

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04Q 7/32 (2006.01)

H04L 9/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 03157592.7

[45] 授权公告日 2006 年 10 月 4 日

[11] 授权公告号 CN 1278575C

[22] 申请日 2003.9.24 [21] 申请号 03157592.7

[30] 优先权

[32] 2002. 9. 24 [33] FR [31] FR0211803

[71] 专利权人 法国无线电话公司

地址 法国巴黎

[72] 发明人 吉恩·菲利普·万瑞

审查员 李秀琴

[74] 专利代理机构 北京集佳知识产权代理有限公司

代理人 王学强

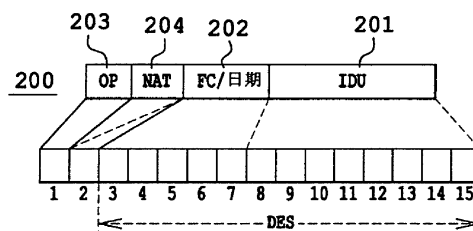
权利要求书 2 页 说明书 16 页 附图 2 页

[54] 发明名称

由服务提供者产生多媒体隔离标识符的方法

[57] 摘要

为保护一移动电话操作者的用户的保密性，该操作者产生一分离标识符，用户可通过该标识符与一内容提供者匿名地连接。该操作产生者是能够使该分离标识符和请求的用户相联系的唯一实体。分离标识符进一步为分离会话标识符，其在每一次用户与提供者的连接中均改变，或为分离上下文标识符，其可在几次连接中都不变。此外，上下文标识符与一用户/提供者对相适应。其进一步分离该用户。该分离标识符的格式与在电话标准中定义的李DS字段的格式兼容。



- 1、一种用于由服务提供者的网关产生与电话网络的标识符兼容的第一多媒体用户隔离标识符的方法，其中在产生步骤中，所述网关产生：
最大大小为 15 位的第一标识符；
- 5 具有至少一个产生位的第一标识符，该产生位可指示该标识符的产生者，
具有至少一个特性限定位的第一标识符，该特性限定位使能限定该第一标识符的特性，
具有 N 个识别位的第一标识符，该识别位使能对所述用户的指示，
10 具有 M 个可变性位的第一标识符，该可变性位依赖于所述特性限定位。
- 2、根据权利要求 1 的方法，其中的位是在数据处理中，能够实现对十进制数进行编码的表示。
- 3、根据权利要求 1 的方法，其中的位是在数据处理中，能够实现对
15 十六进制数进行编码的表示。
- 4、根据权利要求 1-3 中任何一个的方法，其中，所述标识符位对应于该用户的电话号码。
- 5、根据权利要求 4 的方法，其中，该标识符位优选为 8-15 位，而 N 等于 8。
- 20 6、根据权利要求 1-3 中任何一个的方法，其中该产生者位优选为位 1。
- 7、根据权利要求 1-3 中任何一个的方法，其中该特性限定位优选为编号为 2 的位。
- 8、根据权利要求 1-3 中任何一个的方法，其中该 M 位，优选为编号为 2-7 的位，使能对日期进行编码。
- 25 9、根据权利要求 1-3 中任何一个的方法，其中该 M 位，优选为编号为 2-7 的位，使能以月/日/时(mmddhh)格式对日期进行编码。

10、根据权利要求 9 的方法，其中用于编号为 2 的位的值 0 或 1 对应于一时间标识符。

11、根据权利要求 1-3 中任何一个的方法，其中，该 M 位，优选为编号为 2-7 的位，代表从当前年的起始所经历的时间段，以若干个
5 1/900000 来表示。

12、根据权利要求 11 的方法，其中，用于编号为 2 的位的值 0、1、2、3、4、5、6、7 或 8 对应于一时间标识符。

13、根据权利要求 1-3 中任何一个的方法，其中，该 M 位，优选为编号为 2-7 的位，代表自当前年的起始所经历的时间段，以若干个
10 1/800000 来表示。

14、根据权利要求 13 的方法，其中，用于编号为 2 的值 0，1，2，3，4，5，6 或 7 对应于一时间标识符。

15、根据权利要求 1-3 中任何一个的方法，其中该 M 个可变性位使能对内容提供者的识别。

15 16、根据权利要求 15 的方法，该 M 位中的 M-1 位使该内容提供者能够被识别，而该 M 位中的 1 位能够实现对该用户和服务提供者之间的合同的识别。

17、根据权利要求 1-3 中任何一个的方法，其中该标识符位和可变性位被加密。

20 18、根据权利要求 17 中的方法，其中该加密算法为对称的且产生位。

由服务提供者产生多媒体隔离标识符的方法

技术领域

5 本发明的目的是提供一种由服务提供者产生多媒体隔离标识符的方法。本发明的领域是用户通过服务提供者对内容提供者的访问。具体地，本发明的领域涉及电话网络和因特网、语音或 SMS 网络，或用于传送多媒体和非多媒体内容的其他载体之间存在的网关领域。

