[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610168572.6

[43] 公开日 2008 年 6 月 25 日

[11] 公开号 CN 101207613A

[22] 申请日 2006.12.21
[21] 申请号 200610168572.6
[71] 申请人 松下电器产业株式会社
地址 日本大阪府
[72] 发明人 刘学灯 方均伟

[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 王 玮

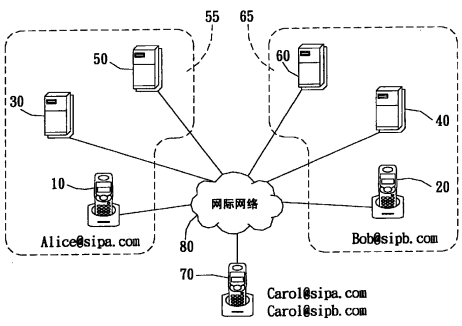
权利要求书 6 页 说明书 12 页 附图 12 页

[54] 发明名称

跨网域信息通信的认证方法、系统及其装置

[57] 摘要

本发明提供一种跨网域信息通信的认证方法，应用在第一网域与第二网域之间，该方法令属于第一网域的第一电子装置通过同时在第一及第二网域注册的中继点装置，向属于第二网域的第二金钥分配中心取得第一金钥并送给该第二电子装置，且该第二电子装置通过该中继点装置，向属于第一网域的该第一金钥分配中心取得第二金钥并送给该第一电子装置，这样，令第一及第二电子装置根据收到的该第一及第二金钥产生共享的第三金钥，以使用该只有第一及第二电子装置知道的共享的第三金钥进行安全的信息通信认证。



1.一种跨网域信息通信的认证方法，应用在要通过网际网络进行信息通信的属于第一网域的第一电子装置与属于第二网域的第二电子装置之间；所述方法包括：

(A) 令所述第一电子装置要求同网域的第一代理服务器找出同时在所述网域注册的中继点装置；

(B) 令所述第一电子装置通过所述中继点装置，向所述第二网域的第二金钥分配中心注册以取得第一金钥，并传送包含所述第一金钥的第一通行证给所述第二电子装置；

(C) 令所述第二电子装置收到所述第一通行证后，通过所述中继点装置，向所述第一网域的第一金钥分配中心注册以取得第二金钥，且传送包含所述第二金钥的第二通行证给所述第一电子装置；及

(D) 令所述第一及第二电子装置根据收到的所述第一及第二金钥产生共享的第三金钥，以进行信息通信认证。

2.根据权利要求 1 所述的跨网域信息通信的认证方法，在步骤(A)中，所述中继点装置已预先向所述第一及第二金钥分配中心注册。

3.根据权利要求 1 所述的跨网域信息通信的认证方法，在进行步骤(A)之前，所述第一代理服务器中预先记录有多个候选中继点装置的信息，所述候选中继点装置在开机状态下，传送网域特定信息向所述第一代理服务器进行注册，而被记录在所述第一代理服务器中。

4.根据权利要求 3 所述的跨网域信息通信的认证方法，其中所述网域特定信息包括与所述第一及第二网域相关的资料，且至少包括所述第一及第二网域的身份资料。

5.根据权利要求 3 所述的跨网域信息通信的认证方法，其中所述网域特定信息包括有关各所述候选中继点装置的能力的资料，且至少包括各所述候选中继点装置的硬件能力以及可处理同时点对点联机的最大服务数。

6.根据权利要求 5 所述的跨网域信息通信的认证方法，在步骤(A)中，所述第一电子装置发出包含有所述第二电子装置的目的信息的要求消息

给所述第一代理服务器，使根据所述要求消息及所述网域特定信息，从所述候选中继点装置中找到适合的中继点装置。

7.根据权利要求 1 所述的跨网域信息通信的认证方法，在步骤(D)中，所述信息通信认证是通过所述第一代理服务器与所述第二网域的第二代理服务器来完成。

8.根据权利要求 7 所述的跨网域信息通信的认证方法，其中所述信息通信是语音通信。

9.根据权利要求 8 所述的跨网域信息通信的认证方法，其中所述第一及第二代理服务器是对话启始协议代理服务器。

10.一种跨网域信息通信认证系统，设置在第一网域中，用于通过网际网络与属于第二网域的第二电子装置进行信息通信；所述系统包括：

第一代理服务器，其中记录有多个候选中继点装置；

第一电子装置，发出要求消息，要求所述第一代理服务器从所述候选中继点装置中找出同时在所述网域注册的中继点装置，以通过所述中继点装置，向所述第二网域的第二金钥分配中心注册取得第一金钥，并传送包含所述第一金钥的第一通行证给第二电子装置；及

第一金钥分配中心，供所述第二电子装置通过所述中继点装置，向其注册并取得第二金钥，并传送包含所述第二金钥的第二通行证给所述第一电子装置，使所述第一及第二电子装置可根据收到的所述第一及第二金钥产生共享的第三金钥，以进行信息通信认证。

11.根据权利要求 10 所述的跨网域信息通信认证系统，其中各所述候选中继点装置包括网域特定信息组织单元、存储配置数据的网域信息存储单元及第一联机单元，各所述候选中继点装置在开机状态下，通过所述网域特定信息组织单元，根据存储在所述网域信息存储单元中的配置数据，产生网域特定信息，通过所述第一联机单元传送至所述第一代理服务器。

12.根据权利要求 11 所述的跨网域信息通信认证系统，其中所述第一代理服务器包括第二联机单元、网域特定信息交换单元及网域管理数据库，所述第二联机单元分析所述网域特定信息，所述网域特定信息交换单元执行网域特定信息更新并将所述网域特定信息存入所述网域管理数据库中。

13.根据权利要求 11 所述的跨网域信息通信认证系统，其中所述中继点装置包括信号收发单元及网络通信单元，且所述网域特定信息经由所述信号收发单元及网络通信单元传送给所述第一代理服务器。

14.根据权利要求 11 所述的跨网域信息通信认证系统，其中所述第一代理服务器包括信号收发单元及网络通信单元，用以接收由各所述中继点装置传来的所述网域特定信息。

15.根据权利要求 11 所述的跨网域信息通信认证系统，其中所述网域特定信息包括与所述第一及第二网域相关的资料，且至少包括所述第一及第二网域的身份资料。

16.根据权利要求 11 所述的跨网域信息通信认证系统，其中各所述网域特定信息包括有关各所述候选中继点装置的能力的资料，且至少包括各所述候选中继点装置的硬件能力以及可处理同时点对点联机的最大服务数。

17.根据权利要求 16 所述的跨网域信息通信认证系统，其中所述要求消息包含目的地信息，所述第一代理服务器还包括发现中继点模块及选择中继点模块，所述发现中继点模块根据所述要求消息的目的地信息轮询所述网域管理数据库，以发现同时在第一及第二网域注册的候选中继点装置并产生轮询结果，所述选择中继点模块根据所述轮询结果过滤所述候选中继点装置并从所述候选中继点装置中选出适用的中继点装置。

18.根据权利要求 17 所述的跨网域信息通信认证系统，其中所述发现中继点模块包括发现候选中继点单元及轮询候选者单元，所述选择中继点模块包括选择中继点单元、过滤候选者单元及选择单元；所述发现候选中继点单元从所述要求消息中取出所述目的地信息传给轮询候选者单元，使以所述目的地信息为索引，轮询记录在网域管理数据库中的所述候选中继点装置信息，以得到轮询结果；所述选择中继点单元根据所述轮询结果过滤不合格的中继点装置，所述过滤候选者单元用于排除已超出最大服务数的候选中继装置；所述选择单元根据候选中继点装置的硬件能力从所述被留下的候选中继点装置中选择最佳的中继点装置。

19.根据权利要求 18 所述的跨网域信息通信认证系统，其中所述发现中继点候选者单元及所述选择中继点单元分别通过所述信号收送单元及

网络通信单元与所述第一电子装置通信。

20.根据权利要求 10 所述的跨网域信息通信认证系统，其中所述第一及第二电子装置以及所述中继点装置是移动通信装置。

21.根据权利要求 10 所述的跨网域信息通信认证系统，其中所述第一及第二电子装置以及所述中继点装置是移动电话。

22.根据权利要求 10 所述的跨网域信息通信认证系统，其中所述信息通信认证是通过所述第一代理服务器与所述第二网域的第二代理服务器完成的。

23.根据权利要求 22 所述的跨网域信息通信认证系统，其中所述信息通信是语音通信。

24.根据权利要求 23 所述的跨网域信息通信认证系统，其中所述第一及第二代理服务器是对话启始协议代理服务器。

25.一种移动通信电子装置，属于第一网域，其可通过网际网络与属于第二网域的第二电子装置进行信息通信；所述行动通信电子装置包括：

中继点请求模块，发出要求消息，要求同网域的第一代理服务器找到同时在所述网域注册的中继点装置；及

跨网域金钥处理单元，通过所述中继点装置，向所述第二网域的第二金钥分配中心注册以取得第一金钥，并传送包含所述第一金钥的第一通行证给所述第二电子装置，以要求其回传包含第二金钥的第二通行证，并处理所述第二通行证，以取出所述第二金钥，而根据所述第一及第二金钥产生用于与所述第二电子装置进行信息通信认证的第三金钥。

26.根据权利要求 25 所述的移动通信电子装置，其中所述跨网域金钥处理单元还包括外来网域处理模块、本地网域处理模块及共同金钥产生单元，其中所述外来网域处理模块通过所述中继点装置，向所述第二金钥分配中心注册以取得第一金钥，并传送包含所述第一金钥的第一通行证给所述第二电子装置，以要求其回传包含第二金钥的第二通行证；所述本地网域处理模块接收并处理所述第二通行证，以取出所述第二金钥；所述共同金钥产生单元根据所述第一及第二金钥产生用于与所述第二电子装置进行信息通信认证的第三金钥。

27.根据权利要求 26 所述的移动通信电子装置，还包括网络通信单元，

且所述中继点请求模块是通过所述网络通信单元连上所述第一代理服务器。

28.根据权利要求 27 所述的移动通信电子装置，还包括认证通信单元，且所述外来网域处理模块及所述本地网域处理模块是通过所述认证通信单元及所述网络通信单元连上网际网络。

