM WEB SERVER 160.
THE NETWORK SERVER'S ACCESS IS AUTHORIZED BY CACHED PRIVACY PROFILE 144 IN NETWORK SERVER.

Then the web server 160 continues with step 316:

Step 316: WEB SERVER PROVIDES USER INFORMATION STORED IN DATABASE 184 TO NETWORK SERVER 140.

Then the network server 140 continues with step 318:

Step 318: CONTEXT INFERENCE ENGINE 142 AT THE NETWORK SERVER 140 THEN SECURELY RETURNS THE CURRENT CONTEXT AWARENESS INFORMATION TO CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100.

Then the wireless device 100 finishes with step 320:

Step 318: CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100 THEN PROVIDES THE CURRENT CONTEXT AWARENESS INFORMATION THROUGH CONTEXT AWARENESS APIs 154 TO THE APPLICATION PROGRAMS REGISTERED TO RECEIVE THAT INFORMATION.

Figure 4 is a functional block diagram of the network server 140, showing the memory 402 storing the application services software programs needed to perform the operations of the invention. The memory is connected by the bus 404 to the cache 144, user database 146, TCP/IP network adapter 406, and central processor 410. The memory 402 stores programs which are sequences of executable instructions which, when executed by the processor 410, carry out the methods of the invention.

Figure 4 is a functional block diagram of the network server, showing the memory storing the application services software programs needed to perform the operations of an embodiment of the invention. Figure 4 discloses the functional components of an exemplary network server 140 arranged as an object model. The object model groups the

object oriented software programs into components that perform the major functions and applications in network server 140. The object model for memory 402 of network server 140 employs a three-tier architecture that includes presentation tier 415, infrastructure objects partition 422, and business logic tier 414. The object model further divides business logic tier 414 into two partitions, application objects partition 422 and data objects partition 426.

Presentation tier 415 retains the programs that manage the device interfaces to network server 140. In Figure 4, presentation tier 415 includes network interface 420. A suitable implementation of presentation tier 415 may use Java servlets to interact with WAP protocol gateway 120 via the hypertext transfer protocol ("HTTP"). The Java servlets ran within a request/response server that manages the exchange of messages between WAP protocol gateway 120 and network server 140. A Java servlet is a Java program that runs within a Web server environment. A Java servlet takes a request as input, parses the data, performs logic operations, and issues a response back to WAP protocol gateway 120. The Java runtime platform pools the Java servlets to simultaneously service many requests. Network interface 420 accepts request messages from WAP protocol gateway 120 and passes the information in the request to visit object 428 for further processing. Visit object 428 passes the result of that processing to network interface 420 for transmission back to the WAP protocol gateway 120. Network interface 420 may also use network adapter 406 to exchange data with another user device.

Infrastructure objects partition 422 retains the programs that perform administrative and system functions on behalf of business logic tier 414. Infrastructure objects partition 422 includes operating system 425, and an object oriented software program component for database server interface 430, and system administrator interface 432.

Business logic tier 414 in Figure 4 includes multiple instances of visit object 428, 428', 428". A separate instance of visit object 428 exists for each network interface 420 session. Each visit object 428 is a stateful session object that includes a persistent storage area from initiation through termination of the session, not just during a single interaction or method call. The persistent storage area retains information associated with the session.

When WAP protocol gateway 120 sends a metadata vector 138 message to network server 140, the message is sent to network interface 420 to invoke a method that creates visit object 428 and stores connection information as a state in visit object 428. Visit object 428 may, in turn, invoke a method in context inference engine 142 application 440 to perform a context inference on the metadata vector and return a current context result.

When WAP protocol gateway 120 sends a privacy control data 150' message to network server 140, the message is sent to network interface 420 to invoke a method that creates visit object 428 and stores connection information as a state in visit object 428. Visit object 428 may, in turn, invoke a method in privacy control 164 application 442 to update the cached privacy profile 144. The application 442, in turn make a method call to privacy profile update application 448 to store the updated data 150' in the cache 144.

When WAP protocol gateway 120 sends a user data update message to network server 140, the message is sent to network interface 420 to invoke a method that creates visit object 428 and stores connection information as a state in visit object 428. Visit object 428 may, in turn, invoke a method in user database application 446 to store the user data in the database 146.

A description of server programming applications developed with Enterprise Java Beans is provided in the book by Ed Roman entitled "Mastering Enterprise Java Beans", published by John Wiley and Sons, 1999. A description of the use of an object model in the design of server applications is provided in the book by Matthew Reynolds entitled "Beginning E-Commerce", Wrox Press Inc, 2000, (ISBN: 1861003986). Java servlets and the development of web site servers is described in the book by Duane K. Fields, et al. entitled "Web Development with Java Server Pages", published by Manning Publications Co., 2000.

The resulting context sensitive web services invention enables a mobile phone or wireless device 100 to use context inference techniques to sense the user's environment and in response, to provide useful information to the user that is appropriate to the user's

perceived environment. The mobile user is provided with the ability to control access by application programs anywhere in the network, to the user's private data.

Although a specific embodiment of the invention has been disclosed, it will be understood by those having skill in the art that changes can be made to the specific embodiment without departing from the spirit and the scope of the invention.

CLAIMS

What is claimed is:

1. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

2. The method of claim 1, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

3. The method of claim 1, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

4. The method of claim 3, wherein the server accesses files from a web server, for selective forwarding to the user's wireless device.

5. The method of claim 3, wherein the wireless device offloads a portion of the processing of the sensor signals with a context inference engine to the server.

6. The method of claim 3, wherein a personal profile of the user is maintained by the server.

7. The method of claim 1, which further comprises:

providing user control of access by application programs to the user's private data.

8. The method of claim 3, which further comprises:

providing user control of access by application programs to the user's private data in the server.

9. The method of claim 1, which further comprises:

providing user control of access by application programs in a web server, to the user's private data.

10. The method of claim 1, which further comprises:

providing the current context result to an application program; and

receiving the useful information for the user from the application program.

11. The method of claim 1, which further comprises:

providing user control of access by an application program to the current context result;

providing the current context result to the application program in response to the user control; and

receiving the useful information from the application program.

12. The method of claim 11, which further comprises:

granting access permission to the application program to access the current context result, based on the user's data stored in a privacy profile.

13. The method of claim 11, wherein providing user control of access is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

14. The method of claim 13, wherein the server accesses files from a web server, for selective forwarding to the user's wireless device.

15. The method of claim 13, wherein the wireless device offloads a portion of the processing of providing user control of access, to the server.

16. The method of claim 13, wherein a personal profile of the user is maintained by the server.

17. The method of claim 16, which further comprises:

providing user control of access by application programs to the user's personal profile.

18. The method of claim 13, which further comprises:

providing user control of access by application programs to the user's personal profile in the server.

19. The method of claim 11, which further comprises:

providing user control of access by application programs in a web server, to the user's private data.

20. The method of claim 19, which further comprises:

enabling context sensitive applications and services within the wireless device while providing to the user control over the privacy user's current context result.

21. The method of claim 19, which further comprises:

enabling context sensitive applications and services within the network server while providing to the user control over the privacy user's current context result.

22. An apparatus to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a processor;

a memory coupled to the processor, programmed to perform the steps of:

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

23. The apparatus of claim 22, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

24. The apparatus of claim 22, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

25. The apparatus of claim 24, wherein the server accesses files from a web server, for selective forwarding to the user's wireless device.

26. A wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a sensor for providing sensor signals characterizing a current environment of the wireless device;

a context inference engine coupled to the sensor, for processing the sensor signals;

said context inference engine providing a current context result from the processing; and

an output device coupled to the context inference engine, for providing useful information to the user in response to the current context result.

27. A wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a privacy control for providing the user control of access by an application program to the user's private data;

a sensor for providing sensor signals characterizing a current environment of the wireless device;

a context inference engine coupled to the sensor, for processing the sensor signals;

said context inference engine coupled to the privacy control, for providing a current context result from the processing to the application program; and

an output device coupled to the privacy control, for providing useful information to the user in response to the application program.

28. A system to provide useful information to the user of a wireless device that is appropriate to the device's current environment, comprising:

a privacy control in a server for receiving a user privacy profile from the wireless device and providing the user control of access by an application program to the user's private data;

a sensor in the wireless device for providing sensor signals characterizing a current environment of the wireless device;

a context inference engine in the server coupled to the wireless device, for processing sensor information derived from the sensor signals;

said context inference engine coupled to the privacy control, for providing a current context result from the processing to the application program; and

an output device in the server, coupled to the privacy control, for transmitting useful information to the wireless device in response to the application program.

29. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

running a program that provides application data to the wireless device;

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals and the application data with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

30. The method of claim 29, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

31. The method of claim 30, wherein the step of running a program occurs in the wireless device.

32. The method of claim 29, wherein the processing of the sensor signals with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

33. The method of claim 32, wherein the step of running a program occurs in a web server coupled to the network server.

34. A system to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a processor;

a memory coupled to the processor, programmed to perform the steps of:

running a program that provides application data to the wireless device;

receiving sensor signals characterizing a current environment of the wireless device;

processing the sensor signals and the application data with a context inference engine;

outputting a current context result from the processing by context inference engine; and

providing useful information to the user in response to the current context result.

35. The system of claim 34, wherein the processing of the sensor signals and the application data with a context inference engine is embodied as programmed instructions executed within the user's wireless device.

36. The system of claim 35, wherein the step of running a program occurs in the wireless device.

37. The system of claim 34, wherein the processing of the sensor signals and the application data with a context inference engine is embodied as programmed instructions executed within a separate network server in response to signals from the user's wireless device.

38. The system of claim 37, wherein the step of running a program occurs in a web server coupled to the network server.

39. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

receiving sensor signals characterizing a current environment of the wireless device;

partially processing the sensor signals with a first context inference engine within the user's wireless device;

sending the partially processed sensor signals to a second context inference engine within a separate network server;

completing the processing the sensor signals with the second context inference engine;

sending a current context result from the second context inference engine to the wireless device; and

providing useful information to the user in response to the current context result.

40. A system to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

a wireless device for receiving sensor signals characterizing a current environment of the wireless device;

a first context inference engine within the user's wireless device for partially processing the sensor signals;

a second context inference engine within a separate network server for receiving the partially processed sensor signals sent from the wireless device and completing the processing the sensor signals;

said second context inference engine sending a current context result from the second context inference engine to the wireless device; and

said wireless device providing useful information to the user in response to the current context result.

41. A method to enable a wireless device to provide useful information to its user that is appropriate to the device's current environment, comprising:

receiving sensor signals characterizing a current environment of the wireless device;

partially processing the sensor signals with a first context inference engine within the user's wireless device;

sending the partially processed sensor signals to a second context inference engine within a separate network server;

completing the processing the sensor signals with the second context inference engine;

forwarding a current context result from the network server to a second server; and

sending useful information from the second server to the user's wireless device in response to the current context result.

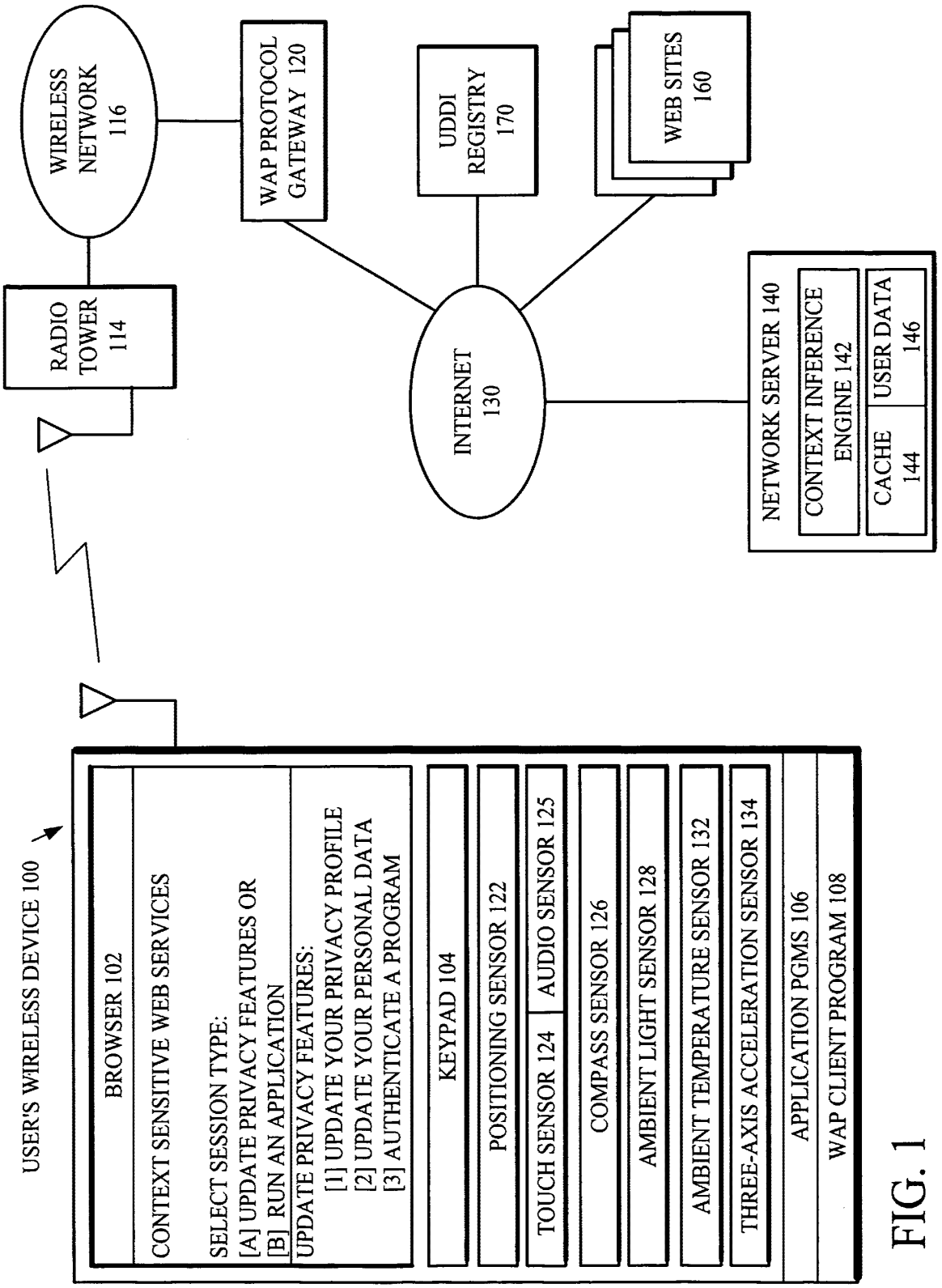

WIRELESS NETWORK 116
WAP PROTOCOL GATEWAY 120
UDDI REGISTRY 170
WEB SITES 160
RADIO TOWER 114
INTERNET 130
NETWORK SERVER 140
CONTEXT INFERENCE ENGINE 142
CACHE 144
USER DATA 146
USER'S WIRELESS DEVICE 100
BROWSER 102
CONTEXT SENSITIVE WEB SERVICES
SELECT SESSION TYPE:
[A] UPDATE PRIVACY FEATURES OR
[B] RUN AN APPLICATION
UPDATE PRIVACY FEATURES:
[1] UPDATE YOUR PRIVACY PROFILE
[2] UPDATE YOUR PERSONAL DATA
[3] AUTHENTICATE A PROGRAM
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
AUDIO SENSOR 125
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134
APPLICATION PGMS 106
WAP CLIENT PROGRAM 108

FIG. 1

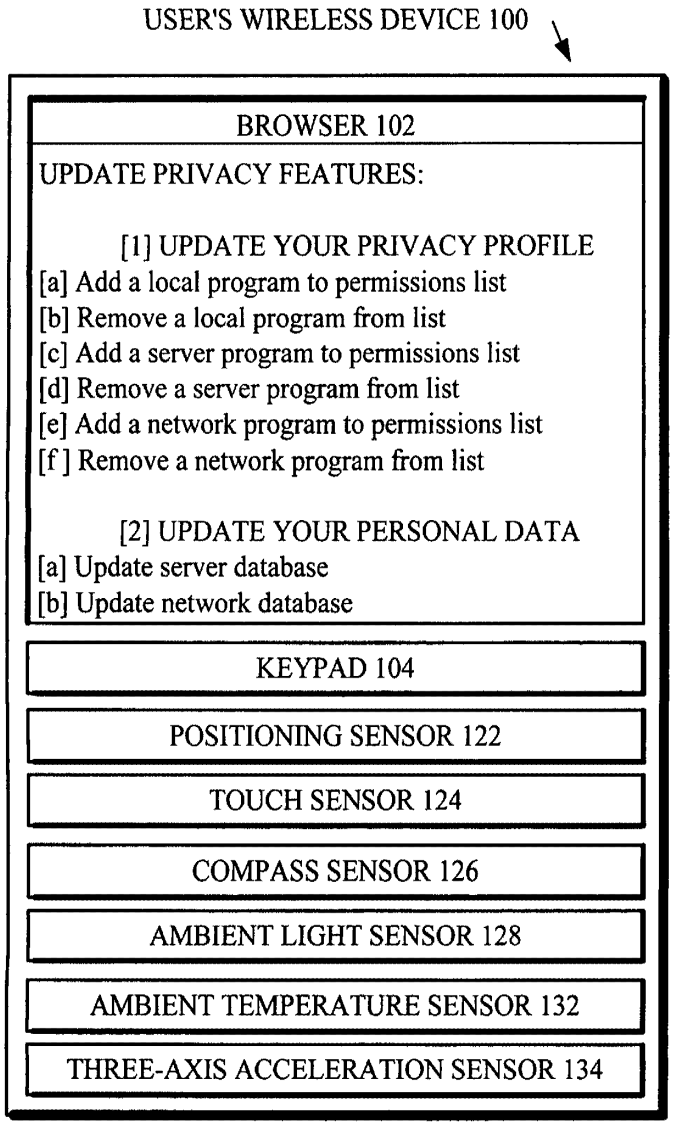

USER'S WIRELESS DEVICE 100
BROWSER 102
UPDATE PRIVACY FEATURES:
[1] UPDATE YOUR PRIVACY PROFILE
[a] Add a local program to permissions list
[b] Remove a local program from list
[c] Add a server program to permissions list
[d] Remove a server program from list
[e] Add a network program to permissions list
[f] Remove a network program from list
[2] UPDATE YOUR PERSONAL DATA
[a] Update server database
[b] Update network database
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1A

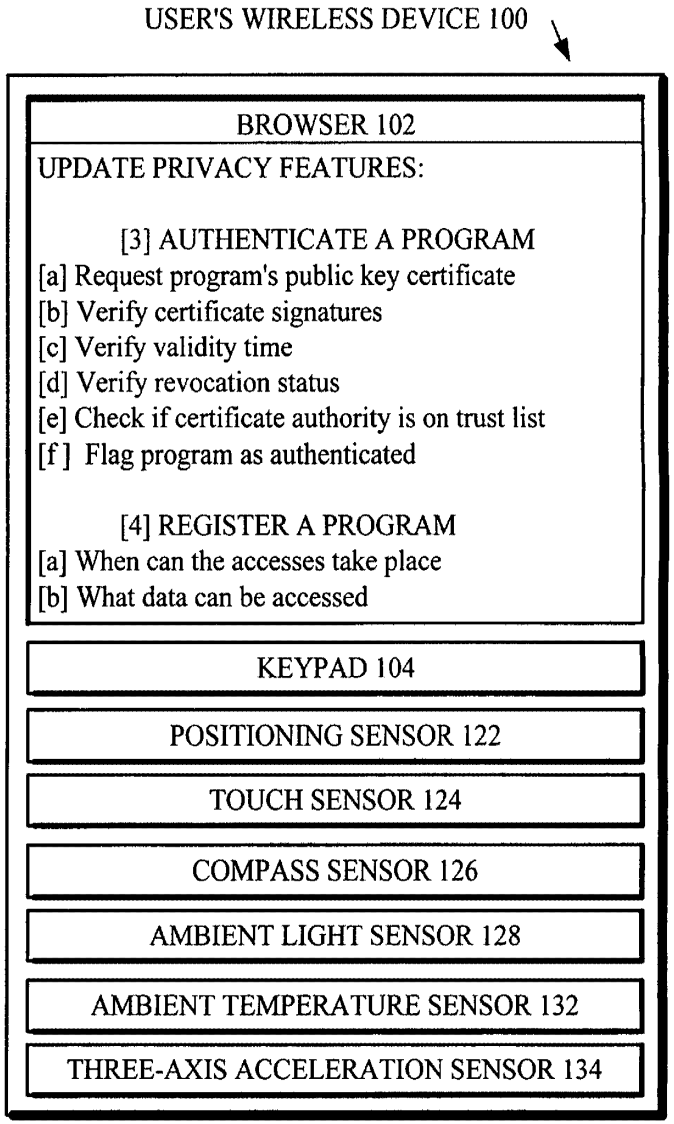

USER'S WIRELESS DEVICE 100
BROWSER 102
UPDATE PRIVACY FEATURES:
[3] AUTHENTICATE A PROGRAM
[a] Request program's public key certificate
[b] Verify certificate signatures
[c] Verify validity time
[d] Verify revocation status
[e] Check if certificate authority is on trust list
[f] Flag program as authenticated
[4] REGISTER A PROGRAM
[a] When can the accesses take place
[b] What data can be accessed
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1B

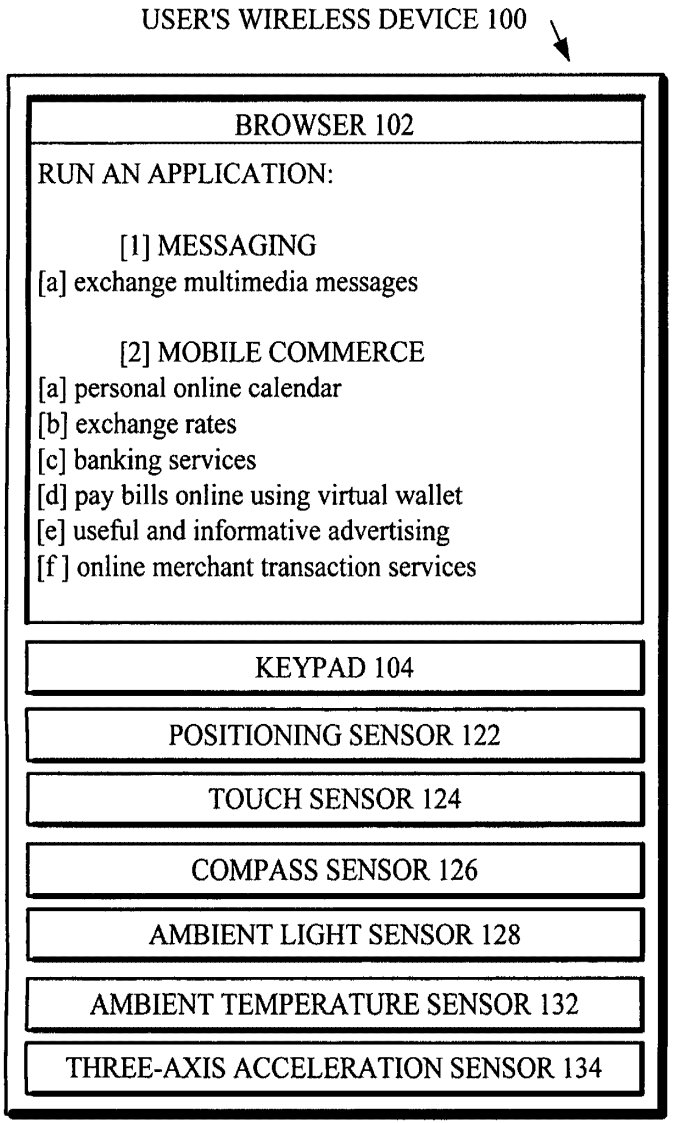

USER'S WIRELESS DEVICE 100
BROWSER 102
RUN AN APPLICATION:
[1] MESSAGING
[a] exchange multimedia messages
[2] MOBILE COMMERCE
[a] personal online calendar
[b] exchange rates
[c] banking services
[d] pay bills online using virtual wallet
[e] useful and informative advertising
[f] online merchant transaction services
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1C

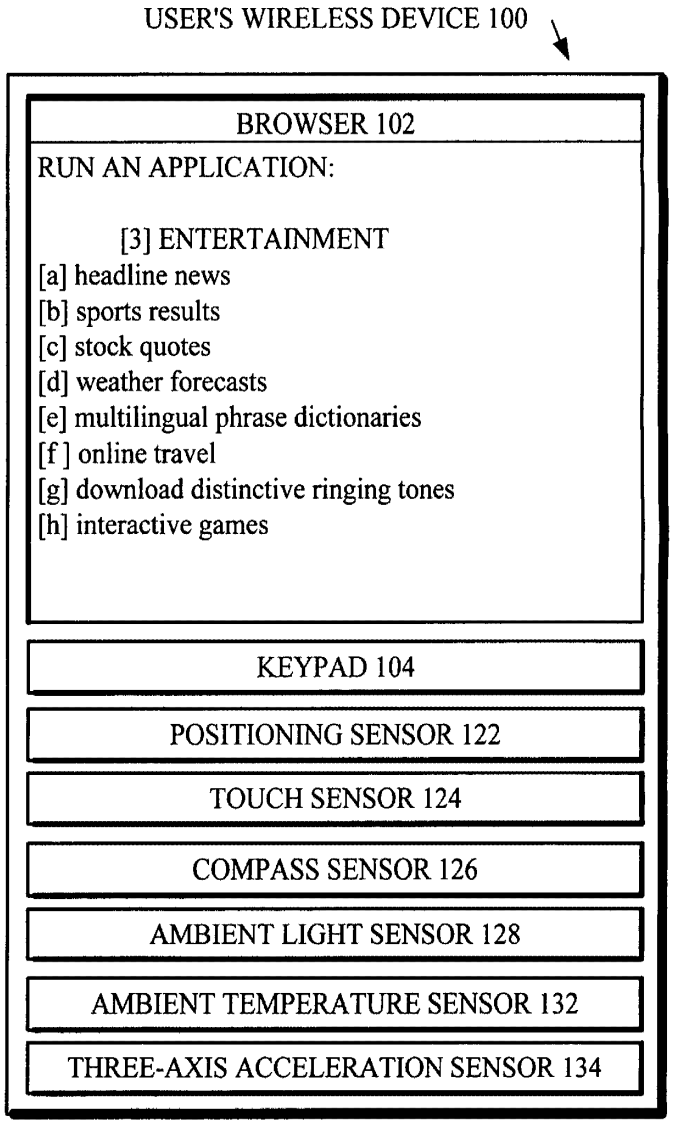

USER'S WIRELESS DEVICE 100
BROWSER 102
RUN AN APPLICATION:
[3] ENTERTAINMENT
[a] headline news
[b] sports results
[c] stock quotes
[d] weather forecasts
[e] multilingual phrase dictionaries
[f] online travel
[g] download distinctive ringing tones
[h] interactive games
KEYPAD 104
POSITIONING SENSOR 122
TOUCH SENSOR 124
COMPASS SENSOR 126
AMBIENT LIGHT SENSOR 128
AMBIENT TEMPERATURE SENSOR 132
THREE-AXIS ACCELERATION SENSOR 134

FIG. 1D

FIG. 2

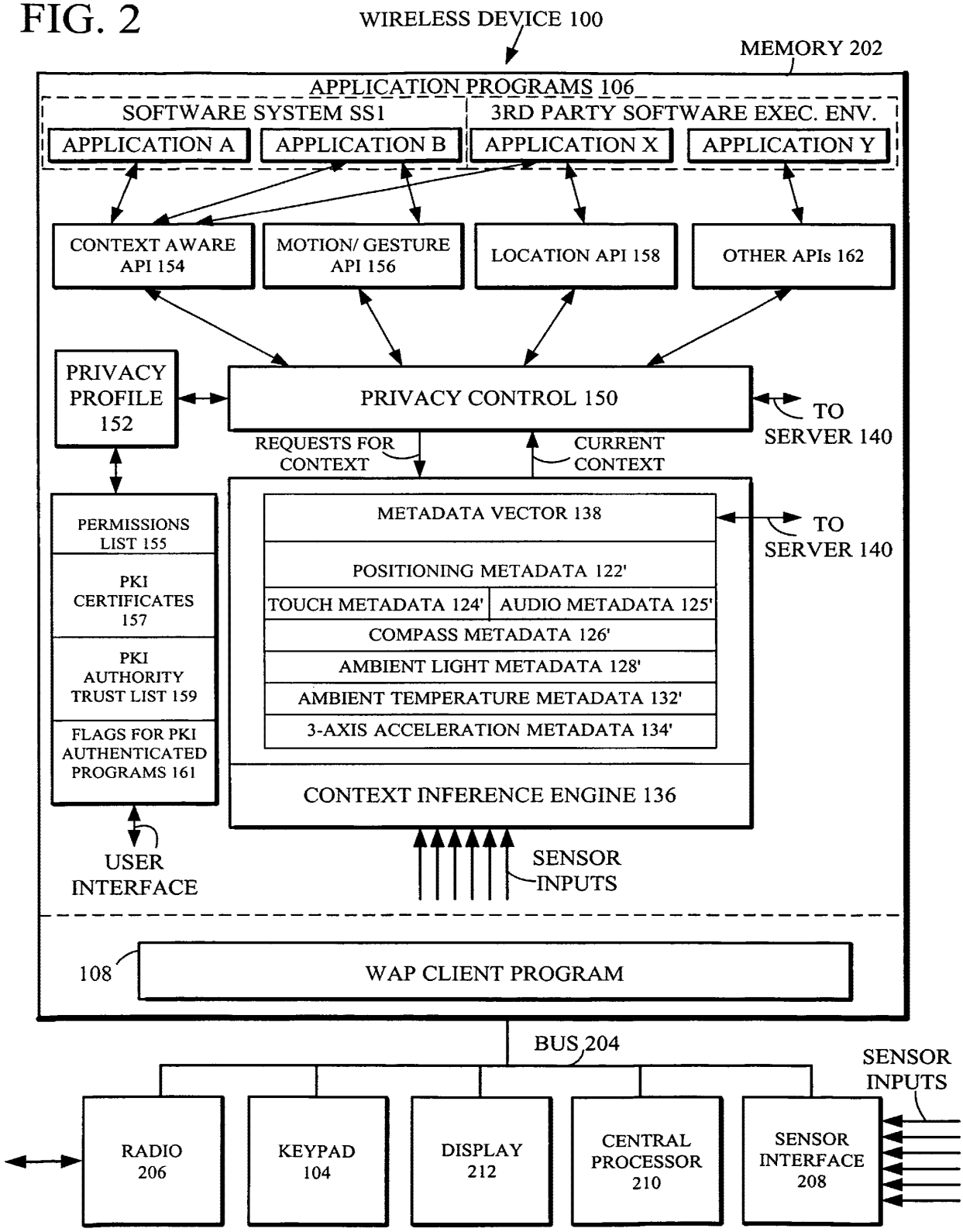

WIRELESS DEVICE 100
MEMORY 202
APPLICATION PROGRAMS 106
SOFTWARE SYSTEM SS1
3RD PARTY SOFTWARE EXEC. ENV.
APPLICATION A
APPLICATION B
APPLICATION X
APPLICATION Y
CONTEXT AWARE API 154
MOTION/ GESTURE API 156
LOCATION API 158
OTHER APIs 162
PRIVACY PROFILE 152
PRIVACY CONTROL 150
TO SERVER 140
REQUESTS FOR CONTEXT
CURRENT CONTEXT
PERMISSIONS LIST 155
PKI CERTIFICATES 157
PKI AUTHORITY TRUST LIST 159
FLAGS FOR PKI AUTHENTICATED PROGRAMS 161
METADATA VECTOR 138
TO SERVER 140
POSITIONING METADATA 122'
TOUCH METADATA 124'
AUDIO METADATA 125'
COMPASS METADATA 126'
AMBIENT LIGHT METADATA 128'
AMBIENT TEMPERATURE METADATA 132'
3-AXIS ACCELERATION METADATA 134'
CONTEXT INFERENCE ENGINE 136
USER INTERFACE
SENSOR INPUTS
108
WAP CLIENT PROGRAM
BUS 204
SENSOR INPUTS
RADIO 206
KEYPAD 104
DISPLAY 212
CENTRAL PROCESSOR 210
SENSOR INTERFACE 208

FIG. 2A

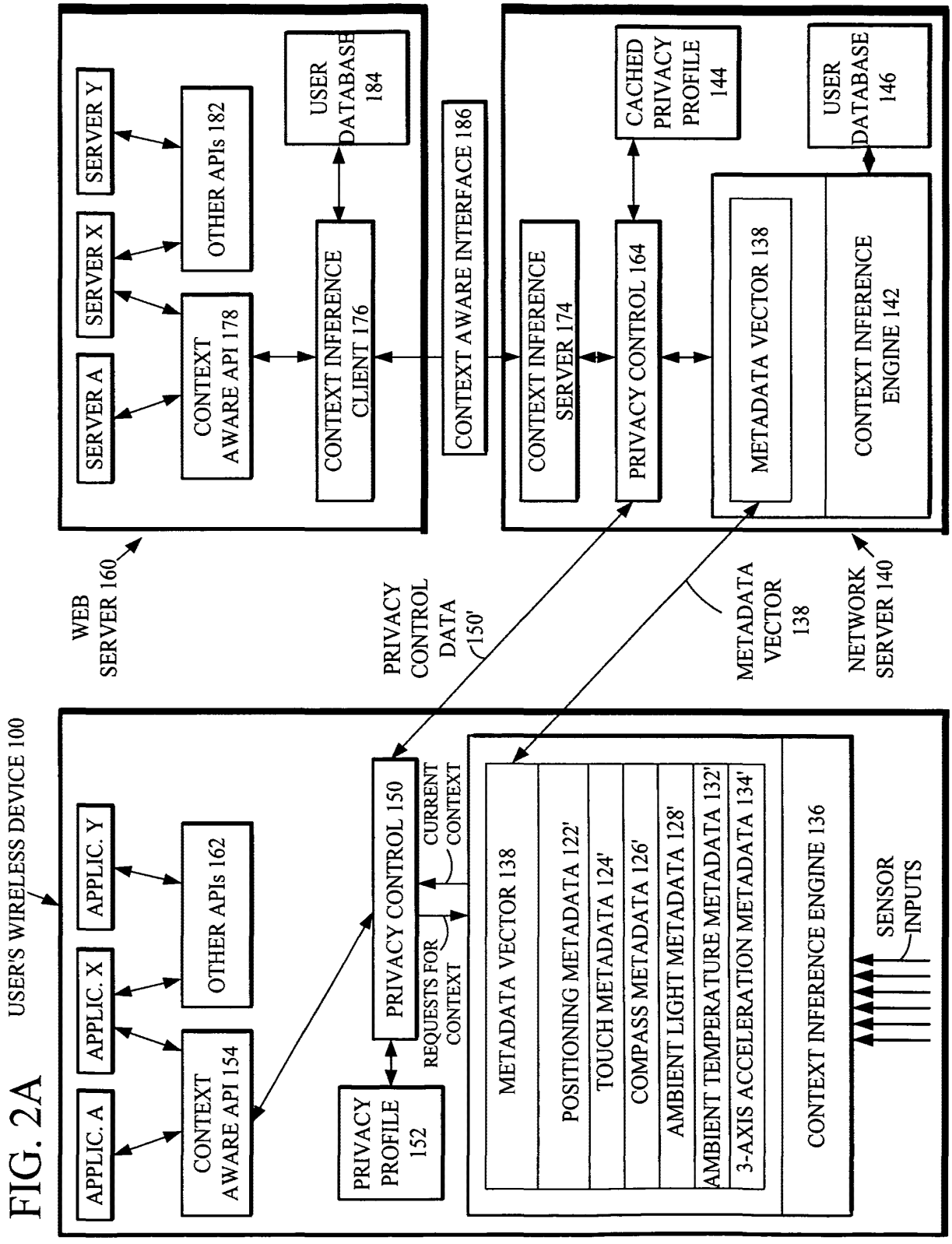

USER'S WIRELESS DEVICE 100
APPLIC. A
APPLIC. X
APPLIC. Y
CONTEXT AWARE API 154
OTHER APIs 162
PRIVACY PROFILE 152
PRIVACY CONTROL 150
REQUESTS FOR CONTEXT
CURRENT CONTEXT
METADATA VECTOR 138
POSITIONING METADATA 122'
TOUCH METADATA 124'
COMPASS METADATA 126'
AMBIENT LIGHT METADATA 128'
AMBIENT TEMPERATURE METADATA 132'
3-AXIS ACCELERATION METADATA 134'
CONTEXT INFERENCE ENGINE 136
SENSOR INPUTS
WEB SERVER 160
SERVER A
SERVER X
SERVER Y
CONTEXT AWARE API 178
OTHER APIs 182
CONTEXT INFERENCE CLIENT 176
USER DATABASE 184
CONTEXT AWARE INTERFACE 186
CONTEXT INFERENCE SERVER 174
PRIVACY CONTROL 164
CACHED PRIVACY PROFILE 144
METADATA VECTOR 138
CONTEXT INFERENCE ENGINE 142
USER DATABASE 146
NETWORK SERVER 140
PRIVACY CONTROL DATA 150'
METADATA VECTOR 138

FIG. 3

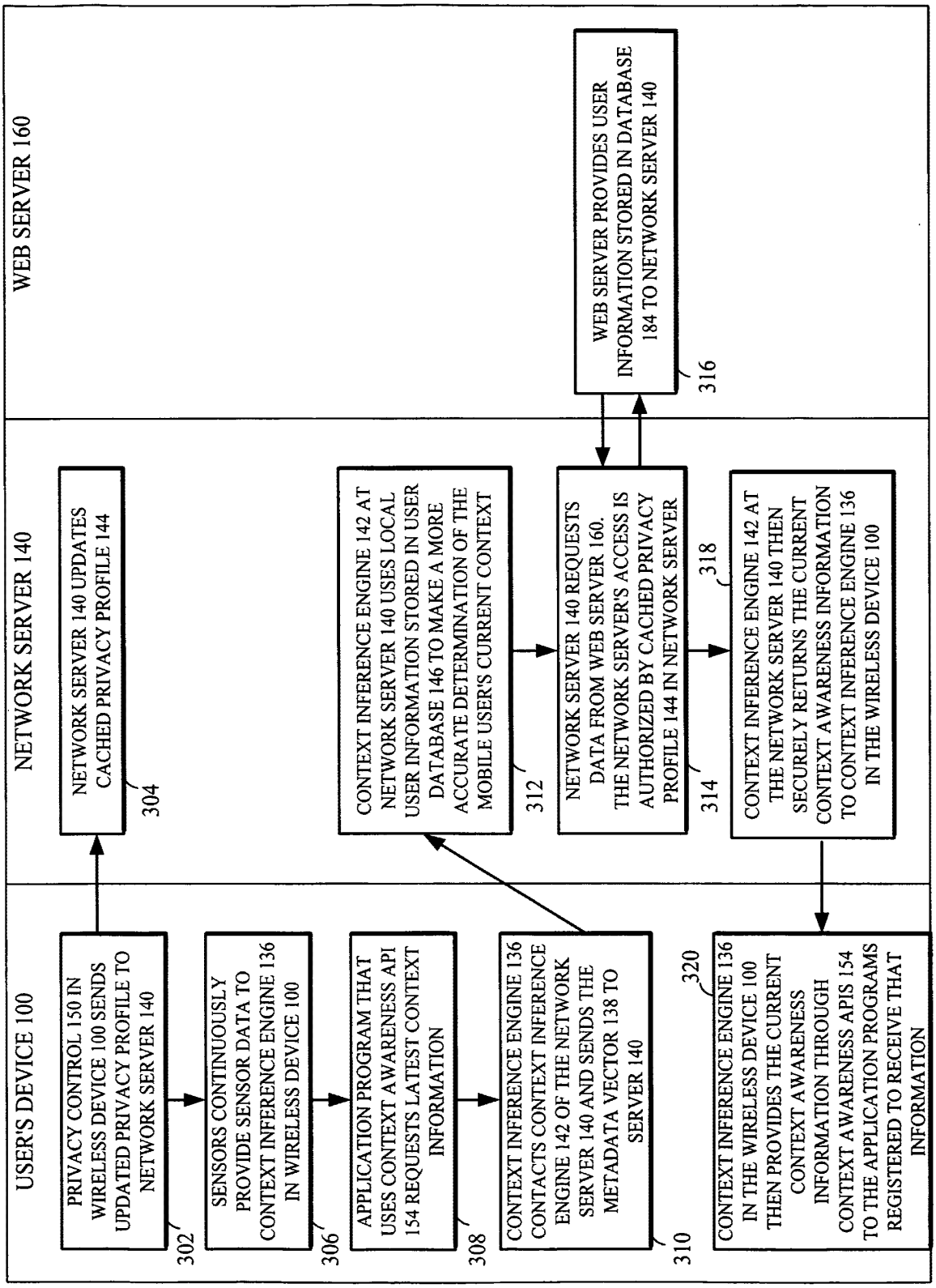
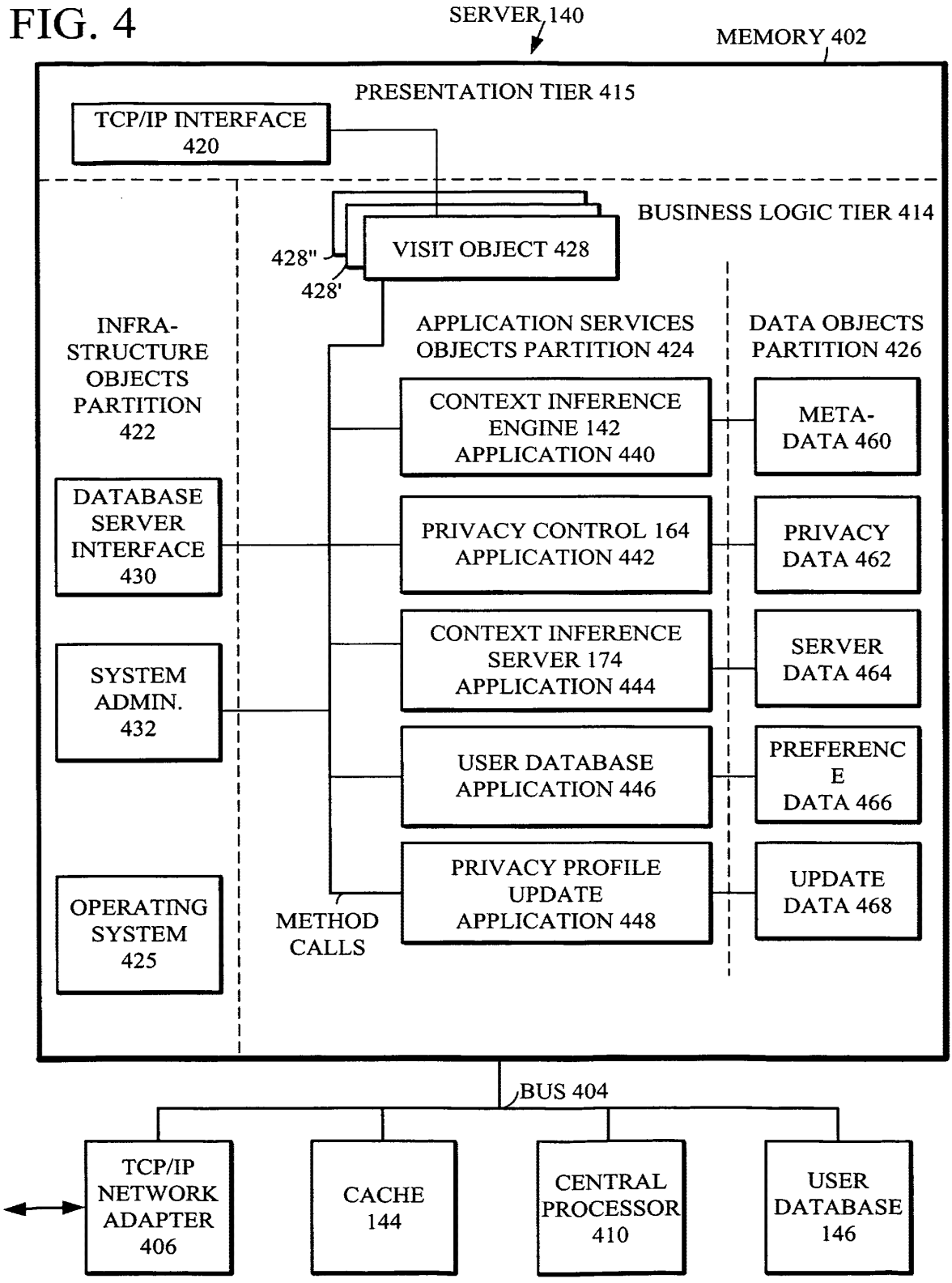

USER'S DEVICE 100
NETWORK SERVER 140
WEB SERVER 160
PRIVACY CONTROL 150 IN WIRELESS DEVICE 100 SENDS UPDATED PRIVACY PROFILE TO NETWORK SERVER 140
302
NETWORK SERVER 140 UPDATES CACHED PRIVACY PROFILE 144
304
SENSORS CONTINUOUSLY PROVIDE SENSOR DATA TO CONTEXT INFERENCE ENGINE 136 IN WIRELESS DEVICE 100
306
APPLICATION PROGRAM THAT USES CONTEXT AWARENESS API 154 REQUESTS LATEST CONTEXT INFORMATION
308
CONTEXT INFERENCE ENGINE 136 CONTACTS CONTEXT INFERENCE ENGINE 142 OF THE NETWORK SERVER 140 AND SENDS THE METADATA VECTOR 138 TO SERVER 140
310
CONTEXT INFERENCE ENGINE 142 AT NETWORK SERVER 140 USES LOCAL USER INFORMATION STORED IN USER DATABASE 146 TO MAKE A MORE ACCURATE DETERMINATION OF THE MOBILE USER'S CURRENT CONTEXT
312
NETWORK SERVER 140 REQUESTS DATA FROM WEB SERVER 160. THE NETWORK SERVER'S ACCESS IS AUTHORIZED BY CACHED PRIVACY PROFILE 144 IN NETWORK SERVER
314
WEB SERVER PROVIDES USER INFORMATION STORED IN DATABASE 184 TO NETWORK SERVER 140
316
CONTEXT INFERENCE ENGINE 142 AT THE NETWORK SERVER 140 THEN SECURELY RETURNS THE CURRENT CONTEXT AWARENESS INFORMATION TO CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100
318
CONTEXT INFERENCE ENGINE 136 IN THE WIRELESS DEVICE 100 THEN PROVIDES THE CURRENT CONTEXT AWARENESS INFORMATION THROUGH CONTEXT AWARENESS APIS 154 TO THE APPLICATION PROGRAMS REGISTERED TO RECEIVE THAT INFORMATION
320

FIG. 4


SERVER 140
MEMORY 402
PRESENTATION TIER 415
TCP/IP INTERFACE 420
BUSINESS LOGIC TIER 414
VISIT OBJECT 428
428"
428'
INFRA-STRUCTURE OBJECTS PARTITION 422
APPLICATION SERVICES OBJECTS PARTITION 424
DATA OBJECTS PARTITION 426
CONTEXT INFERENCE ENGINE 142 APPLICATION 440
META-DATA 460
DATABASE SERVER INTERFACE 430
PRIVACY CONTROL 164 APPLICATION 442
PRIVACY DATA 462
CONTEXT INFERENCE SERVER 174 APPLICATION 444
SERVER DATA 464
SYSTEM ADMIN. 432
USER DATABASE APPLICATION 446
PREFERENCE DATA 466
PRIVACY PROFILE UPDATE APPLICATION 448
UPDATE DATA 468
OPERATING SYSTEM 425
METHOD CALLS
BUS 404
TCP/IP NETWORK ADAPTER 406
CACHE 144
CENTRAL PROCESSOR 410
USER DATABASE 146

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB02/01550

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04M 1/00, 3/00, 3/42, 11/10; H04B 1/38
US CL : 455/3.03, 402, 405, 412-420, 456, 458, 466, 515, 550, 556, 575

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)
U.S. : 455/3.03, 402, 405, 412-420, 456, 458, 466, 515, 550, 556, 575

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,115,611 A (KIMOTO et al) 05 September 2000, figs. 1, 7-8, 10, 12, 19, 27, 31, 42.	1-38
---		---
Y		39-41
Y	US 6,073,075 A (KONDOU et al) 06 June 2000, fig. 3, column 4 lines 26-42.	39-41

☐ 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 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	Date of mailing of the international search report
19 July 2002 (19.07.2002)	27 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer William Trost Telephone No. 703 306-0377

Form PCT/ISA/210 (second sheet) (July 1998)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 January 2006 (12.01.2006)

PCT

(10) International Publication Number
WO 2006/004784 A1

(51) International Patent Classification[7]: H04L 29/06, G06F 1/00

(21) International Application Number: PCT/US2005/022982

(22) International Filing Date: 27 June 2005 (27.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/583,765	28 June 2004 (28.06.2004)	US
60/598,364	3 August 2004 (03.08.2004)	US
60/652,121	11 February 2005 (11.02.2005)	US
60/653,411	16 February 2005 (16.02.2005)	US

(71) Applicant *(for all designated States except US)*: **JAPAN COMMUNICATIONS, INC.** [JP/JP]; 6-25-3 Minami-ohi, Shinagawa-ku, Tokyo, Tokyo 140-0013 (JP).

(72) Inventors; and

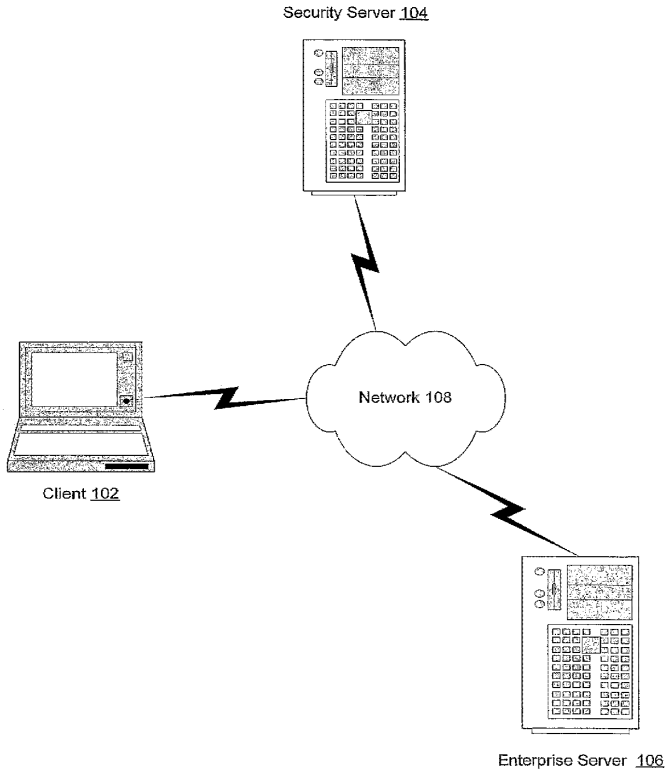
(75) Inventors/Applicants *(for US only)*: **SANDA, Frank, S.** [JP/US]; 29 Plandome Court, Manhasset, New York 11030 (US). **FUKUDA, Naohisa** [JP/JP]; #405, 6-1-8 Kita-Shinagawa, Shinagawa-ku, Tokyo, Tokyo 141-0001 (JP). **LAVES, Edward, W.** [US/US]; 1012 Sleepy Hollow Road, Golden, Colorado 80401 (US). **GURGONE, Raymond, T.** [US/US]; 807 N. Concord Drive, Woodstock, Illinois 60098 (US). **JOHNSTON, Robert, L.** [US/US]; 30 Midland Road, Colorado Springs, Colorado 80906 (US). **ROBINS, David, S.** [US/US]; 6 Wakefield Court, Buffalo Grove, Illinois 60089 (US). **TIDWELL, Justin, Owen** [US/US]; 19058 East Hampden Drive, Aurora, Colorado 80013 (US). **ZEITZ, Karlton, Mark** [US/US]; 6014 S. Zeno Court, Centennial, Colorado 80016 (US). **WORTHINGTON, Laura, J.** [US/US]; 6295 E. Jamison Circle North, Centennial, Colorado 80112 (US).

(74) Agent: **ALEMANNI, John, C.**; Kilpatrick Stockton LLP, 1001 West Fourth Street, Winston-Salem, North Carolina 27101, (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR ENHANCED NETWORK ACCESS



(57) Abstract: Systems and methods for enhanced network access are described. One aspect of one described embodiment includes receiving a request to connect to a network, the request associated with a user, determining a policy associated with the user, identifying at least one available network connection, determining at least one property of the at least one available network connection, evaluating the property based at least in part on the policy, and selecting the at least one available network connection based on the evaluation. In another embodiment, a computer-readable medium (such as, for example random access memory or a computer disk) includes code for carrying out such a method.

WO 2006/004784 A1

GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEMS AND METHODS FOR ENHANCED NETWORK ACCESS

RELATED APPLICATIONS

This application claims priority to Application Serial No. 60/583,765, filed on June 28, 2004, titled "Controlling Use of a Mobile Work Station Based on Network Environment," Application Serial No. 60/598,364, filed on August 3, 2004, titled "Systems and Methods for Enhancing and Optimizing a User's Experience on an Electronic Device," Application Serial No. 60/652,121, filed on February 11, 2005, titled "Remote Access Services," and Application Serial No. 60/653,411, filed on February 16, 2005, titled "Creating an Environment for Secure Mobile Access Anywhere," the entirety of all of which are incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates generally to computer networking and, more particularly to systems and methods for enhanced network access.

BACKGROUND

As the workforce becomes more mobile, enterprises often must provide a means for their users to connect to the enterprise network remotely. Enterprises and their users have much greater flexibility in selecting methods of connecting to the enterprise network as well as other resources, such as the Internet. With this added flexibility comes a concomitant increase in complexity and risk. Thus, although remote access may be necessary, enterprises may resist providing their users with remote access.

Each remote method for connecting to an enterprise network opens a potential security hole that might be exploited. For instance, listeners on a network, such as rogue access points, may be able to determine a user's username/password combination for accessing the network.

Also, each connection type may be purchased from a different network provider. The enterprise must reconcile charges from each of the providers for each of the users accessing the network remotely.

Further, every conventional connection product connecting to the enterprise network provides a unique interface. And although each interface may be relatively straightforward, complexity arises from the enterprise and its users having to deal with multiple interfaces for each of the various network connections the user wishes to make.

SUMMARY

Embodiments of the present invention provide systems and methods for enhanced network access. One aspect of one embodiment of the present invention comprises receiving a request to connect to a network, the request associated with a user, determining a policy associated with the user, identifying at least one available network connection, determining at least one property of the at least one available network connection, evaluating the property based at least in part on the policy, and selecting the at least one available network connection based on the evaluation. In another embodiment, a computer-readable medium (such as, for example random access memory or a computer disk) comprises code for carrying out such a method.

This illustrative embodiment is mentioned not to limit or define the invention, but to provide one example to aid understanding thereof. Illustrative embodiments are discussed in the Detailed Description, and further description of the invention is provided there. Advantages offered by the various embodiments of the present invention may be further understood by examining this specification.

FIGURES

These and other features, aspects, and advantages of the present invention are better understood when the following Detailed Description is read with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram showing an illustrative environment for implementation of one embodiment of the present invention;

Figure 2 is a block diagram illustrating the modules present on a client device 102 in one embodiment of the present invention;

Figure 3 is a block diagram illustrating the modules present on a security server 104 in one embodiment of the present invention;

Figure 4 is a block diagram illustrating the modules present on an enterprise server 106 in one embodiment of the present invention;

Figure 5 is a flowchart illustrating a process for creating a policy for a group in one embodiment of the present invention;

Figure 6 is a flowchart illustrating a process for updating policy information on a client in one embodiment of the present invention; and

Figure 7 is a flowchart illustrating a method for changing a network connection while downloading data in one embodiment of the present invention.

DETAILED DESCRIPTION

Embodiments of the present invention provide systems and methods for enhanced network access. There are multiple embodiments of the present invention. By way of introduction and example, one illustrative embodiment of the present invention provides a method for a client device to seamlessly switch from a first network connection to a second.

As a mobile client device moves from a first location to a second location, the device is provided with an indication that the second network connection is available. The device determines a set of properties regarding the second connection, such as speed, reliability, and cost for the connection. The client device then evaluates these properties based on a set of policies, which are specified by the enterprise with which the user is associated, so that at any one time, the user is connected to the "best" network from the point of view of the enterprise. A rules engine automatically determines which of the two connections is most suitable based on the policies and the properties of the connection.

For instance, the second connection may be faster and cheaper than the first. However, the first connection is more reliable. The enterprise policies weigh speed and cost more highly than reliability. Thus, the client device automatically switches from the first connection to the second connection without any user intervention.

This introduction is given to introduce the reader to the general subject matter of the application. By no means is the invention limited to such subject matter. Illustrative embodiments are described below.

System Architecture

Various systems in accordance with the present invention may be constructed. Referring now to the drawings in which like numerals indicate like elements throughout the several figures, Figure 1 is a block diagram showing an illustrative environment for implementation of one embodiment of the present invention. The system shown in Figure 1 includes a client 102. The client is in communication with a security server 104.

Communication with the security server 104 occurs via a network 108. The network 108 may comprise a public or private network and may include the Internet. The network may also comprise a plurality of networks, including, for example, dedicated phone lines between the various components. In one embodiment, the client 102 communicates with the security server 104 via a virtual private network ("VPN") established over the Internet.

The security server 104 is also in communication with an enterprise server 106 via a network. The network 108 may comprise various elements, both wired and wireless. In one

embodiment, the communication between the security server 104 and enterprise server 106 occurs over a static VPN established over dedicated communication lines.

In one embodiment, a user connects a client device 102 to the network 108 using a network access user interface. The network access user interface is always on and only allows the user to connect to the network 108 via the interface. The network access user interface automatically causes the client 102 to connect to the security server 104 through the network 108. The security server 104 provides value added services to the client 102 and to one or more enterprises. Access to other services, such as the Internet, may be provided via the security server 104.

Although Figure 1 includes only a single client 102, security server 104, and enterprise server 106, an embodiment of the present invention will typically include a plurality of clients 102 and may include a plurality of security servers 104 and enterprise servers 106.

Figures 2 through 4 are block diagrams illustrating components on the client 102, security server 104, and enterprise server 106. Each of the components shown may be a third-party application, a custom application, or a combination of both. Each of the components may also be implemented in hardware, software, or a combination of hardware and software.

Client Devices

Figure 2 is a block diagram illustrating the modules present on a client device 102 in one embodiment of the present invention. Examples of client device 102 are personal computers, digital assistants, personal digital assistants, cellular phones, mobile phones, smart phones, pagers, digital tablets, laptop computers, Internet appliances, and other processor-based devices. In general, a client device 102 may be any suitable type of processor-based platform that is connected to the network 108, and that interacts with one or more application programs. The client device 102 can contain a processor coupled to a computer-readable medium, such as RAM. Client device 102 may operate on any operating system, such as Microsoft® Windows® or Linux. The client device 102 is, for example, a laptop computer executing a network access user interface.

The modules shown in Figure 2 represent functionality of the client 102. The modules may be implemented as one or more computer programs that include one or more modules. For instance, in one embodiment, all the modules shown in Figure 2 are contained within a single network access application. Also, the functionality shown on the client 102 may be implemented on a server in other embodiments of the present invention. Likewise,

functionality shown in Figures 3 and 4 as being on a server may be implemented on the client 102 in some embodiments of the present invention.

The client 102 shown in Figure 2 comprises a VPN client 202. The VPN client 202 allows the client 102 to connect to the enterprise server 106. In one embodiment of the present invention, the VPN client 202 is used to determine whether or not the VPN client 202 is active and whether or not the VPN client 202 is connected to a VPN server. For instance, an embodiment of the present invention may determine whether or not to connect to a particular service based on whether or not the VPN client 202 is enabled.

In another embodiment of the present invention, the VPN client 202 is used for four purposes: (1) to manage policy files, which include information, such as a gateway Internet Protocol (IP) address, secrecy and authentication level, and hash; (2) automatically connecting a VPN; (3) automatically disconnecting the VPN; and (4) monitoring the status of the VPN. Each of these four purposes may be affected by other modules, including, for example, the connection manager 210.

The client 102 also comprises a secure vault 204. The secure vault 204 protects content on the client 102. In one embodiment, the secure vault 204 is responsible for storing encrypted content on the client 102 and allowing access to the encrypted content based on a set of permissions or policies. In such an embodiment, a content creator can provide access via a viewer to secured content and allow a recipient of the content read-only access or allow the recipient to perform other tasks, such as modifying the content and forwarding it to other users. In another embodiment, the secure vault 204 allows the user to create and distribute secure content to other clients 102, the content creator can decide to send a document to several users and allow two of the users full access and one of the users read-only access.

The client 102 shown in Figure 2 also comprises a firewall 206. The firewall 206 allows port blocking via predefined policies. For instance, in one embodiment, an information technology ("IT") manager specifies port blocking based on two zones, a safe zone and a dangerous zone. The IT manager specifies one of these two zones for each of the network interface devices installed on the client 102. The IT manager is then able to set port-blocking rules by zone on the firewall 206.

For example, the IT manager may classify a Wireless Fidelity ("Wi-Fi") network interface as dangerous since it has traditionally been considered fairly unsafe. And the IT manager may apply more restrictive port-blocking rules to the dangerous zone than to the safe zone and network interface devices, such as those used to connect to a wired Local Area Network ("LAN") or a Personal Handyphone System ("PHS") cellular connection. The PHS

standard is a TDD-TDMA based microcellular wireless communications technology and has been traditionally considered relatively safer than Wi-Fi connections. The PHS cellular connection may also be referred to as a wireless wide area network ("WWAN") as opposed to a dial-up connection providing access to a wide area network ("WAN").

In various other embodiments, the port-blocking rules of the firewall 206 may be based on time of day, client IP address, terminating IP address, terminating and originating port, protocol, and other variables. In one embodiment, the port-blocking rules are based on policy data associated with individual users logged into the client 102.

In one embodiment, the port-blocking rules of the firewall 206 include a blacklist. The blacklist allows an IT manager to prevent an application from executing on the client 102. For instance, an IT manager may blacklist a DVD player so that a user is unable to view DVD's on the client 102. The firewall 206 may provide a message to the user informing the user that an application is unavailable.

In another embodiment, the firewall 206 implements a white list. The white list is somewhat more restrictive than the blacklist described above. The white list allows only specified applications to execute. For example, an IT manager may allow only MS Word, Excel, PowerPoint, and Outlook to execute. No other applications will be permitted to execute. The firewall 206 may be a custom firewall or a third-party firewall integrated into an embodiment of the present invention.

The embodiment shown in Figure 2 also includes an antivirus module 208. The antivirus module 208 shown determines whether policy files, virus dictionary, or other virus-related resources are out of date and provides the client 102 with a mechanism for updating the files or data. The antivirus module 208 may restrict access to various connections, applications, and other functionality when the policy files are out of date. For instance, the antivirus module 208 may restrict the client 102 to connecting to a single gateway through which the policy files are available. In one embodiment, the antivirus module 208 comprises a third-party antivirus product that is integrated with the other modules on the client 102.

The client 102 also comprises a connection manager 210, which includes a rules processor. In one embodiment, the connection manager 210 assigns a priority number to every connection, e.g., one to one hundred, and selects the connection with the highest number to connect to.

The connection manager 210 may provide a connection to a variety of networks, including, for example, dial-up, LAN, digital subscriber line ("DSL"), cable modem, Wi-Fi, wireless local area network ("WLAN"), PHS, and satellite.

In one embodiment, the connection manager 210 differentiates between public and private connections. A public connection is a connection provided by a service provider who has a relationship with the administrator of the security server 104, which allows the security server 104 to authenticate the connection. For instance, the security server 104 administrator may have a business arrangement with a hotspot provider. In order to connect, the client 102 connects to a local access point and the authentication of the user occurs automatically at the security server 104. In contrast, a private connection requires that all aspects of the authentication mechanism for a connection are managed in the absence of the security server 104, although the connection manager may provide certain facilities to allow for automated authentication where possible.

In one embodiment, the connection manager 210 makes connections available or unavailable to the client 102 based on policies present on the client 102. The connection manager 210 may also download changes to policy data and transmit quality of service ("QoS") and other data to the security server 104 or the enterprise server 106.

In one embodiment, the connection manager 210 determines the type of connections that are available based on signals provided by hardware associated with the client 102. For example, when the client 102 passes near a hotspot, a Wi-Fi card in the client 102 senses the hotspot and sends a signal to the connection manager 210. For instance, the Wi-Fi card may sense a broadcast service set identifier ("SSID"). Once the signal exceeds a threshold, the connection manager 210 provides a signal to a user of the client 102 that the network is available or may automatically connect to the hotspot. Alternatively, the Wi-Fi card may poll for a non-broadcast SSID. The connection manager 210 may provide a single connection to the client 102 at one time or may provide multiple connections to the client 102.

The client 102 shown in Figure 2 also comprises a QoS collector 212. The QoS collector 212 collects data values, including, for example, the number of bytes sent and received, the average transfer rate, the average signal strength at connection, termination cause, failed connections, and a network identifier. In another embodiment, the QoS collector 212 collects data during the session to determine when a connection provides inconsistent performance.

In one embodiment, the QoS collector 212 collects data regarding a connection during a session but does not send the data for a session until the next session. Thus, if a session is terminated abnormally, the QoS data will still be collected and transferred successfully. In another embodiment, the QoS collector 212 transfers data only when a particular type of connection is detected, such as a high-speed or low cost connection.

The client 102 also comprises a session statistics module 214. The session statistics module stores data representing user characteristics. For instance, the session statistic module 214 may store a list of the applications a user generally accesses, how often the user is connected, the typical CPU and memory utilization measure, keyboard sequences, and other characteristics of a user. If a particular user deviates from the expected characteristics by greater than a threshold, such as N standard deviations, and the significance of the statistic is more than a specified amount, the session statistics module 214 can identify the current user as a potential unauthorized user.

The session statistics module 214 may perform other tasks as well. For instance, in one embodiment, the session statistics module 214 pre-loads applications based on a user's general usage patterns.

The client 102 shown in Figure 2 also comprises a policy reader 216. In one embodiment, a company's policies are housed on the enterprise server 106. For instance, individual groups and users within an enterprise are identified and associated with policies, such as what types of connections they are able to access and what a user's VPN profile is. The user may also be able to specify a VPN policy on the client 102. In such an embodiment, the policy reader 216 downloads the policy rules from the enterprise server 106 and accesses local user policies and reconciles any conflicts between the two.

For example, an IT manager may establish a VPN profile to be used by a user when connecting to a Wi-Fi network. However, the user may wish to create a secondary VPN profile to be used if the first VPN becomes unavailable. The policy reader 216 loads both local and enterprise VPN profiles, resolving any conflict between the two VPN profiles.

In one embodiment, the policy reader 216 accesses data at an enterprise, department, and user level. In such an embodiment, some of the policy rules may be stored in a lightweight directory access protocol ("LDAP") server on the client 102, security server 104, or enterprise server 106. In another embodiment, the policy reader 216 receives only changes to policy data and does not typically download all of the policy data at once. Policies downloaded by the policy reader 216 may be provided to the rules processor of the connection manager 210.

The client 102 may also comprises a client security module 216. In one embodiment, the client security module 216 implements a client asset protection process. When the client security module 216 receives a signal indicating that the client asset protection process is to be executed, the client security module 216 may, for example, disable devices and interfaces

on the client device 102 and may, in some embodiments, encrypt the hard drive of the client device 102 so that the files stored on the drive are not easily accessible.

The client 102 may also comprise a user interface 220. The user interface 220 may control the underlying operating environment or the user's view of the underlying environment. For example, in one embodiment, the user interface 220 supplants the Microsoft® Windows operating system interface from the user's perspective. In other words, the user is unable to access many of the standard Windows features. Such a user interface may be implemented to limit the applications and configuration setting a user is able to access. In some embodiments, such as a personal digital assistant ("PDA"), no user interface is provided by an embodiment of the present invention; the standard PDA user interface is utilized.

The user interface 220 provides the user with an easy-to-use mechanism for accessing network connections. In one embodiment, when the user interface 220 is visible, it provides a very easy-to-use format that displays network connection types and provides other functionality to the user. For example, during complex operations, such as connecting to a new network type, the user can simply select a single button within the user interface 220 and the client 102 will properly disconnect from the previous network, acquire the new network, perform all authentication and policy-based requirements, and then allow the user to continue using an application on the new network. This simple, easy-to-use user interface 220, the complexity of which may be hidden and completely automatic, allows a less-technical user to successfully operate the client 102. All network connection, authentication, secure sign on, VPN parameters, and other aspects of the connection are managed by the user interface 220.

The client 102 shown in Figure 2 also comprises a security agent 222. In some embodiments, the security agent 222 is also referred to as a "bomb." In one embodiment, an IT manager indicates that the security agent 222 should be activated when the client 102 next connects to the enterprise server 106. The IT manager may do so because the client 102 has been reported stolen. Subsequently, the client 102 connects to the enterprise server 106, either directly or indirectly and receives the message to initiate the security agent 222.

In one embodiment, when the security agent 222 activates, it stops all applications from being able to run and encrypts the data on the hard drive of the client 102. For instance, the security agent 222 may implement a white list as described above and then implement a secure vault for all data on the client 102. The connection manager 210 may also be configured so that no connections are possible.

In one such embodiment, since the data is merely encrypted by security agent 222, rather than erased, the data may be recovered if the client 102 is subsequently recovered. For instance, the enterprise may retain the key needed for decrypting the local drive. The client 102 is returned to the enterprise, which then decrypts the drive. In another embodiment, the data on the local drive of the client is rendered inaccessible by, for example, writing over the data multiple times.

The client 102 shown in Figure 2 also comprises an out-of-band communication receiver 224. The out-of-band communication receiver 224 allows the client to receive communications other than through a network-based connection. The connection manager 210 may manage the out-of-band communication. For instance, the command to activate the security agent 222 may be transferred via a short messaging service ("SMS") communication received by the out-of-band communication receiver 224.

Security Server

Figure 3 is a block diagram illustrating the modules present on a security server 104 in one embodiment of the present invention. The security server 104 shown in Figure 3 comprises a remote authentication dial-in user service ("RADIUS") server 302, which may also be referred to as an AAA (authentication, authorization, and accounting) server. RADIUS is the standard by which applications and devices communicate with an AAA server.

The RADIUS server 302 provides authentication services on the security server 104. In some embodiments of the present invention, the RADIUS server 302 proxies to a RADIUS server on the enterprise server 106. In one embodiment, the RADIUS server 302 provides mutual authentication for the client 102 using Extensible Authentication Protocol Transport Layer Security ("EAP-TLS"). Although EAP-TLS itself is strictly an 802.1x authentication protocol, designed primarily for WiFi connections, the underlying TLS authentication protocol may be deployed in both wired and wireless networks. EAP-TLS performs mutual secured sockets layer ("SSL") authentication. This requires both the client device 102 and the RADIUS server 302 to have a certificate. In mutual authentication, each side may prove its identity to the other using its certificate and its private key.

The security server shown in Figure 3 also comprises an LDAP server 304. The LDAP server 304 uses the LDAP protocol, which provides a mechanism for locating users, organizations, and other resources on the network. In one embodiment of the present invention, the LDAP server 304 provides access control at the network layer to various components that an enterprise customer may or may not purchase. For example, a customer

may choose to implement a secure vault as described in relation to Figure 1. In such a case, the customer or users or groups associated with the customer are also associated with the firewall module. The LDAP entry is then used to determine that the firewall is to be enabled on a client.

In some embodiments, the LDAP server 304 is implemented as a list of user identifiers not using the LDAP protocol. In another embodiment, data in the LDAP server 304 is propagated from data present in the enterprise server 106.

The security server 104 shown in Figure 3 also comprises a session manager 306. The session manager 306 controls sessions, including sessions between the client 102 and enterprise server 106. In some embodiments, the session manager 306 also determines how to route data requests. For instance, the session manager 306 may determine that a particular data request should be routed to the Internet rather than to the enterprise server 106. This may be referred to as "splitting the pipe" and provides a mechanism to replace "split tunneling" (a traditional configuration option with most standard VPN clients) at the client device by the more secure split of traffic not intended for the enterprise at the security server, allowing monitoring of all traffic without the enterprise incurring the expense of the extra bandwidth required.

In some embodiments, the client 102 and enterprise server 106 establish a VPN for communication. In such an embodiment, the session manager 306 may be unable to route requests to any location other than the enterprise – the packets are encrypted and thus, cannot be separately evaluated.

In one embodiment, the session manager 306 performs automated authentication of a client device 102 or user. For example, if the session manager 306 determines that a client 102 is approaching a Wi-Fi hotspot, the session manager 306 is able to pre-populate the hotspot with the certificate that the hotspot requires to authenticate the user. In this manner, the authentication appears very fast to the user. The session manager 306 may also control the manner in which data is queued for download to the client device 102.

In one such embodiment, the session manager 306 provides two modes for data queuing. In a first mode, the session manager 306 determines that the network down time will be brief, e.g., the user is moving through a tunnel, which interferes with network access. In such a case, the session manager queues a minimal amount of data. In a second mode, the session manager 306 determines that the network down time will be of a longer duration, e.g., the user is boarding a plane from New York to Tokyo. In such a case, the session manager 306 may queue a larger amount of data. In one such embodiment, the session manager 306

determines the mode by querying the user for the downtime interval. When the user reconnects to the security server 104, the session manager 306 determines the best manner of downloading the queued data and begins the download.

In one embodiment, the session manager 306 comprises a packet shaper (not shown). The packet shaper provides various functional capabilities to the session manager 306. For example, in one embodiment, the packet shaper provides a mechanism for prioritizing packets sent between the enterprise server 106 and the client 102. In one embodiment, the packet shaper utilizes Multiprotocol Label Switching ("MPLS"). MPLS allows a specific path to be specified for a given sequence of packets. MPLS allows most packets to be forwarded at the switching (layer 2) level rather than at the (routing) layer 3 level. MPLS provides a means for providing QoS for data transmissions, particularly as networks begin to carry more varied traffic.

The session manager 306 may also provide session persistence capabilities. For instance, in one embodiment, when a user drops a connection or moves from one provider network coverage area to another, the connection manager 306 persists a virtual connection as the first connection is terminated and the second is initiated.

The session manager 306 may include a server-side rules engine. The server-side rules engine may use historical information, such as the session statistics described above, for statistical attack determination. For instance, session manager 306 may access a stored statistic regarding a client device 102 and based on monitoring of the current statistics for the client device 102 determine that an unauthorized user is using the client device 102.

The security server 104 shown in Figure 3 also comprises a real-time monitor 308. The real-time monitor 308 monitors the status of communications, such as which clients and users are logged on, the amount of data being transferred, ongoing QoS measures, ports in use, and other information.

When the real-time monitor 308 detects a problem, it may issue an alert to network support. In one embodiment, data from the real-time monitor 308 is provided to users via a portal available on the security server 308. In another embodiment, the real-time portal 308 transfers information to the enterprise server 106, from which users access the data.

The embodiment shown in Figure 3 also comprises a historical monitor 310. The historical monitor 310 provides information similar to the real-time monitor 310. However, the underlying data is historical in nature. For instance, in one embodiment, the historical monitor 310 provides audit information for making intelligent business decisions and for dealing with regulatory compliance issues.

The information available via the historical monitor 310 may include, for example, historical QoS data, registration compliance data, and metrics consistency data. The historical data monitor 310 may be used to determine that certain clients are not performing optimally by comparing metrics of various clients over time. For instance, by evaluating information available via the historical data monitor 310, a support person may be able to determine that a radio tuner on a specific client device 102 is failing. If the user of one client device 102 is complaining about the availability of service, but other users are able to successfully access service, then the client device's radio may be the problem.

The historical data monitor 310 may also be used to reconcile information captured on the security server 104 regarding connections and data provided by telecommunication carriers. The data may be used to determine when certain resources need to be increased and when a certain carrier is not performing adequately.

The security server also comprises a database 312. In embodiments of the present invention, the database 312 may be any type of database, including, for example, MySQL, Oracle, or Microsoft SQL Server relational databases. Also, although the database 312 is shown as a single database in Figure 2, the database 312 may actually comprise multiple databases, multiple schemas within one or more databases, and multiples tables within one or more schemas. The database 312 may also be present on one or more other machines, e.g., database servers.

In one embodiment of the present invention, the database 312 stores customer information regarding enterprises served by the security server 104, such as a list of valid users, a list of valid cellular cards, the relationships between the individual users and groups within the enterprise, and other customer information.

For example, in one embodiment, the database 312 stores an association between users and cellular data cards. The enterprise may allocate a single user to a specific data card. Alternatively, the enterprise may associate a group of users with a group of cellular data cards. Other types of data may also be stored in the database 312, such as billing data.

The security server 104 shown in Figure 3 also comprises a QoS server 314. The QoS server 314 uploads information from the QoS collector 212 on the client device 102 and stores the QoS data. The QoS server 314 can collect data from multiple clients and store it in the database 312.

The security server also comprises a QoS tools engine 316. The QoS tools engine 316 displays data made available by the QoS server 314 and other processes, such as the real-time monitor 308.

In one embodiment, the QoS tools engine 316 provides an aggregation of QoS data in a spreadsheet. In another embodiment, the QoS tools engine 316 provides data using map views, pie charts, and graphs. The QoS tools engine 316 may also provide the capability for setting QoS-based alarms and may provide data to users via a portal.

In the embodiment shown in Figure 3, the security server 104 also comprises a portal server 318. The portal server 318 may be, for example, a web server. Any standard web server application may be utilized, including Microsoft® Internet Information Server ("IIS") or Apache.

Although the security server 104 shown in Figures 1 and 3 is illustrated as a single server, it may comprise multiple servers. For example, in one embodiment of the present invention, the security server 104 comprises multiple regional servers.

Also, the description above suggests that data is provided to and queried from the security server 104 by the client 102, i.e., the client pulls the data. However, in some embodiments, the client 102 also comprises a listener (not shown) so that the security server 104 can push data to the client 102.

Enterprise Server

Figure 4 is a block diagram illustrating the modules present on an enterprise server 106 in one embodiment of the present invention. The enterprise server 106 may also be referred to herein as a customer server and may comprise one or more servers for one or more enterprises linked to one or more security servers 104.

The enterprise server 106 shown in Figure 4 comprises a policy server 402. The policy server 402 provides a means for managing the policy rules, including, for example, available VPN profiles, available transports (e.g. WiFi, LAN, PHS, Dialup), firewall rules, such as blacklists and white lists, connection rules, and antivirus rules. The policy server 402 may include other rules as well, such as the level of data throttling to perform for each client or group of clients. Data throttling limits the data transfer rate to a particular client 102 so that connection resources can be optimized.

The policies may be managed at one or more levels. For example, an IT manager may wish to create a VPN profile for the enterprise as a whole, but a different VPN profile for an engineering group since the engineering group needs access to various unique applications.

The policy server 402 may also provide a mechanism for configuring the location of various servers that the client 102 will utilize. For instance, the policy server 402 may allow an IT manager to specify the IP address of an acceleration server 404 or a vault server 406

In one embodiment, the policy server also allows the IT manager to specify which users receive updates for various components on the client 102. The policy server 402 may also allow the IT manager to perform connection configuration. For instance, the IT manager may use the policy server to specify phone numbers for PHS connections, Wi-Fi SSID's for private connections, and other connection configuration information.

The enterprise server 106 shown in Figure 4 also comprises an acceleration server 404. The acceleration server 404 performs processes to improve the performance of data transfer. For instance, the acceleration server 404 may automatically compress images that are to be transferred to a client 102.

In one embodiment, the acceleration server 404 communicates with the policy server 402. An IT manager sets acceleration rules using the policy server 402, and the acceleration server 404 uses these rules to determine what level of acceleration to use for a particular communication. In one embodiment, the IT manager sets a default level of acceleration for all communication and a specific level of acceleration for one group of users. The specific level of acceleration may be referred to as an override.

The enterprise server 106 also comprises a vault server 406. The vault server comprises two components, an automatic component and an administration component. In one embodiment, the automatic component integrates with an enterprise's mail server (not shown) and performs operations on emails to and from the mail server. For instance, the vault server 406 may quarantine an email, automatically encrypt the email before it is sent, add a legal disclaimer to an email, or perform other functions on the email.

In one embodiment, the automatic component of the vault server 406 searches an email based on words or based on the domain or specific address to which the email is addressed or from which the email originated. Using this information, the user can perform functions on the email, such as those described above.

The administration component of the vault server 406 allows a user to terminate access to secure content, either by a specific user or by all users. It also logs activity. Using one embodiment of the vault server 406, a user can indicate that a set of users whose employment has been terminated will no longer have access to any secure content. In an alternative embodiment of the vault server 406, a user can indicate that a given element of secure content, say a price list, is now out of date, and so that piece of secure content will no longer be viewable by any user. When each user accesses the secure content, the vault server 406 logs the event. So for each secure content element, the vault server 406 creates a log of all activity on the secure content.

In one embodiment, the vault server 406 also compresses data. For instance, one embodiment utilizes standard PKZIP compression to compress all content. In another embodiment, an IT manager may identify three types of images and specify a different level of compression for each type of image based on the level of resolution necessary for each type of image.

The enterprise server 108 also comprises a RADIUS server 408 and LDAP server 410, which are similar to those described above in relation to the security server 104. The RADIUS server 302 on the security server 104 may proxy to the RADIUS server 408 on the enterprise server 106. Similarly, data in the LDAP server 410 may be propagated to the LDAP server 204 on the security server 104.

The enterprise server 106 also comprises a one-time password ("OTP") server 412. The OTP server 412 provides a mechanism for authentication. For instance, in one embodiment of the present invention, the enterprise server 106 uses the OTP server 412 to perform a mutual authentication process.

The enterprise server 106 also comprises a concentrator 414. The concentrator 414 provides remote access capability to the client 102. For instance, the concentrator 414 may serve as a means for terminating a VPN between the client 102 and enterprise server 106.

The enterprise server 104 shown in Figure 4 also comprises a portal server 416. The portal server 416 may comprise a standard web server, such as IIS or Apache. The portal server 416 may provide one or more portals. For example, in one embodiment, the portal server 416 provides two portals, portal one and portal two.

Portal one provides a configuration interface for managing the various elements shown in Figures 2 and 3, including, for example, the policy server 402 and LDAP server 410. Portal two provides an interface for accessing data, such as QoS data and session data.

For instance, a user may use historical QoS data on portal two to determine how a particular provider is performing in terms of throughput, user connections, and other QoS metrics. Portal two may also provide real-time information, such as how many users are currently connected.

For instance, in one embodiment, an IT manager determines that twenty users have been rejected by a carrier in the last three minutes due to authentication failure and five users with the same user identifier are currently logged on to five different devices. The IT manager uses this information to detect a potential security problem. Portal two may also be used to set alerts as described above.

It should be noted that the present invention may comprise systems having a different architecture than that which is shown in Figures 1 through 4. For example, in some systems according to the present invention, the security server 104 and enterprise server 106 may comprise a plurality of security and enterprise servers. The system 100 shown in Figures 1 through 4 is merely illustrative, and is used to help explain the illustrative systems and processes discussed below.

Illustrative Methods of Enhanced Network Access

The following illustrative embodiments utilize a central policy server 402 on an enterprise server 106. The client device 102 downloads policies from the policy server 402 and the connection manager 210 utilizes the policies to make connections. In other embodiments, policy files are created and distributed to the client device 102 in other ways. For example, an email attachment or disk may be distributed to each client device 102. Each time an update is necessary, a new disk or email is distributed.

In embodiments of the present invention, policies are created and distributed to client devices 102. The client devices 102 utilize the policies for making connections. Figure 5 is a flowchart illustrating a process for creating a policy for a group in one embodiment of the present invention.

In the embodiment shown in Figure 5, policy administrator first determines a policy 502. The policy may be based on a variety of factors, such as, for example, regulatory issues, the type of data and/or applications to be used, the level of control desired by the enterprise, the physical environment in which a client device or group of client devices will operate, the experience and technical knowledge of the user group associated with the policy, and the job to be performed by the group or groups associated with the policy. The policy may include various elements, including, for example a list of allowed connections or applications and a list of disallowed connections or applications, acceleration preferences, and a VPN profile. The policy may also include connection preferences of the enterprise or of the users. For instance, an enterprise may decide not to use certain WiFi hotspots. The policy may vary by time of day.

The policies may be based on a number of factors, including, for example, an enterprise's need to minimize overall transport cost when billed on a usage basis, an enterprise's wish to minimize perceived security exposure based on assumed insecurity on some transports and specific connections, and an enterprise's wish to ensure the highest speed and most reliable usage experience for their users. The policies may be based on third party

parameters as well. For instance, the policy may be based on the enterprise's security provider's desire to minimize its transport costs overall.

The policy administrator next selects a group to be associated with the policy 504. The administrator may manually enter group names and user identifiers. Alternatively, the administrator may select groups from a central directory, such as the LDAP 410 or a Microsoft Active Directory Server. Each policy may be associated with, for example, an enterprise, a group within the enterprise or across enterprises, or with an individual.

Once the administrator has created a policy and associated the policy with a group, the administrator saves the policy-group association 506. The policy-group association may be stored in a database (not shown) in communication with the policy server 402. Alternatively, the policy-group association may be stored in a file, for example, in an XML format in a file.

The administrator then causes the policy and policy-group association to be distributed to client devices 508. For instance, the policy and policy-group association may reside in the database, which is in communication with the policy server 402, so that when a client device attempts to download a policy, the policy-group association is used to determine which policy or policies to download. The policy and policy-group association may be distributed via a network, such as network 108, or by media, such as CD-ROM. In one embodiment, only changes to the policies are downloaded. In other embodiments, all policies are downloaded each time a download occurs.

In some embodiments, once the policies are downloaded to the client device, the user may make changes to them. For instance, the user may set up an alternative VPN profile on the client if the VPN associated with the VPN profile downloaded from the policy server 402 is temporarily unusable.

Figure 6 is a flowchart illustrating a process for updating policy information on a client in one embodiment of the present invention. In the embodiment shown, the policy reader 216 on the client device 102 loads policies 602. For instance, the policies may exist in an XML file, which the policy reader 216 opens and reads.

The connection manager 210 then determines what the most recently used connection was and whether the most recently used connection is available 604. For example, a user may shut down a client device 102 while the client device 102 is connected to a WiFi hotspot. When the user starts the client device 102, the client device will attempt to connect to the WiFi hotspot.

If the client device 102 is not able to connect to the most recently used connection, the client device 102 attempts to identify a new connection 606. For example, the client device 102 may have moved out of range of the WiFi hotspot to which the client was connected. The client device 102 identifies all currently-available connections. The client device 102 also identifies one or more policies associated with the user. The client device 102 then identifies properties of the network connection or connections and compares the network properties to the policy (rule). A network property may be, for example, quality of service measures, such as security, reliability, and speed may be utilized. The client device 102 may also use cost or a combination of cost and a plurality of other properties in making the determination. In one embodiment, the client device 102 applies a normalization algorithm to the plurality of properties to come up with a single number for each network connection. The client device 102 then compares the single numbers to determine to which network to connect.

Using either the most recently used connection or the newly-identified connection, the client device connects to the policy server (402) 608. For instance, the client device 102 may connect to the most recently used WiFi hotspot and then establish a connection with the policy server 402 and the QoS server 310 over the Internet.

Once the client device 102 has established a connection with the network, the client device uploads QoS data to the QoS server (310) 610. In one embodiment, QoS data from the previous session is uploaded at the start of the current session so that interruptions in service, such as a lost connection, can be accurately tracked.

The client device next downloads the latest policy data from the policy server (402) 612. The policy data may comprise only changes since the last connection. For example, the client device 102 may store a last download date and only download policies from the policy server 402 that have been created or changed since the last update date. The client device may download other information as well. For instance, the administrator may determine that a particular client device 102 has been stolen and set an indicator to cause the client device to encrypt data on its hard drive. When the client device 102 connects, it downloads the indicator.

The process may be transparent to the user. In one embodiment, the download process runs as a service. Each time the client device 102 starts up, the process executes. The process may also include having the client device 102 connect to a VPN automatically so that the user can access enterprise applications.

Figure 7 is a flowchart illustrating a method for changing a network connection while downloading data in one embodiment of the present invention. In the embodiment shown, the connection manager 210 receives an indication to change network connections 702. The indication may be due to an identification of a newly available network, a manual selection by a user, or some other indication. For instance, a hardware device, such as a cellular data card, may indicate that a new connection is available. The user receives the indication and decides to change to the new network and clicks a button on a user interface, indicating the desire to change.

In one embodiment, the connection manager 210 identifies a new network. The connection manager then compares a first property of the currently connected (existing) network to a first property of the second new network. The properties may signify the same or similar information about the two networks, e.g., the type of network. Based on policies, the connection manager 210 determines to which network to connect.

In one embodiment, the connection manger 210 rules engine makes connection decisions based on six core pieces of data for connection that is physically available (the correct device is installed and operating, and a signal is available):

(1) Is the connection allowed for this user;

(2) How secure is the connection deemed to be;

(3) How reliable is the connection deemed to be;

(4) How fast is the connection deemed to be;

(5) How expensive is the connection relative to others for the enterprise; and

(6) How expensive is the connection relative to others for a service provider, such as a network security service provider?

Item (1) in this list is specified based on whether or not the connection is available to the enterprise in general and whether the enterprise has made the connection available to the user (or, more precisely in some implementations, not barred the user from the connection). Item (2) is based on enterprise preference indication. It could also be based on attack detection algorithms automatically applied, e.g., if relatively more attacks on a specific type of connection or specific location are detected, then relatively more attacks are occurring.

Item (3) is based on connection statistics. In one such embodiment, the enterprise has the option to indicate perceived relative reliability measures. Item (4) is also based on connection statistics. Item (5) is based on the pricing plan that the enterprise has entered into with the provider. And item (6) is based on carrier pricing arrangements and usage assumptions for various connections.

One embodiment of the present invention takes each of these six items and uses a normalization algorithm to work these elements (with their relative strengths) into a "weighting" within a range. Then, the rules engine on the client device 102 simply selects the connection with the highest weighting.

In some cases, despite the rules based analysis, an enterprise may not wish for a user to use a specific connection for a given, short period of time. In one embodiment, the system allows the enterprise to specifically exclude a connection for a short time.

Before disconnecting, the connection manager 210 sends a signal to the session persistence server 316 to suspend any currently active data transfer 704. By suspending data transfer, the connection manager 210 helps to eliminate the potential for losing data.

The connection manager 210 then disconnects the client device 102 from the network (108) 706. The process for disconnecting may differ between various networks. During the period when the client device 102 is disconnected, the session persistence server 316 caches data. After a period of time, which may be very brief, the connection 210 manager attempts to reconnect to a network 708. The network 108 may be the most recently used network or may be a newly identified network. The connection may be dropped for a period of time. In one embodiment, a user may specify the duration that the user expects to be disconnected when the disconnect occurs. The persistence server 316 uses this information to determine how much data to cache during the period of disconnection.

The connection manager 210 or persistence server 316 then determines whether the download that was occurring before the disconnect should continue 710. For instance, the connection manager 210 may determine that the new connection is too slow to support the data download. The connection manager 210 may also look to the policies to determine what rules apply to the connection.

If the download, should continue, the connection manager 210 resumes the data transfer 712. The data transfer may then complete or may be subject to subsequent disconnects. If the new network is not suitable to support the download, or if the download is complete, the process ends 714.

For example, in one embodiment, a salesperson needs to download a large document containing a price list. The salesperson's computer is currently connected via a wide area network connection, which is relatively slow. The salesperson enters a coffee shop that the salesperson knows has a high speed WiFi connection.

When the client device 102 indicates that the WiFi connection is available, the user indicates that the client device 102 should change networks. The client device seamlessly

connects to the WiFi network and, based on rules established in the policies, begins downloading the document. If the user must leave the coffee shop before the download is complete, the connection manager 210 can signal the session persistence server 316 to pause the download until the user reenters the coffee shop or connects to another high-speed network.

In one embodiment, session persistence operates on the following process: when a disconnection event occurs, the connection manager 216 buffers application data coming to the client device 102, making applications "believe" that they are still connected. At the same time, session persistence server 216 buffers information on the server side, making the server 104 "believe" that it is still connected. Once a network connection has been reconnected, the connection manager 210 and session persistence server 316 empty the buffers that have built up on both sides.

One such embodiment implements a kernel mode driver at the NDIS layer in the Microsoft Protocol stack (roughly equivalent to layer 3 in the OSI model). This kernel mode driver is implemented as an "Intermediate Driver" on the Microsoft W2K/WXP operating systems. The driver acts as a single "virtual device" through which all network communications goes. This single device routes this traffic to the appropriate physical device (directed through a virtual device associated with a third-party VPN when appropriate), depending on the current physical connection.

In order to make application layer components believe that a network is still up and running, no "disconnect" signal is transmitted to the application layer components when a network interruption occurs. In this way, application layer components treat the connection as if it is simply slow.

The primary interface component between the client 102 and server 104 in such an embodiment is an indication that a client will be disconnecting for a long period of time, but wishes to persist the session over this extended time. In this case, the client 102 provides the user a means to enter the time that the system will be un-connected (say for the duration of a domestic flight), and the client notifies the server of the expected length of the disconnection event.

On the server 104, the session persistence server 316 functions as a proxy for connections from clients to network resources. Be those resources at the enterprise data center or public resources. The server implementation includes a similar intermediate driver architecture to that on the client, combined with application layer components to manage caching locations and recording for billing purposes. There may be cases where enterprises

wish caching to occur at the enterprise. In this case, the system allows for the cache to be on the other side of a static tunnel to the enterprise.

General

The foregoing description of the embodiments of the invention has been presented only for the purpose of illustration and description and is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Numerous modifications and adaptations thereof will be apparent to those skilled in the art without departing from the spirit and scope of the present invention.

That which is claimed:

1. A method comprising:

receiving a request to connect to a network, the request associated with a user;

determining a policy associated with the user;

identifying at least one available network connection;

determining at least one property of the at least one available network connection;

evaluating the property based at least in part on the policy; and

selecting the at least one available network connection based on the evaluation.

2. The method of claim 1, wherein the policy comprises a list of allowed connections.

3. The method of claim 1, wherein the policy comprises a list of disallowed connections.

4. The method of claim 1, wherein the property comprises a property selected from the group consisting of security, reliability, speed, and cost.

5. The method of claim 1, wherein the at least one property comprises a plurality of properties and further comprising applying a normalization algorithm to the plurality of properties.

