[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04M 3/42
H04Q 7/32 H04L 9/00
H04L 9/28

[12] 发明专利申请公开说明书

[21] 申请号 03157591.9

[43] 公开日 2004 年 5 月 12 日

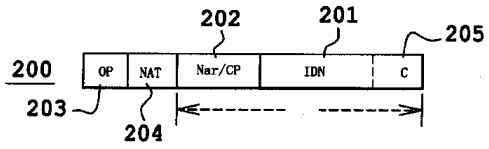
[11] 公开号 CN 1496089A

[22] 申请日 2003.9.24 [21] 申请号 03157591.9
[30] 优先权
[32] 2002. 9.24 [33] FR [31] FR0211808
[71] 申请人 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
[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 13 页 附图 2 页

[54] 发明名称 产生用于分离连接到电信息通信网络用户的第一标识符的方法

[57] 摘要

为保护拨号到一个移动电话操作者的用户的私密性，操作者产生一个分离标识符，通过该标识符用户能够匿名连接到一个内容提供者。 该操作者/产生者可以单独将分离标识符联系到请求的用户。并且，分离标识符是或者一个分离会话标识符，因此是一个在每次用户向提供者的连接中改变的标识符，或者是一个分离上下文标识符，因此是一个在数次连接中保持不变的标识符。 此外，上下文标识符与一对用户/提供者对相适应。 该方法甚至还分离了用户。



ISSN1008-4274

1．一种用于产生一个第一上下文标识符的方法，用于分离通过电信息通信网络和根据用户的使用由服务提供者设置的装置而获取与内容提供者连接的用户，该用户由服务提供者借助于第二标识符识别，其中：

该服务提供者的装置包括网关，用于使第一分离上下文标识符与第二标识符相关联，

该第一分离上下文标识符为其生成请求至少一个第一字段，用于建立第一分离上下文标识符与用户的关联，

该第一分离上下文标识符为其生成请求一个第二字段，用于确保作为内容提供者的函数的第一标识符的可变性，

对第一和第二字段进行代码转换。

2．如权利要求1所述的方法，其中所述的第一字段包括第二标识符。

3．如权利要求1或2所述的方法，其中第二字段的内容依从于存在于用户和服务提供者之间的合同。

4．如权利要求1到3中任一项所述的方法，其中分离上下文标识符的使用期限是由第二字段的内容管理的，该第二字段的内容以一确定的频率而变化，所述的确定频率成为该上下文标识符使用期限的频率。

5．如权利要求1到3中任一项所述的方法，其中上下文标识符的使用期是由用于执行代码转换的密钥而管理的，所述密钥以一确定的频率而变化，所述的确定频率因此成为上下文标识符的使用期的频率。

6．如权利要求1到5中任一项所述的方法，其中第一标识符包括一个第三字段，用于包含标识符的性质。

7．如权利要求1到6中任一项所述的方法，其中第一标识符包括一个第四字段，用于识别服务提供者。

8．如权利要求6或7所述的方法，其中第三字段和/或第四字段没有经过加密。

9．如权利要求1到8中任一项所述的方法，其中第一字段包括一个合同标识符，将用户与服务提供者连接起来。

10．如权利要求1到9中任一项所述的方法，其中该上下文标识符是通用的，并且其中一个相同的上下文标识符使用户可以获得与相同内容提供者的不同类型的服务器的连接。

11．如权利要求1到10中任一项所述的方法，其中第二字段的内容是一段伪随机数据。

12．如权利要求11所述的方法，其中该段伪随机数据是日期。

13．如权利要求11所述的方法，其中对于该网关在一预定的时期内该随机元素是恒定的。

14．如权利要求1到13中任一项所述的方法，其中对第一和第二字段进行代码转换的加密方法，是一个对称块加密方法。

15．如权利要求1到13中任一项所述的方法，其中对第一和第二字段进行代码转换的加密方法，是一个采用块链锁对称加密方法。

产生用于分离连接到电信息通信网络用户的第一标识符的方法

技术领域

本发明的目标是一种用于产生一个分离连接到电信息通信网络的用户的标识符方法。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，本发明的领域涉及存在于电话网络和因特网、语音、SMS、MMS 型电话，或者用于传输多媒体或者单媒体内容的其他载体之间的网关。