29.根据权利要求 27 所述的移动通信电子装置，其中所述中继点请求模块包括要求消息收发单元、通行证要求单元、信号收发单元、中继点要求单元及中继点信息取出单元，所述通行证要求单元产生包含受话端信息的通行证要求消息，通过所述要求消息收发单元及所述网络通信单元送至所述第一网域的第一金钥分配中心；所述中继点要求单元产生包含受话端信息的寻找中继点消息，通过所述信号收发单元及网络通信单元送至所述第一代理服务器以寻找中继点装置；所述中继点信息取出单元从所述第一代理服务器的回复消息中取得中继点装置的信息。

30.根据权利要求 28 所述的移动通信电子装置，其中所述外来网域处理模块包括注册单元、外来网域获得单元、外来网域存储单元及递送单元，所述注册单元用以产生注册要求消息，并通过所述认证通信单元及所述网络通信单元向所述第二金钥分配中心进行注册，以获得注册证号，所述外来网域获得单元根据所述注册证号向所述第二金钥分配中心取得所述第一金钥及所述第一通行证并存储在所述外来网域存储单元中，所述递送单元将所述第一通行证通过所述认证通信单元及所述网络通信单元传送给所述第二通信电子装置。

31. 根据权利要求 26 所述的移动通信电子装置，其中所述本地网域处理模块包括本地网域取得单元及第二存储单元，所述本地网域取得单元用以处理所述第二通行证以取出所述第二金钥并存储在所述第二存储单元中。

32. 根据权利要求 25 所述的移动通信电子装置，其中所述信息通信认证是通过所述第一代理服务器与所述第二网域的第二代理服务器来完成的。

33.根据权利要求 32 所述的移动通信电子装置，其中所述信息通信是语音通信。

34.根据权利要求 33 所述的移动通信电子装置，其中所述第一及第二代理服务器是对话启始协议代理服务器。

35.一种中继点装置，其能够横跨第一网域及第二网域，并与设置在第一网域的第一代理服务器及第一电子装置通信，以协助所述第一电子装置与属于第二网域的第二电子装置进行信息通信；所述中继点装置包括：

网域信息存储单元，用于存储配置数据；

联机单元，用于与所述第一代理服务器联机；及

网域特定信息组织单元，根据所述网域信息存储单元存储的配置数据，产生网域特定信息，并通过所述第一联机单元传送至所述第一代理服务器。

36.根据权利要求 35 所述的中继点装置，还包括相连接的信号收发单元及网络通信单元，而所述第一联机单元与所述信号收发单元连接，以将所述网域特定信息经由所述信号收发单元及网络通信单元传送给所述第一代理服务器。

37.根据权利要求 35 所述的中继点装置，其中所述网域特定信息包括与所述第一及第二网域相关的资料，且至少包括所述第一及第二网域的身份资料。

38. 根据权利要求 35 所述的中继点装置，其中所述网域特定信息包括有关所述中继点装置的能力的资料，且至少包括所述中继点装置的硬件能力以及可处理同时点对点联机的最大服务数。

跨网域信息通信的认证方法、系统及其装置

技术领域

本发明涉及一种信息通信认证方法，特别是指一种跨网域信息通信的认证方法、系统及其装置。

背景技术

近年来由于网络通信技术趋于成熟，使得通过网际网络传送数字语音封包的网络电话(Voice over Internet Protocol，VoIP)、传送消息的短消息服务、影音通信以及多媒体影音串流服务等成为目前热门的网络应用。

以网络电话为例，通话启始协议(Session Initiation Protocol 以下称 SIP)是目前网络电话常用的信令协议(Signaling protocols)标准。在网络电话系统中，使用 SIP 协议的每一个移动电话会向某一特定 SIP 网域注册而分别属于该特定的 SIP 网域，该网域的安全管理是由金钥管理中心 (KMC：key management center，)或金钥分配中心 (KDC：key distribution center)所控管，且由于在同一网域中的移动电话应用同一认证协议，因此在同一网域中，移动电话与服务器之间以及移动电话与移动电话之间可以相互认证而进行安全通信。

但是，当两个移动电话的通话区域跨越两个不同的网域时，则会因为各网域认证协议的不同而必须另外遵循另一共同的认证方式才能进行安全通信，但也因此产生跨网域信任操作(inter-domain trust operations)的问题。

为解决上述问题，作为现有技术的、名称为“Method and system for authentication through multiple proxy servers that require different authentication data”(通过多个需要不同认证资料的代理服务器的认证方法及系统)的美国专利 No.6839761，其主要是针对连续的代理(服务器)，让其在 SIP 要求消息中附加各自的认证资料，以解决在 SIP 中用户与连续代理

者之间的认证，以得到针对不同安全网域的连续的认证凭证，但此专利并没有针对跨网域问题进行解决。

另一种现有技术是美国专利申请公开 No.20050108575，名称为“Apparatus, system and method for facilitating authenticated communication between authentication realms”(简化认证区域之间认证通信的装置、系统及方法)，其主要利用认证网关来解决不同认证协议之间的认证。但是固定的认证网关容易因遭受网络攻击而产生工作效率低的问题。

因此，如何在不需在两个安全网域服务器上使用复杂的跨网域信赖操作的情况下，需要提供一种针对两个跨越两个不同安全网域的通信电子装置取得共同的认证凭证的机制。

发明内容

因此，本发明的目的是提供一种不须在两个安全网域服务器上采用复杂的跨网域信赖操作即可取得共同的认证凭证的跨网域信息通信的认证方法、系统及其装置。

于是，本发明的跨网域信息通信的认证方法，应用于要通过网际网络进行信息通信的属于第一网域的第一电子装置与属于第二网域的第二电子装置之间；该方法包括：(A)令该第一电子装置要求同网域的第一代理服务器找出同时在该网域注册的中继点装置;(B)令该第一电子装置通过该中继点装置，向该第二网域的第二金钥分配中心注册以取得第一金钥，并传送包含该第一金钥的第一通行证给该第二电子装置;(C)令该第二电子装置收到该第一通行证后，透过该中继点装置，向该第一网域的第一金钥分配中心注册以取得第二金钥，且传送包含该第二金钥第二通行证给该第一电子装置；及(D)令该第一及第二电子装置根据收到的该第一及第二金钥产生共享的第三金钥，以进行信息通信认证。

此外，本发明实现上述方法的跨网域信息通信认证系统，设置在第一网域中，用以通过网际网络与属于第二网域的第二电子装置进行信息通信；该系统包括第一代理服务器、第一电子装置及第一金钥分配中心。该第一代理服务器中记录有多个候选中继点装置。该第一电子装置发出要求消息，要求该第一代理服务器由该候选中继点装置中找出同时在该网域注

册的中继点装置，以便通过该中继点装置，向该第二网域的第二金钥分配中心注册以取得第一金钥，并传送包含该第一金钥的第一通行证给第二电子装置。该第一金钥分配中心供该第二电子装置通过该中继点装置，向其注册并取得第二金钥，并传送包含该第二金钥的第二通行证给该第一电子装置，使该第一及第二电子装置可根据收到的该第一及第二金钥产生共享的第三金钥，以进行信息通信认证。

再者，本发明实现上述方法的移动通信电子装置，属于第一网域，其可通过网际网络与属于第二网域的第二电子装置进行信息通信；该行动通信电子装置包括中继点请求模块及跨网域金钥处理单元。该中继点请求模块发出要求消息，要求同网域的第一代理服务器找到同时在该网域注册的中继点装置。该跨网域金钥处理单元通过该中继点装置，向该第二网域的第二金钥分配中心注册以取得第一金钥，并传送包含该第一金钥的第一通行证给该第二电子装置，以要求其回传包含第二金钥的第二通行证，并处理该第二通行证，以取出该第二金钥，而根据该第一及第二金钥产生用以与该第二电子装置进行信息通信认证的第三金钥。

另外，本发明实现上述方法的中继点装置，其可横跨第一网域及第二网域，并与设置在第一网域的第一代理服务器及第一电子装置通信，以协助该第一电子装置与属于第二网域的第二电子装置进行信息通信；该中继点装置包括网域信息存储单元、联机单元及网域特定信息组织单元。该网域信息存储单元存储配置数据。该联机单元与该第一代理服务器联机。该网域特定信息组织单元根据该网域信息存储单元存储的配置数据，产生网域特定信息，并通过该第一联机单元传送至该第一代理服务器。

附图说明

图 1 是本发明的跨网域信息通信的认证方法的优选实施例的网络系统架构图；

图 2 是本实施例的第一 SIP 代理服务器与移动电话的内部功能单元的方框图；

图 3 是本实施例的第一 SIP 代理服务器的部分内部硬件架构与候选中继点装置的内部硬件架构的方框图；

图 4 是本实施例的候选中继点装置向第一 SIP 代理服务器注册的流程图；

图 5 是本实施例的移动电话的中继点请求模块的细部硬件架构电路的方框图；

图 6 是本实施例的第一 SIP 代理服务器寻找中继点装置的流程图；

图 7 是本实施例的第一 SIP 代理服务器内部部分硬件架构的方框图；

图 8 是本实施例的轮询结果示意图；

图 9 是本实施例的过滤候选中继点装置的初步过滤结果的示意图；

图 10 是本实施例的移动电话的外来网域处理模块及本地网域处理模块的细部硬件架构的方框图；

图 11 是本实施例的属于第一网域的移动电话通过中继点装置向第二 KDC 要求第一金钥的流程图；

图 12 是本实施例的属于第二网域的移动电话通过中继点装置向第一 KDC 要求第二金钥的流程图；及

图 13 是本实施例的分属于第一及第二网域的移动电话分别以取得的第一及第二金钥产生共同的第三金钥进行跨网域认证的流程图。

具体实施方式

有关本发明的前述及其它技术内容、特点与功效，在以下配合参考图式的优选实施例的详细说明中，将可清楚的呈现。

参阅图 1 所示，是本发明跨网域信息通信的认证方法的优选实例，应用在要通过网际网络 80 进行语音数据通信(即 VoIP)的属于第一 SIP 网域 55(其 SIP URI 为 sipa.com)的第一电子装置 10(其 SIP URI 为 Alice@sipa.com)与属于第二 SIP 网域 65(其 SIP URI 为 sipb.com)的第二电子装置 20(其 SIP URI 为 Bob@sipb.com)之间，其中，该第一网域 55 中包含第一代理服务器(在本实施例中该第一代理服务器是 SIP 代理服务器，以下称第一 SIP 代理服务器 50)及第一 KDC 30，该第二网域 65 中包含第二代理服务器(在本实施例中该第二代理服务器是 SIP 代理服务器，以下称第二 SIP 代理服务器 60)及第二 KDC40。其中，第一电子装置 10 是发话端，第二电子装置 20 是受话端，且在本实施例中，第一及第二电子装置 10、