6. The method of claim 1, wherein determining the policy comprises retrieving the policy from a central policy repository.

7. The method of claim 1, wherein the at least one available network connection comprises a public connection.

8. The method of claim 1, wherein the at least one available network connection comprises a private connection.

9. The method of claim 1, further comprising receiving a quality of service datum associated with the at least one available network connection.

10. The method of claim 1, wherein the at least one available network connection comprises a plurality of available network connections.

11. A method comprising:

receiving an indication that a new network connection is available for a client device associated with a user;

determining at least one first property associated with the new network connection;

determining at least one second property associated with an existing network connection;

determining a policy associated with the user;

evaluating the at least one first property based at least in part on the policy;

evaluating the at least one second property based at least in part on the policy;

disconnecting from the existing network connection; and

connecting to the new network connection.

12. The method of claim 11, further comprising signaling that the new network connection is available.

13. The method of claim 11, further comprising before disconnecting from the existing network connection, opening a data cache for buffering data during a disconnection.

14. The method of claim 13, further comprising after connecting to the new network connection:

receiving data from the data cache; and

closing the data cache.

15. The method of claim 13, further comprising receiving a measure for determining the size of the data cache.

16. The method of claim 15, wherein the measure comprises an estimated disconnection duration.

17. The method of claim 11, wherein the indication that a new network connection is available comprises a signal from a hardware device.

18. The method of claim 17, wherein the hardware device comprises an adapter selected from the group consisting of a WiFi adapter, a LAN adapter, a cellular adapter (WWAN), and a dial-up (WAN) adapter.

19. A computer-readable medium on which is encoded program code, the program code comprising:

program code for receiving a request to connect to a network, the request associated with a user;

program code for determining a policy associated with the user;

program code for identifying at least one available network connection;

a policy reader operable to determine a policy associated with a user;

a connection manager operable to:

receive a request to connect to a network, the request associated with a user;

identify at least one available network connection;

determine at least one property of the at least one available network connection;

evaluate the property based at least in part on the policy; and

select the at least one available network connection based on the evaluation.

27. The system of claim 26, further comprising a quality of service collector operable to receive a quality of service datum associated with the at least one available network connection.

28. A system comprising:

a policy reader operable to determine a policy associated with a user;

a connection manager operable to:

receive an indication that a new network connection is available;

determine at least one first property associated with the new network connection;

determine at least one second property associated with an existing network connection;

evaluate the at least one first property based at least in part on the policy;

evaluate the at least one second property based at least in part on the policy;

disconnect from the existing network connection; and

connect to the new network connection.

program code for determining at least one property of the at least one available network connection;

program code for evaluating the property based at least in part on the policy; and

program code for selecting the at least one available network connection based on the evaluation.

20. The computer-readable medium of claim 19, further comprising program code for receiving a quality of service datum associated with the at least one available network connection.

21. A computer-readable medium on which is encoded program code, the program code comprising:

program code for receiving an indication that a new network connection is available;

determining at least one first property associated with the new network connection;

determining at least one second property associated with an existing network connection;

determining a policy associated with a user;

evaluating the at least one first property based at least in part on the policy;

evaluating the at least one second property based at least in part on the policy;

disconnecting from the existing network connection; and

connecting to the new network connection.

22. The computer-readable medium of claim 21, further comprising signaling that the new network connection is available.

23. The computer-readable medium of claim 21, further comprising before disconnecting from the existing network connection, opening a data cache for buffering data during a disconnection.

24. The computer-readable medium of claim 23, further comprising after connecting to the new network connection:

receiving data from the data cache; and

closing the data cache.

25. The computer-readable medium of claim 23, further comprising receiving a measure for determining the size of the data cache.

26. A system comprising:

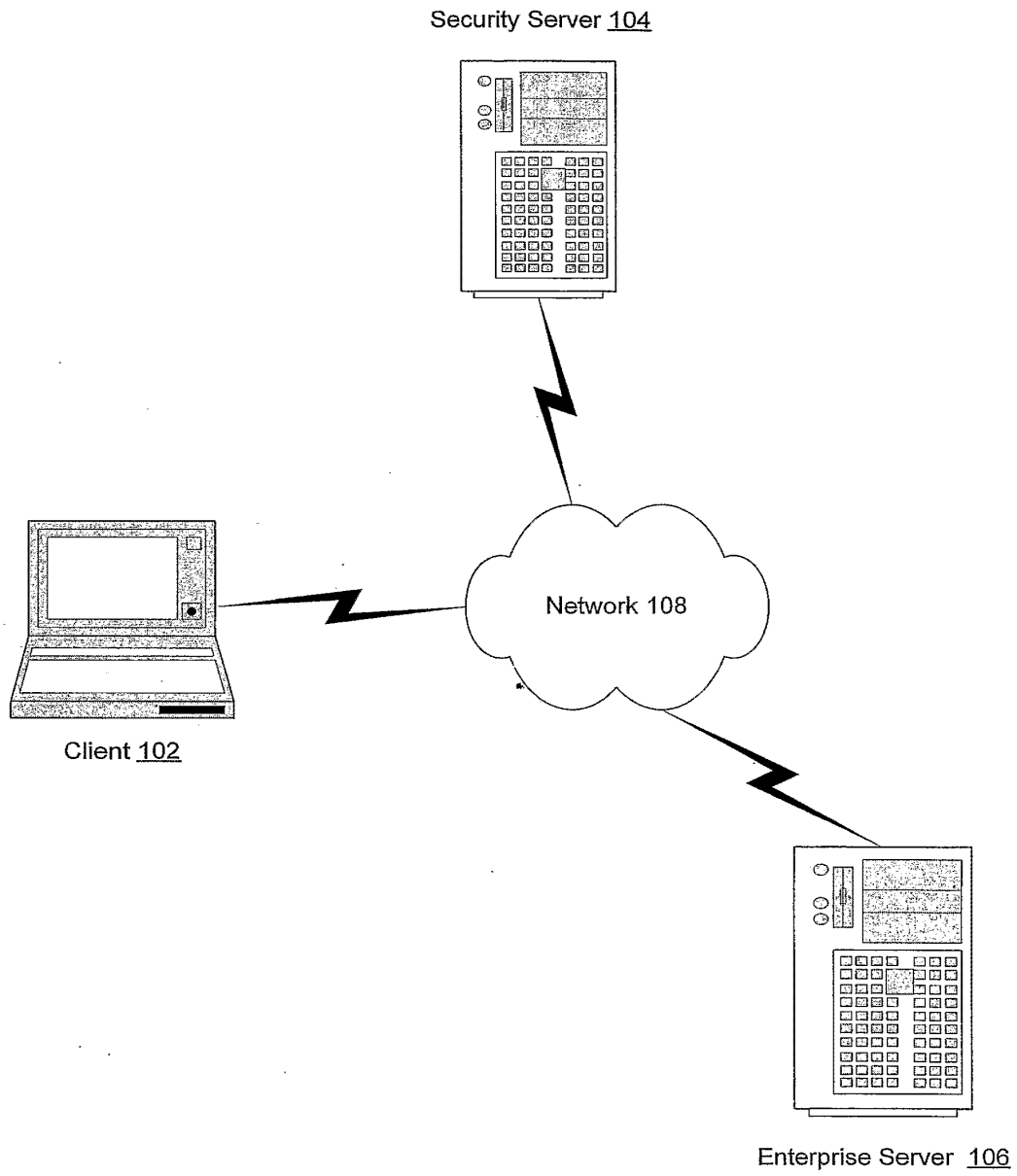

Security Server 104
Network 108
Client 102
Enterprise Server 106

Figure 1

Client 102

202 Client VPN
204 Secure Vault
206 Firewall
208 Antivirus
210 Connection Manager (Rules Processor)
212 QoS Collector
214 Session Statistics
216 Policy Reader
218 Client Security
220 User Interface
222 Security Agent
224 Out-of-Band Communication Receiver

Figure 2

3/7

Security Server 104

302 RADIUS Server (AAA)
304 LDAP
306 Session Manager
308 Real-time Monitor
310 Historical Monitor
312 Database
314 QoS Server
316 QoS Tools Engine
318 Portal Server

Figure 3

Enterprise Server 106

402 Policy Server
404 Acceleration Server
406 Vault Server
408 RADIUS Server
410 LDAP
412 OTP Server
414 Concentrator
416 Portal Server

Figure 4

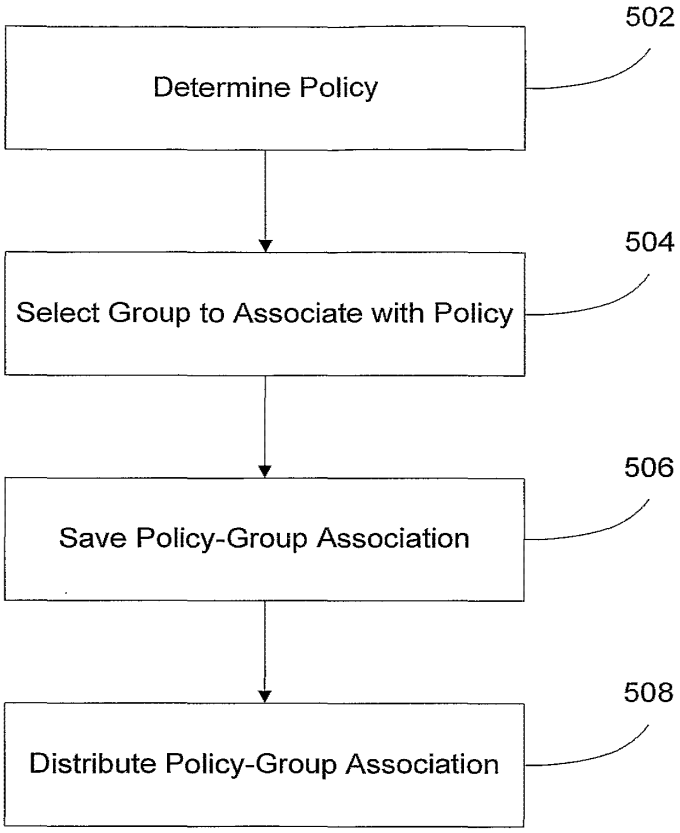

502
Determine Policy
504
Select Group to Associate with Policy
506
Save Policy-Group Association
508
Distribute Policy-Group Association

Figure 5

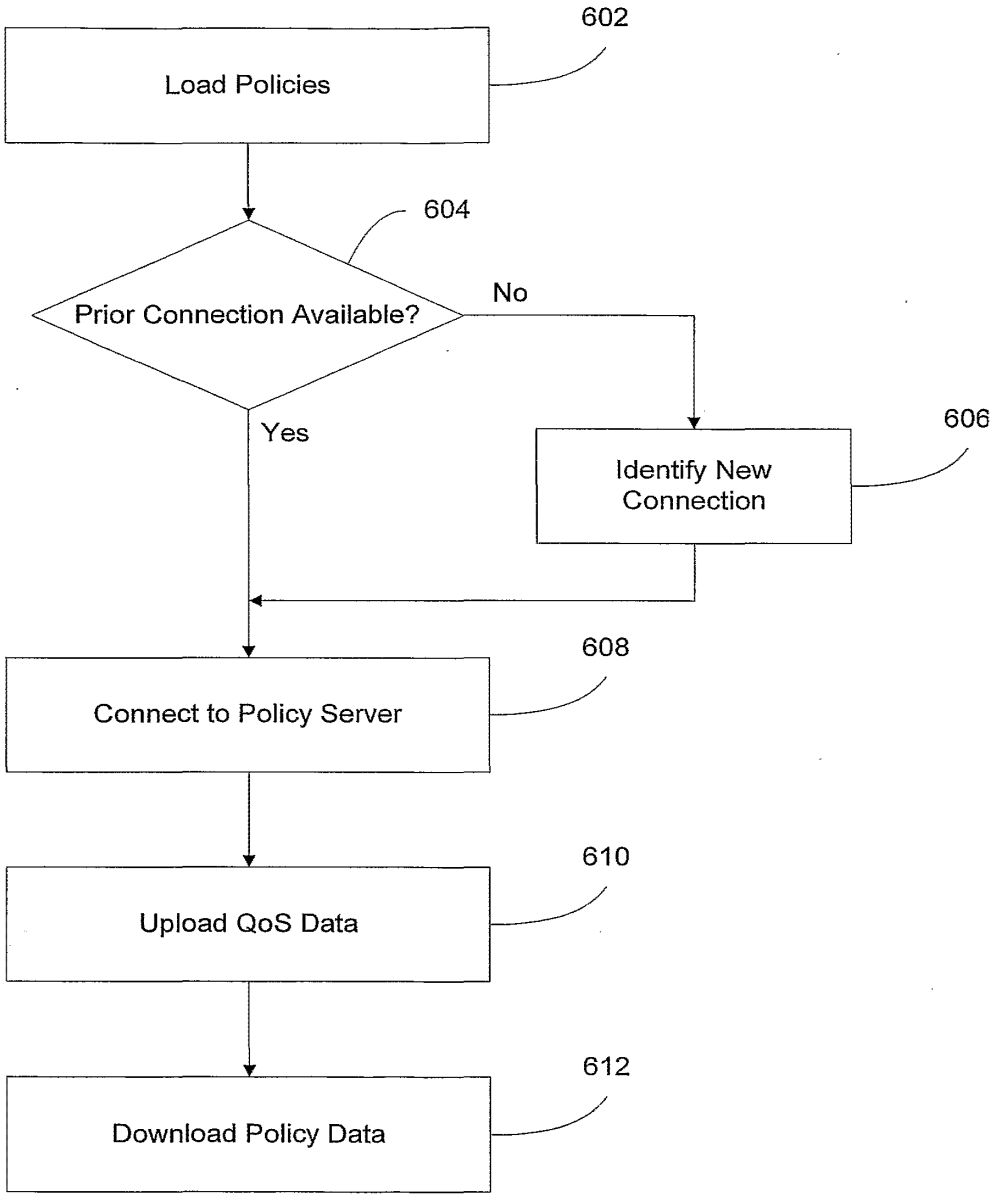

602
Load Policies
604
Prior Connection Available?
No
Yes
606
Identify New Connection
608
Connect to Policy Server
610
Upload QoS Data
612
Download Policy Data

Figure 6

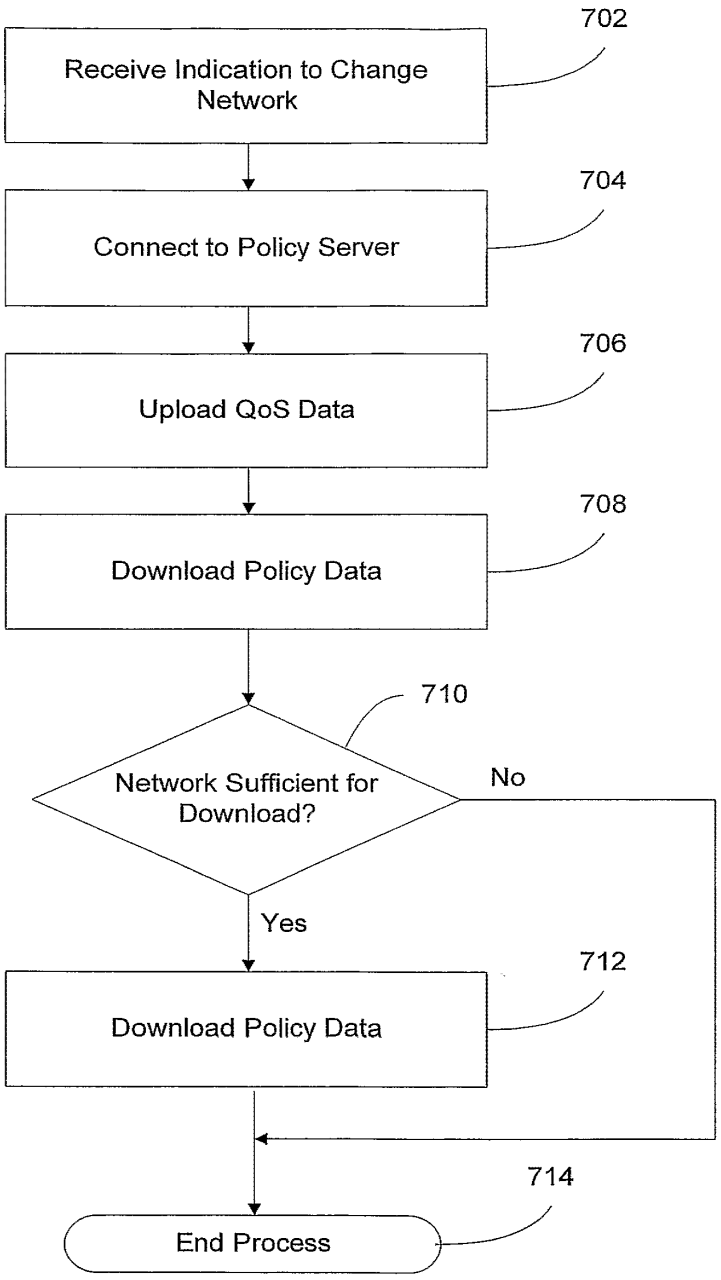

Receive Indication to Change Network
702
Connect to Policy Server
704
Upload QoS Data
706
Download Policy Data
708
Network Sufficient for Download?
710
No
Yes
Download Policy Data
712
End Process
714

Figure 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/022982

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F1/00

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)
IPC 7 H04L G06F

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 practical, search terms used)
EPO-Internal, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 03/073782 A (NOKIA CORPORATION; JOERESSEN, OLAF) 4 September 2003 (2003-09-04) abstract page 1, line 7 - page 2, line 31 page 3, line 6 - page 4, line 27 page 5, line 27 - page 8, line 24 -/--	1-28

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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 document 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	Date of mailing of the international search report
20 October 2005	27/10/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Kopp, K

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/022982

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02/23362 A (NETMOTION WIRELESS, INC; HANSON, AARON, D; STURNIOLO, EMIL, A; MENN, A) 21 March 2002 (2002-03-21) abstract page 1, line 5 - line 12 page 4, line 11 - line 22 page 5, line 10 - line 23 page 6, line 6 - line 21 page 7, line 21 - page 8, line 3 page 11, line 15 - page 14, line 17 page 15, line 18 - page 16, line 2 page 17, line 9 - line 10 page 18, line 23 - page 21, line 18 page 22, line 5 - line 15 page 23, line 12 - line 27 figure 1	1-28
X	US 2004/123150 A1 (WRIGHT MICHAEL ET AL) 24 June 2004 (2004-06-24) abstract figure 6a paragraph '0005! paragraph '0007! - paragraph '0009! paragraph '0012! paragraph '0028! paragraph '0040! - paragraph '0042! paragraph '0044! paragraph '0046! paragraph '0085! - paragraph '0086!	1-28
A	WO 02/077816 A (BOT, INC; USZOK, ANDRZEJ; KUNSTMAN, PAWEL) 3 October 2002 (2002-10-03) page 25, line 3 - line 12	2,3
A	US 5 748 084 A (ISIKOFF ET AL) 5 May 1998 (1998-05-05) abstract figures 3,4 column 1, line 4 - line 7 column 1, line 48 - column 3, line 4 column 3, line 46 - line 53 column 4, line 3 - line 33 column 4, line 62 - column 5, line 33 column 5, line 59 - column 6, line 15 column 6, line 31 - line 54 column 9, line 53 - column 10, line 31	1-28

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2005/022982

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 03073782 A	04-09-2003	AU 2002233595 A1	09-09-2003
		EP 1479257 A1	24-11-2004
		US 2005148359 A1	07-07-2005
WO 0223362 A	21-03-2002	CA 2421609 A1	21-03-2002
		EP 1364296 A1	26-11-2003
		JP 2004509539 T	25-03-2004
US 2004123150 A1	24-06-2004	US 2004123153 A1	24-06-2004
WO 02077816 A	03-10-2002	NONE	
US 5748084 A	05-05-1998	NONE	

Form PCT/ISA/210 (patent family annex) (January 2004)

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION JP2005339247

【課題】

[Problem] without entering a user ID and password automatically authenticates the user, and provides a two-way one-time ID authentication system that does not perform the authentication in the content server. Define the initial authentication code in accordance with the registration of the user ID that is defined in A URL of the content server and the content server, authentication key for the URL of the content server, user ID, and a two-way one-time ID authenticates the initial authentication code managed in association with the authentication server, and mobile terminal to perform to install the authentication key from the authentication server authentication server and the two-way one-time ID authentication, and a gateway server to the mobile terminal to access, the mobile terminal, gateway carries out bidirectional one-time ID authentication using the authentication key with the authentication server via the server, a bidirectional one-time ID authentication system requests a content to the content server via a gateway server when authentication is successful is there. .FIELD 6

Two-way one-time ID authentication system and authentication method

[0001]

[0001] The present invention relates to a bidirectional one-time authentication system and an authentication method for performing a bidirectional one-time ID authentication between the mobile terminal and the server

[0002]

[0002] The content server that provides e-commerce and financial transactions of the service is widely known via the Internet. As shown in FIG. 24, the user communicates over the Internet with the content server using the mobile device or computer or the like, actually the user ID and password, etc. in advance determined when using the service on the input to have authenticated, it may be utilized. In other words, the content server by using the user ID and password, and the like that has been input, take the integrity of the user information, to identify a user who comes to access, and to allow the request if the legitimate user. Patent 2003-1 62507

[0003]

[0003] However, the user ID and password, and the like guess by a third party, there is a fear that leakage, or are prying eyes, if there is such a thing, would also be available easily content server is a third party, there is a fear that is the illegal commerce and financial transactions. Further, the user information managed by the content server, in addition to such as a user ID and a password, for example, the user's address and phone number, E-mail address, date of birth, bank account number or credit used for settlement since even personal information number or the like are managed, the user ID and password, etc. to a third party would be known, there is a possibility that, also known these information at the same time. Therefore, the user has a problem that can not be utilized with confidence services such as e-commerce and financial transaction provided by the content server.

[0004]

[0004] paying attention to these problems, the present invention is, and automates the authentication of users without having to enter a user ID and password, and, two-way one-time ID authentication system and is not carried out by the content server the authentication and to provide an authentication method.

[0005]

[0005] According to a first aspect of the present invention defines an initial authentication code according to the registration of the user ID defined in the URL of the content server and the content server, URL of the content server, user ID, and an initial and the authentication server for managing the authentication code in association with the authentication key to perform a two-way one-time ID authentication, and a mobile terminal that performs the authentication server and the two-way one-time ID authentication to install the authentication key from the authentication server, the portable terminal and a gateway server for accessing said portable terminal, said carries out bidirectional one-time ID authentication by using the authentication key between the authentication server via the gateway server, if the authentication is successful a bidirectional one-time ID authentication system, wherein the request content to the content server via the gateway server to.

[0006]

[0006] The invention described in claim 2 of the present invention, a bidirectional one-time ID authentication system according to claim 1 , wherein the authentication server, one-time ID authentication of the mobile terminal is successful in the authentication server the generates a session ID associated with the authentication key sent to the mobile terminal via the gateway server in the case, the session ID sent via the gateway server together with the content request from said portable terminal when confirming reads the URL and the user ID of the content server sends the gateway server, the gateway server sends the content request to the URL and the user ID and synthesized and the content server of the content server, the content sending of content of a server to the portable terminal via the gateway server, it said mobile devices, characterized by acquiring and displaying the content.

[0007]

[0007] The invention described in claim 3 of the present invention, a bidirectional one-time ID authentication system according to claim 1 or 2, to perform the bidirectional one-time ID authentication by using the authentication key, the authentication via the gateway server if the server one-time ID has been successfully authenticated by requesting the content to the content server, to acquire the content, that you previously installed a browser-type application program to perform the series of processes the features.

[0008]

[0008] The invention described in claim 4 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 3, wherein the application program and the authentication key is installed said portable terminal and activating the application program, carries out bidirectional one-time ID authentication by using the authentication key between the authentication server via the gateway server, the via the gateway server when authentication is successful acquired by requesting the content to the content server, and performing automatically the operation of displaying on said portable terminal.

[0009]

[0009] The invention described in claim 5 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 4, wherein the session ID has a session time, the authentication server the session and features that you disable the session ID when the time has passed.

[0010]

[0010] The invention described in claim 6 of the present invention, a bidirectional one-time ID authentication system according to claim 5, when the session time is the session ID was disabled too, automatically and performing re-authentication by the bi-directional one-time ID authentication.

[0011]

[0011] The invention described in claim 7 of the present invention defines an initial authentication code according to the registration of the user ID defined in the URL of the content server and the content server, URL of the content server, user ID, and an initial and the authentication server for managing the authentication code in association with the authentication key to perform a two-way one-time ID authentication, and a mobile terminal that performs the authentication server and the two-way one-time ID authentication to install the authentication key from the authentication server, the portable terminal and a gateway server for accessing said

portable terminal performs bi-directional one-time ID authentication by using the authentication key between the authentication server via the gateway server, the authentication server, authentication generates the session ID and the token associated with the authentication key on success sends the token to the mobile terminal via the gateway server, differs from the mobile terminal to the token from the mobile terminal type in the terminal, the authentication server,Reads the URL and the user ID of the content server when confirming that the session time of the session ID associated with the token which is sent along with the content request via the gateway server from said different terminal is not passed said along with the session ID is sent to the gateway server, the gateway server sends to the content server and combined with the URL and the user ID of the content server the content request, the content of the content server via the gateway server on sent to different terminals and the mobile terminal together with the session ID, the registered in the Cookie the session ID as well as retrieve and display the content in the different terminals and the mobile terminal, since it was registered in the Cookie a bidirectional one-time ID authentication system characterized in that requesting content using the session ID.

[001 2]

[001 2] The invention described in claim 8 of the present invention, a bidirectional one-time ID authentication system according to claim 7, to perform the bidirectional one-time ID authentication by using the authentication key, bidirectional one-time to acquire the token when the ID authentication is successful, characterized in that to have been installed on the token-type application program to perform the series of processes.

[001 3]

[001 3] The invention described in claim 9 of the present invention, a bidirectional one-time ID authentication system according to claim 7 or 8, wherein the session ID has a session time, the authentication server only said session time disable the session ID when the said case of the session ID in the authentication server is disabled, characterized in that said from the portable terminal activates the application program acquires the token.

[001 4]

The invention according to claim 1 0 of the [001 4] present invention, a bidirectional one-time ID

authentication system according to any one of claims 1 to 9, wherein the authentication key, to activate the application program, said portable terminal the case where the initial authentication code and the required received in by inputting the download destination address of the authentication key, characterized in that it is installed.

[001 5]

[001 5] The invention described in Claim 1 1 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 9, wherein the authentication key, the download destination of the authentication key have been described characterized in that it is installed by clicking on the download destination e-mail to receive the mobile terminal.

[001 6]

[001 6] The invention described in Claim 1 2 of the present invention, characterized by a bidirectional one-time ID authentication system according to any one of claims 1 to 1 1 , for use as a model that can identify the user in the authentication server to.

[001 7]

[001 7] The invention described in Claim 1 3 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 1 1 , for use as a model that can guarantee the anonymity of the user at the authentication server it features a.

[001 8]

[001 8] The invention described in Claim 1 4 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 1 3, can disable the authentication key if you lose the portable terminal characterized in that it comprises a device separate.

[001 9]

[001 9] The invention described in Claim 1 5 of the present invention, a bidirectional one-time ID authentication system according to any one of claims 1 to 1 4, wherein the content server and the gateway server is connected via the Internet If you are, and performing a bidirectional one-time ID authentication between the two servers.

[0020]

[0020] The invention described in Claim 1 6 of the present invention is to define a user ID, the user's address, phone number, and E-mail address, date of birth, bank account number or credit card number used for payment or the like both the content server for managing personal information, and defines the initial authentication code according to the registration of the user ID defined in the URL and the content server of the content servers, URL of the content server, user ID, and the initial authentication code and the authentication server to manage in association with the authentication key for the direction one-time ID authentication, and a mobile terminal that performs the authentication server and the two-way one-time ID authentication to install the authentication key from the authentication server, the portable terminal and a gateway server for accessing said portable terminal performs bi-directional one-time ID authentication by using the authentication key between the authentication server via the gateway server, the gateway server when authentication is successful a content providing system characterized in that requests the content to the content server via.

[0021]

[0021] The invention described in Claim 1 7 of the present invention is to define a user ID, the user's address, phone number, and E-mail address, date of birth, bank account number or credit card number used for payment or the like both the content server for managing personal information, and defines the initial authentication code according to the registration of the user ID defined in the URL and the content server of the content servers, URL of the content server, user ID, and the initial authentication code and the authentication server to manage in association with the authentication key for the direction one-time ID authentication, and a mobile terminal that performs the authentication server and the two-way one-time ID authentication to install the authentication key from the authentication server, the portable terminal and a gateway server for accessing said portable terminal performs bi-directional one-time ID authentication by using the authentication key between the authentication server via the gateway server, the authentication server, authentication was successful the generates a session ID and a token associated with the authentication key sends the token to the mobile terminal via the gateway

server in the case, the token from the mobile terminal type in different terminals and the mobile terminal ,The authentication server reads the URL and the user ID of the content server when confirming that the session time of the session ID associated with the token which is sent along with the content request via the gateway server is not only the feed along with the session ID to the gateway server, the gateway server sends to the content server and combined with the URL and the user ID of the content server the content request, the content of the content server via the gateway server said along with the session ID sent to a different terminal and the mobile terminal, the registered in the Cookie the session ID as well as retrieve and display the content in the different terminals and the mobile terminal, since it was registered in the Cookie session a content providing system characterized in that to request the content using the ID.

[0022]

[0022] The invention described in Claim 1 8 of the present invention, in the authentication server, and defines the initial authentication code according to the registration of the user ID defined in the URL of the content server and the content server, URL of the content server, the user ID, and a step of initial management of the authentication code in association with the authentication key to perform a two-way one-time ID authentication, a step of the mobile terminal to install the authentication key from the authentication server, the portable terminal is the gateway server when the step of performing bidirectional one-time ID authentication, where the one-time ID authentication of the authentication server in the mobile terminal is successful by using the authentication key between the authentication server via said portable terminal the gateway a bidirectional one-time ID authentication method characterized by a step of requesting the content to the content server via the server.

[0023]

[0023] The invention described in Claim 1 9 of the present invention, the authentication if a bidirectional one-time ID authentication method according to claim 1 8, in the authentication server, the one-time ID authentication of the mobile terminal is successful generating a session ID associated with the key, the step of sending to said mobile terminal to the session ID via said gateway server, sent through the gateway server together with the content request from said portable terminal a step of reading the URL and the user ID of the content server when confirming the session ID, a step of sending to the content server the content request at the gateway server synthesizes the URL and the user ID of the content server, a step of sending to said mobile terminal a content of the content server via the gateway server, said portable terminal; and a step of acquiring and displaying the content.

[0024]

[0024] The invention described in Claim 20 of the present invention, in the authentication server, and defines the initial authentication code according to the registration of the user ID defined in the URL of the content server and the content server, URL of the content server, the user ID, and a step of initial management of the authentication code in association with the authentication key to perform a two-way one-time ID authentication, a step of the mobile terminal to install the authentication key from the authentication server, the portable terminal is the gateway server associated with the authentication key if the the step of performing a bidirectional one-time ID authentication using the authentication key, the one-time ID authentication of the mobile terminal in the authentication server is successful between the authentication server via having the steps of generating a session ID and token, the step of sending the token to the mobile terminal via the gateway server, and a step of inputting said token in said mobile terminal different from the terminal and the mobile terminal was two-way one-time ID authentication method according to claim.

[0025]

[0025] The invention described in Claim 21 of the present invention, a bidirectional one-time ID authentication method according to claim 20, via the gateway server from a different terminal from said mobile terminal said token is input a step together with the content request and sends the token, the reading of the URL and the user ID of the content server when confirming that the session time of the session ID associated with the sent come token is not passed session through a step of sending to the gateway server along with ID, a step of sending to the content server the gateway server synthesizes the URL and the user ID of the content server of the content request, the gateway server for the content on the content server and a step to send to different terminals and the mobile terminal together with the session ID on, said the mobile terminal and the step of registering to Cookie the session ID as well as retrieve and display the content in a different terminal, after that, the characterized by a step of requesting the content using the session ID registered in the cookie.

[0026]

According to [0026] the present invention, it is possible to automatically perform authentication

without entering a user ID and password, not the user ID and password, and the like are known to a third party, the user content server There can be used with confidence to e-commerce and service of financial transactions, etc. to provide.

[0027]

[0027] Further, according to the present invention, authentication and access to the content server when starting the application program downloaded to the portable terminal is automatically performed.

[0028]

[0028] Further, according to the present invention, since no authentication by the content server, the content server need only provide information, it is possible to save time and cost of the authentication system construction.

[0029]

[0029] Hereinafter will be described the best mode for carrying out the present invention, but the present invention is not limited to the scope of the following examples, as long as without departing from the scope thereof, appropriately changed and those that can be implemented. First, the one-time ID and a two-way one-time ID authentication, as well as the application program and the authentication key will be explained.

[0030]

[0030] The one-time ID and a two-way one-time ID authentication will be described. One-time ID is identification information that can be used only once in the authentication, is generated based on the common key and the authentication data between devices or between applications. Authentication by an one-time ID, is to ensure the effect of anonymity that a third party while to become able to identify the sender, recipient, can grasp the one-time ID as identification information if a legitimate sender, recipient together with the resulting, for the one-time ID is changed each time the communication between sender and receiver is carried out, the effect is

obtained that a third party can not be predicted for the next one-time ID. The bidirectional one-time ID authentication, in order to authenticate with each other using the one-time ID, it is possible to prevent the spoofing each other.

[0031]

[0031] In the P-SIGMA is the key exchange and authentication method using the one-time ID for example, the key exchange and authentication in the procedure as shown in FIG. 1 have been made. First of all, the client is, proposal of SA (Security Association), to send a random number Rc, DH (Diffie-Hellman) public value gx, OID (the one-time ID) to the server. Note that the proposal of the SA, contains proposals on parameters used encryption algorithm and authentication method, the key exchange.

[0032]

[0032] Next, the server, to identify the client from the received OID, in the case that can not be identified, deny the communication. If it can be identified, send acceptance was SA, random number Rs, DH public value gy, HASHs, IDs that were encrypted with the session key e (the server ID) to the client. It should be noted that the session key e is a pre-shared key, a random number Rs, the function value of a keyed hash function to the random number Rc and DH common key gxy the argument, HASHs is, pre-shared key, a random number Rs, random number Rc, DH public value gx, which is a function value of the pseudo-random number function which takes a gy and IDs.

[0033]

[0033] Next, the client, to verify the HASHs received, to confirm the validity of the server on the basis of this HASHs. If it is correct HASHs, HASHc, send IDc encrypted with the session key e the (client ID) to the server. Here, HASHc is a pre-shared key, a random number Rs, random number Rc, DH public value gx, function value of the pseudo-random number function which takes a gy and IDc. Subsequently, the server to verify the HASHc received, to confirm the validity of the client on the basis of this HASHc. If it is correct HASHc, it terminates the protocol.

[0034]

[0034] In the P-SIGMA, OID (onetime ID) is defined as follows.

[0035]

[0035] OID1 = prf (K, 1) OID2 = prf (K, 2) ... OIDn = prf (K, n)

[0036]

[0036] In this defining expression, OIDn the one-time ID to be used when the n-th SA establishment, prf pseudo random function, K is a pre-shared key or a value generated from the pre-shared key.

[0037]

[0037] Therefore, according to the P-SIGMA, by introducing an OID, while the third party can not be identified the sender-recipient identifying OID if legitimate sender-recipient together effect is obtained such can be grasped as the information, every time the communication between the client and the server is performed (i.e., generation or each update of the SA) for OID to be changed, by a third party to predict the next OID effect can be obtained, such as can not.

[0038]

[0038] some of which was used as the variable shared key arguments that vary from session to this other or variable shared key and the one-time ID the function value of the hash function to a communication order as the argument, (SIGNAL) (Fig. 2, see Fig. 3). Thus, for example, it is variable shared key leaks to a third party, since the variable shared key is to be changed for each session, leaking variable shared key one-time non onetime ID generated using not be able to predict the ID. In other words, wiretapping is possible to generate a superior one-time ID to the difficult and safety. Further, by using the one-time ID (SIGNAL), since to carry out the authentication between the client and the server, while the third party can not be identified the sender-recipient, legitimate senders, recipients it is possible to grasp the one-time ID as

identification information, if any. Therefore, DoS attacks and spoofing resistance can be enhanced with respect to such, even under open network environment, aims to protect the ID information, it is possible to improve the security of communication. Further, it allows remote access, it is also possible to enhance the convenience.

[0039]

[0039] followed by the application program will be described. Bidirectional one-time ID authentication system of the present invention can be utilized by installing the application program to the mobile terminal. Then, by activating an application program installed, automatically carries out bidirectional one-time ID authentication with the authentication server, information can be obtained from the content server. This section describes how to install the application program, a description of the specific operation will be described later.

[0040]

To install the [0040] application program, there is the following method. However, not the method of installation is not limited to this. (1) you will receive an e-mail the download destination has been described of the mobile terminal to the authentication application software, by clicking on the download destination, to download and install the application program from the download site. (2) is notified of the download site of the application program in the mail or the like, the user has to enter the download site, download and install the application program from the download site. (3) software application program is sent by mail, etc., to install using it.

[0041]

[0041] The authentication key is a shared key used in performing the bidirectional one-time ID authentication generates a one-time ID. When performing bidirectional one-time ID authentication can be utilized by installing the pre-authentication key. How to install the authentication key will be explained. The user's address in the content server, phone number, E-mail address, date of birth, and the user information such as user ID is registered, by the operation or the like of an operator in the authentication server, defined in the URL of the content server and the content server It has been registered user ID, and this in accordance to register to define the initial authentication code associated with the authentication key in the corresponding table. When the download site or software application programs by mail or the

like is sent, the initial authentication code is also enclosed. It should be noted that, if necessary, have also been enclosed download destination site address of the authentication key. When to start the installed application program, if the initial authentication code and the necessary will be prompted to request the input of the download destination site address of the authentication key, and the client to enter the site address of the initial authentication code and download destination , the initial authentication code to request the download of the authentication key is sent to the authentication server through a gateway server. On the other hand, if the e-mail download destination application program is sent, the download location and the initial authentication code of the authentication key is described. User by entering the download destination and the initial authentication code of the authentication key, the initial authentication code to request the download of the authentication key is sent to the authentication server through a gateway server. It is to be noted that, by the download destination of the authentication key is to click on it, the initial authentication code also may have been to be sent together, the user by entering or click on the download destination of the authentication key, automatically initial authentication code may request a download of the authentication key is sent to the authentication server via the gateway server.

[0042]

[0042] Then, the authentication application program was started entering the download destination site address of the initial authentication code and authentication key, or by clicking the authentication key download destination, authentication server, which has received the initial authentication code, corresponding to the initial authentication code the authentication key is attached read from the correspondence table, and sends the authentication key to the user of the portable terminal that had download request via the gateway server. Authentication key on a mobile device is installed. Although there is no intended for authentication key is variable, in the present system can also be used with any authentication key.

[0043]

[0043] The above authentication application program and the authentication key by be installed in the portable terminal, when activating an application program on the mobile terminal, automatically an authentication key with the authentication server via the gateway server using carries out bidirectional one-time ID authentication can be acquired by requesting the content to the content server via a gateway server when authentication is successful.

[0044]

[0044] The following describes the first embodiment of the present invention with reference to the drawings. In this embodiment, described browser type bidirectional one-time ID authentication system. As shown in FIGS. 4 to 7, browser type bidirectional one-time ID authentication system includes a portable terminal, comprising an authentication server and a gateway server, mobile device, among via the gateway server and the authentication server carries out bidirectional one-time ID authentication using the authentication key to obtain the session ID if the authentication is successful, is a system for requesting the content to the content server via the gateway server.

[0045]

[0045] Here, the session ID will be explained. Session ID, assigned a unique value in the authentication server, an identifier associated with the authentication key. If the bidirectional one-time ID authentication in the authentication server is successful, thereafter, it adds the session ID when the access request from the mobile terminal to the content server, to authenticate the access to the content server to the authentication server by the session ID We have to get so. The user need not be aware of the addition of session ID, the application is programmed to automatically adds the session ID.

[0046]

[0046] That is, in the present system, performing the gateway server and an authentication server for authenticating the user, are separated and a content server that provides the service content, the portable terminal and the content server to communicate directly and authentication not.

[0047]

[0047] Each of the components will be described below. As described above, the mobile terminal be installed an authentication key and the application program. Here, it is assumed that installing a browser type application program. The mobile terminal is a terminal to access only to the gateway server. In the mobile terminal, it is a mobile phone or PDA (Personal Digital (Data)

Assistants) and the like. Authentication server, the operation or the like of the operator, and registers the URL and the user ID defined by the content server of the content server and the server to be registered in the correspondence table in association with this in accordance defines the initial authentication code authentication key . Also, generating an authentication server performs the two-way one-time ID authentication using the authentication key between the mobile terminal via the gateway server, the session ID if the one-time ID authentication of the mobile terminal is successful in the authentication server to.

[0048]

[0048] Session ID generated in the authentication server is managed by the correspondence table in association with the authentication key. That is, the session ID is therefore associated with the authentication key can be associated also with the content server URL and the user ID associated with the authentication key. Also, the session ID generated is sent together with the one-time ID to the mobile terminal via the gateway server. The authentication server may When confirming the session ID sent via the gateway server from the mobile terminal, reading the content server URL and the user ID associated with the session ID. Gateway server, the communication between the mobile terminal and the authentication server, which controls the communication between the content server and the mobile terminal, in the present system, a mobile terminal, the authentication server, and content server, always via a gateway server to communicate on. Content server is a server that provides services such as e-commerce and financial transactions. The content server, the user ID of the user to use the server is defined, address and phone number, E-mail address, date of birth, personal information such as bank account number or credit card number to be used in the settlement is registered It is managed. This system, by activating a browser-type application program on the mobile device, automatically authentication is performed, it is possible to acquire the contents on the content server.

[0049]

[0049] Hereinafter, with reference to FIGS. 1 0 to 1 3, the operation of the program when starting the installed browser application program of the mobile terminal. When you start the application program on the mobile terminal, it is determined whether or not the beginning to have obtained the authentication key. If the authentication key is not, because you must install the authentication key, authentication key download operation moved to the (preparatory stage), if necessary and the initial authentication code as described above is input the download destination address of the authentication key or click the authentication key download

destination, be installed on the mobile terminal (see Figure 1 0). If the authentication key is acquired proceeds to operation of generating the one-time ID using the authentication key (step 1).

[0050]

[0050] Hereinafter, the operation of step 1 will be described with reference to FIG. When you generate a one-time ID using the authentication key, the mobile terminal sends a one-time ID for mobile terminal authentication to the gateway server, gateway server sends the one-time ID to the authentication server. An authentication server using the authentication key is managed by the correspondence table, authenticates the one-time ID sent from the mobile terminal, generates a session ID if the authentication is successful. Then, the session ID generated is managed by the correspondence table in association with the authentication key in the authentication server. On the other hand, when the mobile terminal authentication is performed by the authentication server, one-time ID for another authentication server authentication with the one-time ID is generated by the authentication server. The authentication server sends the generated one-time ID to the gateway server along with the session ID. In addition, the session ID has a session time, the authentication server and measure the that time and at the same time to generate a session ID. Then, when the session time has passed, it is programmed to disable the session ID. When the gateway server receives the one-time ID and session ID from the authentication server, send them to the mobile terminal. The mobile terminal performs authentication of the authentication server in the one-time ID sent from the authentication server via the gateway server, to acquire the session ID if the authentication is successful. When you get the session ID on a mobile terminal moves to the operation for requesting the content to the content server (step 2).

[0051]

[0051] Hereinafter, the operation in step 2 will be described with reference to FIG. And to get the session ID on a mobile terminal on a mobile terminal to generate an HTTP packet to request the content. The mobile terminal is sent to the gateway server with the session ID of the HTTP packet, the gateway server while sending a session ID to the authentication server, once to hold the HTTP packet. Get the session ID sent from the gateway server in the authentication server, to determine whether the session ID is managed by the correspondence table, the correspondence to the session ID if there is a session ID in the correspondence table is reading the content server URL and user ID are. That is, if it is possible to read the session ID in the session time, it is possible to read the content server URL and the user ID, to be able to read the session ID in the session time, there is no session ID corresponding to the correspondence table so, it is impossible

to read the content server URL and the user ID. If the session ID corresponding to the correspondence table is not present, the authentication server notifies the effect that it is impossible to obtain the content (NG) to the gateway server, the gateway server also notifies the mobile terminal. A mobile terminal which is notified to that effect, as shown in FIG. 1 3, and proceeds to automatically re-operation of generating the one-time ID using the authentication key (step 1). On the other hand, if there is a session ID corresponding to the correspondence table, the authentication server reads the content server URL and the user ID, and sends them to the gateway server. In addition, at that time, to reset the session had been measured in the authentication server time, measure the re-session time. Thus, when transmitted again through the gateway server with the same session ID from the portable terminal, if it is possible to read the session ID in the session time, it is possible to read the content server URL and the user ID.

[0052]

[0052] Gateway server that has received the contents server URL and the user ID is combined with HTTP packet requesting content that is temporarily held, and sends it to the content server. Content server acquires the user ID, performs authentication of a user from among a plurality of users that are managed by the content server by using this, the content subjected to electronic transactions such as electronic commerce and financial transaction based on the HTTP packet it can be obtained. The content server sends the acquired content to the gateway server, the gateway server sends it to the portable terminal. Content acquired by the mobile terminal can be displayed using the browser on your mobile device.

[0053]

[0053] in the browser type bidirectional one-time ID authentication system of the present embodiment, only to start the installed application program on the mobile device, without having to enter a user ID and password, and the like automatically users it is possible to perform authentication. Accordingly, since no personal information of the user ID and password, etc. to a third party it is known, the user can use it at ease services such as e-commerce and financial transaction provided by the content server.

[0054]

[0054] In addition, to have a session time in the session ID to receive when the two-way one-time

ID authentication has been, during the session time of the session ID is valid, again, may not be a two-way one-time ID authentication so, it is possible to reduce the communication time and the packet between the mobile terminal and the server.

[0055]

[0055] Hereinafter, a description will be given of a second embodiment of the present invention with reference to the drawings. In this embodiment, described token type bidirectional one-time ID authentication system. As shown in FIGS. 8 and 9, the token type bidirectional one-time ID authentication system includes a portable terminal, a personal computer, an authentication server, a gateway server, a mobile terminal, the authentication server via a gateway server It carries out bidirectional one-time ID authentication using the authentication key between, certified is associated with the session ID on success token, the token manual input, infrared communication, serial cable, the IC card , a memory card, using Bluetooth, and a means such as a USB cable type to the personal computer, is a system for requesting the content to the content server via the gateway server from the personal computer by using the token.

[0056]

[0056] Here, the token will be explained. Token is generated when the bidirectional one-time ID authentication is successful, it assigns a unique value in the authentication server, an identifier associated with the authentication key and the session ID. Tokens in the case of a content request from a terminal other than the portable terminal, an identifier necessary for associating the session ID generated in the authentication server. It should be noted that, if you want to manually enter the token to the terminal other than the mobile terminal uses a string that can be recognized by the user.

[0057]

[0057] That is, in this system, obtains the token by performing bidirectional one-time ID authentication between the portable terminal and the authentication server via the gateway server, a terminal, such as a different PC from the the token portable terminal Fill in a system that requires the content to the content server from the terminal such as a personal computer via a gateway server. Incidentally, the gateway server and an authentication server which authenticates a user in the system, which separates the content server that provides the service

content, the portable terminal or terminal such as a personal computer and the content server to communicate directly and authentication do not go.

[0058]

[0058] Each of the components will be described below. As described above, the mobile terminal be installed an authentication key and the application program. Here, it is assumed that installing the token type application program. The mobile terminal is a terminal to access only to the gateway server. In the mobile terminal, it is a mobile phone or PDA (Personal Digital (Data) Assistants) and the like. Authentication server, the operation or the like of the operator, and registers the URL and the user ID defined by the content server of the content server and the server to be registered in the correspondence table in association with this in accordance defines the initial authentication code authentication key . The authentication server performs the two-way one-time ID authentication using the authentication key between the mobile terminal via the gateway server, the session ID and token when the one-time ID authentication of the mobile terminal is successful in the authentication server to generate. Session ID and token generated in the authentication server is managed by the correspondence table in association with the authentication key. That is, the session ID and token are therefore associated with the authentication key can be associated also with the content server URL and the user ID associated with the authentication key. The generated token is sent with the authentication onetime ID of the authentication server to the mobile terminal via the gateway server. The token is inputted from the portable terminal to a terminal such as a personal computer, the authentication server, the session ID when confirming the token transmitted from the terminal such as a personal computer via a gateway server, associated with the token, the content it can be read server URL and the user ID. The gateway server, the communication between the mobile terminal and the authentication server, which controls the communication between the content server and the portable terminal, in this system, a portable device or computer, the authentication server, and content server, always gateway server communicate over. Content server is a server that provides services such as e-commerce and financial transactions. The content server, the user ID of the user to use the server is defined, address and phone number, E-mail address, date of birth, personal information such as bank account number or credit card number to be used in the settlement is registered It is managed. This system, by activating a token type application program on the mobile terminal, by obtains the token, and inputs the token to the computer, automatically authentication is performed, to obtain the contents on the content server can.

[0059]

[0059] In the following, with reference to FIGS. 1 4 to 1 7, for explaining the operation of the program when you start the installation token type application program of the mobile terminal. First, as shown in FIG. 1 4, when the access from the personal computer to the gateway server, the gateway server input token is requested to the personal computer. If the token be entered in the computer I do not know, to start the installed token type application program of the mobile terminal, move the operation to get the token (step 1). On the other hand, if the token to enter know, the process proceeds to an operation to request the content by entering the token on a personal computer to the content server (step 2).

[0060]

[0060] When you start the application program on the mobile terminal, it is determined whether or not the beginning to have obtained the authentication key. If the authentication key is not, because you must install the authentication key, authentication key download operation moved to the (preparatory stage), the initial authentication code and if necessary input or authentication key download download destination address of the authentication key click on the above, it is installed on the mobile terminal (see Figure 1 0). If the authentication key is acquired proceeds to operation of generating the one-time ID using the authentication key (see Figure 1 4).

[0061]

[0061] Hereinafter, the operation of step 1 will be described with reference to FIG 1 4. When you generate a one-time ID using the authentication key, the mobile terminal sends a one-time ID to the gateway server, gateway server sends the one-time ID to the authentication server. An authentication server using the authentication key is managed by the correspondence table, it authenticates the one-time ID sent from the mobile terminal, generates a session ID and token when the authentication is successful. Then, the session ID and token generated is managed by the correspondence table in association with the authentication key in the authentication server. On the other hand, when the mobile terminal authentication is performed by the authentication server, one-time ID for another authentication server authentication with the one-time ID is generated by the authentication server. The authentication server sends the generated one-time ID together with the gateway server token. In addition, the session ID has a session time, the authentication server and measure the that time and at the same time to generate a session ID. Then, when the session time has passed, it is programmed to disable the session ID. When the gateway server receives the one-time ID and the token from the authentication server, send them

to the mobile terminal. The mobile terminal performs authentication of the authentication server in the one-time ID sent from the authentication server via the gateway server obtains the token when the authentication is successful. By acquiring the token on a mobile terminal, and then proceeds to an operation that requires the content to the content server by entering the token on a personal computer (step 2)

[0062]

[0062] Hereinafter, the operation in step 2 will be described with reference to FIG. Enter the token on a PC, it is and is sent to the gateway server, the gateway server HTTP packet to request the content is sent as well. Gateway server while sending a token to the authentication server, once to hold the HTTP packet. Get the token authentication server sent from the gateway server, a session ID associated with the token, it is determined whether or not managed by the correspondence table, if there is a session ID in the correspondence table is read the content server URL and user ID is associated with the session ID. That is, if it is possible to read the session ID associated with the session time, it is possible to read the content server URL and the user ID, to be able to read the session ID in the session time, corresponding to the correspondence table because the session ID does not exist, it is impossible to read the content server URL and the user ID. If the session ID corresponding to the correspondence table is not present, the authentication server notifies the effect that it is impossible to obtain the content (NG) to the gateway server, the gateway server also notifies the PC. User who has been notified to that effect, as shown in FIG. 1 7, again manually, in order to obtain a token, to activate the token type application program on the portable terminal to acquire the token. On the other hand, if there is a session ID corresponding to the correspondence table, the authentication server reads the session ID, the content server URL and the user ID, and sends them to the gateway server. In addition, at that time, to reset the session had been measured in the authentication server time, measure the re-session time.

[0063]

[0063] Gateway server that has received the contents server URL and the user ID is combined with HTTP packet requesting content that is temporarily held, and sends it to the content server. Content server acquires the user ID, performs authentication of a user from among a plurality of users that are managed by the content server by using this, the content subjected to electronic transactions such as electronic commerce and financial transaction based on the HTTP packet it can be obtained. Content server sends the acquired content to the gateway server, gateway server and sends it to the personal computer. It displayed using a browser on your computer the

content that you have acquired a personal computer.

[0064]

[0064] In addition, the gateway server sends a session ID obtained by reading by using the token in the authentication server to the PC, the PC is registering the Cookie of the session ID on a personal computer. Thus, as shown in FIG. 1 6, and requests the content from the PC using the session ID registered in the Cookie from the next time. Then, the PC sends the session ID to the authentication server via the gateway server, the authentication server if it is possible to read the session ID, can be read out content server URL and the user ID, it is possible to acquire the content.

[0065]

[0065] In the bidirectional one-time ID authentication system token type of the present embodiment performs the two-way one-time ID authentication with the portable terminal as in the above description, by entering the token, has a Web browser whatever the terminal if the terminal can access the content server. That is, a dedicated application program to use the content server even if it is not installed.

[0066]

[0066] Incidentally, in the case where the above-described first and second embodiments the gateway server and the content server are connected over the Internet, because the user ID is prevented from flowing out, again gateway server and the content server by performing bidirectional one-time ID authentication between, it is possible to further ensure the anonymity of the user on the route. Although described as being separate the server that provides the server and the content to authenticate the user, it may be constructed content providing system together. In addition, in the present system, to provide a device to disable the authentication key that is managed by the authentication server in case you lose your mobile device. This is to prevent the event, being unauthorized use by a third party in case you happen to lose your phone.

[0067]

[0067] The system may be utilized with a model identifying the user in the content server to ensure the anonymity of the user on the path, the two models to ensure the anonymity of the user in the route and on the content server it can.

[0068]

[0068] Model for identifying the user in the content server to ensure the anonymity of the user on the route has been guaranteed anonymity is on the path, configured as a model by the authentication server can identify the user ID of the content server It is. The content server, because you have registered personal information necessary, it is possible to extract the personal information required from the user ID. The user need not transmit personal information. Examples of personal information, name, address, date of birth, bank account number that can be used in the settlement, such as credit card number, and the like. As the model, (see FIG. 19) Internet banking model (see FIG. 18) or virtual shop model, (see FIG. 20) racing Internet voting model, internet ticketing model (see FIG. 21), and the like.

[0069]

[0069] Internet banking model may utilize the services Internet banking system provides without entering a user ID, a password, such as account numbers from the mobile. In addition, virtual store model, it is possible to use a user ID, password, bank account number, the online shopping service that virtual store offers without having to input such as from a mobile credit card number. In addition, in the horse race of the Internet vote, to buy betting tickets and settled in the user's bank account at the direction of the user, automatically dividend after the end of the race will be credited to the bank account of the user. In the Internet ticketing When you purchase a ticket by the bank account number or credit card number, use point is added to the user. It is also possible to replace the usage point accumulated in the prize.

[0070]

[0070] On the other hand, a model that guarantees the anonymity of the user is in the path and on the content server, the content server, the personal information is not registered any, including the user ID. And, configured as a model that can be accessed while guaranteeing

anonymity to the content server. As the model, (see FIG. 22) electronic voting model, and the like electron questionnaire model (see Figure 23). Electronic voting model, the electronic voting server records only result found in the database, can not be known which users have voted. Once the user who vote will be set in the authentication server so that it can not be re-vote. Voting management agencies, voters to allow access to the electronic voting system while maintaining the anonymity, to distribute the application and the authentication key for the mobile terminal to the voters in a secure manner. In addition, the electronic questionnaire model, records filled out the questionnaire only to the database, who is filled out is not be known. Once the user who fill in the questionnaire will be set in the authentication server so that it can not be filled again. Questionnaire executing agency, survey respondents to allow access to the electronic questionnaire server while maintaining the anonymity, to distribute the application and the authentication key for the mobile terminal to the questionnaire respondents in a secure manner.

[0071] initial stage of the first and second embodiment example of a sequence diagram present invention for explaining a sequence diagram bidirectional one-time ID authentication for explaining a sequence diagram bidirectional one-time ID authentication to be described bidirectional one-time ID authentication for the in Fig present invention showing the process of obtaining the session ID in the first embodiment of FIG present invention showing the process of obtaining an authentication key in the first and second embodiments of FIGS present invention showing the 1 of obtaining content in the second embodiment of FIG present invention showing the process of obtaining a token in the second embodiment of FIG present invention showing a process of obtaining content in example process the first embodiment of FIG present invention showing the sequence of obtaining the session ID in the first embodiment of FIG present invention showing the sequence of obtaining the authentication key in the first embodiment of FIG present invention showing the It shows a sequence of obtaining a token in the second embodiment of automatically drawing the invention showing a sequence of performing re-authentication in the first embodiment of FIG present invention showing the sequence of obtaining content in It shows the session ID and the sequence of obtaining content by using the Cookie registration session ID in the second embodiment of FIG present invention showing the sequence of obtaining the contents of the second embodiment of FIG invention

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-339247
(P2005-339247A)
(43)公開日　平成17年12月8日(2005.12.8)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330B	5B085
H04L 9/32	G06F 15/00	330E	5J104
	H04L 9/00	673D	

審査請求 未請求　請求項の数 21　ＯＬ　（全 25 頁）

(21)出願番号　特願2004-157752 (P2004-157752)
(22)出願日　平成16年5月27日 (2004.5.27)

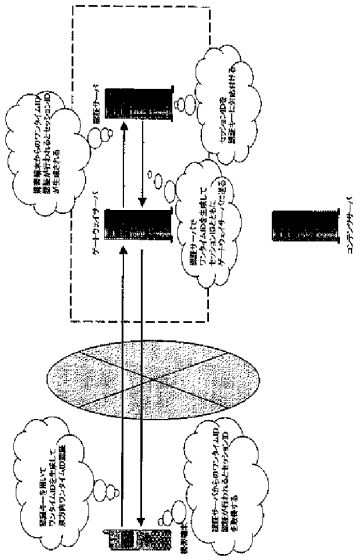
（特許庁注：以下のものは登録商標）
１．Ｂｌｕｅｔｏｏｔｈ
２．ＵＳＢ

(71)出願人　500196087
株式会社セキュアード・コミュニケーションズ
神奈川県川崎市中原区新丸子町９１５－１５
(74)代理人　100081514
弁理士　酒井　一
(74)代理人　100082692
弁理士　蔵合　正博
(72)発明者　大河　克好
東京都町田市三輪緑山１－３－２　緑山ヒルズ２１２

Ｆターム(参考)　5B085 AE02 AE09 AE23 AE29 BA06 BG07
5J104 AA07 KA01 KA04 KA21 NA05 NA38 PA07

(54)【発明の名称】双方向ワンタイムＩＤ認証システム及び認証方法

(57)【要約】
【課題】　ユーザＩＤやパスワードを入力しなくても自動的にユーザの認証を行い、かつ、その認証をコンテンツサーバで行わない双方向ワンタイムＩＤ認証システムを提供する。
【解決手段】　コンテンツサーバのＵＲＬとコンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、認証サーバから認証キーをインストールして認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、携帯端末がアクセスするゲートウェイサーバとを備え、携帯端末は、ゲートウェイサーバを介して認証サーバとの間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合にゲートウェイサーバを介してコンテンツサーバへコンテンツを要求する双方向ワンタイムＩＤ認証システムである。
【選択図】　図6



【特許請求の範囲】
【請求項1】
コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、
前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、
前記携帯端末がアクセスするゲートウェイサーバとを備え、
前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求することを特徴とする双方向ワンタイムＩＤ認証システム。
【請求項2】
前記認証サーバは、前記認証サーバにおいて前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤを生成して前記ゲートウェイサーバを介して前記携帯端末に送り、前記携帯端末から前記コンテンツ要求とともに前記ゲートウェイサーバを介して送られてくる前記セッションＩＤを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬと前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記携帯端末に送り、前記携帯端末では前記コンテンツを取得して表示することを特徴とする請求項１に記載の双方向ワンタイムＩＤ認証システム。
【請求項3】
前記認証キーを用いて双方向ワンタイムＩＤ認証を行わせ、前記認証サーバのワンタイムＩＤ認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求させ、前記コンテンツを取得させる、一連の処理を行わせるブラウザ型のアプリケーションプログラムを前もってインストールしておくことを特徴とする請求項１または２に記載の双方向ワンタイムＩＤ認証システム。
【請求項4】
前記アプリケーションプログラム及び前記認証キーがインストールされた前記携帯端末は、前記アプリケーションプログラムを起動させると、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求して取得し、前記携帯端末上に表示する動作を自動で行うことを特徴とする請求項１乃至３の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項5】
前記セッションＩＤはセッション時間を持ち、前記認証サーバは前記セッション時間が過ぎた場合に前記セッションＩＤを無効にすることを特徴とする請求項１乃至４の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項6】
前記セッション時間が過ぎて前記セッションＩＤが無効になっていた場合、自動的に双方向ワンタイムＩＤ認証による再認証を行うことを特徴とする請求項５に記載の双方向ワンタイムＩＤ認証システム。
【請求項7】
コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、

前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、
前記携帯端末がアクセスするゲートウェイサーバとを備え、
前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、前記認証サーバは、認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成して前記ゲートウェイサーバを介して前記携帯端末に前記トークン
を送り、前記携帯端末から前記トークンを当該携帯端末とは異なる端末に入力し、前記認証サーバは、前記異なる端末から前記ゲートウェイサーバを介してコンテンツ要求とともに送られてくる前記トークンに対応付けられた前記セッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送り、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤをＣｏｏｋｉｅに登録し、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求することを特徴とする双方向ワンタイムＩＤ認証システム。
【請求項8】
前記認証キーを用いて双方向ワンタイムＩＤ認証を行わせ、双方向ワンタイムＩＤ認証が成功した場合に前記トークンを取得させる、一連の処理を行わせるトークン型のアプリケーションプログラムを前もってインストールしておくことを特徴とする請求項７に記載の双方向ワンタイムＩＤ認証システム。
【請求項9】
前記セッションＩＤはセッション時間を持ち、前記認証サーバは前記セッション時間が過ぎた場合に前記セッションＩＤを無効にし、前記認証サーバにおいて前記セッションＩＤが無効になった場合、前記携帯端末から前記アプリケーションプログラムを起動させて前記トークンを取得することを特徴とする請求項７または８に記載の双方向ワンタイムＩＤ認証システム。
【請求項10】
前記認証キーは、前記アプリケーションプログラムを起動させ、前記携帯端末で受け取られる前記初期認証コードと必要な場合は認証キーのダウンロード先アドレスを入力することにより、インストールされることを特徴とする請求項1乃至９の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項11】
前記認証キーは、当該認証キーのダウンロード先が記載された電子メールを前記携帯端末が受信して前記ダウンロード先をクリックすることによりインストールされることを特徴とする請求項1乃至９の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項12】
前記認証サーバでユーザを特定できるモデルとして使用することを特徴とする請求項1乃至１１の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項13】
前記認証サーバでユーザの匿名性を保障できるモデルとして使用することを特徴とする請求項1乃至１１の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項14】
前記携帯端末を紛失した場合に前記認証キーを無効にできる装置を別に備えることを特徴とする請求項1乃至１３の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項15】
前記ゲートウェイサーバと前記コンテンツサーバがインターネットを介して接続されている場合、両サーバ間で双方向ワンタイムＩＤ認証を行うことを特徴とする請求項1乃至

１４の何れかに記載の双方向ワンタイムＩＤ認証システム。
【請求項16】
ユーザＩＤを定義し、当該ユーザの住所、電話番号、やＥ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報を管理するコンテンツサーバと、
前記コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、
前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、
前記携帯端末がアクセスするゲートウェイサーバとを備え、
前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求することを特徴とするコンテンツ提供システム。
【請求項17】
ユーザＩＤを定義し、当該ユーザの住所、電話番号、やＥ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報を管理するコンテンツサーバと、
前記コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、
前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、
前記携帯端末がアクセスするゲートウェイサーバとを備え、
前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、前記認証サーバは、認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成して前記ゲートウェイサーバを介して前記携帯端末に前記トークンを送り、前記携帯端末は前記トークンを当該携帯端末とは異なる端末に入力し、前記認証サーバは前記ゲートウェイサーバを介してコンテンツ要求とともに送られてくる前記トークンに対応付けられたセッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送り、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤをＣｏｏｋｉｅに登録し、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求することを特徴とするコンテンツ提供システム。
【請求項18】
認証サーバにおいて、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する工程と、携帯端末が前記認証サーバから前記認証キーをインストールする工程と、前記携帯端末が前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行う工程と、前記携帯端末において前記認証サーバのワンタイムＩＤ認証が成功した場合に、前記携帯端末は前記ゲートウェイサーバを介してコンテンツサーバへコンテンツを要求する工程とを有することを特徴とする双方向ワン

タイムＩＤ認証方法。
【請求項19】
前記認証サーバにおいて、前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤを生成する工程と、前記セッションＩＤを前記ゲートウェイサーバを介して前記携帯端末に送る工程と、前記携帯端末から前記コンテンツ要求とともに前記ゲートウェイサーバを介して送られてくる前記セッションＩＤを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出す工程と、前記ゲートウェイサーバにおいて前記コンテンツ要求を前記コンテンツサーバのＵＲＬと前記ユーザＩＤと合成して前記コンテンツサーバに送る工程と、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記携帯端末に送る工程と、前記携帯端末が前記コンテンツを取得して表示する工程とを有することを特徴とする請求項１８に記載の双方向ワンタイムＩＤ認証方法。
【請求項20】
認証サーバにおいて、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する工程と、携帯端末が前記認証サーバから前記認証キーをインストールする工程と、前記携帯端末が前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行う工程と、前記認証サーバにおいて前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成する工程と、前記ゲートウェイサーバを介して前記携帯端末に前記トークンを送る工程と、前記携帯端末において前記トークンを当該携帯端末とは異なる端末に入力する工程とを有することを特徴とする双方向ワンタイムＩＤ認証方法。
【請求項21】
前記トークンが入力された前記携帯端末とは異なる端末から前記ゲートウェイサーバを介してコンテンツ要求とともに前記トークンを送る工程と、前記送られてくるトークンに対応付けられた前記セッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送る工程と、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送る工程と、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送る工程と、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤをＣｏｏｋｉｅに登録する工程と、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求する工程とを有することを特徴とする請求項２０に記載の双方向ワンタイムＩＤ認証方法。
【発明の詳細な説明】
【技術分野】
【0001】
本発明は、携帯端末とサーバとの間で双方向ワンタイムＩＤ認証を行う双方向ワンタイム認証システム及び認証方法に関する
【背景技術】
【0002】
インターネット経由で電子商取引や金銭取引等のサービスを提供するコンテンツサーバが広く知られている。図２４に示すように、ユーザは携帯端末やパソコン等を用いてコンテンツサーバとの間でインターネットを介して通信を行い、実際にそのサービスを利用する際には予め決定したユーザＩＤやパスワード等を入力して認証を行った上で、利用することができる。すなわち、コンテンツサーバは入力されたユーザＩＤやパスワード等を用いて、ユーザ情報との整合を取り、アクセスしてくるユーザを特定し、正当なユーザであれば要求を許可するようにしている。
【特許文献1】特開２００３－１６２５０７

【発明の開示】
【発明が解決しようとする課題】
【0003】
しかしながら、ユーザＩＤやパスワード等は第三者により推測、漏えい、あるいは盗み見られてしまうおそれがあり、そのようなことがあると、第三者でも簡単にコンテンツサーバが利用できてしまい、不正な商取引や金銭取引がされてしまうおそれがある。また、コンテンツサーバで管理されているユーザ情報には、ユーザＩＤやパスワード等の他に、例えば、ユーザの住所や電話番号、Ｅ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報等も管理されているので、第三者にユーザＩＤやパスワード等が知られてしまうと、同時にこれらの情報も知られてしまうおそれがある。そのため、ユーザはコンテンツサーバが提供する電子商取引や金銭取引等のサービスを安心して利用することができないという問題がある。
【0004】
こうした問題に着目し、本発明は、ユーザＩＤやパスワードを入力しなくても自動的にユーザの認証を行い、かつ、その認証をコンテンツサーバで行わない双方向ワンタイムＩＤ認証システム及び認証方法を提供することを目的とする。
【課題を解決するための手段】
【0005】
本発明の請求項１に記載の発明は、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、前記携帯端末がアクセスするゲートウェイサーバとを備え、前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求することを特徴とする双方向ワンタイムＩＤ認証システムである。
【0006】
本発明の請求項２に記載の発明は、請求項１に記載の双方向ワンタイムＩＤ認証システムについて、前記認証サーバは、前記認証サーバにおいて前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤを生成して前記ゲートウェイサーバを介して前記携帯端末に送り、前記携帯端末から前記コンテンツ要求とともに前記ゲートウェイサーバを介して送られてくる前記セッションＩＤを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬと前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記携帯端末に送り、前記携帯端末では前記コンテンツを取得して表示することを特徴とする。
【0007】
本発明の請求項３に記載の発明は、請求項１または２に記載の双方向ワンタイムＩＤ認証システムについて、前記認証キーを用いて双方向ワンタイムＩＤ認証を行わせ、前記認証サーバのワンタイムＩＤ認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求させ、前記コンテンツを取得させる、一連の処理を行わせるブラウザ型のアプリケーションプログラムを前もってインストールしておくことを特徴とする。
【0008】
本発明の請求項４に記載の発明は、請求項１乃至３の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記アプリケーションプログラム及び前記認証キーがインストールされた前記携帯端末は、前記アプリケーションプログラムを起動させると、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイ

ムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求して取得し、前記携帯端末上に表示する動作を自動で行うことを特徴とする。

【0009】

本発明の請求項５に記載の発明は、請求項１乃至４の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記セッションＩＤはセッション時間を持ち、前記認証サーバは前記セッション時間が過ぎた場合に前記セッションＩＤを無効にすることを特徴とする。

【0010】

本発明の請求項６に記載の発明は、請求項５に記載の双方向ワンタイムＩＤ認証システムについて、前記セッション時間が過ぎて前記セッションＩＤが無効になっていた場合、自動的に双方向ワンタイムＩＤ認証による再認証を行うことを特徴とする。

【0011】

本発明の請求項７に記載の発明は、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、前記携帯端末がアクセスするゲートウェイサーバとを備え、前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、前記認証サーバは、認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成して前記ゲートウェイサーバを介して前記携帯端末に前記トークンを送り、前記携帯端末から前記トークンを当該携帯端末とは異なる端末に入力し、前記認証サーバは、前記異なる端末から前記ゲートウェイサーバを介してコンテンツ要求とともに送られてくる前記トークンに対応付けられた前記セッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送り、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤをＣｏｏｋｉｅに登録し、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求することを特徴とする双方向ワンタイムＩＤ認証システムである。

【0012】

本発明の請求項８に記載の発明は、請求項７に記載の双方向ワンタイムＩＤ認証システムについて、前記認証キーを用いて双方向ワンタイムＩＤ認証を行わせ、双方向ワンタイムＩＤ認証が成功した場合に前記トークンを取得させる、一連の処理を行わせるトークン型のアプリケーションプログラムを前もってインストールしておくことを特徴とする。

【0013】

本発明の請求項９に記載の発明は、請求項７または８に記載の双方向ワンタイムＩＤ認証システムについて、前記セッションＩＤはセッション時間を持ち、前記認証サーバは前記セッション時間が過ぎた場合に前記セッションＩＤを無効にし、前記認証サーバにおいて前記セッションＩＤが無効になった場合、前記携帯端末から前記アプリケーションプログラムを起動させて前記トークンを取得することを特徴とする。

【0014】

本発明の請求項１０に記載の発明は、請求項1乃至９の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記認証キーは、前記アプリケーションプログラムを起動させ、前記携帯端末で受け取られる前記初期認証コードと必要な場合は認証キーのダウンロード先アドレスを入力することにより、インストールされることを特徴とする。

【0015】

本発明の請求項１１に記載の発明は、請求項1乃至９の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記認証キーは、当該認証キーのダウンロード先が記載された電子メールを前記携帯端末が受信して前記ダウンロード先をクリックすることによりインストールされることを特徴とする。

【0016】

本発明の請求項１２に記載の発明は、請求項1乃至１１の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記認証サーバでユーザを特定できるモデルとして使用することを特徴とする。

【0017】

本発明の請求項１３に記載の発明は、請求項1乃至１１の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記認証サーバでユーザの匿名性を保障できるモデルとして使用することを特徴とする。

【0018】

本発明の請求項１４に記載の発明は、請求項1乃至１３の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記携帯端末を紛失した場合に前記認証キーを無効にできる装置を別に備えることを特徴とする。

【0019】

本発明の請求項１５に記載の発明は、請求項1乃至１４の何れかに記載の双方向ワンタイムＩＤ認証システムについて、前記ゲートウェイサーバと前記コンテンツサーバがインターネットを介して接続されている場合、両サーバ間で双方向ワンタイムＩＤ認証を行うことを特徴とする。

【0020】

本発明の請求項１６に記載の発明は、ユーザＩＤを定義し、当該ユーザの住所、電話番号、やＥ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報を管理するコンテンツサーバと、前記コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、前記携帯端末がアクセスするゲートウェイサーバとを備え、前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合に前記ゲートウェイサーバを介して前記コンテンツサーバへコンテンツを要求することを特徴とするコンテンツ提供システムである。

【0021】

本発明の請求項１７に記載の発明は、ユーザＩＤを定義し、当該ユーザの住所、電話番号、やＥ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報を管理するコンテンツサーバと、前記コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する認証サーバと、前記認証サーバから前記認証キーをインストールして前記認証サーバと双方向ワンタイムＩＤ認証を行う携帯端末と、前記携帯端末がアクセスするゲートウェイサーバとを備え、前記携帯端末は、前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行い、前記認証サーバは、認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成して前記ゲートウェイサーバを介して前記携帯端末に前記トークンを送り、前記携帯端末から前記トークンを当該携帯端末とは異なる端末に入力し、前記認証サーバは前記ゲートウェイサーバを介してコンテンツ要求とともに送られてくる前記トークンに対応付けられたセッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送り、前記ゲートウェイサーバは前記コンテ

ンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送り、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送り、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤをＣｏｏｋｉｅに登録し、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求することを特徴とするコンテンツ提供システムである。

【0022】

本発明の請求項１８に記載の発明は、認証サーバにおいて、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する工程と、携帯端末が前記認証サーバから前記認証キーをインストールする工程と、前記携帯端末が前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行う工程と、前記携帯端末において前記認証サーバのワンタイムＩＤ認証が成功した場合に、前記携帯端末は前記ゲートウェイサーバを介してコンテンツサーバへコンテンツを要求する工程とを有することを特徴とする双方向ワンタイムＩＤ認証方法である。

【0023】

本発明の請求項１９に記載の発明は、請求項１８に記載の双方向ワンタイムＩＤ認証方法について、前記認証サーバにおいて、前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤを生成する工程と、前記セッションＩＤを前記ゲートウェイサーバを介して前記携帯端末に送る工程と、前記携帯端末から前記コンテンツ要求とともに前記ゲートウェイサーバを介して送られてくる前記セッションＩＤを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出す工程と、前記ゲートウェイサーバにおいて前記コンテンツ要求を前記コンテンツサーバのＵＲＬと前記ユーザＩＤと合成して前記コンテンツサーバに送る工程と、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記携帯端末に送る工程と、前記携帯端末が前記コンテンツを取得して表示する工程とを有することを特徴とする。

【0024】

本発明の請求項２０に記載の発明は、認証サーバにおいて、コンテンツサーバのＵＲＬと当該コンテンツサーバで定義されたユーザＩＤの登録に従って初期認証コードを定義し、前記コンテンツサーバのＵＲＬ、ユーザＩＤ、及び初期認証コードを双方向ワンタイムＩＤ認証を行う認証キーと対応付けて管理する工程と、携帯端末が前記認証サーバから前記認証キーをインストールする工程と、前記携帯端末が前記ゲートウェイサーバを介して前記認証サーバとの間で前記認証キーを用いて双方向ワンタイムＩＤ認証を行う工程と、前記認証サーバにおいて前記携帯端末のワンタイムＩＤ認証が成功した場合に前記認証キーに対応付けられたセッションＩＤ及びトークンを生成する工程と、前記ゲートウェイサーバを介して前記携帯端末に前記トークンを送る工程と、前記携帯端末において前記トークンを当該携帯端末とは異なる端末に入力する工程とを有することを特徴とする双方向ワンタイムＩＤ認証方法。

【0025】

本発明の請求項２１に記載の発明は、請求項２０に記載の双方向ワンタイムＩＤ認証方法について、前記トークンが入力された前記携帯端末とは異なる端末から前記ゲートウェイサーバを介してコンテンツ要求とともに前記トークンを送る工程と、前記送られてくるトークンに対応付けられた前記セッションＩＤのセッション時間が過ぎていないことを確認した場合に前記コンテンツサーバのＵＲＬ及びユーザＩＤを読み出して前記セッションＩＤとともに前記ゲートウェイサーバに送る工程と、前記ゲートウェイサーバは前記コンテンツ要求を前記コンテンツサーバのＵＲＬ及び前記ユーザＩＤと合成して前記コンテンツサーバに送る工程と、前記コンテンツサーバのコンテンツを前記ゲートウェイサーバを介して前記セッションＩＤとともに前記携帯端末とは異なる端末に送る工程と、前記携帯端末とは異なる端末では前記コンテンツを取得して表示するとともに前記セッションＩＤ

をＣｏｏｋｉｅに登録する工程と、それ以降は、前記Ｃｏｏｋｉｅに登録されたセッションＩＤを用いてコンテンツを要求する工程とを有することを特徴とする。

【発明の効果】

【0026】

本発明によれば、ユーザＩＤやパスワードを入力しなくても自動的に認証を行うことができるので、第三者にユーザＩＤやパスワード等が知られることはなく、ユーザはコンテンツサーバが提供する電子商取引や金銭取引等のサービスを安心して利用することができる。

【0027】

また、本発明によれば、携帯端末にダウンロードしたアプリケーションプログラムを起動するとコンテンツサーバへの認証とアクセスが自動的に行われる。

【0028】

また、本発明によれば、認証をコンテンツサーバで行わないので、コンテンツサーバは情報を提供するだけでよく、認証システム構築の手間やコストを省くことができる。

【発明を実施するための最良の形態】

【0029】

以下、本発明を実施するための最良の形態を説明するが、本発明は以下の実施例の範囲に限定されるものではなく、その要旨を逸脱しない範囲であれば、適宜に変更及び実施できるものである。はじめに、ワンタイムＩＤと双方向ワンタイムＩＤ認証、ならびにアプリケーションプログラムと認証キーについて説明する。

【0030】

ワンタイムＩＤと双方向ワンタイムＩＤ認証について説明する。ワンタイムＩＤは認証において一回限り使用可能な識別情報であり、装置間あるいはアプリケーション間で共通な鍵や認証データを基に生成される。ワンタイムＩＤによる認証では、第三者が送信者・受信者を特定できなる一方で、正当な送信者・受信者であればワンタイムＩＤを識別情報として把握できるという匿名性を保障する効果が得られるとともに、送信者と受信者間で通信が行われる度にワンタイムＩＤが変更されるために、第三者が次回のワンタイムＩＤを予測できることができないという効果が得られる。双方向ワンタイムＩＤ認証では、このワンタイムＩＤを使って相互に認証を行うために、お互いになりすましを防ぐことができる。

【0031】

例えばワンタイムIDを使った鍵交換・認証方式であるＰ－ＳＩＧＭＡにおいては、図１に示すような手順で鍵交換および認証が行われている。先ず、クライアントが、ＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）の提案、乱数Ｒｃ、ＤＨ（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）公開値ｇｘ　、ＯＩＤ（ワンタイムＩＤ）をサーバに対して送信する。なお、ＳＡの提案には、暗号アルゴリズムや認証方式、鍵交換に使用するパラメータ等に関する提案が含まれている。

【0032】

次いで、サーバが、受け取ったＯＩＤからクライアントを識別し、識別できない場合には、通信を拒否する。識別できる場合には、受諾したＳＡ、乱数Ｒｓ、ＤＨ公開値ｇｙ　、ＨＡＳＨｓ、セッション鍵ｅで暗号化したＩＤｓ（サーバＩＤ）をクライアントに対して送信する。なお、セッション鍵ｅは、既知共有鍵、乱数Ｒｓ、乱数ＲｃおよびＤＨ共通鍵ｇｘｙを引数とする鍵付きハッシュ関数の関数値であり、ＨＡＳＨｓは、既知共有鍵、乱数Ｒｓ、乱数Ｒｃ、ＤＨ公開値ｇｘ　、ｇｙ　およびＩＤｓを引数とする疑似乱数関数の関数値である。

【0033】

次いで、クライアントが、受け取ったＨＡＳＨｓを検証し、このＨＡＳＨｓに基づいてサーバの正当性を確認する。ＨＡＳＨｓが正しければ、ＨＡＳＨｃ、セッション鍵ｅで暗号化したＩＤｃ（クライアントＩＤ）をサーバに対して送信する。ここで、ＨＡＳＨｃは、既知共有鍵、乱数Ｒｓ、乱数Ｒｃ、ＤＨ公開値ｇｘ　、ｇｙ　およびＩＤｃを引数とす

る疑似乱数関数の関数値である。次いで、サーバが、受け取ったＨＡＳＨｃを検証し、このＨＡＳＨｃに基づいてクライアントの正当性を確認する。ＨＡＳＨｃが正しければ、当該プロトコルを終了する。

【0034】

このＰ－ＳＩＧＭＡにおいて、ＯＩＤ（ワンタイムＩＤ）は、次のように定義されている。

【0035】

ＯＩＤ１　＝ｐｒｆ（Ｋ、１）
ＯＩＤ２　＝ｐｒｆ（Ｋ、２）
・・・
ＯＩＤｎ　＝ｐｒｆ（Ｋ、ｎ）

【0036】

この定義式において、ＯＩＤｎ　はｎ番目のＳＡ確立時に用いられるワンタイムＩＤ、ｐｒｆは疑似乱数関数、Ｋは既知共有鍵、若しくは既知共有鍵から生成された値である。

【0037】

このため、上記Ｐ－ＳＩＧＭＡによれば、ＯＩＤを導入したことにより、第三者が送信者・受信者を特定できなくなる一方で、正当な送信者・受信者であればＯＩＤを識別情報として把握できるといった効果が得られるとともに、クライアント・サーバ間で通信が行われる度（すなわち、ＳＡの生成または更新毎）にＯＩＤが変更されるため、第三者が次回のＯＩＤを予測することができないといった効果が得られる。

【0038】

この他にセッション毎に変化する可変共有鍵を引数、あるいは可変共有鍵と通信順序を引数とするハッシュ関数の関数値をワンタイムＩＤ（ＳＩＧＮＡＬ）として用いるようにしたものもある（図２、図３参照）。これにより、例えば、可変共有鍵が第三者に漏れたとしても、セッション毎に可変共有鍵が変化することとなるので、漏れた可変共有鍵を用いて生成されたワンタイムＩＤ以外のワンタイムＩＤを予測できなくなる。すなわち、盗聴が困難で安全性に優れたワンタイムＩＤを生成することが可能になる。また、上記ワンタイムＩＤ（ＳＩＧＮＡＬ）を用いて、クライアント・サーバ間における認証を行うようにしたので、第三者が送信者・受信者を特定できなくなる一方で、正当な送信者・受信者であればワンタイムＩＤを識別情報として把握することができる。したがって、ＤｏＳ攻撃やなりすまし等に対する耐性を強化することができ、オープンなネットワーク環境下においても、ＩＤ情報の保護を図り、通信の安全性を向上させることができる。また、リモートアクセスが可能になり、利便性の向上を図ることもできる。

【0039】

つづいてアプリケーションプログラムについて説明する。本発明の双方向ワンタイムＩＤ認証システムは、携帯端末にアプリケーションプログラムをインストールすることで利用することができる。そして、インストールされたアプリケーションプログラムを起動させることにより、自動的に認証サーバとの間で双方向ワンタイムＩＤ認証を行い、コンテンツサーバから情報を得ることができる。ここでは、アプリケーションプログラムのインストール方法について説明し、具体的な動作についての説明は後述する。

【0040】

アプリケーションプログラムをインストールするには、次のような方法がある。ただし、インストールの方法はこれに限定されるものではない。

（１）携帯端末に認証アプリケーションソフトのダウンロード先が記載された電子メールが届き、そのダウンロード先をクリックすることにより、ダウンロードサイトからアプリケーションプログラムをダウンロードしてインストールする。

（２）郵送等でアプリケーションプログラムのダウンロードサイトが通知され、ユーザがダウンロードサイトを入力して、ダウンロードサイトからアプリケーションプログラムをダウンロードしてインストールする。

（３）郵送等でアプリケーションプログラムのソフトが送られ、それを用いてインストー

ルする。

【0041】

認証キーは、ワンタイムＩＤを生成して双方向ワンタイムＩＤ認証を行う際に用いる共有鍵である。双方向ワンタイムＩＤ認証を行う際には、予め認証キーをインストールすることで利用することができる。認証キーのインストール方法について説明する。コンテンツサーバでユーザの住所、電話番号、Ｅ－ｍａｉｌアドレス、生年月日、及びユーザＩＤ等のユーザ情報が登録されると、認証サーバにおいてオペレータの操作等により、コンテンツサーバのＵＲＬとコンテンツサーバで定義されたユーザＩＤを登録し、これに従い初期認証コードを定義して認証キーと対応付けて対応表に登録する。郵送等でアプリケーションプログラムのダウンロードサイトあるいはソフトが送られてくる場合には、初期認証コードも同封されている。なお、必要な場合は認証キーのダウンロード先のサイトアドレスも同封されている。インストールされたアプリケーションプログラムを起動させると、初期認証コードと必要な場合は認証キーのダウンロード先のサイトアドレスの入力を要求する画面が表示され、クライアントが初期認証コードやダウンロード先のサイトアドレスを入力すると、初期認証コードはゲートウェイサーバを介して認証サーバへ送られて認証キーのダウンロードを要求する。一方、電子メールでアプリケーションプログラムのダウンロード先が送られてくる場合には、認証キーのダウンロード先と初期認証コードが記載されている。ユーザは認証キーのダウンロード先と初期認証コードを入力することにより、初期認証コードがゲートウェイサーバを介して認証サーバへ送られて認証キーのダウンロードを要求する。なお、認証キーのダウンロード先はそれをクリックすることにより、初期認証コードも一緒に送られるようになっていても良く、ユーザは認証キーのダウンロード先を入力またはクリックすることにより、自動的に初期認証コードがゲートウェイサーバを介して認証サーバへ送られて認証キーのダウンロードを要求するようにしても良い。

【0042】

そして、認証アプリケーションプログラムを起動させて初期認証コードや認証キーのダウンロード先サイトアドレスを入力、あるいは認証キーダウンロード先をクリックすると、初期認証コードを受信した認証サーバは、初期認証コードに対応付けられている認証キーを対応表から読み出し、認証キーをゲートウェイサーバを介してダウンロード要求のあったユーザの携帯端末に送る。携帯端末では認証キーがインストールされる。なお、認証キーには可変であるものとないものがあるが、本システムでは何れの認証キーを用いても使用することができる。

【0043】

以上の認証アプリケーションプログラムと認証キーを携帯端末にインストールしておくことで、携帯端末上のアプリケーションプログラムを起動させると、自動的にゲートウェイサーバを介して認証サーバとの間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合にゲートウェイサーバを介してコンテンツサーバへコンテンツを要求して取得することができる。

【実施例】

【0044】

以下、図面を用いて本発明の第１実施例について説明する。本実施例ではブラウザ型の双方向ワンタイムＩＤ認証システムについて説明する。図４乃至７に示すように、ブラウザ型の双方向ワンタイムＩＤ認証システムは、携帯端末と、認証サーバと、ゲートウェイサーバとを備え、携帯端末は、ゲートウェイサーバを介して認証サーバとの間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合にセッションＩＤを取得し、ゲートウェイサーバを介してコンテンツサーバへコンテンツを要求するシステムである。

【0045】

ここでセッションＩＤについて説明する。セッションＩＤは、認証サーバの中でユニークな値を割り当て、認証キーと対応付けられた識別子である。認証サーバの中で双方向ワ

ンタイムID認証が成功した場合、それ以降、携帯端末からコンテンツサーバへのアクセス要求時にセッションＩＤを付加し、セッションＩＤによりコンテンツサーバへのアクセスを認証サーバに認証してもらうようにしている。なお、ユーザはセッションＩＤの付加について意識する必要はなく、アプリケーションが自動的にセッションＩＤ付加するようにプログラムされている。

【0046】

すなわち、本システムでは、ユーザの認証を行うゲートウェイサーバ及び認証サーバと、コンテンツのサービスを提供するコンテンツサーバとを分離しており、携帯端末はコンテンツサーバと直接的に通信や認証を行っていない。

【0047】

以下、各構成について説明する。上記したように、携帯端末にはアプリケーションプログラムと認証キーをインストールしておく。ここではブラウザ型のアプリケーションプログラムをインストールしているものとする。携帯端末はゲートウェイサーバのみにアクセスする端末である。携帯端末には携帯電話やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ（Ｄａｔａ）　Ａｓｓｉｓｔａｎｔｓ）等がある。認証サーバは、オペレータの操作等により、コンテンツサーバのＵＲＬとコンテンツサーバで定義されたユーザＩＤを登録し、これに従い初期認証コードを定義して認証キーと対応付けて対応表に登録するサーバである。また、認証サーバは、ゲートウェイサーバを介して携帯端末との間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証サーバにおいて携帯端末のワンタイムＩＤ認証が成功した場合にセッションＩＤを生成する。

【0048】

認証サーバにおいて生成されたセッションＩＤは、認証キーと対応付けられて対応表にて管理される。すなわち、セッションＩＤは認証キーと対応付けられているので、認証キーと対応付けられているコンテンツサーバＵＲＬ及びユーザＩＤとも対応付けることができる。また、生成されたセッションＩＤはゲートウェイサーバを介して携帯端末にワンタイムＩＤとともに送られる。そして認証サーバは、携帯端末からゲートウェイサーバを介して送られてくるセッションＩＤを確認した場合に、セッションＩＤに対応付けられているコンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができる。ゲートウェイサーバは、携帯端末と認証サーバの間の通信、コンテンツサーバと携帯端末の間の通信を制御するものであり、本システムにおいて、携帯端末、認証サーバ、及びコンテンツサーバは、必ずゲートウェイサーバを介して通信を行う。コンテンツサーバは電子商取引や金銭取引等のサービスを提供するサーバである。コンテンツサーバには、当該サーバを利用するユーザのユーザＩＤが定義され、住所や電話番号、Ｅ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報が登録されて管理されている。本システムは、携帯端末上のブラウザ型のアプリケーションプログラムを起動させることにより、自動的に認証が行われ、コンテンツサーバのコンテンツを取得することができる。

【0049】

以下、図１０乃至１３を用いて、携帯端末にインストールされたブラウザ型のアプリケーションプログラムを起動したときのプログラムの動作を説明する。携帯端末上のアプリケーションプログラムを起動すると、はじめに認証キーを取得しているか否かについて判別される。認証キーが無い場合には、認証キーをインストールしなければならないので、認証キーダウンロードの動作（準備段階）に移り、上記のように初期認証コードと必要な場合は認証キーのダウンロード先アドレスを入力あるいは認証キーダウンロード先をクリックして、携帯端末上にインストールする（図１０参照）。認証キーが取得されている場合には認証キーを用いてワンタイムＩＤを生成する動作に移る（ステップ１）。

【0050】

以下、図１１を用いてステップ１の動作を説明する。認証キーを用いてワンタイムＩＤを生成すると、携帯端末は携帯端末認証用のワンタイムＩＤをゲートウェイサーバに送り、ゲートウェイサーバはワンタイムＩＤを認証サーバに送る。認証サーバでは対応表にて

管理されている認証キーを用いて、携帯端末から送られてくるワンタイムＩＤの認証を行い、認証が成功した場合にセッションＩＤを生成する。そして、生成されたセッションＩＤは、認証サーバで認証キーと対応付けられて対応表にて管理される。その一方、認証サーバで携帯端末の認証が行われると、認証サーバでは上記ワンタイムＩＤとは別の認証サーバ認証用のワンタイムＩＤが生成される。認証サーバは、生成されたワンタイムＩＤをセッションＩＤとともにゲートウェイサーバに送る。また、セッションＩＤはセッション時間を持っており、認証サーバではセッションＩＤを生成すると同時にその時間を計っている。そして、セッション時間が過ぎた場合には、セッションＩＤを無効にするようにプログラムされている。ゲートウェイサーバは認証サーバからワンタイムＩＤとセッションＩＤを受信すると、それらを携帯端末に送る。携帯端末はゲートウェイサーバを介して認証サーバから送られてくるワンタイムＩＤで認証サーバの認証を行い、認証が成功した場合にセッションＩＤを取得する。携帯端末上でセッションＩＤを取得するとコンテンツサーバへコンテンツを要求する動作に移る（ステップ２）。

【0051】

以下、図１２を用いてステップ２の動作を説明する。携帯端末上でセッションＩＤを取得すると携帯端末上ではコンテンツを要求するＨＴＴＰパケットを生成する。携帯端末はＨＴＴＰパケットをセッションＩＤとともにゲートウェイサーバに送り、ゲートウェイサーバはセッションＩＤを認証サーバへ送る一方、ＨＴＴＰパケットを一旦保持する。認証サーバではゲートウェイサーバから送られてくるセッションＩＤを取得し、当該セッションＩＤが対応表にて管理されているか否かを判別し、対応表にセッションＩＤがある場合には当該セッションＩＤに対応付けられているコンテンツサーバＵＲＬ及びユーザＩＤを読み出す。すなわち、セッション時間内にセッションＩＤを読み出すことができれば、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができ、セッション時間内にセッションＩＤを読み出すことができなければ、対応表に対応するセッションＩＤが存在しないので、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができない。対応表に対応するセッションＩＤが存在しない場合、認証サーバはコンテンツを取得することができない旨（ＮＧ）をゲートウェイサーバに通知し、ゲートウェイサーバもその旨を携帯端末に通知する。その旨を通知された携帯端末は、図１３に示すように、自動的に再度、認証キーを用いてワンタイムＩＤを生成する動作（ステップ１）に移る。一方、対応表に対応するセッションＩＤがある場合、認証サーバでは、コンテンツサーバＵＲＬ及びユーザＩＤを読み出し、これらをゲートウェイサーバに送る。また、その時、認証サーバで計っていたセッション時間をリセットし、再度セッション時間を計る。これにより、携帯端末から同じセッションＩＤを用いてゲートウェイサーバを介して再度送られてくる場合、セッション時間内にセッションＩＤを読み出すことができれば、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができる。