背景技术

在现有技术中，内容提供者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。主要可以分出四种访问模式，但是该列表内容并未列出所有的模式。第一种访问模式是因特网型访问。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 协议通过网络，例如因特网，进行通信的设备。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 SMTP（简单邮件传输协议）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执行的访问模式。该模式本身也被再分为两个子模式。第一访问子模式，该模式构成第三访问模式，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（多媒体消息服务）类型协议。第四访问模式是由操作者执行访问的连接模式，也称之为语音模式，其中执行访问的用户与语音服务器连接。

所有四种访问模式都具有一种简单类型的解决方案，其在于产生一

界面，该界面连接服务器过程中提示输入标识符和密码。由于与内容提供者的服务器连接的用户通过移动电话如此操作，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。或者该标识符和密码均完全为数字，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是由字母和数字混合编制的，在这种情况下，使用仅具有 9 个键的键盘输入密码是很繁重乏味的事情。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与这种采用标识符和密码提供连接界面的站点的连接。

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窃取 cookie。由此使用 cookie 不符合高安全性的要求。另一个问题在于 cookie 的声誉较差。这会促使用户清除它们。此外，该用户可配置他用于与内容提供者连接的应用程序或导航器，使得该应用程序不接受 cookie。在此情况下，该用户就无法与内容提供者的服务器连接。

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，在他或她连接内容提供者的服务器时，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连接。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，唯一的解决方案在于不与该内容提供者连接。

在本说明书中，以及实际上，访问内容提供者等效于与内容提供者的服务器连接。

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

向该内容提供者出示的标识符，该标识符不允许任何人，除产生该标识符的实体可以识别民事状况(civil status)和用户的身份。该标识符使得能够通过寻求识别用户的机构所产生的请求而保护该用户的私密性，且所述请求包括该标识符以及产生该标识符的日期。

根据本发明的分离标识符（isolating identifier）请求至少两个用于产生的字段。一个第一字段是用户标识符字段。第二字段是一个字段，该字段用于确保分离标识符的可变性。此可变性是或者由一段伪随机数据或者由用户所陈述的意愿而保证的。然后将第一和第二字段合并，并且进行代码转换，这样任何人都不可以访问第一字段。只有服务提供者，即产生该分离标识符的实体能够解除该加密，由此识别该用户的民事资格和身份。因此真正实现了本发明的目标。

发明内容

本发明的目的在于维护用户的私密性。

本发明的另一目的在于维护网络操作者的客户数据库，并且限制行为分析的活动。

本发明的又一目的在于有助于维护邮件或者通信的保密性。

本发明的再一目的在于使授权的法律实体能够识别用户的民事状况以及身份。

本发明还有一个目的在于使内容提供者管理用于获取与上述内容提供者连接的用户的一个或者多个上下文。

因此本发明的目标在于提供一种用于产生第一上下文标识符的方法，该第一上下文标识符用于分离通过电信息通信网络以及根据用户的使用由服务提供者设定的装置而获取与内容提供者连接的用户，该用户由服务提供者借助于第二标识符识别，其中：

服务提供者的装置包括网关，用于使第一分离上下文标识符与第二

标识符相关联，

第一分离上下文标识符为其产生，请求至少一个第一字段，用于建立第一分离上下文标识符与用户的联系，

第一分离上下文标识符为其产生，请求一个第二字段，用于确保作为内容提供者的函数的第一标识符的可变性，

对第一和第二字段进行代码转换 。

附图说明

通过以下说明和附图将对本发明有更加清析的理解。出示这些附图纯粹为便于说明，而绝不是对发明范围的限制。其中：

图 1 所示为用于实现本发明所述方法的装置。

图 2 所示为根据本发明的分离标识符的一个可能结构。

图 3 所示为实现本发明所述方法的步骤。

具体实施方式

图 1 示出用户使用的用于与内容提供者的服务器(FC)102 连接的装置 101。实际上，装置 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，装置 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。服务器 102 具有一微处理器(μP)103，连接至服务器 102 内部的总线 104。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(IP)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 连接的或已经与之连接的用户一样多。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(ID)。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段，用户可以通过这些信息段自定义他所连接的服务器呈现给他的信息的外观和/或内容。