20 是以移动电话(以下皆以移动电话 10、20 说明)作为例子，但并不以此为限。

另外，如图 2 所示，是本实施例的第一 SIP 代理服务器 50 与移动电话 10 的内部功能单元的方框图，其中第一 SIP 代理服务器 50(第二 SIP 代理服务器 60 同)包括用于与网际网络连接的网络通信单元 500、信号收发单元 502、跨网域注册单元 504、跨网域中继点搜寻单元 506 及网域管理数据库 508；移动电话 10 包括用于与网际网络连接的网络通信单元 100、中继点请求模块 102、认证通信单元 104 及跨网域金钥处理单元 106，这些功能单元的作用将在后面说明。

本实施例的跨网域语音信息通信的认证方法包括：

步骤(A)：

由移动电话 10 向第一 SIP 代理服务器 50 要求提供同时在第一及第二网域 55、65 注册的中继点装置。

在进行步骤(A)之前，该第一 SIP 代理服务器 50 中已记录有多个候选中继点装置的信息，该多个候选中继点装置是在开机状态下，传送其网域特定信息给该第一 SIP 代理服务器 50 进行注册及更新。

首先，该多个候选的中继点装置必须是同时在第一及第二网域 55、65 中注册的装置。且在本实施例中，中继点装置是以移动电话为例，但并不以此为限。该多个候选中继点装置处在开机状态下，会定时或不定时地传送网域特定信息给所属网域的 SIP 代理服务器，让所属网域的 SIP 代理服务器知道它的存在，以便在要进行通话的两个网域 55、65 之间建立桥接关系。

且为产生该网域特定信息，如图 3 所示，各该候选中继点装置 700 包括网络通信单元 702、信号收发单元 704、第一联机单元 706、网域特定信息组织单元 708 及存储配置数据的网域信息存储单元 710。

另外，为处理上述网域特定信息，如图 3 所示，第一 SIP 代理服务器 50(第二 SIP 代理服务器 60 同)的跨网域注册单元 504 还包括网域特定信息交换单元 510 及第二联机单元 512。

同时，参见图 4 的流程所示，候选中继点装置 700 在开机状态下，如图 4 的步骤 1500，触发其网域特定信息组织单元 708 组织存储在其网域信

息存储单元 710 中的配置数据(configuration data)，以构成包含诸如第一及第二 SIP 网域 55、65 的身份及第一及第二 KDC30、40 的身份等的网域特定信息。然后，如步骤 1502，在第一联机单元 706 中，将网域特定信息附加在要求注册信号[REGISTER]中，通过信号收发单元 704 及网络通信单元 702 送至第一 SIP 代理服务器 50。且该网域特定信息中还包含中继点装置本身的硬件能力以及可以处理同时点对点联机的最大服务数等信息。

当第一 SIP 代理服务器 50 通过其网络通信单元 500 及信号收发单元 502 收到该要求注册信号[REGISTER]后，如步骤 1504，其触发第二联机单元 512，使从要求注册信号[REGISTER]中分析并取出网域特定信息，且触发网域特定信息交换单元 510 以该网域特定信息更新原有资料后，将该网域特定信息存入网域管理数据库 508 中，并在完成更新后，如步骤 1506，回传完成消息[200OK]给候选中继点装置 700。至此，该多个候选中继点装置 700 与第二 SIP 网域 65 及第二 KDC40 的桥接关系被建立并注册在第一 SIP 代理服务器 50 中。

接着，参见图 5，移动电话 10 的中继点请求模块 102 用于产生与移动电话 20 通信的通行证要求，并通过网络通信单元 100 向第一 SIP 代理服务器 50 要求中继点装置。中继点请求模块 102 包括要求消息收发单元 108、通行证要求单元 110、信号收发单元 112、中继点要求单元 114 及中继点信息取出单元 116。

因此，当属于第一 SIP 网域 55 的移动电话 10 想要与属于第二 SIP 网域 65 的移动电话 20 进行通话时，如图 6 的步骤 2500，通行证要求单元 110 产生内含受话端(即移动电话 20)信息，例如 Bob@sipb.com 的通行证要求消息[TGS_REQ]，并如步骤 2502，通过要求消息收发单元 108 及网络通信单元 100 将通行证要求消息[TGS_REQ]送至第一 KDC30 时，如步骤 2504，第一 KDC30 会检查该消息是否与第二 SIP 网域 65 有任何互信关系，即第一 KDC30 与第二 KDC40 已预先设定的信任关系，例如两者已预先设定共享的金钥，且本实施例的功效即在不需建立上述的信任关系，即可达到跨网域之网络电话认证。

而由于第一 KDC30 发现两者缺乏互信关系(因为不在同一网域)，因此如步骤 2506，第一 KDC30 回复内含失败(NG)消息的回复消息[TGS_REP]

给移动电话 10，当移动电话 10 通过网络通信单元 100 及要求消息收发单元 108 收到失败的回复消息[TGS_REP]后，即知道所欲通话的移动电话 20 与其分属于不同网域，因此移动电话 10 必需寻找一个介于其与属于外来网域的行动装置 20 之间的中继点。

所以，如步骤 2508，移动电话 10 的中继点要求单元 114 产生内含有受话端信息，例如移动电话 20 的 SIP URI：Bob@sipb.com 的寻找中继点消息[INVITE]，并如步骤 2510，通过信号收发单元 112 及网络通信单元 100 将该寻找中继点消息[INVITE]送至第一 SIP 代理服务器 50 以寻找中继点装置。

为了协助移动电话 10 找到适当的中继点装置，如图 7 所示，第一 SIP 代理服务器 50 的跨网域中继点搜寻单元 506 还包括用于发现中继点并产生轮询结果的发现中继点模块 514，以及根据该轮询结果选出最佳中继点装置的选择中继点模块 516。其中，发现中继点模块 514 又包含发现候选中继点单元 518 及轮询候选者单元 520；选择中继点模块 516 又包含选择中继点单元 522、过滤候选者单元 524 及选择单元 526。

因此，在图 6 的步骤 2512 中，当第一 SIP 代理服务器 50 通过网络通信单元 500 及信号收发单元 502 收到该寻找中继点消息[INVITE]后，其触发该发现候选中继点单元 518 判别该寻找中继点消息[INVITE]，并由寻找中继点消息[INVITE]中解析出受话端信息后，传给轮询候选者单元 520，使以外来网域身份信息(即受话端信息)为索引(搜寻条件)搜寻网域管理数据库 508，亦即轮询(query)记录在网域管理数据库 508 中的该多个候选中继点装置 700 的信息，以找出同时存在第一及第二网域 55、65 中的候选中继点，并得到轮询结果供后续选择中继点使用。该轮询结果以图 8 所示为例，经过轮询网域管理数据库 508 的结果，找到 3 个同时存在第一及第二网域 55、65 中的候选中继点装置(Carol1@sipa.com、Carol2@sipa.com 及 Carol3@sipa.com)。

然后，在步骤 2514，以该轮询结果作为输入，触发该过滤候选者单元 524 执行初步的过滤程序，使根据轮询结果过滤不合格的中继点装置，例如滤掉目前服务数目大于/等于预设服务数目的候选中继点装置，以图 8 为例，滤掉服务数目达到最大的中继点装置 Carol3@sipa.com，最后留下

如图 9 所示的候选中继点装置。之后，将初步过滤后的结果(图 9 所示)交由选择单元 526 执行选取中继点装置程序，以候选中继点装置的硬件能力重新排列轮询结果，并根据诸如具有最强硬体能力或具有最多可服务数等条件，从该多个被留下的候选中继点装置 700 中选择最佳的中继点装置 70。因此，如果按照“最佳的硬件能力”条件，则选取中继点装置 Carol2@sipa.com，如果按照“最大的可服务数目”条件，则选取中继点装置 Carol1@sipa.com。

因此，选出中继点装置 70 后，如步骤 2516，第一 SIP 代理服务器 50 由选择中继点单元 522 产生内含中继点装置 70 的信息，例如 SIP URI 为 Carol1@sipa.com (或 Carol2@sipa.com)的回复消息[404 Not Found]，经由信号收发单元 502 及网络通信单元 500 回传给移动电话 10。移动电话 10 通过网络通信单元 100 及信号收发单元 112 收到该回复消息[404 Not Found]，并由中继点信息取出单元 116 从该回复消息[404 Not Found]中取出中继点装置 70 的信息。至此，移动电话 10 找到了中继点装置 70 作为与移动电话 20 进行跨网域安全认证的中继点，且移动电话 10 拥有中继点装置 70 的身份信息(Carol1@sipa.com 或 Carol2@sipa.com)。

然后，如步骤 2518，移动电话 10 通过通行证要求单元 110、要求消息收发单元 108 及网络通信单元 100 产生并传送通行证要求消息[TGS_REQ]，向第一 KDC30 要求连接至中继点装置 70 的通行证，第一 KDC30 产生中继点装置 70 的通行证(ticket)后，如步骤 2520，回传通行证回复消息[TGS_REP]给移动电话 10。如此，移动电话 10 拿到中继点装置 70 的通行证可作为之后与移动电话 20 的安全凭证的认证使用。

步骤(B)：

移动电话 10 通过该中继点装置 70，向该第二 KDC40 要求第一金钥，并传送包含该第一金钥的第一对话通行证给该移动电话 20。

如图 10 所示，为达成上述动作，移动电话 10(移动电话 20 同)的跨网域金钥处理单元 106 还包括外来网域处理模块 118、本地网域处理模块 120 及共同金钥产生单元 122。其中，外来网域处理模块 118 还包含外来网域获得单元 124、递送单元 126、注册单元 128 及外来网域存储单元 130。本地网域处理模块 120 还包含本地网域获得单元 132 及本地网域存储单元