【0052】

コンテンツサーバＵＲＬ及びユーザＩＤを受信したゲートウェイサーバは、一旦保持されているコンテンツを要求するＨＴＴＰパケットと合成し、これをコンテンツサーバに送る。コンテンツサーバはユーザＩＤを取得し、これを用いてコンテンツサーバで管理されている複数のユーザの中からユーザの認証を行い、ＨＴＴＰパケットを元に電子商取引や金銭取引等の電子取引を行いコンテンツを取得することができる。コンテンツサーバは、取得したコンテンツをゲートウェイサーバに送り、ゲートウェイサーバはそれを携帯端末に送る。携帯端末で取得したコンテンツは携帯端末上のブラウザを用いて表示することができる。

【0053】

本実施例のブラウザ型の双方向ワンタイムＩＤ認証システムでは、携帯端末上にインストールされたアプリケーションプログラムを起動させるだけで、ユーザＩＤやパスワード等を入力しなくても自動的にユーザの認証を行うことができる。これにより、第三者にユーザＩＤやパスワード等の個人情報が知られることはないので、ユーザはコンテンツサーバが提供する電子商取引や金銭取引等のサービスを安心して利用することができる。

【0054】
また、双方向ワンタイムＩＤ認証がされた時に受け取るセッションＩＤにセッション時間を持たせ、そのセッションＩＤのセッション時間が有効な間は、再度、双方向ワンタイムＩＤ認証をしなくて良いので、携帯端末とサーバの間での通信時間やパケットを削減することができる。
【実施例】
【0055】
以下、図面を用いて本発明の第２実施例について説明する。本実施例ではトークン型の双方向ワンタイムＩＤ認証システムについて説明する。図８および図９に示すように、トークン型の双方向ワンタイムＩＤ認証システムは、携帯端末と、パソコンと、認証サーバと、ゲートウェイサーバとを備え、携帯端末は、ゲートウェイサーバを介して認証サーバとの間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証が成功した場合にセッションＩＤに対応付けられたトークンを取得し、そのトークンを手入力、赤外線通信、シリアルケーブル、ＩＣカード、メモリカード、Ｂｌｕｅｔｏｏｔｈ、及びＵＳＢケーブル等の手段を用いてパソコンに入力し、そのトークンを用いてパソコンからゲートウェイサーバを介してコンテンツサーバへコンテンツを要求するシステムである。
【0056】
ここでトークンについて説明する。トークンは、双方向ワンタイムＩＤ認証が成功した場合に生成され、認証サーバの中でユニークな値を割り当て、認証キーとセッションＩＤに対応付けられた識別子である。トークンは携帯端末以外の端末からコンテンツ要求を行う場合に、認証サーバにおいて生成されたセッションＩＤと対応付けるために必要な識別子である。なお、トークンを携帯端末以外の端末に手入力する場合はユーザが認識できる文字列を使用する。
【0057】
すなわち、本システムでは、ゲートウェイサーバを介して携帯端末と認証サーバとの間で双方向ワンタイムＩＤ認証を行うことによりトークンを取得し、そのトークンを携帯端末とは異なるパソコン等の端末に入力し、パソコン等の端末からゲートウェイサーバを介してコンテンツサーバへコンテンツを要求するシステムである。なお、本システムでもユーザの認証を行うゲートウェイサーバ及び認証サーバと、コンテンツのサービスを提供するコンテンツサーバとを分離しており、携帯端末やパソコン等の端末はコンテンツサーバと直接的に通信や認証を行っていない。
【0058】
以下、各構成について説明する。上記したように、携帯端末にはアプリケーションプログラムと認証キーをインストールしておく。ここではトークン型のアプリケーションプログラムをインストールしているものとする。携帯端末はゲートウェイサーバのみにアクセスする端末である。携帯端末には携帯電話やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ（Ｄａｔａ）　Ａｓｓｉｓｔａｎｔｓ）等がある。認証サーバは、オペレータの操作等により、コンテンツサーバのＵＲＬとコンテンツサーバで定義されたユーザＩＤを登録し、これに従い初期認証コードを定義して認証キーと対応付けて対応表に登録するサーバである。また、認証サーバは、ゲートウェイサーバを介して携帯端末との間で認証キーを用いて双方向ワンタイムＩＤ認証を行い、認証サーバにおいて携帯端末のワンタイムＩＤ認証が成功した場合にセッションＩＤとトークンを生成する。認証サーバにおいて生成されたセッションＩＤとトークンは、認証キーと対応付けられて対応表にて管理される。すなわち、セッションＩＤとトークンは認証キーと対応付けられているので、認証キーと対応付けられているコンテンツサーバＵＲＬ及びユーザＩＤとも対応付けることができる。また、生成されたトークンはゲートウェイサーバを介して携帯端末に認証サーバの認証用ワンタイムＩＤとともに送られる。そのトークンは携帯端末からパソコン等の端末に入力され、認証サーバは、パソコン等の端末からゲートウェイサーバを介して送られてくるトークンを確認した場合に、トークンに対応付けられているセッションＩＤ、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができる。ゲートウェイサーバは、携帯端末と認証

サーバの間の通信、コンテンツサーバと携帯端末の間の通信を制御するものであり、本システムにおいて、携帯端末やパソコン、認証サーバ、及びコンテンツサーバは、必ずゲートウェイサーバを介して通信を行う。コンテンツサーバは電子商取引や金銭取引等のサービスを提供するサーバである。コンテンツサーバには、当該サーバを利用するユーザのユーザＩＤが定義され、住所や電話番号、Ｅ－ｍａｉｌアドレス、生年月日、決済に使われる銀行口座番号あるいはクレジット番号等の個人情報が登録されて管理されている。本システムは、携帯端末上のトークン型のアプリケーションプログラムを起動させることにより、トークンを取得し、そのトークンをパソコンに入力することにより、自動的に認証が行われ、コンテンツサーバのコンテンツを取得することができる。

【0059】

以下、図１４乃至１７をもちいて、携帯端末にインストールされたトークン型のアプリケーションプログラムを起動したときのプログラムの動作を説明する。はじめに、図１４に示すように、パソコンからゲートウェイサーバにアクセスすると、ゲートウェイサーバはパソコンにトークンの入力が要求される。パソコンで入力するトークンがわからない場合は、携帯端末にインストールされたトークン型のアプリケーションプログラムを起動し、トークンを取得する動作に移る（ステップ１）。一方、入力するトークンがわかっている場合は、パソコン上でトークンを入力してコンテンツサーバへコンテンツを要求する動作に移る（ステップ２）。

【0060】

携帯端末上のアプリケーションプログラムを起動すると、はじめに認証キーを取得しているか否かについて判別される。認証キーが無い場合には、認証キーをインストールしなければならないので、認証キーダウンロードの動作（準備段階）に移り、初期認証コードと必要な場合は認証キーのダウンロード先アドレスを入力あるいは認証キーダウンロード先をクリックして、携帯端末上にインストールする（図１０参照）。認証キーが取得されている場合には認証キーを用いてワンタイムＩＤを生成する動作に移る（図１４参照）。

【0061】

以下、図１４を用いてステップ１の動作を説明する。認証キーを用いてワンタイムＩＤを生成すると、携帯端末はワンタイムＩＤをゲートウェイサーバに送り、ゲートウェイサーバはワンタイムＩＤを認証サーバに送る。認証サーバでは対応表にて管理されている認証キーを用いて、携帯端末から送られてくるワンタイムＩＤの認証を行い、認証が成功した場合にセッションＩＤとトークンを生成する。そして、生成されたセッションＩＤとトークンは、認証サーバで認証キーと対応付けられて対応表にて管理される。その一方、認証サーバで携帯端末の認証が行われると、認証サーバでは上記ワンタイムＩＤとは別の認証サーバ認証用のワンタイムＩＤが生成される。認証サーバは、生成されたワンタイムＩＤをトークンとともにゲートウェイサーバに送る。また、セッションＩＤはセッション時間を持っており、認証サーバではセッションＩＤを生成すると同時にその時間を計っている。そして、セッション時間が過ぎた場合には、セッションＩＤを無効にするようにプログラムされている。ゲートウェイサーバは認証サーバからワンタイムＩＤとトークンを受信すると、それらを携帯端末に送る。携帯端末はゲートウェイサーバを介して認証サーバから送られてくるワンタイムＩＤで認証サーバの認証を行い、認証が成功した場合にトークンを取得する。携帯端末上でトークンを取得することにより、パソコン上でトークンを入力してコンテンツサーバへコンテンツを要求する動作に移る（ステップ２）

【0062】

以下、図１５を用いてステップ２の動作を説明する。パソコン上でトークンを入力し、それがゲートウェイサーバに送られると、ゲートウェイサーバにはコンテンツを要求するＨＴＴＰパケットも同時に送られる。ゲートウェイサーバはトークンを認証サーバへ送る一方、ＨＴＴＰパケットを一旦保持する。認証サーバではゲートウェイサーバから送られてくるトークンを取得し、当該トークンに対応付けられているセッションＩＤが対応表にて管理されているか否かを判別し、対応表にセッションＩＤがある場合には当該セッションＩＤに対応付けられているコンテンツサーバＵＲＬ及びユーザＩＤを読み出す。すなわ

ち、セッション時間内に対応付けられているセッションＩＤを読み出すことができれば、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができ、セッション時間内にセッションＩＤを読み出すことができなければ、対応表に対応するセッションＩＤが存在しないので、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができない。対応表に対応するセッションＩＤが存在しない場合、認証サーバはコンテンツを取得することができない旨（ＮＧ）をゲートウェイサーバに通知し、ゲートウェイサーバもその旨をパソコンに通知する。その旨を通知されたユーザは、図１７に示すように、マニュアルで再度、トークンを取得するため、携帯端末上のトークン型のアプリケーションプログラムを起動させてトークンを取得する。一方、対応表に対応するセッションＩＤがある場合、認証サーバでは、セッションＩＤ、コンテンツサーバＵＲＬ及びユーザＩＤを読み出し、これらをゲートウェイサーバに送る。また、その時、認証サーバで計っていたセッション時間をリセットし、再度セッション時間を計る。

【0063】

コンテンツサーバＵＲＬ及びユーザＩＤを受信したゲートウェイサーバは、一旦保持されているコンテンツを要求するＨＴＴＰパケットと合成し、これをコンテンツサーバに送る。コンテンツサーバはユーザＩＤを取得し、これを用いてコンテンツサーバで管理されている複数のユーザの中からユーザの認証を行い、ＨＴＴＰパケットを元に電子商取引や金銭取引等の電子取引を行いコンテンツを取得することができる。コンテンツサーバは、取得したコンテンツをゲートウェイサーバに送り、ゲートウェイサーバはそれをパソコンに送る。パソコンでは取得したコンテンツをパソコン上のブラウザを用いて表示する。

【0064】

また、ゲートウェイサーバは、認証サーバでトークンを用いて読み出して取得したセッションＩＤをパソコンに送り、パソコンはパソコン上でセッションＩＤのＣｏｏｋｉｅを登録しておく。これにより、図１６に示すように、次回からＣｏｏｋｉｅに登録されたセッションＩＤを用いてパソコンからコンテンツを要求する。そして、パソコンは、セッションＩＤをゲートウェイサーバを介して認証サーバに送り、認証サーバがセッションＩＤを読み出すことができれば、コンテンツサーバＵＲＬ及びユーザＩＤを読み出すことができ、コンテンツを取得することができる。

【0065】

本実施例のトークン型の双方向ワンタイムＩＤ認証システムでは、上記の説明のように携帯端末で双方向ワンタイムＩＤ認証を行い、トークンを入力することにより、Ｗｅｂブラウザを持っている端末ならどのような端末であっても、コンテンツサーバにアクセスできる。すなわち、専用のアプリケーションプログラムがインストールされていなくてもコンテンツサーバを利用することができる。

【0066】

なお、上記実施例１や実施例２でゲートウェイサーバとコンテンツサーバとがインターネットを介して接続されている場合には、ユーザＩＤが流出するのを防ぐため、ここでもゲートウェイサーバとコンテンツサーバの間で双方向ワンタイムＩＤ認証を行うことにより、経路上のユーザの匿名性をさらに保証することができる。また、ユーザを認証するサーバとコンテンツを提供するサーバとを分離するものとして説明しているが、これらを一体にしたコンテンツ提供システムを構築してもよい。また、本システムでは、携帯端末を紛失した場合に認証サーバで管理されている認証キーを無効にする装置を用意する。これは、万一、携帯端末を紛失してしまった場合に第三者により不正利用されるのを防ぐためである。

【産業上の利用可能性】

【0067】

本システムは、経路上のユーザの匿名性を保証してコンテンツサーバにおいてユーザを特定するモデルと、経路上及びコンテンツサーバにおいてユーザの匿名性を保証するモデルの２種類に利用することができる。

【0068】

経路上のユーザの匿名性を保証してコンテンツサーバにおいてユーザを特定するモデルは、経路上では匿名性が保障されているが、認証サーバによりコンテンツサーバのユーザＩＤを特定できるモデルとして構成される。コンテンツサーバには、必要な個人情報を登録しているため、ユーザＩＤから必要な個人情報を取り出すことができる。ユーザは個人情報を送信する必要はない。個人情報の例としては、名前、住所、生年月日、決済に使える銀行口座番号、クレジット番号などが挙げられる。このモデルとしては、インターネットバンキングモデル（図１８参照）や仮想店舗モデル（図１９参照）、競馬のインターネット投票モデル（図２０参照）、インターネット航空券発券モデル（図２１参照）等が挙げられる。

【0069】

インターネットバンキングモデルは、ユーザＩＤ、パスワード、口座番号などを携帯から入力することなくインターネットバンキングシステムが提供するサービスを利用することができる。また、仮想店舗モデルは、ユーザＩＤ、パスワード、銀行口座番号、クレジット番号などを携帯から入力することなく仮想店舗が提供するオンラインショッピングサービスを利用することができる。また、競馬のインターネット投票では、ユーザの指示でユーザの銀行口座で決済して馬券を購入し、レース終了後には自動的に配当金がユーザの銀行口座に振り込まれる。インターネット航空券発券では、銀行口座番号あるいはクレジット番号により航空券を購入すると、利用ポイントがユーザに加算される。また貯まった利用ポイントを景品に交換することもできる。

【0070】

一方、経路上及びコンテンツサーバにおいてユーザの匿名性を保証するモデルは、コンテンツサーバには、ユーザＩＤを含めて個人情報が何も登録されていない。そして、コンテンツサーバへは匿名性を保障したままアクセスできるモデルとして構成される。このモデルとしては、電子投票モデル（図２２参照）、電子アンケートモデル（図２３参照）等が挙げられる。電子投票モデルは、電子投票サーバでは投票された結果のみをデータベースに記録し、どのユーザが投票したかは知りえない。一度投票したユーザは再投票が出来ないように認証サーバで設定する。投票管理機関は、有権者が匿名性を保って電子投票システムにアクセスできるように、安全な方法で携帯端末用のアプリケーションと認証キーを有権者に配布する。また、電子アンケートモデルは、記入されたアンケートのみをデータベースに記録し、誰が記入したかは知りえない。一度アンケートに記入したユーザは再度記入が出来ないように認証サーバで設定する。アンケート実施機関は、アンケート回答者が匿名性を保って電子アンケートサーバにアクセスできるように、安全な方法で携帯端末用のアプリケーションと認証キーをアンケート回答者に配布する。

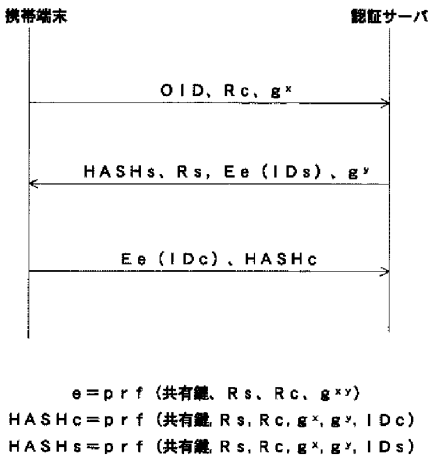
【図面の簡単な説明】

【0071】

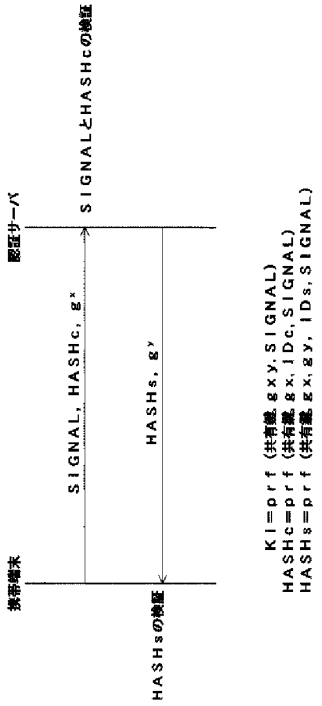
【図1】双方向ワンタイムＩＤ認証について説明するシーケンス図
【図2】双方向ワンタイムＩＤ認証について説明するシーケンス図
【図3】双方向ワンタイムＩＤ認証について説明するシーケンス図
【図4】本発明の第１及び第２実施例での初期段階を示す図
【図5】本発明の第１及び第２実施例での認証キーを取得するまでのプロセスを示す図
【図6】本発明の第１実施例でのセッションＩＤを取得するまでのプロセスを示す図
【図7】本発明の第１実施例でのコンテンツを取得するまでのプロセスを示す図
【図8】本発明の第２実施例でのトークンを取得するまでのプロセスを示す図
【図9】本発明の第２実施例でのコンテンツを取得するまでのプロセスを示す図
【図10】本発明の第１実施例での認証キーを取得するまでのシーケンスを示す図
【図11】本発明の第１実施例でのセッションＩＤを取得するまでのシーケンスを示す図
【図12】本発明の第１実施例でのコンテンツを取得するまでのシーケンスを示す図
【図13】本発明の第１実施例での自動的に再認証を行うシーケンスを示す図
【図14】本発明の第２実施例でのトークンを取得するまでのシーケンスを示す図
【図15】本発明の第２実施例でのセッションＩＤとコンテンツを取得するまでのシーケン

スを示す図
【図16】本発明の第２実施例でのＣｏｏｋｉｅ登録されたセッションＩＤを用いてコンテンツを取得するまでのシーケンスを示す図
【図17】本発明の第２実施例でのマニュアルで再認証を行うシーケンスを示す図
【図18】本発明のシステムをインターネットバンキングモデルに利用した様子を示す図
【図19】本発明のシステムを仮想店舗モデルに利用した様子を示す図
【図20】本発明のシステムを競馬のインターネット投票モデルに利用した様子を示す図
【図21】本発明のシステムをインターネット航空券発券モデルに利用した様子を示す図
【図22】本発明のシステムを電子投票モデルに利用した様子を示す図
【図23】本発明のシステムを電子アンケートモデルに利用した様子を示す図
【図24】従来のインターネット経由で電子商取引や金銭取引等のサービスを提供するコンテンツサーバとユーザとの間で行われる固定情報を使った認証手段を示す図

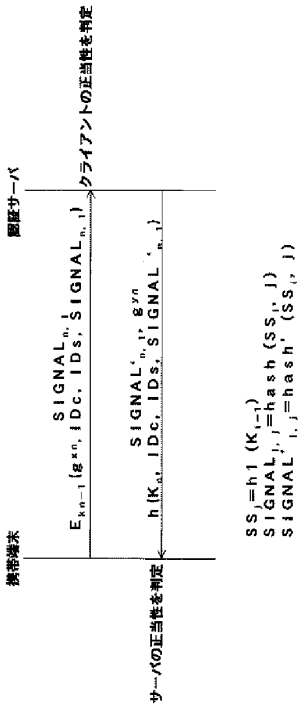
【図1】



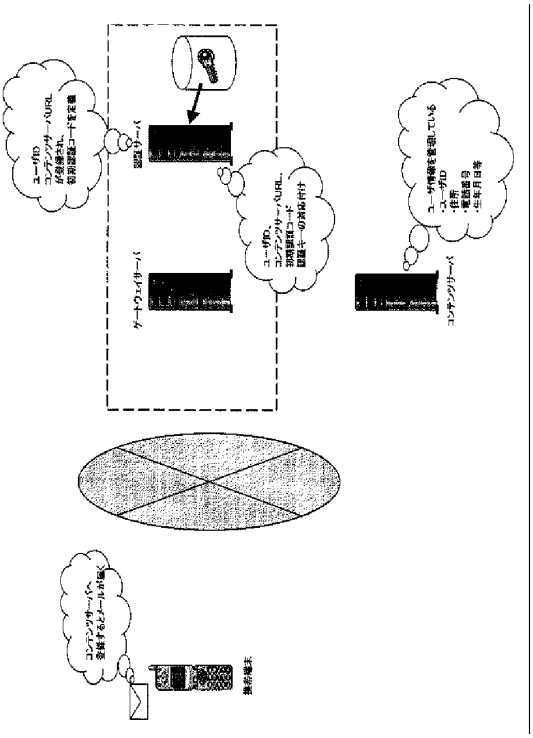
【図2】



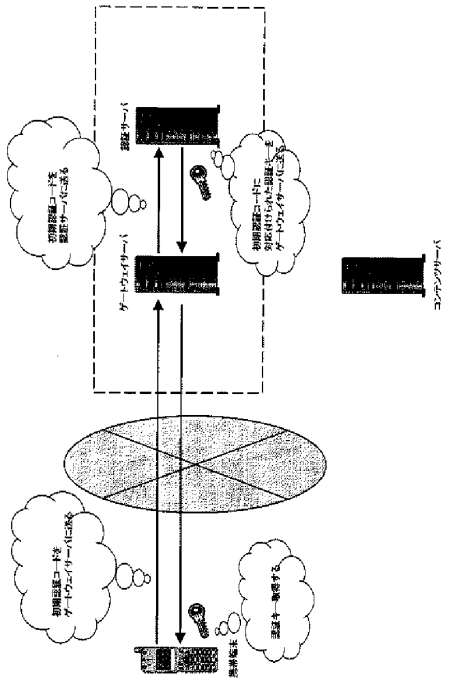
【図3】


認証サーバ
携帯端末
クライアントの正当性を判定
サーバの正当性を判定
SIGNAL n-1
E k n-1 (g x n , IDc, IDs, SIGNAL n-1)
SIGNAL' n-1
h (K n-1 , IDc, IDs, SIGNAL ' n-1)
g y n
SS j =h1 (K i-1)
SIGNAL j, j =hash (SS i, j)
SIGNAL' i, j =hash' (SS i, j)

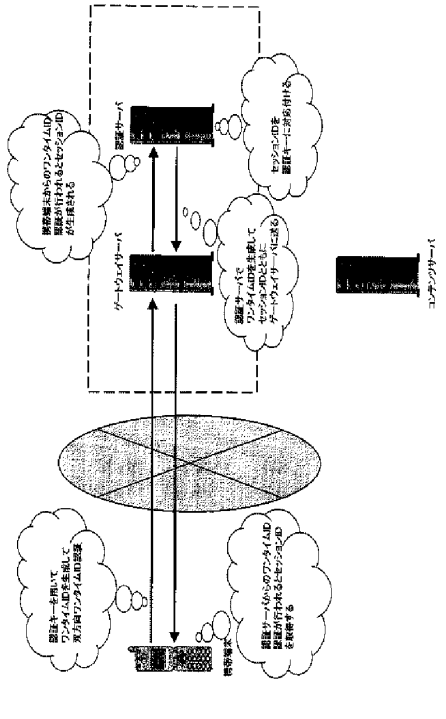
【図4】



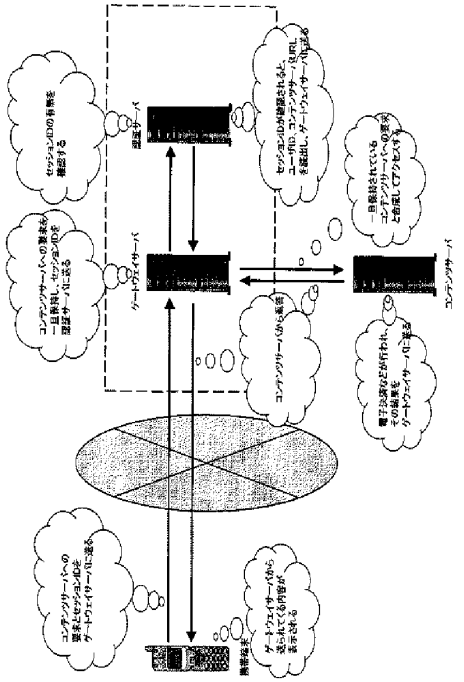
【図5】



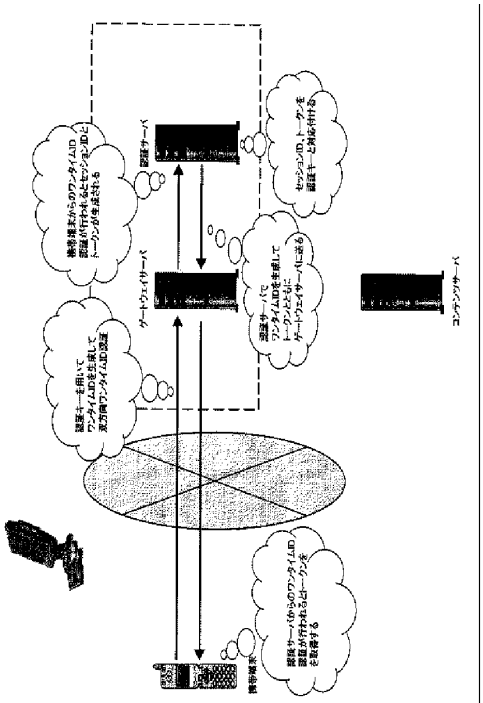
【図6】



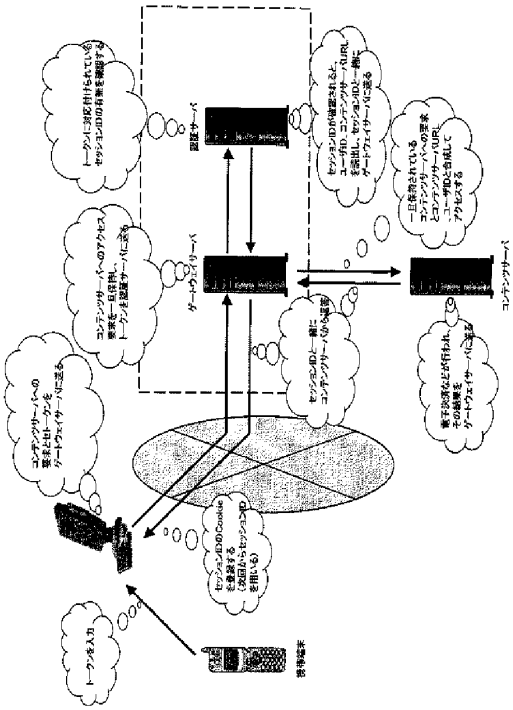
【図7】



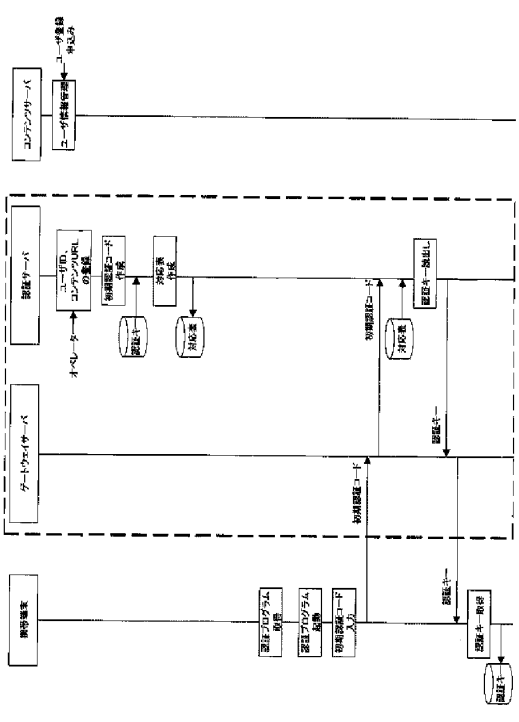
【図8】



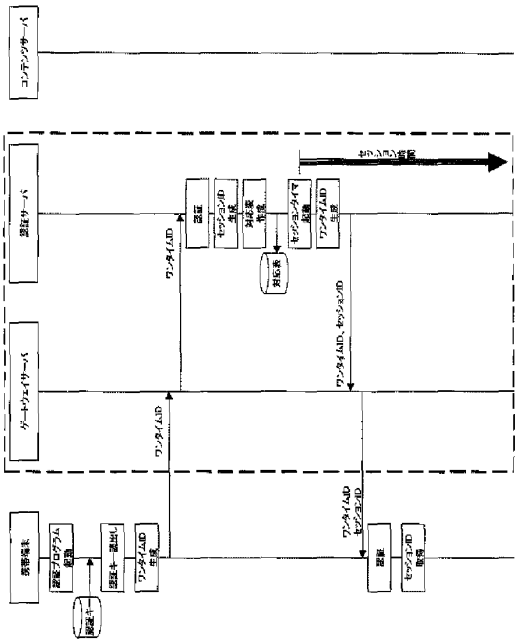
【図9】



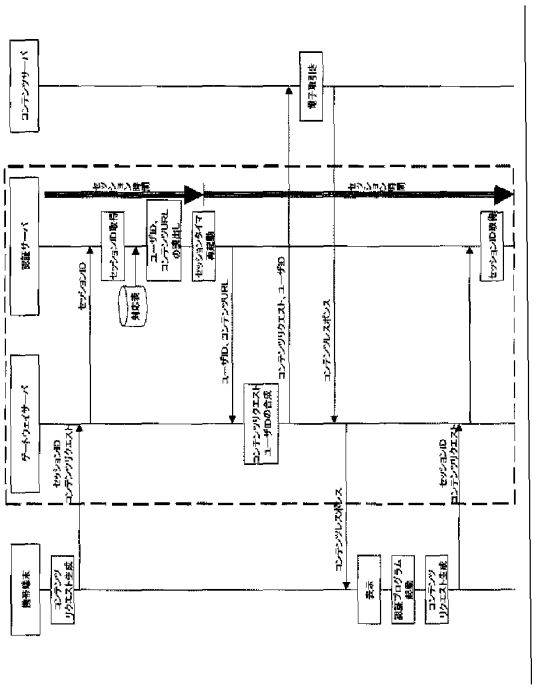
【図10】



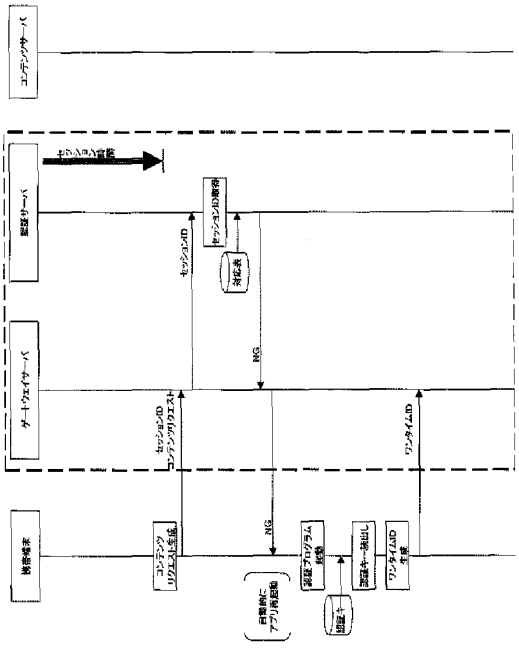
【図11】



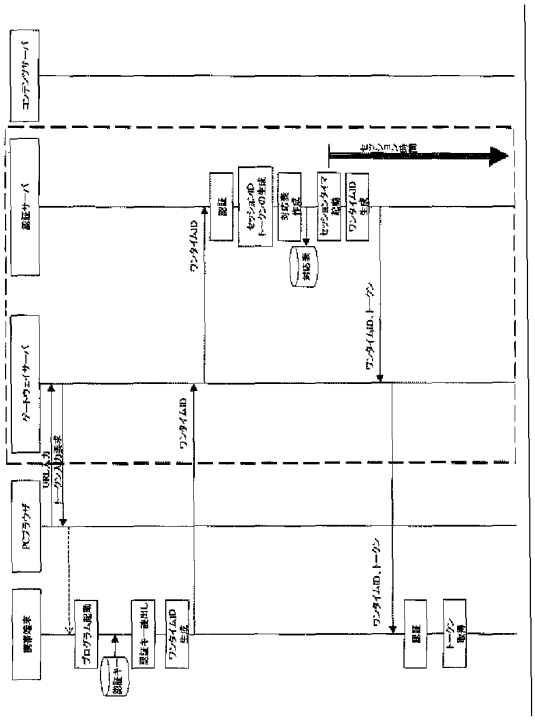
【図12】



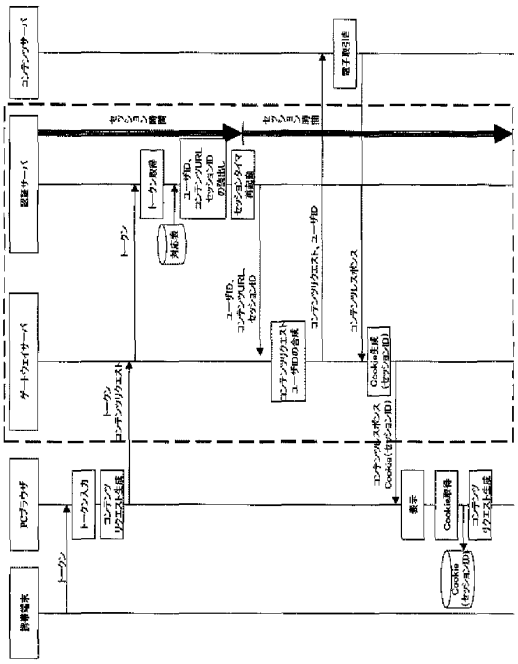
【図13】



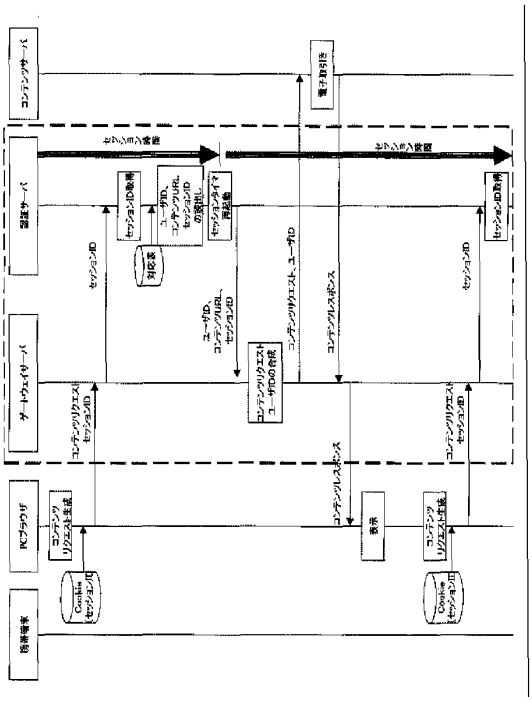
【図14】



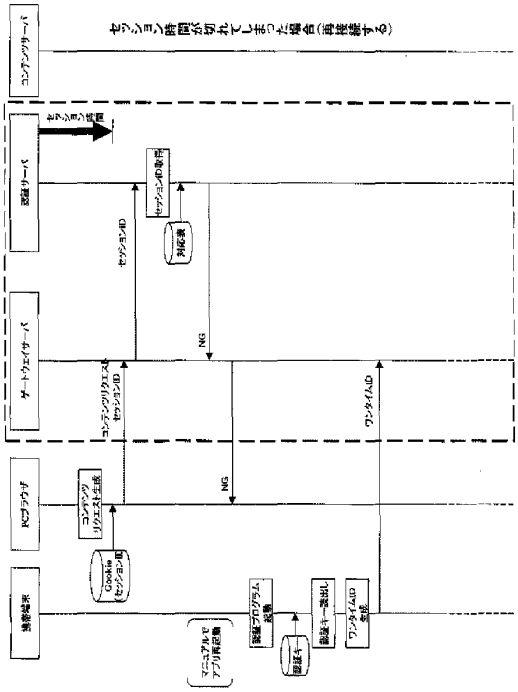
【図15】



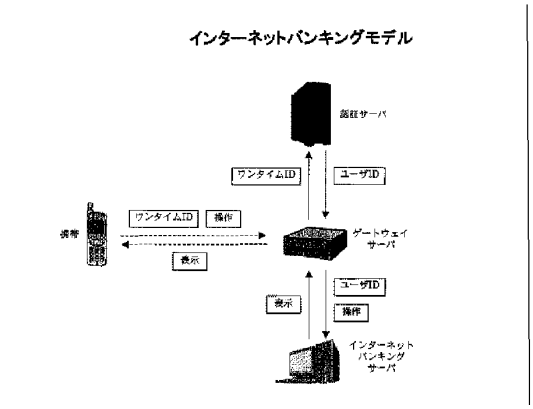
【図16】



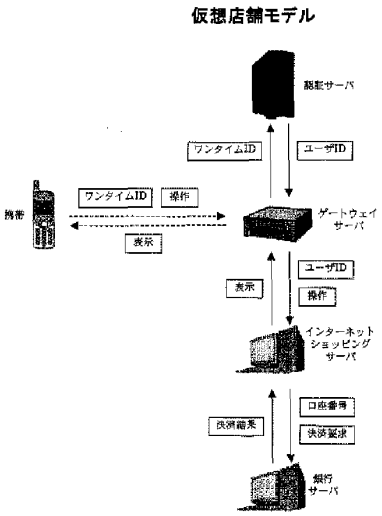
【図17】



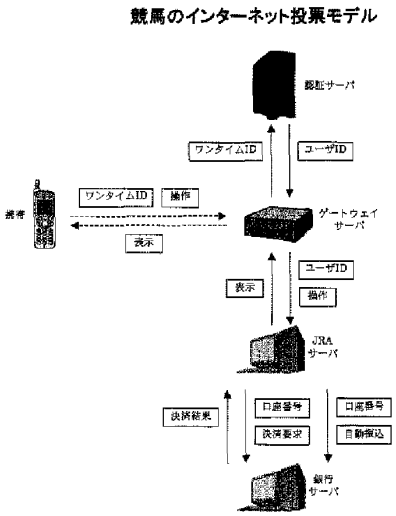
【図18】



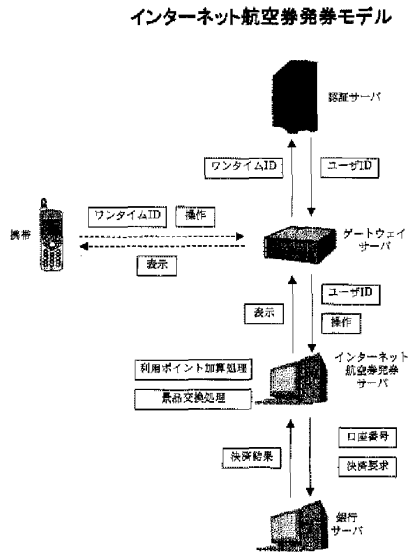
【図19】



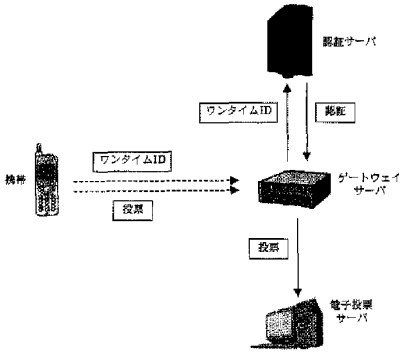
【図20】



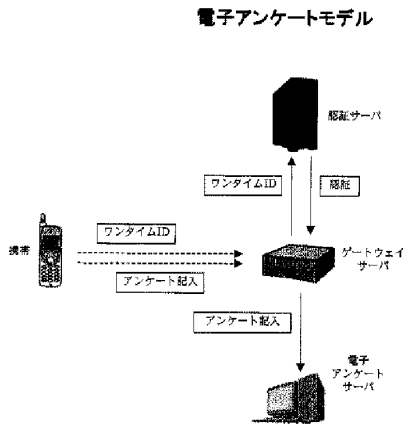
【図21】



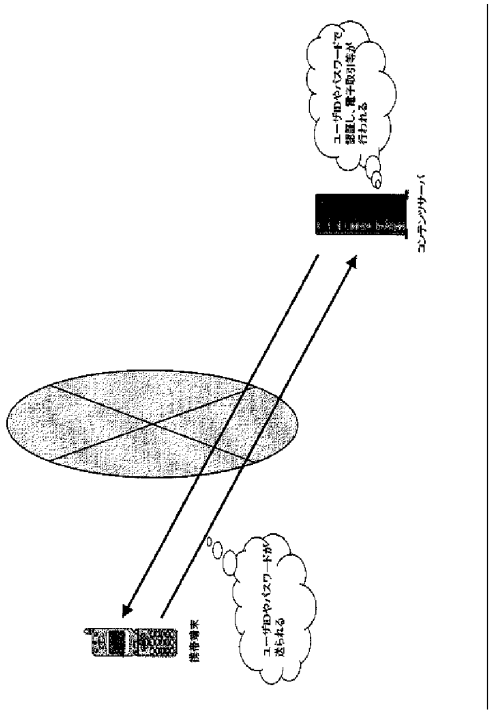
【図22】



【図23】


電子アンケートモデル
認証サーバ
ワンタイムID
認証
携帯
ワンタイムID
ゲートウェイ
サーバ
アンケート記入
アンケート記入
電子
アンケート
サーバ

【図24】


コンテンツサーバ
携帯端末

Patent Translate
Powered by EPO and Google

Notice

This translation is machine-generated. It cannot be guaranteed that it is intelligible, accurate, complete, reliable or fit for specific purposes. Critical decisions, such as commercially relevant or financial decisions, should not be based on machine-translation output.

DESCRIPTION JP2006155263

【課題】

The present invention utilizes existing authentication server for performing personal authentication based on the user ID and password, economical construction having high security authentication system using the one-time ID. A user is, in the case of performing the identity authentication, enter the user ID of its own to the one-time ID generation device 1 0. Onetime ID generating unit 1 0 generates the one-time ID and a user ID and the current time that has been input. The user then sends an authentication request including the above-described one-time ID and password from the terminal device 20 to the authentication server 30. Authentication server 30 transmits the including the one-time ID in the authentication request conversion request to the conversion server 40. The conversion server 40 calculates a user ID and a one-time ID and the current time is included in the conversion request, and returns the authentication server 30. The authentication server 30, by comparing the password registered in the authentication information storage section 35 in association with the user ID, and password in the authentication request, performs user authentication. .FIELD 7

One-time ID authentication system, an authentication server, the conversion server, one-time ID authentication method and program

[0001]

[0001] The present invention relates to a personal authentication technology in a network system, in particular, by using each time a different user ID for each logon (onetime ID), relates to personal authentication technology increase the security level.

[0002]

[0002] The personal authentication system in a network system, various ones have been known. 1 3 is a block diagram showing a conventional most commonly in the personal authentication system that is utilized configured. Referring to the figure, personal authentication system includes an authentication server 1 00, and a terminal device 200 used by a user, they are connected to each other via the Internet, a network 300 such as LAN.

[0003]

[0003] In personal authentication system shown in FIG. 1 3, the user of the terminal device 200, when performing authentication, an authentication request including the own user ID and password, and transmitted from the terminal device 200 to the authentication server 1 00 . Authentication means 1 01 of the authentication server 1 00, upon via the transmitting and receiving unit 1 02 receives an authentication request from the terminal apparatus 200, referring to the authentication information storage unit 1 03 and the user ID and password for each user is registered in association and, perform personal authentication. That is, a password in association with the user ID in the authentication request is registered in the authentication information storage unit 1 03, compares the password in the authentication request, if they match, the authentication succeeds, both the mismatch case, the authentication failure.

[0004]

[0004] However, personal authentication system shown in FIG. 1 3, for each use the same user ID and password, there is a problem in terms of security. Therefore, I like to use different passwords (one-time password) each time the personal authentication system shown in FIG. 1 4 has been proposed (e.g., see Patent Document 1).

[0005]

[0005] Referring to FIG. 1 4, personal authentication system includes an authentication server 400, the terminal device 500 used by a user, and a one-time password generation unit 600, the authentication server 400 and the terminal device 500, the Internet, They are connected to each other via a network 700 such as a LAN.

[0006]

User [0006] terminal 500, when performing personal authentication, first, the one-time password generation unit 600 inputs the user ID of its own. Thus, the one-time password generation unit 600 generates a one-time password based on the input user ID and the current time, and displays the generated one-time password on the display section (not shown). Incidentally, one-time password generation apparatus 600, for example, be realized by a mobile phone incorporating a program for the one-time password generation.

[0007]

[0007] The user inputs and one-time password is displayed, the same and the own user ID to the terminal device 500. Thus, the terminal device 500 transmits an authentication request including the one-time password and user ID to the authentication server 400.

[0008]

[0008] Authentication unit 401 in the authentication server 400 receives the authentication request through the transceiver unit 402, passes the user ID contained in the authentication request to the one-time password generation unit 403, generating a one-time password to instruct. Thus, the one-time password generation unit 403 receives the current time from the clock 404, and generates a one-time password based on the current time and the above user ID. Then, a one-time password generated is compared with the one-time password included in the authentication request, if they match, the authentication succeeds, if they do not match, the authentication failure. JP 2002-259344 JP

[0009]

[0009] According to the authentication system described in Patent Document 1 described above, since different passwords are used each time, it is possible to higher security.

[001 0]

[001 0] Incidentally, even in the engine have already introduced the authentication server 1 00 as shown in FIG. 1 3, increased security is desired. To improve security, may be introduced personal authentication system that performs authentication using the one-time password as shown in FIG. 1 4, then, the cost becomes very high.

[001 1]

[001 1] [purpose of the invention] It is an object of the present invention have the authentication information storage unit in which the user ID and password are registered in association, by utilizing the existing authentication server for performing personal authentication based on the user ID and password, It is to such a high security authentication system using the one-time ID can be economically constructed.

[001 2]

[001 2] The first one-time ID authentication system according to the present invention, And the terminal device, a one-time ID authentication system comprising an authentication server with authentication information storage unit in which the user ID and password of a user are registered in association, and a conversion server, It said terminal device, Has a one-time ID generated based on the user ID and the current time, a structure for transmitting an authentication request including the password to the authentication server, The authentication server, When the authentication request from the terminal device is sent, to generate a translation request including the one-time ID in the authentication request, and sends the converted request the generation to said conversion server, the conversion request from the conversion server when a user ID is sent as a conversion result for, by comparing the password of password and said in authentication request registered in the authentication information storage unit in association with the user ID, if they match, the authentication has a configuration

that success, The conversion server, When the conversion request from the authentication server is sent, calculates a user ID on the basis of the one-time ID and the current time in the conversion request, to have a structure to return the user ID the calculated to the authentication server the features.

[001 3]

[001 3] The second of the one-time ID authentication system according to the present invention, in the first of the one-time ID authentication system, The generates a one-time ID based on the user ID and the current time input by the user of the terminal device, the one-time ID generating apparatus including a one-time ID generating means for displaying on the display unit the one-time ID to the said generated characterized by comprising.

[001 4]

[001 4] Third one-time ID authentication system according to the present invention, in the first one-time ID authentication system, A user ID storage unit by the user ID of the user of the terminal device is registered, The generates a one-time ID based on the user ID and the current time registered in the user ID storage unit, the one-time ID generation including the one-time ID generating means for displaying on the display unit the one-time ID to the said generated characterized by comprising a device.

[001 5]

[001 5] The fourth one-time ID authentication system according to the present invention, in the first to the third one-time ID authentication system, The authentication server, When the authentication request from the terminal device is sent, and a conversion request means for generating a conversion request including the one-time ID in the authentication request, transmits the converted request the generation to said conversion server, When the user ID as a conversion result for the conversion request from the conversion server is sent, it compares the password of password and said in authentication request registered in the authentication information storage unit in association with the user ID, If they match, characterized by comprising a comparison means for the authentication succeeds.

[001 6]

[001 6] The fifth one-time ID authentication system according to the present invention, in the fourth one-time ID authentication system, The conversion server, When the conversion request from the authentication server is sent, it calculates a user ID on the basis of the one-time ID and the current time in the conversion request, provided with a conversion means for transmitting the user ID to the calculated to the authentication server characterized in that was.

[001 7]

[001 7] Sixth onetime ID authentication system according to the present invention, in the second or third one-time ID authentication system, The one-time ID generation device, And functions holding unit at the time of dividing the day into multiple time zones, the one-time ID generation function for each time zone is stored, Of the one-time ID generation function stored in the function number storing unit, generate a one-time ID generation function for time zone including the current time, and the current time, the one-time ID based on the user ID and a one-time ID generation computing means for, The conversion server, And inverse function holding unit at the time of dividing the day into a plurality of time zones, the user ID calculating function for each time period is stored, When the conversion request from the authentication server is sent, of the user ID calculating function for each time period stored in said inverse function holding unit, a user ID calculating function for time zone including the current time When, characterized by comprising a current time, a user ID calculating arithmetic means for calculating a user ID on the basis of the one-time ID in said conversion request.

[001 8]

[001 8] The authentication server according to the present invention, And authentication information storage unit in which the user of the user ID and password has been registered in association with, When the authentication request including the user ID and password sent from the terminal device, generating a conversion request including the one-time ID in the authentication request, a conversion request means for transmitting a conversion request the generation to the conversion server , When the user ID as a conversion result for the conversion request from the conversion server is sent, it compares the password of password and said in authentication request registered in the authentication information storage unit in association with the user ID, If they match, characterized by comprising a comparison means for the authentication succeeds.

[001 9]

[001 9] conversion server according to the present invention, When the conversion request including the one-time ID is sent from the authentication server calculates a user ID on the basis of the one-time ID and the current time in the conversion request, and transmits the user ID to the calculated to the authentication server characterized by comprising a conversion means.

[0020]

[0020] one-time ID authentication method according to the present invention, Terminal device transmits the one-time ID generated based on the user ID and the current time, the authentication request including the password to the authentication server, The authentication server having an authentication information storage unit in which the user having the user ID and password are registered in association with the, when an authentication request from the terminal device is sent, including the one-time ID in the authentication request conversion generate a request, sends the converted request the generation to the conversion server, Returning said conversion server, when a conversion request from the authentication server is sent, calculates a user ID on the basis of the one-time ID and the current time in the conversion request, the user ID the calculated to the authentication server and, The authentication server, when the user ID is sent as a conversion result for the conversion request from the conversion server, a password of password and said in authentication request registered in the authentication information storage unit in association with the user ID comparing the door, if they match, characterized by a successful authentication.

[0021]

[0021] The first program according to the present invention, The computer with the authentication information storage unit in which the user having the user ID and password are registered in association, When the authentication request including the user ID and password sent from the terminal device, generating a conversion request including the one-time ID in the authentication request, translation request means for transmitting a conversion request the generation to the conversion server, When the user ID as a conversion result for the conversion request from the conversion server is sent, it compares the password of password and said in authentication request registered in the authentication information storage unit in association

with the user ID, If they match, to function as a comparison means for a successful authentication.

[0022]

[0022] The second program according to the present invention, The computer, When the conversion request including the one-time ID is sent from the authentication server calculates a user ID on the basis of the one-time ID and the current time in the conversion request, and transmits the user ID to the calculated to the authentication server to function as a conversion means.

[0023]

[0023] [action] When the user performs the authentication, send the authentication request from its own terminal device to the authentication server. The authentication request, and the one-time ID generated based on the user ID and the current time of the user, contains the password for the user. One-time ID, for each its generation time, since the value is different, it is possible to higher security. The authentication server receives the authentication request, generates including the one-time ID in the authentication request conversion request, and sends the conversion server. Conversion server, based on the one-time ID and the current time in the conversion request, calculates a user ID of the user, and returns the user ID calculated in the authentication server. The authentication server performs the user ID is returned, and password in the authentication request, the utilizing the authentication information storage unit personal authentication.

[0024]

According to [0024] the present invention, it becomes possible to economically configure security high personal authentication system using the one-time ID. The reason is that the conversion server to return the one-time ID contained in the authentication request sent from the terminal device to the user ID is provided, the one-time ID to the existing authentication server for performing personal authentication by user ID and password This is because the available in personal authentication using.

[0025]

[0025] With reference to drawings, embodiments of the present invention will be described in detail.

[0026]

[0026] [Description of Configuration of First Embodiment 1 is a block diagram showing an overall configuration of a first embodiment of the one-time ID authentication system according to the present invention. Referring to the figure, the one-time ID authentication system of this embodiment, the one-time ID generation unit 10 used by a user, the terminal device 20 in which the user uses, the authentication server 30, a conversion server 40 wherein, the terminal apparatus 10, the authentication server 30 and the conversion server 40 are connected to each other via the Internet, a network 50 such as a LAN.

[0027]

[0027] onetime ID generating unit 10 generates a one-time ID based on the user ID and the current time input by the user, a function to be presented to the user.

[0028]

[0028] FIG. 2 is a block diagram showing a configuration example of a one-time ID generating apparatus 10 having the function described above, an input section 11 of the numeric keys or the like, a one-time ID generating unit 12, a clock that displays the current time 16, and a display portion 17 such as LCD.

[0029]

[0029] onetime ID generating unit 12 includes a function storage unit 13, a calculating unit 14, and a current time input means 15.

[0030]

[0030] time input unit 1 5 has a function of inputting the current time from the clock 1 6. In this embodiment, the time input unit 1 5, when the timepiece 1 6 is displaying: minutes: Of the second, time: shall enter a fraction only. In other words, time input means 1 5, to enter the time in minutes.

[0031]

[0031] in the function storage unit 1 3, the function to use in generating the one-time ID (one-time ID generation function) is stored.

[0032]

[0032] calculating means 1 4, the user ID input from the input unit 1 1, for the current time the time input unit 1 5 is input, according to the one-time ID generation function stored in the function storage section 1 3 It was calculated onetime ID by performing a calculation, a function of displaying the one-time ID calculated in the display unit 1 7.

[0033]

[0033] In addition, the one-time ID generation means 1 2 of the one-time ID generating device 1 0, are those that can be realized by a CPU (computer), if implemented by a computer, for example, in the following manner. Disc for recording a program for causing a computer to function as a one-time ID generating unit 1 2, a semiconductor memory, prepared other recording medium, to read the program in the computer. The computer, by controlling its operation according to the read program, on the self computer, to implement the one-time ID generating unit 1 2. Further, the one-time ID generation apparatus 1 0 may also be realized by utilizing a portable telephone with a built-in CPU. That is, providing a recording medium such as a recording disk a program for operating the CPU as a onetime ID generating unit 1 2, to read the program to the CPU. The CPU, by controlling its operation according to the read program to realize the one-time ID generating unit on the own CPU.

[0034]

[0034] The terminal device 20 has function for sending an authentication request including the one-time ID and the password to the authentication server 30, a function for presenting the authentication result sent from the authentication server 30 to the user.

[0035]

[0035] FIG. 3 is a block diagram showing a configuration example of a terminal device 20 having the function described above, a transmitting and receiving unit 21, a control unit 22, an input unit 23 such as a keyboard, a display unit 24 such as an LCD It is equipped with a.

[0036]

[0036] transmitting and receiving means 21 has a function of exchanging data via a network 50.

[0037]

[0037] The control unit 22 has a function of transmitting the input unit 23 function for generating an authentication request including the one-time ID and password input, the generated authentication request via the communication means 21 to the authentication server 30, having like function of displaying an authentication result sent from the authentication server 30 on the display unit 24.

[0038]

[0038] In addition, the terminal device 20 is as it can be implemented by a computer such as a personal computer, if implemented by a computer, for example, in the following manner. Disc for recording a program for causing a computer to function as a terminal device, a semiconductor memory, prepared other recording medium, to read the program in the computer. The computer, by controlling its operation according to the read program, on the self computer, realizes transmission and reception unit 21, the control unit 22.

[0039]

[0039] The authentication server 30, when the authentication request including the one-time ID and password sent from the terminal device 20 acquires the user ID corresponding to the one-time ID by using the conversion server 40, the user It has a function of performing authentication based on the ID and the password in the authentication request.

[0040]

[0040] FIG. 4 is a block diagram showing a configuration example of the authentication server 30 having the functions described above, a transmitting and receiving unit 31 , an authentication unit 32, and an authentication information storage unit 35.

[0041]

[0041] in the authentication information storage unit 35, as shown in FIG. 5, the user ID of the user, password, access rights, name, ... it is registered in association.

[0042]

[0042] transmitting and receiving means 31 has a function of exchanging data via a network 50.

[0043]

[0043] authentication means 32 includes a translation request unit 33, the comparing means 34.

[0044]

[0044] conversion request means 33, when receiving an authentication request from the terminal device 20 via the transmitting and receiving unit 31 transmits a containing the one-time ID in the authentication request conversion request to the conversion server 40, the conversion request having the ability to pass the user ID is returned from the conversion server 40 in response to the comparison means 34. Translation request unit 33 has a configuration that is not provided in the authentication server 100 shown in FIG. 13, in the case of realizing the authentication server 30 by using the existing authentication server 100 needs to incorporate this configuration.

[0045]

[0045] comparing means 34 compares the password in association with the user ID is registered in the authentication information storage section 35 passed from the translation request unit 33, and a password in the authentication request from the terminal device 20, If they match, the authentication succeeds, if they do not match, has the function of the authentication failure. Comparing means 34 has a configuration that is provided to the authentication server 100 shown in FIG. 13.

[0046]

[0046] In addition, the authentication server 30, are those that can be implemented by a computer, if implemented by a computer, for example, in the following manner. Disc for recording a program for causing a computer to function as the authentication server, a semiconductor memory, prepared other recording medium, to read the program in the computer. Computer controls its own operation in accordance with the read program, on its own computer, sending and receiving means 31, to achieve the authentication means 32.

[0047]

[0047] conversion server 40, when the conversion request from the authentication server 30 including the one-time ID is sent, it calculates a user ID on the basis of the above one-time ID and the current time, and returns the user ID calculated It has a function.

[0048]

[0048] FIG. 6 is a block diagram illustrating an exemplary configuration of a conversion server 40 having the function described above, comprises a transceiver unit 41, a conversion unit 42, and a clock 46 that displays the current time.

[0049]

[0049] transmitting and receiving means 41 has a function of transmitting and receiving data via the network 50.

[0050]

[0050] conversion unit 42 includes an operation unit 43, an inverse function storage unit 44, and a time input section 45.

[0051]

[0051] time input unit 45 has a function of inputting the current time in minutes from the clock 46.

[0052]

[0052] Conversely function storage unit 44, the one-time ID and the function for obtaining the user ID from the current time (user ID calculating functions) is stored.

[0053]

[0053] calculating means 43, upon receiving a conversion request sent from the authentication server 30 via the transmitting and receiving unit 41, the one-time ID contained in it, in minutes

time input unit 45 is input current has a time, a function of calculating a user ID on the basis of the functions for the user ID calculating held in the inverse function holding unit 44, and transmits the user ID, which is calculated to the authentication server 30.

[0054]

[0054] In addition, the conversion server 40, are those that can be implemented by a computer, if implemented by a computer, for example, in the following manner. Disc for recording a program for causing a computer to function as a conversion server, a semiconductor memory, prepared other recording medium, to read the program in the computer. The computer, by controlling its operation according to the read program, on the self computer, transceiver means 41 , realizing the conversion means 42.

[0055]

[0055] [Description of Operation of First Embodiment Next, with reference to the drawings, the operation of this embodiment will be described in detail.

[0056]

[0056] The user of the terminal device 20, when performing personal authentication, and starts the one-time ID generation unit 10, inputs the user ID of itself from the input unit. 11 (a in Fig. 7).

[0057]

[0057] One-time ID generating device 10 onetime ID generating means 12, when activated, becomes an input waiting state of the user ID, the user ID is input from the input unit 11 by the user, time input means 15 enter the current time in minutes from the clock 16 using the (step S81 , S82 in FIG. 8). Thereafter, generation operation means 14, the one-time ID generation function stored in the function storage unit 13, a user ID input by the user, time input means 15 the one-time ID on the basis of the current time entered (step S83). Here, the function for one-time ID generation, for example, may be employed functions such as (onetime ID) = (User ID) ×

(current time). Thereafter, computing unit 1 4 displays the one-time ID calculated in the display section 1 7 (step S 84).

[0058]

[0058] When the user has the one-time ID is displayed on the display unit 1 7, and inputs the one-time ID and password displayed on the terminal device 20 (b in FIG. 7, c). Control means 22 in the terminal device 20, when the one-time ID and a password are inputted from the input unit 23, and transmits the containing them authentication request to the authentication server 30 (d- in FIG. 7).

[0059]

[0059] conversion request means 33 of the authentication server 30 receives the authentication request sent from the terminal device 20 via the transmitting and receiving unit 31 , generates a conversion request including the one-time ID in the authentication request and it sends it to the conversion server 40 (e in step S 91 , S 92 and 7 in FIG. 9). Thereafter, conversion request means 33, a return waiting state of the conversion result (user IDs) (step S 93).

[0060]

[0060] On the other hand, converter 42 in the conversion server 40 receives the conversion request from the authentication server 30 via the transmitting and receiving unit 41 , as shown in the flowchart of FIG. 1 0, by using the first time input means 45 enter the current time in minutes from the clock 46 (step S1 01). Thereafter, computing unit 43, and functions for the user ID calculating held in the inverse function holding unit 44, and the current time in minutes time input unit 45 is input, the user ID based on the one-time ID in the conversion request calculates and returns the user ID which is calculated to the authentication server 30 (f in step S 1 02, S 1 03 and FIG. 7). Here, the user ID calculating functions stored in the inverse function holding unit 44 is an inverse function of the one-time ID generation function stored in the function storage unit 1 3 of the one-time ID generating device 1 0, for example, , one-time ID generation function is, if the (one-time ID) = (user ID) $\times$ (the current time), the function for the user ID calculation, (user ID) = (one-time ID) $\div$ (the current time) to become. However, the function holding unit 1 3, the one-time ID generation function held by the inverse function holding unit 44, the function for the user ID calculating, not limited to the example described above.

[0061]

[0061] conversion request means 33 of the authentication server 30 in the return waiting state of the conversion result, and a result conversion sent from the conversion server 40 (user ID) is received via the transmitting and receiving means 31 , comparison means it pass to the 34. Thus, comparing unit 34, the authentication information storage section 35, it retrieves the password registered in association with the user ID, and compared with the password in the authentication request sent from the terminal device 20 (in FIG. 9 step S94). Then, if they match notifies the authentication success to the authentication requesting terminal device 20 (step S95 is YES, S 96), in the case of disagreement, and notifies the authentication failure to the terminal device 20 (step S95 is NO , g of S97 and 9). Even if the user ID corresponding to the authentication information storage unit 35 is not registered, the authentication failure.

[0062]

[0062] Control unit 22 in the terminal device 20 receives via the communication means 21 an authentication result (authentication success or authentication failure), and displays it on the display unit 24. If the authentication success is displayed, the user of the terminal device 20, it means that acquired the access right to the system, it is possible to access the system. In contrast, if the authentication failure is displayed, the user performs the operation described above again.

[0063]

[0063] In the embodiment described above, converter 42 in the conversion server 40, upon receiving a conversion request from the authentication server 30, based on a one-time ID in the conversion request, to the present time user although the ID to calculate only one, and the user ID corresponding to the current time, asked two of the user ID of the user ID corresponding to one minute before the time than the current time, those two user ID it may be returned to the authentication server 30. Then, the comparison unit 34 within the authentication server 30 in which two user ID is returned, either one of the two password registered in the authentication information storage section 35 in association with the two user ID, if they match the password in the authentication request, it is determined that the authentication is successful. By doing so, the user of the operating time (time from the generation of the one-time ID, until the user inputs the

one-time ID and password to the terminal device 20), a generation time of the one-time ID, the conversion server even if the difference between the reception time of the conversion request occurs at 40, the difference is within the 1 minute, it can be a successful authentication.

[0064]

[0064] Further, in the embodiment described above, the function holding unit 1 3, inverse function holding unit 44 respectively onetime ID generation function have been adapted to store one by one function for the user ID calculating a plurality of one time ID generation function may be stored functions for the user ID calculating, it may be changed using function depending on the time zone. When doing so, for example, dividing one day into a plurality of time periods, different one-time ID generation function for each time period, a function for calculating a user ID function storage unit 1 3, the customer function storage unit 44 It is registered. In the computing unit 1 4 of the one-time ID generating device 1 0, when generating the one-time ID at step S83 in FIG. 8, of the one-time ID generation function for each time zone is stored in the function storage unit 1 3, and the one-time ID generation function for time zone including the current time, and the current time, and generates a one-time ID with the user ID. Further, the arithmetic unit 43 in the conversion server 40, when calculating the user ID in step S1 02 of FIG. 1 0, of the function for the user ID calculating stored in the inverse function holding unit 44, the time zone including the current time and user ID is calculated for the function of the use, to calculate the current time, the user ID from a one-time ID.

[0065]

[0065] [Effect of the First Embodiment According to this embodiment, it is possible to economically configure security high personal authentication system using the one-time ID. This is because, by providing the conversion server 40 for returning the one-time ID contained in the authentication request sent from the terminal device 20 to the user ID, existing authentication server 30 for authentication by the user ID and password the is because the available in personal authentication using the one-time ID.

[0066]

[0066] Further, according to the present embodiment, it is possible to extremely high security. The reason is because they like to use a different one-time ID generation function, a function for

the user ID calculated for each time.

[0067]

[0067] Second Embodiment Next, a description will be given of a second embodiment of the one-time ID authentication system according to the present invention. One-time ID authentication system of this embodiment, the one-time ID authentication system shown in FIG. 1 , in place of the one-time ID generating apparatus 1 0 shown in FIG. 2, the one-time ID generator 1 0a shown in FIG. 1 1 It is achieved by the use.

[0068]

[0068] onetime ID generator 1 0a shown in FIG 1 1 used in this embodiment, instead of the one-time ID generating unit 1 2, that it includes a one-time ID generating unit 1 2a, and a user ID storage unit 1 9 There points are added are different from the one-time ID generating unit 1 2 shown in FIG.

[0069]

The [0069] user ID holding unit 1 9, the user ID of the user of the terminal device 20 is registered.

[0070]

[0070] onetime ID generating 1 2a are that the user ID input means 1 8 for inputting a user ID stored in the user ID holding unit 1 9 has been added, is different from the one-time ID generating unit 1 2.

[0071]

[0071] Next, the operation of this embodiment. The operation other than the one-time ID

generator 1 2a are the same as the first embodiment, here will be described only the operation of the one-time ID generator 1 2a.

[0072]

User [0072] The terminal device 20, when performing personal authentication, activates the one-time ID generator 1 0a. As a result, the one-time ID generating means 1 2a of the one-time ID generating device 1 0a, enter the current time in minutes from the clock 1 6 using the time input means 1 5, further, a user ID by using the user ID input means 1 8 from the holding portion 1 9 to enter a user ID (step S1 21 , S1 22 in FIG. 1 2). Thereafter, computing unit 1 4 of the one-time ID generating means in 1 2a is a one-time ID generation function stored in the function storage unit 1 3, the current time the time input unit 1 5 is input, the user ID input unit 1 8 inputs and based on the user ID, and generates a one-time ID, and displays the generated one-time ID on the display section 1 7 (step S1 23, S1 24).

[0073]

[0073] [Effects of the Second Embodiment According to the present embodiment, in addition to the effects of the first embodiment, it can be made easier to generate operation onetime ID performed by the user. The reason is that the one-time ID generation unit 1 2a is provided with a user ID storage unit 1 9 by the user ID is registered, when the user the one-time ID generation, there is no need to input the user ID.

[0074]

[0074] can be used for authentication systems required high security.

[0075]

[0075] is a block diagram showing an overall configuration example of a first embodiment of the one-time ID authentication system according to the present invention. Configuration example of the one-time ID generating apparatus 1 0 is a block diagram showing the. It is a block diagram showing a configuration example of the terminal device 20. It is a block diagram showing a

configuration example of the authentication server 30. Is a diagram showing an example of contents of the authentication information storing section 35. It is a diagram illustrating a configuration example of a conversion server 40. It is a diagram for explaining the operation of the first embodiment. It is a flowchart illustrating a processing example of the one-time ID generator 1 0. It is a flowchart illustrating a processing example of the authentication server 30. It is a flowchart illustrating a processing example of a conversion server 40. A configuration example of a one-time ID generator 1 0a used in the second preferred embodiment of a one-time ID authentication system in the present invention is a block diagram showing. It is a block diagram showing a processing example of the one-time ID generator 1 0a. Using a conventional user ID and password is a block diagram showing an example of a personal authentication system. Is a diagram showing an example of a personal authentication system that uses a conventional user ID and one-time password.

Description of the code

[0076] 1 0,1 0a ... one-time ID generation device 1 1 ... input section 1 2,1 2a ... one-time ID generating means 1 3 ... function holding section 1 4 ... computing means 1 5 ... time input means 1 6 ... Clock 1 7 ... display unit 1 8 ... user ID input means 1 9 ... user ID holding section 20 ... terminal equipment 21 ... transmitting and receiving means 22 ... control means 23 ... input section 24 ... display unit 30 ... authentication server 31 ... transmitting and receiving means 32 ... authentication means 33 ... conversion request means 34 ... comparison means 35 ... authentication information storage unit 40 ... conversion server 41 ... transmitting and receiving means 42 ... conversion means 43 ... computing means 44 ... inverse function holding section 45 ... time input means 46 ... Clock 50 ... Network

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-155263
(P2006-155263A)
(43)公開日　平成18年6月15日(2006.6.15)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B085
H04L 9/32	(2006.01)	H04L	9/00	673A	5J104

審査請求 有　請求項の数 11　ＯＬ　（全 16 頁）

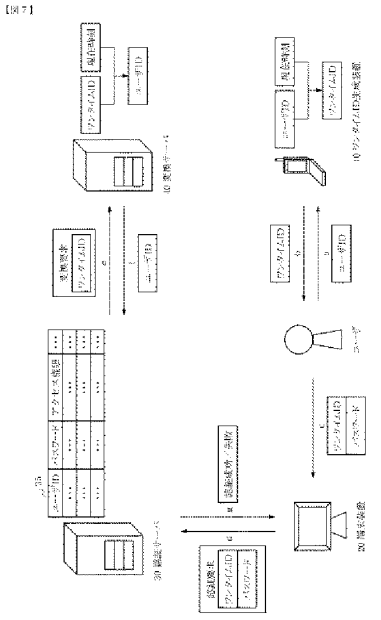
(21)出願番号　特願2004-345458 (P2004-345458)
(22)出願日　平成16年11月30日 (2004.11.30)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100088959
弁理士　境　廣巳
(72)発明者　緒方　真一郎
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B085 AE02 AE03 AE23 BA06 BG07
5J104 KA01 NA05 PA07

(54)【発明の名称】ワンタイムＩＤ認証システム、認証サーバ、変換サーバ、ワンタイムＩＤ認証方法及びプログラム

(57)【要約】
【課題】　ユーザIDとパスワードとに基づいた本人認証を行う既存の認証サーバを利用し、ワンタイムIDを用いたセキュリティの高い本人認証システムを経済的に構成する。
【解決手段】　ユーザは、本人認証を行う場合、ワンタイムID生成装置10に自身のユーザIDを入力する。ワンタイムID生成装置10は、入力されたユーザIDと現在時刻とからワンタイムIDを生成する。その後、ユーザは、上記ワンタイムIDとパスワードとを含む認証要求を端末装置20から認証サーバ30へ送る。認証サーバ30は、認証要求中のワンタイムIDを含んだ変換要求を変換サーバ40へ送信する。変換サーバ40は、変換要求に含まれているワンタイムIDと現在時刻とからユーザIDを算出し、認証サーバ30に返却する。認証サーバ30は、上記ユーザIDに対応付けて認証情報記憶部35に登録されているパスワードと、認証要求中のパスワードとを比較することにより、本人認証を行う。
【選択図】　図7



【特許請求の範囲】
【請求項1】
端末装置と、ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を備えた認証サーバと、変換サーバとを含むワンタイムＩＤ認証システムであって、
前記端末装置が、
ユーザＩＤと現在時刻とに基づいて生成されたワンタイムＩＤと、パスワードとを含む認証要求を前記認証サーバへ送信する構成を有し、
前記認証サーバが、
前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含んだ変換要求を生成し、該生成した変換要求を前記変換サーバへ送信し、前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする構成を有し、
前記変換サーバが、
前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバに返却する構成を有することを特徴とするワンタイムＩＤ認証システム。
【請求項2】
請求項１記載のワンタイムＩＤ認証システムにおいて、
前記端末装置のユーザによって入力されたユーザＩＤと現在時刻とに基づいてワンタイムＩＤを生成し、該生成したワンタイムＩＤを表示部に表示するワンタイムＩＤ生成手段を含むワンタイムＩＤ生成装置を備えたことを特徴とするワンタイムＩＤ認証システム。
【請求項3】
請求項１記載のワンタイムＩＤ認証システムにおいて、
前記端末装置のユーザのユーザＩＤが登録されているユーザＩＤ記憶部と、
該ユーザＩＤ記憶部に登録されているユーザＩＤと現在時刻とに基づいてワンタイムＩＤを生成し、該生成したワンタイムＩＤを表示部に表示するワンタイムＩＤ生成手段とを含むワンタイムＩＤ生成装置を備えたことを特徴とするワンタイムＩＤ認証システム。
【請求項4】
請求項１、２または３記載のワンタイムＩＤ認証システムにおいて、
前記認証サーバが、
前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を前記変換サーバへ送信する変換要求手段と、
前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段とを備えたことを特徴とするワンタイムＩＤ認証システム。
【請求項5】
請求項４記載のワンタイムＩＤ認証システムにおいて、
前記変換サーバが、
前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段を備えたことを特徴とするワンタイムＩＤ認証システム。
【請求項6】
請求項２または３記載のワンタイムＩＤ認証システムにおいて、
前記ワンタイムＩＤ生成装置が、
一日を複数の時間帯に分けた際の、各時間帯用のワンタイムＩＤ生成用関数が格納された関数保持部と、
該関数保持部に格納されているワンタイムＩＤ生成用関数の内の、現在時刻を含む時間

帯用のワンタイムＩＤ生成用関数と、現在時刻と、ユーザＩＤとに基づいてワンタイムＩＤを生成するワンタイムＩＤ生成用演算手段とを備え、
前記変換サーバが、
一日を複数の時間帯に分けた際の、各時間帯用のユーザＩＤ算出用関数が格納された逆関数保持部と、
前記認証サーバから変換要求が送られてきたとき、前記逆関数保持部に保持されている各時間帯用のユーザＩＤ算出用関数の内の、現在時刻を含む時間帯用のユーザＩＤ算出用関数と、現在時刻と、前記変換要求中のワンタイムＩＤとに基づいてユーザＩＤを算出するユーザＩＤ算出用演算手段とを備えたことを特徴とするワンタイムＩＤ認証システム。
【請求項7】
ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部と、
端末装置からユーザＩＤとパスワードとを含む認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を変換サーバへ送信する変換要求手段と、
前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段とを備えたことを特徴とする認証サーバ。
【請求項8】
認証サーバからワンタイムＩＤを含む変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段を備えたことを特徴とする変換サーバ。
【請求項9】
端末装置が、ユーザＩＤと現在時刻とに基づいて生成されたワンタイムＩＤと、パスワードとを含む認証要求を認証サーバへ送信し、
ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を有する前記認証サーバが、前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含んだ変換要求を生成し、該生成した変換要求を変換サーバへ送信し、
前記変換サーバが、前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバに返却し、
前記認証サーバが、前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とすることを特徴とするワンタイムＩＤ認証方法。
【請求項10】
ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を備えたコンピュータを、
端末装置からユーザＩＤとパスワードとを含む認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を変換サーバへ送信する変換要求手段、
前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段として機能させるためのプログラム。
【請求項11】
コンピュータを、
認証サーバからワンタイムＩＤを含む変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段として機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】
【0001】
本発明は、ネットワークシステムにおける本人認証技術に関し、特に、ログオン毎に毎回異なるユーザＩＤ（ワンタイムＩＤ）を使用することにより、セキュリティレベルを高めた本人認証技術に関する。
【背景技術】
【0002】
ネットワークシステムにおける本人認証システムとしては、従来から種々のものが知られている。図１３は、従来最も一般的に利用されている本人認証システムの構成を示したブロック図である。同図を参照すると、本人認証システムは、認証サーバ１００と、ユーザが利用する端末装置２００とを含み、両者はインターネット，ＬＡＮなどのネットワーク３００を介して相互に接続されている。
【0003】
この図１３に示した本人認証システムでは、端末装置２００のユーザは、本人認証を行う場合、自身のユーザＩＤとパスワードとを含む認証要求を、端末装置２００から認証サーバ１００へ送信する。認証サーバ１００内の認証手段１０１は、送受信手段１０２を介して端末装置２００からの認証要求を受信すると、各ユーザのユーザＩＤとパスワードとが対応付けて登録されている認証情報記憶部１０３を参照し、本人認証を行う。即ち、認証要求中のユーザＩＤと対応付けて認証情報記憶部１０３に登録されているパスワードと、認証要求中のパスワードとを比較し、両者が一致する場合は、認証成功とし、両者が不一致の場合は、認証失敗とする。
【0004】
しかしながら、図１３に示した本人認証システムは、毎回同じユーザＩＤ及びパスワードを使用するため、セキュリティの点に問題がある。そこで、毎回異なるパスワード（ワンタイムパスワード）を使用するようにした、図１４に示すような本人認証システムが提案された（例えば、特許文献１参照）。
【0005】
図１４を参照すると、本人認証システムは、認証サーバ４００と、ユーザが利用する端末装置５００と、ワンタイムパスワード生成装置６００とを含み、認証サーバ４００と端末装置５００とは、インターネット，ＬＡＮ等のネットワーク７００を介して相互に接続されている。
【0006】
端末装置５００のユーザは、本人認証を行う場合、先ず、ワンタイムパスワード生成装置６００に、自身のユーザＩＤを入力する。これにより、ワンタイムパスワード生成装置６００は、入力されたユーザＩＤと現在時刻とに基づいてワンタイムパスワードを生成し、生成したワンタイムパスワードを表示部（図示せず）に表示する。尚、ワンタイムパスワード生成装置６００は、例えば、ワンタイムパスワード生成用のプログラムを組み込んだ携帯電話機などにより実現される。
【0007】
ユーザは、ワンタイムパスワードが表示されると、それと自身のユーザＩＤとを端末装置５００に入力する。これにより、端末装置５００は、上記ワンタイムパスワード及びユーザＩＤを含む認証要求を認証サーバ４００へ送信する。
【0008】
認証サーバ４００内の認証手段４０１は、送受信手段４０２を介して認証要求を受信すると、上記認証要求に含まれているユーザＩＤをワンタイムパスワード生成手段４０３に渡し、ワンタイムパスワードの生成を指示する。これにより、ワンタイムパスワード生成手段４０３は、時計４０４から現在時刻を入力し、この現在時刻と上記ユーザＩＤとに基づいてワンタイムパスワードを生成する。そして、生成したワンタイムパスワードと、認証要求に含まれていたワンタイムパスワードとを比較し、両者が一致する場合は、認証成功とし、両者が不一致の場合は、認証失敗とする。
【特許文献1】

特開２００２－２５９３４４号公報
【発明の開示】
【発明が解決しようとする課題】
【0009】
上述した特許文献１に記載されている本人認証システムによれば、毎回異なるパスワードが使用されるため、セキュリティを高いものにすることが可能になる。
【0010】
ところで、既に図１３に示すような認証サーバ１００を導入している機関においても、セキュリティの向上が望まれている。セキュリティを向上させるためには、図１４に示すようなワンタイムパスワードを利用して認証を行う本人認証システムを導入すればよいが、それでは、コストが非常に高くなってしまう。
【0011】
〔発明の目的〕
そこで、本発明の目的は、ユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を有し、ユーザＩＤとパスワードとに基づいた本人認証を行う既存の認証サーバを利用することにより、ワンタイムＩＤを用いたセキュリティの高い本人認証システムを経済的に構成できるようにすることにある。
【課題を解決するための手段】
【0012】
本発明にかかる第１のワンタイムＩＤ認証システムは、
端末装置と、ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を備えた認証サーバと、変換サーバとを含むワンタイムＩＤ認証システムであって、
前記端末装置が、
ユーザＩＤと現在時刻とに基づいて生成されたワンタイムＩＤと、パスワードとを含む認証要求を前記認証サーバへ送信する構成を有し、
前記認証サーバが、
前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含んだ変換要求を生成し、該生成した変換要求を前記変換サーバへ送信し、前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする構成を有し、
前記変換サーバが、
前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバに返却する構成を有することを特徴とする。
【0013】
本発明にかかる第２のワンタイムＩＤ認証システムは、第１のワンタイムＩＤ認証システムにおいて、
前記端末装置のユーザによって入力されたユーザＩＤと現在時刻とに基づいてワンタイムＩＤを生成し、該生成したワンタイムＩＤを表示部に表示するワンタイムＩＤ生成手段を含むワンタイムＩＤ生成装置を備えたことを特徴とする。
【0014】
本発明にかかる第３のワンタイムＩＤ認証システムは、第１のワンタイムＩＤ認証システムにおいて、
前記端末装置のユーザのユーザＩＤが登録されているユーザＩＤ記憶部と、
該ユーザＩＤ記憶部に登録されているユーザＩＤと現在時刻とに基づいてワンタイムＩＤを生成し、該生成したワンタイムＩＤを表示部に表示するワンタイムＩＤ生成手段とを含むワンタイムＩＤ生成装置を備えたことを特徴とする。
【0015】
本発明にかかる第４のワンタイムＩＤ認証システムは、第１～第３のワンタイムＩＤ認

証システムにおいて、
　前記認証サーバが、
　前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を前記変換サーバへ送信する変換要求手段と、
　前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段とを備えたことを特徴とする。
【0016】
　本発明にかかる第５のワンタイムＩＤ認証システムは、第４のワンタイムＩＤ認証システムにおいて、
　前記変換サーバが、
　前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段を備えたことを特徴とする。
【0017】
　本発明にかかる第６のワンタイムＩＤ認証システムは、第２または第３のワンタイムＩＤ認証システムにおいて、
　前記ワンタイムＩＤ生成装置が、
　一日を複数の時間帯に分けた際の、各時間帯用のワンタイムＩＤ生成用関数が格納された関数保持部と、
　該関数保持部に格納されているワンタイムＩＤ生成用関数の内の、現在時刻を含む時間帯用のワンタイムＩＤ生成用関数と、現在時刻と、ユーザＩＤとに基づいてワンタイムＩＤを生成するワンタイムＩＤ生成用演算手段とを備え、
　前記変換サーバが、
　一日を複数の時間帯に分けた際の、各時間帯用のユーザＩＤ算出用関数が格納された逆関数保持部と、
　前記認証サーバから変換要求が送られてきたとき、前記逆関数保持部に保持されている各時間帯用のユーザＩＤ算出用関数の内の、現在時刻を含む時間帯用のユーザＩＤ算出用関数と、現在時刻と、前記変換要求中のワンタイムＩＤとに基づいてユーザＩＤを算出するユーザＩＤ算出用演算手段とを備えたことを特徴とする。
【0018】
　本発明にかかる認証サーバは、
　ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部と、
　端末装置からユーザＩＤとパスワードとを含む認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を変換サーバへ送信する変換要求手段と、
　前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段とを備えたことを特徴とする。
【0019】
　本発明にかかる変換サーバは、
　認証サーバからワンタイムＩＤを含む変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段を備えたことを特徴とする。
【0020】
　本発明にかかるワンタイムＩＤ認証方法は、
　端末装置が、ユーザＩＤと現在時刻とに基づいて生成されたワンタイムＩＤと、パスワードとを含む認証要求を認証サーバへ送信し、

ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を有する前記認証サーバが、前記端末装置から認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含んだ変換要求を生成し、該生成した変換要求を変換サーバへ送信し、

前記変換サーバが、前記認証サーバから変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバに返却し、

前記認証サーバが、前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とすることを特徴とする。

【0021】

本発明にかかる第１のプログラムは、

ユーザのユーザＩＤとパスワードとが対応付けて登録された認証情報記憶部を備えたコンピュータを、

端末装置からユーザＩＤとパスワードとを含む認証要求が送られてきたとき、該認証要求中のワンタイムＩＤを含む変換要求を生成し、該生成した変換要求を変換サーバへ送信する変換要求手段、

前記変換サーバから前記変換要求に対する変換結果としてユーザＩＤが送られてきたとき、該ユーザＩＤに対応付けて前記認証情報記憶部に登録されているパスワードと前記認証要求中のパスワードとを比較し、両者が一致する場合、認証成功とする比較手段として機能させる。

【0022】

本発明にかかる第２のプログラムは、

コンピュータを、

認証サーバからワンタイムＩＤを含む変換要求が送られてきたとき、該変換要求中のワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、該算出したユーザＩＤを前記認証サーバへ送信する変換手段として機能させる。

【0023】

〔作用〕

ユーザは、本人認証を行う場合、自身の端末装置から認証サーバへ認証要求を送る。この認証要求には、ユーザのユーザＩＤと現在時刻とに基づいて生成されたワンタイムＩＤと、上記ユーザのパスワードとが含まれている。ワンタイムＩＤは、その生成時刻毎に、その値が異なるものになるので、セキュリティを高いものにすることができる。認証サーバは、認証要求を受信すると、認証要求中のワンタイムＩＤを含んだ変換要求を生成し、変換サーバに送る。変換サーバは、変換要求中のワンタイムＩＤと現在時刻とに基づいて、ユーザのユーザＩＤを算出し、算出したユーザＩＤを認証サーバに返却する。認証サーバは、返却されたユーザＩＤと、認証要求中のパスワードと、認証情報記憶部とを利用して本人認証を行う。

【発明の効果】

【0024】

本発明によれば、ワンタイムＩＤを利用したセキュリティの高い本人認証システムを経済的に構成することが可能になる。その理由は、端末装置から送られてきた認証要求に含まれているワンタイムＩＤをユーザＩＤに戻す変換サーバを設け、ユーザＩＤとパスワードとによる本人認証を行う既存の認証サーバをワンタイムＩＤを用いた本人認証に利用できるようにしたからである。

【発明を実施するための最良の形態】

【0025】

次に本発明の実施の形態について図面を参照して詳細に説明する。

【0026】

〔第１の実施の形態の構成の説明〕

図１は本発明にかかるワンタイムＩＤ認証システムの第１の実施の形態の全体構成を示すブロック図である。同図を参照すると、本実施の形態のワンタイムＩＤ認証システムは、ユーザが利用するワンタイムＩＤ生成装置１０と、上記ユーザが利用する端末装置２０と、認証サーバ３０と、変換サーバ４０とを含み、端末装置１０，認証サーバ３０および変換サーバ４０は、インターネット，ＬＡＮ等のネットワーク５０を介して相互に接続されている。

【0027】

ワンタイムＩＤ生成装置１０は、ユーザが入力したユーザＩＤと現在時刻とに基づいてワンタイムＩＤを生成し、ユーザに提示する機能を有する。

【0028】

図２は、上記した機能を有するワンタイムＩＤ生成装置１０の構成例を示すブロック図であり、テンキー等の入力部１１と、ワンタイムＩＤ生成手段１２と、現在時刻を表示する時計１６と、ＬＣＤなどの表示部１７とを備えている。

【0029】

ワンタイムＩＤ生成手段１２は、関数保持部１３と、演算手段１４と、現在時刻入力手段１５を備えている。

【0030】

時刻入力手段１５は、時計１６から現在時刻を入力する機能を有する。尚、本実施の形態では、時刻入力手段１５は、時計１６が表示している時：分：秒の内、時：分のみを入力するものとする。即ち、時刻入力手段１５は、分単位の時刻を入力する。

【0031】

関数保持部１３には、ワンタイムＩＤを生成する際に利用する関数（ワンタイムＩＤ生成用関数）が格納されている。

【0032】

演算手段１４は、入力部１１から入力されたユーザＩＤと、時刻入力手段１５が入力した現在時刻とに対して、関数保持部１３に保持されているワンタイムＩＤ生成用関数に従った演算を行うことによりワンタイムＩＤを算出し、算出したワンタイムＩＤを表示部１７に表示する機能を有する。

【0033】

尚、ワンタイムＩＤ生成装置１０内のワンタイムＩＤ生成手段１２は、ＣＰＵ（コンピュータ）によって実現可能なものであり、コンピュータによって実現する場合は、例えば、次のようにする。コンピュータをワンタイムＩＤ生成手段１２として機能させるためのプログラムを記録したディスク，半導体メモリ，その他の記録媒体を用意し、コンピュータに上記プログラムを読み取らせる。コンピュータは、読み取ったプログラムに従って自身の動作を制御することにより、自コンピュータ上に、ワンタイムＩＤ生成手段１２を実現する。また、ワンタイムＩＤ生成装置１０は、ＣＰＵを内蔵した携帯電話機を利用して実現することもできる。即ち、上記ＣＰＵをワンタイムＩＤ生成手段１２として機能させるためのプログラムを記録したディスクなどの記録媒体を用意し、ＣＰＵに上記プログラムを読み取らせる。ＣＰＵは、読み取ったプログラムに従って自身の動作を制御することにより、自ＣＰＵ上にワンタイムＩＤ生成手段を実現する。

【0034】

端末装置２０は、ワンタイムＩＤ及びパスワードを含んだ認証要求を認証サーバ３０へ送信する機能や、認証サーバ３０から送られてきた認証結果をユーザに提示する機能等を有する。

【0035】

図３は、上記した機能を有する端末装置２０の構成例を示すブロック図であり、送受信手段２１と、制御手段２２と、キーボード等の入力部２３と、ＬＣＤ等の表示部２４とを備えている。

【0036】

送受信手段２１は、ネットワーク５０を介してデータをやり取りする機能を有する。

【0037】
制御手段２２は、入力部２３から入力されたワンタイムＩＤ及びパスワードを含む認証要求を生成する機能や、生成した認証要求を送受信手段２１を介して認証サーバ３０へ送信する機能や、認証サーバ３０から送られてきた認証結果を表示部２４に表示する機能などを有する。
【0038】
尚、端末装置２０はパーソナルコンピュータ等のコンピュータによって実現可能なものであり、コンピュータによって実現する場合は、例えば、次のようにする。コンピュータを端末装置として機能させるためのプログラムを記録したディスク，半導体メモリ，その他の記録媒体を用意し、コンピュータに上記プログラムを読み取らせる。コンピュータは、読み取ったプログラムに従って自身の動作を制御することにより、自コンピュータ上に、送受信手段２１、制御手段２２を実現する。
【0039】
認証サーバ３０は、端末装置２０からワンタイムＩＤ及びパスワードを含む認証要求が送られてきたとき、変換サーバ４０を利用して上記ワンタイムＩＤに対応するユーザＩＤを取得し、このユーザＩＤと上記認証要求中のパスワードとに基づいて認証を行う機能を有する。
【0040】
図４は、上述した機能を有する認証サーバ３０の構成例を示すブロック図であり、送受信手段３１と、認証手段３２と、認証情報記憶部３５とを備えている。
【0041】
認証情報記憶部３５には、図５に示すように、ユーザのユーザＩＤ，パスワード，アクセス権限，氏名，…が対応付けて登録されている。
【0042】
送受信手段３１は、ネットワーク５０を介してデータをやり取りする機能を有する。
【0043】
認証手段３２は、変換要求手段３３と、比較手段３４とを備えている。
【0044】
変換要求手段３３は、送受信手段３１を介して端末装置２０からの認証要求を受信したとき、認証要求中のワンタイムＩＤを含んだ変換要求を変換サーバ４０へ送信し、この変換要求に応答して変換サーバ４０から返却されたユーザＩＤを比較手段３４に渡す機能を有する。変換要求手段３３は、図１３に示した認証サーバ１００には備わっていない構成であり、既存の認証サーバ１００を利用して認証サーバ３０を実現する場合には、この構成を組み込む必要がある。
【0045】
比較手段３４は、変換要求手段３３から渡されたユーザＩＤに対応付けて認証情報記憶部３５に登録されているパスワードと、端末装置２０からの認証要求中のパスワードとを比較し、両者が一致する場合は、認証成功とし、両者が不一致の場合は、認証失敗とする機能を有する。比較手段３４は、図１３に示した認証サーバ１００に備わっている構成である。
【0046】
尚、認証サーバ３０は、コンピュータによって実現可能なものであり、コンピュータによって実現する場合は、例えば、次のようにする。コンピュータを認証サーバとして機能させるためのプログラムを記録したディスク，半導体メモリ，その他の記録媒体を用意し、コンピュータに上記プログラムを読み取らせる。コンピュータは、読み取ったプログラムに従って自身の動作を制御し、自コンピュータ上に、送受信手段３１，認証手段３２を実現する。
【0047】
変換サーバ４０は、認証サーバ３０からワンタイムＩＤを含む変換要求が送られてきたとき、上記ワンタイムＩＤと現在時刻とに基づいてユーザＩＤを算出し、算出したユーザ