10 背景技术

 在现有技术中，内容提供商可通过几种方法来识别访问其一种服务的用户。这些方法依赖于用户用来访问该服务的介质。主要可以识别四种模式的访问，但是该列表内容并非是穷尽的。第一种模式的访问是因特网型访问。该因特网访问模式本身可被分为两个子模式，分
15 别称为连接模式和非连接模式。该连接的因特网模式为使用 HTTP（超级文本传输协议）或 WTP（无线传输协议）类型协议的连接模式。服务器，例如，HTTP 服务器，是根据 HTTP 协议与网络，例如因特网通信的设备。该服务器用作主机网页（因特网）或 WAP（无线应用协议）类型网络的主机。还有一种使用 STMP（简单邮件传输协议）
20 类型协议的非连接的因特网接入模式，其中该连接实际上包含邮件型电子消息的交换。

 另一种访问模式是操作者访问模式。该模式本身也被再分为两个子模式。第一访问子模式，其构成第三访问模式，则为可被称做非连接模式的访问模式。该模式使用 SMS（短消息服务）或 MMS（多媒体
25 体消息服务）类型协议。第四访问模式是由操作员访问的连接模式，还被称做语音模式，其中该访问用户与语音服务器联接。

 所有四种访问模式都具有一种简单的解决类型，其在于在与服务器连接期间产生界面，提示输入标识符和密码。由于与内容提供者的

服务器联接的用户通过移动电话进行操作，该可用于使用户键入其标识符（或登录用户名）和密码的方法受到该电话的用户界面的限制。该标识符或密码均完全为数字，在该情况下，它们难于记忆且易于被猜中，或者该标识符和密码包括字母和数字的混合，在这种情况下，
5 使用仅具有 9 个键的键盘输入密码是很冗长乏味的事情。此外，该键入步骤对用户来说是附加步骤，在大多数情况下，使移动电话用户放弃使用标识符和密码与提供该类型连接接口的站点联接。

另一种方法，在第一种类型的服务器的情况下，在于使用 cookie 应用程序。Cookie 是记录在用户机器内的小文件。在连接至内容提供者期间，该内容提供者可访问该 cookie 以识别该用户。该方法存在的一个问题在于有可能通过电子或其他方法来偷窃 cookie。由此使用 cookie 不符合高安全性的要求。另一个问题在于 cookie 的声誉相当差。这会刺激用户清除它们。此外，该用户可配置他用于与上述内容提供者联接的应用程序或导航器，使得该应用程序不接受 cookie。在
10 此情况下，该用户就无法与内容提供者的服务器联接。

对于第三和第四种访问模式，内容提供者最通常的是访问呼叫服务器的个人的电话号码。该内容提供者由此能够通过该电话号码识别这个人。这必定会引起保护隐私的问题。实际上，在他或她联接内容提供商的服务器时，对用户来说他不想被物理识别是非常合法的。实际上，有可能不具名地获得一篇文章。在该情况下，有可能在屏蔽个人号码的情况下进行尝试并获得联接。然而，在此情况下，该服务不可能被计价，且由此不可能进行有效的连接。当前，唯一的解决在于
20 不与该内容提供者联接。

此外，现有技术中存在的解决方案不能完全解决该数据格式的问题。实际上，传输特性因网络的不同而不同，且由此因协议的不同而不同。这些特性主要与发送的信息（数字、字母数字和其他信息）的编码以及可被发送的信息量有关。由此，可用于因特网上的标识符不
25

一定能够用在语音和/或 SMS 网络上。

在本说明书中，以及实际上，与内容提供者联接或访问内容提供者等效于与内容提供者的服务器联接。

本发明通过实现标识符的产生来解决这些问题，所述标识符是用户对该内容提供者出示的标识符，不管网络是何类型，该标识符仅使产生该标识符的实体识别该用户的民事状况。该标识符使得保护该用户的私密性成为可能且使得能够通过寻求识别用户的授权方产生的请求正确地识别该用户，且所述请求包括该标识符以及产生该标识符的日期。

根据本发明的标识符包括至少一个第一用户标识符字段。其它字段确保该标识符的可变性，和/或该标识符的限定条件。可通过随机变量或通过用户表明的期望来确保该可变性。标识符的限定条件包括用于给出与该标识符的特性有关的解释线索的信息。这些线索例如为产生该标识符的操作者，标识符的使用期限等等。该第一字段被加密为使得该第一字段不能被任何人访问。仅有服务提供者，即产生该隔离标识符的实体能够解除该加密，由此物理识别该用户。

根据本发明的标识符的所有字段，包括该加密的字段，其格式与其中传递该标识符的网络的绝大多数约束边界相容。实际上，该条件与电话网络及其用于定义标识符的约束有关。电话网络实际上强制了用于该标识符的最大字段和数字编码。