134。且该外来网域处理模块 118 及该本地网域处理模块 120 皆经由认证通信单元 104 及网络通信单元 100 连上网际网络。

这样，当移动电话 10 要通过中继点装置 70 与移动电话 20 进行跨网域认证时，首先，移动电话 10 触发外来网域获得单元 124，使通过中继点装置 70 向第二 KDC40 进行注册。如图 11 的步骤 3500 所示，开始时，要求注册消息[AP_REQ]在注册单元 128 组成，并通过认证通信单元 104 及网络通信单元 100 送至中继点装置 70。然后，如步骤 3502 及 3504，中继点装置 70 重新产生要求将移动电话 10 注册至第二 KDC40 的要求消息[USR_REG](其中附有移动电话 10 的身份 Alice@sipa.com)，并传给第二 KDC40，当第二 KDC40 收到后，如步骤 3506，第二 KDC40 产生给移动电话 10 的注册 ID，并如步骤 3508，回传附有注册 ID 的注册响应消息[USR_REP]给中继点装置 70，然后如步骤 3510，中继点装置 70 经由移动电话 10 的网络通信单元 100 及认证通信单元 104 将注册响应消息[USR_REP]送给注册单元 128。

在得到第二 KDC40 为其所产生的注册 ID 后，在步骤 3512 及 3514，移动电话 10 通过安全协议，例如 Diffie-Hellman，与第二 KDC40 进行安全信道建立([DH_REQ]及[DH_REP])，接着在步骤 3516 中，使用该注册 ID 与第二 KDC40 进行认证([AUTH_REQRSP])，以确认该注册 ID 确实由第二 KDC40 发给，而在步骤 3518 中，在移动电话 10 与第二 KDC40 两者之间建立经认证且安全的信道。

然后，在步骤 3520，移动电话 10 触发外来网域获得单元 124，使其向第二 KDC40 传送通行证要求消息[TGS_REQ]，以要求给移动电话 20 的通行证。因此在步骤 3522，第二 KDC40 回传包含第一金钥(session key)及要传给移动电话 20 的第一对话通行证(session ticket)(其中包含经过加密的第一金钥)的票卷回复消息[TGS_REP]给移动电话 10，则如步骤 3524，外来网域获得单元 124 将取得的第一金钥及第一对话通行证存储在外来网域存储单元 130 中。且在步骤 3526，递送单元 126 被触发以将第一对话通行证传给移动电话 20([Ticket Delivery])。

另一方面，如图 12 的步骤 3528 所示，移动电话 10 传送内含中继点装置 70 的信息(Carol1@sipa.com 或 Carol2@sipa.com)的要求消息[INVITE]

给移动电话 20 以触发移动电话 20 交换安全凭证。该要求消息[INVITE]经由第一及第二 SIP 代理服务器 50、60 传送到移动电话 20，移动电话 20 在收到要求消息[INVITE]后，在步骤 3530，传送代表开始交换安全凭证的回复消息[200 OK]给移动电话 10。

接着，如步骤 3532，移动电话 20 传送向第一 KDC30 注册的注册要求消息[AP_REQ]给中继点装置 70，当中继点装置 70 收到消息后，在步骤 3534 及 3536，其重新产生内含第二电子装置 20 的身份 Bob@sipb.com 的使用者注册要求消息[USR_REG]，再传给第一 KDC30。接着，在步骤 3538、3540 及 3542 中，第一 KDC30 产生给移动电话 20 的注册 ID 并通过中继点装置 70 回传的回复消息[USR_REP]给移动电话 20。

当移动电话 20 收到该注册 ID 后，在步骤 3544 及 3546 中，移动电话 20 通过安全协议，例如 Diffie-Hellman，与第一 KDC30 进行安全信道建立([DH_REQ]及[DH_REP])，并在步骤 3548，以该注册 ID 与第一 KDC30 进行认证([AUTH_REQRSP])，以确认该注册 ID 确实由第一 KDC30 发给。因此，在步骤 3550 中，移动电话 20 与第一 KDC30 之间即可建立经认证且安全的信道。

然后，在步骤 3552，移动电话 20 送出通行证要求消息[TGS_REQ]向第一 KDC30 要求与移动电话 10 对话的通行证，因此，在步骤 3554，第一 KDC30 回传内含第二金钥及第二对话通行证(其中包含经过加密的第二金钥)的通行证回复消息[TGS_REP]给移动电话 20。在步骤 3556，移动电话 20 得到第二金钥及第二对话通行证并存储在其外来网域存储单元 130 后，在步骤 3558，将第二对话通行证通过递送单元 126 传给移动电话 10。

因此，在图 13 的步骤 3560 中，当移动电话 10 收到第二对话通行证时，即触发其本地网域获得单元 132 由该第二对话通行证中取出第二金钥，并将第二金钥存储在本地网域存储单元 134。然后，在图 13 的步骤 3564 中，移动电话 10 的共同金钥产生单元 122 被触发，以根据存储在本地网域存储单元 134 中的第二金钥，及存储在外来网域存储单元 130 中的第一金钥，使用诸如 pseudo-random 函数产生共享的第三金钥，并将第三金钥存储在本地网域存储单元 134 中。

同样，在图 13 的步骤 3562 中，当移动电话 20 收到第一对话通行证

时，即触发其本地网域获得单元 132 由该第一对话通行证中取出第一金钥，并将第一金钥存储在本地网域存储单元 134，然后，在图 13 的步骤 3566 中，移动电话 20 的共同金钥产生单元 122 被触发，以根据存储在本地网域存储单元 134 中的第一金钥，及存储在外来网域存储单元 130 中的第二金钥，使用诸如 pseudo-random 函数产生共享的第三金钥，并将第三金钥存储在本地网域存储单元 134 中。

这样，可保证第三金钥是只有移动电话 10 及 20 两者知道的共享金钥，该金钥不会被第三者(包括第一及第二 KDC30、40)得知，因此，分属于两个不同网域 55、65 的移动电话 10、20 即可使用第三金钥进行安全的跨网域身份认证，如图 13 的步骤 3568 所示。

此外，应该指出，为了减轻第二 KDC40(第一 KDC30 同)的工作负担，在本实施例中，让第二 KDC40 先将第一对话通行证连同第一金钥传给移动电话 10，再由移动电话 10 将第一对话通行证传给移动电话 20，但并不以此为限，亦即在不考虑第二 KDC40(第一 KDC30 同)工作负担的情况下，亦可由第二 KDC40 将第一对话通行证直接传给移动电话 20。

通过上述说明可知，本发明通过 SIP 代理服务器找寻同时在两个网域注册的非固定式的移动电话作为中继点装置，让分属于不同网域的移动电话可通过该中继点装置进行跨网域认证，不但不需要在两个网域服务器上采用复杂的跨网域信赖机制，而且不易受到网络攻击，使不同网域的移动电话达到安全的跨网域语音通信的功效与目的。

此外，本发明除了应用在跨网域语音通信的安全认证(如上述实施例)外，本发明亦可应用在(1)安全的跨网域短消息服务，例如短消息服务（SMS：Short Message Service)、多媒体消息服务（MMS：Multimedia Messaging Service)、SIP 通知（SIP Notify）及 SIP 消息（SIP Message）等；(2)安全的跨网域视频通信(video communication)或跨网域多媒体影音串流服务(multimedia streaming)，例如 MPEG4、H.264 等，诸如此类的跨网域信息通信安全认证，且由于其实施方式与上述实施例的主要技术手段相同，只是传送信息内容不同而已，在此不再赘述。

以上所说明的仅是本发明的优选实施例，而不能以此限定本发明实施的范围，本领域技术人员在不脱离所附权利要求所限定的精神和范围的情

况下对本发明内容所作的简单的等效变化与修饰，皆属于本发明涵盖的范围。

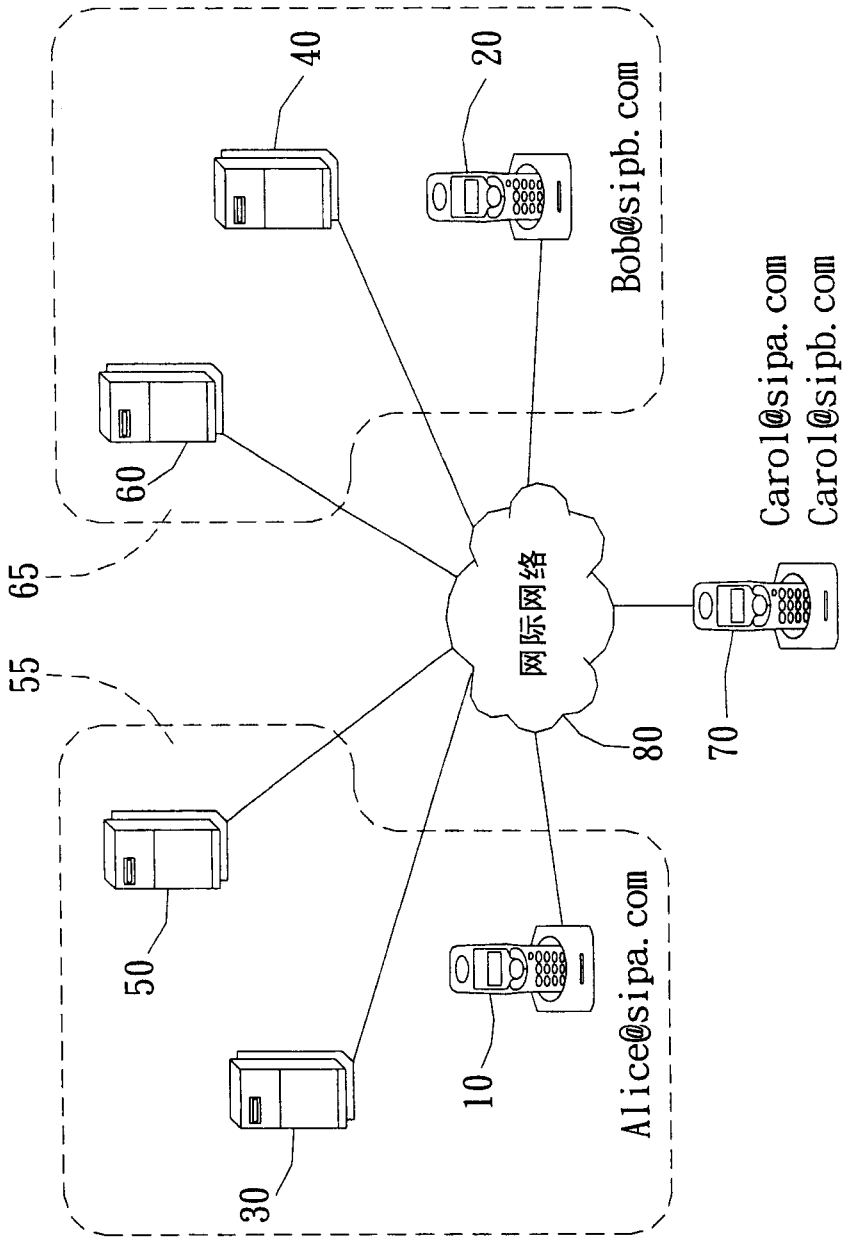

40
20
Bob@sipb.com
60
65
55
网际网络
Carol@sipa.com
Carol@sipb.com
80
70
50
10
30
Alice@sipa.com