ＩＤを返却する機能を有する。
【0048】
図６は上記した機能を有する変換サーバ４０の構成例を示すブロック図であり、送受信手段４１と、変換手段４２と、現在時刻を表示する時計４６とを有する。
【0049】
送受信手段４１は、ネットワーク５０を介してデータを送受信する機能を有する。
【0050】
変換手段４２は、演算手段４３と、逆関数保持部４４と、時刻入力手段４５とを備えている。
【0051】
時刻入力手段４５は、時計４６から分単位の現在時刻を入力する機能を有する。
【0052】
逆関数保持部４４には、ワンタイムＩＤと現在時刻とからユーザＩＤを求めるための関数（ユーザＩＤ算出用関数）が格納されている。
【0053】
演算手段４３は、送受信手段４１を介して認証サーバ３０から送られてきた変換要求を受信したとき、それに含まれているワンタイムＩＤと、時刻入力手段４５が入力した分単位の現在時刻と、逆関数保持部４４に保持されているユーザＩＤ算出用関数とに基づいてユーザＩＤを算出し、算出したユーザＩＤを認証サーバ３０へ送信する機能を有する。
【0054】
尚、変換サーバ４０は、コンピュータによって実現可能なものであり、コンピュータによって実現する場合は、例えば次のようにする。コンピュータを変換サーバとして機能させるためのプログラムを記録したディスク，半導体メモリ，その他の記録媒体を用意し、コンピュータに上記プログラムを読み取らせる。コンピュータは、読み取ったプログラムに従って自身の動作を制御することにより、自コンピュータ上に、送受信手段４１、変換手段４２を実現する。
【0055】
〔第１の実施の形態の動作の説明〕
次に、本実施の形態の動作について各図を参照して詳細に説明する。
【0056】
端末装置２０のユーザは、本人認証を行う場合、ワンタイムＩＤ生成装置１０を起動し、入力部１１から自身のユーザＩＤを入力する（図７のａ）。
【0057】
ワンタイムＩＤ生成装置１０内のワンタイムＩＤ生成手段１２は、起動されると、ユーザＩＤの入力待ち状態となり、ユーザによって入力部１１からユーザＩＤが入力されると、時刻入力手段１５を用いて時計１６から分単位の現在時刻を入力する（図８のステップＳ８１，Ｓ８２）。その後、演算手段１４が、関数保持部１３に格納されているワンタイムＩＤ生成用関数と、ユーザが入力したユーザＩＤと、時刻入力手段１５が入力した現在時刻とに基づいてワンタイムＩＤを生成する（ステップＳ８３）。ここで、ワンタイムＩＤ生成用関数としては、例えば、（ワンタイムＩＤ）＝（ユーザＩＤ）×（現在時刻）などの関数を採用することができる。その後、演算手段１４は、算出したワンタイムＩＤを表示部１７に表示する（ステップＳ８４）。
【0058】
ユーザは、表示部１７にワンタイムＩＤが表示されると、表示されたワンタイムＩＤとパスワードとを端末装置２０に入力する（図７のｂ，ｃ）。端末装置２０内の制御手段２２は、入力部２３からワンタイムＩＤ及びパスワードが入力されると、それらを含んだ認証要求を認証サーバ３０へ送信する（図７のｄ）。
【0059】
認証サーバ３０内の変換要求手段３３は、送受信手段３１を介して端末装置２０から送られてきた認証要求を受信すると、上記認証要求中のワンタイムＩＤを含んだ変換要求を

生成し、それを変換サーバ４０へ送信する（図９のステップＳ９１，Ｓ９２及び図７のｅ）。その後、変換要求手段３３は、変換結果（ユーザＩＤ）の返却待ち状態となる（ステップＳ９３）。

【0060】

一方、変換サーバ４０内の変換手段４２は、認証サーバ３０からの変換要求を送受信手段４１を介して受信すると、図１０のフローチャートに示すように、先ず時刻入力手段４５を使用して時計４６から分単位の現在時刻を入力する（ステップＳ１０１）。その後、演算手段４３が、逆関数保持部４４に保持されているユーザＩＤ算出用関数と、時刻入力手段４５が入力した分単位の現在時刻と、変換要求中のワンタイムＩＤに基づいてユーザＩＤを算出し、算出したユーザＩＤを認証サーバ３０へ返却する（ステップＳ１０２，Ｓ１０３及び図７のｆ）。ここで、逆関数保持部４４に保持されているユーザＩＤ算出用関数は、ワンタイムＩＤ生成装置１０内の関数保持部１３に保持されているワンタイムＩＤ生成用関数の逆関数であり、例えば、ワンタイムＩＤ生成用関数が、（ワンタイムＩＤ）＝（ユーザＩＤ）×（現在時刻）であれば、ユーザＩＤ算出用関数は、（ユーザＩＤ）＝（ワンタイムＩＤ）÷（現在時刻）となる。但し、関数保持部１３，逆関数保持部４４に保持されるワンタイムＩＤ生成用関数，ユーザＩＤ算出用関数は、上記した例に限られるものではない。

【0061】

変換結果の返却待ち状態にある認証サーバ３０内の変換要求手段３３は、変換サーバ４０から送られてくる変換結果（ユーザＩＤ）を送受信手段３１を介して受信すると、それを比較手段３４に渡す。これにより、比較手段３４は、認証情報記憶部３５から、上記ユーザＩＤに対応付けて登録されているパスワードを取り出し、端末装置２０から送られてきた認証要求中のパスワードと比較する（図９のステップＳ９４）。そして、両者が一致する場合は、認証要求元の端末装置２０に認証成功を通知し（ステップＳ９５がＹＥＳ，Ｓ９６）、不一致の場合は、端末装置２０に認証失敗を通知する（ステップＳ９５がＮＯ，Ｓ９７及び図９のｇ）。尚、認証情報記憶部３５に該当するユーザＩＤが登録されていない場合も、認証失敗とする。

【0062】

端末装置２０内の制御手段２２は、送受信手段２１を介して認証結果（認証成功或いは認証失敗）を受信すると、それを表示部２４に表示する。認証成功が表示された場合、端末装置２０のユーザは、システムに対するアクセス権を獲得したことになり、システムにアクセスすることが可能になる。これに対して、認証失敗が表示された場合は、ユーザは、前述した操作を再度行う。

【0063】

尚、上述した実施の形態では、変換サーバ４０内の変換手段４２は、認証サーバ３０からの変換要求を受信したとき、変換要求中のワンタイムＩＤと、現在時刻とに基づいてユーザＩＤを１つだけ算出するようにしたが、現在時刻に対応するユーザＩＤと、現在時刻よりも１分前の時刻に対応するユーザＩＤとの２つのユーザＩＤを求め、それら２つのユーザＩＤを認証サーバ３０に返却するようにしても良い。そして、２つのユーザＩＤが返却された認証サーバ３０内の比較手段３４では、上記２つのユーザＩＤに対応付けて認証情報記憶部３５に登録されている２つのパスワードの内の何れか一方が、認証要求中のパスワードと一致していれば、認証成功と判定する。このようにすることにより、ユーザの操作時間（ワンタイムＩＤの生成時から、ユーザがワンタイムＩＤ及びパスワードを端末装置２０に入力するまでの時間）により、ワンタイムＩＤの生成時刻と、変換サーバ４０における変換要求の受信時刻とに差が生じた場合であっても、その差が１分以内であれば、認証成功とすることができる。

【0064】

また、上述した実施の形態では、関数保持部１３，逆関数保持部４４にそれぞれワンタイムＩＤ生成用関数，ユーザＩＤ算出用関数を１つずつ格納するようにしたが、複数のワンタイムＩＤ生成用関数，ユーザＩＤ算出用関数を格納しておき、時間帯に応じて使用す

る関数を変更するようにしても良い。このようにする場合は、例えば、１日を複数の時間帯に分け、各時間帯用のそれぞれ異なるワンタイムＩＤ生成用関数，ユーザＩＤ算出用関数を関数保持部１３，客関数保持部４４に登録しておく。ワンタイムＩＤ生成装置１０内の演算手段１４では、図８のステップＳ８３でワンタイムＩＤを生成する際、関数保持部１３に格納されている各時間帯のワンタイムＩＤ生成用関数の内の、現在時刻を含む時間帯用のワンタイムＩＤ生成用関数と、現在時刻と、ユーザＩＤとを使用してワンタイムＩＤを生成する。また、変換サーバ４０内の演算手段４３では、図１０のステップＳ１０２においてユーザＩＤを算出する際、逆関数保持部４４に格納されているユーザＩＤ算出用関数の内の、現在時刻を含む時間帯用のユーザＩＤ算出用関数と、現在時刻と、ワンタイムＩＤとからユーザＩＤを算出する。

【0065】

〔第１の実施の形態の効果〕

本実施の形態によれば、ワンタイムＩＤを利用したセキュリティの高い本人認証システムを経済的に構成することが可能になる。その理由は、端末装置２０から送られてきた認証要求に含まれているワンタイムＩＤをユーザＩＤに戻す変換サーバ４０を設けることにより、ユーザＩＤとパスワードとによる本人認証を行う既存の認証サーバ３０を、ワンタイムＩＤを用いた本人認証に利用できるようにしたからである。

【0066】

更に、本実施の形態によれば、セキュリティを極めて高いものにすることが可能になる。その理由は、時間毎に異なるワンタイムＩＤ生成用関数，ユーザＩＤ算出用関数を使用するようにしているからである。

【0067】

〔第２の実施の形態〕

次に、本発明にかかるワンタイムＩＤ認証システムの第２の実施の形態について説明する。本実施の形態のワンタイムＩＤ認証システムは、図１に示したワンタイムＩＤ認証システムにおいて、図２に示したワンタイムＩＤ生成装置１０の代わりに、図１１に示すワンタイムＩＤ生成装置１０ａを用いることにより実現される。

【0068】

本実施の形態で使用する図１１に示すワンタイムＩＤ生成装置１０ａは、ワンタイムＩＤ生成手段１２の代わりに、ワンタイムＩＤ生成手段１２ａを備えている点、およびユーザＩＤ保持部１９が追加されている点が図２に示したワンタイムＩＤ生成手段１２と相違している。

【0069】

ユーザＩＤ保持部１９には、端末装置２０のユーザのユーザＩＤが登録されている。

【0070】

ワンタイムＩＤ生成１２ａは、ユーザＩＤ保持部１９に格納されているユーザＩＤを入力するユーザＩＤ入力手段１８が追加されている点が、ワンタイムＩＤ生成手段１２と相違している。

【0071】

次に、本実施の形態の動作について説明する。尚、ワンタイムＩＤ生成装置１２ａ以外の動作は、第１の実施の形態と同様であるので、ここでは、ワンタイムＩＤ生成装置１２ａの動作についてのみ説明する。

【0072】

端末装置２０のユーザは、本人認証を行う場合、ワンタイムＩＤ生成装置１０ａを起動する。これにより、ワンタイムＩＤ生成装置１０ａ内のワンタイムＩＤ生成手段１２ａは、時刻入力手段１５を用いて時計１６から分単位の現在時刻を入力し、更に、ユーザＩＤ入力手段１８を用いてユーザＩＤ保持部１９からユーザＩＤを入力する（図１２のステップＳ１２１，Ｓ１２２）。その後、ワンタイムＩＤ生成手段１２ａ内の演算手段１４が、関数保持部１３に保持されているワンタイムＩＤ生成用関数と、時刻入力手段１５が入力した現在時刻と、ユーザＩＤ入力手段１８が入力したユーザＩＤとに基づいて、ワンタイ

ムＩＤを生成し、生成したワンタイムＩＤを表示部１７に表示する（ステップＳ１２３，Ｓ１２４）。

【0073】

〔第２の実施の形態の効果〕

本実施の形態によれば、第１の実施の形態の効果に加え、ユーザが行うワンタイムＩＤの生成操作を簡単なものとすることができる。その理由は、ワンタイムＩＤ生成装置１２ａが、ユーザＩＤが登録されたユーザＩＤ保持部１９を備えており、ユーザがワンタイムＩＤ生成時に、ユーザＩＤを入力する必要がないからである。

【産業上の利用可能性】

【0074】

高いセキュリティが求められる認証システムに利用することができる。

【図面の簡単な説明】

【0075】

【図1】本発明にかかるワンタイムＩＤ認証システムの第１の実施の形態の全体構成例を示すブロック図である。

【図2】ワンタイムＩＤ生成装置１０の構成例を示すブロック図である。

【図3】端末装置２０の構成例を示すブロック図である。

【図4】認証サーバ３０の構成例を示すブロック図である。

【図5】認証情報記憶部３５の内容例を示す図である。

【図6】変換サーバ４０の構成例を示す図である。

【図7】第１の実施の形態の動作を説明するための図である。

【図8】ワンタイムＩＤ生成装置１０の処理例を示すフローチャートである。

【図9】認証サーバ３０の処理例を示すフローチャートである。

【図10】変換サーバ４０の処理例を示すフローチャートである。

【図11】本発明にかかるワンタイムＩＤ認証システムの第２の実施の形態で使用するワンタイムＩＤ生成装置１０ａの構成例を示すブロック図である。

【図12】ワンタイムＩＤ生成装置１０ａの処理例を示すブロック図である。

【図13】従来のユーザＩＤとパスワードとを使用する本人認証システムの一例を示すブロック図である。

【図14】従来のユーザＩＤとワンタイムパスワードとを使用する本人認証システムの一例を示す図である。

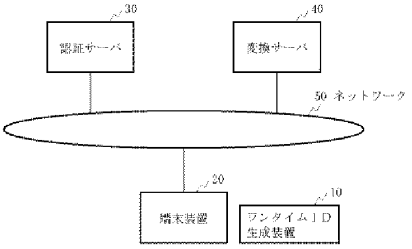
【符号の説明】

【0076】

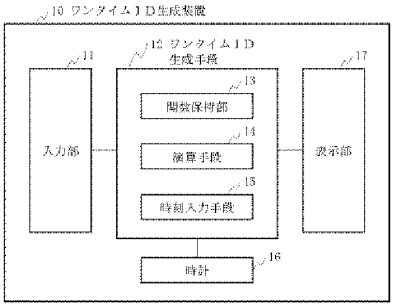
１０，１０ａ…ワンタイムＩＤ生成装置
１１…入力部
１２，１２ａ…ワンタイムＩＤ生成手段
１３…関数保持部
１４…演算手段
１５…時刻入力手段
１６…時計
１７…表示部
１８…ユーザＩＤ入力手段
１９…ユーザＩＤ保持部
２０…端末装置
２１…送受信手段
２２…制御手段
２３…入力部
２４…表示部
３０…認証サーバ
３１…送受信手段

３２…認証手段
３３…変換要求手段
３４…比較手段
３５…認証情報記憶部
４０…変換サーバ
４１…送受信手段
４２…変換手段
４３…演算手段
４４…逆関数保持部
４５…時刻入力手段
４６…時計
５０…ネットワーク

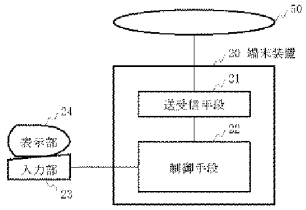
【図1】



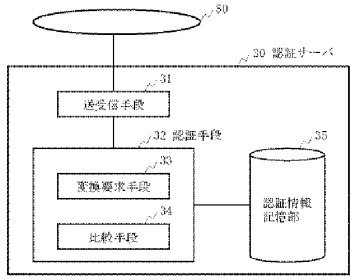
【図2】



【図3】



【図4】



【図5】

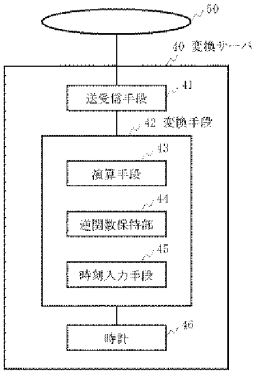
【図５】

35 認証情報記憶部

ユーザＩＤ	パスワード	アクセス権限	氏名	・・・
ｉｄ１	ｐ１	ａ１	ｘｘｘ	・・・
ｉｄ２	ｐ２	ａ２	ｙｙｙ	・・・
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

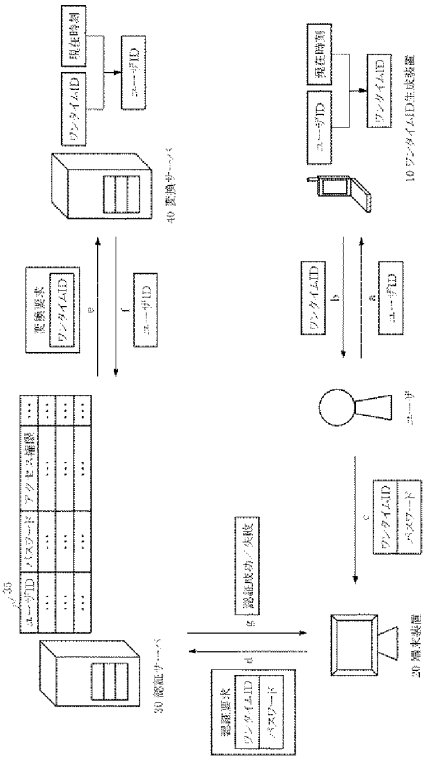
【図6】

【図６】



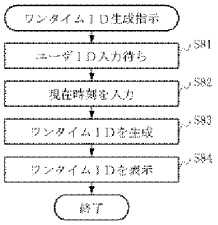
【図7】

【図７】



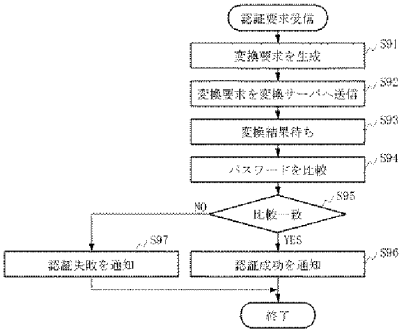
【図8】

【図８】



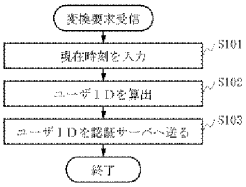
【図9】

【図９】



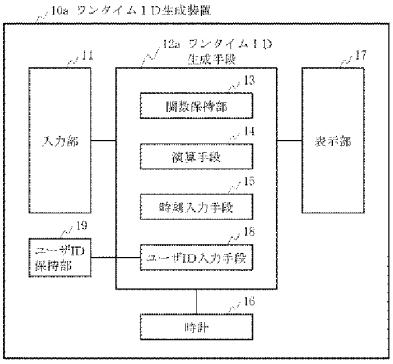
【図10】

【図１０】



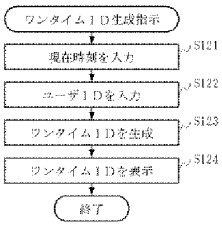
【図11】

【図１１】



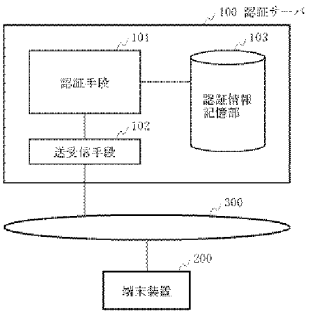
【図12】

【図１２】



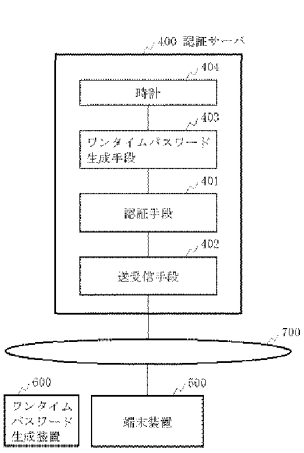
【図13】

【図１３】



【図14】

【図１４】



Sign in

Patents English Chinese Find prior art Discuss this application View PDF Download PDF

Air download method of increment business of user identifying module

CN 1345154 A

Publication number	CN1345154 A
Publication type	Application
Application number	CN 01134713
Publication date	Apr 17, 2002
Filing date	Nov 8, 2001
Priority date	Nov 8, 2001
Inventors	赵文军, 姜旻, 王志红
Applicant	大唐微电子技术有限公司
Export Citation	BiBTeX, EndNote, RefMan

Referenced by (15), Classifications (2), Legal Events (3)

External Links: SIPO, Espacenet

ABSTRACT

The invnetion discloses a method used to download on-air a value added service to subscriber identification module (SIM) in digital mobile phone. The STK and application program is directly downloaded to subscriber's SIM card by using CLASS 2 SIM-specific message format. The STK menu data is provided for SIM card to add new service, and the application program is used for realizing STK application. The invented method takes full advantage of existing software and hardware facility, making user apply for new service without need to replace STK card, also without need going to appointed business hall.

DESCRIPTION translated from Chinese

VAS Subscriber Identity Module aerial download methods

Field of the Invention This invention relates to a digital mobile communication system of the new technology, particularly, relates to a value-added services digital mobile telephone SIM (Subscriber Identity Module) card over the air method, the technology can move expanding communications, mobile banking, mobile securities, and mobile e-commerce and many other value-added services in mobile phones widely applied, is a digital mobile phone and record carrier with conductive marks, printed circuits or semiconductor circuit elements (such as credit cards or identification Card) Technical Field.

Due to limited STK technology can meet the different requirements of various customers personalized to meet the diverse needs of people on the information queries, so that the data service downsizing, personal computer and mobile from PC to mobile phones, but also for commercial advertising bring success and more market opportunities, so the market has achieved some success. Currently around STK ISP has been able to provide weather forecasts, news, check train schedules, aircraft flight information, stock inquiries and other aspects of business, and more value-added services are around STK gradually opened. However, the contradiction between the limited capacity of the rapidly growing business needs and unlimited scope for each SIM card between them has become increasingly prominent.

At present, various value-added services are usually one-time use of STK technology advance to write a variety of business needs of the user STK SIM card, if the user wants to change or add four new value-added services to a fixed place of business must By setting hall where computer and Internet connection of 2 and front terminal (POS machines) 3, to download the server from a new business STK download relevant business data and procedures (see Figure 1), or simply replace another Zhang STK cards. Due to the limited number of such pre-terminal (POS machines), and are usually placed in a fixed location - Fixed mobile phone operating room, so the user can only to a fixed location can only add value to the business of deletions, modifications tedious the process is bound to give it a lot of trouble, will inevitably affect the user to use various STK business initiative, which adversely affect competition in the market for operators.

CLAIMS (5) translated from Chinese

1. A digital mobile telephone subscriber identification module (SIM card) of value-added services over the air method, characterized in that: the method is implemented by STK menu data and the SIM card provided to add new services to the STK application application which together with two short messages (CLASS 2SIM-specific message) in the form of downloaded to the user's SIM card achieved.

The digital mobile telephone subscriber identification module (SIM card) of the value-added services over the air method according to claim 1, characterized in that: the method comprises at least the following steps: (1) by an ordinary user short message service provider, namely STK new business download server sends "New Business Download List" application requesting service providers to provide a list of available download services; (2) STK new business download server after receipt of the application, The new services STK download list with two short messages sent to the application user; (3) the application user to download a list of these new services based on STK received, you can choose to add one of them STK business, but also can choose The new service is added STK position, and after a good choice, the information is sent back to the server to download STK new business; (4) STK new business download server after receiving the application needs of users of information, related processing and then through the secondary short message data and procedures that apply STK business users need to download to the user to specify the location of the SIM card, to complete the download process STK business.

The digital mobile telephone subscriber identification module (SIM card) of value-added services over the air method according to claim 1, characterized in that: the method may also include the steps of: in the SIM card STK menu Preset Multiple content is empty menu, the user can be classified add in these menus change according to personal preferences menu name and download business.

4. According to the digital mobile telephone subscriber identification module (SIM card) of value-added services over the air method according to claim 1, characterized in that: the method may further

The present invention is a digital mobile telephone in the subscriber identification module (SIM card) of the value-added services over the air method is implemented as follows: it is to add new services through the menu to the SIM card STK menu data and applications to achieve STK together with two applications both short message (CLASS 2SIM-specific message) in the form of downloaded to the user's SIM card achieved.

The method includes at least the following steps: (1) a short message to the user through common service providers, namely STK new business download server sends "New Business Download List" application, request service providers to provide a list of services available for download; (2) STK new business download server after receiving the application, the new business will STK download list with a secondary message is sent to the application user; (3) the application user to download a list of new services based on STK received above, You can choose to add one of them STK business, but you can also choose to add the location of the new STK business, and after a good choice, the information is sent back to the server to download STK new business; (4) STK new business download servers Upon receipt of the application needs of users of information, related processing, and then through the secondary short message data and procedures that apply STK business users need to download to the user to specify the location of the SIM card, to complete STK Business download process.

The method may also include the following steps: pre more content in the SIM card STK menu is empty menu, the user can be classified add in these menus change according to personal preferences menu name and download business.

The method may further comprise the steps of: STK business has been downloaded, the user can choose to delete to make room to download other new business.

The secondary display is a short message on the screen is not in ME, as the data is transferred directly and transparently to the SIM card storage, data processing; and only STK card supports sending and receiving short messages of this kind.

Using the method of the invention, a mobile communications company and value-added business service providers can leverage existing software and hardware devices, without adding more investment, as long as the development of the corresponding supporting software to download the application and make the business has been expanding . And users do not have to replace the STK card, do not have to specify the operating room to use the pre-terminal (POS machines) download new business, you can freely, easily and flexibly select the STK services they need. For example, users can be based on individual needs and preferences anytime, anywhere-air download STK business; and its existing SIM card STK services, users can also choose to delete, to free up more space to download new business. Thus, to some extent, also solves the contradiction between limited and unlimited capacity needs of users between SIM card and can save users the associated costs. Users can also according to their habits and preferences, will assign various STK business into different groups, in order to facilitate their use; moreover, the group name can also be modified by the user. In summary, the present invention has a fairly optimistic about market prospects.

Figure 2 is a digital mobile telephone of the present invention in VAS STK SIM card over the air network system connection diagram.

Figure 3 is a realization of the method of the present invention is a digital mobile telephone in VAS STK SIM card over the air. Fig.

STK menu both an application STK application implemented method of the present invention is a digital mobile telephone in the subscriber identification module (SIM card) of value-added services over the air is to add new services provided by the SIM card to be implemented together with the data and two short message (CLASS 2) in the form of downloaded to the user's SIM card achieved.

See Fig. 3 a schematic view of the operation: (1) First, by the user by using an ordinary short message to their mobile phone via the GSM network service provider, i.e. STK "new business download list" application download server sends a new service; (2) Then, the network operator via SMS center its digital mobile telephone exchange received the application user and transparently passed to the new business STK ISP download server, and the server to download the new business after receipt of the application, then by SMSC digital mobile telephone exchange will STK new business list with a secondary message is sent to the application user; (3) the application of new business users based on the above list STK received, you can choose to add one of them STK business , but you can also choose to add a new STK business location; and a good selection, and then together with the relevant information needs to be sent back to the server to download STK new business; (4) STK new business application download server receives the user's Related demand information after appropriate treatment, then the original data and programs through the network link to the secondary short message to the application desired to download user STK service to the subscriber's SIM card, i.e. complete business STK download process.

comprise the steps of: STK downloaded service, The user can choose to delete to make room to download other new business.

The digital mobile telephone subscriber identification module (SIM card) of value-added services over the air method according to claim 1, wherein: said second short message is a screen display is not on ME directly as the data is transferred transparently to the SIM card storage, data processing; and only STK card supports sending and receiving short messages of this kind.

Here the secondary short message different from ordinary short message, is displayed on the screen is an ME is not directly transmitted to the SIM card as a data storage, data processing; STK card supports only send and receive short messages of this kind.

In addition, the method of the present invention can also be preset in the SIM card STK menu is empty multiple menus, the user can choose according to your preferences and change the menu name and downloadable business class to add in these menu section . For already downloaded STK services, users can also choose to delete to make room to download other new business.

Between devices constituting a network system of the present invention has a SIM card in a digital mobile telephone set, GSM networks and new services STK downloading server simulation experiment, the effect of the test was successful, to achieve the object of the invention.

REFERENCED BY

Citing Patent	Filing date	Publication date	Applicant	Title
CN100334914C *	Dec 21, 2004	Aug 29, 2007	乐金电子(中国)研究开发中心有限公司	Device and method for maintaining applied information consistency of portable terminal
CN100334917C *	Dec 31, 2004	Aug 29, 2007	大唐微电子技术有限公司	A method and system for compatibility test of subscriber identification module tool kit card
CN100405864C	Aug 4, 2006	Jul 23, 2008	浙江省电信有限公司	Implementing method for air loading technology based on PAS network
CN100450279C	Mar 22, 2005	Jan 7, 2009	华为技术有限公司	Method for realizing user data management based on wireless system
CN100452893C	Aug 4, 2006	Jan 14, 2009	凤凰微电子（中国）有限公司	System and method for realizing value-added business based on user identification module
CN100454932C	Jun 8, 2004	Jan 21, 2009	雅斯拓（北京）智能卡科技有限公司	Method for realizing short-message memory on expanded SIM card
CN100459737C	Feb 25, 2005	Feb 4, 2009	北京握奇数据系统有限公司	Information transmitting/receiving method and system
CN101217728B	Dec 29, 2007	Jan 30, 2013	北京握奇数据系统有限公司	A blank card for wireless card writing, wireless card writing server and wireless card writing method
CN101257682B	Mar 6, 2008	Dec 15, 2010	上海展趣网络科技有限公司; 上海长丰智能卡有限公司	External control method for SIM card
CN101453714B	Dec 3, 2007	Mar 27, 2013	中兴通讯股份有限公司	Method and system for application download of near-field communication mobile payment system
CN101557580B	May 15, 2009	Oct 26, 2011	中兴通讯股份有限公司	Data processing method and system
US7734707	Aug 1, 2006	Jun 8, 2010	Beijing Watch Data System Co., Ltd.	Don't disturb service management system and implementation thereof
US8255706	Dec 7, 2007	Aug 28, 2012	Beijing Watch Data System Co., Ltd.	Dual usage smart card of CPU and logical encryption and its data synchronization method
US8266619	Jan 25, 2007	Sep 11, 2012	Beijing Watch Data System Co., Ltd.	Embedded operating system architecture for smart card
WO2012152031A1 *	Dec 26, 2011	Nov 15, 2012	Zte Corporation	Wireless communication terminal and its software upgrade method

* Cited by examiner

CLASSIFICATIONS

International Classification	H04M1/66, H04M3/42

LEGAL EVENTS

Date	Code	Event	Description
Feb 20, 2002	C10	Request of examination as to substance	
Apr 17, 2002	C06	Publication	
Sep 8, 2004	C02	Deemed withdrawal of patent application after publication (patent law 2001)	

Google Home - Sitemap - USPTO Bulk Downloads - Privacy Policy - Terms of Service - About Google Patents - Send Feedback

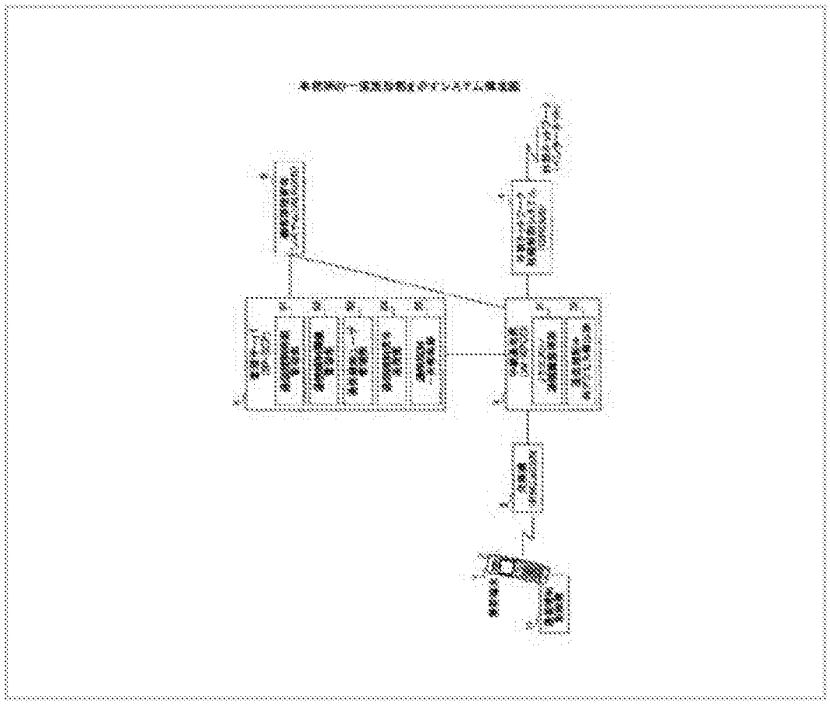
(11)Publication number	2006-197137
(43)Date of publication of application	27.07.2006
(51)Int.Cl.	H04M 3/42 (2006.01) H04M 11/00 (2006.01) H04M 15/00 (2006.01) H04Q 7/38 (2006.01)
(21)Application number	2005-005684
(22)Date of filing	12.01.2005
(71)Applicant	NTT DOCOMO INC
(72)Inventor	TANIGUCHI HIROTO ASANO YOSHITOKI

(54)DATA COMMUNICATION REGULATING METHOD OF FIXED RATE SYSTEM USER, DATA COMMUNICATION REGULATION CONTROLLER AND PORTABLE TERMINAL

(57)Abstract

PROBLEM TO BE SOLVED: To provide a fixed rate system user communication regulating method for finitely applying communication regulation to a specific user, and for applying firm communication regulation which can not be easily released at a portable terminal side at the time of defining data communication such as packet communication as an object.

SOLUTION: This data communication regulating method comprises a process for monitoring the data communication status of a fixed rate system user, and for judging whether or not the number of times of request or communication quantity within a predetermined period exceed a predetermined threshold, a process for setting the fixed rate system user as the object of communication regulation when it is judged that they exceed the predetermined threshold and a process for transmitting a communication regulation signal including the information of a communication regulation time to the portable terminal of the fixed rate system user when access is performed again from the fixed rate system user set as the object of communication regulation. The data communication of the portable terminal of the fixed rate system user is put in an inhibited status across the communication regulation time.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-197137
(P2006-197137A)
(43)公開日　平成18年7月27日(2006.7.27)

(51)Int.Cl.		F I			テーマコード（参考）
H04M 3/42	(2006.01)	H04M	3/42	A	5K024
H04M 11/00	(2006.01)	H04M	11/00	303	5K025
H04M 15/00	(2006.01)	H04M	15/00	G	5K067
H04Q 7/38	(2006.01)	H04B	7/26	109K	5K101

審査請求 未請求　請求項の数 9　OL　（全 9 頁）

(21)出願番号　特願2005-5684(P2005-5684)
(22)出願日　平成17年1月12日(2005.1.12)

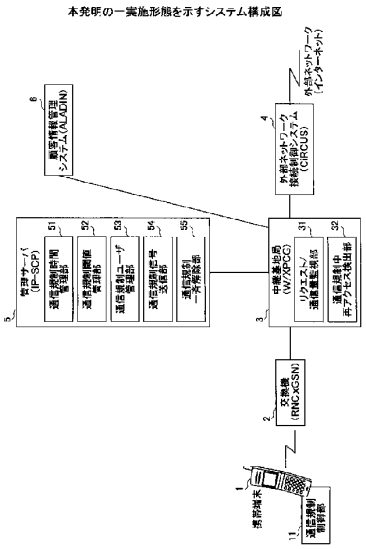
(71)出願人　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　谷口　博人
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　浅野　義時
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内

Fターム(参考)　5K024 AA61 AA63 CC11 FF03
5K025 AA05 AA08 BB01 CC01 JJ02
KK06

最終頁に続く

(54)【発明の名称】定額制ユーザのデータ通信規制方法、データ通信規制制御装置および携帯端末

(57)【要約】
【課題】　パケット通信等のデータ通信を対象とし、特定のユーザに対して限定的に通信規制をかけることができるとともに、携帯端末側で簡単に通信規制を解除することのできない強固な規制をかけることができる定額制ユーザ通信規制方法等を提供する。
【解決手段】　定額制ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断する工程と、上記所定の閾値を超えたと判断された場合に当該定額制ユーザを通信規制対象に設定する工程と、上記通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号を当該定額制ユーザの携帯端末に送信する工程とを備え、上記定額制ユーザの携帯端末のデータ通信を上記通信規制時間にわたって禁止状態にする。
【選択図】　図３



【特許請求の範囲】
【請求項１】
定額制ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断する工程と、
上記所定の閾値を超えたと判断された場合に当該定額制ユーザを通信規制対象に設定する工程と、
上記通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号を当該定額制ユーザの携帯端末に送信する工程とを備え、
上記定額制ユーザの携帯端末のデータ通信を上記通信規制時間にわたって禁止状態にすることを特徴とする定額制ユーザのデータ通信規制方法。
【請求項２】
上記閾値および上記通信規制時間は基地局毎に設定されることを特徴とする請求項１に記載の定額制ユーザのデータ通信規制方法。
【請求項３】
上記通信規制信号はショートメッセージサービスにより送信されることを特徴とする請求項１または２のいずれか一項に記載の定額制ユーザのデータ通信規制方法。
【請求項４】
通信規制の一斉解除時に、通信規制解除信号を通信規制の対象となっている定額制ユーザの携帯端末に送信する工程を備え、
上記定額制ユーザの携帯端末のデータ通信を通常使用可能状態にすることを特徴とする請求項１乃至３のいずれか一項に記載の定額制ユーザのデータ通信規制方法。
【請求項５】
上記通信規制解除信号はショートメッセージサービスにより送信されることを特徴とする請求項４に記載の定額制ユーザのデータ通信規制方法。
【請求項６】
定額制ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断する手段と、
上記所定の閾値を超えたと判断された場合に当該定額制ユーザを通信規制対象に設定する手段と、
上記通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号を当該定額制ユーザの携帯端末に送信する手段とを備え、
上記定額制ユーザの携帯端末のデータ通信を上記通信規制時間にわたって禁止状態にすることを特徴とするデータ通信規制制御装置。
【請求項７】
基地局側から通信規制時間の情報を含む通信規制信号を受信した場合に、データ通信を上記通信規制時間にわたって禁止状態にする手段を備えたことを特徴とする携帯端末。
【請求項８】
上記通信規制信号を受信した場合に、通信規制中である旨を画面に表示する手段を備えたことを特徴とする請求項７に記載の携帯端末。
【請求項９】
基地局側から通信規制解除信号を受信した場合に、データ通信を通常使用可能状態にする手段を備えたことを特徴とする請求項７または８のいずれか一項に記載の携帯端末。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は定額制ユーザのデータ通信規制方法、データ通信規制制御装置および携帯端末に関する。
【背景技術】

【０００２】
昨今、携帯電話等の携帯端末によるインターネットアクセスの利用が拡大しており、ユーザの通信料（パケット料金）の負担を軽減すべく、「定額制」と呼ばれる、通信量にかかわらず料金を一定としたサービスが導入されるに至っている。しかし一方で通信料が一定になるためデータ通信の過剰利用が懸念されるようになった。
【０００３】
そこで定額制サービスに於いては、特定の定額制ユーザによる必要以上のデータ通信リソースの独占を禁止すべく、過度のアクセスを行う特定のユーザに対しては通信事業者側で強制的に通信を切断することが契約上において一般に許容されている。一方で、通信量に応じて課金される「従量制」のユーザに対しては、その通信品質を保証する義務があり、定額制ユーザの通信を犠牲にしても従量制ユーザの通信を保証する必要がある。
【０００４】
ただしこのデータ通信規制は、あくまでもデータ通信と音声通信を同時に規制するのではなく、データ通信に特化した通信規制方法である。従って、通信規制を受けているユーザも、音声通信に関しては通常通り実施することが可能である。
【０００５】
図１は従来における通信規制の概念図であり、通常の利用にあっては携帯端末１０１から交換機１０２および中継基地局１０３を介してインターネット等の外部ネットワークにアクセスが行われるものであるが、中継基地局１０３において携帯端末１０１から過度のアクセスを検出した場合、携帯端末１０１から交換機１０２を介して中継基地局１０３に与えられるアクセス要求（リクエスト）を中継基地局１０３において許否することで通信規制を行うようにしていた。
【０００６】
一方、従来から各種通信における輻輳時の通信規制方法については様々な技術が開示されている（例えば、特許文献１を参照。）。特許文献１には、基地局が無線ゾーンの輻輳状態を常に監視し、輻輳レベルを算出して輻輳情報として移動端末に通知し、輻輳レベルに応じて移動端末の発信規制を行う技術が開示されている。
【特許文献１】特開２００１－７８２６０号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
図１に示した従来の通信規制方法では、通信規制により中継基地局１０３後段の通信リソースの独占は防止することができるが、携帯端末１０１から繰り返し行われるリクエスト（外部ネットワークに接続できないことで行われるリクエストのリトライ）が全て交換機１０２を経由することとなり、交換機１０２の負荷を低減することができないという問題があった。
【０００８】
一方、特許文献１に記載される技術は、無線ゾーンの輻輳状態に応じて多くのユーザに対して一律に規制をかけるものであり、定額制ユーザの中でも過度なアクセスを行う特定のユーザだけを対象とした規制を行えるものではない。また、特許文献１に記載される技術はパケット通信等のデータ通信に特化したものではない。
【０００９】
本発明は上記の従来の問題点に鑑み提案されたものであり、その目的とするところは、パケット通信等のデータ通信を対象とし、特定のユーザに対して限定的に通信規制をかけることができるとともに、携帯端末側で簡単に通信規制を解除することのできない強固な規制をかけることができる定額制ユーザのデータ通信規制方法、データ通信規制制御装置および携帯端末を提供することにある。
【課題を解決するための手段】
【００１０】
上記の課題を解決するため、本発明にあっては、請求項１に記載されるように、定額制

ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断する工程と、上記所定の閾値を超えたと判断された場合に当該定額制ユーザを通信規制対象に設定する工程と、上記通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号を当該定額制ユーザの携帯端末に送信する工程とを備え、上記定額制ユーザの携帯端末のデータ通信を上記通信規制時間にわたって禁止状態にする定額制ユーザ通信規制方法を要旨としている。

【００１１】

また、請求項２に記載されるように、上記閾値および上記通信規制時間は基地局毎に設定されるものとすることができる。

【００１２】

また、請求項３に記載されるように、上記通信規制信号はショートメッセージサービスにより送信されるものとすることができる。

【００１３】

また、請求項４に記載されるように、通信規制の一斉解除時に、通信規制解除信号を通信規制の対象となっている定額制ユーザの携帯端末に送信する工程を備え、上記定額制ユーザの携帯端末のデータ通信を通常使用可能状態にすることができる。

【００１４】

また、請求項５に記載されるように、上記通信規制解除信号はショートメッセージサービスにより送信されるものとすることができる。

【００１５】

また、請求項６に記載されるように、定額制ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断する手段と、上記所定の閾値を超えたと判断された場合に当該定額制ユーザを通信規制対象に設定する手段と、上記通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号を当該定額制ユーザの携帯端末に送信する手段とを備え、上記定額制ユーザの携帯端末のデータ通信を上記通信規制時間にわたって禁止状態にする通信規制制御装置として構成することができる。

【００１６】

また、請求項７に記載されるように、基地局側から通信規制時間の情報を含む通信規制信号を受信した場合に、データ通信を上記通信規制時間にわたって禁止状態にする手段を備えた携帯端末として構成することができる。

【００１７】

また、請求項８に記載されるように、上記通信規制信号を受信した場合に、通信規制中である旨を画面に表示する手段を備えるようにすることができる。

【００１８】

また、請求項９に記載されるように、基地局側から通信規制解除信号を受信した場合に、データ通信を通常使用可能状態にする手段を備えるようにすることができる。

【発明の効果】

【００１９】

本発明の定額制ユーザのデータ通信規制方法、データ通信規制制御装置および携帯端末にあっては、パケット通信等のデータ通信を対象とし、特定のユーザに対して限定的に通信規制をかけることができるとともに、携帯端末側で簡単に通信規制を解除することのできない強固な規制をかけることができる。

【発明を実施するための最良の形態】

【００２０】

以下、本発明の好適な実施形態について説明する。

【００２１】

図２は本発明における通信規制の概念図である。図２において、通常の利用にあっては定額制ユーザの所持する携帯電話のごとき携帯端末１から交換機２および中継基地局３を

介してインターネット等の外部ネットワークにアクセスが行われるものであるが、中継基地局３において定額制ユーザの携帯端末１から過度のアクセスを検出した場合、その定額制ユーザを通信規制の対象に設定し、再び同じユーザからアクセスが行われた場合、通信規制時間の情報を含む通信規制信号を定額制ユーザの携帯端末１に交換機２を介して送信する。これにより携帯端末１は指定された通信規制時間にわたり外部ネットワークへのアクセスのためのデータ通信が禁止状態となる。従って、通信規制時間により規定された期間は携帯端末１から交換機２にリクエストが発生することがなくなり、交換機２の負荷を有効に低減させることができる。

【００２２】

図３は本発明の一実施形態を示すシステム構成図である。図３において、携帯端末１には、通常の音声通話、データ通信等の機能の他に、基地局側から通信規制時間の情報を含む通信規制信号を受信した場合に、データ通信を指定された通信規制時間にわたって禁止状態にするとともに、通信規制中である旨を画面に表示する等の処理を行う通信規制制御部１１が設けられている。なお、通信規制制御部１１は主としてソフトウェア（コンピュータプログラム）によって実現される。

【００２３】

一方、基地局側の構成として、ＲＮＣ(Radio Network Controller)、ｘＧＳＮ(GPRS Support Node, GPRS: General Packet Radio Service)等の交換機２と、Ｗ／ＸＰＣＧ(Wireless/eXtended wireless Protocol Conversion Gateway)等の中継基地局３と、ＣｉＲＣＵＳ(treasure Casket of i-mode（登録商標） service, high Reliability platform for CUStomer)等の外部ネットワーク接続制御システム４と、ＩＰ－ＳＣＰ(IP-based Service Control Point)等の管理サーバ５と、ＡＬＡＤＩＮ(ALl Around DoCoMo INformation system)等の顧客情報管理システム６とが設けられている。

【００２４】

中継基地局３には、通常の中継機能の他に、定額制ユーザのデータ通信状態を監視し、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたか否かを判断し、閾値を超えた場合に管理サーバ５に通知を行うリクエスト／通信量監視部３１と、通信規制対象に設定された定額制ユーザから再びアクセスが行われたことを検出して管理サーバ５に通知を行う通信規制中再アクセス検出部３２とを備えている。

【００２５】

管理サーバ５には、中継基地局３の存在するエリアのデータ通信の輻輳状態に応じて通信規制時間を個別に設定管理する通信規制時間管理部５１と、同じく中継基地局３の存在するエリアのデータ通信の輻輳状態に応じて、通信規制の対象とすべき定額制ユーザのリクエスト回数およびもしくは通信量の超過を判断する閾値を個別に設定管理する通信規制閾値管理部５２と、所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えたと判断された場合にその定額制ユーザを通信規制対象に設定し、中継基地局３におけるその定額制ユーザの通信を規制する通信規制ユーザ管理部５３と、通信規制対象に設定された定額制ユーザから再びアクセスが行われた場合に通信規制時間の情報を含む通信規制信号をその定額制ユーザの携帯端末１に送信する通信規制信号送信部５４と、災害発生時等に、通信規制を一斉解除すべく、通信規制解除信号を通信規制の対象となっている定額制ユーザの携帯端末１に送信する通信規制一斉解除部５５とを備えている。

【００２６】

図４は上記の実施形態の動作例を示すシーケンス図であり、以下、図４に沿って上記の実施形態の動作を説明する。

【００２７】

先ず、通常の利用にあっては、定額制ユーザの所持する携帯端末１から交換機２、中継基地局３、外部ネットワーク接続制御システム４を介してインターネット等の外部ネットワークにアクセスが行われる（ステップＳ１～Ｓ８）。

【００２８】

ここで、中継基地局３はリクエスト／通信量監視部３１により定額制ユーザの携帯端末

１の通信状態を監視している。なお、携帯端末１のユーザが定額制ユーザであるかどうかは、顧客情報管理システム６から管理サーバ５を介して、あるいは、顧客情報管理システム６から直接に、契約情報を取得することで判断が可能である。また、リクエスト回数および通信量の超過を判断する閾値は、予め管理サーバ５から通知される。

【００２９】

そして、定額制ユーザの携帯端末１による所定期間内のリクエスト回数およびもしくは通信量が所定の閾値を超えた場合、中継基地局３のリクエスト／通信量監視部３１は管理サーバ５に対して閾値の超過を通知する（ステップＳ９）。

【００３０】

管理サーバ５では、中継基地局３から特定の定額制ユーザのリクエスト回数およびもしくは通信量の超過の通知を受けると、その定額制ユーザを通信規制対象に設定するとともに（ステップＳ１０）、中継基地局３に対してその定額制ユーザの通信を規制するよう通知を行う（ステップＳ１１）。中継基地局３では、以後、その定額制ユーザの通信規制が解除されるまでデータ通信の中継を行わない。

【００３１】

次いで、通信規制の対象となった定額制ユーザの携帯端末１から交換機２を介して中継基地局３に再びアクセスがあると（ステップＳ１２、Ｓ１３）、中継基地局３の通信規制中再アクセス検出部３２はその再アクセスを検出し、管理サーバ５に通知する（ステップＳ１４）。

【００３２】

再アクセスの通知を受けた管理サーバ５では、通信規制信号送信部５４により、通信規制対象に設定された定額制ユーザの携帯端末１に対し、通信規制時間管理部５１で管理される通信規制時間の情報を含む通信規制信号を、例えばＳＭＳ(Short Message Service)の機能により送信する（ステップＳ１５～Ｓ１７）。

【００３３】

通信規制信号を受信した携帯端末１は、通信規制制御部１１によりデータ通信の機能を通信規制時間で指定された時間にわたって禁止状態にするとともに（ステップＳ１８）、例えば図５に示すような「規制中のためしばらくたってからご利用ください」といったメッセージを画面に表示する。通信規制時間は管理サーバ５において中継基地局３の存在するエリアのデータ通信の輻輳状態に応じて設定管理されるものであり、例えば、ユーザの多い繁華街では長く設定される。リクエスト回数および通信量の超過を判断する閾値は、ユーザの多い繁華街では低めに設定される。

【００３４】

データ通信が禁止状態となっている期間において、携帯端末１からは通常では外部ネットワークへのアクセスは行えないが、プログラムをリセットする等により強引に通信規制を解除した場合であっても、中継基地局３においてそのユーザの中継が許否されるため、アクセスを行うことはできない。通信規制時間が終了すると、携帯端末１の通信規制制御部１１はデータ通信の機能を通常使用可能状態に復帰させる。

【００３５】

一方、災害発生時等において広くデータ通信を許容する必要がある場合、管理サーバ５は通信規制一斉解除部５５により通信規制を一斉解除し（ステップＳ１９）、通信規制ユーザ管理部５３における規制対象を削除するとともに、その時点で通信規制の対象となっている定額制ユーザの携帯端末１に対して中継基地局３を介してＳＭＳ等により通信規制解除信号を送信する（ステップＳ２０～Ｓ２２）。

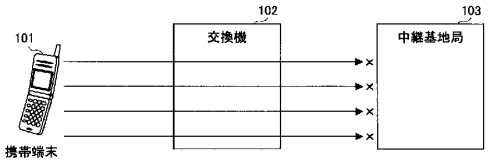
【００３６】

通信規制解除信号を受信した中継基地局３は定額制ユーザの規制を解除するとともに、同じく通信規制解除信号を受信した携帯端末１は、通信規制制御部１１によりデータ通信を通常使用可能状態に復帰させる（ステップＳ２３）。これにより携帯端末１は交換機２、中継基地局３、外部ネットワーク接続制御システム４を介した外部ネットワークへのアクセスが可能となる。

【００３７】
このように、パケット通信等のデータ通信を対象として、リクエスト、データ通信量の多い特定のユーザに対して限定的に通信規制をかけることができるとともに、携帯端末１側で簡単に通信規制を解除することのできない強固な規制をかけることができる。また、災害発生時等における通信規制の解除を適切に行うことができる。
【００３８】
以上、本発明の好適な実施の形態により本発明を説明した。ここでは特定の具体例を示して本発明を説明したが、特許請求の範囲に定義された本発明の広範な趣旨および範囲から逸脱することなく、これら具体例に様々な修正および変更を加えることができることは明らかである。すなわち、具体例の詳細および添付の図面により本発明が限定されるものと解釈してはならない。
【図面の簡単な説明】
【００３９】
【図１】従来における通信規制の概念図である。
【図２】本発明における通信規制の概念図である。
【図３】本発明の一実施形態を示すシステム構成図である。
【図４】実施形態の動作例を示すシーケンス図である。
【図５】携帯端末における表示画面の例を示す図である。
【符号の説明】
【００４０】
１　携帯端末
１１　通信規制制御部
２　交換機
３　中継基地局
３１　リクエスト／通信量監視部
３２　通信規制中再アクセス検出部
４　外部ネットワーク接続制御システム
５　管理サーバ
５１　通信規制時間管理部
５２　通信規制閾値管理部
５３　通信規制ユーザ管理部
５４　通信規制信号送信部
５５　通信規制一斉解除部
６　顧客情報管理システム

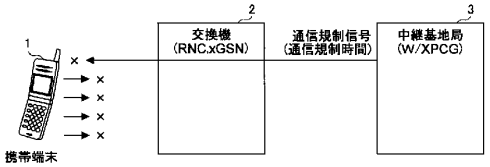
【図１】

従来における通信規制の概念図



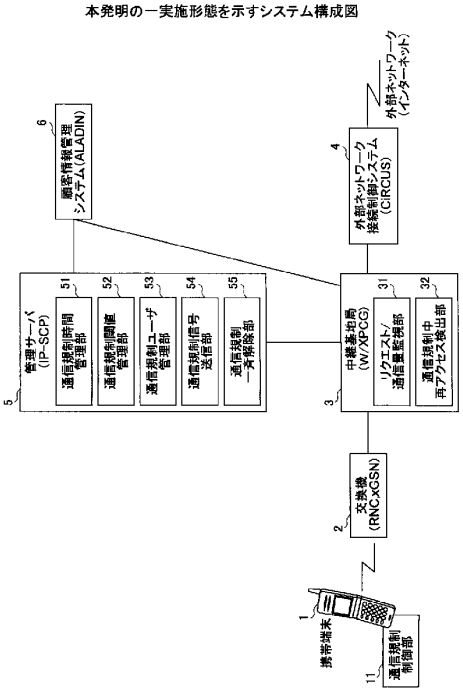
【図２】

本発明における通信規制の概念図



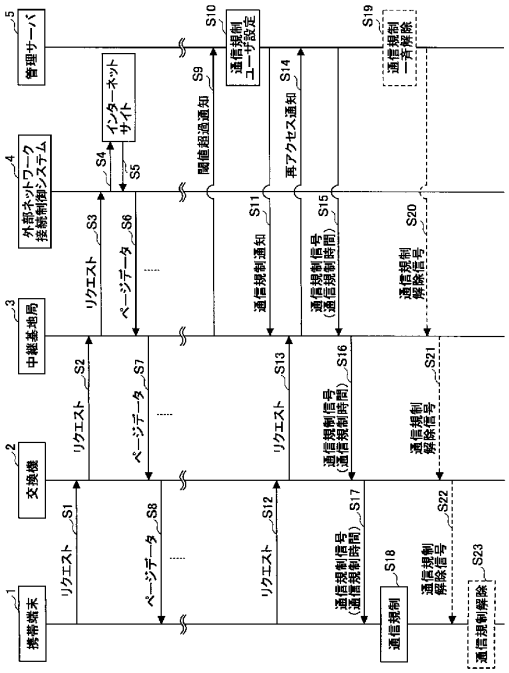
【図３】

本発明の一実施形態を示すシステム構成図



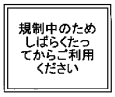
【図４】

実施形態の動作例を示すシーケンス図



【図５】

携帯端末における表示画面の例を示す図



フロントページの続き

Ｆターム(参考) 5K067 AA28 BB04 BB21 CC08 DD27 DD53 EE02 EE10 EE12 EE16
GG01 HH12 HH22
5K101 LL12 MM07 NN18 NN21 PP03 TT06

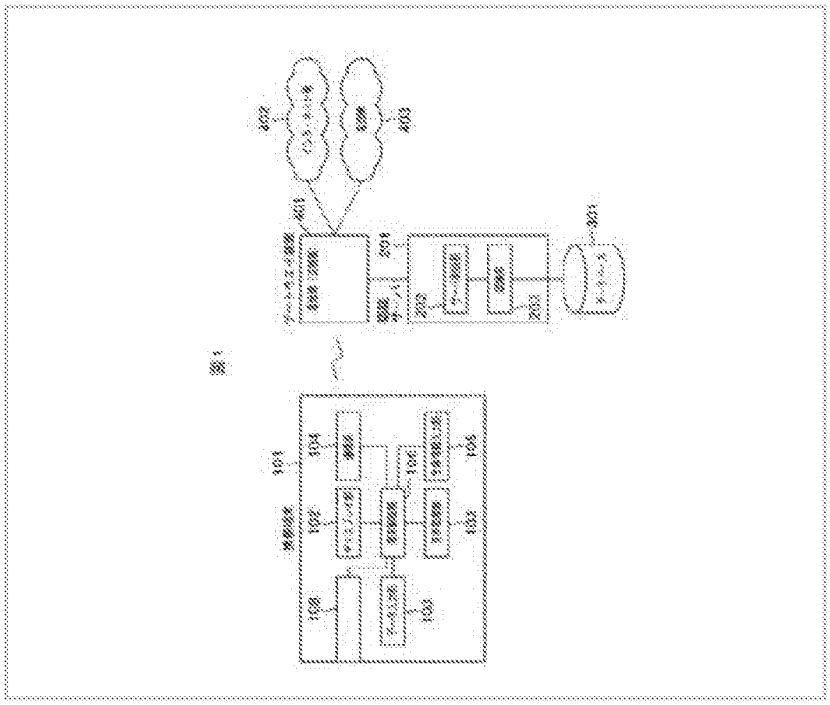
(11)Publication number	2006-344007
(43)Date of publication of application	21.12.2006
(51)Int.Cl.	G06F 21/20 (2006.01) H04L 9/32 (2006.01) H04Q 7/38 (2006.01) H04M 1/67 (2006.01)
(21)Application number	2005-169118
(22)Date of filing	09.06.2005
(71)Applicant	HITACHI LTD
(72)Inventor	OKAWA SATOICHI WATABE YOSHIRO YAMAKAWA YASUAKI TANGE TOMOYUKI HASEGAWA ATSUSHI

(54)PORTABLE TERMINAL IDENTIFICATION SYSTEM

(57)Abstract

PROBLEM TO BE SOLVED: To easily and surely carry out identification for a prepaid portable terminal.

SOLUTION: The portable terminal is equipped with; a biological information input section 105; a data input section 103; a storage section 108; a portable terminal 102 having a radio transmission section 104; a gateway device 401 having a function to decide a signal path of a data signal and a voice signal transmitted from this portable terminal and a function to set permission and inhibit of connection of the portable terminal; a database 301; and an authentication server 201 which authenticates a user by collating data of user's biological information already registered into the database and data of user's biological information transmitted from the portable terminal with the user's telephone number, when the effective period of the portable terminal registered in the database has not expired and sets permission and inhibit of the connection of the portable terminal to the gateway device based on the result of the authentication process.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-344007
(P2006-344007A)
(43)公開日　平成18年12月21日(2006.12.21)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330F	5B285
H04L 9/32	(2006.01)	H04L	9/00	673D	5J104
H04Q 7/38	(2006.01)	H04B	7/26	109R	5K027
H04M 1/67	(2006.01)	H04M	1/67		5K067

審査請求 未請求　請求項の数 7　OL　（全 12 頁）

(21)出願番号　特願2005-169118 (P2005-169118)
(22)出願日　平成17年6月9日 (2005.6.9)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000350
特許業務法人　日東国際特許事務所
(72)発明者　大川　諭一
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内
(72)発明者　渡部　喜朗
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内

最終頁に続く

(54)【発明の名称】携帯端末本人確認システム

(57)【要約】　(修正有)
【課題】プリペイド携帯端末の本人確認を、簡単で確実に行う。
【解決手段】生体情報入力部１０５、データ入力部１０３、記憶部１０８、無線送信部１０４を有する携帯端末１０２と、該携帯端末から送信されたデータ信号や音声信号の信号経路を決定する機能及び前記携帯端末の回線使用の許可設定及び禁止設定を行う機能を有するゲートウエイ装置４０１と、データベース３０１と、該データベースに登録されている前記携帯端末利用の期限が有効である場合において、前記データベースに既に登録されている利用者の生体情報に関するデータと前記利用者の電話番号を持つ携帯端末より送られてきた利用者の生体情報に関するデータを照合することにより前記利用者本人の認証処理を行い、該認証処理の結果に基づいて前記ゲートウエイ装置に対して前記携帯端末の回線使用の許可設定及び禁止設定を行う認証サーバ２０１とを備えた。
【選択図】図１

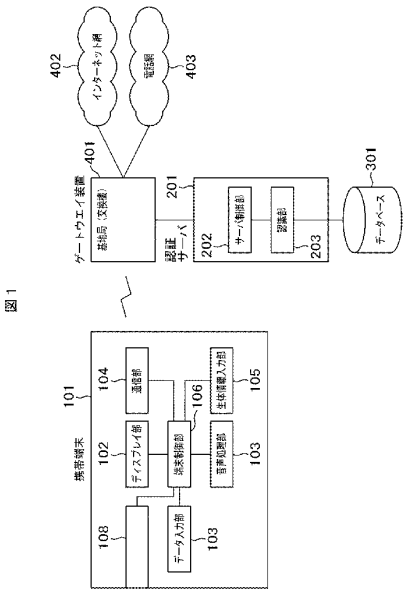


図１

【特許請求の範囲】
【請求項１】
利用者の生体情報を読み込むための生体情報入力部、サービスを受けるためのデータ信号や音声信号を入力する入力部及び利用者の電話番号に関する情報を記憶した記憶部を有し、前記生体情報入力部で読み込まれた利用者の生体情報に関するデータおよび前記記憶部に記憶された利用者の電話番号に関する情報並びに前記入力部から入力されたデータ信号や音声信号を通信部から無線通信によって送信する機能を有する携帯端末と、
該携帯端末がサービスを受けるために携帯端末から送信されたデータ信号や音声信号の信号経路を決定する機能及び前記携帯端末の回線使用の許可設定及び禁止設定を行う機能を有するゲートウエイ装置と、
前記利用者の生体情報に関するデータを前記利用者の電話番号に関する情報および前記携帯端末利用の有効期限と関連付けて登録して管理するデータベースと、
該データベースに登録されている前記携帯端末利用の期限が有効である場合において、前記データベースに既に登録されている利用者の生体情報に関するデータと前記利用者の電話番号を持つ携帯端末より送られてきた利用者の生体情報に関するデータを照合することにより前記利用者本人の認証処理を行い、該認証処理の結果に基づいて前記ゲートウエイ装置に対して前記携帯端末の回線使用の許可設定及び禁止設定を行う認証サーバとを備えたことを特徴とする携帯端末本人確認システム。
【請求項２】
前記認証サーバは、更に、前記データベースに登録された前記携帯端末利用の有効期限に基づいて前記携帯端末が利用の有効期限が近づいたことを検出し、これを前記携帯端末に通知する機能を有し、
前記携帯端末は、更に、前記認証サーバから前記通知を受けた際、表示または音声により、前記携帯端末が利用の有効期限が近づいたことおよび該有効期限の延長を促すことを知らせる機能を有することを特徴とする請求項１記載の携帯端末本人確認システム。
【請求項３】
前記携帯端末は、更に、前記有効期限が近づいたことの通知を受けて利用者が確認した際、前記生体情報入力部より利用者の生体情報に関するデータを入力し、該入力された利用者の生体情報に関するデータを前記認証サーバへ送信する機能を有し、
前記認証サーバは、更に、前記データベースに既に登録されている利用者の生体情報に関するデータと前記携帯端末から送信を受けた利用者の生体情報に関するデータとの照合を行った結果、前記携帯端末に入力された生体情報が利用者本人のものであることを確認できた場合に限り前記データベースに対して前記携帯端末の利用有効期限の延長設定を行う機能を有することを特徴とする請求項２記載の携帯端末本人確認システム。
【請求項４】
前記認証サーバは、更に、前記照合を行った結果、前記携帯端末に入力された生体情報が利用者本人のものとは認められなかった場合には、前記携帯端末の有効期限延長が設定されなかったことを前記携帯端末に通知する機能を有することを特徴とする請求項３記載の携帯端末本人確認システム。
【請求項５】
前記認証サーバは、更に、前記携帯端末から応答が無く、有効期限切れが検出されたとき、前記ゲートウエイ装置に対して前記携帯端末の回線使用の禁止設定を行う機能を有することを特徴とする請求項２又は４記載の携帯端末本人確認システム。
【請求項６】
前記認証サーバは、更に、有効期限切れが発生して使用できなくなったことを前記携帯端末に通知する機能を有することを特徴とする請求項５記載の携帯端末本人確認システム。
【請求項７】
前記携帯端末は、プリペイド式携帯端末で構成されることを特徴とする請求項１乃至６の何れか一つに記載の携帯端末本人確認システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、生体情報を使用して、プリペイド式携帯端末を持つ利用者に対して、本人確認を確実で簡単に行うことのできる認証技術に関する。
【背景技術】
【０００２】
端末販売店舗のみならず、コンビニエンスストア等でも購入でき、契約時の手続きが容易なことから、プリペイド式携帯電話が普及しつつある。このようなプリペイド式携帯電話サービスを今後も維持していくためには、不正利用をできるだけ抑止することが可能な方法を導入することが必須となってきている。
【０００３】
ところで、現在、提供されているプリペイド携帯電話サービスにおいて、本人確認を行うには、運転免許証、パスポート、外国人登録証明書など写真入の公的書類の提示が必要になっている。そのため、利用者は、本人確認のため、定期的に店舗等に出向き、写真入公的書類との照会をする必要がある。また、各利用者の登録状態を一人ずつ手入力にて管理する必要がある。
【０００４】
また、個々の携帯端末の操作制限を実現する方法として、生体情報を利用する方法が一部メーカより提供されている携帯端末で採用されている。この方法は、携帯端末内部に登録された生体情報と携帯端末に装備されている読取装置から入力された生体情報とを照合することにより、操作制限あるいは解除の設定を行うというものである。
【０００５】
携帯端末利用サービスにおいて、生体情報を利用した適用例として、例えば特開２００４－１３７５３号公報（従来技術１）に記載の技術が知られている。この従来技術１は、管理制限区域への入隊室管理に応用している。あらかじめ生体情報を記録したＩＣカードを用意しておき、カードリーダが装備されている携帯端末に挿入し、携帯端末からドアの開錠要求を行う。送られた情報は、管理制限区域入口にあるドアコントローラに送信される。ドアコントローラには、生体情報の読取装置があり、ここから生体情報を入力し、先に送った生体情報との照合により、ドア開錠・施錠を制御するものである。
【０００６】
また、従来技術１に類似する技術としては、例えば特開２００１－１１７８７８号公報（従来技術２）がある。この従来技術２は、携帯電話から入力された生体情報を、サービスプロバイダへ送信し、さらに認証サーバへ送信される。そして、認証サーバには、あらかじめ登録してある利用者の生体情報が保存されており、このデータとサービスプロバイダから送られてきた生体情報と照合し、結果をサービスプロバイダに返信する、といった適用例である。
【０００７】
上記従来技術１及び２は、いずれも認証をその都度行う必要があり、現行のプリペイド携帯電話サービスの本人確認の方法としては、手続きが煩雑で使い勝手がよくない。
【０００８】
また、一度の本人確認を行うことにより、有効期限内であれば何度でもサービス提供を受けることが可能となるシステムの公知例としては、特開２００１－２９８７７９号公報（従来技術３）が知られている。この従来技術３においては、指紋データおよび有効期限情報は、携帯端末側で管理することになっている。
【０００９】
【特許文献１】特開２００４－１３７５３号公報
【特許文献２】特開２００１－１１７８７８号公報
【特許文献３】特開２００１－２９８７７９号公報
【発明の開示】

【発明が解決しようとする課題】
【００１０】
上記従来技術１及び２では、サービスの利用が必要になるたびに、その都度認証が必要であるという課題がある。プリペイド携帯端末のサービスを考えると、一度認証されたら、ある一定期間は認証することなく、サービス提供されることが望ましい。さらに、なりすまし等の不正利用問題を回避しつつ、店舗等まで出向く手間を省くことが可能な認証方法が要求される。
【００１１】
また、従来技術３においては、生体情報および有効期限管理を携帯端末側で行うため、第３世代携帯端末で一般的になってきているＵＳＩＭカード等の差し替えにより携帯端末を切り替えるたびに、各携帯端末に対して再設定を行う必要があるという課題を有していた。
【００１２】
本発明の目的は、上記課題を解決すべく、携帯端末の切り替えに対しても特別な手続き等を行うことなく、プリペイド携帯端末等の本人確認を、簡単で確実に行うことができるようにした携帯端末本人確認システムを提供することにある。
【課題を解決するための手段】
【００１３】
上記目的を達成するために、本発明は、利用者の生体情報を読み込むための生体情報入力部、サービスを受けるためのデータ信号や音声信号を入力する入力部及び利用者の電話番号に関する情報を記憶した記憶部（例えばＵＳＩＭカード等）を有し、前記生体情報入力部で読み込まれた利用者の生体情報に関するデータおよび前記記憶部に記憶された利用者の電話番号に関する情報並びに前記入力部から入力されたデータ信号や音声信号を通信部から無線通信によって送信する機能を有する携帯端末と、該携帯端末がサービスを受けるために携帯端末から送信されたデータ信号や音声信号の信号経路を決定する機能及び前記携帯端末の回線使用の許可設定及び禁止設定を行う機能を有するゲートウエイ装置と、前記利用者の生体情報に関するデータを前記利用者の電話番号に関する情報および前記携帯端末利用の有効期限と関連付けて登録して管理するデータベースと、該データベースに登録されている前記携帯端末利用の期限が有効である場合において、前記データベースに既に登録されている利用者の生体情報に関するデータと前記利用者の電話番号を持つ携帯端末より送られてきた利用者の生体情報に関するデータを照合することにより前記利用者本人の認証処理を行い、該認証処理の結果に基づいて前記ゲートウエイ装置に対して前記携帯端末の回線使用の許可設定及び禁止設定を行う認証サーバとを備えたことを特徴とする携帯端末本人確認システムである。
【００１４】
また、本発明は、前記認証サーバは、更に、前記データベースに登録された前記携帯端末利用の有効期限に基づいて前記携帯端末が利用の有効期限が近づいたことを検出し、これを前記携帯端末に通知する機能を有し、前記携帯端末は、更に、前記認証サーバから前記通知を受けた際、表示または音声により、前記携帯端末が利用の有効期限が近づいたことおよび該有効期限の延長を促すことを知らせる機能を有することを特徴とする。
【００１５】
また、本発明は、前記携帯端末は、更に、前記有効期限が近づいたことの通知を受けて利用者が確認した際、前記生体情報入力部より利用者の生体情報に関するデータを入力し、該入力された利用者の生体情報に関するデータを前記認証サーバへ送信する機能を有し、前記認証サーバは、更に、前記データベースに既に登録されている利用者の生体情報に関するデータと前記携帯端末から送信を受けた利用者の生体情報に関するデータとの照合を行った結果、前記携帯端末に入力された生体情報が利用者本人のものであることを確認できた場合に限り前記データベースに対して前記携帯端末の利用有効期限の延長設定を行う機能を有することを特徴とする。
【００１６】

また、本発明は、前記認証サーバは、更に、前記照合を行った結果、前記携帯端末に入力された生体情報が利用者本人のものとは認められなかった場合には、前記携帯端末の有効期限延長が設定されなかったことを前記携帯端末に通知する機能を有することを特徴とする。

【００１７】

また、本発明は、前記認証サーバは、更に、前記携帯端末から応答が無く、有効期限切れが検出されたとき、前記ゲートウエイ装置に対して前記携帯端末の回線使用の禁止設定を行う機能を有することを特徴とする。

【００１８】

また、本発明は、前記認証サーバは、更に、有効期限切れが発生して使用できなくなったことを前記携帯端末に通知する機能を有することを特徴とする。

【００１９】

また、本発明は、前記携帯端末は、プリペイド式携帯端末で構成されることを特徴とする。

【発明の効果】

【００２０】

本発明によれば、プリペイド式携帯電話サービス等において、わざわざ店舗等に出向くことなく、簡単で確実な方法で本人確認を行うことができる。

【００２１】

また、本発明によれば、ＵＳＩＭカード等による携帯端末の切り替えに対しても、特別な手続き等を行うことなく適用可能である。

【発明を実施するための最良の形態】

【００２２】

本発明に係る、不正使用をできるだけ抑制でき、しかも端末販売店舗のみならず、コンビニエンスストア等でも購入でき、契約時の手続きが容易なプリペイド式携帯電話サービス等を受けることができ、さらに利用者の電話番号と生体情報を用いて関連付けてシステム全体で利用制限の管理を実現できる携帯端末本人確認システムの実施の形態について図面を用いて説明する。

【００２３】

上記利用者の電話番号としては、例えば、携帯端末へのＵＳＩＭ（Universal Subscriber Identity Module：汎用加入者識別モジュール）カード等の差し替えにより、複数端末の使い分け（例えば、一般通信用端末とデータ通信用端末の使い分け）、端末の更新（端末の機種変更）、さらには海外事業者端末との使い分け（チップ・イン・ローミング）が可能となる。

【００２４】

図１は、本発明に係る、不正使用をできるだけ抑制したプリペイド式携帯電話サービス等を受けることにできる携帯端末本人確認システムの一実施の形態の全体機能構成を示す図である。

【００２５】

本発明に係る携帯端末本人確認システムは、プリペイド式携帯電話サービス等を受けることにでき、さらに利用者固有の電話番号に関する情報を格納したＵＳＩＭカード等の差し替え可能で、生体情報を入力可能な携帯端末１０１と、上記利用者固有の電話番号によって携帯端末１０１がサービスを受けるために携帯端末１０１から送信されたデータ信号や音声信号の信号経路（インターネット網４０２や電話網４０３等からなる通信網を介したサービス装置への信号経路）を決定する機能及び認証サーバ２０１からの制御信号により上記電話番号（例えばＵＳＩＭカード等固有の電話番号）を持つ携帯端末の回線使用の許可設定及び禁止設定を行う機能を有するゲートウエイ装置（基地局（交換機））４０１と、新規登録時にあらかじめ携帯端末から取り込んだ利用者の生体情報に関するデータを上記携帯端末から得られる電話番号に関する情報と前記携帯端末利用の有効期限とを関連付けて登録して管理する機能を有するデータベース３０１を有し、該データベース３０１

に登録されている前記携帯端末利用の期限が有効である場合において、前記データベース３０１に既に登録されている利用者の生体情報に関するデータと前記利用者の電話番号を持つ携帯端末より送られてきた利用者の生体情報に関するデータを照合することにより前記利用者本人の認証処理を行い、該認証処理の結果に基づいて前記ゲートウエイ装置に対して前記携帯端末の回線使用の許可設定及び禁止設定を行う認証サーバと、
該データベース３０１に登録されているデータと上記電話番号を持つ携帯端末１０１より送られてきた生体情報を照合し、携帯端末の本人確認時に認証処理を行い、該認証結果によりゲートウエイ装置に対し使用許可あるいは使用停止の設定を行う認証サーバ２０１とを備えて構成される。なお、携帯端末１０１とゲートウエイ装置４０１とは無線通信によって接続される。またゲートウエイ装置４０１と認証サーバ２０１との間は有線或いは無線によって接続される。

【００２６】

携帯端末１０１は、データ信号を入力するデータ入力部１０７と、メッセージを表示するディスプレイ部１０２と、音声信号の入出力を行う音声処理部１０３と、上記データ信号や音声信号の変復調処理を行って、ゲートウエイ装置（基地局（交換機））４０１との間で無線通信を行うための通信部１０４と、利用者固有の指紋などに代表される生体情報を読み込むための生体情報入力部１０５と、前記ディスプレイ部１０２、音声処理部１０３、通信部１０４、生体情報入力部１０５が相互にデータをやり取りするための端末制御部１０６とを有し、プリペイド式携帯電話サービス等を受けることにでき、さらに利用者固有の電話番号に関する情報を記憶したＵＳＩＭカード等（記憶部）１０８の差し替え可能に構成される。ここで、音声処理部１０３は、図２に示すように、音声を入力するマイク１０３１と、音声を出力するスピーカ１０３２と、上記マイク１０３１からの入力音声信号を入力音声データに変換して例えば端末制御部１０６に入力し、例えば端末制御部１０６から得られる出力音声データを上記スピーカ１０３２への出力音声信号に変換するデータ変換部１０３３とを有して構成される。生体情報入力部１０５は、図３に示すように、利用者本人の指紋などに代表される生体情報を読み込むスキャナ部１０５１と、該スキャナ部１０５１から読み込まれた生体情報を生体データに変換して例えば端末制御部１０６に出力するデータ変換部１０５２とを有して構成される。なお、データ入力部１０７及び音声処理部１０３のマイク１０３１などは、携帯端末がサービスを受けるためのデータ信号や音声信号を入力する入力部を構成する。また、上記通信部１０４は、更に、生体情報入力部１０５で読み込まれた利用者本人の生体情報に関するデータおよびＵＳＩＭカード等（記憶部）１０８に記憶された利用者の電話番号に関する情報もゲートウエイ装置（基地局（交換機））４０１へ無線通信によって送信されることになる。

【００２７】

ゲートウエイ装置４０１は、上記携帯端末１０１がサービスを受けるために携帯端末１０１から送信されたデータ信号や音声信号の信号経路（通信網を介したサービス装置への信号経路）を決定する機能及び認証サーバ２０１内のサーバ制御部２０２からの制御信号により、上記電話番号を持つ携帯端末の回線使用の許可設定及び禁止設定を行う機能を有する。ここでいうゲートウエイ装置とは、一般的な意味で使われているゲートウエイトは異なり、当該携帯端末の使用許可および使用停止を制御できる装置という位置付けの意味で用いている。

【００２８】

データベース３０１は、新規登録時にあらかじめ取り込んだ利用者本人の生体情報に関するデータを上記携帯端末から得られる電話番号に関する情報と上記携帯端末利用の有効期限とを関連付けて登録して管理する機能を有する。

【００２９】

認証サーバ２０１は、接続された上記データベース３０１に登録されているデータと上記電話番号を持つ携帯端末１０１より送られてきた生体情報を照合し、携帯端末の本人確認時に認証処理を行う認証部２０３と、該認証部２０３からの認証結果によりゲートウエイ装置４０１に対し使用許可あるいは使用停止の設定を行うサーバ制御部２０２とを有し

て構成される。

【００３０】

次に、本発明に係る携帯端末本人確認システムにおける新規登録処理の一実施例について図４を用いて説明する。図４は、新規登録処理の一実施例を示す流れ図である。新規登録時においては、まだ本発明に係る携帯端末１０１は使用できないので、この部分は、上記ディスプレイ部１０２、音声処理部１０３、通信部１０４、生体情報入力部１０５の機能を含む登録装置１０１に置き換わる。このとき、登録装置１０１がＵＳＩＭカード等（記憶部）１０８の差し替え可能に構成される場合にはＵＳＩＭカード固有の電話番号に関する情報が設定されることになる。ステップ６０１で、利用者は登録装置１０１に対して、新規登録要求送信を行う。新規登録要求を受信した認証サーバ２０１は、ステップ６０２でデータベース３０１を検索し、ステップ６０３で、これから登録しようとしている上記電話番号に対応した利用者のデータがすでにデータベース３０１に登録されていないかどうか確認する。すでに登録されていると判断された場合、認証サーバ２０１は登録装置１０１に対し、ステップ６０４で、新規登録の拒否通知を行う。ステップ６０３で、未登録データと判断された場合、認証サーバ２０１は登録装置１０１に対し、ステップ６０５で上記電話番号に対応した利用者の生体情報の入力要求を行う。生体情報の入力要求を受けた登録装置１０１は、ステップ６０６で登録装置１０１上に生体情報の入力を促すメッセージを出す。これに対し、利用者はステップ６０７で、登録装置１０１より上記電話番号に対応した生体情報信号を入力・送信する。登録装置１０１より送信された上記電話番号に関する情報に対応した生体情報信号を認証サーバ２０１が受信すると、認証サーバ２０１はステップ６０８でデータベース３０１に対し、ステップ６０９で上記電話番号に関する情報対応した生体情報の登録および上記携帯端末使用の有効期限設定を行うと同時に、ゲートウエイ装置４０１に対し、上記電話番号による携帯端末の使用許可設定を行う。使用許可設定が完了すると、ゲートウエイ装置４０１は、認証サーバ２０１に対して、ステップ６１０で使用許可応答を行う。使用許可応答を受信した認証サーバ２０１は、ステップ６１１で登録装置１０１に対して使用許可応答信号を送信し、該使用許可応答信号を受信した登録装置１０１は、ステップ６１２で使用が許可されたことをディスプレイ部１０２又は／及び音声処理部１０３を用いて利用者に通知する。なお、登録装置１０１と認証サーバ２０１との信号の送受信はゲートウエイ装置４０１を介して行われる。以上が新規登録時の流れとなり、認証サーバ２０１は定期的にデータベース３０１にアクセスを行い、有効期限が近づくまではゲートウエイ装置４０１に対して上記電話番号による携帯端末の使用を許可したままとなる。利用者も有効期限内であれば、利用の都度本人確認を行うことなく、上記電話番号による携帯端末を利用することができる。

【００３１】

次に、本発明に係る携帯端末本人確認システムにおける継続手続きの一実施例について図５を用いて説明する。図５は、継続手続きの一実施例を示す流れ図である。認証サーバ２０１内部において、システム内の通信トラヒィックが低い時間帯（例えば深夜など）に例えば１日１回、サーバ制御部２０２は認証部２０３に対して、既に登録されている携帯端末について、有効期限との関係を調べるよう指示する。該指示を受けた認証部２０３は、データベース３０１にアクセスし、登録されている全ての携帯端末について、現在日と有効期限日との関係を調査し、その結果を一括して把握することができる。調査した結果は、認証部２０３よりサーバ制御部２０２に通知される。このようにして、認証サーバ２０１は有効期限切れが近づいている電話番号の携帯端末および有効期限切れが発生している電話番号の携帯端末に関するデータを取得する。この結果、認証サーバ２０１は、新規登録時または前回の継続手続き時に設定された有効期限まで、規定の日数以内になると、ステップ６２１で上記電話番号による携帯端末１０１に対して有効期限切れが近づいていることを通知することができる。通知を受信した携帯端末１０１は、ステップ６２２で利用者に対して期限切れが近づいていることをディスプレイ部１０２又は音声処理部１０３を用いて通知する。図７は、ステップ６２２に対応するメッセージをディスプレイ部１０２に表示させた実施例である。利用者は、ステップ６２３で上記電話番号による携帯端末

１０１より認証サーバ２０１に対して、有効期限延長要求を行う。要求を受けた認証サーバ２０１は、ステップ６２４でデータベース３０１を検索し、ステップ６２５で要求を送信してきた上記電話番号による携帯端末１０１に関する情報が登録されているかどうかを確認する。データベース３０１に未登録の上記電話番号による携帯端末からの要求であると判断された場合、ステップ６２６で利用者に対し期限延長拒否通知を行う。この後、利用者が有効期限の延長手続きを行わずに有効期限が切れてしまうと、ゲートウエイ装置４０１により使用が禁止され、上記電話番号による携帯端末１０１は利用できなくなる。使用禁止の流れについては、図６の説明において具体的に述べる。ステップ６２５で認証サーバ２０１が、データベース３０１に登録済の上記電話番号による携帯端末からの要求であると判断したときは、ステップ６２７で上記電話番号による携帯端末１０１に対し、生体情報の入力要求を送信する。生体情報入力要求を受信した上記携帯端末１０１は、利用者に対し生体情報の入力を促すメッセージを出力する。利用者は、上記携帯端末１０１より生体情報を入力し、認証サーバ２０１に送信する。生体情報信号を受信した認証サーバ２０１は、ステップ６３０でデータベース３０１に登録されている上記電話番号に関する情報に対応した生体情報に関するデータと、いま上記電話番号による携帯端末１０１から送信されてきた生体情報に関するデータとを照合する。該生体情報に関するデータの照合を行った結果、同じ利用者の生体情報のデータではないと判断されたとき、認証サーバ２０１は上記電話番号による携帯端末１０１に対し、期限延長が拒否されたことを通知する。通知を受けた上記電話番号による携帯端末１０１は利用者に対し、ステップ６３１で有効期限の延長が拒否されたことを通知する。この後、利用者が有効期限の延長手続きを行わずに有効期限が切れてしまうと、ゲートウエイ装置４０１で禁止され、上記電話番号による携帯端末１０１は利用できなくなる。使用禁止の流れについては、図６の説明において具体的に述べる。ステップ６３０で同じ利用者の生体情報のデータであると判断すると、認証サーバ２０１は、上記電話番号による携帯端末１０１から送信されてきた生体情報のデータは利用者本人からの要求であると判断し、ステップ６３２でデータベース３０１に対し、期限延長の設定を行う。期限延長の設定が完了すると、認証サーバ２０１はステップ６３３で上記電話番号による携帯端末１０１に対し、有効期限の延長が許可されたことを通知する。許可信号を受信した上記携帯端末１０１は、利用者に対し、ステップ６３４で有効期限が延長されたことをディスプレイ部１０２又は音声処理部１０３を用いて通知する。

【００３２】

次に、本発明に係る携帯端末本人確認システムにおける使用禁止処理の一実施例について図６を用いて説明する。図６は、使用禁止処理の一実施例を示す流れ図である。認証サーバ２０１は、新規登録時または前回の継続手続き時に設定された有効期限まで、規定の日数以内になると、ステップ６４１で電話番号による携帯端末１０１に対して有効期限切れが近づいていることをゲートウエイ装置４０１を介して通知する。有効期限切れが近づいていることを調べる方法は上記図５の説明で述べた通りである。通知を受信した電話番号による携帯端末１０１は、ステップ６４２で利用者に対して期限切れが近づいていることをディスプレイ部１０２又は音声処理部１０３を用いて通知する。期限切れが近づいているにもかかわらず、利用者が、上記図５で説明した、有効期限延長期限の手続きを行わなかった場合、さらに日数が経過すると、認証サーバ２０１がステップ６４３で有効期限切れを検出する。有効期限切れを検出した認証サーバ２０１は、ステップ６４４でゲートウエイ装置４０１に対し、当該携帯端末の使用禁止設定指示を行う。使用禁止設定の指示を受けたゲートウエイ装置４０１は、ステップ６４５で使用禁止設定の処理を行い、処理が終わると認証サーバ２０１に対して応答する。応答信号を受信した認証サーバ２０１は、ステップ６４６で上記電話願号による携帯端末１０１に対して使用禁止応答信号を送信する。応答信号を受信した上記携帯端末１０１は、ステップ６４７で利用者に対し、当該携帯端末の使用が禁止されたことを例えばディスプレイ部１０２又は音声処理部１０３を用いて通知する。図８は、ステップ６４７に対応するメッセージをディスプレイ部１０２に表示させた実施例である。

【００３３】
以上説明したように本実施の形態は、プリペイド携帯電話における本人確認の方法に関する発明であるが、これを管理区域への入退室管理システムにも応用できる。また、本実施の形態によれば、電話番号と生体情報をリンクさせて、サーバ側でまとめて情報を管理するため、第３世代携帯端末で一般的になっている、ＵＳＩＭカード等による携帯端末切り替えに対しても、特別な手続き等を行うことなく適用可能である。

【図面の簡単な説明】

【００３４】
【図１】本発明に係る携帯端末本人確認システムの一実施の形態を示すシステム構成図である。
【図２】図１に示す携帯端末における、音声処理部の一実施例を示す構成図である。
【図３】図１に示す携帯端末における、生体情報入力部の一実施例を示す構成図である。
【図４】本発明に係る携帯端末本人確認システムにおいて、新規登録処理の一実施例を示すフロー図である。
【図５】本発明に係る携帯端末本人確認システムにおいて、継続手続きの一実施例を示すフロー図である。
【図６】本発明に係る携帯端末本人確認システムにおいて、使用禁止処理の発生の一実施例を示すフロー図である。
【図７】本発明に係る、利用者に対して有効期限切れが近づいていることをメッセージにてディスプレイ部に出力した表示の実施例を示す図である。
【図８】本発明に係る、利用者に対して有効期限が切れてしまったことをメッセージにてディスプレイ部に出力した表示の実施例を示す図である。

【符号の説明】

【００３５】
１０１…携帯端末、１０２…ディスプレイ部、１０３…音声処理部、１０３１…マイク部、１０３２…スピーカ部、１０３３…音声データ変換部、１０４…通信部、１０５…生体情報入力部、１０５１…スキャナ部、１０５２…生体情報データ変換部、１０６…端末制御部、１０７…データ入力部、１０８…記憶部（ＵＳＩＭカード等）、２０１…認証サーバ、２０２…サーバ制御部、２０３…認証部、３０１…データベース、４０１…ゲートウエイ装置（基地局（交換機））、４０２…インターネット網、４０３…電話網。

【図１】

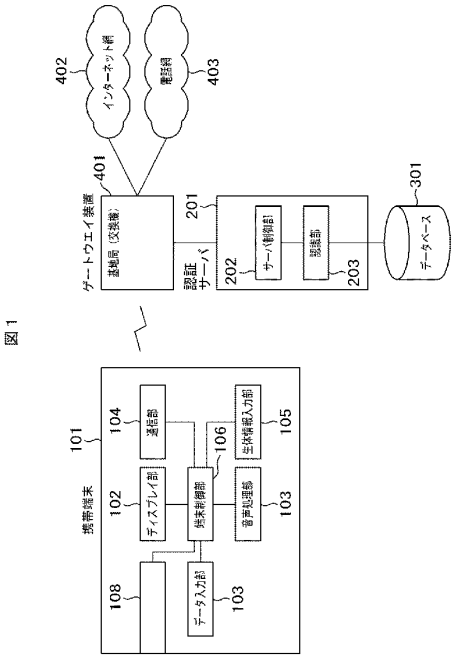
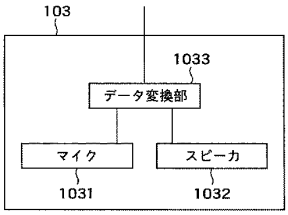


図１

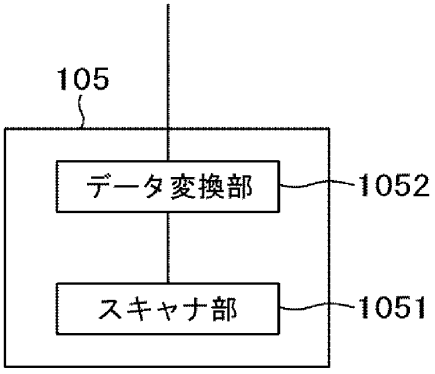
【図２】

図２



【図３】

図３



【図４】

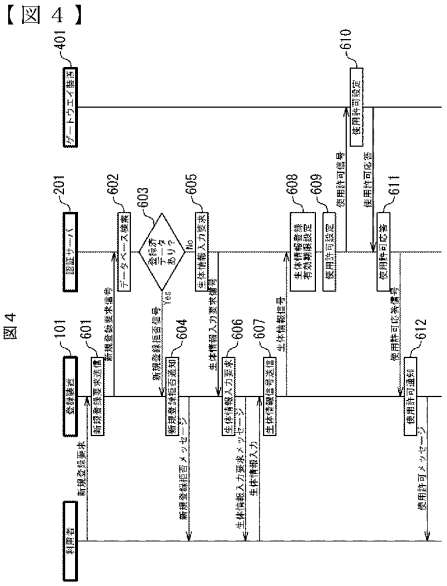
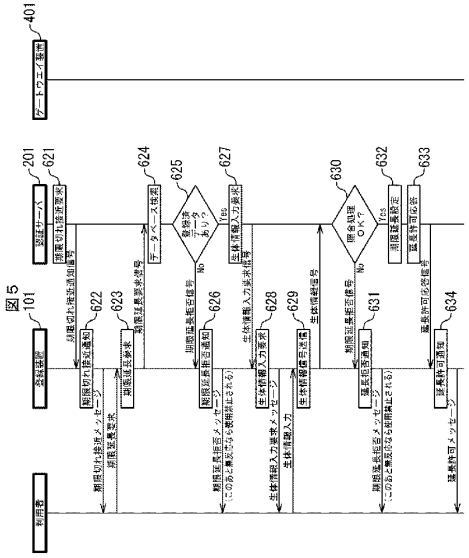
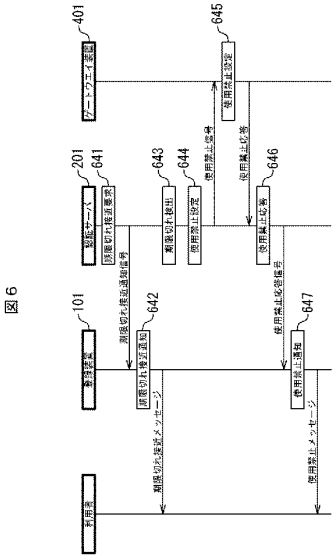


図４

【図５】



【図６】



【図７】

図７

To：USER @aaa.bbb.jp
Fm：ADMIN @xxx.yyy.jp
Message：
この端末は、有効期限が近づいております。
（期限： yyyy 年 mm 月 dd 日）
下記リンク先にアクセスして、有効期限延長の手続きを行ってください。
ここをクリック

【図８】

図８

To：USER @aaa.bbb.jp
Fm：ADMIN @xxx.yyy.jp
Message：
この端末は、有効期限切れになっております。
（期限： yyyy 年 mm 月 dd 日）
引き続きご利用を希望される場合は、最寄のzzzショップまでご連絡下さい。

フロントページの続き

(72)発明者　山川　泰明
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内
(72)発明者　丹下　智之
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内
(72)発明者　長谷川　篤
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所ネットワークソリューション事業部内

Fターム(参考)　5B285 AA04　CB12
5J104 AA07　KA16　PA01　PA02　PA07
5K027 AA11　BB09　HH23
5K067 AA32　AA33　BB04　DD17　DD27　EE02　EE10　EE16　FF02　HH22
HH36　KK15

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 September 2005 (09.09.2005)

PCT

(10) International Publication Number
WO 2005/083934 A1

(51) International Patent Classification[7]: H04L 12/16, H04Q 7/20

(21) International Application Number: PCT/CA2005/000286

(22) International Filing Date: 25 February 2005 (25.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/548,096 27 February 2004 (27.02.2004) US

(71) Applicant *(for all designated States except US)*: **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Philip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SHENFIELD, Michael** [CA/CA]; 38 Stockdale Crescent, Richmond Hill, Ontario L4C 3S9 (CA). **GORING, Bryan** [CA/CA]; 1542 Morse Place, Milton, Ontario L9T 5V4 (CA). **TSENTER, Igor** [CA/CA]; 62 Hawkview, Woodbridge, Ontario L4H 2E2 (CA).