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。

当用户使用装置 101 取得与服务器 102 的连接时时，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 ISDN 网络，被连接至服务提供者的网关(GW)112，对于该服务提供者，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，网络 111 可构成无论采用什么将基站连接至该服务提供者的网关 112 的任意一种技术解决方案。服务提供者例如为一移动电话操作者。

该内容提供者(CP)，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(μP)，连接至总线 114。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。

在网络 111 上，装置 101 以及由此其用户由一用户标识符 117 识别。在网络 108 上，装置 101 的用户由分离标识符 118 识别。网关 112 的一个作用是建立标识符 117 和分离标识符 118 之间的连接。网关 112 的另

一个典型的作用是在网络 111 上使用的协议和网络 108 上使用的协议之间进行协议转换。标识符 117，例如，为装置 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的(physical)人与其相联系。这样的公共标识符是，例如，一个电话号码，一个邮件地址，一个公共因特网地址等。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，即，用以阻止内容提供者识别这些人的民事状况和身份。

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 执行的一个任务。

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 中产生分离标识符(IID)118 的指令代码，且在一优选实施例中，包括对应于产生内容提供者的代码 120 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 由分离标识符 118 识别用户的指令代码。采用此指令代码用于例如将来自服务器 102 的响应发送到装置 101。存储区域 119d 具有用于从该内容提供者的标识符 120 确定标识符修正符的指令码(DNS)。区域 119e 具有用于执行加密操作的指令码。优选地，这是一种对称加密操作。

该网关 112 具有一存储器 121，用于联系内容提供者标识符(CPID)和该内容提供者代码，以及待被产生的分离标识符的特性的标识。

图 2 所示为用于根据本发明的分离标识符的可能结构。图 2 示出一个需要四个字段的分离标识符 200。在本说明书中的以下内容中，当提及字段，词语“包括”应该用于将多个字段与一个标识符相关联。然而，这并不一定需要一个简单的数值并置。也可以由服务提供者根据可逆处理而将这些值彼此组合。

第一字段 201 对应于标识符 117，用于识别网络 111 上的装置 101 的

用户。字段 201 使服务提供者可以识别用户的民事状况以及身份。在这种情况下，例如，对于一个移动电话操作者，字段 201 不仅包括移动电话号码的有效位(IDN)，而且如果必要的话，还包括一个合同(C)标识符 205，用于将电话号码连接到用户。可以不采用合同号码，但是这样做将要承担如果电话号码被分配到另一用户时将引起混乱的风险。当将电话号码重新分配至另一用户时，此合同号码是有用的。这种合同号码是对例如一电话号码的分配号码的计数器。第二字段 202 对应于取得分离标识符 200 的改变的方法，该改变作为用户要求或者内容提供者代码的函数(Var/CP)。字段 202 和 201 通过区域 119e 的指令目标而进行组合以及/或者代码转换。代码转换优选地是一种对称加密。代码转换也可以通过从表格或者从号码序列或者从一哈希函数代入而完成。在本说明书的以下内容中，我们将使用加密的实例，但是代码转换可以是任何一种可逆的代码转换。这样一个分离标识符是这种组合/代码转换操作的结果，即，它是一个对于除服务提供者以外的任何单位都不可理解的二进制数序列。术语“不可理解”是指不可能将该序列和民事资格以及身份联系在一起。

作为另一方式，分离标识符 200 具有一个字段 203，该字段可以使识别生成标识符的服务提供者成为可能，以及字段 204，例如使对用于分离标识符 200 的版本，以及/或者特性进行编码成为可能。分离标识符 200 在与网关 112 以及服务器 102 的通信过程中作为分离标识符 118。在服务器 102 的用户存储器 106 的 106a 栏中记录了分离标识符 118。在这种变化方式中，分离标识符是由字段 203、204 以及以先前段落中所述的组合/代码转换操作的并置。因此存在不可理解的一部分，由于这部分由内容提供者进行了代码转换，而有一部分是可以理解的，这是由于没有对这部分进行代码转换。

图 3 所示为实施本发明所述的方法的方案的步骤。

图 3 示出步骤 301，其中移动电话 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(CPID)120，以及一个包括该请求本身的字段 122。这种请求是，例如，一个“Get”请求，如在 HTTP 协议中所定义的。需要注意：由于装置 101 是一个移动电话，所以它利用的是 WTP 协议。在步骤 301 生成并且发送的请求在步骤 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。一旦到该内容提供者标识符，则微处理器 113 能够确定用于该内容提供者的代码以及标识符性质。如果在表 121 中没有出现该内容提供者标识符，则微处理器 113 采用缺省的工作模式。在本实例中，假设该缺省的工作模式存在于产生一分离会话标识符。