因此真正实现了本发明的目的。

发明内容

本发明的一个目的是维护用户的私密性。

本发明的另一个目的是保护网络操作者的客户数据库，以及限制行为分析的活动。

本发明的另一个目的是有助于保护邮件或通信的保密性。

本发明的另一个目的是使授权法律实体能够识别用户的民事状况。

本发明的再一个目的是使内容提供者管理用于与所述内容提供者连接的用户的一个或多个上下文。

5 本发明的另一个目的是保持与最大数量的网络兼容。

因此本发明的目的是提供一种由服务提供者（112）产生与电话网络的标识符（ID）（117）兼容的第一多媒体用户标识符（118，200）的方法，其中：

该第一标识符的最大长度为 15 位，

10 该第一标识符至少具有一个产生位，使其有可能标明该标识符的生产者，

该第一标识符至少具有一个特性定义位，从而能够定义该第一标识符的特性，

该第一标识符具有 N 个能够标明该用户的识别位，

15 该第一标识符具有 M 个由特性定义位而定的可变位。

附图说明

从以下说明和附图能够更清楚地理解本发明。给出这些附图纯粹用于表示，而决不是用于来限制本发明的范围。在这些附图中：

20 图 1 示出用于实施根据本发明的方法的装置。

图 2 示出用于根据本发明的一隔离标识符的可能的结构。

图 3 示出实施根据本发明的方法的步骤。

具体实施方式

25 图 1 示出用户使用的用于与内容提供者的服务器（FC）102 联接的设备 101。实际上，设备 101 是能够根据若干协议建立连接的移动电话。这些协议包括因特网兼容、语音兼容以及 SMS 兼容的协议。

换句话说,设备 101,即移动电话 101,能够根据 WAP 模式、语音模式和/或 SMS 模式建立通信。

服务器 102 能够根据上述提及的用于电话 101 的至少一种协议进行通信。该服务器 102 具有一微处理器 103,连接至该服务器 102 内部的总线 104。该总线 104 可用于将该微处理器连接至程序存储器 105、用户存储器 106 以及用于例如与因特网 108 连接的接口电路 107。

存储器 105 具有若干指令代码,其在微处理器执行不同的操作时,用于控制该微处理器。具体地,存储器 105 具有用于执行上述至少一个协议的指令码。

存储器 106,例如,为一数据库。为达此目的,该存储器 106 被描述为一表格,其包括的行数至少和可能与服务器 102 连接的或已经与该服务器 102 连接的用户一样多。每行具有一定数目的字段。列 106a 对应于用户标识符字段。这是根据本发明的标识符。当服务器 102 接收到一请求时,该请求包括该标识符。这使得服务器 102 能够识别该用户,且例如确定该用户的首选项 (preference)。一组首选项也被称做上下文 (context)。上下文包括不同的信息,用户可以通过这些信息自定义他所连接的服务器呈现给他的信息的外观和内容。

在该例中,存储器 106 包括在服务器 102 中。实际上,该存储器/数据库 106 可以以该服务器 102 连接的另一个服务器为主机,以访问所述数据库的内容。

当用户使用待连接至该设备 101 的服务器 102 时,电话 101 建立与基站 110 的射频连接 109。基站 110 本身通过网络 111,例如一 ISDN 网络,被连接至服务提供者的网关(GW)112,其中,例如,电话 101 的用户为该服务提供者的用户。该 ISDN 网络 111 实际上是一交换电话网络的全部或一部分。实际上,该网络 111 可构成用于将基站连接至该服务提供者的网关 112 的无论什么样的技术方案。服务提供者例如为一移动电话操作者。

该内容提供者，例如是该因特网的访问网关，也即通常所说的因特网入口、天气预报语音服务器或标准 SMS 服务器。

网关 112 具有微处理器 113，连接至总线 114。该总线 114 还具有与其连接的下列电路：用于与网络 111 接口的接口电路 115 和用于
5 与网络 108 接口的电路 116。由此该网关 112 为网络 111 和 108 之间的网关。

在该网络 111 上，该设备 101 以及由此其用户由一用户标识符（IDU）117 识别。在该网络 108 上，该设备 101 的用户至少通过隔离标识符 118 被识别。该网关 112 的一个作用是建立标识符 117 和隔离标识符 118 之间的联接。网关 112 的另一个典型的作用是在网络 111
10 上使用的协议和网络 108 上使用的协议之间的进行协议转换。该标识符 117，例如，为该设备 101 的用户的电话号码。该标识符 117 为公共标识符，其使每人都能使实际人与其相联系。本发明的一个目的是防止该内容提供者物理识别连接至该服务器 102 的个人。

15 该网关 112 具有一程序存储器。该存储器 119 具有包括指令代码的不同的区域，每一个区域对应于由该微处理器 113 执行的任务。

该存储器 119 的区域包括区域 119a，其包括对应于由网关 112，即实际上由微处理器 113 从至少该标识符 117 产生隔离标识符(IDI) 118 的指令代码，且在一优选实施例中，包括对应于该内容提供者的
20 标识符 120 产生的指令代码。