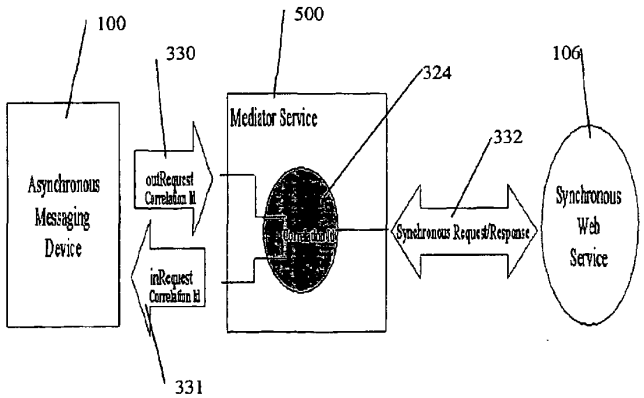
(74) Agent: **TISDALL, Grant**; Gowling Lafleur Henderson LLP, Suite 4900, Commerce Court West, Toronto, Ontario M5L 1J3 (CA).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR COMMUNICATING ASYNCHRONOUSLY WITH WEB SERVICES USING MESSAGE SET DEFINITIONS



(57) Abstract: A system and method for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages. The system and method comprising: a message correlation set configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the asynchronous response message when received, the first identifier different from the second identifier; a message manager for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

WO 2005/083934 A1

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

System and Method for Communicating Asynchronously with Web Services Using Message Set Definitions

BACKGROUND

This application relates generally to wireless communication and specifically to network messaging for mobile communication devices.

There is a continually increasing number of mobile communication devices in use today, such as mobile telephones, PDAs with wireless communication capabilities, and two-way pagers. Software applications which run on these mobile communication devices increase their utility. For example, a mobile phone may include an application which retrieves the weather for a range of cities, or a PDA may include an application that allows a user to shop for groceries. These software applications take advantage of the mobility of these devices and connectivity to a wireless network in order to provide timely and useful services to users, regardless of where the users are. However, due to the restricted resources of mobile communications devices, and the complexity of delivering data wirelessly to a mobile communication device, developing software applications for mobile communications devices remains a difficult and time-consuming task.

Web Services are emerging as the de-facto mechanism to allow disjoint parties to collaborate on the Internet. Web services allow businesses and other parties to collaborate in a universal, platform and language neutral way and promise to overcome traditional barriers encountered in linking numerous and diverse information systems. Web services are still in their relative infancy, with many technology players cooperating to define the emerging standards, and corporations beginning to throw their weight behind the thrust to link disparate systems over the web using this standard approach. A common model employed in web service offerings is the traditional synchronous request-response type interaction whereby the consumer of the service passes some information and receives something in response. In this scenario the user of the device requests or **"pulls"** the content from the network. In other words, the content is

BNSDOCID: <WO_____2005083934A1_I_>

constantly present in the network, but the user needs to issue a retrieval request to access the information (e.g. using a browser on the mobile device).

In real-life applications there is a lot of information that is available to a user but hardly accessible, as the user doesn't know when the information is posted or when there is a change in the status of the posted content. Such information ideally needs to be **"pushed"** to the user either periodically or when certain predefined events occur. Some examples of possible push situations are unrequested arrival of new e-mail, stock market information, multi-user game updates, etc. This ability to push information spontaneously implies an asynchronous messaging framework. From a practical point of view, wireless communications have higher cost than wired communications and usually are characterized by higher latency times, making a 'pull' from a wireless device inherently expensive. Slow connection times sometimes might be critical to the user's experience. Push technology can be wireless friendly. Its users can benefit in a number of ways: push technology can make useful data instantly available, can improve user perception of the wireless network; can make data delivery cost effective (since the device does not have to repeatedly poll for data); and can extend battery life.

Wireless push would involve a server that, given a user's specific one-time request to be notified with specific data on predefined conditions, would send this data to the user's device as soon as the data is available and/or the conditions have been met. The communication protocol and user/device addressing are device-specific and the server must be aware of them. Web Services have become a ubiquitous standard for access to content resources as well as communicating to back-end servers. Their number and complexity have increased considerably in recent years. However, invoking Web Service operations from a wireless device using the synchronous communication method exclusively can be expensive and impractical.

SUMMARY OF THE INVENTION

Systems and methods disclosed herein provide a correlated asynchronous messaging environment to obviate or mitigate at least some of the above presented disadvantages.

BNSDOCID: <WO____2005083934A1_I_>

Wireless push would involve a server that, given a user's specific one-time request to be notified with specific data on predefined conditions, would send this data to the user's device as soon as the data is available and/or the conditions have been met. The communication protocol and user/device addressing are device-specific and the server must be aware of them. Web Services have become a ubiquitous standard for access to content resources as well as communicating to back-end servers. Their number and complexity have increased considerably in recent years. However, invoking Web Service operations from a wireless device using the synchronous communication method exclusively can be expensive and impractical. Contrary to current systems and methods there is provided a system and method for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages. The system and method comprising: a message correlation set configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the asynchronous response message when received, the first identifier different from the second identifier; a message manager for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

There is provided a system for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the system comprising: a message correlation set configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in

BNSDOCID: <WO____2005083934A1_I_>

the asynchronous response message when received, the first identifier different from the second identifier; a message manager for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

There is further provided a method for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the method comprising the steps of: sending an asynchronous request message of the communication messages; receiving an asynchronous response message of the communication messages; linking the asynchronous request message with the corresponding asynchronous response message by employing a message correlation set including a set of correlation definitions, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the asynchronous response message when received, the first identifier different from the second identifier; associating a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

There is further provided a computer program product for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the computer program product comprising: a computer readable medium; a message correlation set module stored on the medium and configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in

BNSDOCID: <WO____2005083934A1_I_>

the asynchronous response message when received, the first identifier different from the second identifier; a message manager module for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set module, the first and second data parameters also part of the message correlation set as data definitions.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features will become more apparent of embodiments of the present invention in the following detailed description, in which reference is made to the appended drawings by way of example wherein:

Figure 1 is a block diagram of a communication system;

Figure 2 is a block diagram of a mobile communication device of Figure 1;

Figure 3 is an asynchronous messaging and data relationship example of the web service of Figure 1;

Figure 4 is an example synchronous operation of the web service of Figure 3;

Figure 5 shows a mediator service correlating asynchronous to synchronous messaging of the examples of Figures 3 and 4;

Figure 6 shows an example configuration of the mediator service and runtime of Figures 1 and 5;

Figure 7 is further embodiment the system of Figure 5; and

Figure 8 is a block diagram of a component application program of Figure 9.

DESCRIPTION

Network System

Referring to Figure 1, a network system 20 comprises mobile communication devices 100 for interacting with one or more web services 106 provided via a coupled wireless network 102 and the Internet 104. The devices 100 transmit and receive requests/response messages 105, respectively, when in communication with the web services 106. The devices 100 can operate as web clients of the web services 106 by using the requests/response messages 105 in the form of message header information and associated data content, for example requesting and

BNSDOCID: <WO____2005083934A1_I_>

receiving product pricing and availability from an on-line merchant. The web service 106 is an example of a system with which client application programs 302 (see Figure 2) on the communication devices 100 interact via the wireless network 102 and the Internet 104 in order to provide utility to users of the communication devices 100. The messages 105 sent between the communication devices 100 and the web service 106 could traverse a message-map service (not shown) which converts the messages 105 between the differing formats used by the devices 100 and the web service 106.

For satisfying the appropriate requests/response messages 105, the web service 106 could communicate with the devices 100 through various protocols (such as but not limited to HTTP and component API) for exposing relevant business logic (methods) to client application programs 302 (see Figure 2) once provisioned on the devices 100. The application programs 302 of the devices 100 can use the business logic of the web service 106 similarly to calling a method on an object (or a function). It is recognized that the client application program 302 can be downloaded/uploaded in relation to the web service 106, through the messages 105 via the network 102, 104, directly to the devices 100. It is further recognized that the devices 100 can communicate with one or more web services 106 via the networks 102, 104.

Server Environment

Referring to Figure 1, the web service 106 provides information messages 105 which are used by the client application programs 302 on the communication devices 100. Alternatively, or in addition, the web service 106 may receive and use the information messages 105 provided by the client application programs 302 executed on the communication devices 100, or perform tasks on behalf of client application programs 302 executed on the communication devices 100. The web service 106 can be defined as a software service, which can implement an interface expressed using Web Services Description Language (WSDL) registered in Universal Discovery Description and Integration (UDDI), for example,and can communicate through messages 105 with client devices 100 by being exposed over the Internet 104 through an appropriate protocol such as the Simple Object Access Protocol (SOAP), for example. In some implementations, SOAP is a specification that defines the XML format for the messages 105, including a well-formed XML fragment enclosed in SOAP elements. Other parts of SOAP specify how to

BNSDOCID: <WO_____2005083934A1_I_>

represent program data as XML and how to use SOAP to do Remote Procedure Calls (RPC). These optional parts of SOAP are used to implement RPC-style applications where a SOAP request message 105 containing a callable function, and the parameters to pass to the function, is sent from the client device 100, and the service 106 returns the response message 105 with the results of the executed function. SOAP also supports document style applications where the SOAP message 105 is a wrapper around an XML document. A further optional part of SOAP defines the HTTP binding (e.g. header), whereas some SOAP implementations support MSMQ, MQ Series, SMTP, or TCP/IP transport protocols. Alternatively, the web service 106 may use other known communication protocols, message 105 formats, and the interface may be expressed in other web services 106 languages than described above. Accordingly, the services supplied by the web service 106 are utilized by the user of the devices 100 over the network 102, 104.

Client Environment

Referring to Figures 2 and 3, the applications 302 are software applications which can be written, for example, in eXtensible Markup Language (XML) and a subset of ECMAScript. An example application 302 is described in detail, for completeness purposes, with reference to Figure 10 in the Application Program 302 section found at the end of this Description Section. XML and ECMAScript are standards-based languages which allow software developers to develop the applications 302 in a portable and platform-independent way. The applications 302 can be transmitted over-the-air via the wireless network 102 and loaded into a memory module 210 of a device infrastructure 204. Alternatively, the applications 302 may be loaded via a serial connection, a USB connection, or a short-range wireless communication system such as IR, 802.11(x) and/or Bluetooth™ onto the device 100. Once loaded onto the mobile communication device 100, the applications 302 are executed by a framework 206 on the mobile communication device 100, which converts applications 302 into native code which is executed by the processor in the device infrastructure 204. Alternatively, the applications 302 may be executed as native code or interpreted by another software module or operating system on the mobile communication device 100, which provides the framework 206 as a native runtime environment, hereafter referred to generically by reference numeral 206.

Referring again to Figure 3, the applications 302 are organised as multiple tier/layer 310 applications 302, such as but not limited to a messaging layer 404 and a data layer 400. It is recognised that the application 302 can contain other layers 310, such as but not limited to a presentation layer 402 and a workflow layer 406, as further explained below with reference to Figure 10. The application 302 is configured to have a set of data definitions 314 in the data layer 400, a set of asynchronous message definitions 316 in the message layer 404 and mappings 318 that specify how the message definitions 316 are related to the underlying data definitions 314. In general, it is recognised that the application definitions 314,316 (including definitions 320,322 – see Figure 10) of the respective layers 310 can be expressed in a structured definition language such as but not limited to XML.

Data Components 400 can be defined as application 302 data represented in native code or XML, or other structured definition language. Message Components 402 can be defined as messaging data represented in native code or XML, or other structured definition language. Message components 402 may define mapping relationships to Data Components 400 that specify their definition, or how underlying data is affected through transmission or reception of the messages 330,331a,331b. The Device Runtime or framework 206 can be defined as the software that hosts and evaluates the application 302. The Device Runtime 206 provides services to manage data associated to the application 302, provides capability for asynchronous incoming 331b and outgoing messages 330 generated by the application 302, and manages relationships between messages and data. Message Mapping can be defined as a relationship existing between data 400 and message 402 components that specifies partial or complete definition of the message based on a data mapping, and how messaging interactions affect the underlying data.

Generally the data definitions 314 are distinguished as having a set of sub-elements 323 (or fields), and define a key field or identifier 324 by which the mapping 318 (from the corresponding message definition 316) to the associated data element 323 may be resolved. Messages 105 derived from the message definitions 316 can define a set of fields but may not specify key fields, which is implemented through mappings 318. The messages 105 are typically short lived; are consumed and then discarded, whereas data elements 323 corresponding to the data definitions 314 are long lived and may be restored at any time from the persistent storage

BNSDOCID: <WO____2005083934A1_I_>

210 (see Figure 2) by providing the appropriate key field value 324 by the storage service (not shown) of the device runtime 206. The messages 105, either synchronous-based or asynchronous-based, represent interactions with entities (i.e. web-services 106) outside of the Device Runtime 206 and these messages 105 are typically not correlated by the web services 106 themselves. The messages 105 may be defined as originating (i.e. out message 105) from the device runtime 206 and targeted to the external web service 106, or may be transmitted (i.e. in message 105) to the device runtime 206.

Further, message definitions 316 may define relationships to data elements 323 called mappings 318 that determine how origination or reception of the related message 105 affects the related data element 323, as for example defined by the data definition 314 of the data layer 400. This mapping 318 relation is uniquely identified by the key field 324 mapping 318 that may be determined as follows, such as but not limited to:

the mapping 318 is made directly to the data definition 314: the message 105 takes its complete definition from the data definition 314 such that the data element key field 324 value is extracted from identical message definition 316 field element (generally referred to hereafter as message mapping 318 wherein all fields of the message 105 correspond to all fields of the data definition 314); and

the mapping 318 is from a field of the message definition 316 to a field of the data definition 314: the message 105 partially defines itself such that the data element key field 324 value is extracted from mapped message field (generally referred to hereafter as field mapping 318 wherein selected fields of the data definition 314 are mapped 318 to selected fields of the message definition 316).

As an example, referring to Figure 3, consider an asynchronous web service 106 (see Figure 1) that models a pizza parlour. This web service 106 exposes the capability to register the wireless device 100 as a PizzaClient application 302 (see Figure 2) and may aynchronously deliver the user an asynchronous response message 331, e.g. a Coupon message 326 or a Special message 328, to the wireless application 302 running on the runtime environment 206 of the device 100. The set of corresponding data elements 323 and asynchronous response messages 331 to interact with the web service 106 are depicted in Figure 3, which illustrates the

BNSDOCID: <WO_____2005083934A1_I_>

PizzaClient data elements 323 and message field level mappings 318 to the outRegisterUser outgoing request message 330. The PizzaClient application 302 may contain none or more Coupon data elements 323 which are message mapped 318 directly to the inAddCoupon incoming message 326. Finally the Special data element 323 is message mapped 318 directly to the inAddSpecial incoming message 328. It is noted that the inAddCoupon 326 and inAddSpecial 328 are asynchronous messages 331, such that each arriving message 326,328 identifies its own key field (from mapping 318) that affects the underlying data element 323. For example, once the messages 326,328 are received by the application 302, the persistence service (e.g. data manager) of the device 100 may create a new data element or update an existing data element resident in the storage 210 (see Figure 2).

Further, referring to Figure 4, suppose that the Pizza Shop now wants to extend their web service 106 by allowing the user of the device 100 to order a pizza. The web service 106 can be enhanced to provide a synchronous message operation 332 that accepts some order criteria and returns order confirmation and delivery time. The order request is distinguished by an order id (this becomes the data key 324 preferably a unique identifier), and the order confirmation id 325 is associated with uncorrelated data from the web service 106 describing the success of the order. Correlation of the return data from the Web Service's 106 perspective is achieved by the synchronous request-response nature of the submission operation 332. However correlation of the returned data within the framework of the asynchronous messaging model (see Figure 3) of the device runtime environment 206 is not immediately apparent, due to the fact that the order confirmation data returned by the web service 106 is uncorrelated to the request by any key 324 information, which if included would tie the result to the original order data element. As depicted in Figure 4, two asynchronous message definitions 316 are used to generate corresponding messages 105 to handle the order placement (outPlaceOrder) and reception of order confirmation (orderConfirmation). The mediator 500 (see Figure 5) is used to help link the order confirmation information directly to the originating Order data element, as further described below.

Referring again to Figures 1 and 2, the client runtime environment 206 provided by the devices 100 can be configured to make the devices 100 operate as web clients of the web

BNSDOCID: <WO____2005083934A1_I_>

services 106. The client runtime environment 206 of the devices 100 is preferably capable of generating, hosting and executing the client application programs 302 (which are in the form of tiered/layered 310 applications – see Figure 3) on the device 100. Further, specific functions of the client runtime environment 206 can include such as but not limited to support for language, coordinating memory allocation, networking, management of data during I/O operations, coordinating graphics on an output device of the devices 100 and providing access to core object oriented classes and supporting files/libraries.

The terminal runtime environment 206 of the devices 100 preferably supports the following basic functions for the resident executable versions of the client application programs 302, such as but not limited to:

provide a communications capability to send the messages 105 to the Web Services 106 connected via the network 102, 104;

provide data input capabilities by the user on the input interface 202 (see Figure 2) of the devices 100 to supply data parts for Web Services' outgoing messages 105 (messages to the service 106);

provide data presentation or output capabilities for Web Services' response messages 105 (incoming messages) or uncorrelated notifications of the web service 106 on the output interface 202;

provide data storage services to maintain local client data in the memory module 210 (see Figure 9) of the device 100; and

provide an execution environment for a scripting language for coordinating operation of the application layers 400, 402, 404, 406 (see Figure 10) of the client application programs 302.

Therefore, the native client terminal runtime environment 206 provides an interface for the client application programs 302 and to the device 100 functionality of a processor 208 and associated operating system of a device infrastructure 204. The runtime environment 206 preferably supplies a controlled, secure and stable environment on the device 100, in which the component application programs 302 execute. The runtime environment 206 provisions the definitions of the layers 400, 402, 404, 406 to create the actual web client.

BNSDOCID: <WO____2005083934A1_I_>

Communication Device

Referring to Figures 1 and 2, the communication devices 100 are devices such as but not limited to mobile telephones, PDAs, two-way pagers and dual-mode communication devices (see Figure 9). The devices 100 include a network connection interface such as a wireless transceiver 200 coupled via connection 218 to the device infrastructure 204. The wireless transceiver 200 is connectable during operation of the devices 100 to the network 102, 104, such as to the wireless network 102 by RF links, which enable the devices 100 to communicate with each other and with external systems (such as the web service 106) via the network 102, 104. The wireless transceiver 200 also helps the device 100 to coordinate the requests/response messages 105 between the client application programs 302 and the service 106. The network 102, 104 supports the transmission of data in the requests/response messages 105 between devices 100 and external systems, which are connected to the network 102, 104. The network 102, 104 may also support voice communication for telephone calls between the communication devices 100 and devices which are external to the network 102, 104. A wireless data transmission protocol can be used by the wireless network 102, such as but not limited to DataTAC, GPRS or CDMA. The connection between the wireless network 102 and the Internet 104 includes an Internet Gateway (not shown), which provides for the messages 105 and associated data content to flow between the connected devices 100 and the web service 106.

Referring again to Figure 2, the devices 100 also have the user interface 202, coupled to the device infrastructure 204 by connection 222, to interact with a user (not shown). The user interface 202 can include one or more user input interface such as but not limited to a QWERTY keyboard, a keypad, a trackwheel, a stylus, a mouse, a microphone, and the user output interface such as an LCD screen display and/or a speaker. If the screen is touch sensitive, then the display can also be used as the user input device as controlled by the device infrastructure 204. The user interface 202 is employed by the user of the device 100 to coordinate the requests/response message messages 105 over the system20(see Figure 1) as employed by client application programs 302 executed in the runtime environment 206.

Referring again to Figure 2, operation of the communication device 100 is enabled by the device infrastructure 204. The device infrastructure 204 includes the computer processor 208

BNSDOCID: <WO____2005083934A1_I_>

and the associated memory module 210. The computer processor 208 manipulates the operation of the network interface 200, the user interface 202 and the runtime environment 206 of the communication device 100 by executing related instructions, which are provided by an operating system and client application programs 302 located in the memory module 210. Further, it is recognized that the device infrastructure 204 can include a computer readable storage medium 212 coupled to the processor 208 for providing instructions to the processor and/or to load/update client application programs 302 in the memory module 210. The computer readable medium 212 can include hardware and/or software such as, by way of example only, magnetic disks, magnetic tape, optically readable medium such as CD/DVD ROMS, and memory cards. In each case, the computer readable medium 212 may take the form of a small disk, floppy diskette, cassette, hard disk drive, solid state memory card, or RAM provided in the memory module 210. It should be noted that the above listed example computer readable mediums 212 can be used either alone or in combination.

Mediator Service 500

The desire to migrate towards an asynchronous messaging 105 paradigm in relation to the device 100 is further explained with reference to Figure 5, by example only, wherein a message set 600 (see figure 6) is used to facilitate asynchronous communication between the device 100 and the synchronous web service 106. For situations in which the web service 106 is an asynchronous web service 106, the message set 600 (see Figure 6) is also applicable, as further described below, wherein the device 100 may communicate directly with the asynchronous web service 106 preferably without the proxy function of the mediator 500. . It is recognized that the mediator service 500 could be hosted: on the device 100 as either part of the application 302 or as a separate service/program; on a third party server; and/or on the web service 106, as desired.

Application Synchronous Message Set 600

Referring to Figure 6, the message set 600 can be defined as a data to message set that provides for a synchronous relation of otherwise uncorrelated (asynchronous) messages 330,331. It is recognized that the message set 600 can be described in a structured definition language (e.g. markup language) such as but not limited to XML. An example of the message set is the data elements 324a,b,c and 325a,b of the data definition 314 of Figure 4. It is noted that the

BNSDOCID: <WO____2005083934A1_I_>

mediator service 500 can optionally proxy synchronous messaging 332 interaction with the web service 106 into the asynchronous exchange of messages 330,331 to the Device Runtime 206 of the device 100. The message Set 600 is a logical grouping of messages definitions 330,331 (see figure 4) of the message definition tier 404 and data elements 324a,b,c of the data tier 400 included for the outgoing asynchronous message 330 content and the data elements 325a,b included in the incoming asynchronous message 331 content. The data definition 314 of the data tier 400 states a correlation between otherwise unrelated asynchronous messages by defining the data 324a,b,c and 325a, as the message set 600. The message set 600 applies a restriction to the otherwise unrestricted asynchronous messaging 330;331 paradigm.

For example, the message set can be further defined as: a single data element definition 314 to which messages 330,331are correlated; one or more outgoing messages 330 that are derived from the data definition 314; and one or more incoming messages 331 that are applied to the data definition 314.

Referring to Figure 7 for example, the problem of correlating a Pizza Shop order could be addressed by defining the Message Set 600 in figure 6, where the outPlaceOrder message 330 and orderConfirmation message 31 are correlated to the Order data definition 314 and clearly define how outgoing and incoming asynchronous messages 330,331 affect the underlying data elements as defined by the definition 314. The outPlaceOrder message 330 complies to the agreement of outgoing messages in the message set 600 by linking to the key field 324a of Order definition 314, i.e. outgoing message 330 definitions may be constrained in that they provide a linkage 440 (see figure 4) to the key element 324a of the data definition 314. This may arise due to Message Mapping or Field Mapping, as described above. The orderConfirmation incoming message 331 conforms to the incoming message requirement of the message set 600 for example by not linking to any key field 324a of the Order data definition 314, rather containing an identifier field 325a that is also part of the message set 600, i.e. incoming message 331 definitions specify Field Mapping 442 directions to the Message Set 600 enclosed by the data element definition 314. Incoming message 331 definitions may be constrained in that they cannot employ Message Mapping 440, and for example no Field Mapping 442 may reference the key field element 324a of the data definition 314.

BNSDOCID: <WO____2005083934A1_I_>

It is further emphasized in relation to Figure 7 that the Mediator Service 500 may act as a proxy to the device runtime 206 asynchronous messaging 330,331 so as to assist the device 100 to interact asynchronously with a synchronous message 332 based web service 106. However, the Mediator Service may or may not be present between the device 100 and the web service 106 in cases where the web service is asynchronous based and has knowledge of the message set definitions 600. A further scenario is that the mediator service 500 is present between the device 100 and the web service 106 and has knowledge of the message set 600 definitions and can therefore either interact with the web service 106 in a synchronous fashion or asynchronously as dictated by the configuration of the web service 106. The Mediator Service 500, where used, is able to maintain correlation information of the message set 600 between the incoming device message 330 (i.e. in essence the outgoing request to the web service 106) and the outgoing device message 331 (in essence the response by the web service 106). It is further recognized that where used, the mediator service 500 can be part of the device 100, part of the web service 106, and/or configured as a third party proxy.

Message Set Components

Referring to Figure 6, in this system 20, the management of correlation of asynchronous messages 330,331 can be split between the intelligent Device Runtime 206 and the Mediator service 500 using the message set definitions 600. The larger part of this management burden can be borne by the device framework 206. The Device Runtime 206 is primarily responsible for managing the Message Set 600 and relationships, and correlating received messages 331 to prior originating messages 330. The Mediator Service 500, for example, splits the web service 106 request into the asynchronous exchange of messages 330,331 with the device 10, if needed, and associates the correlation information of the message set 600 between related messages 330,331.

Device Runtime Modules

The runtime environment 206 can have a Message Correlation Service 602 responsible for enforcing the rules of the Message Set 600, correlating outgoing asynchronous messages 330

BNSDOCID: <WO____2005083934A1_I_>

to incoming asynchronous messages 331 to a single mapped data instance as per the data definitions 314 of the message set 600. Subsystems of the service 602 can include a message Decoder 604 for converting Communication Service 608 message protocol (i.e. for incoming messages 331) into internal operable message format of the device 100 where needed, an Encoder 606 for converting internal message representation of the device 100 into format required to support protocol of the Communication Service 608 (i.e. for outgoing messages 330), and the Message Manager 610 for performing the correlation of messages 330,331 to a data instance as used by the application 302 and utilizes a message envelope of the messages 330,331 to carry the correlation Id 324a. The runtime environment 206 can also have a Data Persistence Manager 612 that persists and provides access to all instances of Data components 400 defined by the application 302. The Persistence Manager 612 permits resolution of a data instance by a key field data value 324a. It is recognised that the data instances mentioned are instantiated versions of the data definition 314 as utilised by the device 100 during operation of the application 302 as a result of direct or indirect interaction with the web service 106. A UI Service 614 provides interaction with the user of the device interface 202 (see Figure 2) via visualization of screen definitions 404 (of the application 302), knows when a user action corresponds to changes in underlying data, and knows when a particular user action results in interaction with the associated web service (e.g. sends the message 330). It is also recognised that the Communication Service 608 can provide an over the air (OTA) interface of the device 100.

For example, one scenario is for the Communication Service 608 to use a synchronous mechanism to transmit messages 330,331 to the Mediator Service 500 or the web service 106 directly (not shown), and can offer a synchronous listener interface for arriving messages from the mediator 500 or web service 106. As such the Communication Service 608 can provides a device facing asynchronous messaging mechanism to device applications 302, i.e. provide synchronous messaging 330,331 between the mediator 500 or web service 106 while providing asynchronous messaging internally of the device 100 with the message manager 610. a second scenario is for the communication service 608 to act as a simple messaging network 20 interface for the device 100 and therefore transfer asynchronous messages 330,331 outgoing and incoming with respect to the device 100.

BNSDOCID: <WO____2005083934A1_I_>

Mediator Service Modules

When utilized as a proxy between asynchronous and synchronous environments, the mediator service 500 can have a Synchronous Dispatcher module 614 for performing the messaging 332 interaction with the synchronous web service 106. The Synchronous Dispatcher 614 maintains the correlationId 324a between the arriving device message 330 and the departing device message 331. The Synchronous Dispatcher 614 is able to detect when the message 330 has arrived and is sitting at an Async Receiver 616, which receives and queues arriving device message 330 envelopes. On receipt of the message 330, the receiver 616 releases the connection (i.e. returns immediately to the device 100). As well, The Synchronous Dispatcher 615 is able to detect when the message 332 has arrived from the web service 106 and forwards the appropriate message 331 to an Async transmitter 618, which initiates the outgoing connection to the device 100, passes the outgoing message 331envelope with correlation Id 325a as received from the web service 106. Finally, an optional Decoder 620 for transforming the incoming device message 330 into an internal operable format that can be utilized by the Synchronous Dispatcher 615 for submission to the webservice 106, and an optional Encoder 622 for transforming the web service 106 result data (e.g. data element 325b) into the outgoing device message 331from an internal operable format.

Message Set and Mediator Service Operation

This section describes the interactions between the device runtime 206 and the web service 106 to satisfy asynchronous messaging in the context of a Pizza Shop order process example. Referring to Figure 6, the following steps can be performed such as but not limited to:

1. In response to user interaction with a screen of the user interface 202, the Screen Service 614 updates a data element associated to the screen, i.e. the device Runtime generates the Order data element based the interaction with the application 302 user;
2. The Screen Service 614 detects via application metadata of the message set 600 that a rule indicating that the message 330 is sent on update of this data item. The Screen Service 614 requests the Message Manager 610 to send the appropriate message 330, and supplies the data instance (e.g. data definition 314) required to allow message creation;

BNSDOCID: <WO____2005083934A1_I_>

3. The Message Manager 610 examines the Message Set 600 definitions of the application 302, and determines that the message 330 requested in 1 is part of the Message Set 600. The key field 324a of mapped data is determined from the message set 600 definition (e.g. link 440 – see figure 4) and this value is reserved as the *correlationId* 324a;
4. The Message Manager 610 passes the data instance and outgoing message metadata definition 600 to the Encoder module 604. The Encoder module 604 takes the internal metadata representation of the message 330, and the provided values, and generates the message 330 supporting the protocol of the Communication Service 608, such that the device Runtime 206 generates the outPlaceOrder message330 from the Order data definitions 314 using mapping instructions in the Message Set 600. The outPlaceOrder message can contain the *id* 324a, *user*324b and *special* 324c fields derived from the Order *orderId*, *userId* and *specialName* fields of the data definition 314 as specified in the message set 600. The Device Runtime 206 detects that the orderId 324a represents the key field of the data element representing the data definition 314 and includes a token in the outPlaceOrder message 330 envelope that distinguishes this field as the correlation id 324a;
5. The Message Manager 610 adds the *correlationId* 324a to the envelope of the encoded message 330 request. The entire envelope is passed to the Communication Service 608 for delivery to the Mediator Service 500, if used, otherwise directly to the web service 106;

6. The Communication Service 608 initiates a connection to the Mediator Service Async Receiver 616 (or directly to the web service 106) and passes the message 330. The Async Receiver 616, if used, returns immediately to the Communication Service 608. Accordingly, the Device Runtime 206 transmits the outPlaceOrder message 330 to the Mediator Service 500, if used, which detects the correlation id 324a of the message 330;

Where Mediator synchronous request handling is used

7. The Mediator Service Synchronous Dispatcher 615 detects that the message 330 has arrived from the device 100. The message 330 is picked up from the Async Receiver 616;

BNSDOCID: <WO____2005083934A1_I_>

8. The Synchronous Dispatcher 615 obtains the *correlationId* 324a from the message 330 envelope and passes the message 330 data to the Decoder 620 to obtain the message content;
9. The Synchronous Dispatcher 615 initiates a synchronous request 332, for example, to the web service 106 with the data obtained in step 8. The Mediator Service 500 initiates the synchronous request 332 to the web service 106 using the outPlaceOrder parameters 324a,b,c, where the field 324b can identify the user and/or device 100 and/or application 302 originating the message 330. the field 324c can be a data value sent to the web service 106 as generated by the application 302. The web service 106 processes the information 324a,b,c of the message 330 and immediately returns a result 325a,b. The web service response 332 is returned in the same cycle as the request 332;
10. The Synchronous Dispatcher 615 passes the response data to the Encoder 622 to produce the required device response message 331. The Synchronous Dispatcher 615 adds the *correlationId* 325a to the envelope of the message 331 in response to the data received from the web service 106. The Mediator Service 500 therefore obtains the result 325a,b and generates the orderConfirmation message 331. The correlation id 325a is embedded in the envelope of the orderConfirmation message 330 as well as any data 325b (e.g. an update to the data element deliverytime of the data definition 314. The Mediator Service 500 transmits the message 331asynchronously/synchonously to the Device Runtime 206; and
11. The message 331 is passed to the Async Transmitter 618 which...
12. Calls the device 100 passing the message 331. The device 100 returns to the Mediator service 500 immediately.

It is recognised that in the above given mediator example that the web service could be substituted in the mediator's 500 stead, where the web service 106 would be responsible for placing the id 325a in the message 331 as per the expected shared definitions of the message set 600. At the device 100, further steps:

Device 100 asynchronous message reception and handling

BNSDOCID: <WO_____2005083934A1_I_>

13. The device Communication Service 608 passes the received message 331 to the Message Manager 610. The Message Manager 610 obtains the *correlationId* 325a from the envelope of the message 331;
14. The Message Manager 610 passes the message 331 to the Decoder 606 which converts the message 331 into an internal operable representation if needed;
15. The Message Manager 610 queries the Message Set 600 definitions and determines that the received message 331 belongs to a particular set as per the id 325a. The Message Manager 610 determines the Data instance to which incoming messages apply. The Device Runtime 206 receives the orderConfirmation message 330 and detects that this message is part of the Pizza Order message set 600; and
16. The Message Manager 610 resolves the data instance using the *correlationId* 325a as the id value, and updates the data instance according to mapping rules described in the Message Set 600. It extracts the correlation id 325a, resolves the underlying data element (Order) in view of field element 325b and applies the orderConfirmation mappings to this instance.

Application Program 302

Referring to Figure 8, a block diagram of the component application program 302 comprises the data layer 400, the presentation layer 402 and the message layer 404, which are coordinated by workflow layer 406 through communications 214 with the client runtime environment 206. The structured definition language can be used to construct the definitions 314,316,320 of the layers 400, 402, 404 as a series of metadata records, which consist of a number of pre-defined elements representing specific attributes of a resource such that each element can have one or more values. Each metadata schema typically has defined characteristics such as but not limited to; a limited number of elements, a name of each element, and a meaning for each element. Example metadata schemas include such as but not limited to Dublin Core (DC), Anglo-American Cataloging Rules (AACR2), Government Information Locator Service (GILS), Encoded Archives Description (EAD), IMS Global Learning Consortium (IMS), and Australian Government Locator Service (AGLS). Encoding syntax allows the metadata of the layers 400, 402, 404 to be processed by the device infrastructure 204 (see Figure 2), and encoding schemes include such as but not limited to XML, HTML, XHTML,

BNSDOCID: <WO_____2005083934A1_I_>

XSML, RDF, Machine Readable Cataloging (MARC), and Multipurpose Internet Mail Extensions (MIME). The client runtime environment 206 can operate on the metadata descriptors of the layers 400, 402, 404 to provision an executable version of the application program 302. It is recognised that the layers 402 and 406 can be provided by other means for the application 302, such as but not limited to native code and other defined execution languages. The application 302 can make use of the data 400 and message 404 layers to implement mappings 318 (see Figure 3) between fields of the definitions 314,316,320 to help correlate asynchronous messaging 105 between the device 100 and the web service 106.

Referring again to Figure 8, the data layer 400 defines data entities (definitions 314) which are used by the application program 302. Examples of data entities which the data layer 400 may describe are orders, users, and financial transactions. The Data layer 400 defines what information is required to describe the data entities, and in what format the information is expressed. For example, the data layer 400 may define such as but not limited to an order which is comprised of a unique identifier for the order which is formatted as a number, a list of items which are formatted as strings, the time the order was created which has a date-time format, the status of the order which is formatted as a string, and a user who placed the order which is formatted according to the definitions 314 of the data layer 400.

Referring again to Figure 8, the message layer 404 defines the format of messages 105 used by the application program 302 to communicate with external systems such as the web service 106. For example, one of the message definitions 316 may describe such as but not limited to a message for placing an order which includes the unique identifier for the order, the status of the order, and notes associated with the order.

It is noted that the use of layers 402 and 406 may be optional for the application 302.

Referring again to Figure 8, the optional presentation layer 402 defines the appearance and behavior of the application program 302 as it displayed by the user interface 202. The presentation layer 402 can specify GUI screens and controls, and actions to be executed when the user interacts with the application 302 using the user interface 202. For example, the presentation

BNSDOCID: <WO_____2005083934A1_I_>

definitions 320 may define screens, labels, edit boxes, buttons and menus, and actions to be taken when the user types in an edit box or pushes a button. The majority of Web Service 106 consumers use a visual presentation of Web Service 106 operation results, and therefore provide the runtime environment 206 on their devices 100 capable of displaying user interface screens.

Referring to Figures 1 and 8, it is recognized that in the above described client application program 302 definitions hosting model, the presentation layer 402 may vary depending on the client platform and environment of the device 100. For example, in some cases Web Service consumers do not require a visual presentation. The application definitions 314,316,320,322 of the application program 302 can be hosted in a Web Service registry as a bundle of platform-neutral data 400, message 404, workflow 406 layer descriptors with a set of platform-specific presentation layer 402 descriptors for various predefined client runtimes 206 (see Figure 2). When the discovery or deployment request message 105 is issued the client type should be specified as a part of this request message 105. In order not to duplicate data, message, and workflow metadata while packaging application programs 302 for different client platforms of the communication devices 100, application definitions 314,316,320,322 can be hosted on the web service 106 (for example) as a bundle of platform-neutral component definitions 314,316,322 linked with different sets of presentation definitions 320. When a user makes a discovery or download request message 105, the client runtime type of the communication devices 100 is validated and the proper bundle is constructed for delivery by the web service 106 to the device 100 over the network 102, 104. For those Web Service 106 consumers, the client application programs 302 would contain the presentation layer 402 linked with the data 400 and message 404 layers through the workflow layer 406. It is recognized that the hosting model includes message 404 and data 400 layers with the remainder of the application functionality (presentation and workflow) expressed in a manner that cooperates with these defined layers 400, 404, such as but not limited to native code and other defined components as desired.

Referring again to Figure 8, the optional workflow layer 406 of the application program 302 defines processing that occurs when an action is to be performed, such as an action specified by a presentation layer 402 as described above, or an action to be performed when messages 105

BNSDOCID: <WO_____2005083934A1_I_>

(see Figure 1) arrive from the system 20. Presentation, workflow and message processing are defined by the workflow layer 406. The workflow layer 406 can be written as a series of instructions in a programming language or a scripting language, such as but not limited to ECMAScript, and can be compiled into native code and executed by the runtime environment 206, as described above. An example of the workflow layer 406 content may be to assign values to data, manipulate screens, or send the message 105. As with presentation layer 402, multiple workflow definitions 322 can be created to support capabilities and features that vary among devices 100. The appropriate workflow definition can be determined and sent at the time of downloading and provisioning of the application program 302.

ECMA (European Computer Manufacturers Association) Script is a standard script language, wherein scripts can be referred to as a sequence of instructions that is interpreted or carried out by another program rather than by the computer processor. Some other example of script languages are Perl, Rexx, VBScript, JavaScript, and Tcl/Tk. The scripting languages, in general, are instructional languages that are used to manipulate, customize, and automate the facilities of an existing system, such as the devices 100. In such systems, useful functionality is already available through the user interface 202 (see Figure 2), and the scripting language is a mechanism for exposing that functionality to program control. In this way, the device 100 is said to provide a host runtime environment of objects and facilities which completes the capabilities of the scripting language.

Specifically, EMCAScript is an object-oriented programming language for performing computations and manipulating computational objects within the host runtime environment. ECMAScript can be used as a Web scripting language, providing a mechanism to perform service 106 computation as part of the Web-based client-server architecture of the system20(see Figure 2). ECMAScript provides core scripting capabilities for a variety of host runtime environments, and therefore the core scripting language can be considered platform neutral for a number of particular host runtime environments. The runtime environment 206 (see Figure 2) can provide the ECMAScript host runtime environment for client-side computation of the communication devices 100, such as but not limited to; objects that represent windows, menus, pop-ups, dialog boxes, text areas, anchors, frames, history, cookies, and input/output. Further,

BNSDOCID: <WO____2005083934A1_I_>

the host runtime environment of the runtime environment 206 provides a means to attach scripting code to events such as but not limited to change of focus, page and image loading, unloading, error, and abort, selection, form submission, and mouse actions. In implementations using ECMA scripting, the code appears within the workflow layer 406, combines user interface elements and fixed and computed text and images, and is reactive to user interaction on the user interface 202. The web service 106 (see Figure 1) provides a different host environment for server-side computation including objects representing requests, clients, and files, and mechanisms to lock and share data. By using the client side and server side scripting together, it is possible to distribute computation between the client communication devices 100 and the service 106 while providing a customized user interface 202 for the Web-based application programs 302.

ECMAScript also defines a set of built-in operators which may not be, strictly speaking, functions or methods. ECMAScript operators include such as but not limited to various unary operations, multiplicative operators, additive operators, bitwise shift operators, relational operators, equality operators, binary bitwise operators, binary logical operators, assignment operators, and the comma operator. ECMAScript syntax resembles Java syntax, however, ECMAScript syntax is relaxed to enable it to serve as an easy-to-use scripting language for developers. For example, a variable in ECMAScript is not required to have its type declared nor are types associated with properties, and defined functions are not required to have their declarations appear textually before calls to them. It is recognized that in a class-based object-oriented programming language, in general, state is carried by instances, methods are carried by classes, and inheritance is only of structure and behavior. In ECMAScript, the state and methods are carried by objects, and structure, behavior, and state are all inherited.

Application Program 302 Example

Accordingly, referring to Figure 8, the client application programs 302 can be defined as a set of platform-neutral component definitions 314,316, namely for data 400 and message 404 layers, and the optional presentation layer 402 using XML (or any other suitable structured definition language). The optional workflow layer 406 can be defined using ECMAScript (or any other suitable platform-neutral scripting language). The client runtime environment 206 (see

BNSDOCID: <WO_____2005083934A1_I_>

Figure 2) can generate component templates based on meta-definitions when the definitions 314,316,320,322 of the application program 302 are provisioned on the communication device 100. With a large variety of terminal runtime environments 206, the cross-platform standards such as XML or ECMAScript can be used to define application component metadata instead of pre-building the application programs 302. This delayed binding can allow the generic application definitions of the component application programs 302 to be run on a wide variety of terminal system environments 206, represented by various different communication devices 100.

The following example shows how a Web Services client application program 302 could be expressed using a structured definition language, such as but not limited to XML, and a platform neutral scripting/programming language, such as but not limited to ECMAScript, with defined components conforming with the following Document Type Definition (DTD):

```
<!ELEMENT wcApp (desc?, iconUrl?, res*, wcData*, wcMsg*, style*, wcScr*, wcFlow)>

<!ATTLIST wcApp
        name CDATA #REQUIRED
        title CDATA #IMPLIED
        vendor CDATA #IMPLIED
        version CDATA #IMPLIED
        transportKey CDATA #IMPLIED
        installNotifURL CDATA #IMPLIED
        registerURL CDATA #IMPLIED
>
<!ELEMENT desc (#PCDATA)>
<!ELEMENT iconUrl (#PCDATA)>
<!ELEMENT res (#PCDATA)>
<!ATTLIST res
        name CDATA #REQUIRED
        url CDATA #REQUIRED
        type (xml | image | sound | any) #REQUIRED
        deferred (true | false) "false"
>

Example Data definitions 314
<!ELEMENT wcData (dfield+)>
<!ATTLIST wcData
        name CDATA #REQUIRED
        persisted (true | false) "true"
>
<!ELEMENT dfield (#PCDATA)>
<!ATTLIST dfield
        name CDATA #REQUIRED
        type (String | Number | Boolean | Date | Any) "Any"
        array (true | false) "false"
```


BNSDOCID: <WO____2005083934A1_I_>

```
        cmp (true | false) "false"
        cmpName CDATA #IMPLIED
        key (0 | 1 | 2) "0"
    >
    Example Message definitions 316
    <!ELEMENT wcMsg (mfield*)>
    <!ATTLIST wcMsg
        name CDATA #REQUIRED
        mapping CDATA #IMPLIED
    >

    <!ATTLIST wcMsg
        pblock CDATA #IMPLIED
    >
    <!ELEMENT mfield (#PCDATA)>
    <!ATTLIST mfield
        name CDATA #REQUIRED
        type (String | Number | Boolean | Date | Array | XML) #IMPLIED
        mapping CDATA #IMPLIED
    >

    Example Presentation definitions 320
    <!ELEMENT wcScr (layout?, menu?, refresh?, event?)>
    <!ATTLIST wcScr
        name CDATA #REQUIRED
        title CDATA #IMPLIED
        main (true | false) "false"
        dialog (true | false) "false"
        param CDATA #IMPLIED
    >
    <!ELEMENT style (font?)>
    <!ATTLIST style
        name CDATA #REQUIRED
        bgColor CDATA #IMPLIED
    >
    <!ELEMENT font EMPTY>
    <!ATTLIST font
        name CDATA #REQUIRED
        color CDATA #IMPLIED
        size CDATA #IMPLIED
        bold (true | false) "false"
        italic (true | false) "false"
        underline (true | false) "false"
    >
    <!ELEMENT refresh (msg+)>
    <!ELEMENT msg (#PCDATA)>
    <!ELEMENT layout (layout*, label*, separator*, edit*, image*, choice*, button*, textarea*)>
    <!ATTLIST layout
        type (grid | flow | border | vertical) #REQUIRED
        param CDATA #IMPLIED
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
    >
    <!ELEMENT menu (item*)>
    <!ELEMENT item (action, condition?)>
    <!ATTLIST item
```


BNSDOCID: <WO_____2005083934A1_I_>

```
        name CDATA #REQUIRED
        label CDATA #REQUIRED
        shortcut CDATA #IMPLIED
>
<!ELEMENT action EMPTY>
<!ATTLIST action
        screen CDATA #IMPLIED
        pblock CDATA #IMPLIED
        param CDATA #IMPLIED
        acceptChanges (true | false) "true"
>
<!ELEMENT condition EMPTY>
<!ATTLIST condition
        pblock CDATA #REQUIRED
        param CDATA #IMPLIED
        result (true | false) "true"
>
<!ELEMENT event EMPTY>
<!ATTLIST event
        type (onInit | onClick | onChange | onFocusOut) "onInit"
        pblock CDATA #IMPLIED
        screen CDATA #IMPLIED
        param CDATA #IMPLIED
>
<!ELEMENT separator EMPTY>
<!ELEMENT label (condition?, event?)>
<!ATTLIST label
        name CDATA #REQUIRED
        value CDATA #REQUIRED
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
>
<!ELEMENT edit (condition?, event?)>
<!ATTLIST edit
        name CDATA #REQUIRED
        value CDATA #IMPLIED
        mapping CDATA #IMPLIED
        type (char | number | date | pwd | phone | email) "char"
        readOnly (true | false) "false"
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
>
<!ELEMENT textarea (condition?, event?)>
<!ATTLIST textarea
        name CDATA #REQUIRED
        value CDATA #IMPLIED
        mapping CDATA #IMPLIED
        readOnly (true | false) "false"
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
>
<!ELEMENT image (condition?, event?)>
<!ATTLIST image
        name CDATA #REQUIRED
        resName CDATA #REQUIRED
        placement CDATA #IMPLIED
```


BNSDOCID: <WO____2005083934A1_I_>

```
>
<!ELEMENT choice (condition?, event?, entry*)>
<!ATTLIST choice
        name CDATA #REQUIRED
        value CDATA #IMPLIED
        mapping CDATA #IMPLIED
        type (singleList | multiList | dropdown | checkbox | radio) "singleList"
        readOnly (true | false) "false"
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
>
<!ELEMENT entry (#PCDATA)>
<!ELEMENT button (condition?, event?)>
<!ATTLIST button
        name CDATA #REQUIRED
        label CDATA #REQUIRED
        image (true | false) "false"
        placement CDATA #IMPLIED
        style CDATA #IMPLIED
>
```

Example Workflow definitions 322

```
<!ELEMENT wcFlow (pblock+)>
<!ELEMENT pblock (#PCDATA)>
<!ATTLIST pblock
        id CDATA #REQUIRED
        param CDATA #IMPLIED
>
```

As given above, the XML elements define the example component application 302 including a wcApp element, a wcData element, a wcMsg element, a wcSrc element, and a wcFlow element. Referring to Figure 8, the wcApp element is a top-level element which defines the application program 302. The wcData element defines the example data layer 400, which is comprised of a group of named, typed fields. The wcMsg element defines the example message layer 404, which similarly defines a group of named, typed fields. The wcSrc element defines the example presentation layer 402. The example presentation layer 402 is a label, a separator, an image, a button, an edit field, a text area, a single-selection list, a multi-selection list, a drop-list, a checkbox, a radio button, or a screen containing a group of other presentation definitions 320.

Referring to the above example component application program 302 and Figure 8, the wcFlow element defines the example workflow layer 406. The pblock attributes of the XML elements specify a pblock element nested in the wcFlow element. Each pblock element comprises script which defines part of the workflow of the application program 302. The script is

BNSDOCID: <WO_____2005083934A1_I_>

written in ECMAScript. In order to define the behavior of the application 302, the optional workflow layer 406 uses ECMAScript to reference and manipulate the data layer 400, the presentation layer 402, and the message layer 404. The workflow layer 406 can also reference external object types, which allow actions to be performed on the components defined in the application 302. For example, a wcMsg type allows a message defined by a message definition 316 to be evaluated to determine whether mandatory fields have been supplied, and to be sent to an external system such as the web service 106. A wcData type allows the size of collections of data entities defined by data definition 314 to be determined, and allows data entities to be deleted. A wcScr type allows a presentation definition 320 to be displayed to the user. Similarly, a special dialog external object allows a message to be displayed to the user on the user interface 202 (see Figure 2).

BNSDOCID: <WO_____2005083934A1_I_>

WE CLAIM:

1. A system for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the system comprising:

a message correlation set configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the asynchronous response message when received, the first identifier different from the second identifier;

a message manager for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

2. The system of claim 1, wherein the first identifier is configured for insertion in the request message by the mobile device and the second identifier is configured for insertion in the response message by the data source.

3. The system of claim 1 further comprising a communication service for providing a communication interface between the message manager and the network.

4. The system of claim 3, wherein the communication manager is configured to provide communication of the messages between the communication manager and the message manager asynchronously.

BNSDOCID: <WO_____2005083934A1_I_>

5. The system of claim 4, wherein the communication manager is configured to provide communication of the messages between the communication manager and the network asynchronously.

6. The system of claim 2 further comprising a screen service for initiating the message request based on a user data event from a user interface of the device.

7. The system of claim 6, wherein the message manager is configured for querying the message correlation set to determine if the data corresponding to the user event is defined by the message correlation set as the first data parameter.

8. The system of claim 7, wherein the message manager is configured to select the first correlation identifier of the message correlation set corresponding to the identified first data parameter as part of the message correlation set.

9. The system of claim 6 further comprising a persistence manager for resolving the persistence of the first data parameter value according to the first correlation identifier.

10. They system of claim 2, wherein the message correlation set is described in a structured definition language.

11. A method for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the method comprising the steps of:

sending an asynchronous request message of the communication messages;

receiving an asynchronous response message of the communication messages;

linking the asynchronous request message with the corresponding asynchronous response message by employing a message correlation set including a set of correlation definitions, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the

BNSDOCID: <WO_____2005083934A1_I_>

asynchronous response message when received, the first identifier different from the second identifier;

associating a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set, the first and second data parameters also part of the message correlation set as data definitions.

12. The method of claim 11, wherein the first identifier is configured for insertion in the request message by the mobile device and the second identifier is configured for insertion in the response message by the data source.

13. The system of claim 11 further comprising the step of providing a communication interface between a message manager and the network.

14. The system of claim 13, wherein the communication interface is configured to provide communication of the messages between the communication interface and the message manager asynchronously.

15. The system of claim 14, wherein the communication interface is configured to provide communication of the messages between the communication interface and the network asynchronously.

16. The system of claim 12 further comprising the step of initiating the message request based on a user data event from a user interface of the device.

17. The system of claim 16 further comprising the step of querying the message correlation set to determine if the data corresponding to the user event is defined by the message correlation set as the first data parameter.

BNSDOCID: <WO____2005083934A1_I_>

18. The system of claim 17 further comprising the step of selecting the first correlation identifier of the message correlation set corresponding to the identified first data parameter as part of the message correlation set.

19. The system of claim 16 further comprising the step of resolving the persistence of the first data parameter value according to the first correlation identifier.

20. They system of claim 12, wherein the message correlation set is described in a structured definition language.

21. A computer program product for correlating asynchronous communication messages between a mobile device and a data source over a network, the mobile device for executing an application to provide interaction with the data source based on content of the communication messages, the computer program product comprising:

a computer readable medium;

a message correlation set module stored on the medium and configured to include a set of correlation definitions for linking an asynchronous request message of the communication messages with a corresponding asynchronous response message of the communication messages, the correlation definitions including a first correlation identifier for including in the asynchronous request message when generated and a second correlation identifier expected in the asynchronous response message when received, the first identifier different from the second identifier;

a message manager module for coordinating the transmission and receipt of the messages so as to associate a first data parameter of the request message with a second data parameter of the response message by matching the first and second identifiers of the messages with the correlation definitions of the message correlation set module, the first and second data parameters also part of the message correlation set as data definitions.

BNSDOCID: <WO_____2005083934A1_I_>

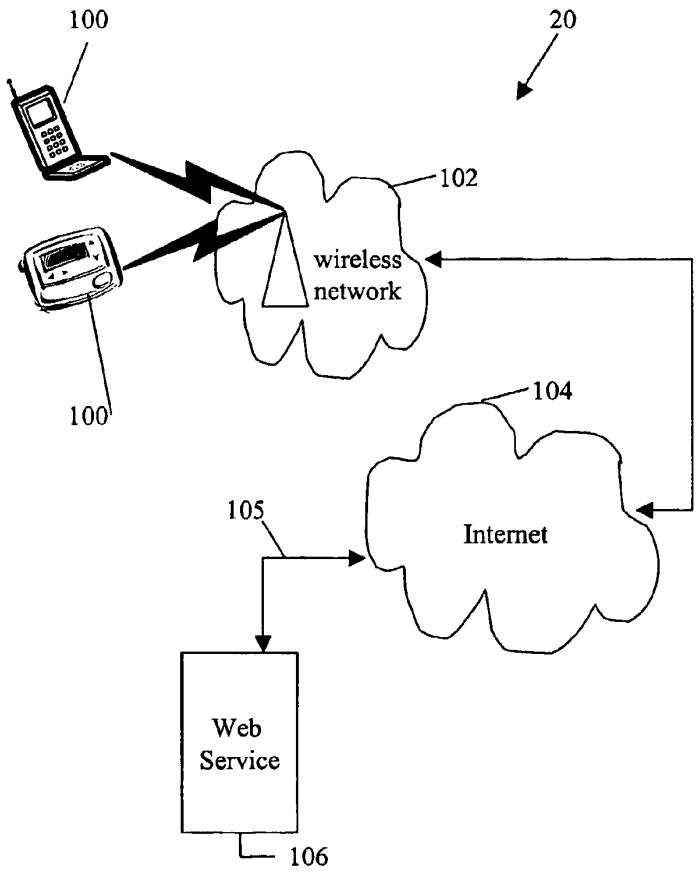


Figure 1

BNSDOCID: <WO_____2005083934A1_I_>

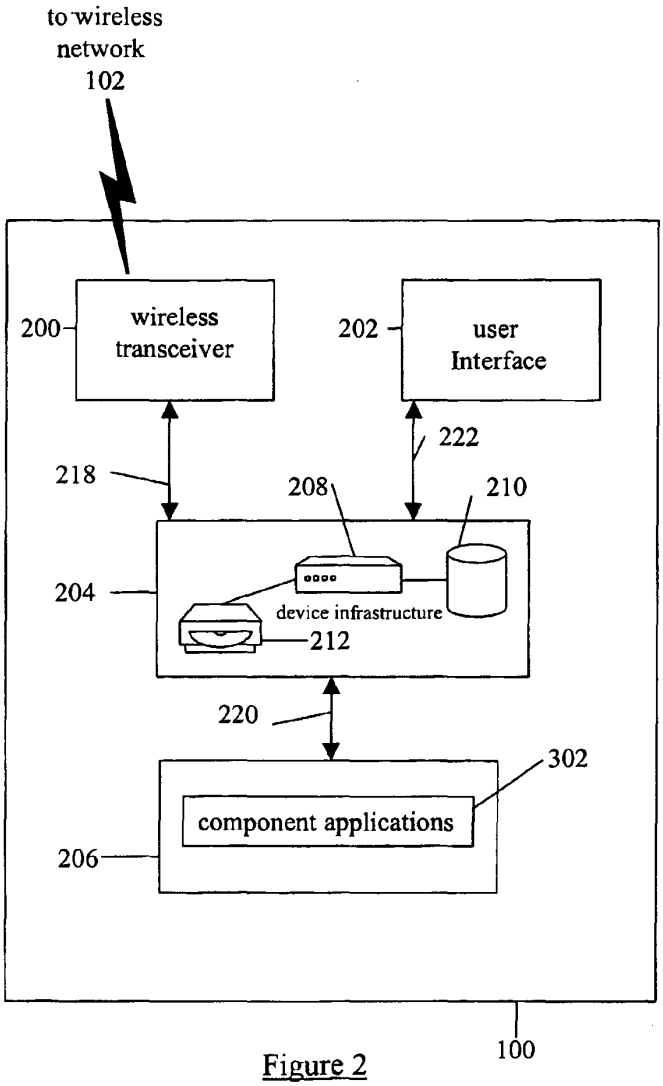


Figure 2

BNSDOCID: <WO_____2005083934A1_I_>

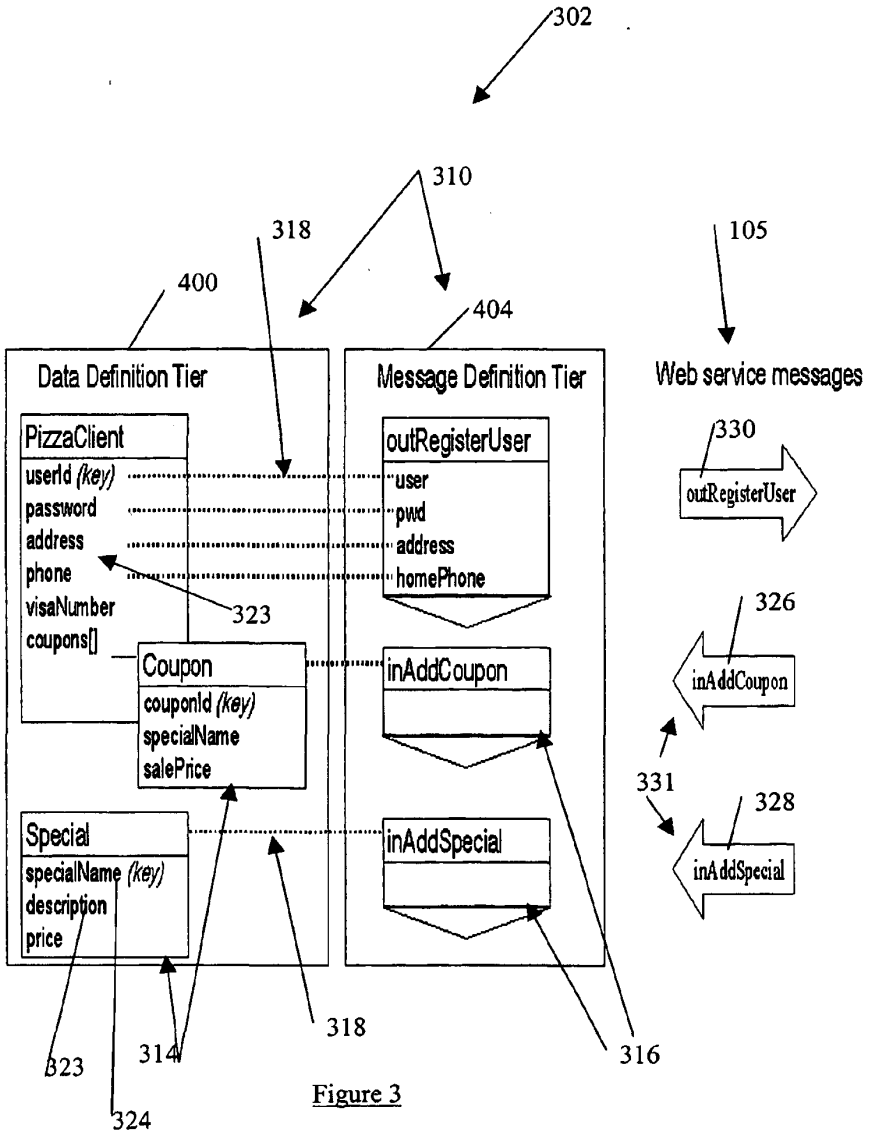


Figure 3

BNSDOCID: <WO_____2005083934A1_I_>

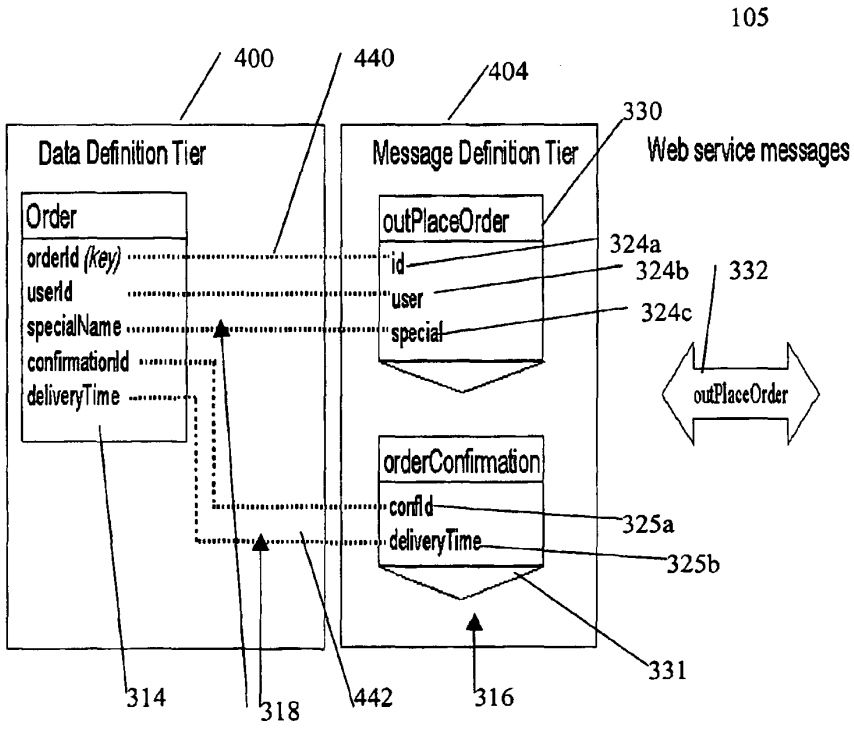


Figure 4

BNSDOCID: <WO_____2005083934A1_I_>

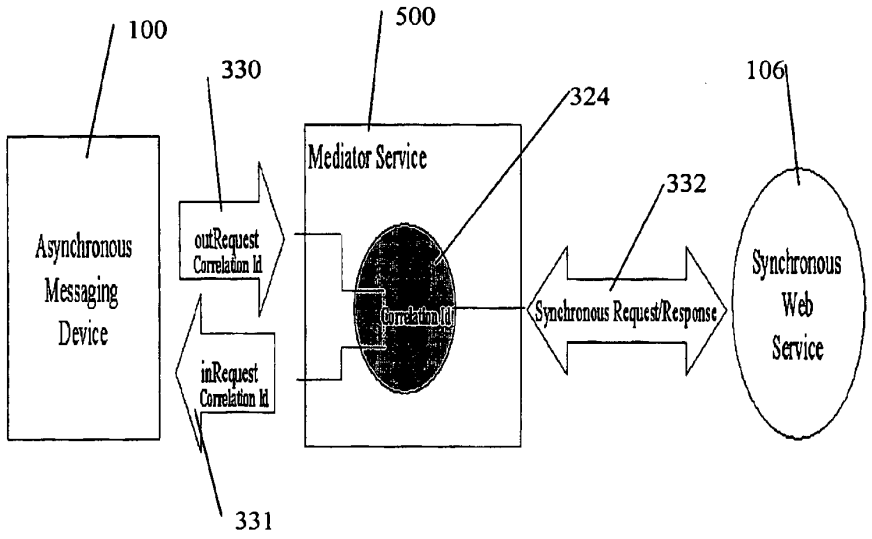


Figure 5

BNSDOCID: <WO_____2005083934A1_I_>

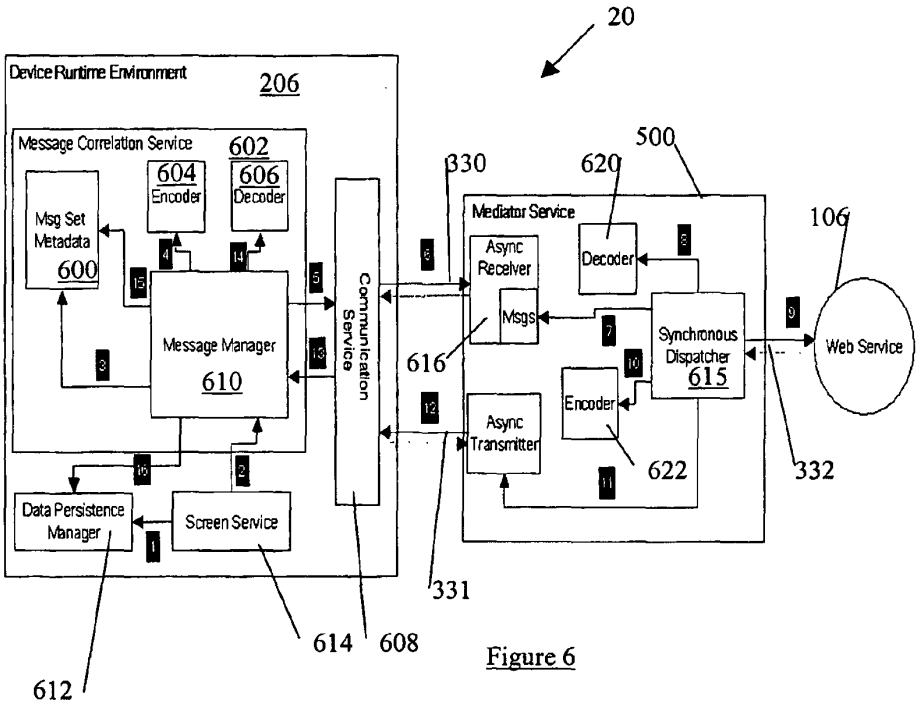


Figure 6

BNSDOCID: <WO_____2005083934A1_I_>

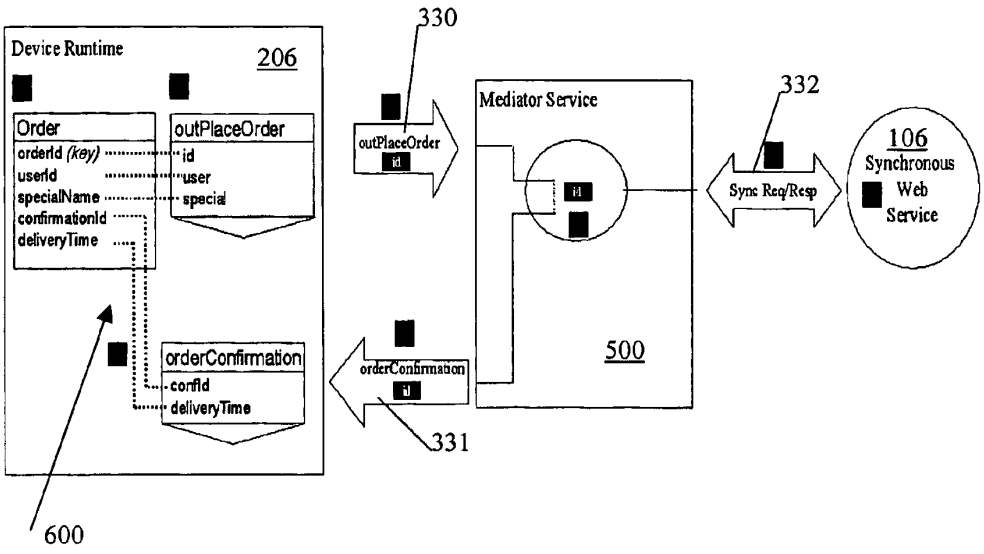


Figure 7

BNSDOCID: <WO_____2005083934A1_I_>

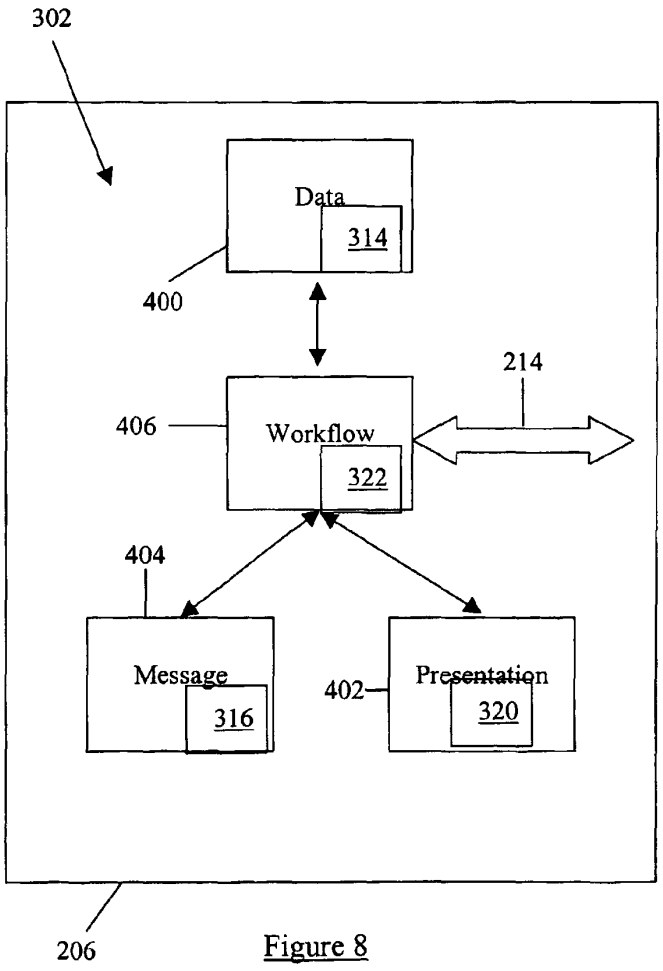


Figure 8

BNSDOCID: <WO_____2005083934A1_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2005/000286

A. CLASSIFICATION OF SUBJECT MATTER
IPC7 H04L 12/16, H04Q 7/20

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)
IPC7 H04L 12/16, H04Q 7/20

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Delphion, Canadian Patent Database - Search Terms used: web, service, asynchronous, mobile, device,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/0023127 (SABETI) 21.02.2002	1-21
A	US 2003/0206192 (CHEN et al.) 06.11.2003	1-21
A, P	US 2004/0255046 (RINGSETH et al.) 16.12.2004	1-21
A	US 6,035,324 (CHANG et al.) 07.03.2000	1-21
A, P	WO 2004/066081 (CHEENATH) 05.08.2004	1-21

[ ] Further documents are listed in the continuation of Box C.

[X] 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	Date of mailing of the international search report
08 June 2005 (08-06-2005)	5 July 2005 (05-07-2005)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001(819)953-2476	Donald Lefebvre (819) 997-2822

BNSDOCID: <WO_____2005083934A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CA2005/000286

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US6035324	07-03-2000	GB2330502 A	21-04-1999
		JP11134277 A	21-05-1999
		SG71145 A1	21-03-2000
		SG97884 A1	20-08-2003
		TW463112 B	11-11-2001
		US6035324 A	07-03-2000
US2002023137	21-02-2002	DE10030521 A1	17-01-2002
		EP1168761 A2	02-01-2002
		US2002023137 A1	21-02-2002
US2003206192	06-11-2003	AU2002367759 A1	22-09-2003
		EP1430412 A1	23-06-2004
		US2003206192 A1	06-11-2003
		WO03077139 A1	18-09-2003
US2004255046	16-12-2004	US2004255046 A1	16-12-2004
WO04066081	05-08-2004	WO04066081 A3	07-04-2005
		US20040143645 A1	22-07-2004

BNSDOCID: <WO_____2005083934A1_I_>

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2007 (25.10.2007)

PCT

(10) International Publication Number
WO 2007/120310 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2006/061532

(22) International Filing Date:
1 December 2006 (01.12.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/742,155 1 December 2005 (01.12.2005) US
11/394,782 31 March 2006 (31.03.2006) US

(71) Applicant *(for all designated States except US)*: **QUALCOMM Incorporated** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LIOY, Marcello** [CA/US]; 11629 Miro Circle, San Diego, California 92131 (US). **DYCK, Jeffrey** [CA/US]; 4816 Mt. Harris Drive, San Diego, California 92117 (US).

(74) Agents: **WADSWORTH, Philip R.** et al.; 5775 Morehouse Drive, San Diego, California 92121 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

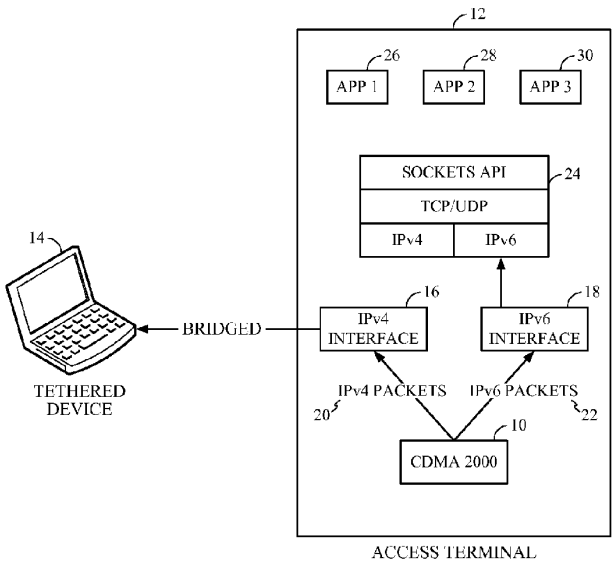
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: CONCURRENT INTERNET PROTOCOL CONNECTIVITY TO AN ACCESS TERMINAL AND A TETHERED DEVICE



(57) Abstract: Using split interfaces for Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4), and bridging the IPv4 interface, makes it possible to support a Tethered Device (TD) and an Access Terminal (AT) having concurrent IP connectivity. This configuration enables the support of IP Multimedia Subsystem (IMS) applications in the AT using IPv6 while concurrently supporting general Internet usage on a TD. It is also possible to bridge an IPv6 interface to the TD.

WO 2007/120310 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONCURRENT INTERNET PROTOCOL CONNECTIVITY TO AN ACCESS TERMINAL AND A TETHERED DEVICE

Claim of Priority under 35 U.S.C. §119

[0001] The present Application for Patent claims priority to Provisional Application No. 60/742,155 entitled "Method For Supporting Concurrent IP Connectivity To An Access Terminal And Tethered Device Each Using Different IP Protocols In CDMA 2000 Networks," Filed December 1, 2005, and assigned to the assignee hereof and hereby expressly incorporated by reference herein.

BACKGROUND

Field

[0002] The present disclosed embodiments relates generally to cellular communications, and more specifically to concurrent Internet Protocol (IP) connectivity to an Access Terminal (AT) and a Tethered Device (TD).

Background

[0003] It is desirable to support one Internet Protocol (IP) protocol to an Access Terminal (AT) and another to a Tethered Device (TD). An example of where this is desirable is with the launch of the new IP Multimedia Subsystem (IMS) services, which will provide a rich set of new Multimedia services in the mobile environment. One of these services will the Voice over IP (VoIP), which will replace traditional circuit switched voice, which is how voice services are supported today. In order to support these IMS services, an AT must be continuously connected to the IP Network, which is also known as "always-on." Typically in the case for Code Division Multiple Access (CDMA) 2000 networks this implies that it is not possible to support a TD as the AT is already in a data session.

[0004] There is therefore a need in the art for concurrent IP connectivity to an AT and a TD.

SUMMARY

[0005] Using split interfaces for Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4), and bridging the IPv4 interface, makes it possible to support a TD and

an AT having concurrent IP connectivity. This configuration enables the support of IMS applications in the AT using IPv6 while concurrently supporting general Internet usage on a TD. It is also possible to bridge the IPv6 interface to the TD.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. 1 is an illustration of a concurrently connected Access Terminal and Tethered Device.

DETAILED DESCRIPTION

[0007] The embodiments described herein make it possible to provide service concurrently to the AT and TD. Different IP protocol versions can be used by the AT and TD. In the case of IMS, it is desirable to use IP version 6 (IPv6) for the AT in order to be always on an assigned IP for as long as the AT is powered on. In order to support a wide scale deployment of these services, it would require as many IP addresses as there are ATs. In the case of IPv4 there is a dearth of addresses, so IPv6 is preferred for the AT.

[0008] For most general Internet services, such as web browsing and email, still use IP version 4 (IPv4). Thus for the TD it is desirable to have IPv4 connectivity.

[0009] The embodiments described below with reference to FIG. 1 describe how to provide IPv6 in the AT while concurrently supporting IPv4 to a TD. However, the same technique could be used to provide IPv4 to the AT and IPv6 to the TD.

[0010] IP packets arriving over an air interface 10 and based on an IP version are received by an AT 12 and are either forwarded up an AT stack 24 (for example, IPv6 packets 22) or forwarded to a TD 14 (for example, IPv4 packets 20).

[0011] There are a variety of ways this could be done:

[0012] 1. Examine the incoming packets and apply the forwarding as described in the paragraph above.

[0013] 2. Use the notion of Network Interfaces, which provide an abstraction layer, between the physical layer (in this case the CDMA2000 air interface data protocols, such as Radio Link Protocol (RLP) and Point-to-Point Protocol (PPP)) and the generic IP stack above (commonly referred to as the Transmission Control Protocol/Internet Protocol (TCP/IP) suite). This is described in more detail below.

[0014] The use of the Network Interface can provide a variety of processing options with respect to IP packets passing through them, such as filtering and routing/bridging information.

[0015] It is possible in the interface itself to identify whether or not packets should be forwarded directly to another interface without processing them further. This further processing is typically done at the IP layer, and consists of routing. Routing is the act of examining the IP addresses in the header and determining if the packet is destined for the local host, which is the device doing the routing, or another host. Typically if it is intended for another host, a determination may need to be made over which link to transmit it – if there are multiple links. If the interface is configured to directly forward the packets to another interface (or link), this is referred to as bridging the two interfaces together. This is typically used when it is known that all of the packets arriving in one interface must be transmitted over another interface, regardless of the addressing information they contain. An example of this is a Wireless LAN bridge. Any packets arriving on the Ethernet interface must be forwarded over the WLAN interface without exception.

[0016] In an AT it is desirable to have separate network interfaces for IPv4 and IPv6 as there is much information for each protocol that is independent, but needs to be duplicated, such as the state of the interface (disabled, available, configuring, etc.), IP address(es), and so forth.

[0017] Using the properties of bridging and the separation of the IPv6 and IPv4 interfaces allows an IPv4 interface 16 to be set up in bridging mode such that it forwards all IPv4 packets 20 to the TD, while leaving an IPv6 interface 18 in non-bridged mode, which results in the IPv6 packets 22 being delivered to the IP stack 24, and the payload ultimately being delivered to the IMS application. This allows IPv6 IMS applications 26, 28, and 30 on the AT 12 to work concurrently with generic IPv4 Internet applications on the TD 14.

[0018] Using this split interface/bridging solution, it is also possible to run IPv6 addresses on the TD 14 while supporting IPv4 applications on the AT 12.

[0019] When it becomes desirable to support IPv6 applications on the TD 14 as well, because the IPv6 packets are going to the IP layer 24 they could be routed to the TD as well if they are not destined for the AT 12, but rather for the TD. This would allow

both IPv4 and IPv6 applications on the TD running concurrently with IPv6 applications running on the AT.

WHAT IS CLAIMED IS:

CLAIMS

1. An Access Terminal for having concurrent Internet Protocol Activity with a Tethered Device, the Access Terminal comprising:

an Internet Protocol stack;

a first Internet Protocol version interface adapted in a non-bridged mode for delivering first Internet Protocol version packets to the Internet Protocol stack; and

a second Internet Protocol version interface adapted in a bridged mode for delivering second Internet Protocol version packets to the Tethered Device.

2. The Access Terminal of claim 1 wherein the first Internet Protocol version interface is an Internet Protocol version 6.

3. The Access Terminal of claim 2 wherein the second Internet Protocol version interface is an Internet Protocol version 4.

4. The Access Terminal of claim 1 wherein the first Internet Protocol version interface is an Internet Protocol version 4.

5. The Access Terminal of claim 4 wherein the second Internet Protocol version interface is an Internet Protocol version 6.

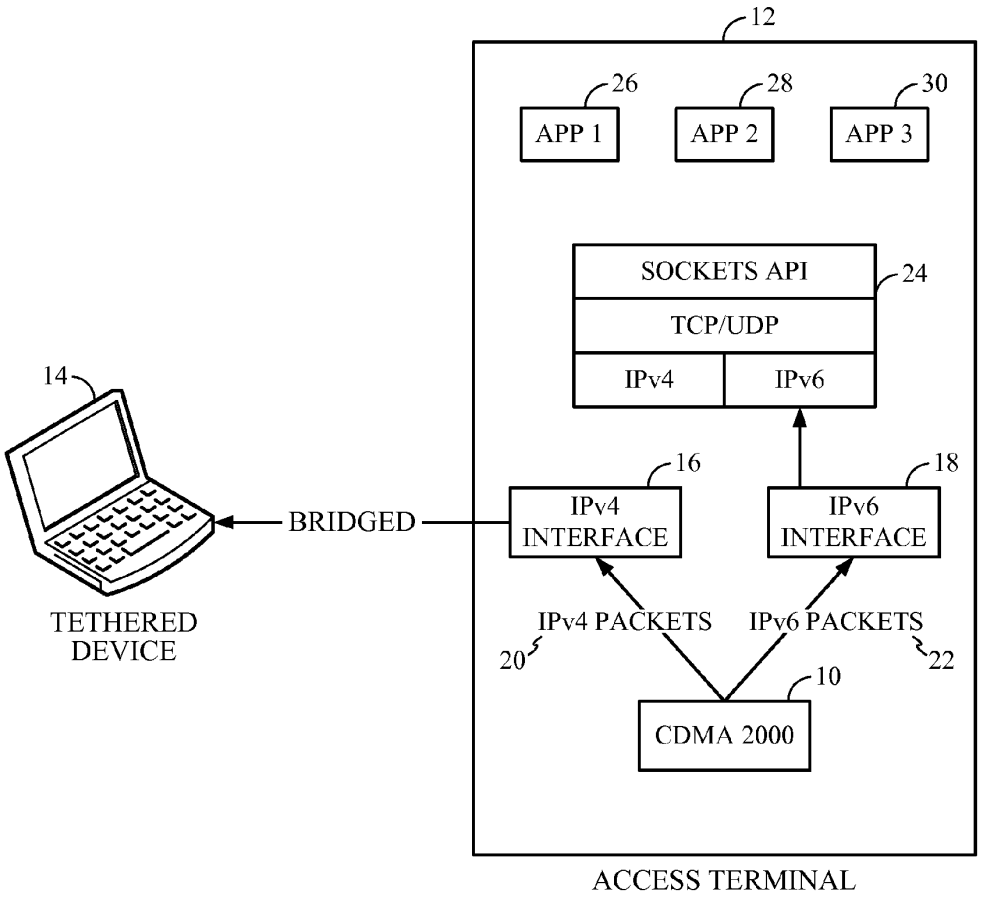

12
26
28
30
APP 1
APP 2
APP 3
SOCKETS API
24
TCP/UDP
IPv4
IPv6
14
16
18
IPv4
INTERFACE
IPv6
INTERFACE
BRIDGED
TETHERED
DEVICE
IPv4 PACKETS
IPv6 PACKETS
20
22
10
CDMA 2000
ACCESS TERMINAL

FIG. 1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017063 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US02/26556

(22) International Filing Date: 21 August 2002 (21.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/313,968 21 August 2001 (21.08.2001) US

(71) Applicant *(for all designated States except US)*: **APOGEE NETWORKS** [US/US]; 1455 Broad Street, 4th Floor, Bloomfield, NJ 07003 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **LEUNG, Yiu, Kau** [US/US]; 5 Knob Hill Road, Morganville, NJ 07751 (US). **PRICE, John, Davis** [US/US]; 5 Ashland Court, Colts Neck, NJ 07722 (US). **FEINBERG, Brion** [US/US]; 51 Amagansett Drive, Morganville, NJ 07751 (US).

(74) Agents: **DUNNAM, Michael, P.** et al.; Woodcock Washburn LLP, One Liberty Place, 46th Floor, Philadelphia, PA 19103 (US).

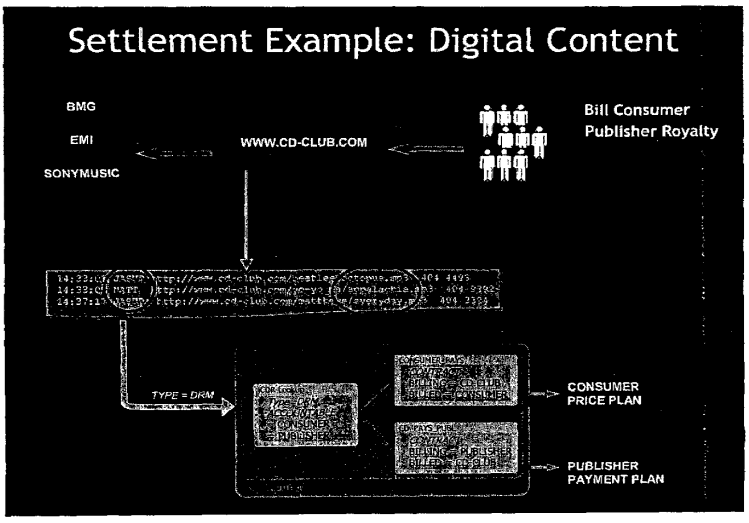
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: SETTLEMENT OF TRANSACTIONS SUBJECT TO MULTIPLE PRICING PLANS____



(57) Abstract: The invention includes a method, system, and computer-readable medium having computer-executable instructions for rating a transaction. The inventive method includes processing a transaction, where the transaction is processed when a service is provided from a service provider to a service consumer, accessing via a computer network multiple pricing plans related to the transaction, and rating the transaction in accordance with the multiple pricing plans. The method further may include receiving output states from at least one pricing plan. The rating may be accomplished within one pricing plan, or within a group of pricing plans.

WO 03/017063 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SETTLEMENT OF TRANSACTIONS SUBJECT TO MULTIPLE PRICING PLANS

Cross Reference to Related Applications

This application claims priority under 35 U.S.C. § 119 (e) from provisional application no. 60/313,968 filed August 21, 2001. The provisional application 60/313,968 is incorporated by reference herein, in its entirety, for all purposes.

Technical Field

The invention relates generally to the processing of data, and more particularly to efficiently and generically aggregating data available on a communication network and billing/paying multiple parties for access to the content of the aggregated data.

Background of the Invention

Recently, the collection and processing of data transmitted over communication networks, like the Internet, has moved to the forefront of business objectives. In fact, with the advent of the Internet, new revenue generating business models have been created to account for the consumption of content received from a data network (*i.e.*, content-based billing). For example, content distributors, application service providers (ASPs), Internet service providers (ISPs), and wireless Internet providers have realized new opportunities based on the value of the content that they deliver. As a result of this content-billing initiative, it has become increasingly important to resolve intelligently and flexibly the corresponding transactions according to the business needs of the customer.

Often, even in traditional commerce streams, there are many different participants between the maker and the consumer of the good. Some of these so-called "middlemen" simply may facilitate access to the good, while others may add useful characteristics to the good. This is especially true in a distributed network environment, like the Internet, that impose additional burdens on capturing the

transaction process because of the unlimited number of data sources and the correspondingly unlimited number of data types. As a result, adequately describing the transacting of the goods and services in such an environment, or even across any of the traditional environments requires a technique that is capable of understanding and processing the participants and the various types of data.

To date, resolving the characteristics of a transaction has been accomplished over data-specific environments using certain application-specific (*i.e.*, "non-generic") methods. For example, a typical telephone bill captures the characteristics of a voice-based telecommunications transaction. In particular, the participants may be identified as the party initiating the call (*i.e.*, the "calling party" telephone number), the party receiving the call (*i.e.*, the "called party" telephone number), and one or more parties connecting the communication (*i.e.*, the "local" or "long distance carrier"). This simple example adequately captures all of the necessary aspects of the telephone call to properly account for the transaction by requiring payment from certain parties (*e.g.*, the calling and/or the called party) to certain other parties (*e.g.*, the local and/or long distance carrier). While these "hard-coded" transaction resolution techniques are sufficient to accommodate only specific environments involving well-defined participants, they are correspondingly too rigid to efficiently satisfy the ever-changing face of a communication network like the Internet. Also, these "hard-coded" techniques are too specific to operate across the many and varied transaction environments that exist throughout the business world.

Therefore, there exists a need to provide a flexible technique that can capture and resolve transactions of any type and involving any participants without requiring modification of the technique for each type. Such a technique would serve to accommodate multi-faceted network environments like the Internet, as well as to provide a single solution that would apply to any business environment.

Summary of the Invention

The invention includes a method, system, and computer-readable medium having computer-executable instructions for rating a transaction. The inventive

method includes processing a transaction, where the transaction is processed when a service is provided from a service provider to a service consumer, accessing via a computer network multiple pricing plans related to the transaction, and rating the transaction in accordance with the multiple pricing plans. The method further may include receiving output states from at least one pricing plan. The rating may be accomplished within one pricing plan, or within a group of pricing plans. Also, accessing the multiple pricing plans may be accomplished via interconnected building blocks located within each of the pricing plans. The method also may include a revenue fold that summarizes the output of multiple pricing plans, including child and parent accounts. Selection of the appropriate child accounts may be a function of end dates that are within a parent account's time period. The method further may pool revenue/usage data as a function of billing cycles, and update the pooled revenue/usage data by summing the values of data from selected account plan periods. Values of the pooled revenue/usage data may be obtained via a building block. The inventive method also may determine a commission, wherein the commission is a credit given to an account.

Brief Description of the Drawings

Other features of the invention are further apparent from the following detailed description of the embodiments of the invention taken in conjunction with the accompanying drawings, of which:

Figure 1 is a block diagram of a system for analyzing content transmitted over a communication network, according to the invention;

Figure 2 is a block diagram further describing the components of the system described in Figure 1;

Figures 3A and 3B provide a flow diagram further detailing the operation the system described in Figure 1;

Figure 4 provides a block diagram of the system described in Figure 1, providing greater detail of a configuration and operation of a transaction layer;

Figures 5A and 5B provide a flow diagram of a method for identifying the characteristics of a transaction, according to the invention;

Figure 6 is a block diagram further detailing the operation and configuration of the transaction layer, according to the invention;

Figure 7 is a flow diagram that details the operation and configuration of the transaction layer of transaction layer, according to the invention;

Figure 8 illustrates a sample settlement scenario for settling the fees associated with the download of certain content;

Figure 9 illustrates a general system description of settlement technologies useful in accordance with the invention to accommodate multiple aggregation of usage, multiple ownership of content, and multiple settlement options;

Figure 10 illustrates a settlement example for digital music downloaded by a consumer from an on-line music club that implements a pricing plan to the consumer and a publisher payment plan using the settlement techniques of the invention;

Figure 11 illustrates a transaction pricing usage based settlement model for use in settling low volume, high value transactions;

Figure 12 illustrates a billing cycle pricing, usage based settlement model for use in settling high volume, low value transactions;

Figure 13 illustrates a revenue sharing settlement using folds in accordance with a first embodiment of the invention;

Figure 14 illustrates a revenue sharing settlement using revenue/usage pools in accordance with a second embodiment of the invention;

Figure 15 illustrates a revenue pool contribution example for the embodiment of Figure 14;

Figure 16 illustrates a revenue pool accessor example for the embodiment of Figure 14;

Figure 17 illustrates a revenue sharing settlement using commissions in accordance with a third embodiment of the invention;

Figure 18 provides an example of computing revenue fold;

Figure 19 illustrates how accounts and pools with different billing cycles contribute to and access from pool instances; and

Figure 20 provides an example of how an account with billing period ending will get one commission from account.

Detailed Description of the Invention

System Overview

Figure 1 is a block diagram of a system 100 for analyzing content transmitted over a communication network. Although the following description will be discussed in the context of collecting, processing and billing for data transmitted over the Internet, it should be appreciated that the invention is no so limited. In fact, the invention may be applied to any type of network, including a private local area network, for example. Also, the invention may be used for purposes other than billing for the usage of content. For example, the invention may be used to analyze the type of data transmitted over a particular network, or to determine the routing patterns of data on a network. Furthermore, the invention may be used to facilitate the intelligent collection and aggregation of data relevant to a particular industry. In addition, the invention may be used to track specific Internet protocol (IP) network resources and to detect fraud, for example.

In addition, it should be appreciated that the term "content" may be defined as data that is transmitted over the network. In the context of the Internet, content may include .mp3 files, hypertext markup language (html) pages, videoconferencing data, and streaming audio, for example. The terms "content provider" and "customer" will be used throughout the description as well. Content provider may refer to the primary creator or provider of the content, while customer is the primary recipient of the content. Both the producer and customer may be a human or a computer-based system.

As shown in Figure 1, an instrumentation layer 101 provides raw data to a content collection layer 102. Instrumentation layer 101 may consist of various data sources, for example, network routers. The network routers may provide information

regarding the various types of routed data, including for example, data format, originating Internet protocol (IP) address, and destination IP address. One example of such information is Cisco System's NetFlow™.

Content collection layer 102 collects information about the delivery of the content, as well as the substance of the content itself. Content collection layer 102 also may sort, filter, aggregate, and store the content according to the particular needs of the end user. In effect, content collection layer is responsible for extracting meaningful information about IP traffic, and so it is provided with an understanding of the data sources in instrumentation layer 101. Content collection layer 102 also may transform the data from the plurality of sources in instrumentation layer 101 into standard formats for use in a transaction layer 103.

Content collection layer 102 is in communication with transaction layer 103. Generally, content collection layer 102 reports to transaction layer 103 that a relevant communication event has occurred and should be considered by the remainder of system 100. A communication event may be defined as any transfer of data between systems. Transaction layer 103 captures the predetermined agreements among all of the parties involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer 103 is charged with understanding the nature of the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 is in communication with a settlement layer 104. Settlement layer 104 captures the operations that are necessary to understand the significance of the transaction defined by transaction layer 103. For example, settlement layer 104 may rate a particular transaction by assigning a monetary value to the transaction. Settlement layer 104 also may divide the burdens and benefits of the monetary value among the relevant parties. In this way, settlement layer 104 ensures that certain parties receive a particular portion of the payment made by the other parties. Settlement layer 104 also may be responsible for delivering this burden and benefit information to the appropriate parties with the appropriate identifiers (*e.g.*,

account numbers). As will be explained in more detail below, the present invention is directed to operations of the settlement layer 104.