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或者 SMS 服务器的电话号码。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一个 URL(统一资源定位符)，一个邮件地址等。

如果，在表 121 中，内容提供者标识符 120 对应于一个分离会话标识符的性质，则操作进行到步骤 303 用于生成一个分离会话标识符。否则，则操作进行到步骤 304，用于生成分离上下文标识符。

无论是分离会话标识符还是分离上下文标识符，二者具有图 2 所示的相同结构。区别一个会话标识符和一个上下文标识符之处在于字段 202 的内容。在会话标识符的情况下，字段 202 包括一段随机数据。该段随机数据是由例如从 1970 年 1 月 1 日 00.00 时起经过的秒数构成。也可以是由伪随机数生成器而产生的任意数字，该伪随机数生成器是在产生该随机元素的时间初始化的。通常，该段伪随机数据是一个随机数字。

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。

可以将字段 204 用于例如对标识符的性质进行编码。因此当其为分

离会话标识符时，字段 204 具有一个值，而当其为分离上下文标识符时，具有另一个值。当确定了字段 202 的值时，微处理器 113 能够生成一个根据本发明的分离标识符。微处理器 113 对由字段 202 和字段 201 所形成的字段组进行加密。然后微处理器 113 将加密的结果与管理网关 102 的操作者(OP)的标识符 203 相关联，并且与分离标识符的性质(NAT)204 相关联。因此，得到分离标识符 118。可以看出分离标识符的大小与标识符 117 的大小不同。可以想到的是字段 203 和 204 是任选的。

一旦已生成分离标识符 118，则操作进行到步骤 305，用于产生并且将请求发送到服务器(I GET)102。在步骤 305 中生成的请求包括一个分离标识符 118，一个内容提供者标识符 120 以及一个请求字段 123。实际上，字段 120 和 123 与字段 120 和 122 是相同的。在本实例中，在步骤 305 中生成的请求是采用 HTTP 格式的。在此实例中，字段 120 则是一个目的地 IP 地址。在实际当中，步骤 305 中由网关 112 所生成的请求采用与电话 101 试图连接的服务器相兼容的格式(语音、SMS、IP 等)。

分离标识符字段 118 采用图 2 所说明的格式。分离标识符 118 因此包括一个识别产生该分离标识符的操作者的字段，一个用于根据是否分离标识符为会话标识符还是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。该加密字段在译码后，包括两个字段。这两个字段对应于字段 202 和 201。内容提供者不能够执行解码，并因此不能读取字段 201 和 202。

当发送请求后，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，以查找有关连接到服务器 102 的用户的某些信息。实际上，如果是一个分离会话标识符，则表 106 几乎不可能包括有关用户的信息。事实上，由于会话标识符在每一会话期均改变，所以相同的用户将不会与使用相同分离会话标识符的服务器 102 连接二次。对于本说明书，术语“会话”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，由于根据本发明的分离会话标识符包括一条有关创造日期或者期满的信息。

上下文标识符可以具有一个更长的使用期，例如 6 到 18 个月或者更多。上下文标识符的使用期是由，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。在采用字段 204 的一种变换方式中，分离上下文标识符是因此而键入的，并且具有一个产生日期。上下文标识符因此具有一个以例如月或者年表示的使用期限。

使用期限的选择，以及管理方式的选择，是由负责网关 112 的单位而决定的。使用期得到保证的事实使内容提供者可以使信息，也称作上下文与分离标识符相关联。

在步骤 306 的可能操作之中，服务器 102 可以生成并且向网关 112 发送一个来自标识符 118 的请求(I SERVICE)。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 RESP)。这是步骤 109。

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构成的字段 120，以及字段 123，该字段则包括对于请求的响应。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 RESP)。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 的响应传送到电话 101。操作然后进行到步骤 311，其中装置 101 接收针对在步骤 301 中发送的请求的响应(U RESP)。