区域 119b 具有使网关 112 能够在该网关 112 收到来自该服务器 102 的请求时验证标识符 118 的指令码。区域 119c 具有使网关 112 由隔离标识符 118 识别用户的指令码。这被用于例如将来自服务器 102 的响应发送到设备 101。存储区域 119d 具有用于从该内容提供者的
25 标识符 120 确定标识符修正符的指令码(DNS)。区域 119e 具有用于执行代码转换操作的指令码，在该例中，代码转换操作为加密操作。优选地，这是一种对称的加密操作。然而，它也可能是简单的排列或

扰频操作。

该网关 112 具有一存储器 121，用于联系内容提供者的标识符和该内容提供者的代码，以及待被产生的一隔离标识符的特性的标识。

图 2 示出根据本发明的隔离标识符的可能的结构以及其通过在电话标准等级中定义的，尤其是在语音电话标准中定义的 NDS 字段适用于从电话网络的传输。该标准规定 NDS 字段的 15 位编码。服务提供者不必使用由该标准设定的全部的空间来识别用户。然而，该网络协议总是传送用于 NDS 域的 15 位，其由此可被用于传送识别用户的信息以及附加的信息。

图 2 示出包括四个字段的隔离标识符 200。长度为 N 位的第一字段 201 对应于识别该网络 111 上的设备 101 的用户的标识符 117。长度为 M 位的第二字段 202 对应于使该隔离标识符 200 随用户的要求或内容提供者代码而变的装置。字段 202 和 201 借助于区域 119e 的指令代码被加密。

在一种变形中，该隔离标识符 200 具有一字段 203，通过该字段有可能识别产生该标识符的服务提供者，和例如有可能对用于该隔离标识符 200 的版本或特性进行编码的字段 204。该隔离标识符 200 在网关 112 和服务器 120 之间进行通信期间用作隔离标识符 118。在该服务器 102 的用户存储器 106 的列 106a 中记录的是隔离标识符 118。

图 2 示出该标识符 200 的各个字段的长度的总和不出 NDS 字段的长度，即 15 位。一位是用于代表/编码十进制数字的计算机表示。实际上，一个十进制的位包括四个二进制的位，且仅使用编码 0000，0001，0010，0011，0100，0101，0110，0111，1000 和 1001。总的原则是该十进制位能够编码 16 种状态。总的来说，仅使用这十种状态。因此选择该 16 种状态的任何 10 种状态均适用。图 2 还示出用于字段 201-204 的长度。该标识符的这些字段的长度可用于该情况。由此，例如，如果期望字段 203 具有更多位，则可缩短字段 201 或 202。

类似的，该字段的位置是指示性的。例如，在当前例子中，该字段 202 占 3-7 位；实际上，如果 M 等于 5，则它可占去该 NDS 字段的 15 位中的 5 位。这对字段 201，203 和 204 的位置也适用。

图 3 示出其中实现根据本发明的方法的方案的步骤。

- 5 图3示出步骤301，其中电话101向内容提供者102发送一条请求 (U GET)。该请求包括一个用户标识符117，一个内容提供者标识符 120，以及一个包括该请求本身的字段122。这种请求是，例如，如在 HTTP协议中所定义的一个“Get”请求。需要注意：由于设备101是一个移动电话，所以它利用的是WTP协议。在步骤301产生并且发送的
- 10 请求在步骤302中由网关112接收。在步骤302中，微处理器113从请求中提取内容提供者标识符120。然后扫描表121以查找该内容提供者标识符。一旦找到该内容提供者标识符，微处理器113能够确定用于该内容提供者的代码以及一标识符特性。如果在表121中没有出现内容提供者的标识符，则微处理器113采用缺省的工作模式。在本实例中，
- 15 假设该缺省的工作模式在于产生一隔离会话期标识符。

标识符120，在一优选的实例中，是采用IPV4(因特网协议版本4)格式的地址。也可以是一个语音服务器的电话号码，或者SMS或MMS标识符。它也可以是一个采用IPV6(因特网协议版本6)格式的因特网地址或者URL(统一资源定位符)。

- 20 如果，在表121中，内容提供者标识符120对应于一个隔离会话期标识符的特性，则操作进行到步骤303用于产生一个隔离会话期标识符。否则，操作进行到步骤304，用于产生该隔离上下文标识符。

无论是隔离会话期标识符还是隔离上下文标识符，二者均具有图

2所示的相同结构。会话期标识符和上下文标识符的区别在于字段202的内容。在会话期标识符的情况下，字段202包括一段随机元素。该随机元素例如由从1970年1月1日00.00时开始经过的秒数构成。该随机元素也可以是由伪随机数产生器产生的任意数字，该伪随机数产生器是在产生该随机元素的时间启动的。该随机元素也可以是在每次新产生一个标识符时递增的计数器的值。通常，该随机元素为一个随机或伪随机数字。