图 1

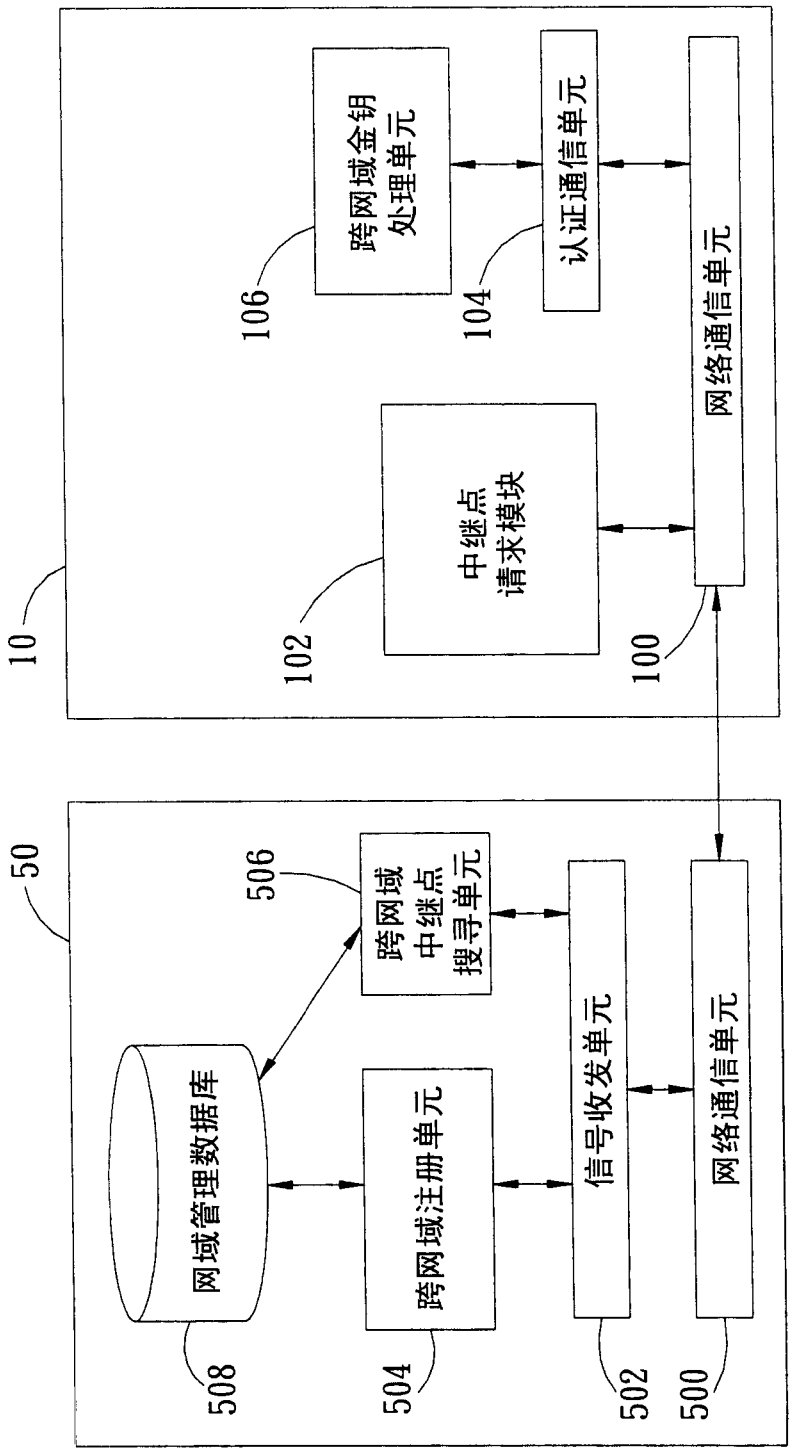

10
102
中继点
请求模块
106
跨网域金钥
处理单元
104
认证通信单元
100
网络通信单元
50
506
跨网域
中继点
搜寻单元
网域管理数据库
跨网域注册单元
信号收发单元
网络通信单元
508
504
502
500

图 2

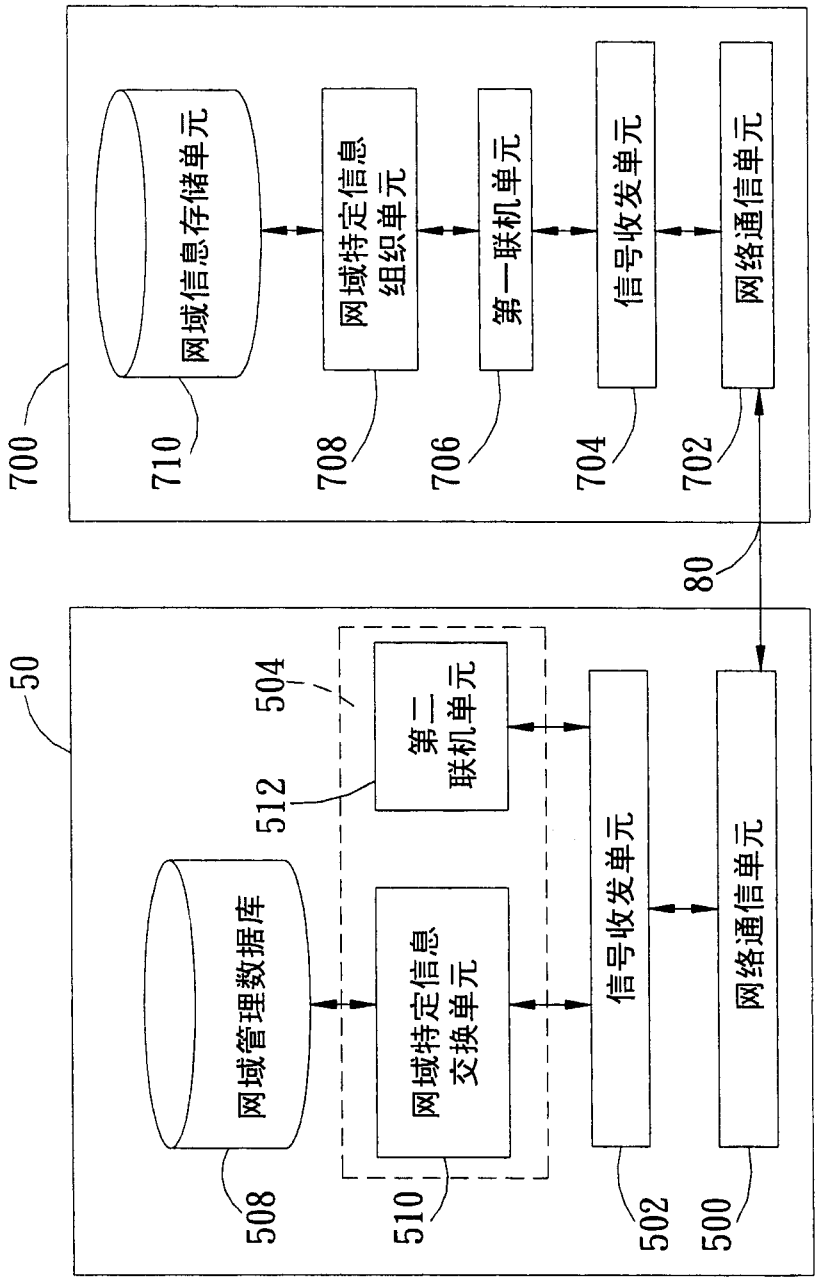

700
710
网域信息存储单元
708
网域特定信息组织单元
706
第一联机单元
704
信号收发单元
702
网络通信单元
80
50
504
512
第二联机单元
网域管理数据库
网域特定信息交换单元
信号收发单元
网络通信单元
508
510
502
500