Figure 2 is a block diagram further describing the components of system 100. As shown in Figure 2, instrumentation layer 101 includes data sources 201-203 that each provide raw data 204-206, respectively, to collection layer 102. As discussed, data sources 201-203 may include various internetworking devices like routers, bridges, and network switches. Data sources 201-203 provide raw data to an input data adapter 207. Accordingly, input data adapter 207 understands the operation of and the data provided by data sources 201-203. Although one input data adapter is shown in Figure 2, it should be appreciated that more than one input data adaptermay be used in system 100. For example, each data source may have a dedicated input data adapter.

Input data adapter 207 understands the incoming data and extracts the data into the appropriate fields. This field-delimited data, called flow objects 208, are sets of attributes. The attributes may be any characteristics that are provided by, or can be derived from, raw data 204-206 provided by data sources 201-203, respectively. For example, flow objects 208 may include a set of attributes describing the source and destination, including source IP address, destination IP address, source interface, and destination interface. Because input data adapter 207 is charged with understanding raw data 204-206 from data sources 201-203, as well as the required flow objects 208 of system 100, it is capable of transforming the raw data to the flow objects, where the flow objects may all be of a standard format.

Input data adapter 207 provides flow objects 208 to a content data language 209. Content data language 209 may transform the attributes in flow objects 208 into other attributes that are desired by a particular customer. For example, content data language 209 may derive a network identifier attribute that is not readily available from a data source, from a source address attribute and a destination address attribute that are provided by flow object 208 attributes from input data adapter 207. This derivation may be based on a customer's desire to determine which network conveyed the transaction between the source and the destination. Therefore, following this

example, content data language 209 will know to extract the source address attribute and the destination address attribute from flow objects 208.

Content data language 209 may perform other functions as well. For example, content data language 209 may perform a generic lookup function 219 that is built into content data language 209. Generally, generic lookup 219 describes a technique for mapping any number of attributes to any number of other derived attributes. For example, generic lookup 219 may be used to map a unique resource locator (URL) attribute to a particular content-type attribute.

Content data language 209 also is in communication with a correlator 211. Generally, correlator 211 connects the many daily network content events from various network devices, like routers for example. Often, the connected data may come from distinctly different data sources at distinctly unrelated times. Correlator 211 allows this data to be intelligently connected to each other, regardless of how different the sources or of how disparate the time received. For example, a Netflow™ enabled router and a Radius™ enabled network access switch may each provide certain data that is relevant to one particular transaction. However, because portions of the data come from different devices, the data may arrive at system 100 at different times, and in different formats. Also, because each provides data that is necessary to complete one transaction, the data from each cannot be considered separately. Correlator 211 allows this data to be intelligently grouped regardless of the format of the data or of the time the data pieces are received.

Furthermore, correlator 209 may rearrange the order of the received flow objects 208 to suit the needs of the remainder of system 100. By performing such correlation without having to first store all of the data on a disk (*e.g.*, a database), significantly faster processing is achieved. Correlator 209 may perform this correlation in real-time, for example.

Although system 100 has been described using content data language 209 and correlator 211, it should be appreciated that flow objects 208 may proceed directly to a filter 212, if no correlation is required and if no attribute derivation is required, for example. Filter 212 analyzes flow objects 208 to ensure that the provided attributes

are desired by system 100. If flow objects 208 are not needed (*i.e.*, a mismatch), filter 212 may prevent flow objects 208 from passing to an aggregator 213. Also, although filter 212 has been shown as a separate device in system 100, it should be appreciated that the functionality of filter 212 may be incorporated into aggregator 213.

Filter 212 passes the matching flow objects to aggregator 213. Aggregator 213 may provide additional filtering and classification of the multitude of daily network content transactions, based on user criteria. Aggregator 213 may perform such filtering and classification in real-time. Aggregator 213 provides the filtered and classified information to an output data adapter 214. Output data adapter 214 may convert the data from aggregator 213 into one or more content detail records for storage in CDR database 215. Therefore, CDR database 215 stores a complete description of a content event.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 passes the CDR onto ownership resolution component 216. A proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. These tasks are accomplished by ownership resolution component 216 and transaction resolution component 221.

Ownership resolution component 216 serves to define the participants of the communication event. In particular, because raw data 204-206 may not provide sufficient "ownership" data relating to the parties involved in the content transaction, such "ownership" data must be provided by system 100 to properly account for the entire transaction. Ownership resolution component 216 operates to provide such ownership-based data to system 100.

Ownership resolution component 216 is in communication with transaction resolution component 221. Transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content.

Such predetermined relationships may be previously agreed upon by the participants, or may be created and agreed upon with the implementation of system 100. Therefore, transaction component 103 understands the nature of the parties, the actions that one or more parties perform, and the influence of such action on the respective parties.

Transaction component 216 provides the transaction information to a rating component 217. Rating component 217 provides a weight or significance (*e.g.*, a price) to the transaction, so as to provide a tangible value to the transaction. Rating component 217 may make this determination based on various metrics including the type of the content, the quantity of content consumed, the place and time delivered, or the quality of the content, for example. Therefore, rating component 217 allows system 100 to provide some contextual value, indicting the significance or relevance that certain content or information has to the individual customer.

Rating component 217 provides the rated transaction to a presentment component 218. Presentment component 218 may provide the capability for a customer 220 to view their real-time billing information, for example, over the network. Presentment component 218 also may attach relevant identifiers to the bill (*e.g.*, account numbers, etc.).

Figures 3A and 3B provide a flow diagram further detailing the operation 300 of system 100. As shown in Figure 3A, in step 301, raw data 204-206 is received from data sources 201-203. In step 302, input data adapter 207 converts raw data 204-206 to flow objects 208, where flow objects 208 are sets of attributes, determined from raw data 204-206. In step 303, it is determined whether there is a need to derive new attributes from the existing attributes found in flow objects 208. If there is such a need, in step 304, CDL 209 is used to derive new attributes from existing attributes. Also, as discussed above, attributes may be correlated by correlator 211.

In step 305, flow objects 208 are filtered by filter 212. In step 306, the matching flow objects (*i.e.*, those passed by filter 212) are further filtered and classified by aggregator 213. In step 307, output data adapter 214 converts the data aggregated by aggregator 213 to a format compatible with transaction layer 103.

As shown in Figure 3B, in step 308, output adapter 214 may format the aggregated data into one or more content data records for storage in CDR database 215. In step 309, ownership resolution component 216 identifies the parties involved in the transaction. In step 310, transaction resolution component 221 captures the predetermined agreements among the parties, as well as the value added by each of the individual parties. In step 311, the CDR is rated based on predetermined metrics (*e.g.*, time of transmission, quality of content). In step 312, a bill is presented to the customer.

Content Transaction Layer

A transaction, including a business transaction for example, may be any activity between two or more participants that affects certain parties. The affected parties may be considered the participants to the transaction, although parties and participants may be mutually exclusive entities. It should be appreciated that the terms "parties" and "owners" may be used interchangeably throughout. Also, a transaction may include one or more events, where an event may be some action (*e.g.*, the transfer of a service or good) that the participants conduct with each other. Such events may be the exchange of data over a communication network, for example. Also, it should be appreciated that the same event or action may take place in any direction (*e.g.*, from party A to party B or from party B to party A). The "subject" of the action is the party who performs the activity, while the "object" of the action is the party who is affected or influenced in any way by the action.

Transaction layer 103 is responsible for capturing the characteristics of the transaction, including the parties, participants, subject, object, event/action type, direction of the action, for example. The scope of the characteristics captured by transaction layer 103 will vary with the nature of instrumentation layer 101, the capability of content collection layer 102, and the requirements of settlement layer 104. Generally, transaction layer 103 captures the predetermined agreements among all of the parties involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer 103 is charged with understanding the nature of

the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 is a data store that holds each CDR for further processing by ownership resolution component 216 and transaction resolution component 221. In the context of a billable electronic business transaction, a proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. As discussed, ownership resolution component 216 serves to define the participants of the communication event, while transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216.

Transaction layer 103 is generic in that it operates without requiring an understanding of instrumentation layer 101 and content collection layer 102. Instead, transaction layer 103 takes the relevant characteristics of the transaction provided by instrumentation layer 101 and content collection layer 102, and selects and generates those characteristics required by settlement layer 104.

Although the operation of transaction layer 103 will be described in the context of an electronic event over a communication network for the purposes of billing for the event, it should be appreciated that the invention is not so limited, but is so described the purpose of clarity. For example, it should be appreciated that the invention may include functions other than billing, including security, network capacity planning, and content monitoring, for example. Also, the generic techniques described may be applied beyond the context of an electronic event over a communication network.

Figure 4 provides a block diagram of system 100 providing greater detail of the configuration and operation of transaction layer 103. As shown in Figure 4, content collection layer 102 provides a usage record 401 to transaction layer 103. A series of fields 403-408 comprise usage record 401. Although fields 403-408 will be

identified by certain labels for the purpose of clarity, it should be appreciated that fields 403-408 may identify any of the many possible characteristics of the transaction.

In the example provided by Figure 4, fields 407 and 408 identify the parties or participants to the transaction. In particular, field 407 identifies "User A" and field 408 identifies "User B." User A may be the subject party and User B may be the object party. For example, in the context of a telecommunication event, User A may be the "calling" party and User B may be the "called" party. Field 405 and field 406 identify a measurable quantity of the event. In particular, following the example of the telecommunications event, field 405 identifies a duration (in minutes) of the event and field 406 identifies the quantity of data exchanged during the event (in megabytes). Field 403 and field 404 may identify a "start time" and an "end time," respectively, of the communication event.

Although fields 403-408 provide just one example, in any case, it should be appreciated that user record 401 will include certain characteristics provided by instrumentation layer 101 and/or derived by content collection layer 102. These characteristics typically are provided to transaction layer 103 because they have some particular significance to identifying the characteristics necessary to allow settlement layer 104 to provide some accounting of the transaction. Therefore, usage record 401 may not necessarily include all of the characteristics provide by instrumentation layer 101 and/or derived by content collection layer 102, because certain characteristics may not relevant to the settlement of the transaction (*e.g.*, network type). Yet, usage record 401 will include those available characteristics that pertain to permitting settlement layer 104 to properly account for the transaction.

Once usage record 401 passes through transaction layer 103, a modified usage record 402 may be provided to settlement layer 104. Modified usage record 402 may be modified by transaction layer 103 to include additional details of the transaction event required by settlement layer 104 and/or required by the customer's system to which the usage record applies (*e.g.*, a usage billing system). As shown for modified usage record 402, an account A field 409 and an account B field 410 may be added to

further identify the transaction. In one example, account A field 409 may include an alphanumeric designator that identifies the account number that has been assigned by the customer's billing system for User A. In the context of the telecommunications system, account A field 409 may hold User A's ten-digit home telephone number, for example.

In any case, the components of transaction layer 103 operate to identify these additional fields, based on the requirements of the customer's system and of settlement layer 104. In particular, ownership resolution component 216 operates to ensure that the necessary participants or parties to the transaction are identified, while transaction resolution component 221 operates to ensure that the relationships among the parties or participants are identified.

Identification of the relevant entities and their relationships may be accomplished using "lookups" in data stores located within ownership resolution component 216 and transaction resolution component 221, for example. For example, a data table may have a "User" data field and an associated "Account" data field. When User A is received by ownership resolution component 216, it will conduct a lookup in the data table and identify Account A as the appropriate account associated with User A. Also, transaction resolution component 221 may have a data table that permits a lookup of the relationship between User A and User B, identified in usage record 401. For example, upon receiving field 407 designating User A and field 408 designating User B, transaction resolution component 221 may conduct a lookup of an algorithm that identifies the appropriate burdens and benefits (*e.g.*, debit and credit of money) assigned to each of the users with respect to each other.

It also should be appreciated that transaction layer 103 may not provide additional characteristics to usage record 401, as described but may select the relevant characteristics (*i.e.*, those characteristics needed by settlement layer 104) from the characteristics made available by instrumentation layer 101 and/or derived by content collection layer 102. In fact, usage record 401 may include all of the necessary characteristics to properly account for the transaction. In this case, ownership resolution component 216 and transaction resolution component 221 select the

relevant characteristics from the available characteristics. As will be explained in more detail below, the information added to the usage record 402 may also constitute pricing plans and the settlement layer may be configured to handle more sophisticated settlement strategies involving multiple parties and multiple pricing plans over a multiplicity of noncontiguous time periods.

Figures 5A and 5B provide a flow diagram of a method 500 for identifying the characteristics of a transaction using system 100. As shown in Figure 5A, in step 501, raw data 204-206 is received into system 100. Raw data 204-206 includes certain characteristics provided by data sources 201-203, respectively, in instrumentation layer 101. In step 502, content collection layer 102 processes (*e.g.*, aggregates, correlates and filters) raw data 204-206. In step 503, content collection layer 102 provides the processed data to CDR database 215 in transaction layer 103. CDR database 215 stores the data for further processing by transaction layer 103.

In step 505, it is determined whether the contents of the data provided to transaction layer 103 already include the needed ownership data. If the data includes the needed ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507. If, on the other hand, the data provided to transaction layer 103 does not already include the needed ownership data, the required data is identified (*e.g.*, using database lookups) by ownership resolution component 216, in step 506. Once ownership resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507.

As shown in Figure 5B, in step 508 it is determined whether the contents of the data provided to transaction layer 103 already include the needed relationship data (*i.e.*, data defining the burdens and benefits encountered by the parties/participants to the transaction). If the data includes the needed relationship data, the relevant data is selected by transaction resolution component 221 and provided to settlement layer 104, in step 510. If, on the other hand, the data provided to transaction layer 103 does not already include the needed relationship data, the required data is identified (*e.g.*,

using database lookups) by transaction resolution component 221, in step 509. Once ownership resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 510.

Ownership and Transaction Resolution

Figure 6 is a block diagram further detailing the operation and configuration of transaction layer 103. It should be appreciated that elements described for transaction layer 103 are not exclusive, but provide just one example of a configuration for transaction layer 103. In particular, the functionality of the previously described ownership resolution component 216 and transaction resolution component 221 will be described in greater detail in the various components described with reference to Figure 6. In practice, however, it should be appreciated that transaction layer 103 may comprise of any number of components that ensure that the necessary parties to a transaction are identified generically.

As shown in Figure 6, transaction layer 103 includes a configuration repository 601, a configuration database 610, a configuration manager 603, and a fail over detector 604. In addition, transaction layer 103 includes a transaction layer engine 608 in communication with configuration repository 601, configuration manager 603, and fail over detector 604.

Transaction layer engine 608 includes a rules processor 605, a CDR reader 606, and a transaction writer 607. Transaction layer engine 608 processes raw data 204-206 in usage record 401 and creates a modified usage record 402, based upon the requirements of settlement layer 104. It should be appreciated that there may be more than one transaction layer engine 608 for each transaction layer 103. However, a single transaction layer engine 608 is shown for the purpose of clarity and brevity.

CDR reader 106 understands the nature of the transaction and operates to read a particular usage record 401 stored in CDR database 215. CDR reader 106 then submits usage record 401 to rules processor 605. Rules processor 605 applies rules (*e.g.,* written in XML) to usage record 401 so as to determine ownership and the relationships among the ownership, for each individual usage record 401. Rules

processor 605 may then generate one or more modified usage records 402, based on the application of the rules to usage record 401. Once rules processor 605 generates the modified usage record 402, transaction writer 607 operates to write a transaction (based on the modified usage record 402) to CDR database 215. Modified usage record 402 is then used by settlement layer 104 to further process the transaction (*e.g.*, rate the transactions monetarily).

Fail over detector 604 operates to provide fault tolerance and initiate a fail over engine (not shown) for a failed transaction layer engine, in accordance with one or more mathematical algorithms, the discussion of which is beyond the scope of the invention. Configuration manager 603 provides an external interface to transaction layer 103 using a business editor 609. Business editor 609 may be manipulated by a user or customer using a graphics user interface (GUI). In particular, the GUI of business editor 609 receives commands from a user and translates them into actions to be performed on usage record 401, for example, by rules processor 605. Configuration repository 601 operates to provide an abstraction to configuration database 610. Configuration database 610 may be a relational database or a set of extensible markup language (XML) computer-readable files, for example.

Figure 7 is a flow diagram that details the operation of transaction layer 103, as shown in Figure 6. As discussed, it should be appreciated that multiple transaction engines may be used to implement a process. Where the invention is instituted using computer-readable instruction, transaction layer engine 608 may be implemented as a computer-executable instruction or thread. Therefore, multiple transaction layer engines may be implemented by having multiple computer-readable instructions.

In step 701, transaction layer engine 608 reads usage record 401 using CDR reader 606. In step 702, rules processor 605 applies one or more rules to usage record 401 read by CDR reader 606, so as to determine one or more "accountables." Accountables are labels that are used to facilitate identifying the parties or owners to a transaction. Accountables may be defined and/or modified by an external user (*e.g.*, a customer) using the graphical user interface provided by business editor 609. Also, it should be appreciated that accountables may be defined for a new usage types for

which no rules in rules processor 605 are provided. The identification of accountables is the function of ownership resolution component 216, as described with reference to Figure 4.

In step 703, "contracts" are identified that define the relationships or agreements between one or more accountables. In the context of a billing system, a contract identifies which parties pays (*i.e.*, the billed party) and which party receives payment (*i.e.*, the billing party). A particular contract may be identified and executed when one or more "conditions" are satisfied. The identification of contracts is conducted by transaction resolution component 221, as described with reference to Figures 2 and 4. A condition is an expression of a logical assertion that can be evaluated as true or false. In transaction layer 103, for example, a condition may be true if a certain data element is present and false if the data element is not present. The following is an example of a condition in XML:

```
<condition name="condition1" function="IsPresent" outcome="true"
type="Accountable" id="ColoProvider"/>
```

In step 704, once the contracts are determined, they are executed. In step 705, usage record 401 is changed to modified usage record 402 based upon the execution of the contract and the identification of the accountables. In step 706, modified usage record 402 may be written to a data table using transaction writer 607, so that settlement layer 104 can rate it, in step 707. Therefore, a transaction may be represented as modified usage record 402, where modified usage record may include the elements of usage record 401 in addition to the accountable and contract elements (*e.g.*, fields 409-410 as discussed with reference to Figure 4).

Although the discussion provided an example of a single contract and two accountables for a single usage record, it should be appreciated that many contracts and many accountables (*i.e.*, and therefore many "transactions") may be derived from a single usage record, because there may be multiple transactions implicated from a single usage record 401. For example, usage record 401 may involve three parties

each having a contract with the other respective parties. In this example, therefore, there may be three separate contracts for a single usage record 401, and three individual accountables for each party or owner. Moreover, as will be explained below, the contracts may operate according to pricing plans that vary over time and from party to party.

In addition to requiring a certain accountable, it may be necessary to determine a value of the accountable. For example, transaction layer 103 may determine not only that the "called party" accountable be a part of the transaction, but also that a value for the called party (*e.g.*, "856-555-1212" or "John Doe") be identified. Also, it may be necessary to transform one accountable into another accountable to satisfy the requirement of settlement layer 104. For example, settlement layer 104 may require the called party accountable (either determined by transaction layer 103 or provided in usage record 401) be transformed into a network identifier accountable.

In either case, the value or transformation of accountables or contracts may be determined using certain predetermined functions or "primitives." A primitive defines a transformation or a valuation of an accountable or contract. As discussed, transformations may allow a value of an accountable to be determined using another accountable, for example. Primitives define and direct such transformations. The input to a primitive can be one of fields 403-408 from usage record 401 or a previously determined accountable, for example.

Primitives may be described and distinguished based on their prescribed functionality. For example, one type of primitive may be a database lookup. A database lookup is a primitive that operates to transform one accountable or contract to another accountable or contract. Also, a database lookup primitive may function to assign a value to an accountable or contract, as a result of conducting a lookup of the accountable or contract in a database. It should be appreciated that the database lookup primitive also allows flexibility in that any database that has Java Database Connectivity (JDBC) drivers (*e.g.*, Oracle, Microsoft SQL Server, Sybase, Database 2) can be used to perform complex lookups. In this way, therefore, previous

accountable or contact transformations can be linked to find new accountables or contracts, respectively.

Other types of primitives may include direct value assignment, and a function primitive that looks up data in an external database. Other primitives may include a function primitive that it allows a third party based library (*e.g.*, Java-based) to be used. Another primitive may be a "regular expression" based primitive that allows parsing of complex text-based fields with a full feature (*e.g.*, PERL5 compliant) pattern specification. Common used techniques would include parsing URLs, filenames and paths, calling/called telephone numbers, email address, for example. In addition, a CDR database 215 lookup primitive allows holding on to an ownership entity if no further processing is required. This primitive is used where usage record 401 provides the information needed by settlement layer 104 without any need for more data correlation and/or manipulation by transaction layer 103.

A default primitive may be a hard-coded primitive that is used where the value is known and/or is not dependent on usage record 401. For example, such a primitive may be used where a party is always present in a consumption event, regardless of the other relevant parties. A network address primitive allows determination of a network entity given an arbitrary string. An area code primitive may be used to determine an area code of a telephone number given the complete telephone number. This primitive may be relevant for a Voice-over-IP application. These examples primitives are not exclusive, but are meant to provide a few examples of the manipulation and correlation that may be achieved by the primitives on the accountables and contracts.

The following is an example of an accountable primitive in XML:

```
<accountable>
<name> ColoProvider </name>
<role> ServiceProvider </role>
<usageType> RMONHost </usageType>
<valid from="past" to="present" />
<primitive type="default">
<value> Exodus </value>
</primitive>
</accountable>
```

Each accountable that is involved in a contract will have an assigned "role." It follows, therefore, that an accountable that is not involved in a contract may not need to have an assigned role. The role associates the particular accountable for integration with settlement layer 104.

Similar to the accountable, a contract is implemented using a set of primitives. The following is an example of a contract primitive in XML. In the example, a Web hosting scenario is present where a content provider (*e.g.*, CNN) places content on one or more Web servers and pays a Web Hoster for doing so based on some predefined pricing plan.

In order to define the accountables, certain elements of usage record 401 may be assumed as follows: Web Hit Time, Web Server Name/IP address, Client IP address, bytes, Mime type, and URL. In this example, if a rule in the business world requires the "Content Provider" of the Web Server (*e.g.*, CNN) to pay to the Web Hoster, there are two accountables: Web Hoster and Content Provider. The XML definition of a contract that captures this business rule may be as follows:

```
01  <contract>
02  <name> ContentProvider-Pays-WebHoster </name>
03  <usageType> WebHosting </usageType>
04  <valid from="past" to="present" />
05  <condition function="IsPresent" type="Accountable"
    name="condition1"  id=" ContentProvider " />
06  <condition function="IsPresent" type="Accountable"
    name="condition2" id="WebHoster" />
07  <billedFunction>
08  <status> enabled </status>
09  <primitive type="internal-account-lookup">
10  <database name="GlobalDB"/>
11  <argument order="1" type="Accountable"
    name="ContentProvider"/>
12  </primitive>
13  </billedFunction>
14  <billingFunction>
15  <status> disabled </status>
16  <primitive type="internal-account-lookup">
17  <database name="GlobalDB"/>
```

```
18      <argument order="1" type="Accountable"
name="WebHoster"/>
19      </primitive>
20      </billingFunction>
21      </contract>
```

In this example, a contract has a name defined in line 02 as "ContentProvider-Pays-WebHoster." The contract also defines an element or usage type called "WebHosting" in line 03. The contract also has two sets of conditions in lines 05 and 06, called "IsPresent," which consider whether "ContentProvider" and "WebHoster" elements are present, respectively. Therefore, this particular contract will be selected and executed by transaction layer 103 if these elements are present.

Also, in this contract example, there are two primitives that are specified. There is a first primitive for finding the account number of the billed entity "ContentProvider," which begins on line 07 and ends on line 13, and there is a primitive for determining the account of the billing entity "WebHoster" beginning on line 14 and ending on line 20. Therefore, the example contract contemplates the "who pays to whom" logic, and results in the execution of a contract that creates a modified usage record 402, which captures the transaction. Notably, in lines 09 and 16, both primitives are defined as database lookups.

As noted above, to settle a transaction, the system must determine who should compensate whom and by how much. Many processes contribute to such "settlement." Accordingly, the settlement layer 104 is not necessarily a particular logical component but may be spread throughout the system. In operation, a typical "settlement" might occur as described below with respect to Figure 8.

Figure 8 illustrates a sample content event as received by transaction layer 103 pursuant to the processes described above. In this example, "content.com" is identified as the billed party for a caching service, and IP address "128.33.2.41" is identified as the billed party for consuming content type "audio video interleave" (.avi). This IP address may be mapped to a customer account that may vary over time. The system also may identify the log provider (*e.g.*, web host service) and may identify the content property owner (*e.g.*, "Disney") as the party to receive a royalty,

or some other form of compensation, for the download. This ownership may create rules based on the unique resource locator (URL) substring and other event information. Also, links may be provided from the event to the multiple accounts related to that event. The use of pricing plans and pools, as described below, allow business rules to be captured regarding compensation for events, for example, in ways that greatly increase system flexibility. In this example, a fee may be charged to "content.com," while revenue may be paid back to the log provider.

Settlement of Transactions Subject to Multiple Pricing Plans

In many transactions, the accounts include one or more pricing plans that are customized to particular customers. As shown in Figure 9, the settlement technologies used to settle such transactions may allow for multiple ownership of content, multiple aggregation of usage, and provide a variety of revenue sharing models. Several of such models will be described below including folds with parent account plans, revenue pooling, and commission relationships between plans.

Figure 10 illustrates a settlement example for the case of digital content, such as digital music content downloadable off of the Internet. In this example, an on-line music club (*e.g.,* BMG, EMI, Sony) has a contractual relationship with the consumers as well as the music publishers (*e.g.,* "www.cd-club.com") and, at settlement, allocates payment according to the price plan(s) with the consumer and the payment plan(s) with the publishers. These payment plans recognize that each song may have a different price and that the revenue paid to the publisher, author, etc. may vary over time depending upon the frequency of download, for example. The price to the consumer also may vary with use. Figures 11 and 12 illustrate settlement models that take into account transaction pricing and billing cycle pricing for such usage based settlements. As those skilled in the art will appreciate, the per transaction usage based model may be best utilized for low volume, high value transactions, while the billing cycle pricing usage based model may be better for high volume, low value transactions.

The present invention allows for the networking of a multiplicity of pricing plans during rating process 217 in settlement layer 104. Thus, the system described

below is implemented primarily in ratings 217 described above with respect to Figure 2.

Pricing Plan Overview

In accordance with the invention, pricing plans may be created by interconnecting rating building blocks with customizable properties. Each rating building block may be specialized in one well-defined function that falls roughly into five classes: usage selection and filtering, usage computation, accumulation, rate computation, and bill presentation. By interconnecting these rating building blocks, together with the ability to add new rating building blocks to the system, very flexible and extensible pricing plans can be created. The computation may be desirably constrained within one pricing plan.

A new class of rating building blocks also may be defined to extend the usefulness of pricing plans. This new class of rating building blocks allows a plan to access the states of another pricing plan or a group of pricing plans. These states can be usages and/or charges associated with line items and/or intermediate computations. With this new capability, computation is not constrained within one pricing plan but within a network of pricing plans working together. This new computation offers, but is not limited to, many settlement features.

A revenue fold summarizes revenue, which is the output of a pricing plan, from child accounts and presents the folded revenue to their corresponding parent accounts as input to their pricing plans. This process may start from the lowest level and continue on up to the root level. The value of revenue fold may be available to a parent account in a pricing plan through a building block (*e.g.*, "RevenueToDate"). As illustrated in Figure 13, the revenue fold settlement model of the invention may provide for pricing plans at each level in the hierarchy and allow for the use of resellers.

Revenue/usage pools are similar to global variables except that they include the concept of billing cycles. Different periods of a pool imply different instances and therefore different values. A pool value may be updated during invoice processing by summing the values of invoice line items associated with the pool from appropriate

account plan periods. An account plan period is considered appropriate if the end date is within the period of the particular pool instance. Note that it is possible to have zero or more than one account plan periods from the same account to be included in the same pool instance. The computation of a pool value may not be cumulative between updates. When a pool value needs to be updated, the computation may start over with the previous value of a pool having no consequence. For example, the value of a pool may be accessible from a pricing plan through a building block (*e.g.*, "PoolAccessor") with the pool name as its property. The output of the "PoolAccessor" is the sum of the pool instances having the same pool name and billing period end dates within the start and end dates of the account plan period. As shown in Figure 14, this settlement feature is useful in revenue sharing scenarios where total revenue and resources are pooled together and total revenue is shared among the contributing accounts based on contributed resources. The pools may be hierarchy independent and defined by the pricing plans. A revenue pool contribution example is given in Figure 15, and a revenue pool accessor example is given in Figure 16.

A commission is a credit given to an account. The credit amount is computed based on the revenue, or states of another account. The two accounts involved in the transaction are commission source account and commission destination account. As shown in Figure 17, the commission source account (commission generator plan) generates the commission contribution iCDR using a building block (*e.g.*, "CommissionGenerator") with "AccountNumber" and "CommissionDescription" as its properties. The amount, not necessarily revenue, going into the CommissionGenerator (commission plan) is the commission amount. When used in conjunction with existing rating building blocks, commission features such as the following can be supported: commission going to multiple accounts, commission based on total revenue or a subset of the revenue (*e.g.*, only monthly and usage charges, but not setup charges), commission for the first "n" billing period only (or different rate after first "n" periods), and step rate.

The commission destination account may receive the commission data through a building block (*e.g.*, "CommissionAccumulator"). Additional commission features such as the following can be supported on the destination account: a recurring base commission, promotional commission rate, and step commission rate. The commission settlement model also may be hierarchy independent and permit variable settlement arrangements.

When computation involves a network of pricing plans, the correct output of a particular pricing plan may be dependent on the processing of another pricing plan. The output of the other pricing plan may in turn dependent on yet another pricing plan. A cyclic dependence can even exist. In order to have the correct computation for the network of pricing plans as a whole, the system detects and continues processing until all pricing plans reach their final values. Accordingly, the settlement processing software in accordance with the invention has a built-in mechanism to repeat processing of the pricing plans until their values are final. The algorithm will stop after a configurable loop count to prevent infinite processing in case there is a cyclic dependence.

Billing Cycle Considerations

Because more than one account may be involved in settlement, it is possible that they have different billing periods. The following section details how each settlement feature is processed for the settlement models of the invention when accounts with different billing periods are involved.

Revenue fold summarizes revenue from child accounts and presents the folded revenue to their parent accounts. This process starts from the lowest level and continues up to the root level. In actual settlement processing, revenue fold is a post order traversal of a tree whose nodes are account plan periods, where a post order tree traversal traverses each sub tree of the root in post order followed by the root. The child account plan periods are selected if the end dates are within the parent's account plan period. It is possible to have zero or more than one account plan period from the same account included in one revenue fold. The root account's account plan period is defined by the invoice processing start and end dates.

An iCDR is generated for each revenue fold. The iCDR is rated by the pricing plan for the account plan period receiving the revenue fold. Therefore, pricing plans for non-leaf accounts take revenue fold into consideration. The value of revenue fold is available in a pricing plan through a building block (*e.g.*, "RevenueToDate").

Figure 18 provides an example of computing revenue fold. To compute the revenue fold for account 1001, the revenue from all child accounts of 1001 with account plan period end dates between 3/1 and 4/1 are summed. In this example, the revenue for account 2001 for the billing period 2/7 to 3/7, account 2002 for the billing period 2/15 to 3/15, account 2003 for the billing period 2/22 to 3/22 are summed. Before the summing of the revenue of these accounts can occur, their own revenues are determined. In order to determine the revenue of these child accounts, their child accounts with account plan period end dates between their account plan period start and end dates are selected and summed. The following example shows that to determine the revenue for account 2003 for the billing period 2/22 to 3/22, revenue for account 3001 for the billing period 2/1 to 3/1 and account 3002 for the billing period 2/15 to 3/15 are summed. This process repeats until the leaf level account is reached.

The value of a pool is accessible from a pricing plan through a rating building block (*e.g.*, "PoolAccessor"). The output of "PoolAccessor" is the sum of the pool instances having billing period end dates within the start and end dates of the account plan period. It is possible to have zero or more than one instance selected given a particular account plan period depending on the billing period of the pool and the account. Therefore, given the same plan, "PoolAccessor" output may vary according to the account plan period. This technique ensures that each invoice line item associated with a pool will be included a pool instance and that each pool instance will be accessed once by an account which accesses the pool.

Figure 19 illustrates how accounts and pools with different billing cycles contribute to and access from pool instances. For example, line items associated with pool A for account 1001 with billing period from 4/1 to 6/1 and account 1002 with billing periods from 3/22 to 4/22 and 4/22 to 5/22 will contribute to the pool A's

instance with period from 4/1 to 6/1. The output of the PoolAccessor will be zero for account 2001 during the period 4/1 to 5/1. For billing period from 5/1 to 6/1, account 2001 will get the value of pool A's instance with period from 4/1 to 6/1. Account 2002 with billing period from 4/1 to 6/1 will also get pool A's 4/1 to 6/1 instance. The account plan period from 4/1 to 8/1 for account 2003 will get the sum of the two pool A's instances, 4/1 to 6/1 and 6/1 to 8/1.

During invoice processing, one or more iCDRs will be generated for each commission producing account plan periods. The generated record will have the destination account number, amount, and a timestamp. The timestamp is the end date of the account plan period that generated the record. The record will then be rated by the destination account in the appropriate account plan period.

Figure 20 provides an example of how an account 2001 with billing period ending 6/1 will get one commission from account 1001 for the period 4/1 to 6/1 and two commissions from account 1002 for the periods 3/22 to 4/22 and 4/22 to 5/22.

An invoice output may be dependent on the processing of settlement features. In turn, processing of settlement features may be dependent on correct invoice output. For example, if the pricing plan associated with an invoice accesses one or more pools, revenue/usage pool processing should be completed successfully before a correct invoice can be produced. To process a revenue/usage pool correctly, account plan periods associated with a pool have to produce a correct invoice that in turn may be dependent on revenue fold. There may not be a single, correct pre-defined order of processing for these settlement features. In some cases, the same settlement features may have to be processed more than once (*e.g.*, revenue fold, generate commission and then revenue fold again).

The settlement processing has a built-in mechanism to repeat processing of the settlement features in a fixed sequence until the values are final. To prevent the algorithm from looping forever, there is a configurable maximum loop count. If the result is not final after the maximum loop count, a warning will be given, and the user may remove the circular dependency (if one exists) and/or increases the maximum loop count.

The invention described above is directed to a system and method for handling the networking of pricing plans in the settlement of transactions. The invention often was described in the context of the Internet, but is not so limited to the Internet, regardless of any specific description in the drawing or examples set forth herein. For example, the invention may be applied to wireless networks, as well as non-traditional networks like Voice-over-IP-based networks and/or private networks. It will be understood that the invention is not limited to the use of any of the particular components or devices herein. Indeed, this invention can be used in any application that requires aggregating data. Further, the system disclosed in the invention can be used with the method of the invention or a variety of other applications.

While the invention has been particularly shown and described with reference to the embodiments thereof, it will be understood by those skilled in the art that the invention is not limited to the embodiments specifically disclosed herein. Those skilled in the art will appreciate that various changes and adaptations of the invention may be made in the form and details of these embodiments without departing from the true spirit and scope of the invention as defined by the following claims.

What is claimed is:

1. A method of rating a transaction, comprising:

processing a transaction, wherein the transaction is processed when a service is provided from a service provider to a service consumer;

accessing via a computer network multiple pricing plans related to the transaction; and

rating the transaction in accordance with the multiple pricing plans.

2. The method of claim 1, wherein at least one of the pricing plans includes at least one of the following: revenue folds, revenue/usage pools, and commissions.

3. The method of claim 1, further comprising receiving output states from at least one pricing plan.

4. The method of claim 1, wherein the rating is accomplished within one pricing plan.

5. The method of claim 1, wherein the rating is accomplished within a group of pricing plans.

6. The method of claim 1, wherein the accessing is accomplished via interconnected building blocks located within each of the pricing plans.

7. The method of claim 1, wherein the building blocks perform at least one of the following functions: data usage selection and filtering, data usage computation, data accumulation, rate computation, and presentation of required payment.

8. The method of claim 6, wherein the building blocks have customizable properties.

9. The method of claim 6, wherein the building blocks allow a first pricing plan to access states of another pricing plan.

10. The method of claim 9, wherein the states are usages and charges associated with one or more pricing plans.

11. The method of claim 6, wherein the building blocks allow a first pricing plan to access the states of a group of pricing plans.

12. The method of claim 11, wherein the states are usages and charges associated with one or more pricing plans.

13. The method of claim 1, further comprising a revenue fold, wherein the revenue fold summarizes the output of multiple pricing plans.

14. The method of claim 13, wherein the revenue fold summarizes child accounts and inputs the summary information to pricing plans of corresponding parent accounts.

15. The method of claim 13, wherein the value of the revenue fold is available to the pricing plan via a building block.

16. The method of claim 13, wherein the revenue fold is available to child and parent accounts.

17. The method of claim 13, further comprising selecting child accounts with end dates that are within a parent account's time period.

18. The method of claim 1, further comprising pooling revenue/usage data as a function of billing cycles.

19. The method of claim 18, further comprising updating the pooled revenue/usage data by summing the values of data from selected account plan periods.

20. The method of claim 18, further comprising selecting the account plan period as a function of the end date of the account plan with respect to the pooled revenue/usage data.

21. The method of claim 18, further comprising accessing a value of the pooled revenue/usage data via a building block.

22. The method of claim 1, further comprising determining the value of a pricing plan as a function of another pricing plan.

23. The method of claim 22, further comprising providing a configurable loop count.

24. A computer-readable medium having computer-executable instructions, comprising:

processing a transaction, wherein the transaction is processed when a service is provided from a service provider to a service consumer;

accessing via a computer network multiple pricing plans related to the transaction; and

rating the transaction in accordance with the multiple pricing plans.

25. The computer-readable medium of claim 24, having computer-executable instructions further comprising receiving output states from at least one pricing plan.

26. The computer-readable medium of claim 24, having computer-executable instructions further comprising a revenue fold, wherein the revenue fold summarizes the output of multiple pricing plans.

27. The computer-readable medium of claim 24, having computer-executable instructions further comprising selecting child accounts with end dates that are within a parent account's time period.

28. The computer-readable medium of claim 24, having computer-executable instructions further comprising pooling revenue/usage data as a function of billing cycles.

29. The computer-readable medium of claim 24, having computer-executable instructions further comprising determining a commission, wherein the commission is a credit given to an account.

30. The computer-readable medium of claim 24, having computer-executable instructions further comprising determining the value of a pricing plan as a function of another pricing plan.

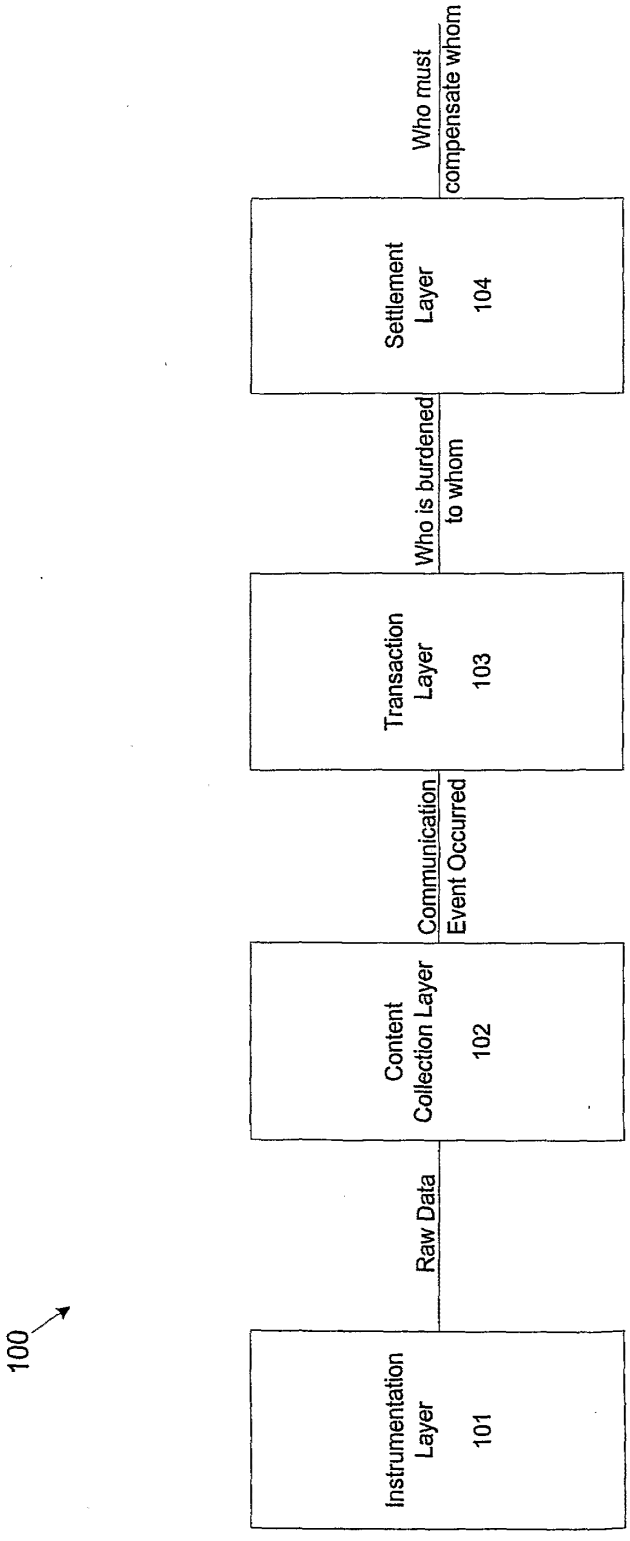

100
Instrumentation Layer 101
Raw Data
Content Collection Layer 102
Communication Event Occurred
Transaction Layer 103
Who is burdened to whom
Settlement Layer 104
Who must compensate whom

Figure 1

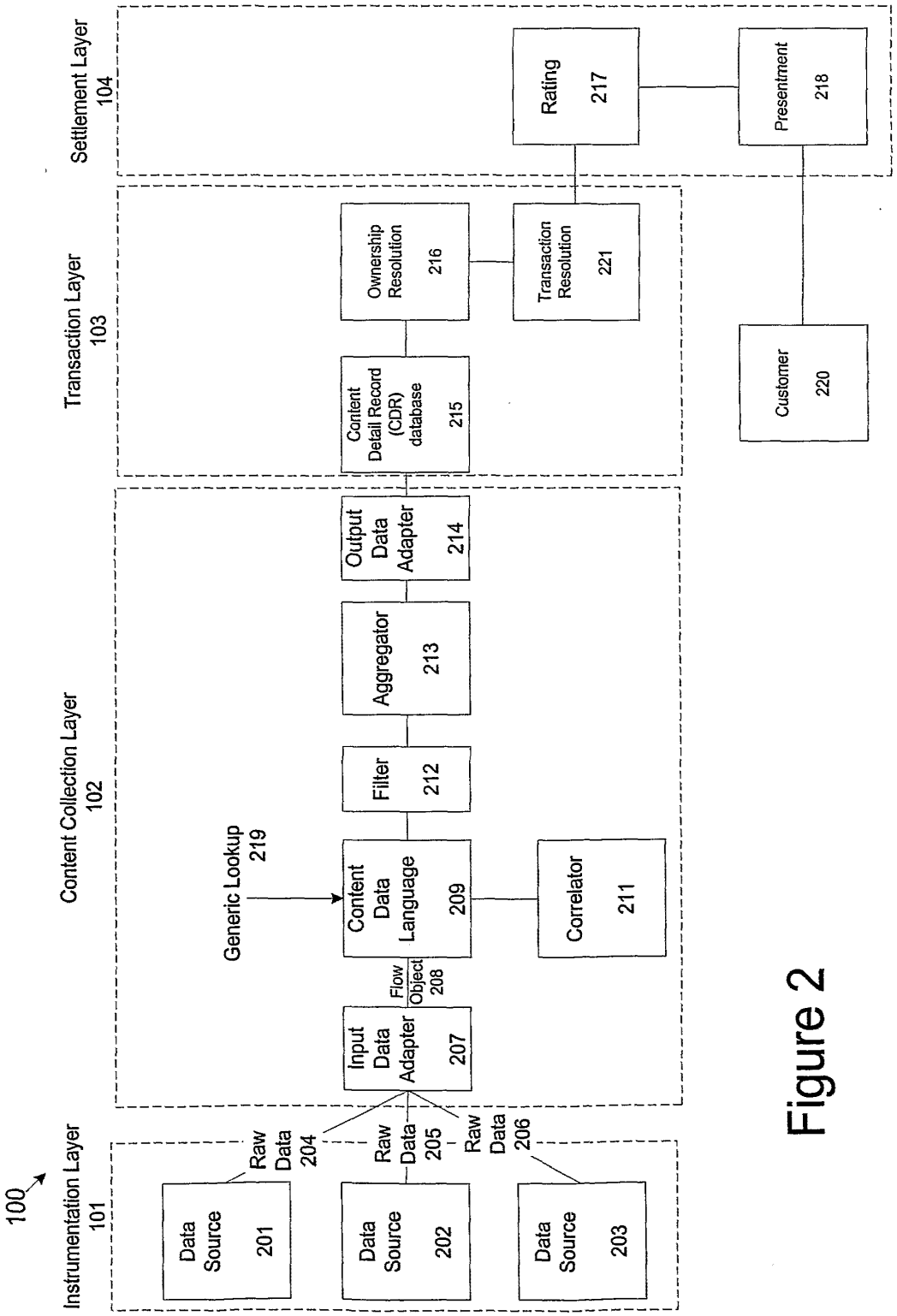

100
Instrumentation Layer 101
Data Source 201
Data Source 202
Data Source 203
Raw Data 204
Raw Data 205
Raw Data 206
Content Collection Layer 102
Input Data Adapter 207
Flow Object 208
Content Data Language 209
Generic Lookup 219
Filter 212
Aggregator 213
Output Data Adapter 214
Correlator 211
Transaction Layer 103
Content Detail Record (CDR) database 215
Ownership Resolution 216
Transaction Resolution 221
Settlement Layer 104
Rating 217
Presentment 218
Customer 220

Figure 2

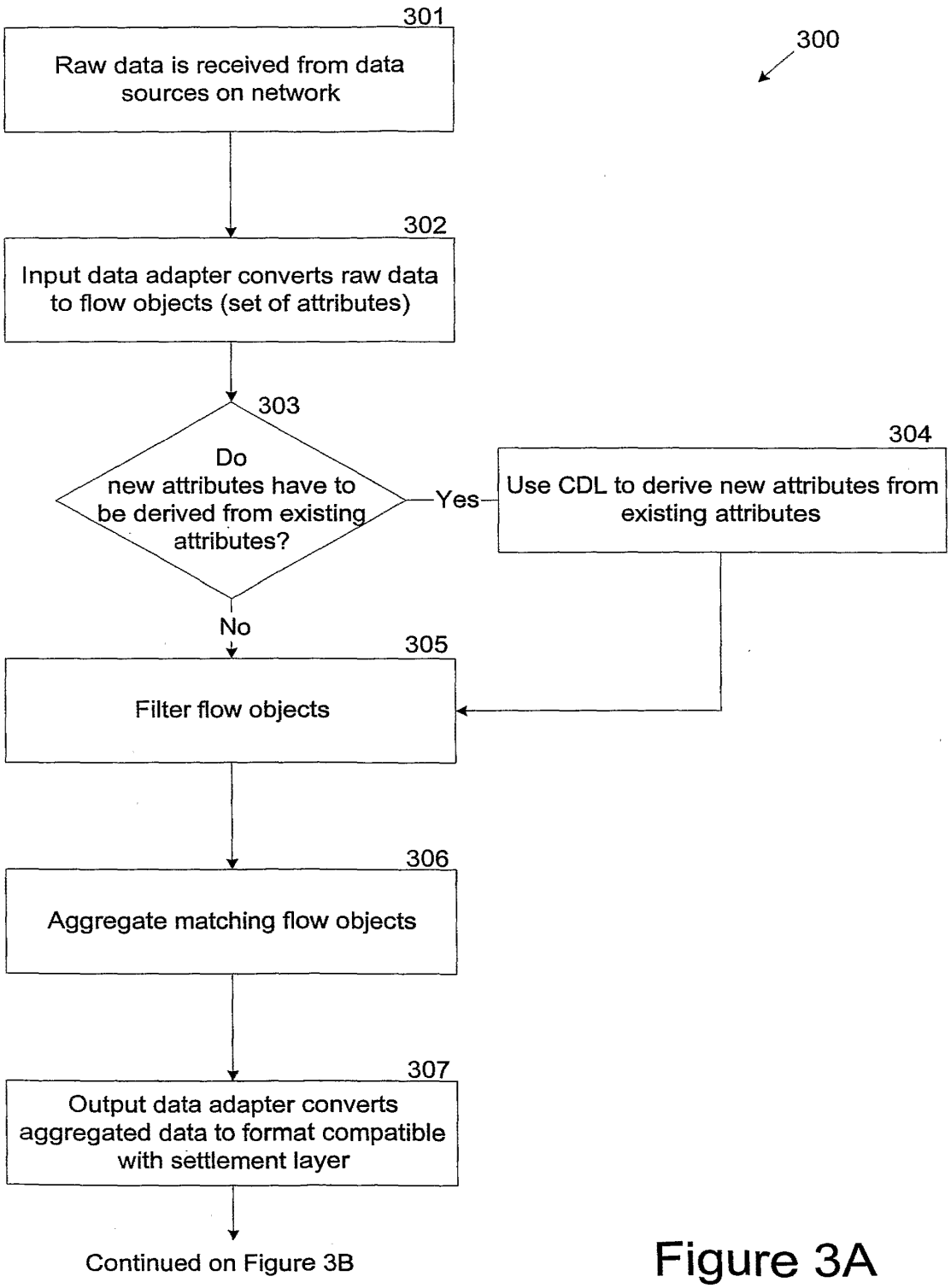

301
Raw data is received from data sources on network
300
302
Input data adapter converts raw data to flow objects (set of attributes)
303
Do new attributes have to be derived from existing attributes?
Yes
304
Use CDL to derive new attributes from existing attributes
No
305
Filter flow objects
306
Aggregate matching flow objects
307
Output data adapter converts aggregated data to format compatible with settlement layer
Continued on Figure 3B

Figure 3A

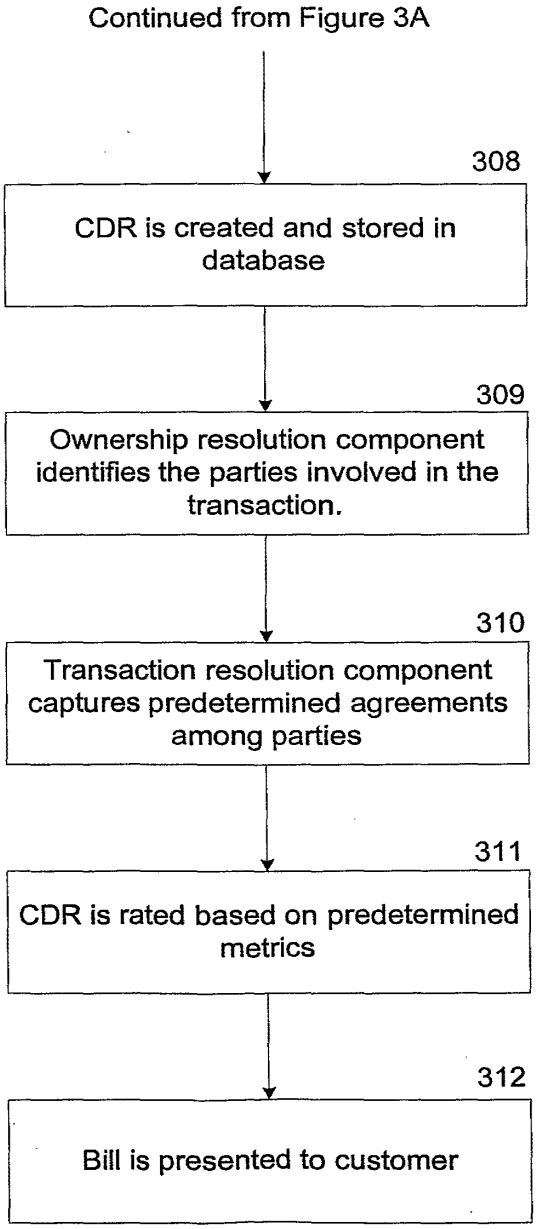

Continued from Figure 3A
308
CDR is created and stored in database
309
Ownership resolution component identifies the parties involved in the transaction.
310
Transaction resolution component captures predetermined agreements among parties
311
CDR is rated based on predetermined metrics
312
Bill is presented to customer

Figure 3B

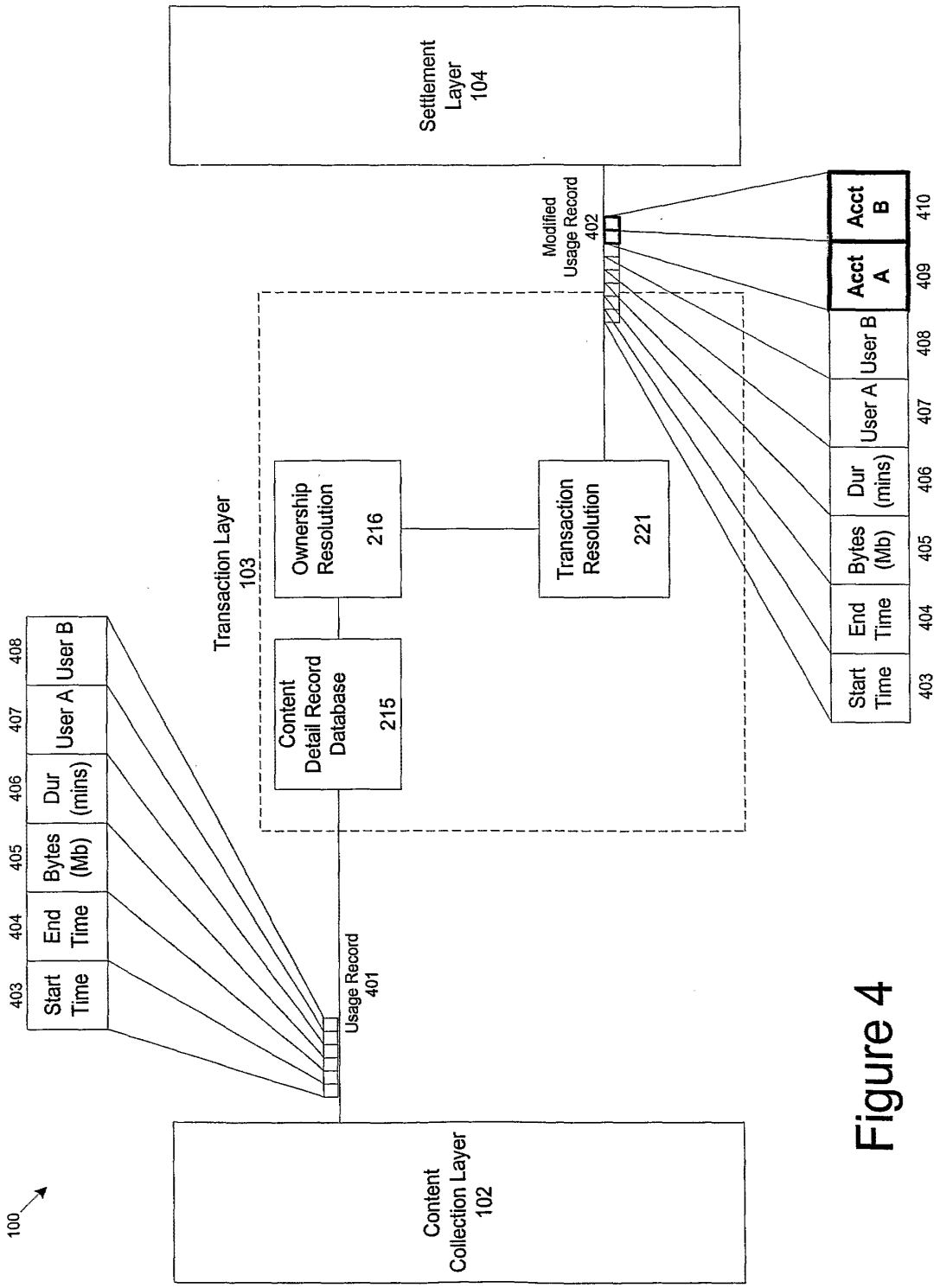

100
Content Collection Layer 102
Usage Record 401
Start Time 403
End Time 404
Bytes (Mb) 405
Dur (mins) 406
User A 407
User B 408
Transaction Layer 103
Content Detail Record Database 215
Ownership Resolution 216
Transaction Resolution 221
Modified Usage Record 402
Settlement Layer 104
Start Time 403
End Time 404
Bytes (Mb) 405
Dur (mins) 406
User A 407
User B 408
Acct A 409
Acct B 410

Figure 4

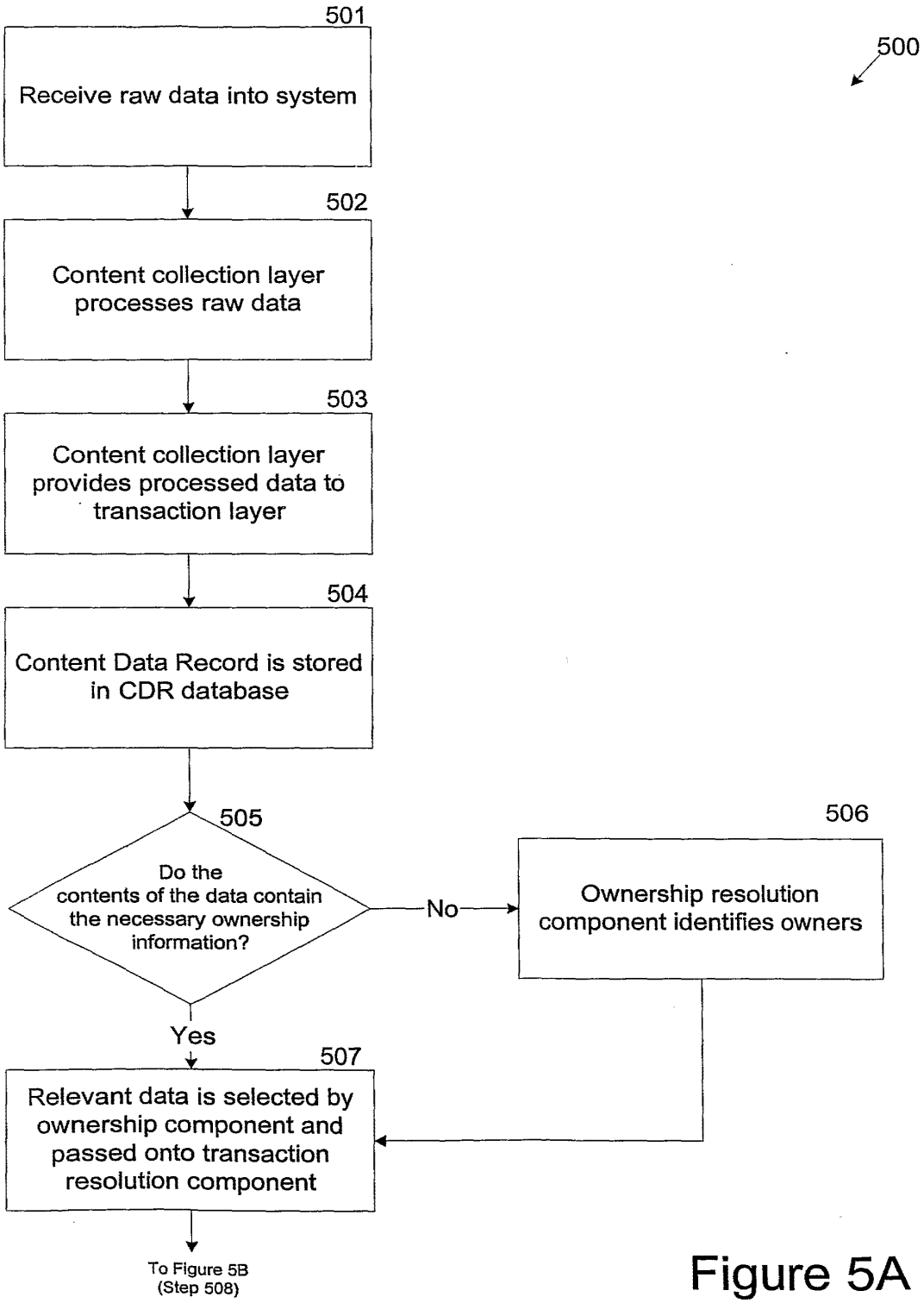

500
501
Receive raw data into system
502
Content collection layer processes raw data
503
Content collection layer provides processed data to transaction layer
504
Content Data Record is stored in CDR database
505
Do the contents of the data contain the necessary ownership information?
No
506
Ownership resolution component identifies owners
Yes
507
Relevant data is selected by ownership component and passed onto transaction resolution component
To Figure 5B (Step 508)

Figure 5A

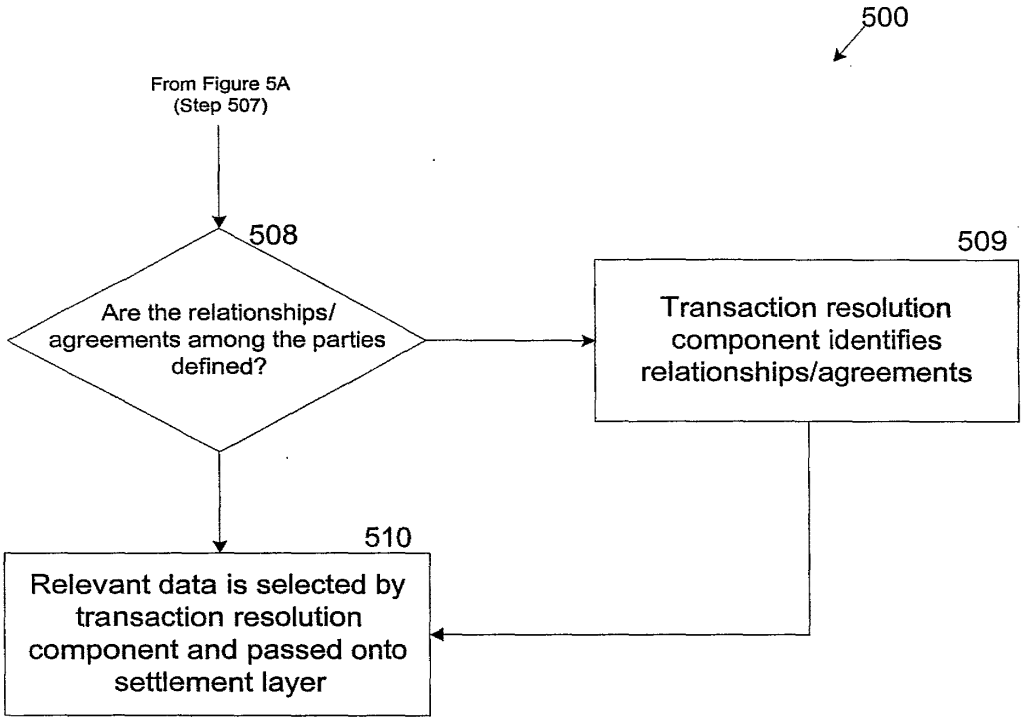

500
From Figure 5A
(Step 507)
508
Are the relationships/ agreements among the parties defined?
509
Transaction resolution component identifies relationships/agreements
510
Relevant data is selected by transaction resolution component and passed onto settlement layer

Figure 5B

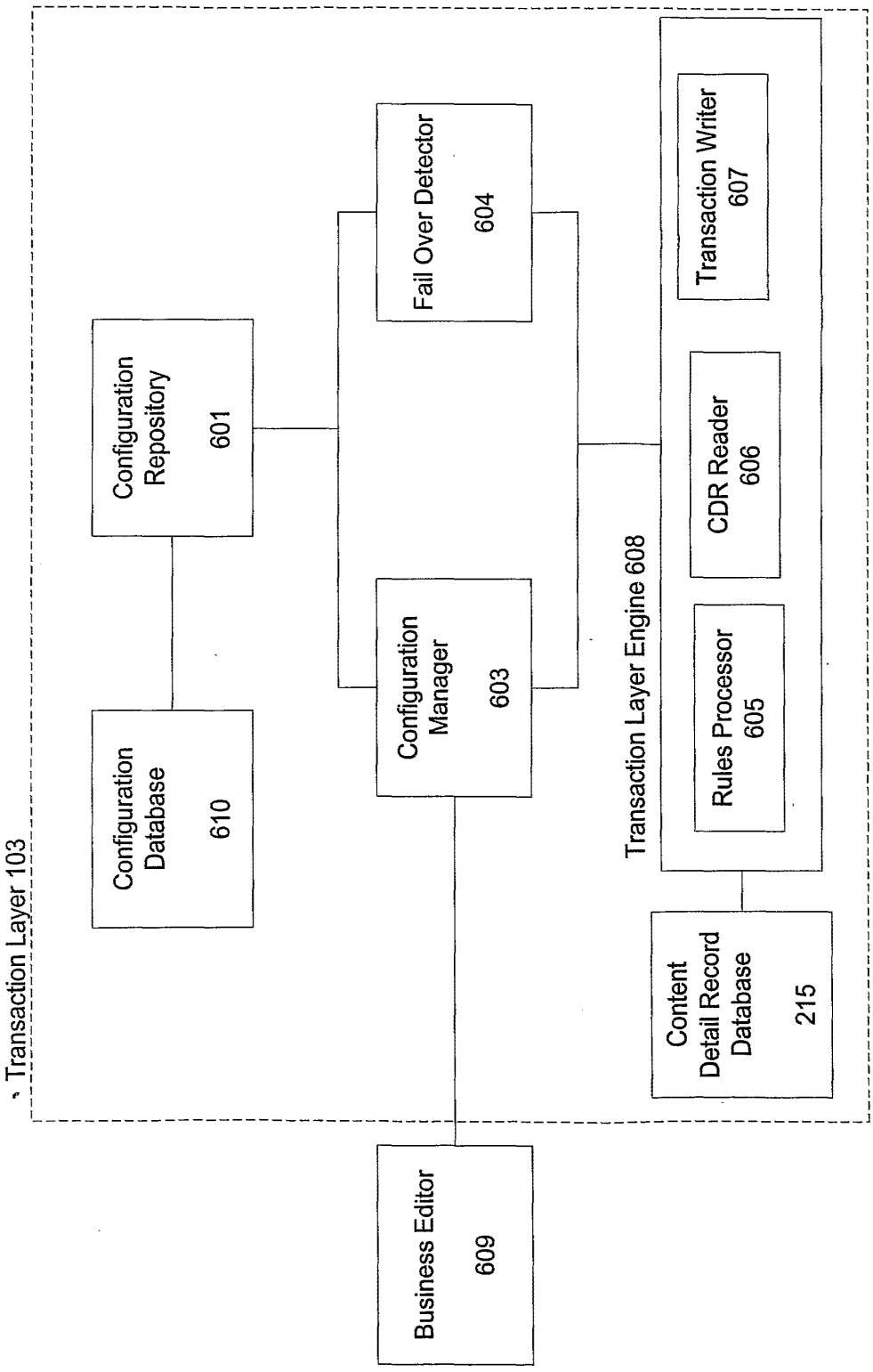

Transaction Layer 103
Configuration Repository 601
Configuration Database 610
Fail Over Detector 604
Configuration Manager 603
Transaction Layer Engine 608
Transaction Writer 607
CDR Reader 606
Rules Processor 605
Content Detail Record Database 215
Business Editor 609

Figure 6

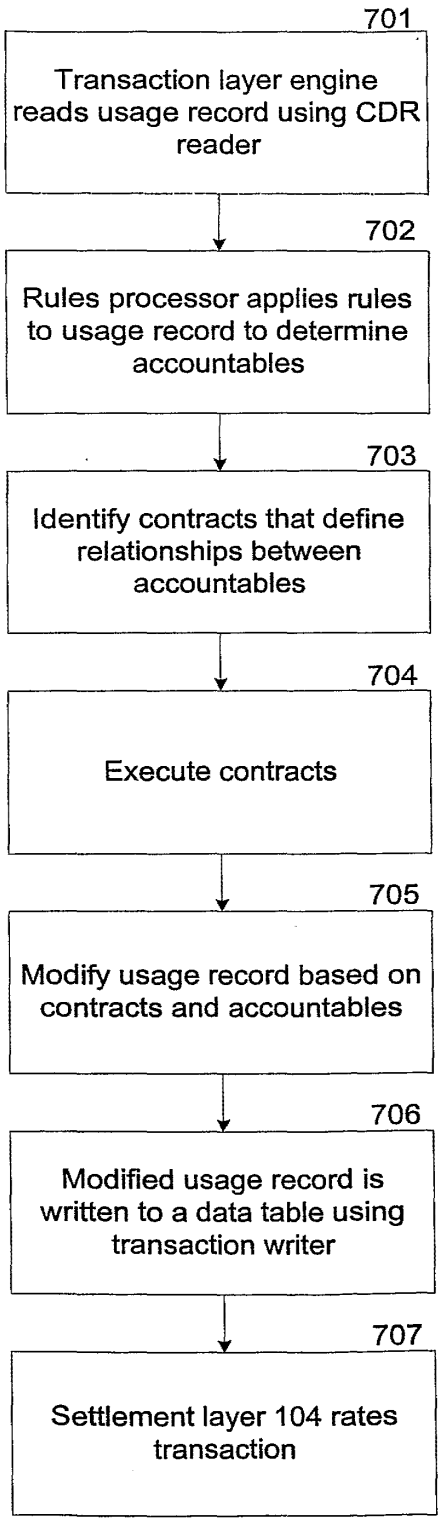

701
Transaction layer engine reads usage record using CDR reader
702
Rules processor applies rules to usage record to determine accountables
703
Identify contracts that define relationships between accountables
704
Execute contracts
705
Modify usage record based on contracts and accountables
706
Modified usage record is written to a data table using transaction writer
707
Settlement layer 104 rates transaction
700

Figure 7

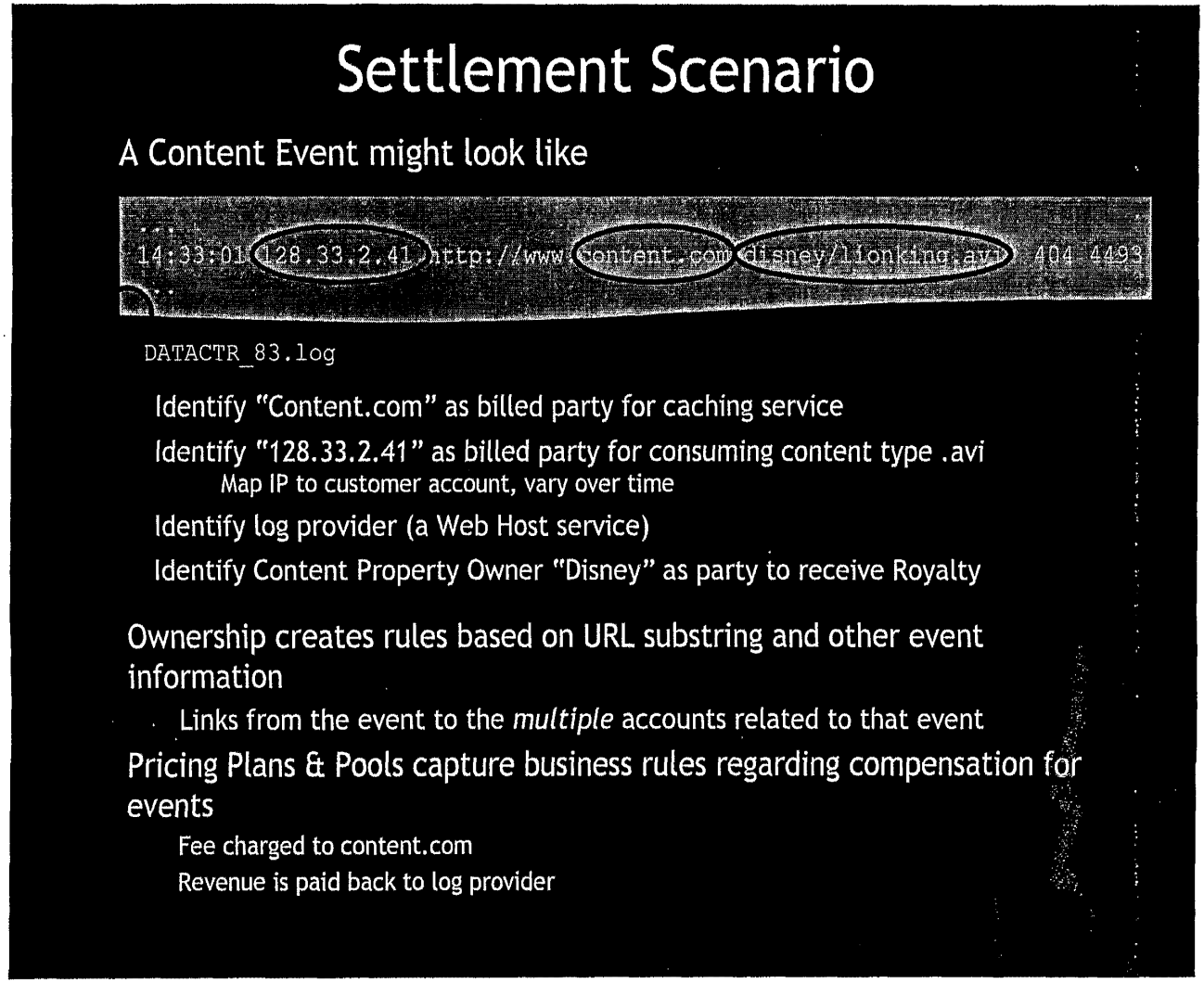

Settlement Scenario
A Content Event might look like
14:33:01 128.33.2.41 http://www.content.com disney/lionking.avi 404 4493
DATACTR_83.log
Identify "Content.com" as billed party for caching service
Identify "128.33.2.41" as billed party for consuming content type .avi
Map IP to customer account, vary over time
Identify log provider (a Web Host service)
Identify Content Property Owner "Disney" as party to receive Royalty
Ownership creates rules based on URL substring and other event information
Links from the event to the multiple accounts related to that event
Pricing Plans & Pools capture business rules regarding compensation for events
Fee charged to content.com
Revenue is paid back to log provider

Figure 8

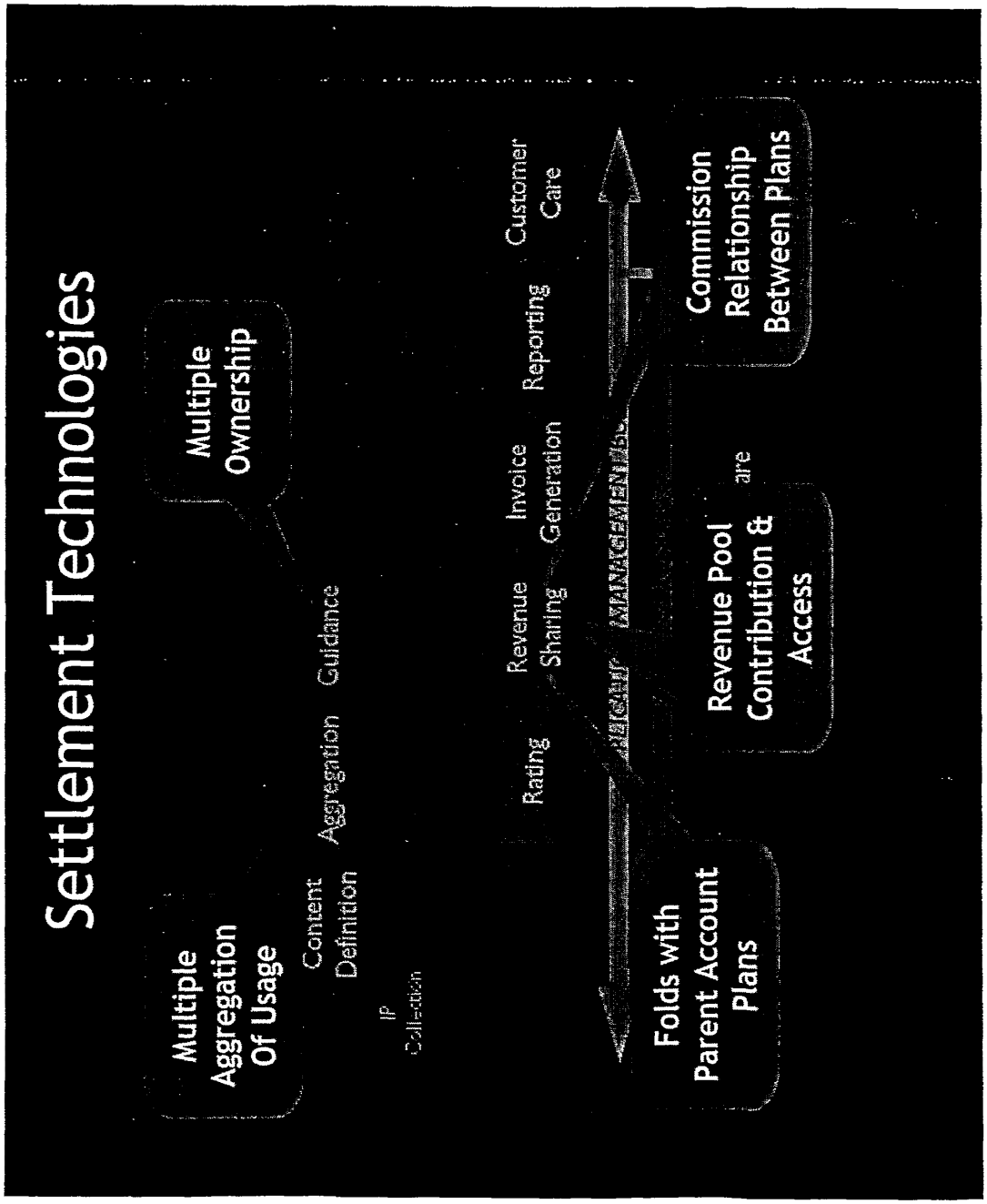

Settlement Technologies
Multiple Aggregation Of Usage
Content Definition
Aggregation
Guidance
IP Collection
Multiple Ownership
Rating
Revenue Sharing
Invoice Generation
Reporting
Customer Care
Folds with Parent Account Plans
Revenue Pool Contribution & Access
are
Commission Relationship Between Plans

Figure 9

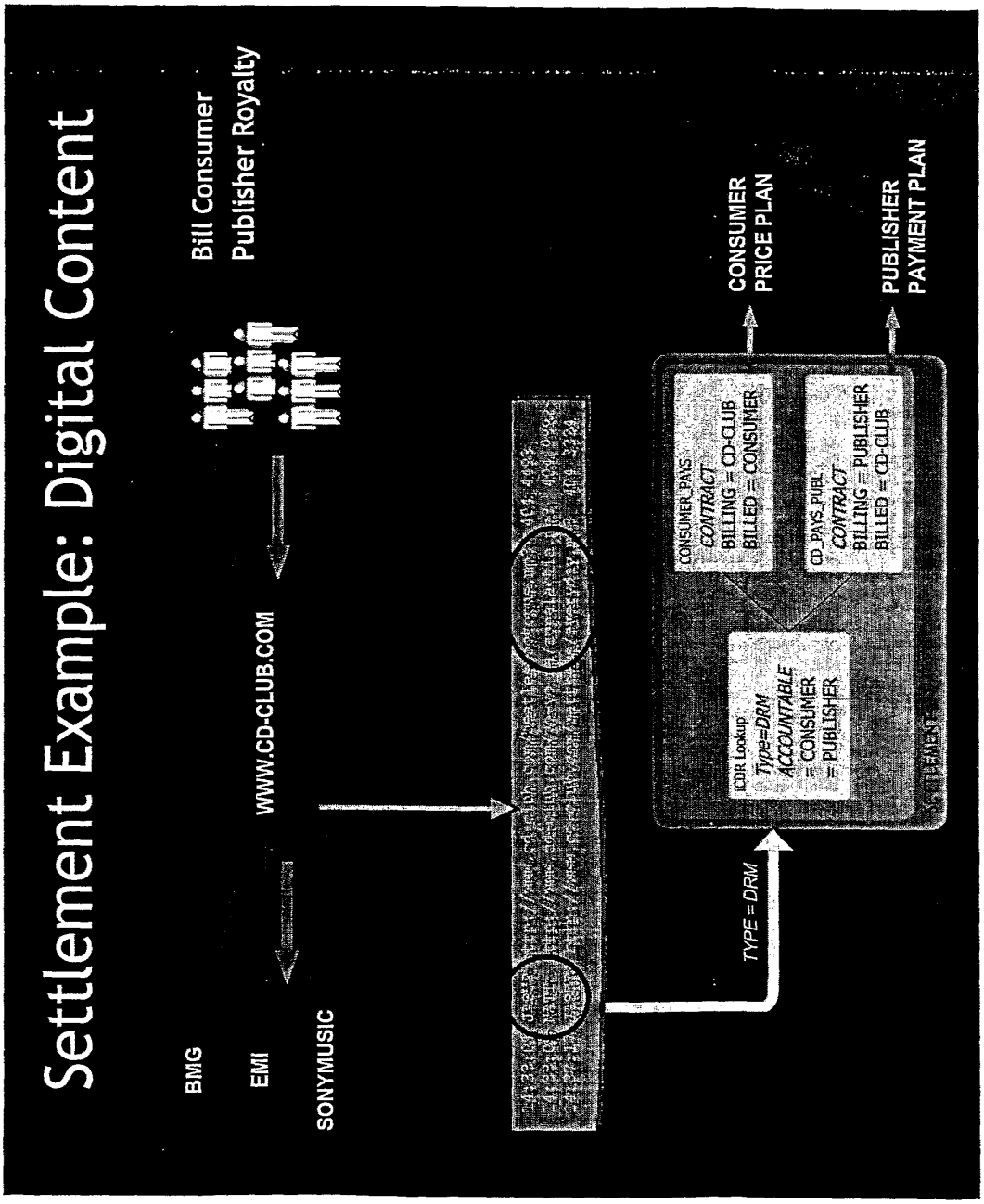

Settlement Example: Digital Content
Bill Consumer
Publisher Royalty
BMG
EMI
SONYMUSIC
WWW.CD-CLUB.COM
CONSUMER
PRICE PLAN
PUBLISHER
PAYMENT PLAN
CONSUMER_PAYS
CONTRACT
BILLING = CD-CLUB
BILLED = CONSUMER
CD_PAYS_PUBL
CONTRACT
BILLING = PUBLISHER
BILLED = CD-CLUB
CDR Lookup
Type=DRM
ACCOUNTABLE
= CONSUMER
= PUBLISHER
TYPE = DRM

Figure 10

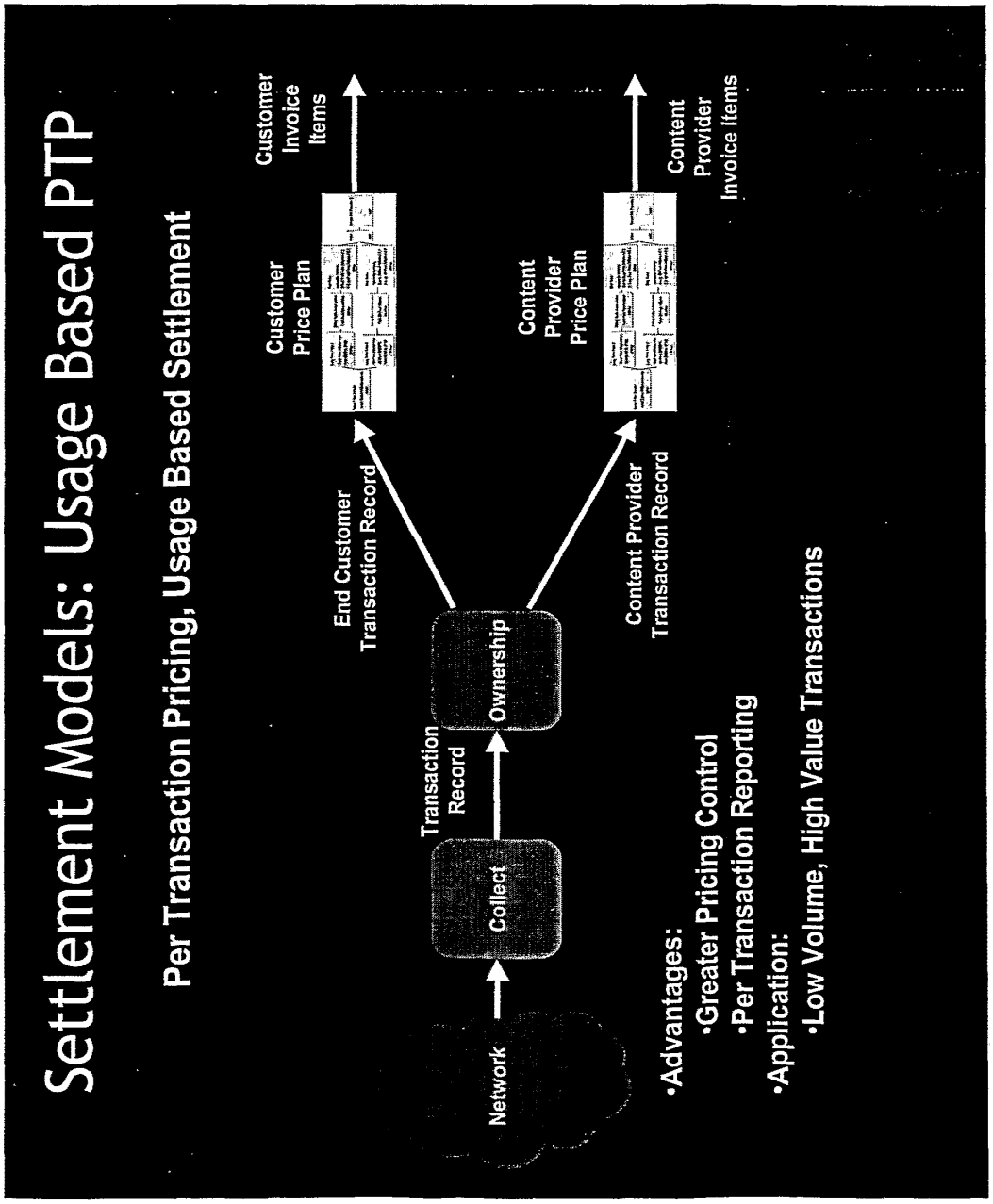

Settlement Models: Usage Based PTP
Per Transaction Pricing, Usage Based Settlement
Customer Invoice Items
Customer Price Plan
End Customer Transaction Record
Content Provider Price Plan
Content Provider Invoice Items
Content Provider Transaction Record
Transaction Record
Ownership
Collect
Network
•Advantages:
•Greater Pricing Control
•Per Transaction Reporting
•Application:
•Low Volume, High Value Transactions

Figure 11

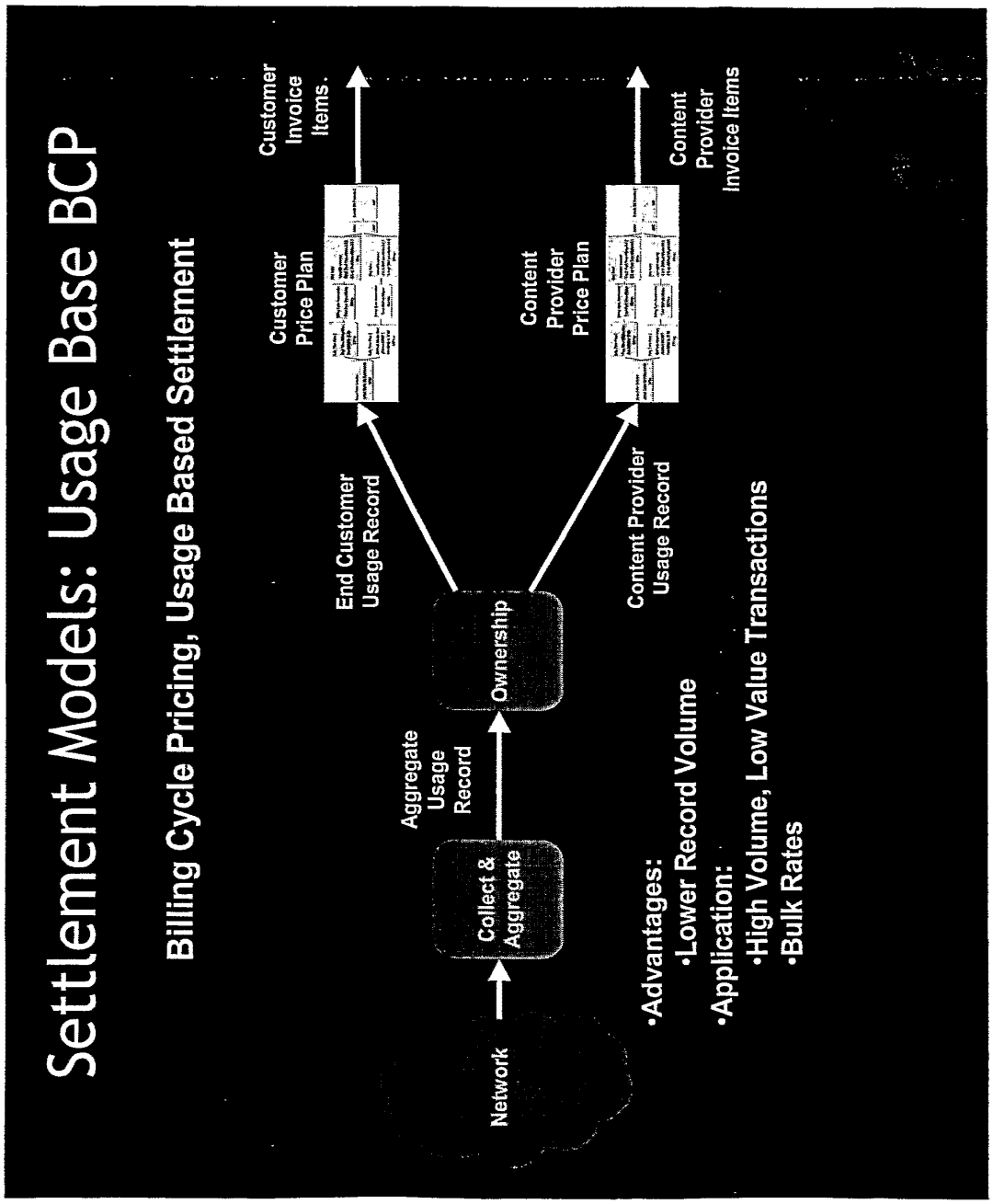

Settlement Models: Usage Base BCP
Billing Cycle Pricing, Usage Based Settlement
Customer Invoice Items.
Customer Price Plan
Content Provider Price Plan
Content Provider Invoice Items
End Customer Usage Record
Content Provider Usage Record
Aggregate Usage Record
Ownership
Collect & Aggregate
Network
•Advantages:
•Lower Record Volume
•Application:
•High Volume, Low Value Transactions
•Bulk Rates

Figure 12

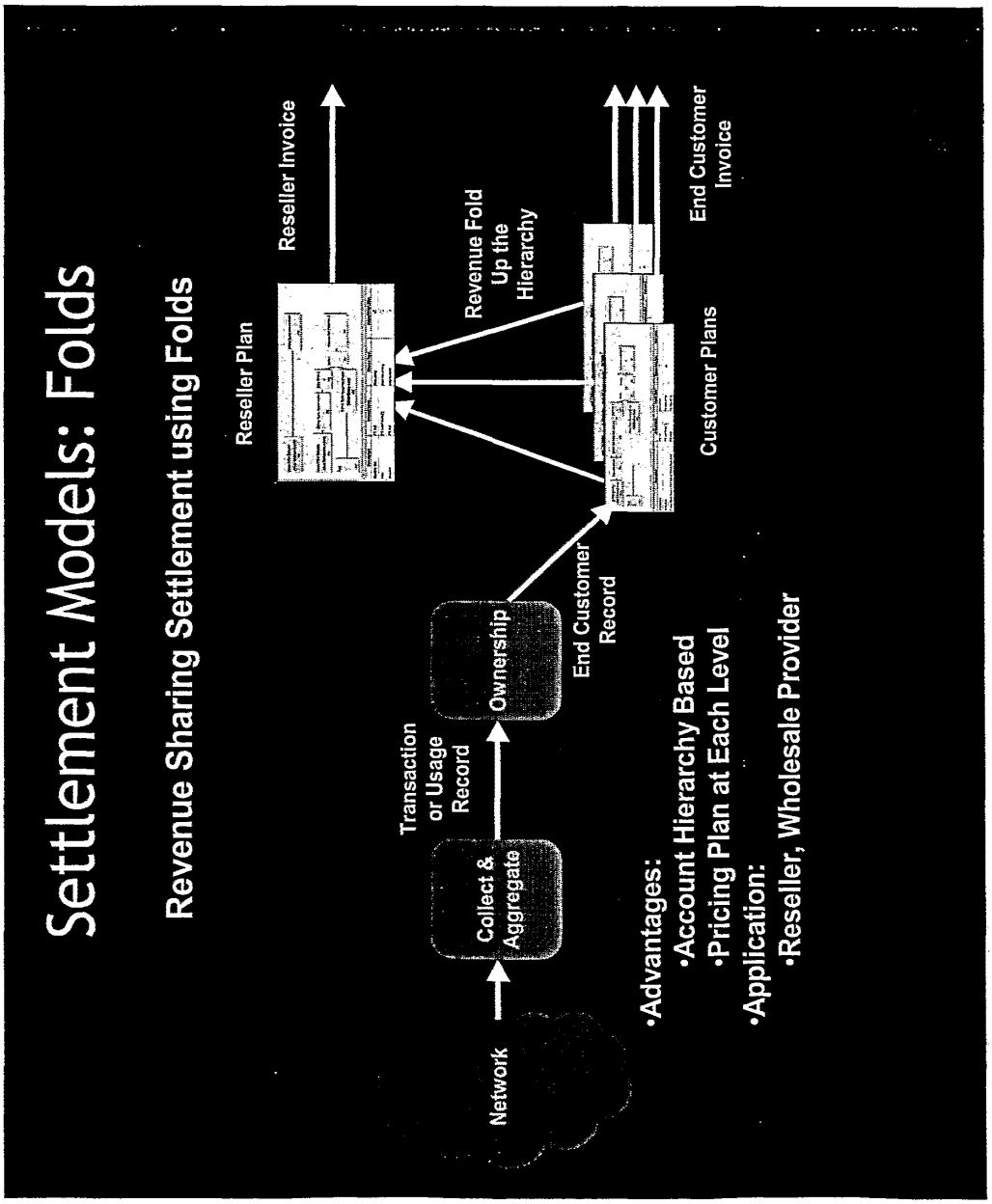

Settlement Models: Folds
Revenue Sharing Settlement using Folds
Reseller Plan
Reseller Invoice
Revenue Fold Up the Hierarchy
End Customer Invoice
Customer Plans
Transaction or Usage Record
Collect & Aggregate
Ownership
End Customer Record
Network
•Advantages:
•Account Hierarchy Based
•Pricing Plan at Each Level
•Application:
•Reseller, Wholesale Provider