在步骤 310 中，对标识符的代码转换的可以伴随对标识符有效性的验证。此验证在例如分离标识符 118 的加密部分的加密之后，并因此在检索字段 202 的值之后进行。因此该验证依赖于标识符的性质。如果是

会话标识符，则字段 202 对应于一日期。然后将此数据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，并且不会将其传送装置 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。该请求包括一个用户分离标识符，一个内容提供者标识符，以及一个请求字段。这种请求可以，例如与一个用户识别请求、一个用于定位用户的请求，或者一个有关装置性质的信息请求相关，该用户使用该装置与接服务器 102 取得连接。此列表没有列出所有的情况。在步骤 312 中，服务器 102 接收该服务请求。在步骤 312 中，网关 112 以对分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；否则，过程进行到步骤 314，响应该服务请求(PROC.)。

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(SERVICE RESP)，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 生成一个针对此服务请求的响应，并且将此响应传送到服务器 102。否则，不存在对服务请求的响应。

在步骤 314 中，服务器 102 接收服务请求的响应。此响应使服务器 102 将表 106 升级或者生成步骤 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 可以向装置 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，也可以向装置 101 发送一个压入(push)请求(I PUSH)。此压入请求是在步骤 316 中由网关 112 接收的。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此压入请求，并且标识符 118 应该是有效的。如果标识符是无效的，则过程进行到结束步骤 319，在该步骤中不会对服务器 102 所发送的压入请求没有给出任何肯定的响应(U PUSH)。

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 将分离标识符 118 译码为标识符 117，并且将该经过译码的压入请求传送到电话 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，例如对装置 101 中的数据更新。这种数据库可以，例如与装置 101 的用户希望保持的联系相关，或者与装置 101 为访问不同的服务可能与之连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)或者 3DES 算法。可以采用此算法的块加密版或者链锁加密版。该链锁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分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，以便得到更多关于标识符所识别的用户的私人生活的信息。对内容提供者来说，也不可能袭击提供者的数据库，由于内容提供者不能确定民事状况和用户的身份，或者相同的用户总与相同的分离标识符相连接的事实。因此，对用户的私密性可得到最大的保护。

以标识符开始并且仅针对产生此标识符的操作者，可能在服务提供者的合作下将一操作追溯到物理用户，因此法律方面的标准也可得到满足。

一个用户可以选择通过一直采用会话标识符进行连接。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分离标识符而连接到相同的站点。然后内容提供者则无法确定连接两次的用户是相同的用户。

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分离上下文标识符。然后内容提供者将根据能够附加到分离上下文标识符的信息而调整其响应。

通过将一用户标识符，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。

如果我们考虑一个采用个人计算机通过因特网服务提供者(或者 ISP)而连接到内容提供者，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。

本发明也具有使管理分离标识符的机构免于存储这些分离标识符的优点。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。

最后，根据本发明的一个分离标识符既是在电话标准 NDS 字段也是以在网络上使用的任何协议的帧传送的。因此根据本发明的分离标识符是通用的，并且对于用户还可以实现采用相同的分离上下文标识符而与相同的内容提供者的不同类型的服务连接。这极大地简化了能够不依赖于服务器的类型而统一其上下文管理的内容提供者的任务。