图 3

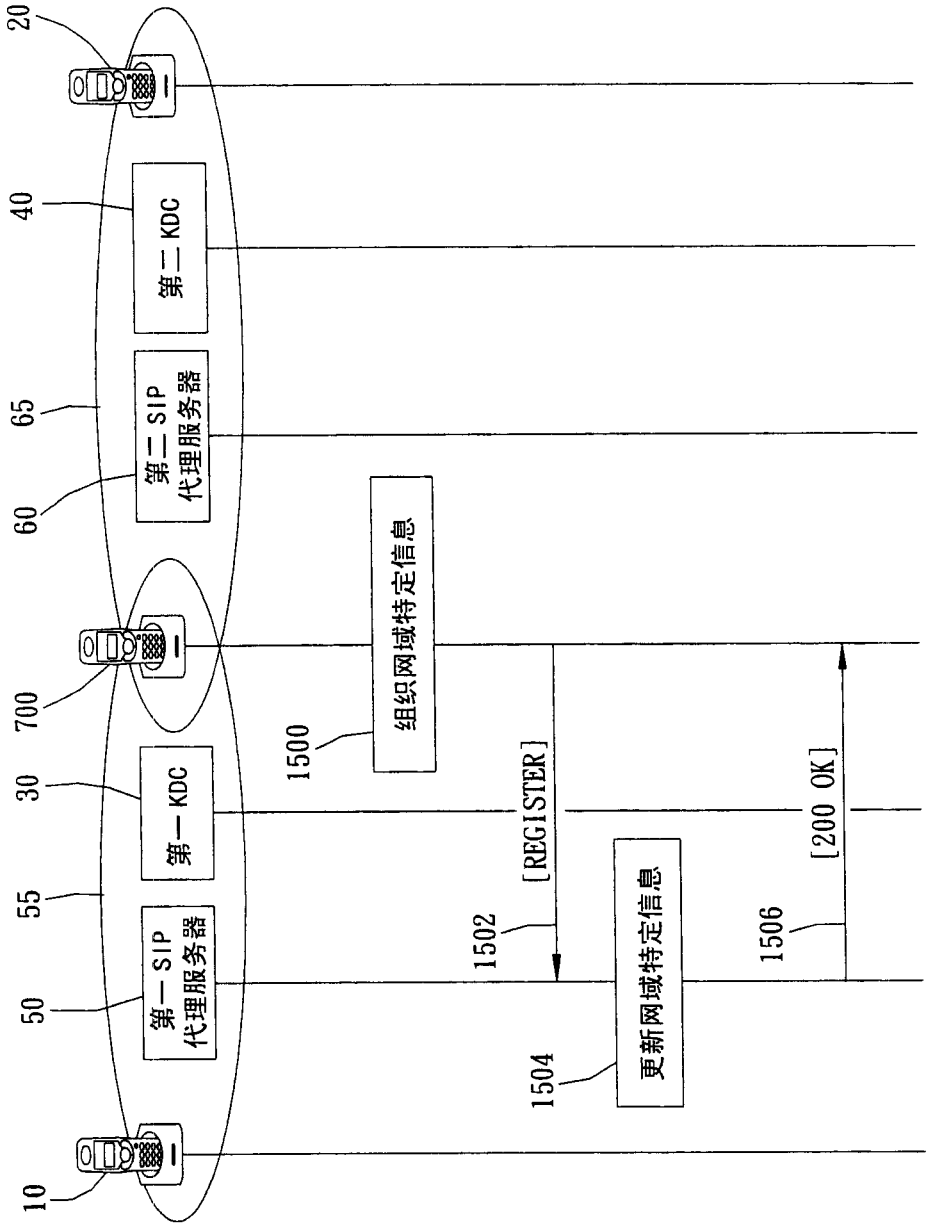

20
40
第二 KDC
65
第二 SIP
代理服务器
60
700
1500
组织网域特定信息
30
第一 KDC
55
第一 SIP
代理服务器
50
10
[REGISTER]
1502
1504
更新网域特定信息
[200 OK]
1506

图 4

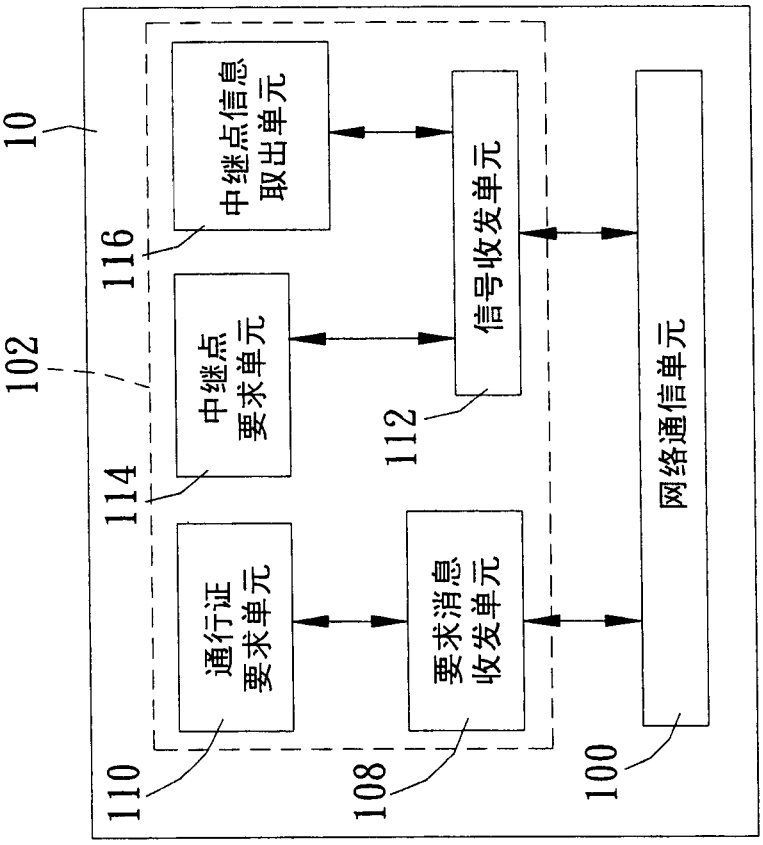

10
102
116
114
112
110
108
100
中继点信息取出单元
中继点要求单元
信号收发单元
通行证要求单元
要求消息收发单元
网络通信单元

图 5

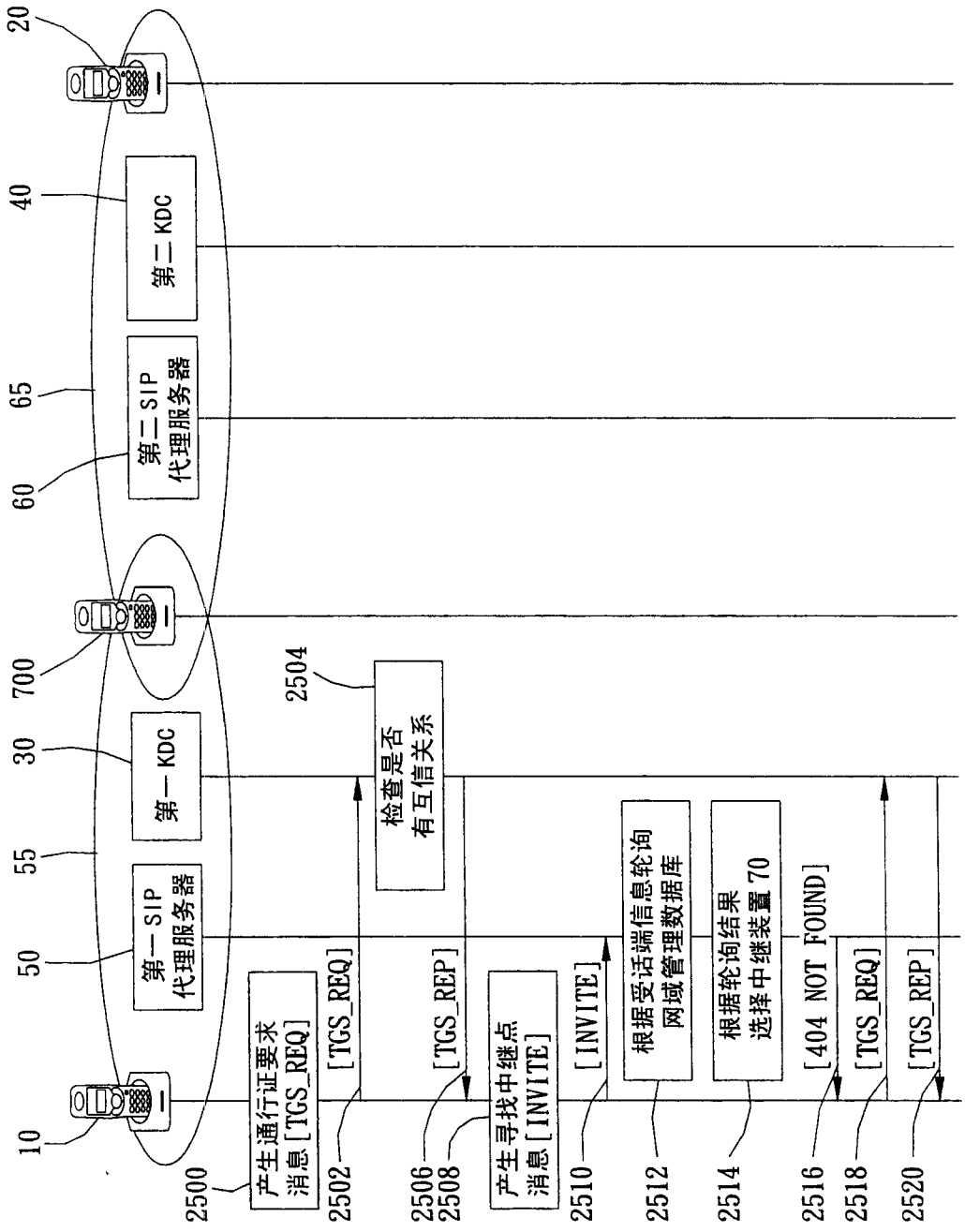

10
20
30
40
50
55
60
65
700
第一 KDC
第二 KDC
第一 SIP 代理服务器
第二 SIP 代理服务器
2500
产生通行证要求消息[TGS_REQ]
2502
[TGS_REQ]
2504
检查是否有互信关系
2506
2508
[TGS_REP]
产生寻找中继点消息[INVITE]
2510
[INVITE]
2512
根据受话端信息轮询网域管理数据库
2514
根据轮询结果选择中继装置70
2516
[404 NOT FOUND]
2518
[TGS_REQ]
2520
[TGS_REP]