在为上下文标识符的情况下，字段202包括，例如内容提供者识别符或日期。

10 在为日期的情况下，对于字段202，其可以使创建该隔离标识符的日期，或是该隔离标识符的有效性终止的日期。在一变化的实施例中，可能出现的情况是该会话期和隔离上下文标识符均由日期形成。在该情况下，可通过其有效性持续时间来识别一上下文标识符，其有效性持续时间远远长于会话期标识符，其有效性不超过四分之一个小时。

15 在步骤304中，字段202对应于在步骤302中在内存121中所读取的内容提供者代码。该内容提供者代码则优选为与该位格式兼容的位代码。

20 可以将字段204用于例如对标识符的特性进行编码。因此当其为隔离会话期标识符时，字段204是一个值，而当其为上下文标识符时，字段204为另一个值。当确定了字段202的值时，微处理器113能够产生一个根据本发明的隔离标识符。微处理器113对由字段202和字段

201所形成的字段组(set)进行加密。然后微处理器113使加密的结果与管理网关112的操作者相关联,并且与隔离标识符的特性204相关联。因此,得到隔离标识符118。可以看出隔离标识符的大小可以与标识符117的大小不同。

5 一旦已产生隔离标识符118,则操作进行到步骤305,用于产生一请求并且将该请求发送到服务器102。在步骤305中产生的该请求包括一个隔离标识符118,一个内容提供者标识符120以及一个请求字段123。在实际中,字段120和123与字段120和122是相同的。在本实例中,在步骤305中产生的请求是采用HTTP格式的。在此实例中,字段
10 120则是一个目的地IP地址。实际上,步骤305中由网关112所产生的请求采用与电话101的用户试图联接的服务器相兼容的格式(语音、SMS、IP等)。

隔离标识符字段 118 采用图 2 所说明的格式。隔离标识符 118 因此包括标识产生该隔离标识符操作者的字段,一个用于根据隔离标识
15 符为会话期标识符或者上下文标识符对其性质进行编码的字段,以及一个加密字段。该加密字段在被译码后,包括两个字段。这两个字段对应于字段 202 和 201。

在本发明中,有一种与 NDS 字段的格式联系的附加的约束。该
20 字段 118 必需与 NDS 格式兼容。这意味着该字段 118 的长度为 15 位,且字段 201 至 204 包含在该 15 位中。

不管当前考虑的情况如何,可以考虑该字段 201 能够识别该服务提供者的用户。典型的,该字段 201 将包括电话号码的有效位,即在法国为 8 位,在其他国家为 5 位或更多位。由此,在法国,字段 201 通过当前例子中为 8-15 位的标识符数字来记录。这代表 8 位,实

际上，其可以是该 15 位中的任何一个 8 位的组。由此剩余 7 位用于
字段 202-204。

该 7 个剩余位中的第一位，优选位数 1，被认为能够对产生该隔离标识符 200 的实体进行编码。当符合 NDS 字段格式标准时，这能够
5 能够对 10 个操作者型实体进行编码，当不符合这些标准时，能够对 5 个操作者(OP)型实体进行编码。该位还被称做产生者位，其对应于字段 203。

在一优选实施例中，该 7 个剩余位的第二位，例如位数 2，用于
根据一其是会话期标识符还是上下文标识符对该标识符的特性进行
10 编码。其还被称做特性(NAT)位；其对应于字段 204 且是可选择的。

在一种变体中，这些剩余位，在本例子中为第 2-7 位，用于例如
以月、日和时的格式对日期进行编码，每条信息占用两位。注意，在
该变体中，位数 2 对两条信息进行编码，一个与特性有关，另一个与
日期有关。在该特定情况下，假设位数 2 的值 0 或 1 对应于会话期标
15 识符，则编号为 2-7 的位被解释为日期。如果位数 2 等于 3，则编号
为 3-7 的位为内容提供者代码，且存在一上下文标识符。如果编号为
2 的位等于从 4-9 的数字，则其被保留供以后使用。

有其他可能的用于对日期进行编码的格式。例如，可以以一年的
若干份来计算从当前年开始的日期。如果我们考虑若干个一年的
20 1/900000，则位数 2 取值 0-8 意思是编号为 2-7 的位对日期进行编码，
且该标识符为时间标识符或会话期标识符。如果我们考虑若干个一年
的 1/800000，则位数 2 的值 0-7 表示编号为 2-7 的位对日期进行编码
且标识符为时间标识符或会话期标识符。

当位数 2 指示该标识符为上下文标识符时，则编号为 3-7 的位能
25 够对内容提供者进行编码。在该情况下，3-7 位中的一位还可用于对
合同的版本进行编码，由此所使用的电话号码的所有者一定向产生隔
离标识符的操作者产生隔离标识符。例如如果该号码的所有者改变，

或如果该号码的所有者想保持该号码不变,但想要擦除他对内容提供者的访问的任何踪迹,该合同号是有用的。

实际上,不对有关生产者和特性的信息进行加密。在当前例子中对应于数字 3-15 的其他信息被加密。该加密算法占用一个 13 位的字,且产生 13 位的字。由此,所产生的该隔离标识符 200 与规定数位使用的标准相兼容。所使用/产生的字的大小随被加密的信息量而变。