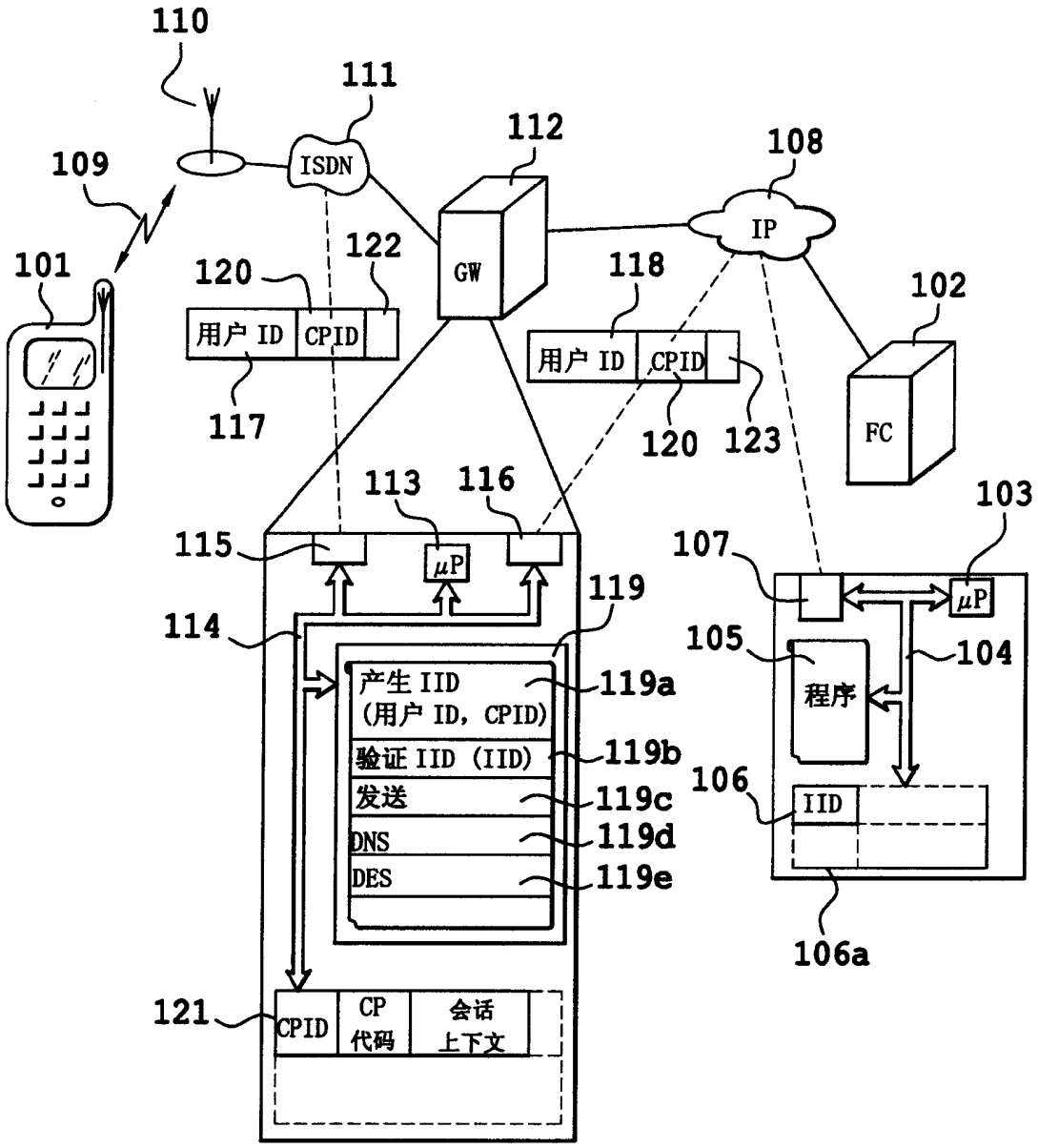

110
111
112
108
109
ISDN
GW
IP
101
120
122
118
102
用户 ID
CPID
用户 ID
CPID
117
120
123
FC
113
116
103
115
μP
107
μP
119
114
105
104
产生 IID
(用户 ID, CPID)
119a
程序
验证 IID (IID)
119b
106
发送
119c
IID
DNS
119d
DES
119e
106a
121
CPID
CP
代码
会话
上下文