图 6

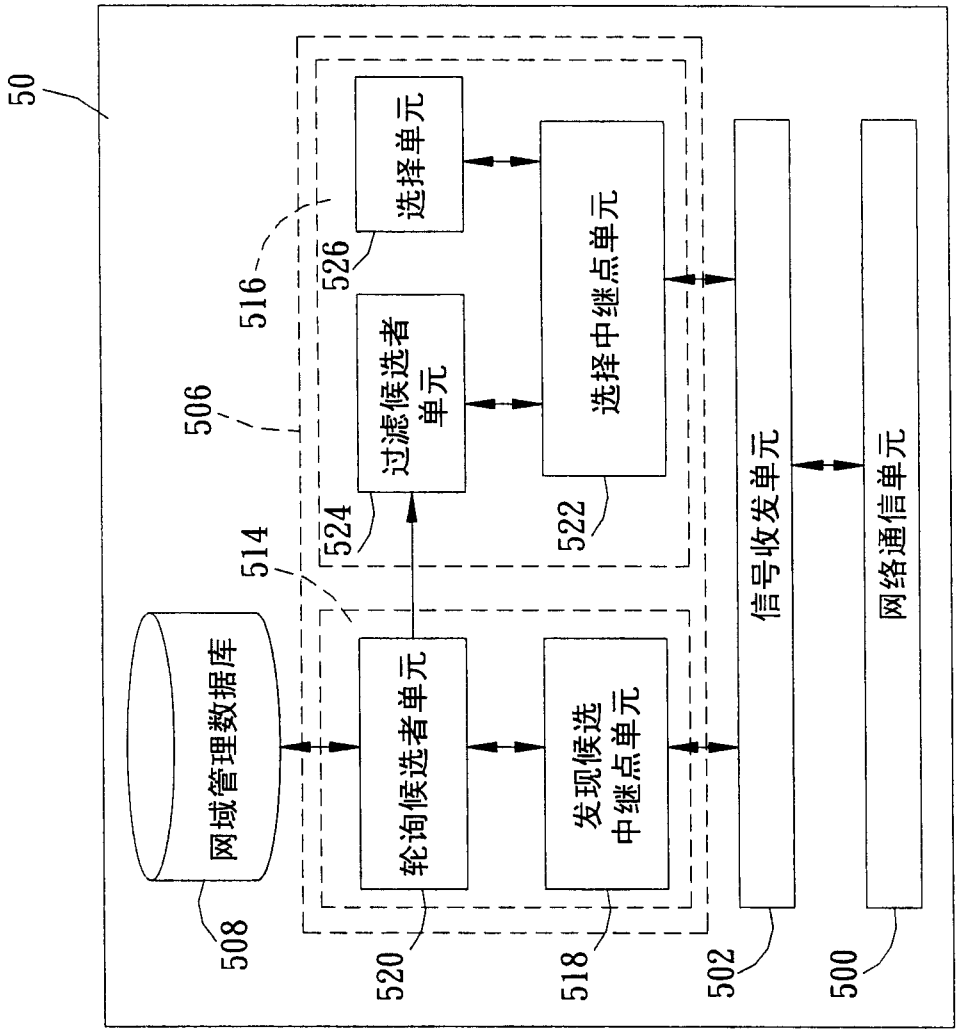

50
网域管理数据库
508
轮询候选者单元
520
发现候选中继点单元
518
514
506
516
过滤候选者单元
524
选择单元
526
选择中继点单元
522
信号收发单元
502
网络通信单元
500

图 7

候选中继点装置	硬件能力	最大服务数	目前服务数
Carol1@sipa.com	Pentium 4 (1GHz)	5	0
Carol2@sipa.com	Pentium 4 (2GHz)	2	1
Carol3@sipa.com	Pentium 4 (3GHz)	5	5

图 8

候选中继点装置	硬件能力	最大服务数	目前服务数
Carol1@sipa.com	Pentium 4 (1GHz)	5	0
Carol2@sipa.com	Pentium 4 (2GHz)	2	1

图 9

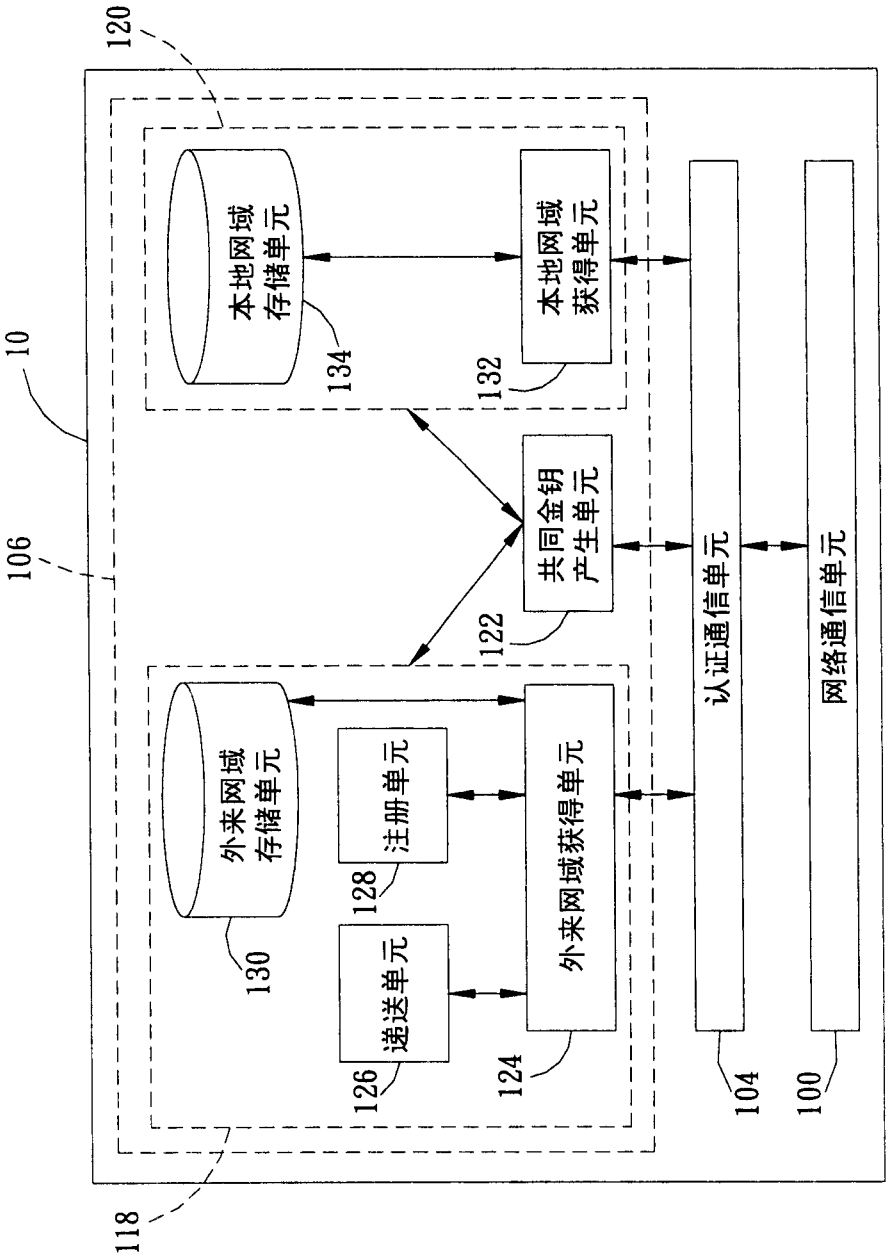

120
10
106
本地网域
存储单元
134
本地网域
获得单元
132
共同金钥
产生单元
122
外来网域
存储单元
130
注册单元
128
递送单元
126
外来网域获得单元
124
认证通信单元
104
网络通信单元
100
118

图 10

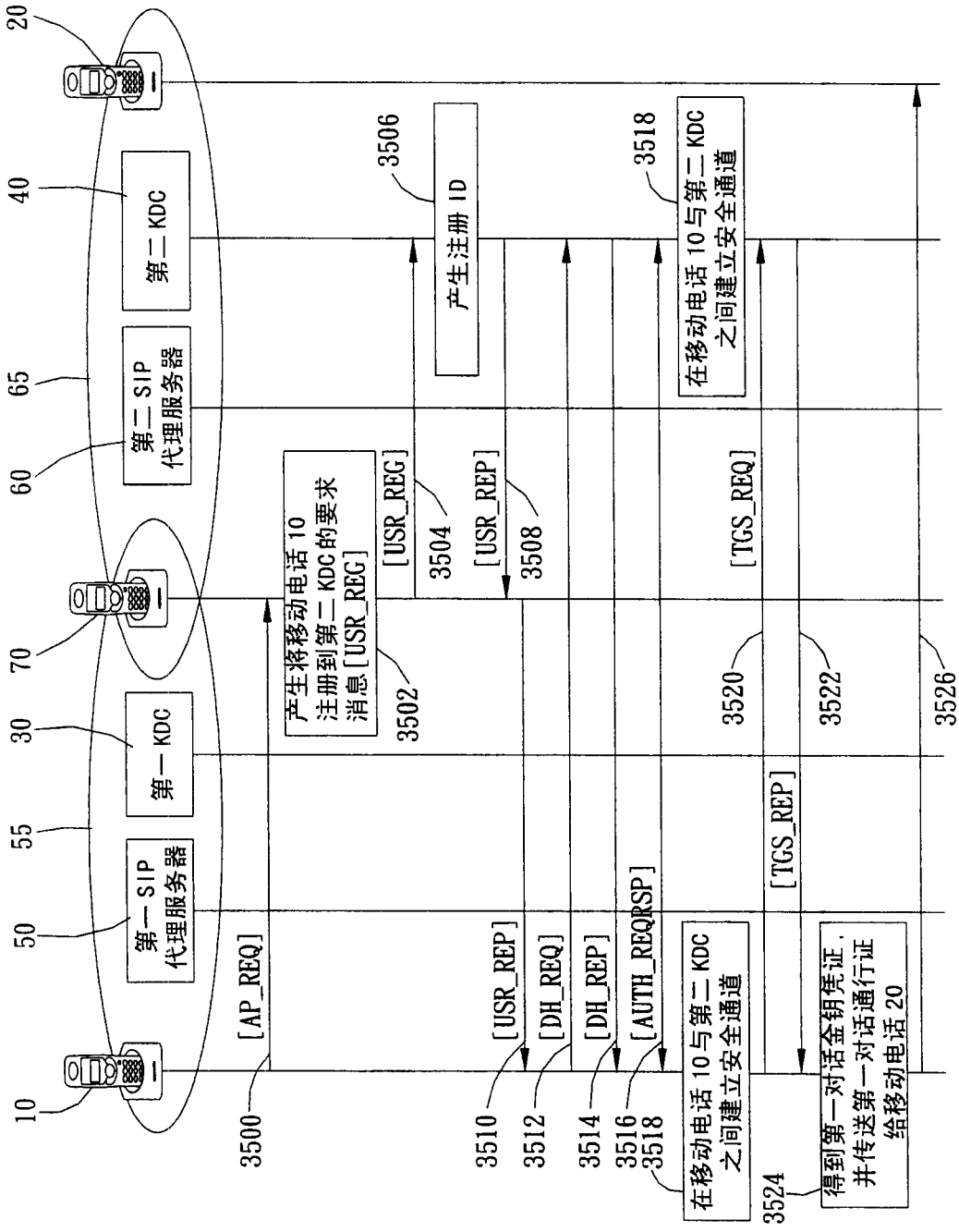

10
20
30
40
50
55
60
65
70
第一 SIP 代理服务器
第一 KDC
第二 SIP 代理服务器
第二 KDC
[AP_REQ]
3500
产生将移动电话 10 注册到第二 KDC 的要求消息 [USR_REG]
3502
[USR_REG]
3504
产生注册 ID
3506
[USR_REP]
3508
[USR_REP]
3510
[DH_REQ]
3512
[DH_REP]
3514
[AUTH_REQ/RSP]
3516
在移动电话 10 与第二 KDC 之间建立安全通道
3518
在移动电话 10 与第二 KDC 之间建立安全通道
3518
[TGS_REQ]
3520
[TGS_REP]
3522
得到第一对话金钥凭证，并传送第一对话通行证给移动电话 20
3524
3526