由此产生的该 NDS 格式标识符与所有现代的传输协议相兼容。

当在步骤305发送该请求(I GET)后,操作进行到步骤306,服务器102接收在步骤305发送的请求(I REC)。在步骤306中,服务器102因此访问字段118和123。字段118实现对表106的访问,以查找有关正与服务器102联接的用户的某些信息。实际上,如果是一个隔离会话期标识符,则表106几乎不可能包括有关该用户的信息。事实上,由于会话期标识符在每一次会话期时均改变,所以同一用户将不会与使用相同隔离会话期标识符的服务器102联接二次。对于本说明书,术语“会话期”应理解为限定的一段时间,例如一刻钟。可以容易地测量会话期的持续时间,由于根据本发明的隔离会话期标识符包括有关创建日期的一条信息。

上下文标识符可以具有一个更长的使用期限,例如6到18个月或者更多。上下文标识符的使用期限是由,例如,用于进行加密的密钥而管理的,该密钥以上下文标识符的使用期限的频率而改变。上下文标识符的使用期限也可以由以该上下文标识符的使用期限的频率而变化的字段202的内容来管理。

使用期限的选择,以及管理方式的选择,是由负责网关112的实

体决定的。使用期限得到保证的事实使内容提供者可以使信息，也称作上下文与隔离标识符相关联。

在步骤306的可能操作之中，服务器102可以产生并且向网关112发送一个来自标识符118的请求。这是步骤307。服务器可以将信息记录在表106中。这是步骤308。服务器可以产生并且发送对于来自电话101的用户的请求的响应(I REP)。这是步骤309。

当服务器102产生一个对于在步骤305所发送的请求的响应时，其建立一个响应帧，包括识别用户的字段118，包括进行响应的服务器的标识符的字段120，以及字段123，该字段则包括对于该请求的响应。在步骤310中，网关112接收针对在步骤301中发送的请求的响应（U REP）。网关112随即执行标识符118和117之间的代码转换以将来自于服务器102的响应发送到电话101。操作然后进行到步骤311，其中设备101接收针对在步骤301中发送的请求的响应（U REP）。

在步骤310中，对标识符的代码转换可以伴随对该标识符有效性的验证。此验证例如在对隔离标识符118的加密部分的加密之后，且由此在检索字段202的值之后进行。因此该验证依赖于该标识符的特性。如果是会话期标识符，则字段202对应于一日期。然后将该日期与接收响应的日期进行比较。如果在这两个日期之间的差大于一预定的时间段，例如一刻钟，则认为该请求是无效的，并且不会将其发送制至设备101。

如果是上下文标识符，则将字段202的内容与在表121中与对应于标识符120的行的代码字段的内容进行比较。如果匹配，则该请求是

有效的；如果不匹配，则该请求被拒绝。

在步骤307中，服务器102向服务器112发送一个服务请求(I
SERVICE)。该请求包括一个用户隔离标识符，一个内容提供者标识
符，以及一个请求字段。这种请求可以，例如与用户识别请求、定位
5 用户的请求，或者对于有关该设备的特性信息的请求，该用户使用该
设备与服务器102取得连接。此列表不是穷举的。在步骤312中，服务
器112接收该服务请求。在步骤312中，网关112以对隔离标识符的有
效性的验证而开始。此验证的实现如上所述。如果该标识符是无效的，
则操作进行到结束步骤319，在该步骤中网关112不符合该服务请求；
10 否则，操作进行到步骤314，响应该服务请求。

在本发明的一种变换方式中，对于每个内容提供者，表121还包
括一个内容提供者可以要求的服务列表。然后在步骤313中，网关112
验证发送该请求的内容提供者真正有资格发送此请求，即，该内容提
供者能够要求该服务。如果情况是这样，则网关112产生一个针对此
15 服务请求的响应，并且将此响应发送到服务器102。否则，不对该服
务请求作出响应。

在步骤314中，服务器102接收该服务请求的响应。此响应使服务
器102将表106升级或者产生步骤309的响应。事实上，可以设想在步
骤301所发送的请求是一个获知靠近用户所在位置的餐馆的列表的请
20 求。在此情况下，服务器102需要知晓用户的位置。因此服务器102
向网关112发送一个位置请求。对此位置的响应使服务器102可以向设
备101的用户发送适当的响应。

通过根据本发明的标识符，服务器102，在步骤315中，也可以向设备101发送一个压入(push)请求。此压入请求在步骤316中由网关112接收。此压入请求接受标识符118的验证。此验证与在步骤310以及312和313中所述的验证是相同的。换言之，由字段120所识别的内容提供者必须得到授权发送压入请求，并且标识符118应该是有效的。如果标识符是无效的，则操作进行到结束步骤319，在该步骤中对服务器所发送的压入请求没有给出任何肯定的响应。