图 1

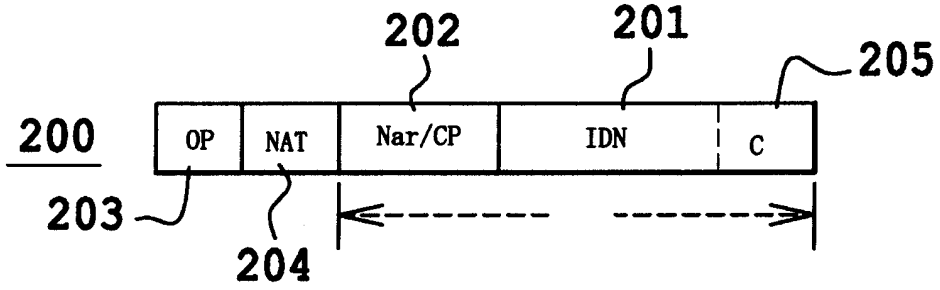

202
201
205
200
OP
NAT
Nar/CP
IDN
C
203
204

图 2

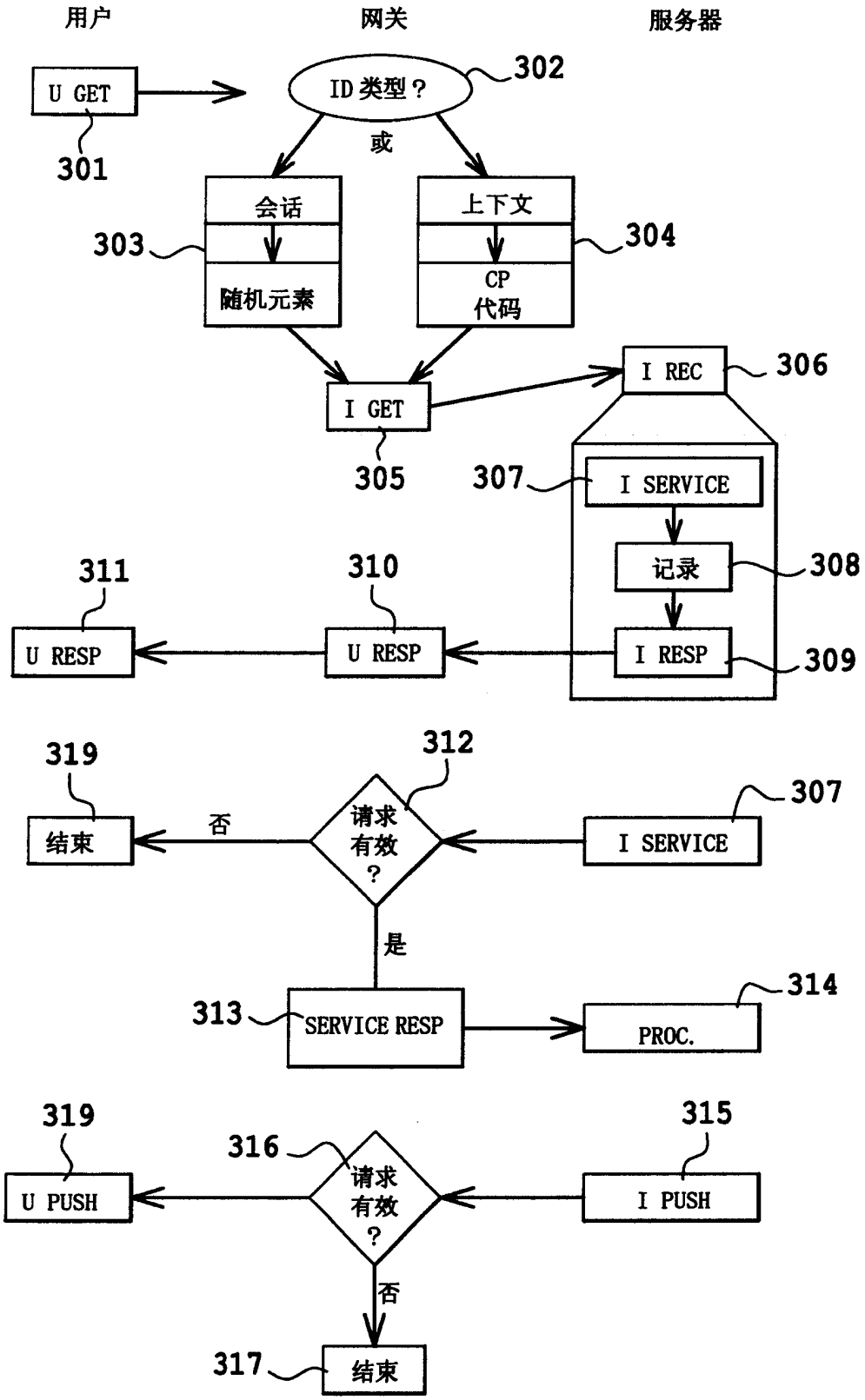

用户
网关
服务器
U GET
301
ID类型？
302
或
会话
随机元素
303
上下文
CP
代码
304
I GET
305
I REC
306
I SERVICE
307
记录
308
I RESP
309
U RESP
310
U RESP
311
结束
319
否
请求
有效
？
312
I SERVICE
307
是
SERVICE RESP
313
PROC.
314
U PUSH
319
316
请求
有效
？
I PUSH
315
否
结束
317

图 3