图 11

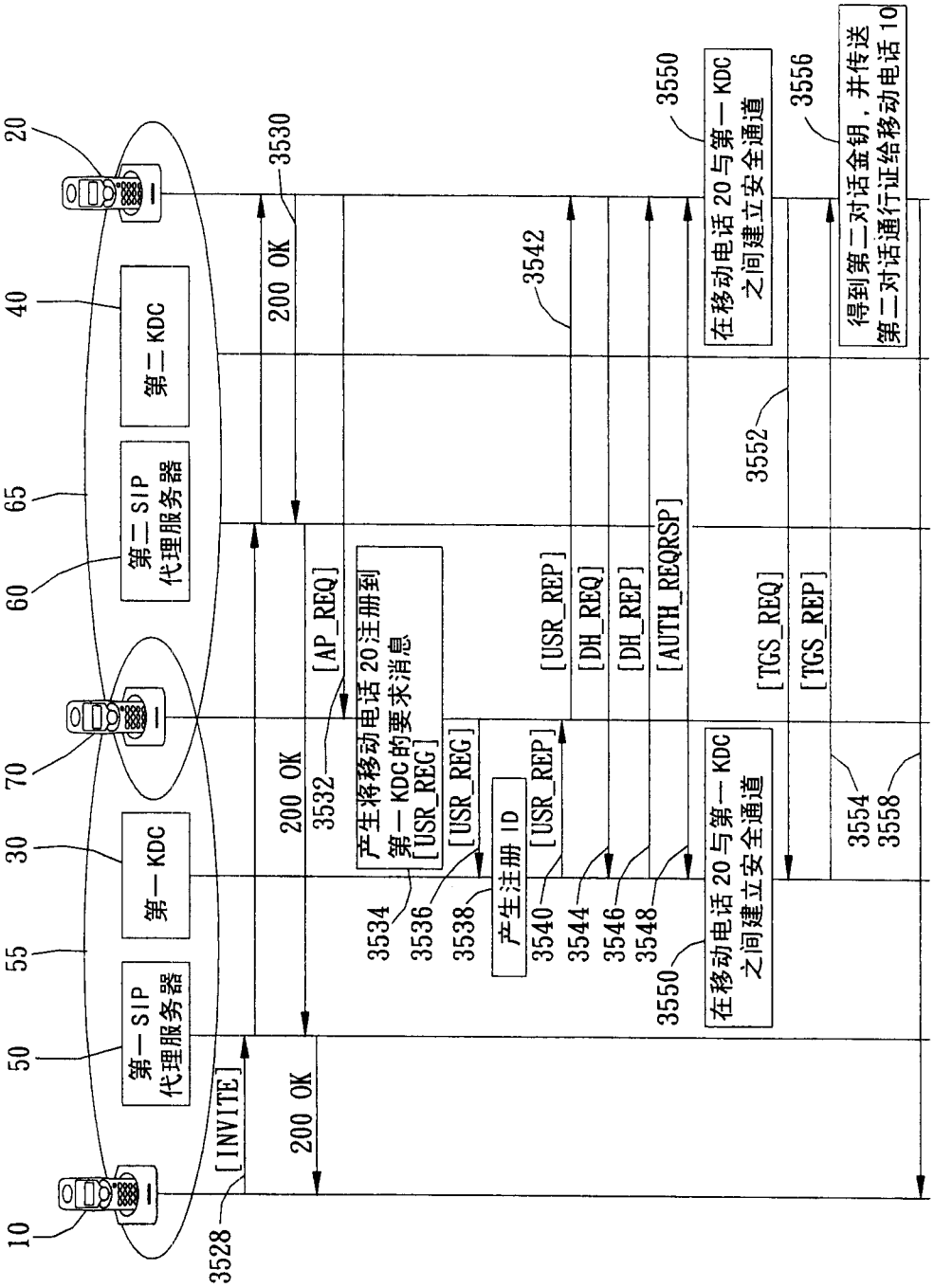

10
20
30
40
50
55
60
65
70
第一 SIP 代理服务器
第一 KDC
第二 SIP 代理服务器
第二 KDC
[INVITE]
200 OK
3528
3530
[AP_REQ]
3532
产生将移动电话 20 注册到第一 KDC 的要求消息
[USR_REG]
3534
3536
[USR_REG]
3538
产生注册 ID
[USR_REP]
3540
[USR_REP]
3542
[DH_REQ]
3544
[DH_REP]
3546
[AUTH_REQRSP]
3548
3550
在移动电话 20 与第一 KDC 之间建立安全通道
3550
在移动电话 20 与第一 KDC 之间建立安全通道
3552
[TGS_REQ]
[TGS_REP]
3554
3556
得到第二对话金钥，并传送第二对话通行证给移动电话 10
3558
200 OK

图 12

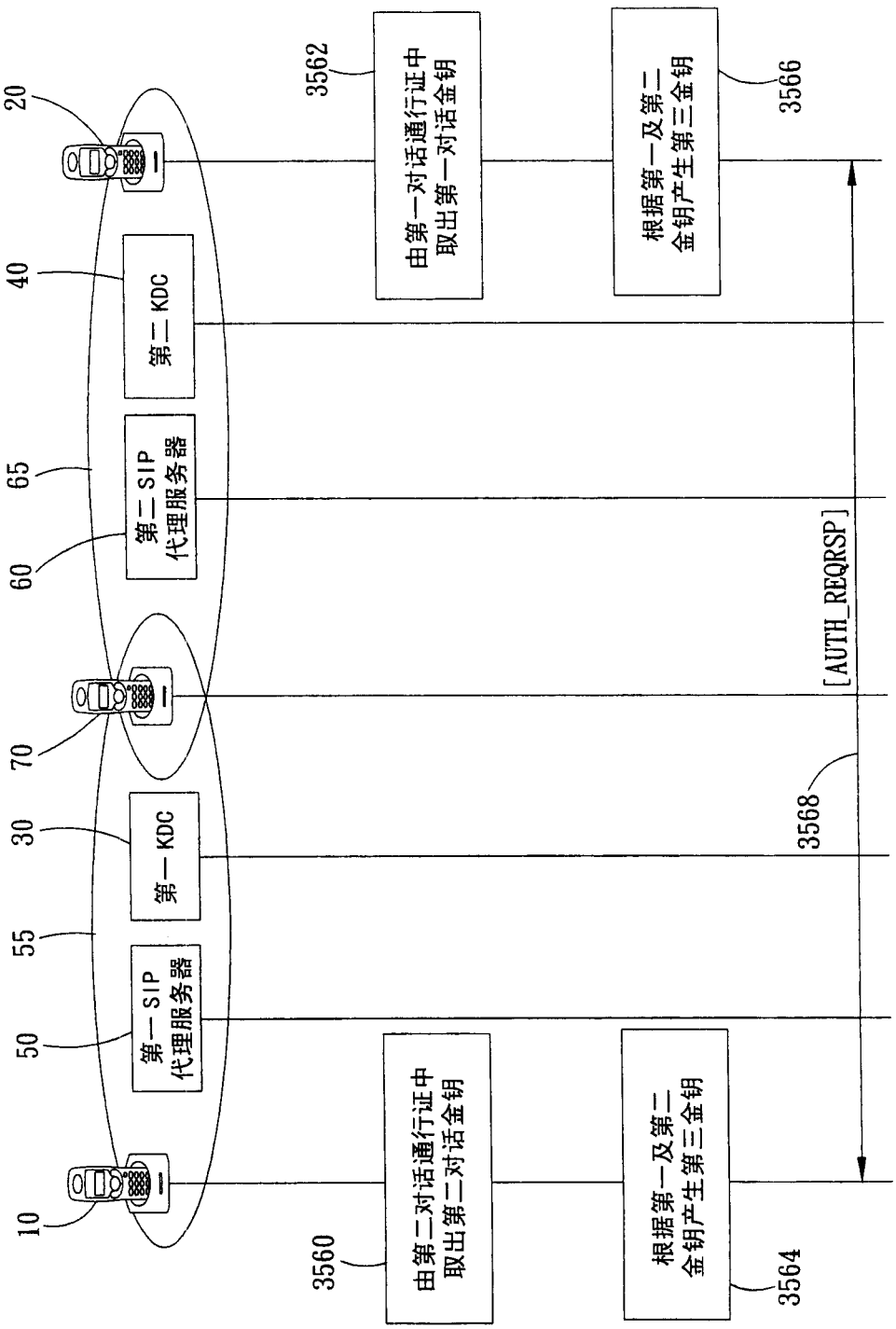

10
20
30
40
50
55
60
65
70
第一 SIP 代理服务器
第一 KDC
第二 SIP 代理服务器
第二 KDC
3560
由第二对话通行证中取出第二对话金钥
3562
由第一对话通行证中取出第一对话金钥
3564
根据第一及第二金钥产生第三金钥
3566
根据第一及第二金钥产生第三金钥
3568
[AUTH_REQRSP]

图 13