如果步骤316显示在步骤315所发送的压入请求是有效的，则网关112将隔离标识符118译码为标识符117，并且将该经过译码的压入请求发送到电话101。在步骤317中，电话101接收并且处理此压入请求。这种压入请求是，例如对设备101中的数据升级。这种数据库可以与，例如，设备101的用户希望保持的联系相关，或者与设备101为访问不同的服务可能与之联接的服务器列表相关。

用于对字段202和201进行加密的加密算法优选地是DES(数据加密系统)系列算法。可以采用此算法的块式加密版或者连锁式加密版。该连锁式加密版可以实现确保标识符200的所有加密的部分由于可变字段202而不同。本发明的变形可以采用其他的加密算法，诸如AES(高级加密系统)系列算法。

本发明以及由其所定义的隔离上下文标识符的一个优点是一个用户对于每个内容提供者可以具有不同的上下文标识符。因此内容提供者不可能利用其他内容提供者的数据库对他的数据库进行核对，以便得到更多有关与标识符所识别的用户的私人生活的信息。也不可能

袭击数据库，或侵犯通信的保密性。由此，可最大程度地保护用户的私密性。

由于以标识符开始并且仅针对产生此标识符的操作者，有可能将一操作追溯到实际用户，因此法律方面的标准也可得到满足。

- 5 一个用户可以选择通过采用会话期标识符进行联接。因此，在时间上合理隔开的两个连接过程中，已做出这种选择的用户将通过出示两种不同的隔离标识符而联接到相同的站点。然后内容提供者则无法确定联接两次的用户是相同的用户。

- 10 用户可以选择对上下文标识符具有追索权(recourse)。此时，网关112在已做出这种选择的用户连接的过程中将生产一个隔离上下文标识符。然后该内容提供者将根据能够附加到隔离上下文标识符的信息而修改其响应。

通过使一用户标识符，诸如标识符117与用户的选择相关联的表，用户的选择在通过网关112上受到管理。

- 15 如果我们考虑用户采用个人计算机通过因特网服务提供者(或者ISP)而联接到内容提供者，则本发明是完全可换位的。在这种情况下，个人计算机和网关之间的连接模式是无线频率(GSM、UMTS等)模式，有线(交换电话网络)模式，或者其他类似模式。

- 20 本发明也具有使该管理隔离标识符的实体免于存储这些隔离标识符的优点。事实上，由于这些标识符是由数据而计算的，该数据在计算时可以容易地获得，因此不需要存储它们。