Figure 13

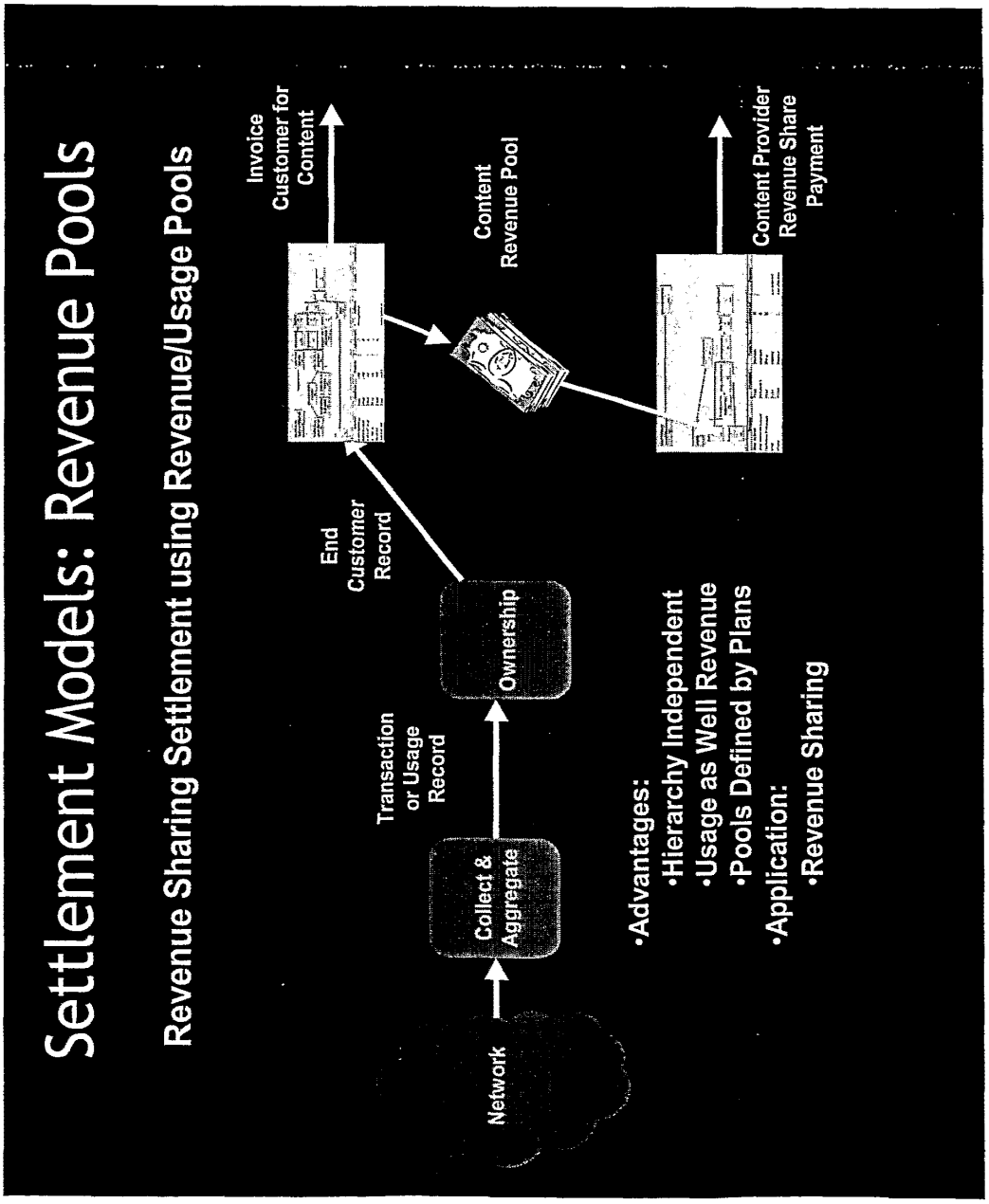

Settlement Models: Revenue Pools
Revenue Sharing Settlement using Revenue/Usage Pools
Network
Collect & Aggregate
Transaction or Usage Record
Ownership
End Customer Record
Invoice Customer for Content
Content Revenue Pool
Content Provider Revenue Share Payment
•Advantages:
•Hierarchy Independent
•Usage as Well Revenue
•Pools Defined by Plans
•Application:
•Revenue Sharing

Figure 14

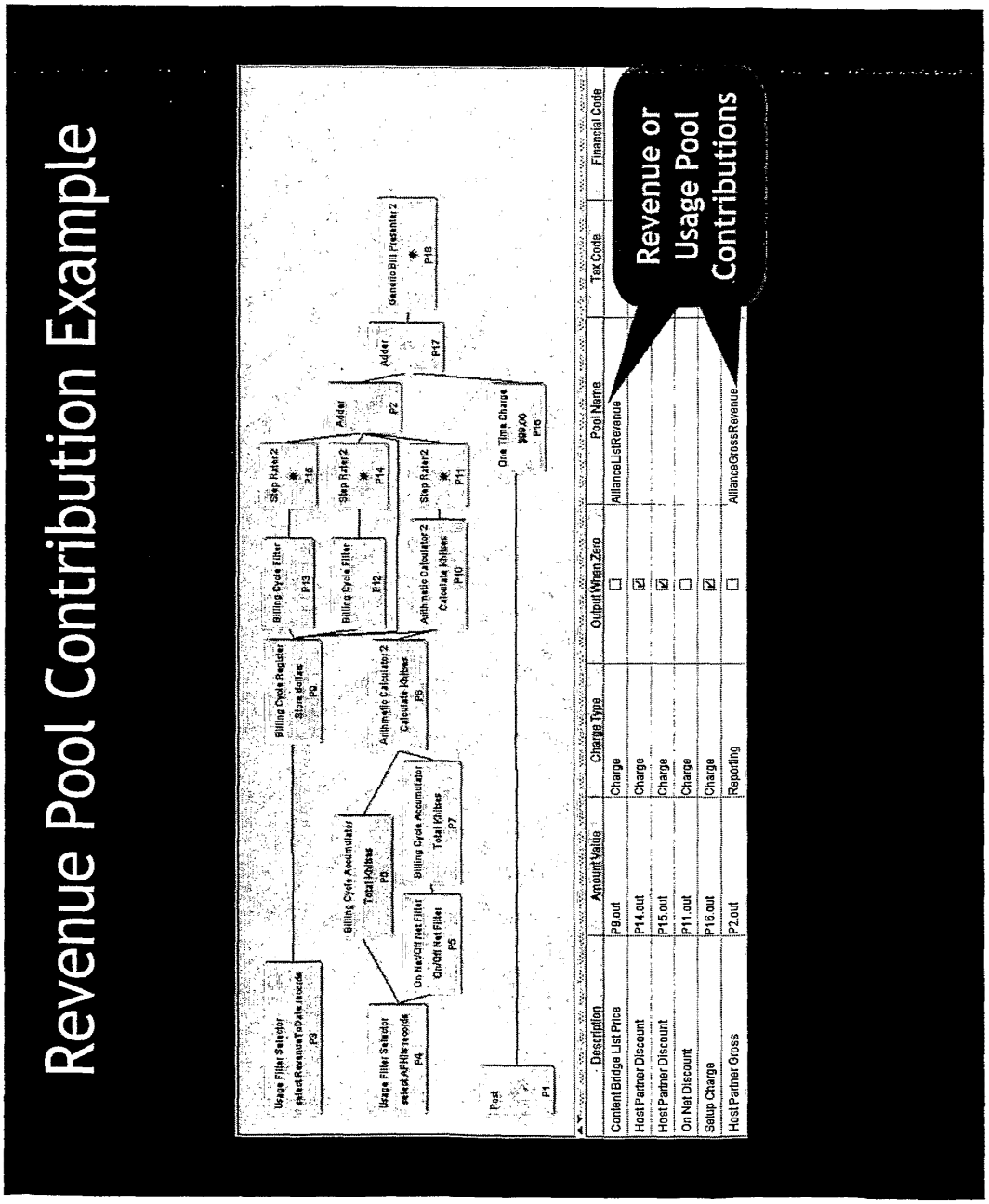
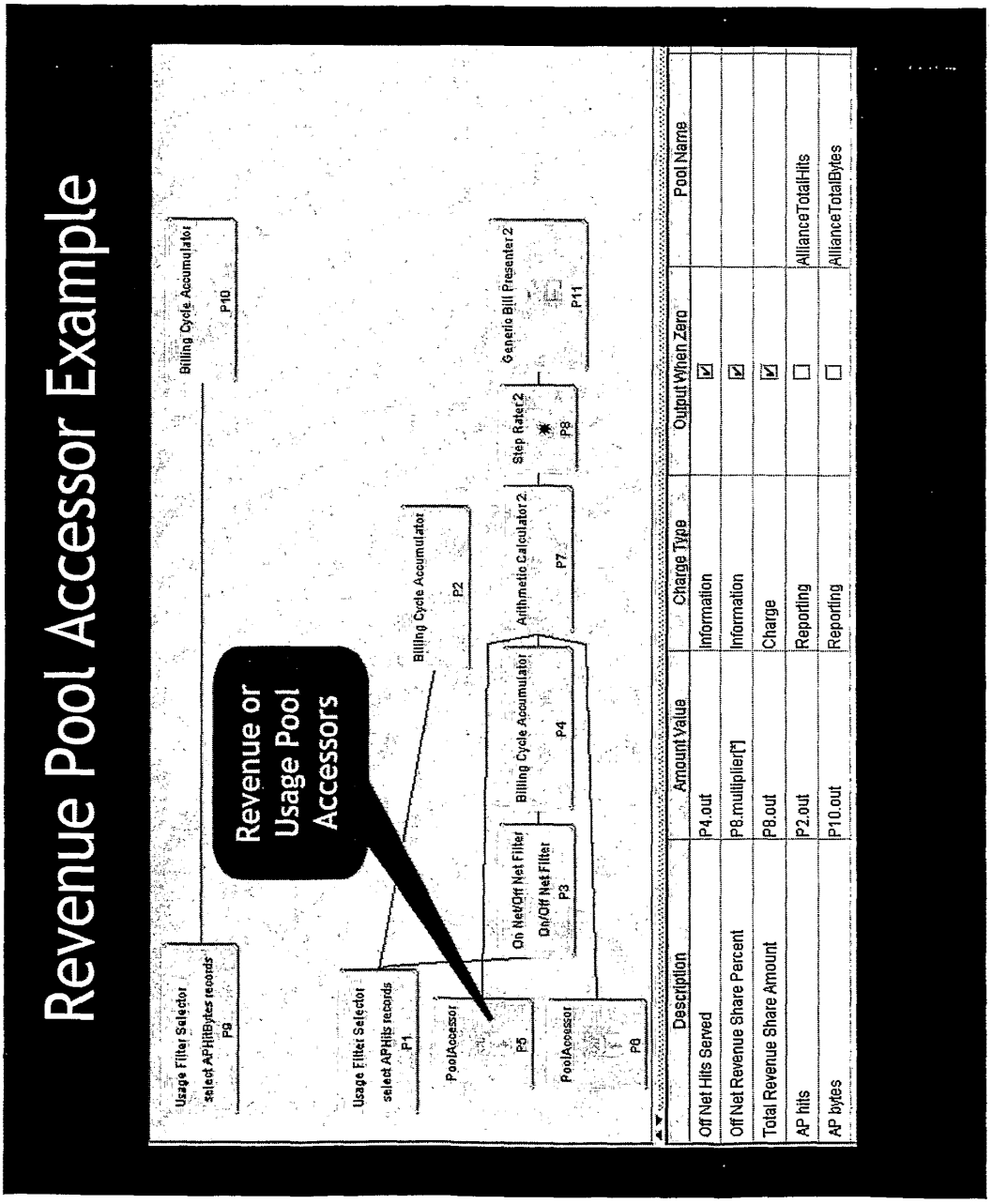

Revenue Pool Contribution Example
Revenue or Usage Pool Contributions
Post
P1
Usage Filter Selector select Revenue Tofrom records
P3
Usage Filter Selector select APIfile records
P4
On Net/Off Net Filter On/Off Net Filter
P5
Billing Cycle Accumulator Total Kbites
P6
Billing Cycle Accumulator Total Kbites
P7
Billing Cycle Register Store Kbites
P9
Arithmetic Calculator2 Calculate Kbites
P8
Billing Cycle Filter
P13
Billing Cycle Filter
P12
Arithmetic Calculator2 Calculate Kbites
P10
Step Rate2
P15
Step Rate2
P14
Step Rate2
P11
Adder
P2
One Time Charge $99.00
P16
Adder
P17
Generic Bill Presenter2
P18
Description
Amount Value
Charge Type
Output When Zero
Pool Name
Tax Code
Financial Code
Content Bridge List Price
P9.out
Charge
AllianceListRevenue
Host Partner Discount
P14.out
Charge
Host Partner Discount
P15.out
Charge
On Net Discount
P11.out
Charge
Setup Charge
P16.out
Charge
Host Partner Gross
P2.out
Reporting
AllianceGrossRevenue

Figure 15



Description	Amount Value	Charge Type	Output When Zero	Pool Name
Off Net Hits Served	P4.out	Information	☑	
Off Net Revenue Share Percent	P8.multiplier[*]	Information	☑	
Total Revenue Share Amount	P8.out	Charge	☑	
AP hits	P2.out	Reporting	☐	AllianceTotalHits
AP bytes	P10.out	Reporting	☐	AllianceTotalBytes

Figure 16

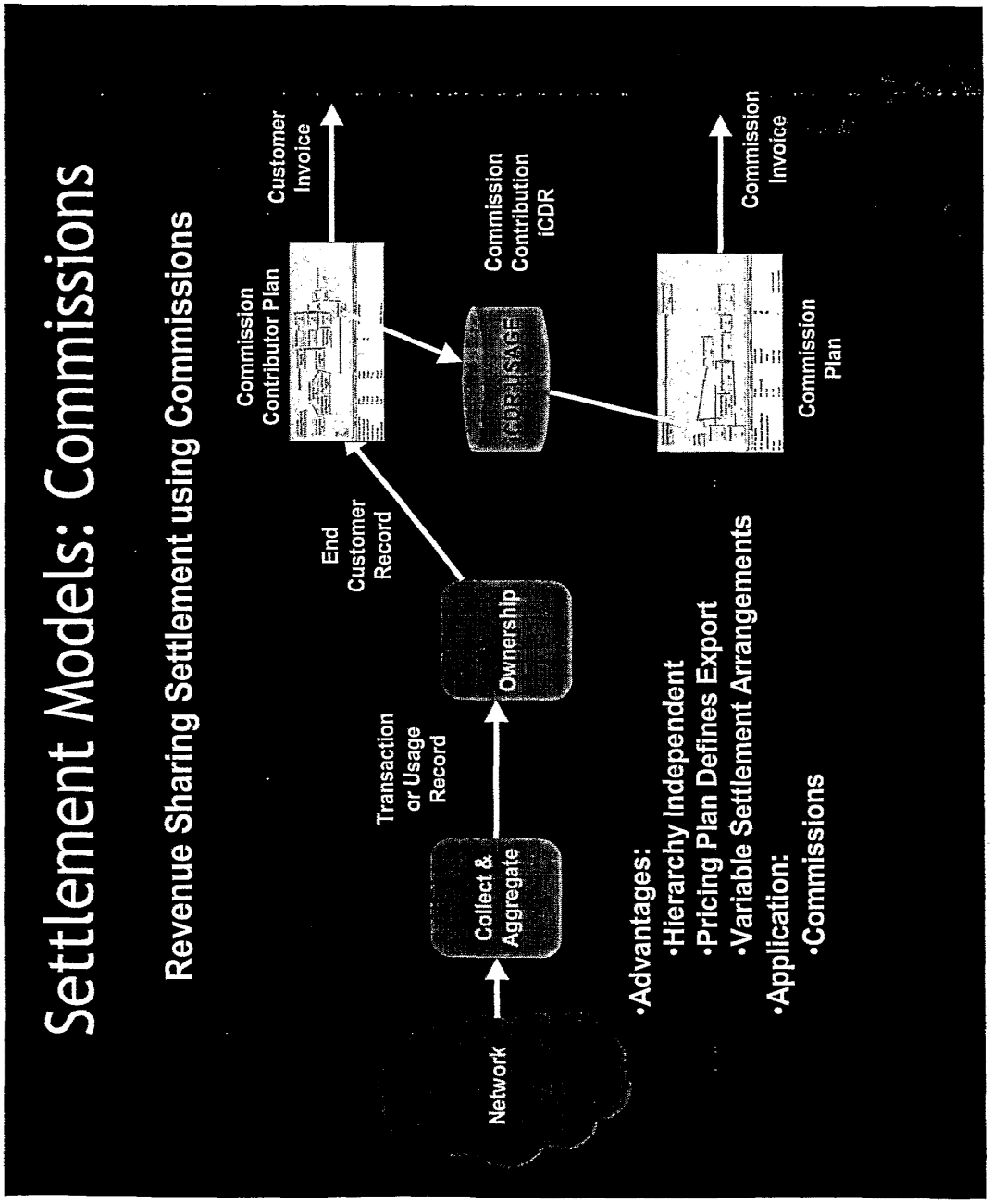

Settlement Models: Commissions
Revenue Sharing Settlement using Commissions
Network
Collect & Aggregate
Transaction or Usage Record
Ownership
End Customer Record
Commission Contributor Plan
Customer Invoice
Commission Contribution ICDR
Commission Plan
Commission Invoice
•Advantages:
•Hierarchy Independent
•Pricing Plan Defines Export
•Variable Settlement Arrangements
•Application:
•Commissions

Figure 17

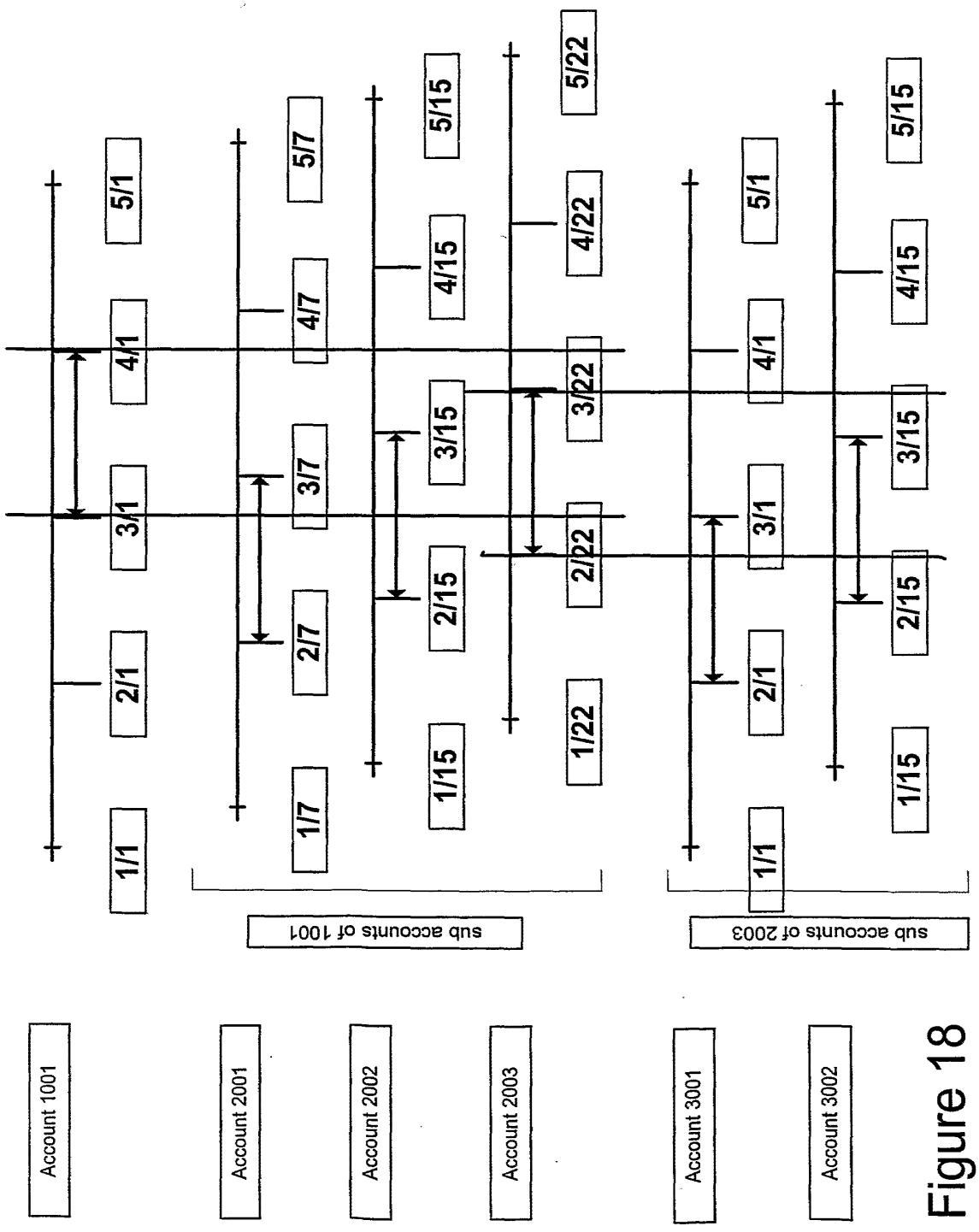

Account 1001
Account 2001
Account 2002
Account 2003
Account 3001
Account 3002
sub accounts of 1001
sub accounts of 2003
1/1
2/1
3/1
4/1
5/1
1/7
2/7
3/7
4/7
5/7
1/15
2/15
3/15
4/15
5/15
1/22
2/22
3/22
4/22
5/22

Figure 18

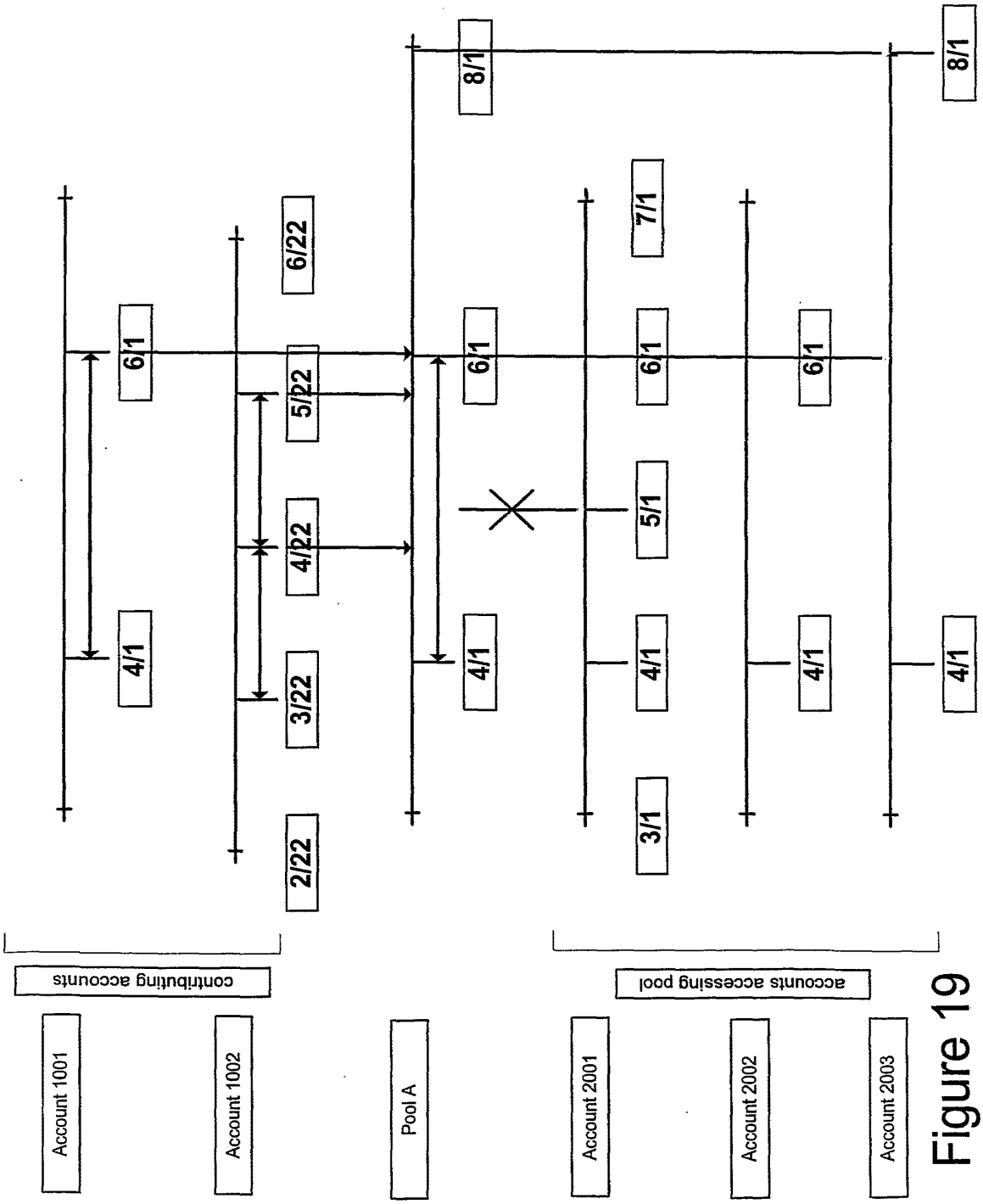

8/1
8/1
6/22
7/1
6/1
6/1
6/1
6/1
5/22
5/1
4/22
4/1
4/1
4/1
4/1
4/1
3/22
3/1
2/22
contributing accounts
accounts accessing pool
Account 1001
Account 1002
Pool A
Account 2001
Account 2002
Account 2003

Figure 19

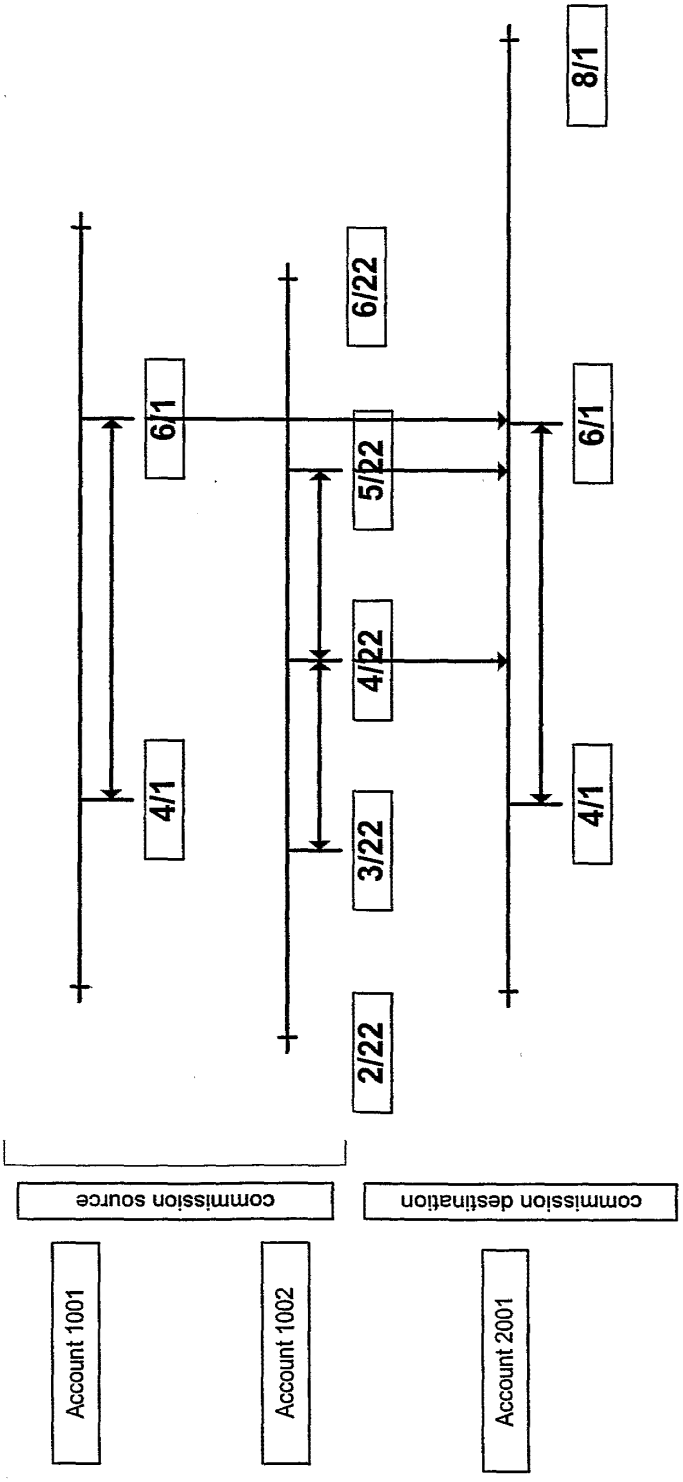

Account 1001
Account 1002
Account 2001
commission source
commission destination
6/1
4/1
2/22
3/22
4/22
5/22
6/22
8/1
6/1
4/1

Figure 20

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 August 2002 (29.08.2002)

PCT

(10) International Publication Number
WO 02/067616 A1

(51) International Patent Classification[7]: H04Q 7/38, H04M 15/00

(21) International Application Number: PCT/FI02/00128

(22) International Filing Date: 15 February 2002 (15.02.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20010302 16 February 2001 (16.02.2001) FI

(71) Applicant *(for all designated States except US)*: **SONERA OYJ** [FI/FI]; Teollisuuskatu 15, FIN-00510 Helsinki (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **YLI-KORHONEN, Jukka** [FI/FI]; Tarkka-ampujankatu 17 D 56, FIN-90120 Oulu (FI). **JUNTUNEN, Ari** [FI/FI]; Sihtikuja 1 D 51, FIN-90520 Oulu (FI). **KEINÄNEN, Kimmo** [FI/FI]; Talvikkitie 18 A 3, FIN-90580 Oulu (FI).

(74) Agent: **KOLSTER OY AB**; Iso Roobertinkatu 23, P.O.Box 148, FIN-00121 Helsinki (FI).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), DE (utility model), DK (utility model), DM, DZ, EC, EE (utility model), ES, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM, METHOD AND NETWORK NODE FOR PROVIDING SERVICE-SPECIFIC BILLING IN A TELECOMMUNICATIONS SYSTEM

P	ID	N	S1	V	S2	SV	BV
Elvis	PT	price_today	:	number	&	0	500
Elvis	EC	extra_cutback	=	number	&	0	250
Iiris	SP	single_payment	-	number	*	250	250

(57) Abstract: In a multi-provider environment, where a network operator provides bearer services and a service provider provides the actual service, customizing billing for services requires accurate contracts concerning the content and structure of billing data transmitted by the service provider. In order to eliminate this problem, a billing content is determined for a service in such a manner that the content is available to the network operator and it determines parameters (N) provided in service billing data and indicates how to find the parameters from the billing data (ID, S1, S2). For determining billing data, definition rules are defined in advance to indicate at least the type of data that should be specified for each parameter.

WO 02/067616 A1

System, method and network node for providing service-specific billing in a telecommunications system

FIELD OF THE INVENTION

The invention relates to billing for a service transmitted in a telecommunications system, and particularly to providing service-specific billing.

BACKGROUND OF THE INVENTION

Services provided in telecommunications systems are more and more often produced in a multi-provider environment, where a network operator provides bearer services and one or more service providers provide the actual services. A service provider does not maintain a network but purchases the required bearer services from the network operator. Thus, the total price of a service is a combination of the price of the connection and the price of the actual service or content. Even in a multi-provider environment the best way to charge a client is that the network operator attends to authentication and billing of the user of the service according to the user's phone number also on behalf of the service provider. An actual bill is based on billing data transmitted by the service provider in a service response, and collected and processed by a billing data collecting system of the network operator.

A problem with such billing is that the operator and the service provider must have accurate contracts concerning the content and structure of the billing data in order that a service could be billed for in the way the service provider wants. In case of a large number of service providers, the network operator does not necessarily have time or is not able to agree in detail on the contents of the billing data with each service provider, which means that either the introduction of a service into the market will be delayed, or the service provider must arrange billing in some other manner or use an existing billing method, which may not be the best for the service in question.

BRIEF DESCRIPTION OF THE INVENTION

An objective of the invention is to develop a method and equipment implementing the method so as to solve the aforementioned problems. The objective of the invention is achieved by a method, system and network nodes, which are characterized by what is disclosed in the independent claims. The preferred embodiments of the invention are disclosed in the dependent claims.

The invention is based on detecting this problem and on solving it by providing a system of a network operator, preferably a system for process-

ing billing data, with a mechanism for informing the network operator of the form in which the billing data should be disclosed. The mechanism is preferably created by determining rules for defining billing parameters and by determining, by means of these rules, a billing content of a service, which is available to the network operator when forming a call detail record, and by storing the billing content in the system so as to be available to a process producing tickets. A billing content determines the service-specific parameters used in a call detail record, i.e. a ticket, and indicates how to locate the parameters in the billing data. The processing system can constitute a part of the system for collecting billing data.

An advantage of the invention is the ability to transmit and process billing data, which has different contents for different services since the billing parameters can be freely selected. Another advantage of the invention is that no specific service contract is needed between the network operator and the service provider, since the invention enables determining the structure of the billing data in such a manner that the network operator's system identifies the billing parameters and their values. Therefore the operator can provide user authentication and billing services globally to service providers. This even enables billing for free browsing, where a user is able to use all the services and not only the services of the operator or partners thereof.

BRIEF DESCRIPTION OF THE FIGURES

The invention will be described below in more detail by means of the preferred embodiments and with reference to the accompanying drawings, in which

Figure 1 shows a simplified network architecture,

Figure 2 shows an example of determining a billing content according to a first preferred embodiment of the invention,

Figure 3 shows formation of a ticket according to the first preferred embodiment of the invention, and

Figure 4 shows an example of a ticket according to the first preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention can be applied in connection with any telecommunications system where the data required for billing a subscriber is transmitted together with service data. Such systems include for example third-

generation mobile systems, such as the Universal Mobile Telecommunications System (UMTS), and mobile systems similar to the pan-European GSM (Global System for Mobile Communications), such as the GSM 1800 and the PCS (Personal Communication System), and systems based on the aforementioned systems, such as GSM 2+ systems. GSM 2+ services include the general packet radio service (GPRS) and customized applications for mobile network enhanced logic (CAMEL). The invention can also be applied in fixed systems. The invention will be described below by using as an example the GSM providing a WAP (Wireless Application Protocol) service, without restricting the invention thereto, however. The WAP is a protocol specification that enables apparatuses utilizing wireless data transmission, such as mobile phones, to use Internet services.

Figure 1 shows a simplified network architecture of a first preferred embodiment of the invention, and it illustrates only some elements of a system architecture J. Network nodes shown in Figure 1 are logical units, the implementation of which can differ from that of the figure. It is obvious to a person skilled in the art that the system can also comprise other functions and structures, which do not have to be described in more detail herein. The description of the system is by no means restrictive but only suggestive.

The system shown in Figure 1 consists of a system of a network operator VJ and a system of a service provider PJ. In the example of Figure 1, a mobile station MS user has set up a connection to a server S providing a WAP service via the network operator's network PLMN via a WAP gateway W_GW in a previously known manner. In the first preferred embodiment of the invention, the WAP gateway W_GW picks the billing data from a service response transmitted by the server and stores it in a log file, which is retrieved by a charging gateway CG connected to the network operator's network PLMN and which is processed into call detail records, i.e. tickets. An example of a ticket is shown in Figure 4. The tickets are then transmitted to a billing centre BC, which attends to billing of a user. The picking of billing data refers to picking of data used to form a ticket, such as a part of the service response containing the data required in billing. In a service response, billing data can be located for example in an HTTP (Hyper Text Transport Protocol) header. In another embodiment of the invention, the WAP gateway W_GW does not store the billing-related data that was picked into a log file but transmits the data to the charging gateway CG for example via a real-time interface. The details of

the billing, e.g. how billing data is transmitted, collected and retrieved and where it is stored, are not significant for the invention. For example, arranging billing for the WAP service is described in more detail in Finnish Patent Application 20000589 (Arranging billing in a telecommunications system), which is incorporated herein by reference.

The charging gateway CG comprises an interface I, via which service-specific billing contents LS can be determined in the charging gateway. Examples of such billing contents are shown in Figure 2. The interface I thus provides configuring means for determining the content and structure of the billing data and the ticket and for storing them by means of the definition rules for billing parameters. Billing contents are preferably stored in a memory M of the charging gateway. The network operator has usually determined the definition rules and the service provider determines the actual billing content of the service, i.e. it determines the required parameters and provides parameter specifications. The actual billing content is input/processed into the memory M of the charging gateway via the interface I by the operator or the service provider, depending on their mutual agreement. The interface I can also be arranged to check, in connection with the input or processing of the billing content, that the parameter specifications comply with the definition rules. The definition rules are preferably the same for all the service providers, but the network operator can also customize the rules separately for each service provider. Inputting billing contents does not preferably require a service contract between the service provider and the network operator, but the service provider may be able to input billing contents for example via the Internet after having accepted certain rules and passed a log-in process. The charging gateway CG also comprises processing means, i.e. a process P, which converts the billing data into a ticket by means of the billing content specified for the service. The operation of the process P will be described in more detail in connection with Figure 3.

Depending on the embodiment, the interface I can be located in a different network node than the stored billing contents LS. Neither has to be located in the charging gateway. A network node where the billing contents LS are stored comprises means for receiving requests on billing contents and means for processing and transmitting responses.

In addition to prior art means, a system implementing the functionality of the present invention and the network nodes of the system comprise

means for creating and storing service-specific billing contents. The system and the network nodes can also comprise means for processing a billing content. The means are preferably implemented by using the present network nodes, especially the processors and memory thereof. All the modifications required to implement the invention can be carried out in the form of added or updated software routines, application-specific integrated circuits (ASIC) and/or programmable circuits.

Figure 2 shows a manner according to the first preferred embodiment of the invention of determining service-specific billing contents stored in a database table where each service-specific parameter to be taken into account in billing is provided with required data, i.e. the parameters are determined according to the definition rules. It is assumed in the first preferred embodiment of the invention that a billing ticket consists of standard data and service-specific data. Parameters for the standard data are determined generally in the first preferred embodiment, i.e. they are shared by all services. Such standard data includes for example user identifier, service name, service status data, and time. Standard data or some part of it can be transmitted with service-specific billing data, but for example in case of WAP services they are usually obtained in some other manner. Service-specific data is determined in the billing content of a service. The parameters that should be or may be specified in the billing content naturally depend on the operator, the billing system used by the operator, and the form in which billing data is transmitted. These matters are described in the definition rules. The essential fact in the billing content of an individual service is that it can be connected to a specific service and that at least one billing parameter is determined in such a manner that the billing parameter and the value thereof can be somehow separated from the billing data. However, in the first preferred embodiment of the invention it is not necessary to determine a billing content for all the services if standard data is sufficient to bill for a service.

In the example shown in Figure 2, it is assumed for the sake of clarity that the service name identifies the service sufficiently, i.e. the service cannot be confused with any other service, and different service providers do not have services with similar names. In embodiments where a mere service name does not identify a service sufficiently accurately, a service to be billed for can be identified for example based on the names of both the service provider and the service.

In the first preferred embodiment of the invention, the definition rules do not restrict in any way the ability of service providers to determine the parameters to be taken into account in billing, and the only requirement is that each parameter of a service billing content is provided with not only a name N but also the following data:

- The service P to which the parameter is related. A parameter defined by means of a service can be connected to the service billing content,
- A parameter identifier ID used in billing data to help locate the parameter and the value thereof,
- A separator S1 between an identifier and the value thereof in the billing data,
- Value type V,
- The allowed range of variation of the value indicated by means of the lowest value SV and the highest value GV, and
- A separator S2 between the identifiers.

On the basis of this data, a single ticket may contain 1 to n items of service-specific billing data, which are mutually independent. The billing data can even consist of data not used by the network operator in its own billing. For example based on the specifications shown in Figure 2, a ticket formed of a service called 'Elvis' contains the billing value of two parameters in the service-specific data, and a ticket formed of a service called 'Iiris' contains the billing value of one parameter. The same parameter can also be used in different services and with different ranges of variation. Eliminating parameters from or adding new parameters into a service is easy and simple in the first preferred embodiment of the invention. It is also easy and simple to alter parameter specifications, for example to update the allowed range of variation.

In a preferred embodiment of the invention, the operator can restrict parameter specifications for example by limiting the maximum number of parameters used in one service or by restricting the allowed value types to numbers only. The operator can also determine its own set of billing parameters, which it offers to service providers. The service providers then select from the set of billing parameters the parameters they want to use in billing for each service.

In a preferred embodiment of the invention, parameters and their values to be used in standard data are also specified in the billing content of

each service. In this way standard data can also be configured specifically for each service/service provider.

In another preferred embodiment of the invention, a common billing content is also determined and used for services with no specified billing content of their own. A common billing content can also be determined specifically for each service provider and/or service type. If a service-type-specific billing content is used, the service type is indicated in a service response either directly or indirectly in order that the correct billing content can be selected when forming a ticket. The same applies to service-provider-specific billing contents as well. The service type can be concluded for example based on the service when the system maintains data that links each service to a service type.

In a preferred embodiment of the invention, also a broader description of a parameter, such as the manner of use or the meaning in billing, can be stored in the billing content.

In another preferred embodiment of the invention, several different identifiers with different value ranges can be stored for one parameter in a billing content. In this embodiment, only one such identifier is shown in the billing data.

If the highest allowed value of the identifiers is equal to the lowest allowed value, in a preferred embodiment of the invention the billing data does not have to contain a value for the parameter, but it is possible to use the value determined in the billing content when forming a ticket.

In the other embodiments of the invention, the predetermined definition rules can differ from what is shown in Figure 2. It is sufficient that the definition rules ensure that the parameters in the billing content are known and that they will be found from the billing data.

Figure 3 shows a flowchart of how a ticket (or a part thereof, if one ticket combines the billing data of several service responses) is formed according to the first preferred embodiment of the invention from the billing data in the service response. It is assumed in the example of Figure 3 that the service provider has transmitted billing data or that the billing data field is not empty. An empty billing data field is preferably not processed at all. The example of Figure 3 does not determine at which stage the tickets should be transmitted to the billing centre. In the first preferred embodiment of the invention, service-specific billing data is transmitted in HTTP headers of a service response. Transmitting billing data as a part of an HTTP header has an advantage that

the data is not transmitted from the gateway, such as the WAP gateway, to the subscriber of the service. Furthermore, an HTTP header is an efficient channel of data transmission between a service provider and an operator.

Since it is not significant for the invention how the billing data is found for example from a log file, the starting point of Figure 3 is that in step 301 the processing of billing data is initiated. For example in the first preferred embodiment of the invention, the WAP gateway picks the billing data from the HTTP header of the service response for the WAP service on the basis of a carriage return. An example of billing data will be described below. The payer is identified first in step 302. The payer can be for example the end user or the service provider, such as a service provider providing a commercial WAP/SMS push service. A payer is identified according to the system used. In the present WAP services, a user is identified based on a phone number received during the set-up of the connection. In the future third-generation mobile systems and in general Internet-based services, the end user can be identified for example from the service log-in data transmitted by the service provider. It is also possible to identify both the payer and the user. After the payer has been identified, the service to which the billing data is related is identified in step 303. The service can be identified either directly by means of an identifier indicating the service name in the HTTP header, or by means of an analysis of a URL (Uniform Resource Locator) address. After the service has been identified, the standard data is retrieved from the billing data and stored (or the part of the standard data not received via some other route/earlier) in a ticket in step 304, and the service billing content is retrieved in step 305. The service billing content is retrieved in the first preferred embodiment of the invention by checking the database table shown in Figure 2 and by picking all the parameters with their specifications that relate to the service to be billed for. In step 306, it is checked whether a billing content was obtained. In other words, it is checked whether a billing content has been specified for the service. If a billing content was obtained (i.e. has been specified), the processing of the first parameter is initiated in step 307 and a corresponding identifier is retrieved from the HTTP header in step 308. If such an identifier was found (step 309), the value given for the identifier is retrieved in step 310. It is thereafter checked in step 311 whether the value is allowed, i.e. whether it is within predetermined limits and of a specified type. If the value was allowed, the parameter name and value are stored in the ticket in step 312, and it is checked in step 313 whether the

parameter was the last parameter of the billing content. If the parameter was not the last one, the next parameter is subjected to processing in step 314, whereafter the process proceeds from step 308 by searching the HTTP header for the corresponding identifier.

If the parameter was the last one (step 313), the processing of the billing data is terminated in step 315.

If the parameter value was not allowed (step 311), a failure report is generated to the system in step 316, and the ticket field in question is left empty. After the failure report has been generated, the process proceeds to step 313 to check whether the processed parameter was the last one in the billing content.

If a parameter identifier was not located (step 309), the process proceeds to the last step 313 to check whether the processed parameter was the last parameter in the billing content. In other words, it is assumed in the first preferred embodiment of the invention that this time the service provider did not want to use this parameter for billing. Such a parameter can be for example an additional discount parameter.

If a billing content was not obtained (step 306), it has not been determined for the service, wherefore the processing of the billing data is terminated in step 315.

In a preferred embodiment of the invention, at least some of the parameter specifications of the standard data are contained in the service billing content. In this embodiment, the billing content must be retrieved (step 306) before step 304, i.e. the retrieval and storage of the standard data.

In a preferred embodiment of the invention, all the parameters, including the parameters of the standard data transmitted in the billing data, such as a service identifier, are determined at least specifically for each service provider. In this embodiment, the processing of the billing data is initiated by first identifying the service provider, whereafter the database table is checked in order to retrieve the service-provider-specific parameters, such as a service identifier and possibly at least some of the standard data. After the service has been identified, the parameters specified for the service are retrieved. This provides the billing content, and the parameter values thereof are retrieved in the manner described above.

The steps of Figure 3 are not in an absolute order of time. Some of the aforementioned steps can take place simultaneously or in another order,

such as steps 304 and 305. Some steps can be skipped, or steps not shown in Figure 3 can be implemented between the steps. Some steps can also be replaced with a corresponding step. For example in an embodiment where the log file only comprises notes containing billing data and where a service-type-specific billing content is used for each service, step 306 can be skipped and step 303 can be replaced with a step of identifying the service type.

Figure 4 shows an xml (eXtendable Mark up Language) ticket CDR according to the first preferred embodiment of the invention, where the WAP service 'Elvis' has been subscribed to from mobile phone number 040555555. The billing content of the service has been specified as shown in Figure 2 and the billing data is indicated as follows in the HTTP header of the service response:

X-up-billing-Info:SN=elvis&PT:67&EC=15

In the first preferred embodiment, the ticket comprises standard data 1 and a part 2 that changes according to the service. The service-specific part 2 is determined according to the billing content defined for the service. In the first preferred embodiment of the invention, the standard data 1 includes a calling party identifier 11, billing data 12 in the HTTP header, a service name 13, and a service price class 14, which is used to distribute different services of the same service provider to different price classes. The standard data is followed by the changing part 2 of the ticket, which is not found in tickets related to a service for which a billing content has not been specified. By means of the definitions shown in Figure 2, the process forming a ticket is able to retrieve from the billing data an identifier and a value corresponding to each parameter specified for the service 'Elvis'.

Even though the above description relates to the use of the billing content for altering a ticket, it can also be applied to other functions related to billing, such as selecting what to store in a log file.

It is obvious to a person skilled in the art that as the technology develops, the basic idea of the invention can be implemented in several manners. The embodiments of the invention described above or the individual characteristics thereof can be combined to provide new embodiments. Thus, the invention and the embodiments thereof are not restricted to the above examples, but they may vary within the scope of the claims.

CLAIMS

1. A method of providing service-specific billing in a telecommunications system, where a system of a network operator transmits services of at least one service provider to a subscriber, and forms call detail records to be used in billing and containing at least one billing parameter and the value thereof, **characterized** in that the method comprises at least the following steps of:

determining rules for defining billing parameters,

determining, by means of the definition rules, a billing content for at least one service, the content containing at least one service-specific billing parameter and indicating how the parameter is found from billing data transmitted during the use of the service, and

storing the billing content in the telecommunications system such that it is available to the system of the network operator.

2. A method according to claim 1, **characterized** in that the method also comprises a step of forming, from the billing data, a call detail record, which contains at least a service-specific part comprising service-specific billing parameters and their values defined in the billing content.

3. A method according to claim 1 or 2, **characterized** in that the method also comprises the steps of

determining at least one set of billing parameters, and

selecting the billing parameters to be used in the billing content from the set of billing parameters.

4. A method according to claim 1, 2 or 3, **characterized** by determining a billing content for one service.

5. A method according to claim 1, 2 or 3, **characterized** by determining a billing content for a service type, and indicating the service type in the billing data.

6. A telecommunications system (J) comprising

a system of a service provider (PJ) for transmitting at least one service to a subscriber and for providing billing data related to the service, and

a system of a network operator (VJ) for transmitting the service from the service provider's system to the subscriber of the service, and for providing a call detail record to be used in billing of the subscriber by means of the billing data, and

a memory (M) for storing different specifications,

characterized in that

the system of the network operator (VJ) comprises an interface (I) for storing a billing content (LS) in the memory (M) for the service, the billing content determining at least one service-specific billing parameter of the billing data according to the predetermined definition rules, such that the billing parameter is found from the billing data transmitted during the use of the service.

7. A system according to claim 6, **characterized** in that the system of the network operator (VJ) is arranged to utilize the specifications of the billing content in forming a call detail record from the billing data related to the service.

8. A system according to claim 6, **characterized** in that the system of the network operator (VJ) is arranged to form a call detail record (CDR) for the service from standard data (1) containing the same parameters for all the services, and from service-specific data (2) according to the billing content defined for the service.

9. A system according to claim 6, 7 or 8, **characterized** in that the interface (I) is also arranged to alter the specifications of the billing content.

10. A system according to claim 6, 7, 8 or 9, **characterized** in that the interface (I) is also arranged to check, in connection with said storage, whether the parameter specifications comply with the definition rules.

11. A system according to claim 6, 7, 8, 9 or 10, **characterized** in that the system (J) is based on a GPRS system.

12. A system according to claim 6, 7, 8, 9 or 10, **characterized** in that the system (J) is based on a UMTS.

13. A network node (CG) in a telecommunications system where a system of a network operator transmits services of at least one service provider to a subscriber and provides call detail records used in billing, and where the service provider transmits billing data in connection with a service,

characterized in that

the network node comprises configuring means (I) for specifying parameters contained in the service billing data according to predetermined definition rules, such that the system of the network operator can use the specifications in forming a call detail record related to the service.

14. A network node according to claim 13, **characterized** in

that the configuring means (I) are arranged to alter the parameter specifications.

15. A network node according to claim 13 or 14, **characterized** in that the network node also comprises processing means (P) for forming a call detail record from the billing data related to the service, such that at least a part of the call detail record is formed according to the parameter specifications for the service.

16. A network node (CG) in a telecommunications system, where a system of a network operator transmits services of at least one service provider to a subscriber, and where the service provider transmits billing data in connection with a service, the network node comprising processing means (P) for forming a call detail record from the billing data related to the service,

characterized in that

the processing means (P) are arranged to determine a billing content specified for the service according to predetermined definition rules in the system of the network operator, the billing content containing at least service-specific billing parameters and indicating how the parameters can be found from the billing data, the processing means being also arranged to form a call detail record in such a manner that at least a part of the call detail record complies with the billing content.

17. A network node (CG) according to any one of claims 13 to 16, **characterized** in that the means (I, P) are implemented by software routines.

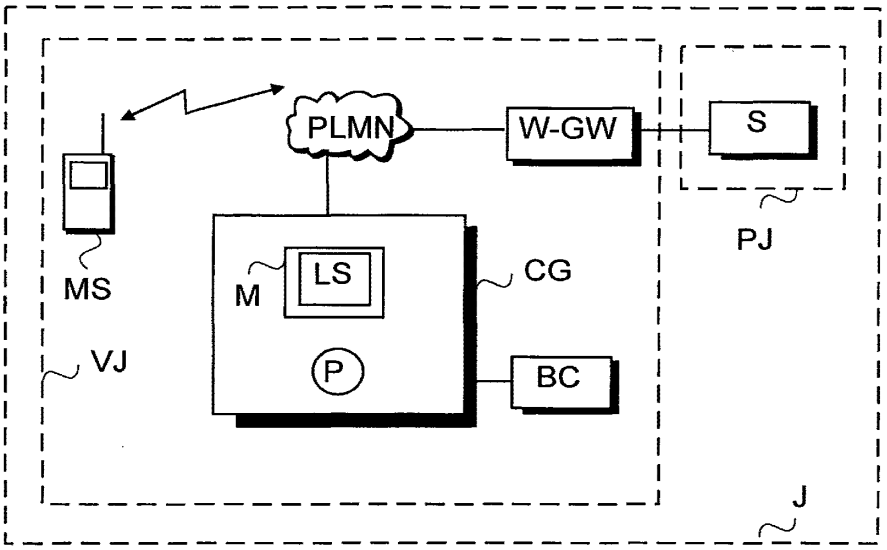


FIG.1

P	ID	N	S1	V	S2	SV	BV
Elvis	PT	price_today	:	number	&	0	500
Elvis	EC	extra_cutback	=	number	&	0	250
Iiris	SP	single_payment	-	number	*	250	250

FIG.2

CDR

<user_msisdn>040555555</user_msisdn>

11 <header>SN=elvis&RC=99&PT:67&EC=15</header>

12 <service_name>ELVIS</service_name>

13 <rate_category>99</rate_category>

1

<psd>
<price_today>67</price_today>
<extra_cutback>15</extra_cutback>
</psd>

2

FIG.4

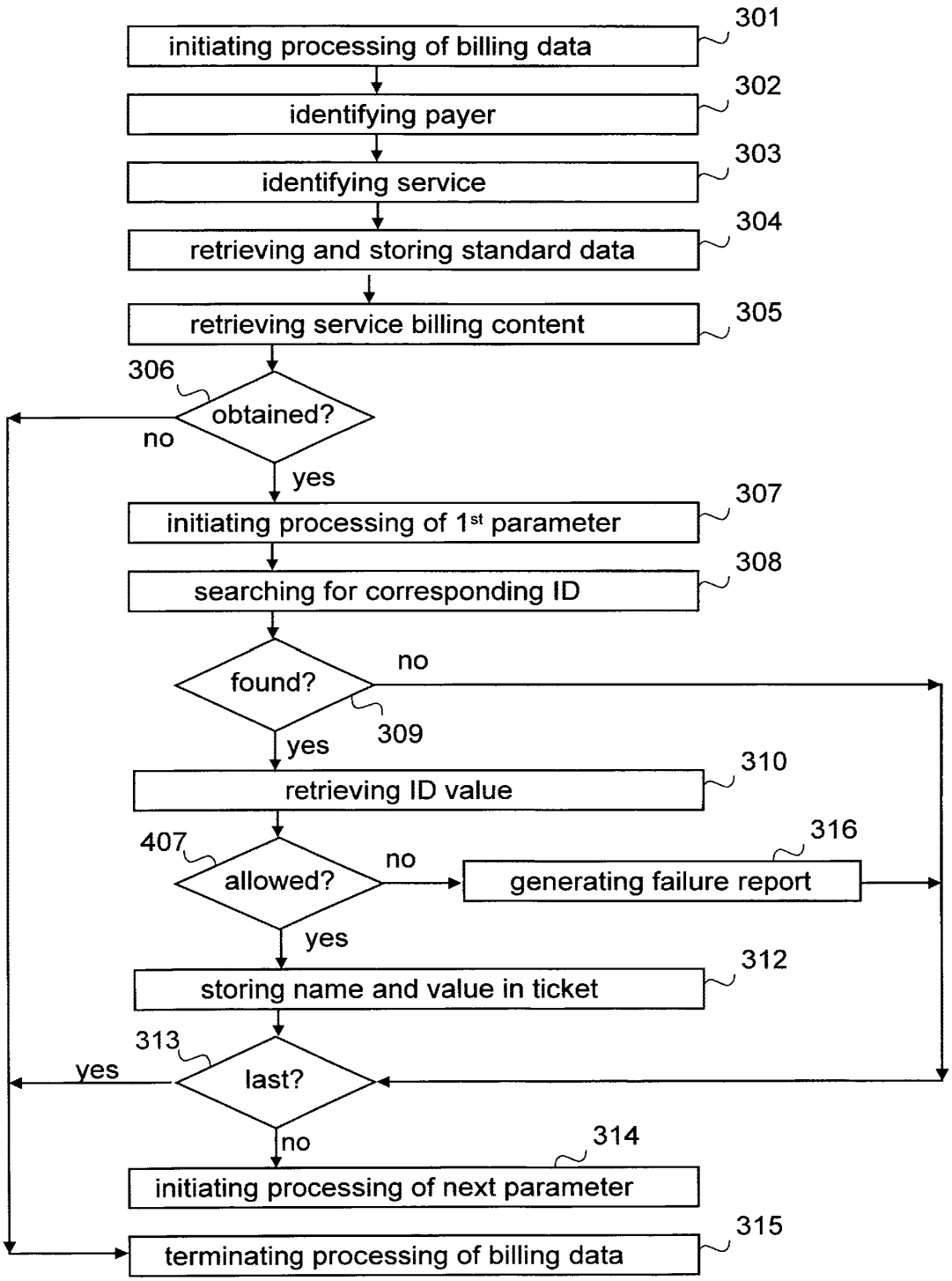

initiating processing of billing data
301
identifying payer
302
identifying service
303
retrieving and storing standard data
304
retrieving service billing content
305
306
obtained?
no
yes
initiating processing of 1st parameter
307
searching for corresponding ID
308
found?
no
309
yes
retrieving ID value
310
407
allowed?
no
316
generating failure report
yes
storing name and value in ticket
312
313
yes
last?
no
314
initiating processing of next parameter
315
terminating processing of billing data

FIG.3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 02/00128

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38, H04M 15/00
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)

IPC7: H04Q

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

SE,DK,FI,NO classes as above

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5982864 A (JAGADISH ET AL), 9 November 1999 (09.11.99), column 3, line 48 - column 4, line 18, figure 1b, column 7, line 28 - line 32, column 5, line 19 - line 22	1-9,11-17
A	abstract	10
	--	
A	US 6047051 A (GINZBOORG ET AL), 2 April 2000 (02.04.00), abstract	1-17
	--	
P,A	WO 0191003 A2 (ZTANGO, INC), 29 November 2001 (29.11.01), claim 3, abstract	1-17
	--	

[X] Further documents are listed in the continuation of Box C. [X] 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	Date of mailing of the international search report
23 May 2002	06 -06- 2002
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Malin Söderman /js Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 02/00128

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	WO 0133456 A2 (AP ENGINES, INC), 10 May 2001 (10.05.01), page 2, line 15 - line 21, abstract ---	1-17
A	WO 0065812 A1 (TELIA AB), 2 November 2000 (02.11.00), page 19, line 6 - line 15 --- --------	1-17

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT
Information on patent family members

01/05/02

International application No.
PCT/FI 02/00128

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5982864 A	09/11/99	NONE	
US 6047051 A	02/04/00	AU 730689 B	15/03/01
		AU 4871297 A	03/06/98
		BR 9713014 A	25/01/00
		EP 1012760 A	28/06/00
		FI 964524 A	12/05/98
		NZ 335701 A	27/10/00
		WO 9821676 A	22/05/98
WO 0191003 A2	29/11/01	AU 6333001 A	03/12/01
		US 2002029197 A	07/03/02
WO 0133456 A2	10/05/01	AU 1346901 A	14/05/01
WO 0065812 A1	02/11/00	AU 1191900 A	01/05/00
		EP 1117340 A	25/07/01
		EP 1180297 A	20/02/02
		NO 20015022 A	18/12/01
		SE 9901509 A	28/10/00

Form PCT/ISA/210 (patent family annex) (July 1998)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2011 (06.01.2011)

PCT

(10) International Publication Number
WO 2011/002450 A1

(51) International Patent Classification:
H04M 15/00 (2006.01) *H04W 4/24* (2009.01)

(21) International Application Number:
PCT/US2009/049255

(22) International Filing Date:
30 June 2009 (30.06.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicants *(for all designated States except US)*: **ALCATEL-LUCENT USA INC** [US/US]; 600-700 Mountain Avenue, Murray Hill, New Jersey 07974-0636 (US). **ALCATEL-LUCENT SHANGHAI BELL COMPANY** [CN/CN]; 388#, Ningqiao Road, Pudong Jinqiao, Shanghai 201206 (CN).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **CAI, Yigang** [CN/US]; 23643 Royal Worlington Drive, Naperville, Illinois 60564 (US). **LI, Xiangyang** [CN/CN]; Bo Ya Xi Yuan 13-1-502# Nong Da Nan Lu, Hai Dian District, Beijing 100094 (CN).

(74) Agent: **BORNSEN, Brett**; Alcatel-Lucent Usa Inc, Docket Administrator - Room 2F-192, 600-700 Mountain Avenue, Murray Hill, New Jersey 07974-0636 (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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

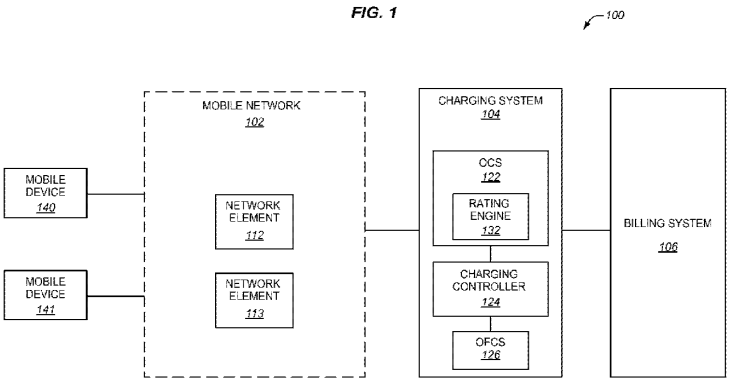
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS,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

Published:

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

(54) **Title**: FRONT-END CHARGING SYSTEM THAT GENERATES CHARGING DATA PER ENTITY HAVING A REVENUE SHARE

FIG. 1



(57) **Abstract**: Charging systems and methods are disclosed for determining the share of call revenue for multiple entities. One embodiment comprises a charging controller that is coupled to a mobile network and an online charging system. The charging controller receives charging data for a call in the mobile network, and processes the charging data and charging rules to identify entities that have a share in revenue for the call. The charging controller generates a charging request message indicating the entities having a revenue share in the call, and transmits the charging request message to the online charging system to cause the online charging system to determine the revenue share for each of the entities.

WO 2011/002450 A1

FRONT-END CHARGING SYSTEM THAT GENERATES CHARGING DATA PER ENTITY HAVING A REVENUE SHARE

Background

1. Field of the Invention

The invention is related to the field of communication networks and, in particular, to charging and billing in communication networks.

2. Statement of the Problem

When a phone call is placed over a communication network, there may be multiple entities that share in the revenue received for the call. For instance, the network operator that actually operates and maintains the network over which the call is placed shares in the revenue. If the call extends to a foreign communication network, such as for an international call, then the network operator of the foreign communication network shares in the revenue for the call. If a call extends to a roaming mobile user, then the network operator of the mobile network in which the user is roaming shares in the revenue. The process of determining which entities share in the revenue of a call is sometimes referred to as mediation.

In traditional communication networks, charging functions for calls are performed by network components, such as switches. Switches collect charging data for the calls, and generate Charging Detail Records (CDR) that include the charging data. Switches all over the entire network forward the CDRs to a billing system in service provider's IT system (often referred to as a back-end or back-office billing system). The back-office billing system stores information that may be used for the mediation process. For example, the billing system stores agreements that a network operator may have with a foreign network operator for international calls, stores agreements that a network operator may have with mobile networks for roaming scenarios, etc. The billing system also performs settlement processes to invoice customers for the telephone services, and to provide vouchers or credits to other entities.

In more recent charging architectures, postpaid charging is implemented through an Offline Charging System (OFCS) and an associated billing system. Similarly, prepaid charging is implemented through an Online Charging System (OCS) and an associated billing system. To provide offline and online charging, the OCS and the billing systems

each maintain their own rating engine. Also, the billing systems each maintain profiles for the subscribers, profiles for the wholesale customers, and profiles for other network operators having contractual agreements. The overlap of the rating engines and the profiles wastes significant resource in the network. Operational inefficiencies and technical overhead for maintaining two separate charging systems may lead to the drawback in marketing and business activities for a network operator. Presently, the network operators are subject to great pressures to reduce the operational costs.

Summary

Embodiments described herein are able to manage the flow of revenue to the appropriate entities for a call using a converged charging system. The converged charging system centralizes prepaid charging, postpaid charging, interconnect charging, wholesale charging, content charging, roaming charging, etc. Thus, revenues for a call may be divided among multiple entities based on the applicable charging types. This will significantly reduce the work in the back office, and create near real-time billing. The converged charging system also enables the rating or billing-related activity to share a common rating engine and a common account balance management function, which reduces the cost for system deployment, operation, and maintenance.

One embodiment comprises a charging controller that is coupled to a mobile network and an online charging system. The charging controller is operable to receive charging data for a call in the mobile network, and to process the charging data for the call and charging rules to identify entities that have a share in revenue for the call. The charging controller is further operable to generate a charging request message indicating the entities having a revenue share in the call, and to transmit the charging request message to the online charging system to cause the online charging system to determine the revenue share for each of the entities.

In another embodiment, the online charging system is operable to receive the charging request message from the charging controller, and to identify a profile for each of the entities having a revenue share. The online charging system is further operable to determine a revenue share amount for each of the entities based on their profile and a rating, to generate charging records indicating the revenue share amount for each of the entities, and to transmit the charging records to the charging controller.

In yet another embodiment, the charging controller is further operable to receive the charging records, to correlate the charging records to generate a consolidated charging record that indicates the revenue share amount for each of the entities, and to transmit the consolidated charging record to a billing system.

Other exemplary embodiments may be described below.

Description of the Drawings

Some embodiments of the present invention are now described, by way of example only, and with reference to the accompanying drawings. The same reference number represents the same element or the same type of element on all drawings.

FIG. 1 illustrates a communication network in an exemplary embodiment.

FIG. 2 is a flow chart illustrating a method of charging for a call by generating charging data for each entity having a revenue share in an exemplary embodiment.

FIG. 3 is a flow chart illustrating a method of determining the revenue share for multiple entities in an exemplary embodiment.

FIG. 4 is a flow chart illustrating a method of correlating charging records in an exemplary embodiment.

FIG. 5 illustrates another communication network in an exemplary embodiment.

FIG. 6 illustrates how the revenue for a call is divided among entities in an exemplary embodiment.

FIG. 7 is a message diagram illustrating how revenue for a call is divided in an exemplary embodiment.

Description of Embodiments

The figures and the following description illustrate specific exemplary embodiments of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements that, although not explicitly described or shown herein, embody the principles of the invention and are included within the scope of the invention. Furthermore, any examples described herein are intended to aid in understanding the principles of the invention, and are to be construed as being without limitation to such specifically recited examples and conditions. As a result, the invention is not limited to the specific embodiments or examples described below, but by the claims and their equivalents.

FIG. 1 illustrates a communication network 100 in an exemplary embodiment. Communication network 100 includes a mobile network 102, a charging system 104, and a billing system 106. Mobile network 102 may comprise a circuit-based network, such as a CDMA network or a GSM network, may comprise a packet-based network, such as an IP Multimedia Subsystem (IMS) network, or a mix of the two. Mobile network 102 is able to provide service to mobile devices 140-141 to place voice calls, to initiate data sessions, to send or receive text messages or multimedia messages, etc. Mobile network 102 includes a plurality of network elements 112-113 that are operable to serve a session/call or provide a service for a session/call within mobile network 102. For example, network element 112 may comprise a Serving-Call Session Control Function (S-CSCF) while network element 113 may comprise an application server (AS) in an IMS network. Alternatively, network element 112 may comprise a Mobile Switching Center (MSC) while network element 113 may comprise an SGSN of a UMTS network.

Charging system 104 comprises any system, server, or function operable to provide online and/or offline charging for sessions/calls in mobile network 102. For the online/offline charging, charging system 104 is able to generate consolidated charging records for sessions/calls within mobile network 102, and send the CDRs to billing system 106. Charging system 104 includes an online charging system (OCS) 122, a charging controller 124, and an offline charging system (OFCS) 126. OCS 122 includes a common rating engine 132 that may be shared by OCS 122 and OFCS 126, and may include other functions that are not shown. OFCS 126 may also include a variety of functions that are not shown for the sake of brevity, such as a Charging Data Function (CDF)/Charging Gateway Function (CGF) as defined by the 3GPP in Release 6, or a Charging Collector Function (CCF) as defined by the 3GPP in Release 5.

Billing system 106 comprises any system, server, or function operable to receive a consolidated charging record for a session/call, and to invoice one or more customers for the session/call based on the consolidated CDR or issue a voucher or credit.

For a call, there may be a variety of different types of charging involved. Some common types of charging are as follows. One type of charging is referred to as retail charging. Retail charging occurs between a mobile network operator (MNO) or a mobile virtual network operator (MVNO) and an end user. Thus, retail charging defines how end users pay for services provided by the MNO (or MVNO).

Another type of charging is referred to as wholesale (or MVNO) charging. Wholesale charging occurs between an MVNO and an MNO. A wholesale customer purchases mobile products and services from an MNO for resale. Wholesale charging defines how the MVNO pays for services provided by the MNO.

Another type of charging is referred to as content charging. Content charging occurs between a content provider and an MNO (or MVNO). The content provider supplies some content/service to end users via the MNO/MVNO network. Thus, content charging defines how the MNO/MVNO pays for the content supplied by the content provider.

Another type of charging is referred to as interconnect charging. Interconnect charging occurs between an MNO and another network operator. When a call is originated in the MNO's network but is terminated in network of the other operator (or vice-versa), interconnect charging defines how the MNO pays for services provided by the other network operator.

Another type of charging is referred to as roaming charging. Roaming charging occurs between an MNO and other MNO that is serving a roaming user. When an end user of one MNO (visiting MNO) is roaming in the network of another MNO (visited MNO), roaming charging defines how the visiting MNO pays for services provided by the visited MNO.

There may be other types of charging that apply to the description provided below. One common thread for each of these charging types is that multiple entities will share in the revenue of a call. Thus, the revenue has to be divided at some point and allocated appropriately to each of the entities. In a traditional charging architecture, a charging system generates CDRs that include charging data for a call. A back-office billing system then processes the charging data from the CDRs to divide the revenue for the call to entities that have a share. Thus, the revenue is divided in back-office systems instead of in the actual charging system. In the embodiments described below, a new charging controller 124 is implemented in the charging architecture to divide the revenue. Thus, revenue sharing entities for a call are identified in charging system 104 instead of in back office systems.

Assume for this embodiment that mobile device 140 is involved in a call over mobile network 102. One or both of network elements 112-113 may provide a service for the call, and generate charging data for providing the service. Those skilled in the art will appreciate that other mobile networks (not shown) and other fixed networks (not shown)

may also be involved in the call. Network elements 112-113 then transmit the charging data to charging system 104. For example, if prepaid charging applies for the call, then network elements 112-113 may transmit a Diameter Ro Credit Control Request (CCR) to charging system 104. If postpaid charging applies for the call, then network elements 112-113 may transmit a Diameter Rf Accounting Request (ACR) to charging system 104. Charging controller 124 manages charging for the call as is illustrated in FIG. 2.

FIG. 2 is a flow chart illustrating a method 200 of charging for a call by generating charging data for each entity having a revenue share in an exemplary embodiment. The steps of method 200 will be described with reference to communication network 100 in FIG. 1, but those skilled in the art will appreciate that method 200 may be performed in other networks and systems. The steps of the flow charts described herein are not all inclusive and may include other steps not shown. The steps may also be performed in an alternative order.

In step 202, charging controller 124 receives charging data for the call in mobile network 102. The charging data may be received in a charging request message from mobile network 102, such as a Diameter Ro CCR or a Diameter Rf ACR. Alternatively, the charging data may be received in a CDR from OCS 122 or OFCS 126. In step 204, charging controller 124 processes the charging data for the call and charging rules to identify entities that have a share in revenue for the call. Charging controller 124 stores charging rules that define conditions for different types of charging. For example, the charging rules may include retail rules defining conditions for retail charging. The charging rules may include wholesale rules defining conditions for wholesale charging. The charging rules may include interconnect rules defining conditions for interconnect charging. The charging rules may include content rules defining conditions for content charging. The charging rules may include roaming rules defining conditions for roaming charging.

As an example, charging controller 124 may process the calling party number and wholesale rules to determine that wholesale charging applies, and to determine the identity of the wholesale entity. Charging controller 124 may also process the called party number and interconnect rules to determine that interconnect charging applies, and to determine an identity of the network operator entity providing the interconnect service. Based on the charging data, charging controller 124 is able to generate a list of entities that have a share in the revenue for the call.

In step 206, charging controller 124 generates a charging request message indicating the entities having a revenue share in the call. For example, charging controller 124 may generate a Diameter Ro CCR, and insert the identities of the revenue sharing entities in the CCR. In step 208, charging controller 124 transmits the charging request message to OCS 122. Charging controller 124 may transmit a separate charging request message for each of the identified revenue sharing entities, or may transmit a single charging request message for all of the identified revenue sharing entities. Based on the data included in the charging request message, OCS 122 is able to determine the revenue share for each of the entities, which is further illustrated in FIG. 3.

FIG. 3 is a flow chart illustrating a method 300 of determining the revenue share for multiple entities in an exemplary embodiment. The steps of method 300 will be described with reference to communication network 100 in FIG. 1, but those skilled in the art will appreciate that method 300 may be performed in other networks and systems. In step 302, OCS 122 receives the charging request message from charging controller 124. In step 304, OCS 122 identifies a profile for each of the entities having a revenue share as indicated in the charging request message. OCS 122 may maintain a database of profiles for each entity. For example, OCS 122 may maintain a profile for mobile device 140 that indicates a service plan subscription of its end user. OCS 122 may maintain a profile of other MNO's having a roaming agreement with the operator of mobile network 102. OCS 122 may maintain a profile of fixed networks having an interconnect agreement with the operator of mobile network 102. OCS 122 may also maintain a profile of content providers having an agreement to supply content to end users of mobile network 102. Alternatively, the profiles may be maintained on an external database that is accessible to OCS 122.

In step 306, OCS 122 determines a revenue share amount for each of the entities based on their profile and a rating provided by rating engine 132. For example, assume that overall charging for a call is $30. Based on the profiles and the ratings, OCS 122 may determine that entity 1 shares $10 of the revenue, entity 2 shares $10 of the revenue, and entity 3 shares $10 of the revenue. In step 308, OCS 122 generates charging records, such as a CDR, indicating the revenue share amount for each of the entities. For example, OCS 122 may generate an individual charging record for each of the entities indicating the amount the entity is owed or the amount payable to the entity. OCS 122 then transmits the charging records to charging controller 124 in step 310.

The charging records generated by OCS 122 include a new set of data for each revenue sharing entity. The new set of data includes an entity ID, which may be an end user subscriber ID, an MNO ID, an MVNO ID, a content provider ID, another network operator ID, etc. The new set of data also includes a charging type, such as retail charging, wholesale charging, content charging, interconnect charging, roaming charging, etc. The new set of data also includes a revenue share amount. The revenue share amount indicates the monetary amount of service usage owed by each entity or payable to each entity. The revenue share amount may be an accumulated amount per payment billing cycle, or a special call charge amount. For retailing charging, the revenue share amount represents the service units the end user pays to the MVNO/MNO. For wholesale charging, the revenue share amount represents the service units the MVNO pays to the MNO for network/service usage. For content charging, the revenue share amount represents the service units the MNO pays for the content supplied by the content provider. For interconnect charging, the revenue share amount represents the service units the MNO pays for the other network operator that interconnects the call. For roaming charging, the revenue share amount represents the service units the visiting MNO pays to the visited MNO for a local user to roam in a foreign network.

FIG. 4 is a flow chart illustrating a method 400 of correlating charging records in an exemplary embodiment. The steps of method 400 will be described with reference to communication network 100 in FIG. 1, but those skilled in the art will appreciate that method 400 may be performed in other networks and systems. In step 402, charging controller 124 receives the charging records for the entities having a revenue share. In step 404, charging controller 124 correlates the charging records to generate a consolidated charging record that indicates the revenue share amount for each of the entities. The consolidated charging record also includes the new set of data for each revenue sharing entity, such as entity ID, charging type, and revenue share amount. In step 406, charging controller 124 transmits the consolidated CDR to billing system 106.

Billing system 106 may then perform a settlement process based on the data included in the consolidated charging record to generate billing invoices and generate vouchers or credits for each revenue sharing entity. Because charging controller 124 has already divided the revenue for the call in the consolidated charging record, billing system 106 does not need to perform this process. Billing system 106 only needs to issue the

vouchers to the proper entities for the revenue share amounts indicated in the consolidated charging record.

Examples

FIG. 5 illustrates another communication network 500 in an exemplary embodiment. Communication network 500 includes a mobile network 502, a charging system 504, and a billing system 506. Mobile network 502 is able to provide service to mobile device 540 to place voice calls, to initiate data sessions, to send or receive text messages or multimedia messages, etc. Charging system 504 includes an online charging system (OCS) 522, a charging controller 524, and an offline charging system (OFCS) 526.

OCS 522 handles online charging (or prepaid) for calls in mobile network 502. OCS 522 includes an online charging function (OCF) 530, an account balance management function (ABMF) 531, a rating engine 532, a profile database 533, and a tariff database 534. OCS 522 is enhanced to perform multiple-event charging based on one request event (i.e., a CCR). OCS 522 will use the different subscription IDs of the request to access each account profile separately, so OCS 522 will rate the call charge for each entity. After charging is finished, OCS 522 will generate a CDR indicating each entity's call cost, such as for retail charging, wholesale charging, content charging, interconnect charging, roaming charging, etc.

OCF 530 comprises any system, server, or function operable to manage online charging in OCS 522 by accessing ABMF 531 and rating engine 532, exchanging charging messages with network elements in mobile network 502, and performing other functions. ABMF 531 comprises any system, server, or function operable to maintain accounts for users, and more particularly to maintain an amount of service units in the accounts of the users. Rating engine 532 comprises any system, server, or function operable to determine the cost of service usage according to a tariff defined by the network operator. Rating engine 532 will perform tariff plan determination by accessing the tariff index of each entity, such as a unit determination, a price determination, a tariff determination, a counter, etc.

Rating engine 532 will not only hold the retail tariff plan for end user's service usage, but also holds the tariff plan for MNO's partnership, such as the price plan with MVNO, content provider, or other operators based on the service level agreement. OCF

530 will use the price plan index in each retail/partner's account profile to access the tariff to determine each entity's call charge.

Profile database 533 comprises any database or data structure operable to store profiles for retail customers, wholesale customers, content providers, interconnect operators, roaming operators, etc. Profile database 533 may alternatively store addresses for the profiles in order to remotely access the profiles. Tariff database 534 comprises any database or data structure operable to store a tariff plan or tariff plan index. Rating engine 532 is able to perform a tariff plan determination by accessing the tariff plan data of an entity, such as a unit determination, a price determination, a tariff determination, a counter, etc. OCF 530 will use the price plan index in each retail/partner's account profile to access the rating tariff index to determine each entity's call charge.

OFCS 526 handles offline charging (or postpaid) for calls in mobile network 502. OFCS 526 may include a Charging Data Function (CDF), a Charging Gateway Function (CGF), or other charging elements which are not specifically shown in FIG. 5.

Charging controller 524 comprises any system, server, or function operable to control overall charging for calls in mobile network 502. Charging controller 524 processes charging rules to determine which entities share in revenue for calls in mobile network 502. Charging controller 524 then generates a separate Diameter Ro CCR for each of the revenue sharing entities, and transmits CCRs to OCS 522 to determine the cost or the amount payable to the entity.

Assume for example that an end user of mobile device 540 subscribes to a service offered by OnStar Corporation, which is an in-vehicle service providing in-vehicle security, hands free calling, turn-by-turn navigation, remote diagnostics, etc. OnStar may be considered an MVNO in this example. OnStar leases its mobile services from mobile network 502, which is operated by Verizon Wireless (or some other mobile service provider). Verizon Wireless may thus be considered the MNO for the end user in this example. Assume further that the end user of mobile device 540 places a call (through the OnStar service) to another end user. The called end user subscribes to a service offered by another service provider, such as Vodafone in England. Vodafone may thus be considered the MNO for the called end user in this example.

Assume further that the overall charge for the call from the calling end user to the called end user is $30, and that the calling end user is responsible for payment for the call. FIG. 6 illustrates how the revenue for the call is divided among the entities in an exemplary

embodiment. According to the retail agreement between the calling end user 602 and OnStar (MNVO 604), calling end user 602 pays $30 to MVNO 604 for the call. This is an example of retail charging. MVNO 402 (OnStar) leases its mobile services from Verizon Wireless (MNO 606). According to the wholesale agreement between MVNO 604 and MNO 606, MVNO 604 pays $20 to MNO 606 for the mobile services. This is an example of wholesale charging. To connect the call to called end user 610, MNO 606 needs to connect to a foreign network operated by Vodafone (MNO 608). According to the interconnect agreement between MNO 606 and MNO 608, MNO 606 pays $10 to MNO 608 for the interconnect fees. This is an example of interconnect charging. Thus, the revenue for the call is divided between MVNO 604 (OnStar), MNO 606 (Verizon Wireless), and MNO 608 (Vodafone). In the embodiments provided herein, the dividing of the revenue is performed in the charging system instead of in back office systems. FIG. 7 further illustrates how this is done.

FIG. 7 is a message diagram illustrating how revenue for a call is divided in an exemplary embodiment. Mobile network 502 transmits a Diameter Ro CCR to OCS 522. The CCR includes charging data for the call in mobile network 502, such as a calling party number, a called party number, time stamps, etc. Although a Diameter Ro CCR is received in this example, other charging messages may be received in other examples, such as INAP messages. OCS 522 processes a subscription ID (subscription ID = MSISDN of the end user of mobile device 540) to access to the account profile for the end user. OCS 522 then calculates the overall charge for the call, which is $30 that is owed from the end user to OnStar. OCS 522 also generates a rated CDR (CDR1) indicating the call charge of $30, and sends the rated CDR to a mediation device (such as CDF or CGF) in OFCS 526. OFCS 526 then sends the rated CDR to charging controller (CC) 524. Those skilled in the art will appreciate that OCS 522 may send the rated CDR to charging controller (CC) 524 directly.

In response to receiving the rated CDR having charging data for the call, charging controller 524 processes charging rules to identify which entities are entitled to share in the revenue for the call. The following illustrates some exemplary rules for the different types of charging that may apply to the call.

Retail Rules:

Rule 1: CDR is not rated AND calling party number belongs to local operator AND call direction = originated call THEN:

Retail chargeable entity = calling party;

Trigger a Diameter Ro CCR [subscription ID = MSISDN of calling party, subscription type = retail charging,…] to OCS to determine the call cost for the calling party.

Rule 2: CDR is not rated AND called party number belongs to local operator AND call direction = terminate call AND subscriber location in home zone THEN:

Terminated local call is free to hear/accept;

Set the CDR as free call.

Rule 3: CDR is not rated AND called party number belongs to local operator AND call direction = terminate call AND subscriber location in roaming zone THEN:

Retail chargeable entity = called party

Trigger a Diameter Ro request [Subscription ID = MSISDN of called party, Subscription Type = retail charging,…] to OCS to determine the call cost for the called party.

Wholesale Rules:

Rule 1: Calling party number belongs to local operator AND call direction = originated call AND the prefix number of the calling party number is an MVNO call number THEN:

Map out the MVNO ID based on prefix number of the calling party number;

Wholesale chargeable entity = MVNO;

Trigger a Diameter Ro CCR [Subscription ID = MVNO ID, Subscription Type = wholesale charging,…] to OCS to determine the call cost for the MVNO.

Rule 2: Called party number belongs to local operator AND call direction = terminated call AND the prefix number of the called party number is an MVNO call number AND subscriber location in roaming zone THEN:

Map out the MVNO ID based on prefix number of the called party number;

Wholesale chargeable entity = MVNO;

Trigger a Diameter Ro CCR [Subscription ID = MVNO ID, Subscription Type =wholesale charging,…] to OCS to determine the call cost for the MVNO.

Interconnect Rules:

Rule 1: Calling party number belongs to the local operator AND called party number doesn't belong to local operator AND call direction = originated call THEN:

Map out the Interconnect Partner ID based on prefix number of the called party number;

Interconnect Partner entity = Interconnect Operator ID;

Trigger a Diameter Ro CCR [Subscription ID = Interconnect Operator ID, Subscription Type = interconnect charging,…] to OCS to determine the call cost for the interconnect partner.

Roaming Rules:

Rule 1: Calling party number doesn't belong to the local operator AND calling party's visited PLMN belongs to local operator THEN:

Map out the Inbound Partner ID based on prefix number of the calling party number;

Inbound Partner entity = Inbound Partner ID;

Trigger a Diameter Ro CCR [Subscription ID = Inbound Partner ID, subscription type = inbound roaming charging,…] to OCS to determine the call cost for inbound roaming partner.

Content Rules:

Rule 1: Calling party number belongs to the local operator AND (Service ID = *xxx* OR Merchant ID = *yyy* OR Content Provider = *zzz*) THEN:

Map out the Content Provider ID based on Service ID, Content ID, or Merchant ID;

Trigger a Diameter Ro CCR [Subscription ID = Content Provider ID, subscription type = content revenue sharing charging,…] to OCS to determine the call cost for the content provider.

In this example, charging controller 524 processes the wholesale rules and the prefix number of mobile device 540 that is included in the CDR. Based on the wholesale rules, charging controller 524 determines that this is an MVNO number of Verizon Wireless. Thus, charging controller 524 maps out the MVNO ID based on IMSI prefix, wherein the

MVNO ID is the identifier for OnStar. Charging controller 524 then transmits a Diameter Ro CCR (with subscription ID = MVNO ID) to OCS 522.

OCS 522 uses the MVNO ID in the CCR to access the OnStar account profile in profile database 533. OCS 522 then determines the call charge for the MVNO, which is the amount OnStar pays to Verizon Wireless ($20). OCS 522 then generates the rated CDR (CDR2) that includes the wholesale charge amount of $20, and transmits the rated CDR to OFCS 526.

Charging controller 524 also processes the interconnect rules and the prefix number of called party number in the CDR. Based on the interconnect rules, charging controller 524 determines that the call is an interconnect call. Charging controller 524 maps out the MNO ID based on called party number prefix, wherein in MNO ID is the identifier for Vodafone. Charging controller 524 then transmits a Diameter Ro CCR (with subscription ID = MNO ID) to OCS 522.

OCS 522 uses the MNO ID in the CCR to access the Vodafone account profile in profile database 533. OCS 522 then determines the call charge for the MNO, which is the amount Verizon Wireless pays to Vodafone ($10). OCS 522 then generates the rated CDR (CDR3) that includes the interconnect charge amount of $10, and transmits the rated CDR to OFCS 526.

OFCS 526 correlates the three rated CDRs to generate a consolidated CDR that indicates the revenue share amount for each of the entities. In this example, the consolidated CDR indicates the retail charge of $30, the wholesale charge of $20, and the interconnect charge of $10. The consolidated CDR includes the new set of data for each revenue sharing entity, such as entity ID, charging type, and revenue share amount. OFCS 526 then transmits the consolidated CDR to billing system 506. Although OFCS 526 is shown as correlating the CDRs in this embodiment, charging controller 524 may correlate the CDRs in other embodiments.

Billing system 506 may then perform a settlement process based on the data included in the consolidated CDR to generate billing invoices and generate vouchers or credits for each revenue sharing entity. In the above example, Verizon Wireless will receive a $20 voucher from OnStar, and Vodafone will receive a $10 voucher from Verizon Wireless for this call. Because charging controller 524 has already divided the revenue for the call in the consolidated CDR, billing system 506 does not need to perform this process.

Billing system 506 only needs to issue the vouchers to the proper entities for the revenue share amounts indicated in the consolidated CDR.

Any of the various elements shown in the figures or described herein may be implemented as hardware, software, firmware, or some combination of these. For example, an element may be implemented as dedicated hardware. Dedicated hardware elements may be referred to as "processors", "controllers", or some similar terminology. When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared. Moreover, explicit use of the term "processor" or "controller" should not be construed to refer exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, a network processor, application specific integrated circuit (ASIC) or other circuitry, field programmable gate array (FPGA), read only memory (ROM) for storing software, random access memory (RAM), non volatile storage, logic, or some other physical hardware component or module.

Also, an element may be implemented as instructions executable by a processor or a computer to perform the functions of the element. Some examples of instructions are software, program code, and firmware. The instructions are operational when executed by the processor to direct the processor to perform the functions of the element. The instructions may be stored on storage devices that are readable by the processor. Some examples of the storage devices are digital or solid-state memories, magnetic storage media such as a magnetic disks and magnetic tapes, hard drives, or optically readable digital data storage media.

Although specific embodiments were described herein, the scope of the invention is not limited to those specific embodiments. The scope of the invention is defined by the following claims and any equivalents thereof.

CLAIMS:

We claim:

1. A charging system comprising:

a charging controller coupled to a mobile network and an online charging system, the charging controller operable to receive charging data for a call in the mobile network, to process the charging data for the call and charging rules to identify entities that have a share in revenue for the call, to generate a charging request message indicating the entities having a revenue share in the call, and to transmit the charging request message to the online charging system to cause the online charging system to determine the revenue share for each of the entities.

2. The charging system of claim 1 further comprising:

the online charging system operable to receive the charging request message from the charging controller, to identify a profile for each of the entities having a revenue share, to determine a revenue share amount for each of the entities based on their profile and a rating, to generate charging records indicating the revenue share amount for each of the entities, and to transmit the charging records to the charging controller.

3. The charging system of claim 2 wherein the charging records each include an entity ID, a charging type, and the revenue share amount.

4. The charging system of claim 3 wherein the revenue share amount indicates a monetary amount owed to another entity.

5. The charging system of claim 2 wherein:

the charging controller is further operable to receive the charging records, to correlate the charging records to generate a consolidated charging record that indicates the revenue share amount for each of the entities, and to transmit the consolidated charging record to a billing system.

6. The charging system of claim 1 wherein the charging rules include retail rules defining conditions for retail charging.

7. The charging system of claim 1 wherein the charging rules include wholesale rules defining conditions for wholesale charging.

8. The charging system of claim 1 wherein the charging rules include interconnect rules defining conditions for interconnect charging.

9. The charging system of claim 1 wherein the charging rules include content rules defining conditions for content charging.

10. The charging system of claim 1 wherein the charging rules include roaming rules defining conditions for roaming charging.

11. A method of determining the share of call revenue for a call, the method comprising:

receiving charging data for a call placed over a mobile network in a charging controller that is coupled to the mobile network and to an online charging system;

processing the charging data for the call and charging rules to identify entities that have a share in revenue for the call;

generating a charging request message indicating the entities having a revenue share in the call; and

transmitting the charging request message to the online charging system to cause the online charging system to determine the revenue share for each of the entities.

12. The method of claim 11 further comprising:

receiving the charging request message in the online charging system from the charging controller;

identifying a profile for each of the entities having a revenue share;

determining a revenue share amount for each of the entities based on their profile and a rating;

generating charging records indicating the revenue share amount for each of the entities; and

transmitting the charging records from the online charging system to the charging controller.

13. The method of claim 12 wherein the charging records each include an entity ID, a charging type, and a revenue share amount.

14. The method of claim 13 wherein the revenue share amount indicates a monetary amount owed to another entity.

15. The method of claim 12 further comprising:

receiving the charging records in the charging controller from the online charging system;

correlating the charging records to generate a consolidated charging record that indicates the revenue share amount for each of the entities; and

transmitting the consolidated charging record from the charging controller to a billing system.

16. The method of claim 11 wherein the charging rules include retail rules defining conditions for retail charging.

17. The method of claim 11 wherein the charging rules include wholesale rules defining conditions for wholesale charging.

18. The method of claim 11 wherein the charging rules include interconnect rules defining conditions for interconnect charging.

19. The method of claim 11 wherein the charging rules include content rules defining conditions for content charging.

20. The method of claim 11 wherein the charging rules include roaming rules defining conditions for roaming charging.

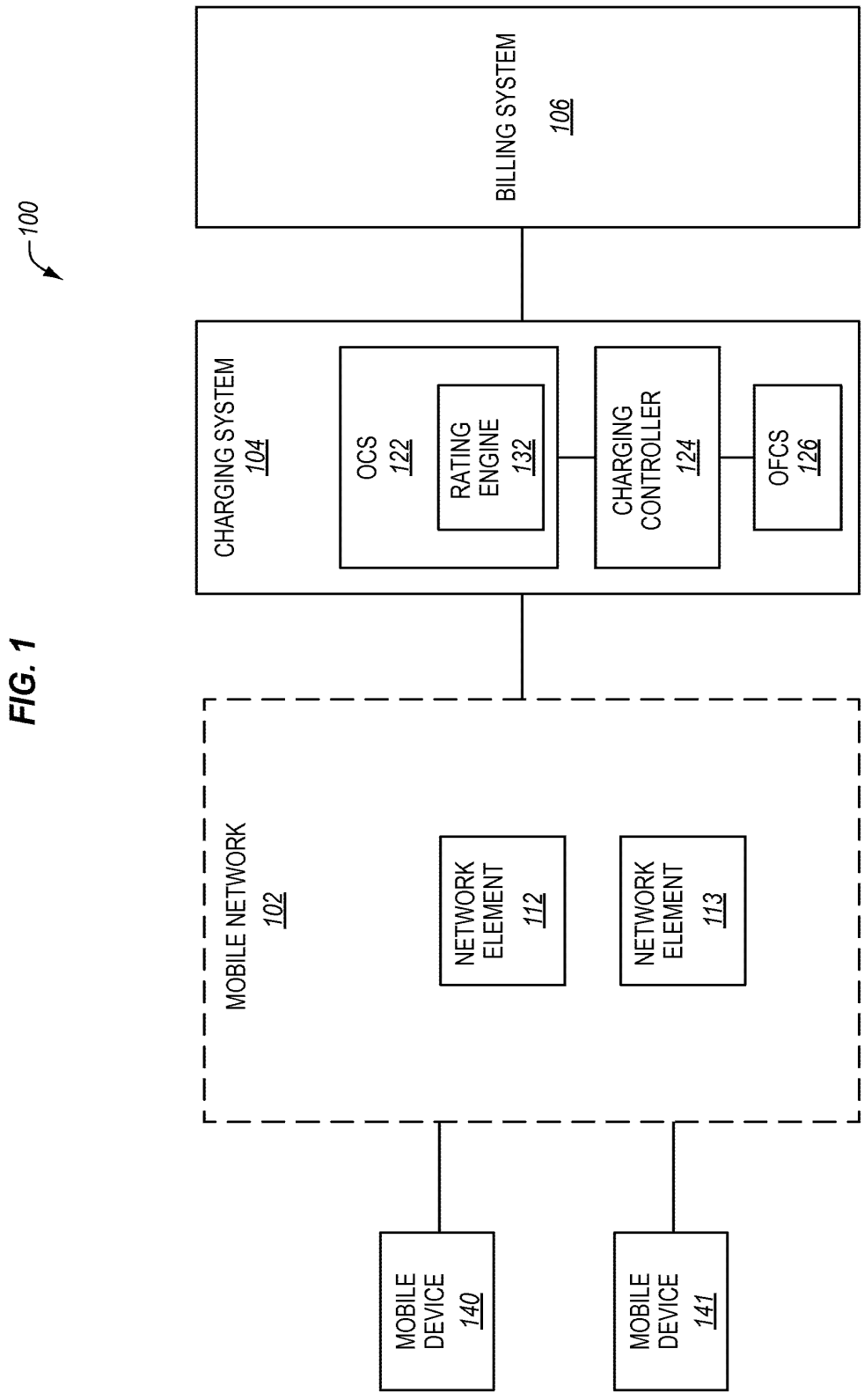

100
BILLING SYSTEM
106
CHARGING SYSTEM
104
OCS
122
RATING ENGINE
132
CHARGING CONTROLLER
124
OFCS
126
MOBILE NETWORK
102
NETWORK ELEMENT
112
NETWORK ELEMENT
113
MOBILE DEVICE
140
MOBILE DEVICE
141

FIG. 1

FIG. 2

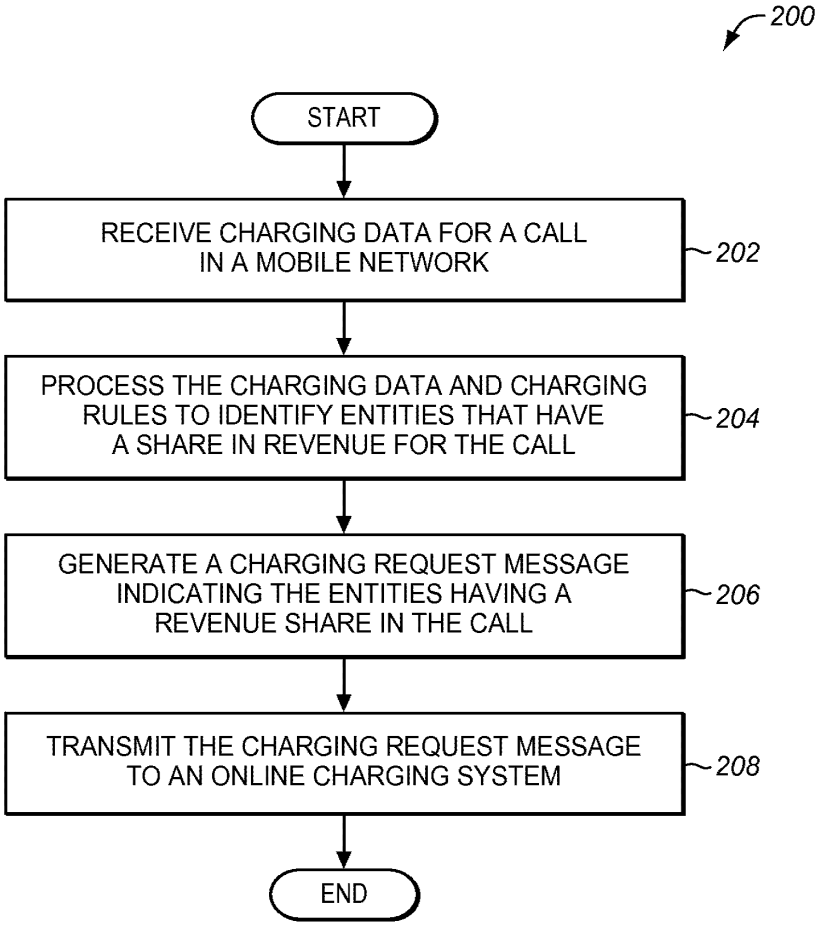

200
START
RECEIVE CHARGING DATA FOR A CALL IN A MOBILE NETWORK
202
PROCESS THE CHARGING DATA AND CHARGING RULES TO IDENTIFY ENTITIES THAT HAVE A SHARE IN REVENUE FOR THE CALL
204
GENERATE A CHARGING REQUEST MESSAGE INDICATING THE ENTITIES HAVING A REVENUE SHARE IN THE CALL
206
TRANSMIT THE CHARGING REQUEST MESSAGE TO AN ONLINE CHARGING SYSTEM
208
END

FIG. 3

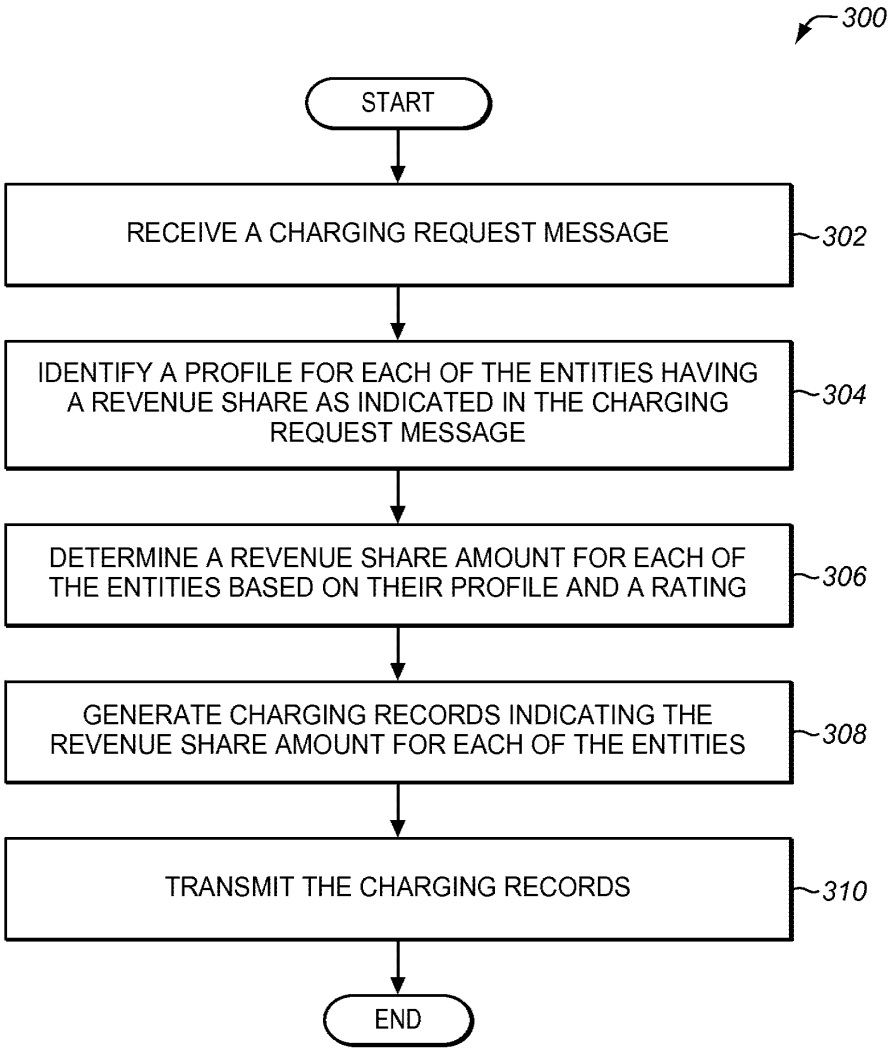

300
START
RECEIVE A CHARGING REQUEST MESSAGE
302
IDENTIFY A PROFILE FOR EACH OF THE ENTITIES HAVING A REVENUE SHARE AS INDICATED IN THE CHARGING REQUEST MESSAGE
304
DETERMINE A REVENUE SHARE AMOUNT FOR EACH OF THE ENTITIES BASED ON THEIR PROFILE AND A RATING
306
GENERATE CHARGING RECORDS INDICATING THE REVENUE SHARE AMOUNT FOR EACH OF THE ENTITIES
308
TRANSMIT THE CHARGING RECORDS
310
END

FIG. 4

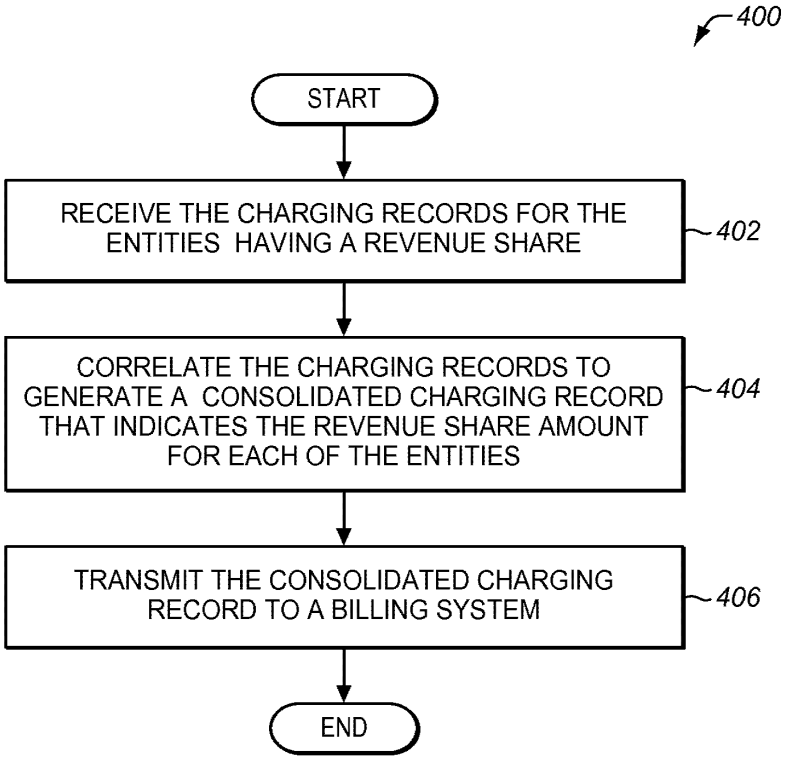
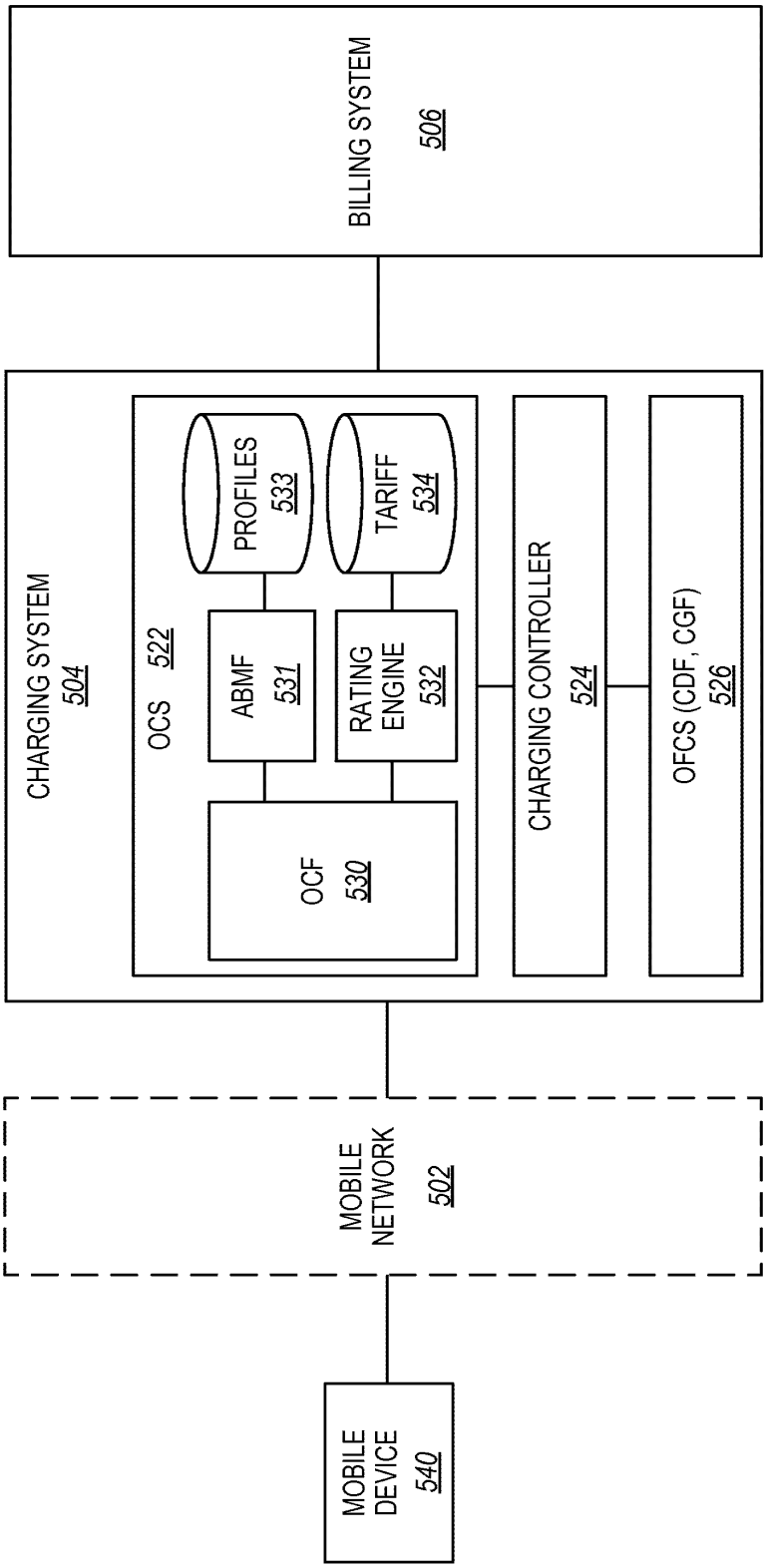

400
START
RECEIVE THE CHARGING RECORDS FOR THE ENTITIES HAVING A REVENUE SHARE
402
CORRELATE THE CHARGING RECORDS TO GENERATE A CONSOLIDATED CHARGING RECORD THAT INDICATES THE REVENUE SHARE AMOUNT FOR EACH OF THE ENTITIES
404
TRANSMIT THE CONSOLIDATED CHARGING RECORD TO A BILLING SYSTEM
406
END

FIG. 5


500
BILLING SYSTEM
506
CHARGING SYSTEM
504
OCS
522
PROFILES
533
TARIFF
534
ABMF
531
RATING ENGINE
532
OCF
530
CHARGING CONTROLLER
524
OFCS (CDF, CGF)
526
MOBILE NETWORK
502
MOBILE DEVICE
540

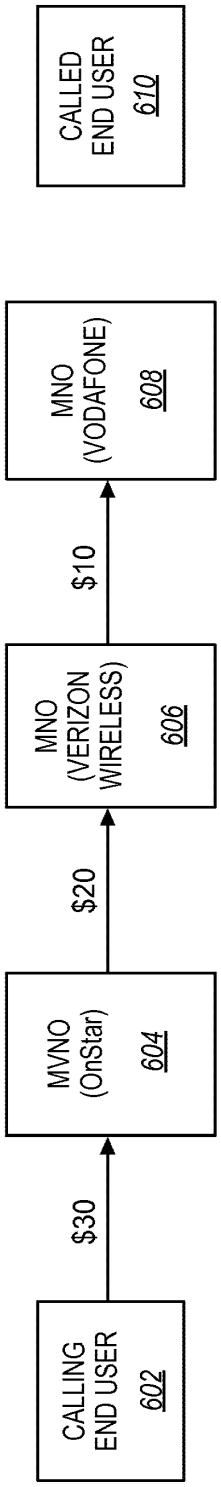

CALLING END USER 602
$30
MVNO (OnStar) 604
$20
MNO (VERIZON WIRELESS) 606
$10
MNO (VODAFONE) 608
CALLED END USER 610

FIG. 6

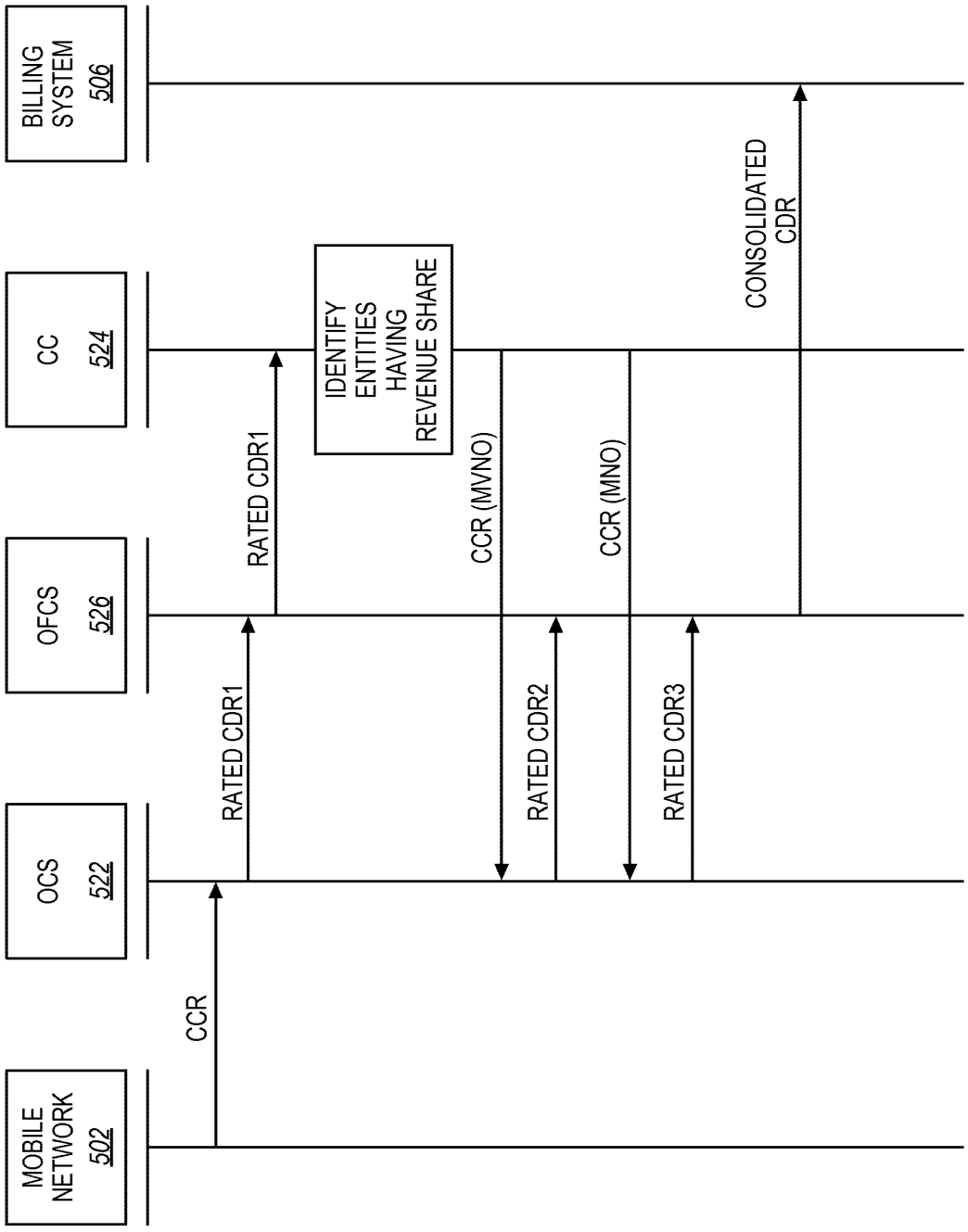

MOBILE NETWORK 502
OCS 522
OFCS 526
CC 524
BILLING SYSTEM 506
CCR
RATED CDR1
RATED CDR1
IDENTIFY ENTITIES HAVING REVENUE SHARE
CCR (MVNO)
RATED CDR2
CCR (MNO)
RATED CDR3
CONSOLIDATED CDR

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2009/049255

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04M15/00 H04W4/24
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)
H04M H04W

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 practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	XIANG YANG LI ET AL: "Converged network common charging controller function" BELL LABS TECHNICAL JOURNAL, WILEY, CA, US, vol. 13, no. 2, 21 June 2008 (2008-06-21), pages 161-183, XP001514359 ISSN: 1089-7089 page 167 - page 179 figures 4-15 ----- -/--	1-20

[X] Further documents are listed in the continuation of Box C.

[X] 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 document 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	Date of mailing of the international search report
30 March 2010	09/04/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Patlaka, Efi

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Maria Koutsopoulou: "A platform for charging, billing and accounting in future mobile networks" 24 January 2005 (2005-01-24), XP002574421 Retrieved from the Internet: URL:http://cgi.di.uoa.gr/~mkoutsop/data/Koutsopoulou_NGNM2004_almost_final.pdf> [retrieved on 2010-03-23] paragraph [0003] - paragraph [0005]	1-20
A	EP 1 545 114 A1 (CIT ALCATEL [FR] ALCATEL LUCENT [FR]) 22 June 2005 (2005-06-22) claims 1-10 paragraph [0028]	1-20
A	ANONYMOUS: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Management; Charging specification for Release 1; Draft ETSI DTS 02032" ETSI STANDARDS, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, vol. TISPAN, no. Version 1, 1 October 2005 (2005-10-01), XP014031462 ISSN: 0000-0001 the whole document	1-20
A	US 2004/224662 A1 (O'NEIL DOUGLAS R [US] ET AL) 11 November 2004 (2004-11-11) claim 8 claims 12, 13 claims 19, 20	1-20
A	WO 03/017065 A2 (APOGEE NETWORKS [US]; DESHMUKH ABHI [US]; HERNANDEZ MILTON [US]; GUHA) 27 February 2003 (2003-02-27) the whole document	1-20
A	EP 1 320 214 A1 (MARKPORT LTD [IE]) 18 June 2003 (2003-06-18) paragraph [0044] paragraph [0047] paragraph [0051]	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2009/049255

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1545114 A1	22-06-2005	AT 372643 T	15-09-2007
		CN 1630239 A	22-06-2005
		US 2005135577 A1	23-06-2005
US 2004224662 A1	11-11-2004	US 2009286507 A1	19-11-2009
		US 2007042750 A1	22-02-2007
WO 03017065 A2	27-02-2003	AU 2002332604 A1	03-03-2003
EP 1320214 A1	18-06-2003	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017065 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US02/26595

(22) International Filing Date: 20 August 2002 (20.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/934,123 21 August 2001 (21.08.2001) US

(71) Applicant *(for all designated States except US)*: **APOGEE NETWORKS** [US/US]; 1455 Broad Street, 4th Floor, Bloomfield, NJ 07003 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DESHMUKH, Abhi** [IN/US]; 253A, Kinderkamack Road, River Edge, NJ 07661 (US). **HERNANDEZ, Milton** [DM/US]; Apt. D, 1 Cononial Court, River Edge, NJ 07661 (US). **GUHA, Jayanta** [—/US]; 860 Main Street, Apt. 5B, Hackensack, NJ 07601 (US).

(74) Agents: **DUNNAM, Michael, P.** et al.; Woodcock Washburn LLP, One Liberty Place, 46th Floor, Philadelphia, PA 19103 (US).

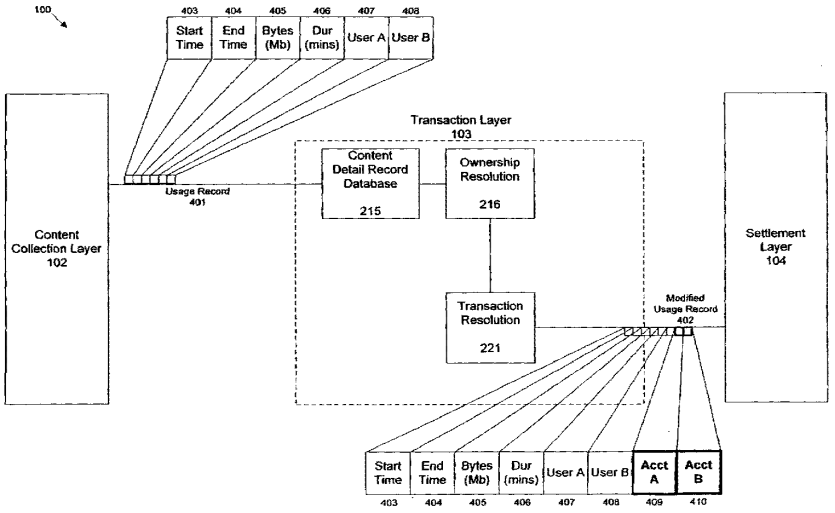
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: CONTENT OWNERSHIP RESOLUTION



(57) Abstract: The invention describes a method, system, and computer-readable medium having computer-executable instructions for determining parties to a transaction. The inventive method includes receiving data related to an event, where the data includes one or more data elements. The inventive method also includes selecting the data elements that identify the parties to the transaction, determining whether additional data elements are required to identify the parties to the transaction, and identifying the additional data elements. The event may be an exchange of data between the parties over a communication network, and the data related to the event may be stored in a usage record. The additional data element may identify an owner or party to the transaction, called an accountable. The party may have direct or indirect association in the transaction and may not be obvious from the record of the transaction itself.

WO 03/017065 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONTENT OWNERSHIP RESOLUTION

Technical Field

The invention relates generally to the processing of data, and more particularly to efficiently and generically aggregating data available on a communication network.

Background of the Invention

Recently, the collection and processing of data transmitted over communication networks, like the Internet, has moved to the forefront of business objectives. In fact, with the advent of the Internet, new revenue generating business models have been created to account for the consumption of content received from a data network (*i.e.*, content-based billing). For example, content distributors, application service providers (ASPs), Internet service providers (ISPs), and wireless Internet providers have realized new opportunities based on the value of the content and services that they deliver. As a result of this content-and-services-billing initiative, it has become increasingly important to resolve intelligently and flexibly the corresponding transactions according to the business needs of the customer.

Often, even in traditional commerce streams, there a many different participants between the maker and the consumer of the goods. Some of these so-called "middlemen" simply may facilitate access to the good, while others may add useful characteristics to the good. This is especially true in a distributed network environment, like the Internet,

that impose additional burdens on capturing the transaction process because of the unlimited number of data sources and the correspondingly unlimited number of data types. As a result, adequately describing the transacting of the goods and services in such an environment, or even across any of the traditional environments requires a technique that is capable of understanding and processing the participants and the various types of data.

To date, resolving the characteristics of a transaction has been accomplished over data-specific environments using certain application-specific (*i.e.*, "non-generic" or custom) methods. For example, a typical telephone bill captures the characteristics of a voice-based telecommunications transaction. In particular, the participants may be identified as the party initiating the call (*i.e.*, the "calling party" telephone number), the party receiving the call (*i.e.*, the "called party" telephone number), and one or more parties connecting the communication (*i.e.*, the "local" or "long distance carrier"). This simple example adequately captures all of the necessary aspects of the telephone call to properly account for the transaction by requiring payment from certain parties (*e.g.*, the calling and/or the called party) to certain other parties (*e.g.*, the local and/or long distance carrier). While these "hard-coded" transaction resolution techniques are sufficient to accommodate only specific environments involving well-defined participants (e.g., the telecommunications network), they are correspondingly too rigid to efficiently satisfy the ever-changing face of a communication network like the Internet. Also, these "hard-

coded" techniques are too specific to operate across the many and varied transaction environments and domains that exist throughout the business world.

Therefore, there exists a need to provide a flexible technique that can capture and resolve transactions of any type in any business domain involving any number and kind of participants without requiring modification of the technique for each type. Such a technique would serve to accommodate multi-faceted networked environments like the Internet, as well as to provide a single solution that would apply to any business environment.

Summary of the Invention

The invention describes a method, system, and computer-readable medium having computer-executable instructions for determining parties to a transaction. The inventive method includes receiving data related to an event, where the data includes one or more data elements. The inventive method also includes selecting the data elements that identify the parties to the transaction, determining whether additional data elements are required to identify all or some of the parties to the transaction, and identifying the additional data elements. The event may be an exchange of data between the parties over a communication network, and the data related to the event may be stored in a usage record. The additional data element may identify an owner or party to the transaction, called an accountable. Determining whether additional elements are required may be a function of the received data, and/or a function of the requirements of a customer

settlement system. The customer settlement system may be a data security system, a network capacity planning system, a content monitoring system, and/or a billing application, for example. The identifying of additional data elements or accountables may be initiated by a building block known as a primitive that includes multiple specific methods, including a database lookup, a direct value assignment, a regular expression parsing or match, a CDR database lookup, hard-coded, network address, area code, substring manipulation or a custom code execution. All or some of the inventive method steps may be conducted on a computer-readable medium using computer-executable instructions.

The inventive system for determining parties to a transaction includes an instrumentation layer, a content collection layer in communication with the instrumentation layer, and a transaction layer in communication with the content collection layer. The instrumentation layer provides raw data, while the content collection layer generically processes the raw data, and the transaction layer identifies one or more parties to the transaction. Also, the content collection layer may provide the raw data to the transaction layer in a usage record, and the transaction layer may modify the usage record as a function of identifying the parties to the transaction. The inventive system may further include a settlement layer in communication with the transaction layer, wherein the settlement layer rates the modified usage record. The transaction layer may include a database for storing the data processed by the content collection layer.

Brief Description of the Drawings

Other features of the invention are further apparent from the following detailed description of the embodiments of the invention taken in conjunction with the accompanying drawings, of which:

Figure 1 is a block diagram of a system for analyzing content transmitted over a communication network, according to the invention;

Figure 2 is a block diagram further describing the components of the system described in Figure 1;

Figures 3A and 3B provide a flow diagram further detailing the operation the system described in Figure 1;

Figure 4 provides a block diagram of the system described in Figure 1, providing greater detail of a configuration and operation of a transaction layer;

Figures 5A and 5B provide a flow diagram of a method for identifying the characteristics of a transaction, according to the invention;

Figure 6 is a block diagram further detailing the operation and configuration of the transaction layer, according to the invention; and

Figure 7 is a flow diagram that details the operation and configuration of the transaction layer of transaction layer, according to the invention.

Detailed Description of the Invention

System Overview

Figure 1 is a block diagram of a system 100 for analyzing content transmitted over a communication network. Although the following description will be discussed in the context of collecting, processing and billing for data transmitted over the Internet, it should be appreciated that the invention is no so limited. In fact, the invention may be applied to any type of network, including a private local area network, for example. Also, the invention may be used for purposes other than billing for the usage of content. For example, the invention may be used to analyze the type of data transmitted over a particular network, or to determine the routing patterns of data on a network. Furthermore, the invention may be used to facilitate the intelligent collection and aggregation of data relevant to a particular industry. In addition, the invention may be used to track specific Internet protocol (IP) network resources and to detect fraud, for example. It should also be appreciated that the invention may contemplate non-network and non-computer related business domains like commodity trading (*e.g.*, grains, crude oil) where multiple parties are involved. Therefore, although the invention is often described in the context of the Internet, it should be appreciated that the invention may equally applied to traditional business environments.

In addition, it should be appreciated that the term "content" may be defined as data that is transmitted over the network. In the context of the Internet, content may include .mp3 files, hypertext markup language (html) pages, videoconferencing data, and streaming audio, for example. The terms "content provider" and "customer" will be used throughout the description as well. Content provider may refer to the primary creator or

provider of the content, while customer is the primary recipient of the content. Both the producer and customer may be a human or a computer-based system.

As shown in Figure 1, an instrumentation layer 101 provides raw data to a content collection layer 102. Instrumentation layer 101 may consist of various data sources, for example, network routers. The network routers may provide information regarding the various types of routed data, including for example, data format, originating Internet protocol (IP) address, and destination IP address. One example of such information is Cisco System's NetFlow™.

Content collection layer 102 collects information about the delivery of the content, as well as the substance of the content itself. Content collection layer 102 also may sort, filter, aggregate, correlate and store the content according to the particular needs of the end user. In effect, content collection layer is responsible for extracting meaningful information about IP traffic, and so it is provided with an understanding of the data sources in instrumentation layer 101. Content collection layer 102 also may transform the data from the plurality of sources in instrumentation layer 101 into standard formats for use in a transaction layer 103.

Content collection layer 102 is in communication with transaction layer 103. Generally, content collection layer 102 reports to transaction layer 103 that a relevant communication event has occurred and should be considered by the remainder of system 100. A communication event may be defined as any transfer of data between systems. Transaction layer 103 captures the predetermined agreements among all of the parties

involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer 103 is charged with understanding the nature of the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 is in communication with a settlement layer 104. Settlement layer 104 captures the operations that are necessary to understand the significance of the transaction defined by transaction layer 103. For example, settlement layer 104 may rate a particular transaction by assigning a monetary value to the transaction. Settlement layer 104 also may divide the burdens and benefits of the monetary value among the relevant parties. In this way, settlement layer 104 ensures that certain parties receive a particular portion of the payment made by the other parties. Settlement layer 104 also may be responsible for delivering this burden and benefit information to the appropriate parties with the appropriate identifiers (*e.g.,* account numbers).

Figure 2 is a block diagram further describing the components of system 100. As shown in Figure 2, instrumentation layer 101 includes data sources 201-203 that each provide raw data 204-206, respectively, to collection layer 102. As discussed, data sources 201-203 may include various internetworking devices like routers, bridges, and network switches. Data sources 201-203 provide raw data to an input data adapter 207. Accordingly, input data adapter 207 understands the operation of and the data provided

by data sources 201-203. Although one input data adapter is shown in Figure 2, it should be appreciated that more than one input data adapter may be used in system 100. For example, each data source may have a dedicated input data adapter.

Input data adapter 207 understands the incoming data and extracts the data into the appropriate fields. This field-delimited data, called flow objects 208, are sets of attributes. The attributes may be any characteristics that are provided by, or can be derived from, raw data 204-206 provided by data sources 201-203, respectively. For example, flow objects 208 may include a set of attributes describing the source and destination, including source IP address, destination IP address, source interface, and destination interface. Because input data adapter 207 is charged with understanding raw data 204-206 from data sources 201-203, as well as the required flow objects 208 of system 100, it is capable of transforming the raw data to the flow objects, where the flow objects may all be of a standard format.

Input data adapter 207 provides flow objects 208 to a content data language 209. Content data language 209 may transform the attributes in flow objects 208 into other attributes that are desired by a particular customer. For example, content data language 209 may derive a network identifier attribute that is not readily available from a data source, from a source address attribute and a destination address attribute that are provided by flow object 208 attributes from input data adapter 207. This derivation may be based on a customer's desire to determine which network conveyed the transaction between the source and the destination. Therefore, following this example, content data

language 209 will know to extract the source address attribute and the destination address attribute from flow objects 208.

Content data language 209 may perform other functions as well. For example, content data language 209 may perform a generic lookup function 219 that is built into content data language 209. Generally, generic lookup 219 describes a technique for mapping any number of attributes to any number of other derived attributes. For example, generic lookup 219 may be used to map a unique resource locator (URL) attribute to a particular content-type attribute.

Content data language 209 also is in communication with a correlator 211. Generally, correlator 211 connects the many daily network content events from various network devices, like routers for example. Often, the connected data may come from distinctly different data sources at distinctly unrelated times. Correlator 211 allows this data to be intelligently connected to each other, regardless of how different the sources or of how disparate the time received. For example, a Netflow™ enabled router and a Radius™ enabled network access switch may each provide certain data that is relevant to one particular transaction. However, because portions of the data come from different devices, the data may arrive at system 100 at different times, and in different formats. Also, because each provides data that is necessary to complete one transaction, the data from each cannot be considered separately. Correlator 211 allows this data to be intelligently grouped regardless of the format of the data or of the time the data pieces are received.

Furthermore, correlator 209 may rearrange the order of the received flow objects 208 to suit the needs of the remainder of system 100. By performing such correlation without having to first store all of the data on a disk (*e.g.*, a database), significantly faster processing is achieved. Correlator 209 may perform this correlation in real-time, for example.

Although system 100 has been described using content data language 209 and correlator 211, it should be appreciated that flow objects 208 may proceed directly to a filter 212, if no correlation is required and if no attribute derivation is required, for example. Filter 212 analyzes flow objects 208 to ensure that the provided attributes are desired by system 100. If flow objects 208 are not needed (*i.e.*, a mismatch), filter 212 may prevent flow objects 208 from passing to an aggregator 213. Also, although filter 212 has been shown as a separate device in system 100, it should be appreciated that the functionality of filter 212 may be incorporated into aggregator 213.

Filter 212 passes the matching flow objects to aggregator 213. Aggregator 213 may provide additional filtering and classification of the multitude of daily network content transactions, based on user criteria. Aggregator 213 may perform such filtering and classification in real-time. Aggregator 213 will be discussed in greater detail with reference to Figures 4-7. Aggregator 213 provides the filtered and classified information to an output data adapter 214. Output data adapter 214 may convert the data from aggregator 213 into one or more content detail records for storage in CDR database 215. Therefore, CDR database 215 stores a complete description of a content event.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 passes the CDR onto ownership resolution component 216. A proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. These tasks are accomplished by ownership resolution component 216 and transaction resolution component 221.

Ownership resolution component 216 serves to define the direct and indirect participants of the communication event. In particular, because raw data 204-206 may not provide sufficient "ownership" data relating to the parties involved in the content transaction, such "ownership" data must be provided by system 100 to properly account for the entire transaction. Ownership resolution component 216 operates to provide such ownership-based data to system 100.

Ownership resolution component 216 is in communication with transaction resolution component 221. Transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Such predetermined relationships may be previously agreed upon by the participants, or may be created and agreed upon with the implementation of system 100. Therefore, transaction component 103 understands the nature of the parties, the actions that one or

more parties perform, and the influence of such action on the respective parties. Ownership resolution component 216 and transaction resolution component 221 will be discussed in greater detail.

Transaction component 216 provides the transaction information to a rating component 217. Rating component 217 provides a weight or significance (*e.g.*, a price) to the transaction, so as to provide a tangible value to the transaction. Rating component 217 may make this determination based on various metrics including the type of the content, the quantity of content consumed, the place and time delivered, or the quality of the content for example. Therefore, rating component 217 allows system 100 to provide some contextual value, indicting the significance or relevance that certain content or information has to the individual customer.

Rating component 217 provides the rated transaction to a presentment component 218. Presentment component 218 may provide the capability for a customer 220 to view their real-time billing information, for example, over the network. Presentment component 218 also may attach relevant identifiers to the bill (*e.g.*, account numbers, etc.).

Figures 3A and 3B provide a flow diagram further detailing the operation 300 of system 100. As shown in Figure 3A, in step 301, raw data 204-206 is received from data sources 201-203. In step 302, input data adapter 207 converts raw data 204-206 to flow objects 208, where flow objects 208 are sets of attributes, determined from raw data 204-206. In step 303, it is determined whether there is a need to derive new attributes from

the existing attributes found in flow objects 208. If there is such a need, in step 304, CDL 209 is used to derive new attributes from existing attributes. Also, as discussed above, attributes may be correlated by correlator 211.

In step 305, flow objects 208 are filtered by filter 212. In step 306, the matching flow objects (*i.e.*, those passed by filter 212) are further filtered and classified by aggregator 213 (as discussed more fully with reference to Figures 4-7). In step 307, output data adapter 214 converts the data aggregated by aggregator 213 to a format compatible with transaction layer 103.

As shown in Figure 3B, in step 308, output adapter 214 may format the aggregated data into one or more content data records for storage in CDR database 215. In step 309, ownership resolution component 216 identifies the parties involved in the transaction. In step 310, transaction resolution component 221 captures the predetermined agreements among the parties, as well as the value added by each of the individual parties. In step 311, the CDR is rated based on predetermined metrics (*e.g.*, time of transmission, quality of content). In step 312, a bill is presented to the customer.

Content Transaction Layer

A transaction, including a business transaction for example, may be any activity between two or more participants that affects certain parties. The affected parties may be considered the participants to the transaction, although parties and participants may be mutually exclusive entities. It should be appreciated that the terms "parties" and "owners" may be used interchangeably throughout. Also, a transaction may include one or more events, where an event may be some action (*e.g.*, the transfer of a service or good) that the participants conduct with each other. Such events may be the exchange of data over a communication network, for example. Also, it should be appreciated that the same event or action may take place in any direction (*e.g.*, from party A to party B or from party B to party A). The "subject" of the action is the party who performs the activity, while the "object" of the action is the party who is affected or influenced in any way by the action.

Transaction layer 103 is responsible for capturing the characteristics of the transaction, including the parties, participants, subject, object, event/action type, direction of the action, for example. The scope of the characteristics captured by transaction layer 103 will vary with the nature of instrumentation layer 101, the capability of content collection layer 102, and the requirements of settlement layer 104. Generally, transaction layer 103 captures the predetermined agreements among all of the parties involved in system 100 regarding the value of the transferred content, as well as the value added by each of the individual parties in transferring such content. Therefore, transaction layer

103 is charged with understanding the nature of the parties, as well as the understanding the actions that one or more parties perform and the influence of such action on the respective parties.

Transaction layer 103 includes CDR database 215, an ownership resolution component 216, and a transaction resolution component 221. CDR database 215 is a data store that holds each CDR for further processing by ownership resolution component 216 and transaction resolution component 221. In the context of a billable electronic business transaction, a proper accounting of a communication event, for any purpose including billing, requires both identifying the participants and defining the relationships among those participants. As discussed, ownership resolution component 216 serves to define the participants of the communication event, while transaction resolution component 221 serves to capture the predetermined relationships and/or agreements among the parties defined by ownership resolution component 216.

Transaction layer 103 is generic in that it operates without requiring an understanding of instrumentation layer 101 and content collection layer 102. Instead, transaction layer 103 takes the relevant characteristics of the transaction provided by instrumentation layer 101 and content collection layer 102, and selects and generates those characteristics required by settlement layer 104.

Although the operation of transaction layer 103 will be described in the context of an electronic event over a communication network for the purposes of billing for the event, it should be appreciated that the invention is not so limited, but is so described the

purpose of clarity. For example, it should be appreciated that the invention may include functions other than billing, including security, network capacity planning, and content monitoring, for example. Also, the generic techniques described may be applied beyond the context of an electronic event over a communication network.

Figure 4 provides a block diagram of system 100 providing greater detail of the configuration and operation of transaction layer 103. As shown in Figure 4, content collection layer 102 provides a usage record 401 to transaction layer 103. A series of fields 403-408 comprise usage record 401. Although fields 403-408 will be identified by certain labels for the purpose of clarity, it should be appreciated that fields 403-408 may identify any of the many possible characteristics of the transaction.

In the example provided by Figure 4, fields 403 and 404 identify the parties or participants to the transaction. In particular, field 403 identifies "User A" and field 404 identifies "User B." User A may be the subject party and User B may be the object party. For example, in the context of a telecommunication event, User A may be the "calling" party and User B may be the "called" party. Field 405 and field 406 identify a measurable quantity of the event. In particular, following the example of the telecommunications event, field 405 identifies a duration (in minutes) of the event and field 406 identifies the quantity of data exchanged during the event (in megabytes). Field 407 and field 408 may identify a "start time" and an "end time," respectively, of the communication event.

Although fields 403-408 provide just one example, in any case, it should be appreciated that user record 401 will include certain characteristics provided by instrumentation layer 101 and/or derived by content collection layer 102. These characteristics typically are provided to transaction layer 103 because they have some particular significance to identifying the characteristics necessary to allow settlement layer 104 to provide some accounting of the transaction. Therefore, usage record 401 may not necessarily include all of the characteristics provide by instrumentation layer 101 and/or derived by content collection layer 102, because certain characteristics may not relevant to the settlement of the transaction (*e.g.*, network type). Yet, usage record 401 will include those available characteristics that pertain to permitting settlement layer 104 to properly account for the transaction.

Once usage record 401 passes through transaction layer 103, a modified usage record 402 may be provided to settlement layer 104. Modified usage record 402 may be modified by transaction layer 103 to include additional details of the transaction event required by settlement layer 104 and/or required by the customer's system to which the usage record applies (*e.g.*, a usage billing system). As shown for modified usage record 402, an account A field 409 and an account B field 410 may be added to further identify the transaction. In one example, account A field 409 may include an alphanumeric designator that identifies the account number that has been assigned by the customer's billing system for User A. In the context of the telecommunications system, account A field 409 may hold User A's ten-digit home telephone number, for example.

In any case, the components of transaction layer 103 operate to identify these additional fields, based on the requirements of the customer's system and of settlement layer 104. In particular, ownership resolution component 216 operates to ensure that the necessary participants or parties to the transaction are identified, while transaction resolution component 221 operates to ensure that the relationships among the parties or participants are identified.

Identification of the relevant entities and their relationships may be accomplished using "lookups" in data stores located within ownership resolution component 216 or user-defined actions specified on external systems and applications and transaction resolution component 221, for example. For example, a data table may have a "User" data field and an associated "Account" data field. When User A is received by ownership resolution component 216, it will conduct a lookup in the data table and identify Account A as the appropriate account associated with User A. Also, transaction resolution component 221 may have a data table that permits a lookup of the relationship between User A and User B, identified in usage record 401. For example, upon receiving field 407 designating User A and field 408 designating User B, transaction resolution component 221 may conduct a lookup of an algorithm that identifies the appropriate burdens and benefits (*e.g.*, debit and credit of money) assigned to each of the users with respect to each other.

It also should be appreciated that transaction layer 103 may not provide additional characteristics to usage record 401, as described but may select the relevant

characteristics (*i.e.*, those characteristics needed by settlement layer 104) from the characteristics made available by instrumentation layer 101 and/or derived by content collection layer 102. In fact, usage record 401 may include all of the necessary characteristics to properly account for the transaction. In this case, ownership resolution component 216 and transaction resolution component 221 select the relevant characteristics from the available characteristics.

Figures 5A and 5B provide a flow diagram of a method 500 for identifying the characteristics of a transaction using system 100. As shown in Figure 5A, in step 501, raw data 204-206 is received into system 100. Raw data 204-206 includes certain characteristics provided by data sources 201-203, respectively, in instrumentation layer 101. In step 502, content collection layer 102 processes (*e.g.*, aggregates, correlates and filters) raw data 204-206. In step 503, content collection layer 102 provides the processed data to CDR database 215 in transaction layer 103. CDR database 215 stores the data for further processing by transaction layer 103.

In step 505, it is determined whether the contents of the data provided to transaction layer 103 already include the needed ownership data. If the data includes the needed ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507. If, on the other hand, the data provided to transaction layer 103 does not already include the needed ownership data, the required data is identified (*e.g.*, using database lookups, accountable primitives) by ownership resolution component 216, in step 506. Once ownership

resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 507.

As shown in Figure 5B, in step 508 it is determined whether the contents of the data provided to transaction layer 103 already include the needed relationship data (*i.e.*, data defining the burdens and benefits encountered by the parties/participants to the transaction). If the data includes the needed relationship data, the relevant data is selected by transaction resolution component 221 and provided to settlement layer 104, in step 510. If, on the other hand, the data provided to transaction layer 103 does not already include the needed relationship data, the required data is identified (*e.g.*, using database lookups) by transaction resolution component 221, in step 509. Once ownership resolution component 216 identifies the required ownership data, the relevant data is selected by ownership resolution component 216 and provided to transaction resolution component 221, in step 510.

Ownership and Transaction Resolution

Figure 6 is a block diagram further detailing the operation and configuration of transaction layer 103. It should be appreciated that elements described for transaction layer 103 are not exclusive, but provide just one example of a configuration for transaction layer 103. In particular, the functionality of the previously described ownership resolution component 216 and transaction resolution component 221 will be

descried in greater detail in the various components described with reference to Figure 6. In practice, however, it should be appreciated that transaction layer 103 may comprise of any number of components that ensure that the necessary parties to a transaction are identified generically.

As shown in Figure 6, transaction layer 103 includes a configuration repository 601, a configuration database 610, a configuration manager 603, and a fail over detector 604. In addition, transaction layer 103 includes a transaction layer engine 608 in communication with configuration repository 601, configuration manager 603, and fail over detector 604.

Transaction layer engine 608 includes a rules processor 605, a CDR reader 606, and a transaction writer 607. Transaction layer engine 608 processes raw data 204-206 in usage record 401 and creates a modified usage record 402, based upon the requirements of settlement layer 104. It should be appreciated that there may be more than one transaction layer engine 608 for each transaction layer 103. However, a single transaction layer engine 608 is shown for the purpose of clarity and brevity.

CDR reader 106 understands the nature of the transaction and operates to read a particular usage record 401 stored in CDR database 215. CDR reader 106 then submits usage record 401 to rules processor 605. Rules processor 605 applies rules (*e.g.*, written in XML) to usage record 401 so as to determine ownership and the relationships among the ownership, for each individual usage record 401. Rules processor 605 may then generate one or more modified usage records 402, based on the application of the rules to

usage record 401. Once rules processor 605 generates the modified usage record 402, transaction writer 607 operates to write a transaction (based on the modified usage record 402) to CDR database 215. Modified usage record 402 is then used by settlement layer 104 to further process the transaction (*e.g.,* rate the transactions monetarily).

Fail over detector 604 operates to provide fault tolerance and initiate a fail over engine (not shown) for a failed transaction layer engine, in accordance with one or more mathematical algorithms, the discussion of which is beyond the scope of the invention. Configuration manager 603 provides an external interface to transaction layer 103 using a business editor 609. Business editor 609 may be manipulated by a user or customer using a graphics user interface (GUI). In particular, the GUI of business editor 609 receives commands from a user and translates them into actions to be performed on usage record 401, for example, by rules processor 605. Configuration repository 601 operates to provide an abstraction to configuration database 610. Configuration database 610 may be a relational database or a set of extensible markup language (XML) computer-readable files, for example.

Figure 7 is a flow diagram that details the operation of transaction layer 103, as shown in Figure 6. As discussed, it should be appreciated that multiple transaction engines may be used to implement a process. Where the invention is instituted using computer-readable instruction, transaction layer engine 608 may be implemented as a computer-executable instruction or thread. Therefore, multiple transaction layer engines may be implemented by having multiple computer-readable instructions.

In step 701, transaction layer engine 608 reads usage record 401 using CDR reader 606. In step 702, rules processor 605 applies one or more rules to usage record 401 read by CDR reader 606, so as to determine one or more "accountables." Accountables are labels that are used to facilitate identifying the parties or owners to a transaction. Accountables may be defined and/or modified by an external user (*e.g.,* a customer) using the graphical user interface provided by business editor 609. Also, it should be appreciated that accountables may be defined for a new usage types for which no rules in rules processor 605 are provided. The identification of accountables is the function of ownership resolution component 216, as described with reference to Figure 4.

In step 703, "contracts" are identified that define the relationships or agreements between one or more accountables. In the context of a billing system, a contract identifies which party pays (*i.e.,* the billed party) and which party receives payment (*i.e.,* the billing party). A particular contract may be identified and executed when one based on "conditions" are satisfied, however, such conditions may not be required. The identification of contracts is conducted by transaction resolution component 221, as described with reference to Figures 2 and 4. A condition is an expression of a logical assertion that can be evaluated as true or false. In transaction layer 103, for example, a condition may be true if a certain data element is present and false if the data element is not present. The following is an example of a condition in XML:

<condition name="condition1" function="IsPresent" outcome="true" type="Accountable" id="ColoProvider"/>

In step 704, once the contracts are determined, they are executed. In step 705, usage record 401 is changed to modified usage record 402 based upon the execution of the contract and the identification of the accountables. In step 706, modified usage record 402 may be written to a data table using transaction writer 607, so that settlement layer 104 can rate it, in step 707. Therefore, a transaction may be represented as modified usage record 402, where modified usage record may include the elements of usage record 401 in addition to the accountable and contract elements (*e.g.,* fields 409-410 as discussed with reference to Figure 4).

Although the discussion provided an example of a single contract and two accountables for a single usage record, it should be appreciated that many contracts and many accountables (*i.e.,* and therefore many "transactions") may be derived from a single usage record, because there may be multiple transactions implicated from a single usage record 401. For example, usage record 401 may involve three parties each having a contract with the other respective parties. In this example, therefore, there may be three separate contracts for a single usage record 401, and three individual accountables for each party or owner.

In addition to requiring a certain accountable, it may be necessary to determine a value of the accountable. For example, transaction layer 103 may determine not only that the "called party" accountable be a part of the transaction, but also that a value for the

called party (*e.g.*, "856-555-1212" or "John Doe") be identified. Also, it may be necessary to transform one accountable into another accountable to satisfy the requirement of settlement layer 104. For example, settlement layer 104 may require the called party accountable (either determined by transaction layer 103 or provided in usage record 401) be transformed into a network identifier accountable.

In either case, the value or transformation of accountables or contracts may be determined using certain predetermined functions or "primitives." A primitive allows the user to specify how to find the value of a particular accountable or how to find billing and/or billed account numbers associated with a particular contract. As discussed, transformations may allow a value of an accountable to be determined using another accountable (*i.e.*, called "linked accountables"), for example. Primitives define and direct such transformations. The input to a primitive can be one of fields 403-408 from usage record 401 or a previously determined accountable, for example.

Primitives may be described and distinguished based on their prescribed functionality. For example, one type of primitive may be an external database lookup. A database lookup is a primitive that operates to transform one accountable or contract to another accountable or contract. Also, a database lookup primitive may function to assign a value to an accountable or contract, as a result of conducting a lookup of the accountable or contract in a database. It should be appreciated that the database lookup primitive also allows flexibility in that any database that has Java Database Connectivity (JDBC) drivers (*e.g.*, Oracle, Microsoft SQL Server, Sybase, Database 2) can be used to

perform complex lookups. For native databases that do not have JDBC connectivity, however, it should be appreciated that native methods for native databases may be accommodated through the primitives. In this way, therefore, previous accountable or contact transformations can be linked to find new accountables or contracts, respectively.

Other types of primitives may include direct value assignment, and a function primitive. A function primitive provides flexibility and extensibility by allowing a third party based library (*e.g.*, Java-based or native libraries) to be used. The arguments of a function primitive may be text strings. Also, the arguments of a function primitive may be expressed in terms of fields in CDR database 215 (*i.e.*, string-based fields in usage record 401), and other previously determined accountables. Therefore, function primitives permit the integration of proprietary and domain-specific algorithms to be implemented to perform ownership related processing.

Another primitive may be a "regular expression" based primitive that allows parsing of complex text-based fields with a full feature (*e.g.*, PERL5 compliant) pattern specification. Common used techniques would include parsing URLs, filenames and paths, calling/called telephone numbers, email address, for example. In addition, a CDR database 215 lookup primitive allows holding on to an ownership entity if no further processing is required. This primitive is used where usage record 401 provides the information needed by settlement layer 104 without any need for more data correlation and/or manipulation by transaction layer 103.

A default primitive may be a hard-coded primitive that is used where the value is known and/or is not dependent on usage record 401. For example, such a primitive may be used where a party is always present in a consumption event, regardless of the other relevant parties. A network address primitive allows determination of a network entity given an arbitrary string. An area code primitive may be used to determine an area code of a telephone number given the complete telephone number. This primitive may be relevant for a Voice-over-IP application. These examples primitives are not exclusive, but are meant to provide a few examples of the manipulation and correlation that may be achieved by the primitives on the accountables and contracts.

The following is an example of an accountable primitive in XML:

```
<accountable>
<name> ColoProvider </name>
<role> ServiceProvider </role>
<usageType> RMONHost </usageType>
<valid from="past" to="present" />
<primitive type="default">
<value> Exodus </value>
</primitive>
</accountable>
```

Each accountable that is involved in a contract will have an assigned "role." It follows, therefore, that an accountable that is not involved in a contract may not need to have an assigned role. The role associates the particular accountable for integration with settlement layer 104. This means that the concept of a role is used for the TL/AMI integration.

Similar to the accountable, a contract is implemented using a set of primitives. The following is an example of a contract primitive in XML, and is provided to further describe the invention. In the example, a Web hosting scenario is present where a content provider (*e.g.,* CNN) places content on one or more Web servers and pays a Web Hoster for doing so based on some predefined pricing plan.

In order to define the accountables, certain elements of usage record 401 may be assumed as follows: Web Hit Time, Web Server Name/IP address, Client IP address, bytes, Mime type, and URL. In this example, if a rule in the business world requires the "Content Provider" of the Web Server (*e.g.,* CNN) to pay to the Web Hoster, there are two accountables: Web Hoster and Content Provider. The XML definition of a contract that captures this business rule may be as follows:

```
01  <contract>
02  <name> ContentProvider-Pays-WebHoster </name>
03  <usageType> WebHosting </usageType>
04  <valid from="past" to="present" />
05  <condition function="IsPresent" type="Accountable"
    name="condition1"  id=" ContentProvider " />
06  <condition function="IsPresent" type="Accountable"
    name="condition2" id="WebHoster" />

07  <billedFunction>
08  <status> enabled </status>
09  <primitive type="internal-account-lookup">
10  <database name="GlobalDB"/>
11  <argument order="1" type="Accountable"
    name="ContentProvider"/>
12  </primitive>
13  </billedFunction>
```

```
14    <billingFunction>
15    <status> disabled </status>
16    <primitive type="internal-account-lookup">
17    <database name="GlobalDB"/>
18    <argument order="1" type="Accountable" name="WebHoster"/>
19    </primitive>
20    </billingFunction>
21    </contract>
```

In this example, a contract has a name defined in line 02 as "ContentProvider-Pays-WebHoster." The contract also defines an element or usage type called "WebHosting" in line 03. The contract also has two sets of conditions in lines 05 and 06, called "IsPresent," which consider whether "ContentProvider" and "WebHoster" elements are present, respectively. Therefore, this particular contract will be selected and executed by transaction layer 103 if these elements are present.

Also, in this contract example, there are two primitives that are specified. There is a first primitive for finding the account number of the billed entity "ContentProvider," which begins on line 07 and ends on line 13, and there is a primitive for determining the account of the billing entity "WebHoster" beginning on line 14 and ending on line 20. Therefore, the example contract contemplates the "who pays to whom" logic, and results in the execution of a contract that creates a modified usage record 402, which captures the transaction. Notably, in lines 09 and 16, both primitives are defined as database lookups.

The invention is directed to a system and method for of determining of direct and/or indirect parties involved in a transaction. The invention often was described in the context of the Internet, but is not so limited to the Internet, regardless of any specific description in the drawing or examples set forth herein. For example, the invention may be applied to wireless networks, as well as non-traditional networks like Voice-over-IP-based networks, private networks, and/or non-technology related business environments, like commodity trading for example. It will be understood that the invention is not limited to the use of any of the particular components or devices herein. Indeed, this invention can be used in any application that requires the determining of direct or indirect parties involved in a transaction. Further, the system disclosed in the invention can be used with the method of the invention or a variety of other applications.

While the invention has been particularly shown and described with reference to the embodiments thereof, it will be understood by those skilled in the art that the invention is not limited to the embodiments specifically disclosed herein. Those skilled in the art will appreciate that various changes and adaptations of the invention may be made in the form and details of these embodiments without departing from the true spirit and scope of the invention as defined by the following claims.

What is Claimed is:

1. A method of determining parties to a transaction, comprising:

receiving data related to an event, wherein said data comprises one or more data elements;

selecting said data elements that identify the parties to the transaction;

determining whether additional data elements are required to identify the parties to the transaction; and

identifying the additional data elements.

2. The method of claim 1, wherein said event is an exchange of data between the parties over a communication network.

3. The method of claim 1, wherein said data related to said event is stored in a usage record.

4. The method of claim 1, wherein the parties include at least one of the following: a subject party and an object party.

5. The method of claim 1, wherein said determining is a function of the received data.

6. The method of claim 1, wherein said determining is a function of the requirements of a customer settlement system.

7. The method of claim 6, wherein said customer settlement system includes at least one of the following: a data security system, a network capacity planning system, and a content monitoring system.

8. The method of claim 1, wherein said data element is an accountable.

9. The method of claim 1, wherein said identifying of additional data elements is initiated by a primitive.

10. The method of claim 9, wherein said primitive includes at least one of the following: a database lookup, direct value assignment, regular expression, CDR database lookup, hard-coded, network address, substring manipulation, area code, and a user-specified action.

11. A system for determining parties to a transaction, comprising:

an instrumentation layer, wherein the instrumentation layer provides raw data;

a content collection layer in communication with the instrumentation layer, wherein the content collection layer generically processes the raw data; and

a transaction layer in communication with the content collection layer, wherein the transaction layer identifies one or more parties to the transaction.

12. The system of claim 11, wherein said content collection layer provides said raw data to said transaction layer in a usage record.

13. The system of claim 12, wherein said transaction layer modifies said usage record as a function of identifying the parties to the transaction.

14. The system of claim 11, further comprising a settlement layer in communication with said transaction layer, wherein the settlement layer rates the modified usage record.

15. The system of claim 12, wherein said transaction layer comprises a data base for storing said data processed by said content collection layer.

16. A computer-readable medium having computer-executable instructions for:

receiving data related to an event, wherein said data comprises one or more data elements;

selecting said data elements that identify the parties to the transaction;

determining whether additional data elements are required to identify the parties to the transaction; and

identifying the additional data elements.

17. The computer-readable medium of claim 16, wherein said computer-executable instructions are extensible.

18. The computer-readable medium of claim 16, wherein said event is an exchange of data between the parties over a communication network.

19. The computer-readable medium of claim 16, wherein said data related to said event is stored in a usage record.

20. The computer-readable medium of claim 16, wherein the parties include at least one of the following: a subject party and an object party.

21. The computer-readable medium of claim 16, wherein said determining is a function of the received data.

22. The computer-readable medium of claim 16, wherein said determining is a function of the requirements of a customer settlement system.

23. The computer-readable medium of claim 22, wherein said customer settlement system includes at least one of the following: a data security system, a network capacity planning system, and a content monitoring system.

24. The computer-readable medium of claim 16, wherein said data element is an accountable.

25. The computer-readable medium of claim 16, wherein said identifying of additional data elements is initiated by a primitive.

26. The computer-readable medium of claim 25, wherein said primitive includes at least one of the following: a database lookup, direct value assignment, regular expression, CDR database lookup, hard-coded, network address, substring manipulation, area code, and user-specified action.

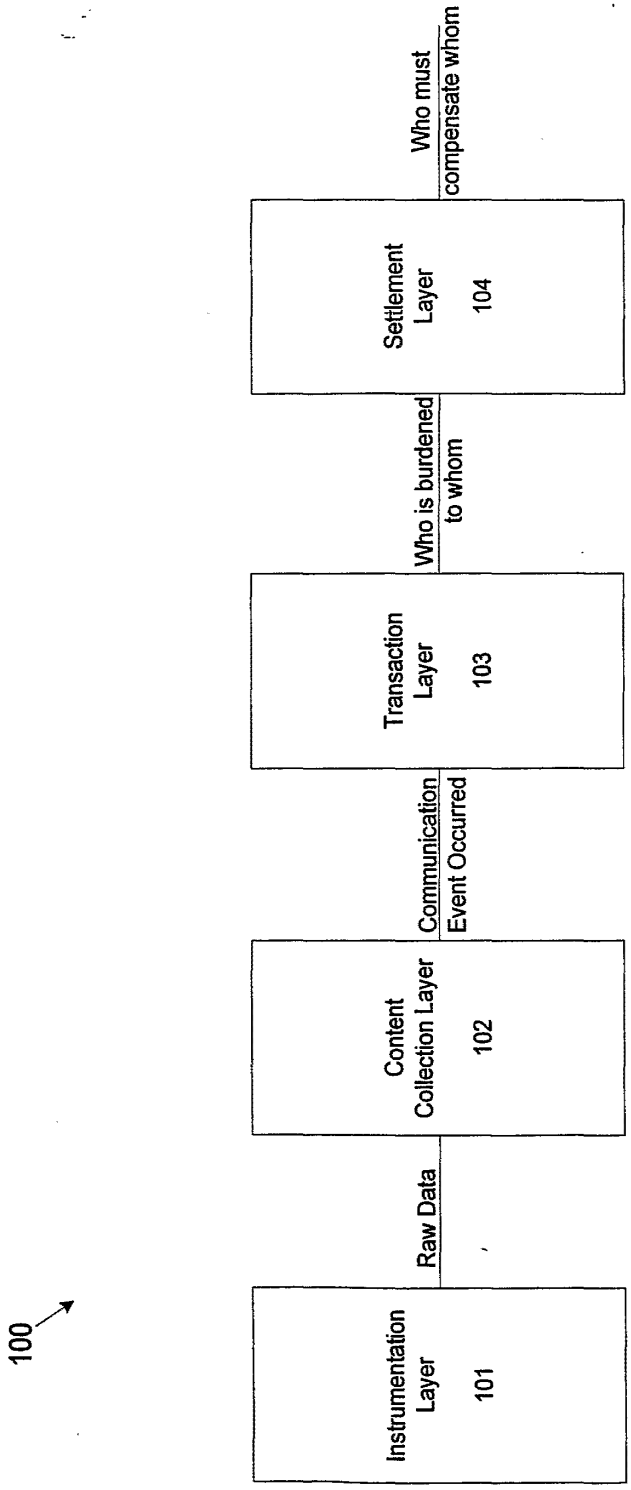

100
Instrumentation Layer
101
Raw Data
Content Collection Layer
102
Communication Event Occurred
Transaction Layer
103
Who is burdened to whom
Settlement Layer
104
Who must compensate whom

Figure 1

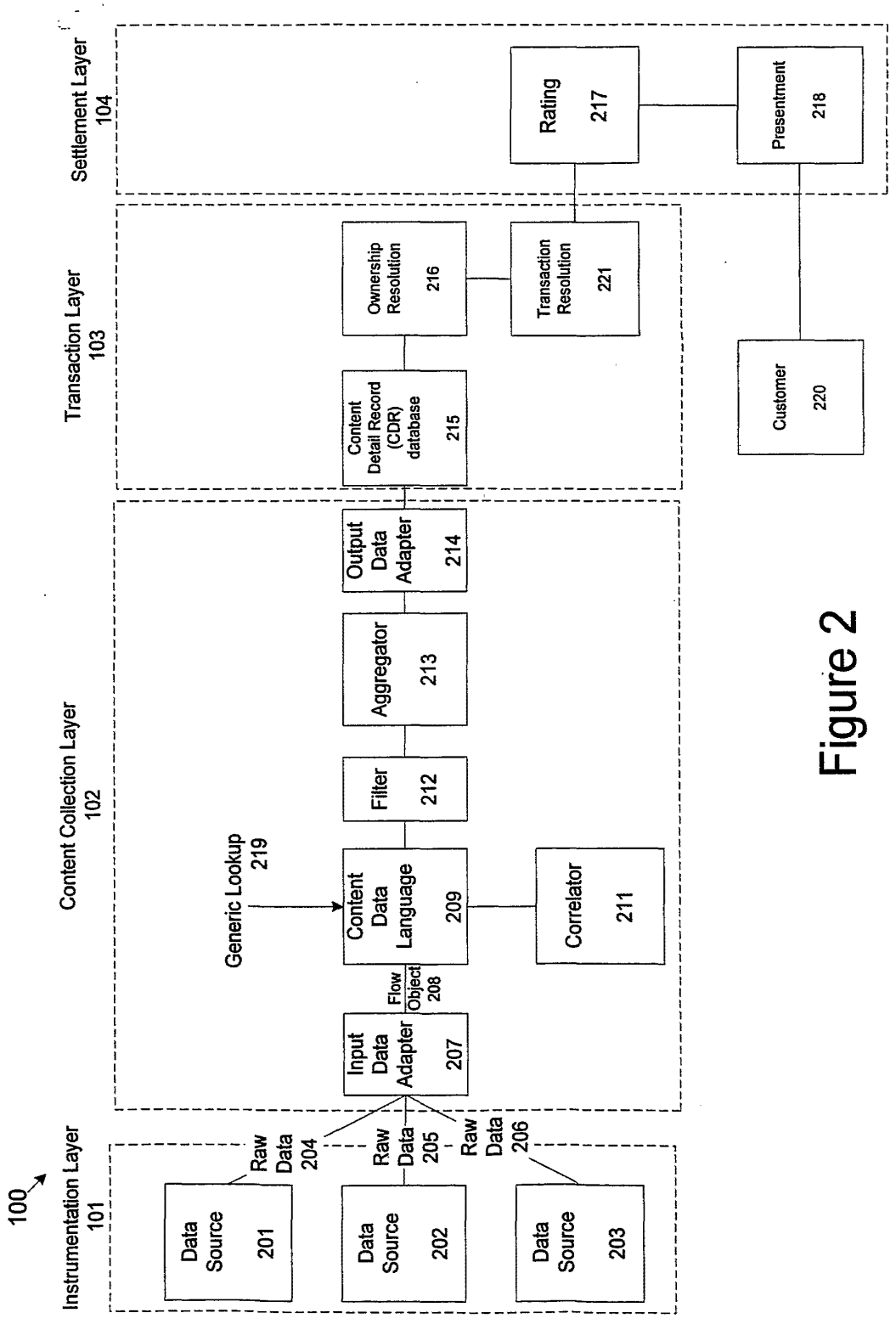

100
Instrumentation Layer 101
Data Source 201
Data Source 202
Data Source 203
Raw Data 204
Raw Data 205
Raw Data 206
Content Collection Layer 102
Input Data Adapter 207
Flow Object 208
Content Data Language 209
Generic Lookup 219
Correlator 211
Filter 212
Aggregator 213
Output Data Adapter 214
Transaction Layer 103
Content Detail Record (CDR) database 215
Ownership Resolution 216
Transaction Resolution 221
Settlement Layer 104
Rating 217
Presentment 218
Customer 220

Figure 2

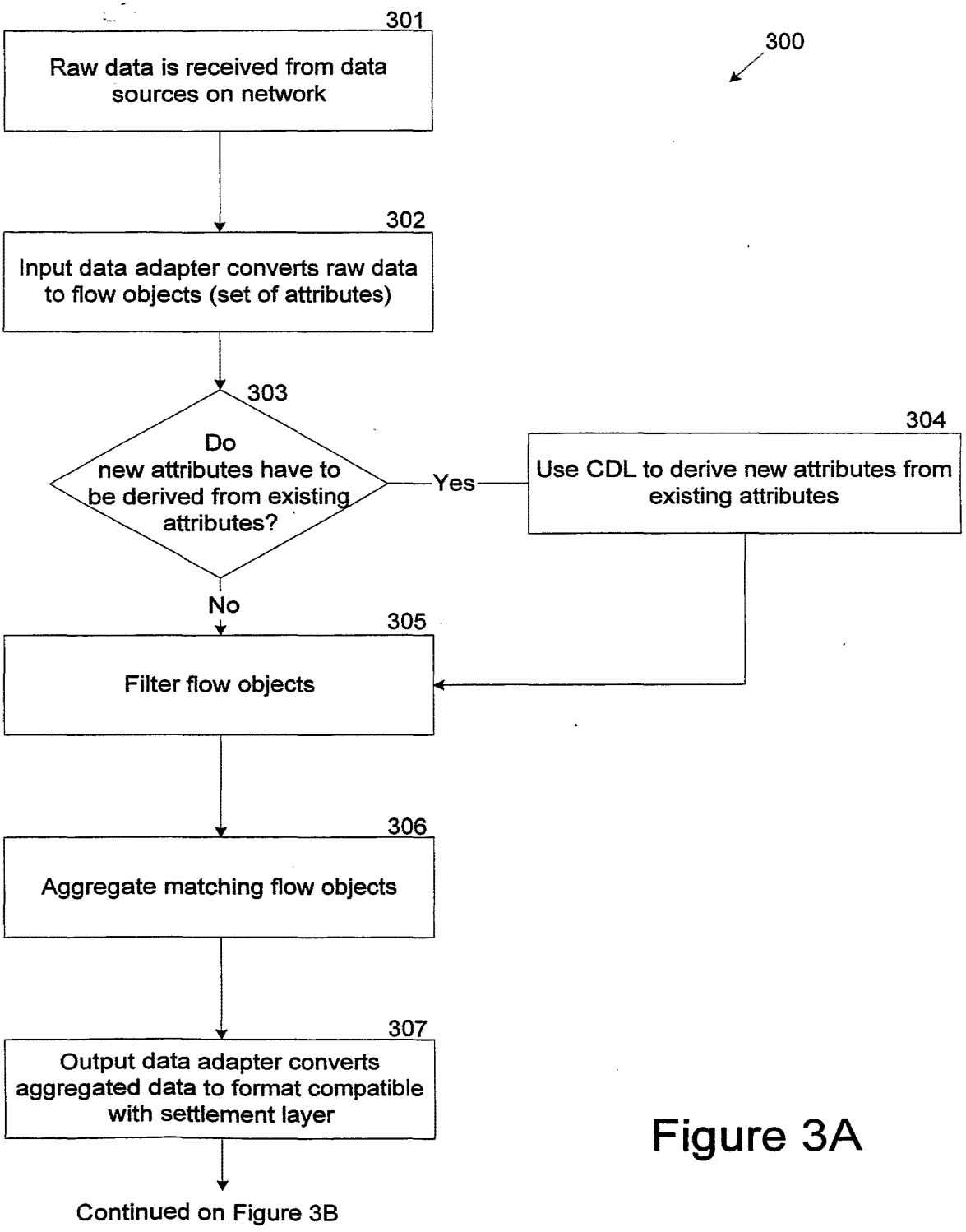

300
301
Raw data is received from data sources on network
302
Input data adapter converts raw data to flow objects (set of attributes)
303
Do new attributes have to be derived from existing attributes?
Yes
304
Use CDL to derive new attributes from existing attributes
No
305
Filter flow objects
306
Aggregate matching flow objects
307
Output data adapter converts aggregated data to format compatible with settlement layer
Continued on Figure 3B

Figure 3A

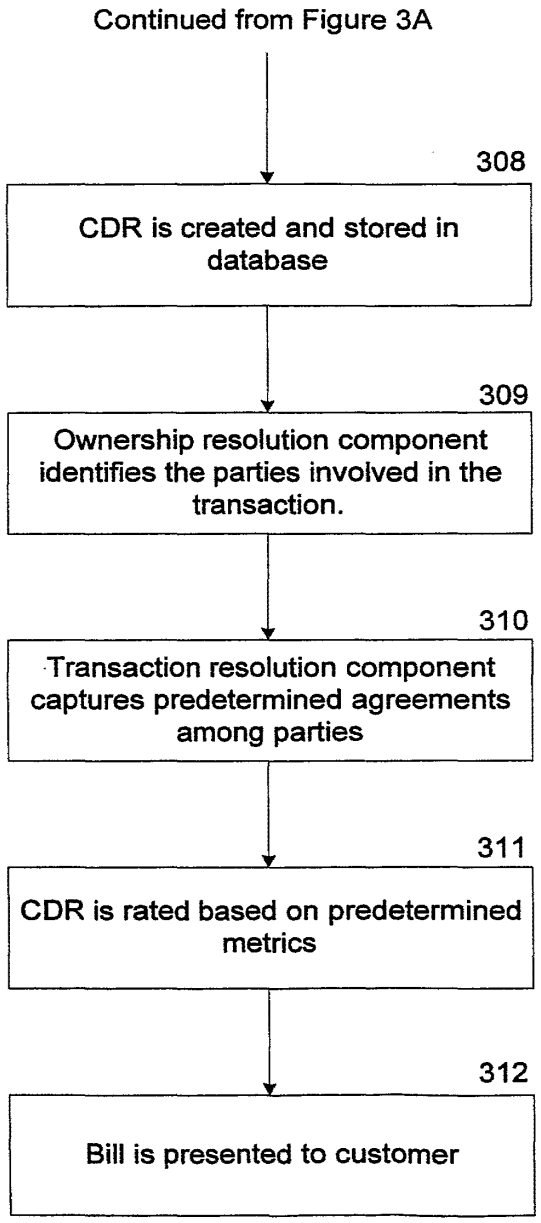

Continued from Figure 3A
308
CDR is created and stored in database
309
Ownership resolution component identifies the parties involved in the transaction.
310
Transaction resolution component captures predetermined agreements among parties
311
CDR is rated based on predetermined metrics
312
Bill is presented to customer

Figure 3B

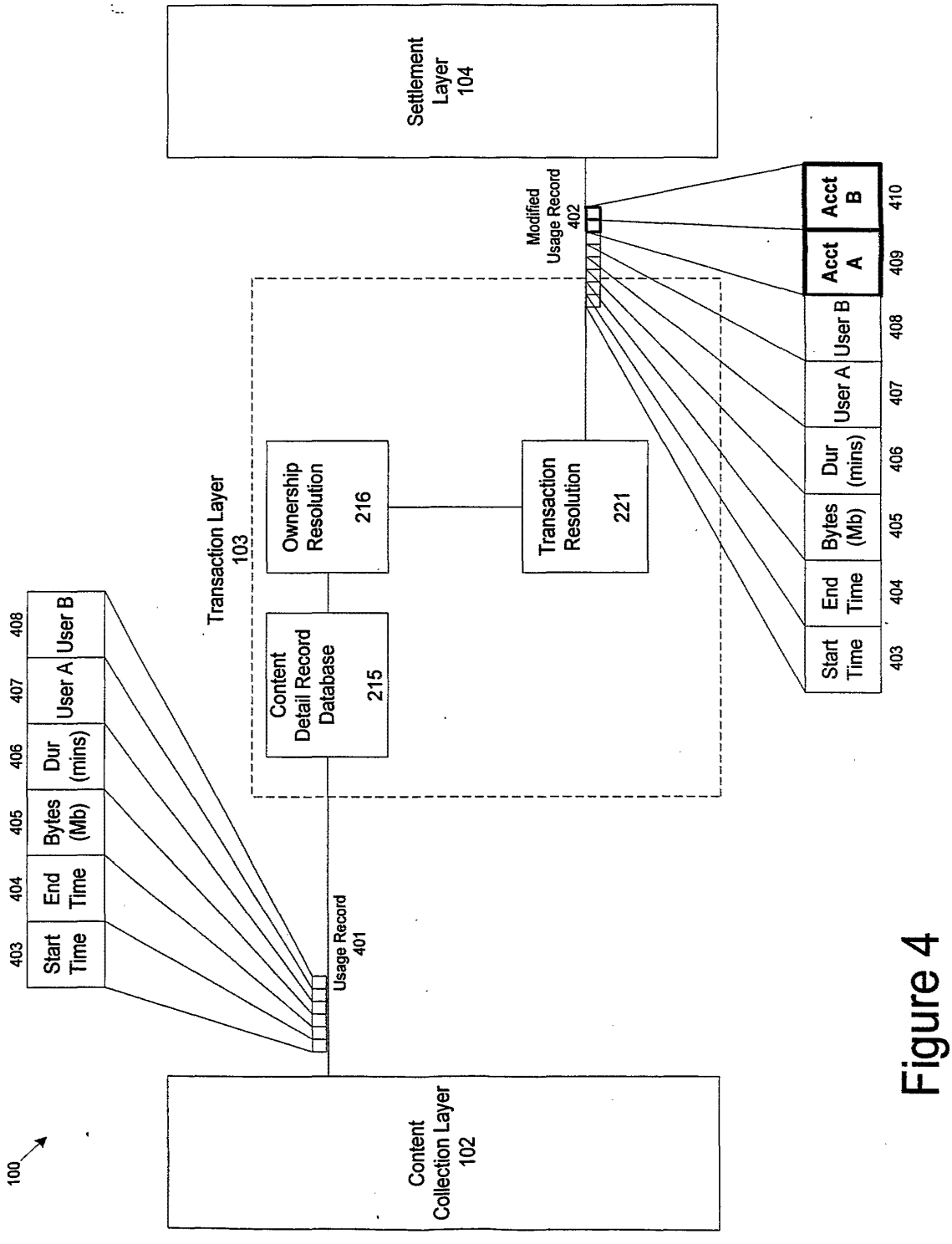

100
Content Collection Layer 102
Settlement Layer 104
Transaction Layer 103
Content Detail Record Database 215
Ownership Resolution 216
Transaction Resolution 221
Usage Record 401
Modified Usage Record 402
403 Start Time
404 End Time
405 Bytes (Mb)
406 Dur (mins)
407 User A
408 User B
409 Acct A
410 Acct B

Figure 4

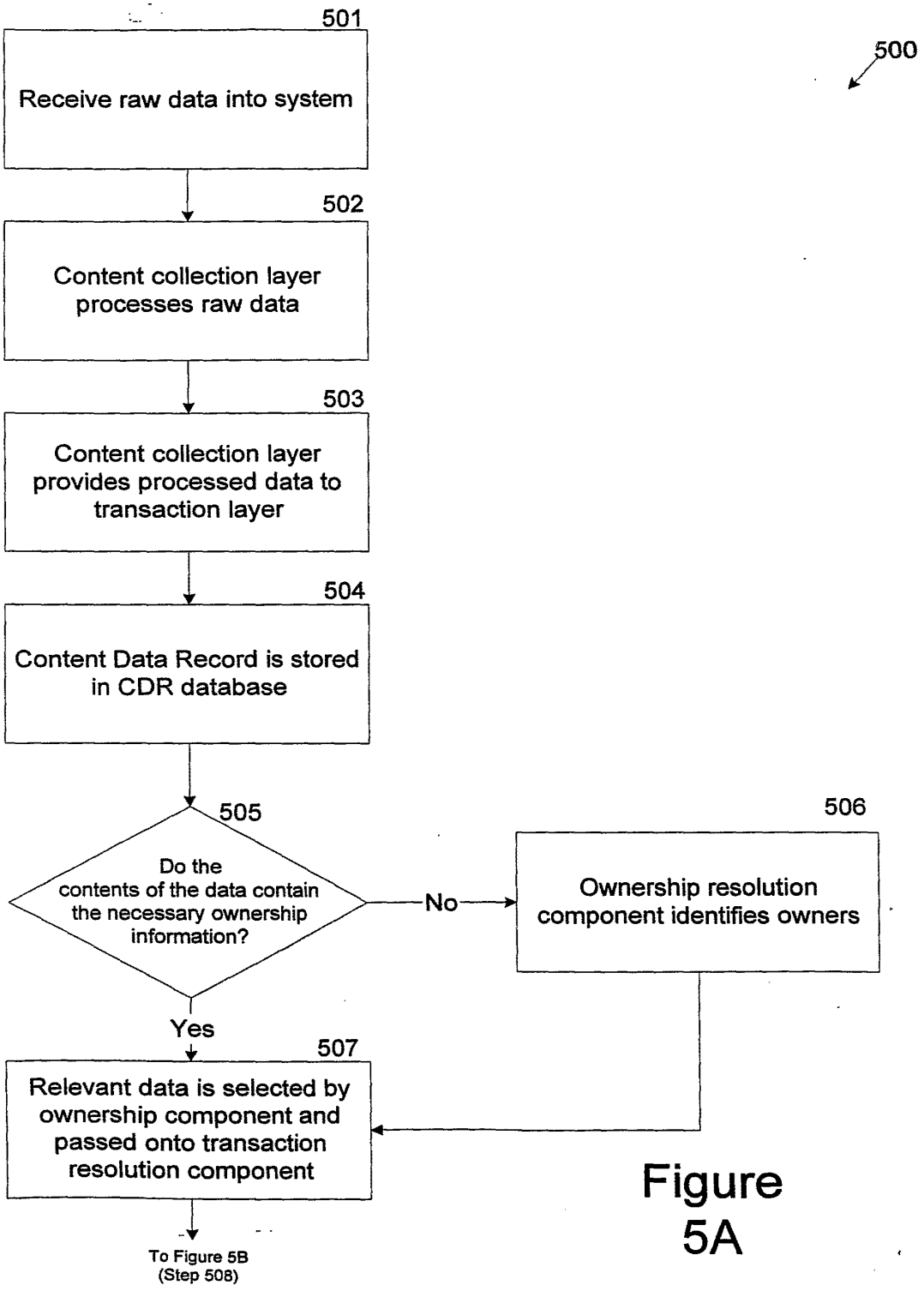

500
501
Receive raw data into system
502
Content collection layer processes raw data
503
Content collection layer provides processed data to transaction layer
504
Content Data Record is stored in CDR database
505
Do the contents of the data contain the necessary ownership information?
No
506
Ownership resolution component identifies owners
Yes
507
Relevant data is selected by ownership component and passed onto transaction resolution component
To Figure 5B (Step 508)

Figure 5A

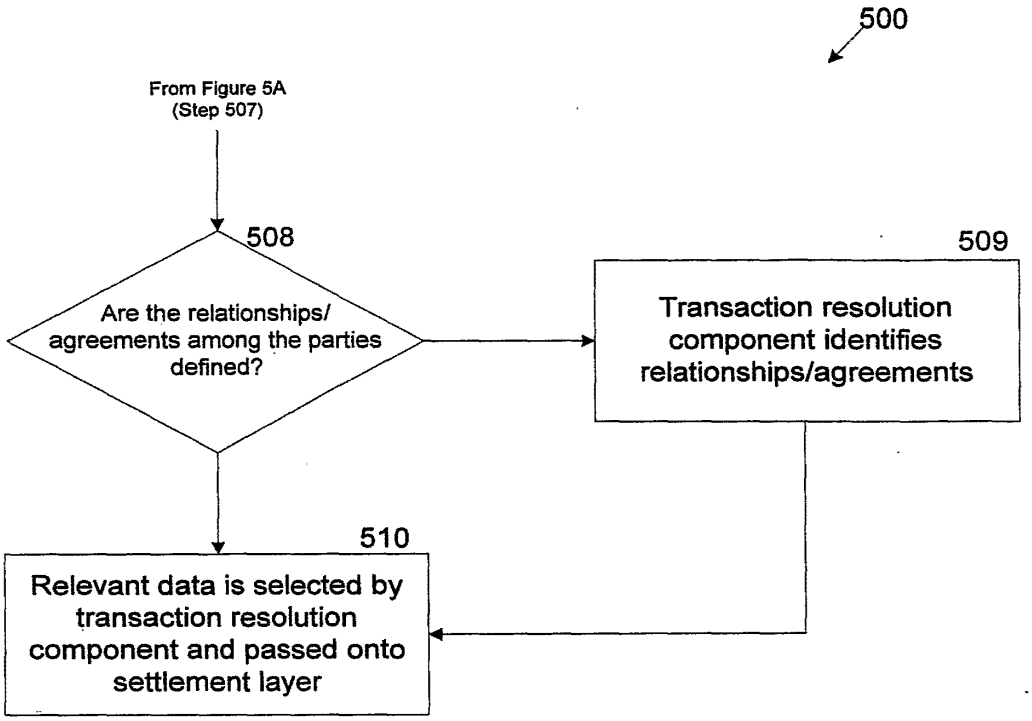

500
From Figure 5A
(Step 507)
508
Are the relationships/ agreements among the parties defined?
509
Transaction resolution component identifies relationships/agreements
510
Relevant data is selected by transaction resolution component and passed onto settlement layer

Figure 5B

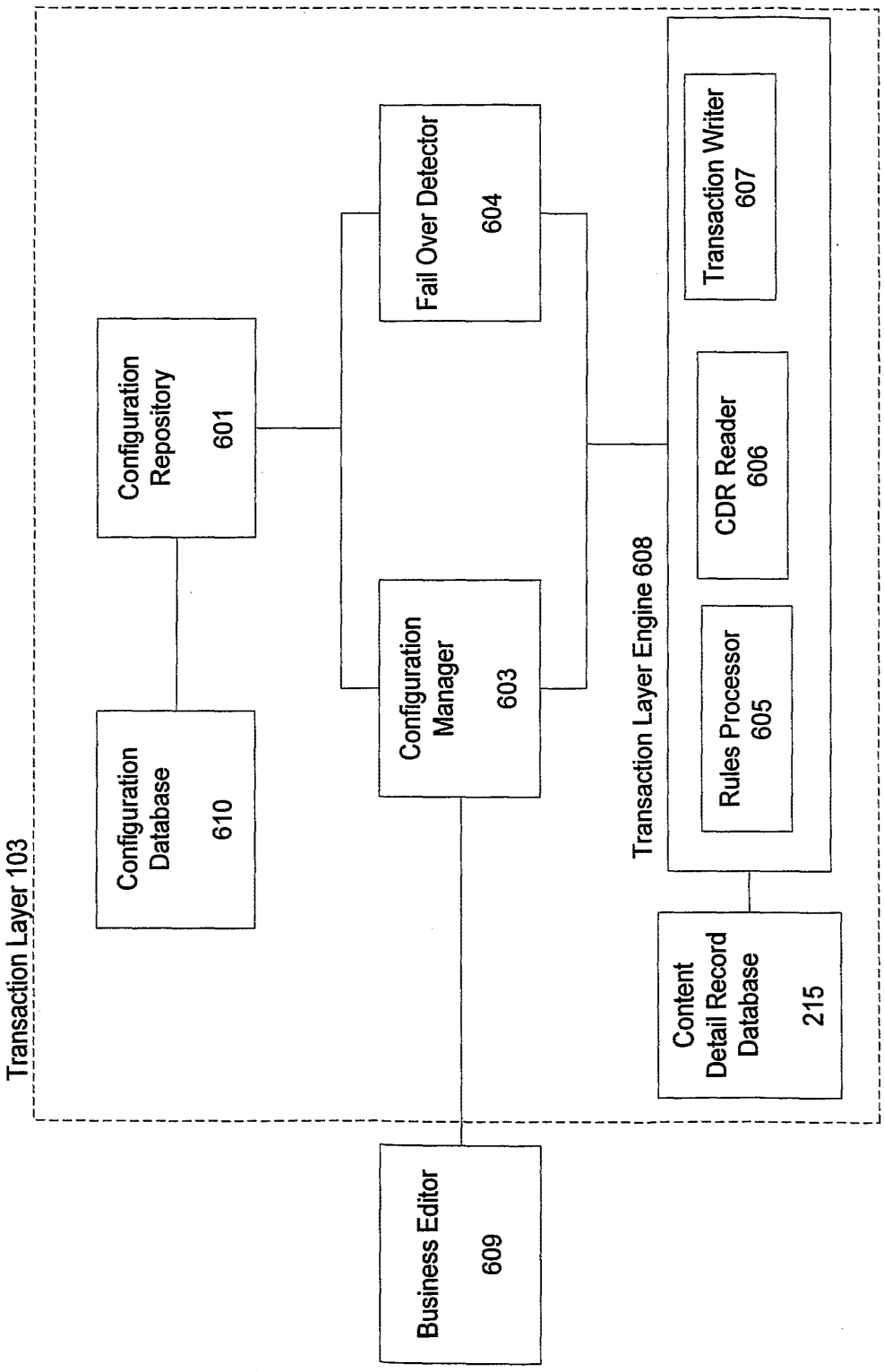

Transaction Layer 103
Configuration Repository 601
Configuration Database 610
Fail Over Detector 604
Configuration Manager 603
Transaction Layer Engine 608
Transaction Writer 607
CDR Reader 606
Rules Processor 605
Content Detail Record Database 215
Business Editor 609

Figure 6

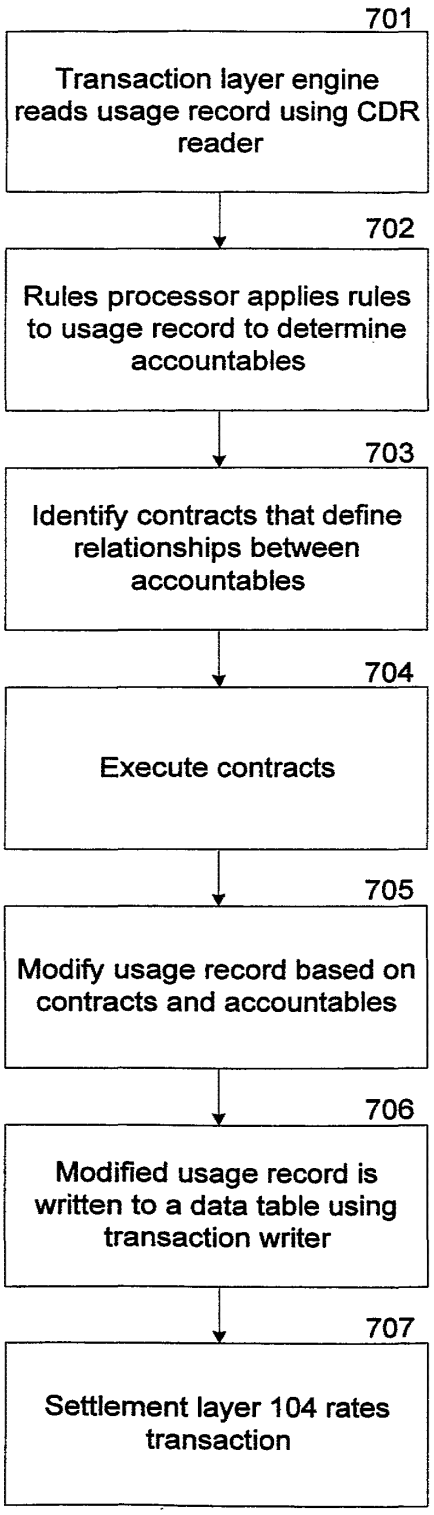

701
Transaction layer engine reads usage record using CDR reader
702
Rules processor applies rules to usage record to determine accountables
703
Identify contracts that define relationships between accountables
704
Execute contracts
705
Modify usage record based on contracts and accountables
706
Modified usage record is written to a data table using transaction writer
707
Settlement layer 104 rates transaction
700

Figure 7