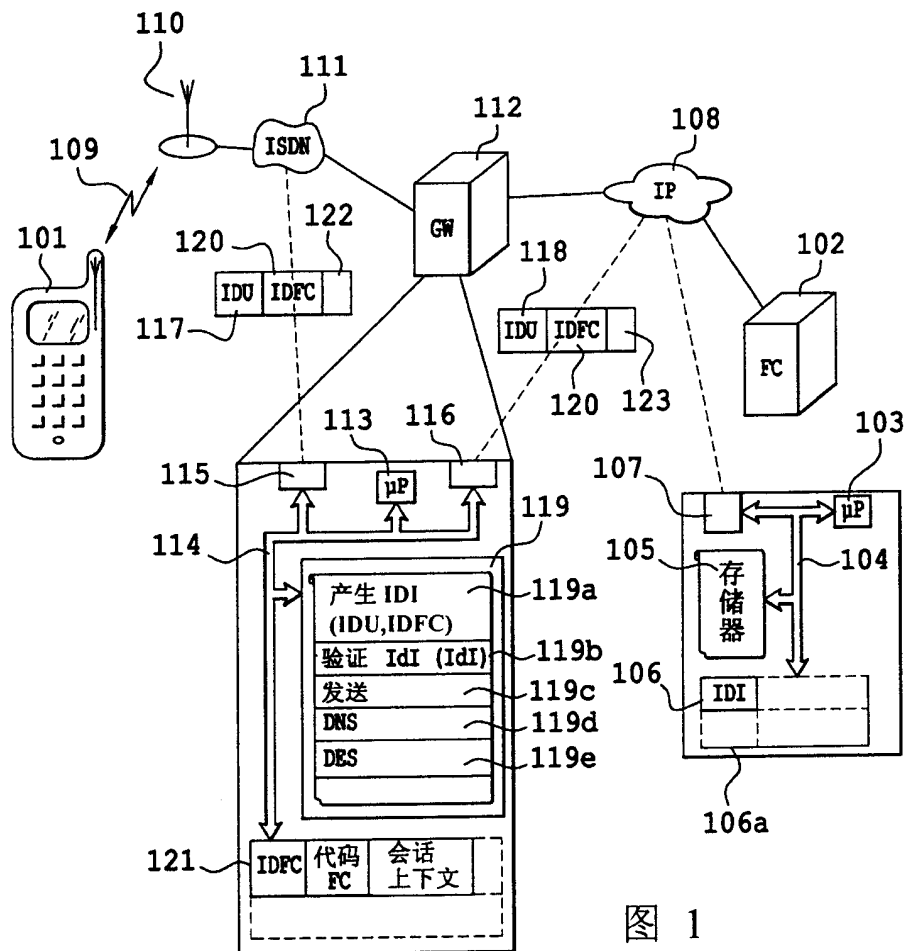


图 1

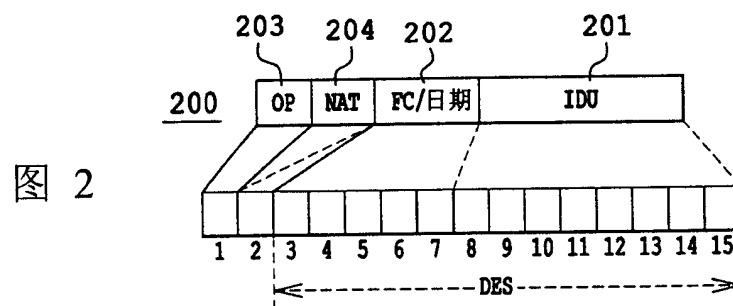


图 2

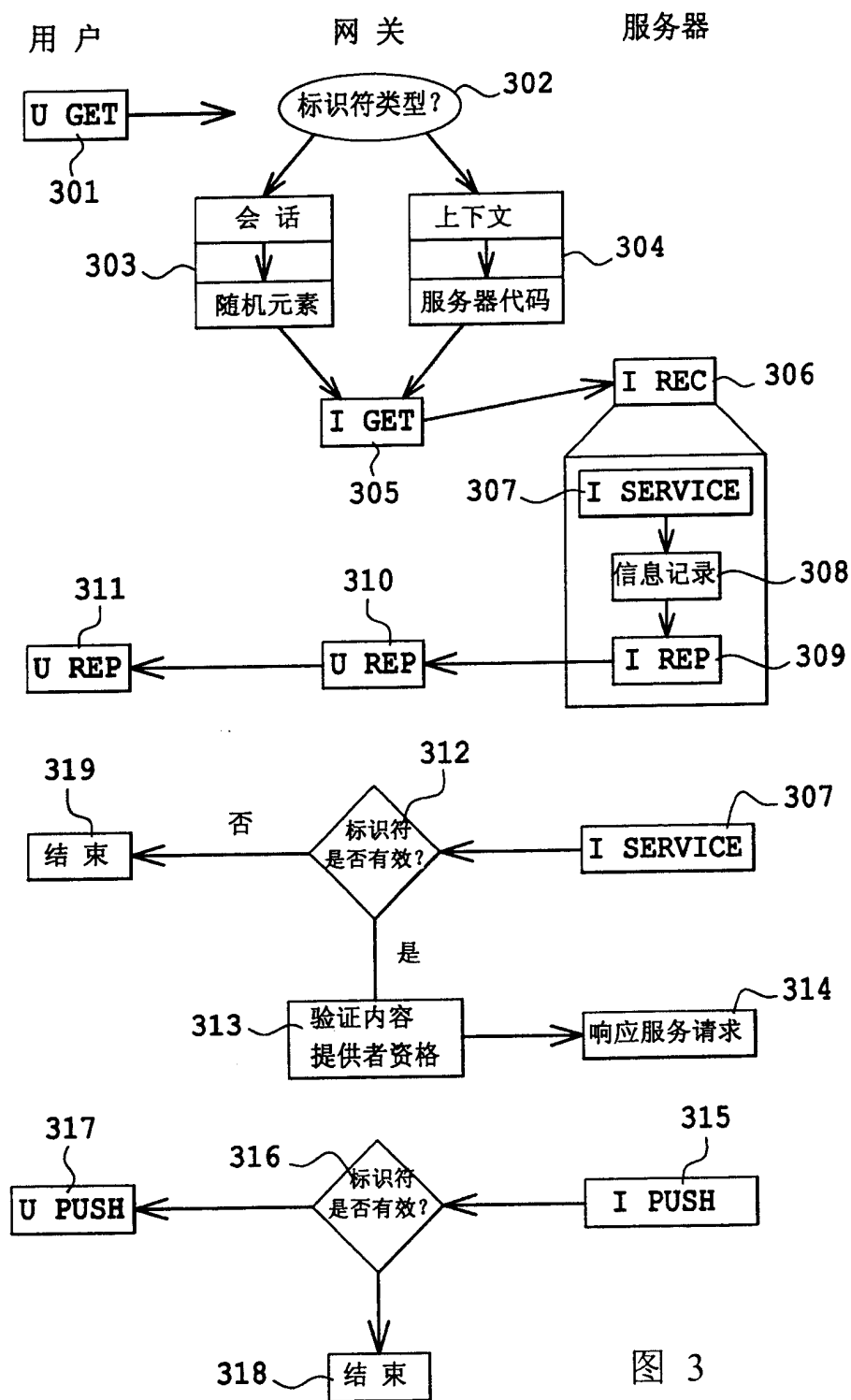


图 3