(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1701561 B
(45)授权公告日 2010.05.05

(21)申请号 200480001195.6

(22)申请日 2004.07.12

(30)优先权数据
273445/2003 2003.07.11 JP

(85)PCT申请进入国家阶段日
2005.04.30

(86)PCT申请的申请数据
PCT/JP2004/009944 2004.07.12

(87)PCT申请的公布数据
WO2005/011192 JA 2005.02.03

(73)专利权人 日本电信电话株式会社
地址 日本东京都

(72)发明人 鹤冈行雄 菊地能直 水野伸太郎
高桥健司 唐泽圭

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 黄小临 王志森

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)

(56)对比文件
WO 01/67708 A2,2001.09.13, 全文.
JP 特开2003-108517 A,2003.04.11, 全文.
JP 特开平5-333775 A,1993.12.17, 全文.
WO 03/055170 A1,2003.07.03, 说明书第4页第2段-第6页第2段,第12页第3段-第14页第3段,第20页第1段,附图1.
JP 特开2003-66836 A,2003.03.05, 全文.

审查员 刘剑波

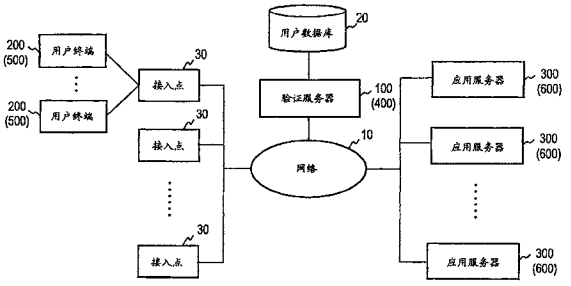
权利要求书 4 页 说明书 18 页 附图 19 页

(54)发明名称

基于地址的验证系统及其装置和程序

(57)摘要

由验证服务器分配给用户的地址被用作从用户终端发送的分组的IP地址,则防止了如果IP地址被窃取时的非法使用。验证服务器100根据从用户终端发送的用户验证信息来执行用户的验证,并且一旦成功验证,将地址分配给用户终端,并发出将返回到用户终端的包含地址的票。用户终端将票中包含的地址设定为源地址,并且在请求建立会话时,向应用服务器300发送票。在检验到该票真实之后,服务器300存储该票并且建立与用户终端的会话。用户终端利用会话向服务器300发送包含源地址的服务请求分组。如果源地址与所存储的票中包含的地址一致,则服务器300向用户提供服务。



CN 1701561 B

1. 一种基于地址的验证系统，在验证系统中，验证用户的验证服务器、发送用户验证信息的用户终端、以及通过用户终端向用户提供服务的应用服务器连接在一起，以便在它们之间能够通过网络进行通信，其中

所述验证服务器包括：

验证部件，用于根据作为验证请求而从用户终端发送的用户验证信息来验证用户；

地址分配部件，用于向成功验证用户的用户终端分配地址；

验证信息产生部件，用于根据包括所分配的地址的信息来产生验证信息；

票发出部件，用于发出包含由地址分配部件分配的所分配的地址和所述验证信息的票；和

票发送部件，用于向用户终端发送由票发出部件发出的票；

所述用户终端包括：

用户验证信息发送部件，用于为了验证请求而向验证服务器发送用户验证信息；

票接收部件，用于接收从验证服务器发送的包含所分配的地址的票；

用于将票中包含的所分配的地址设定为将要从用户终端发送的分组的源地址的部件；

用于向应用服务器发送包含所述票的分组以建立会话的部件；和

服务请求部件，用于通过所述会话向应用服务器发送请求服务的分组；以及

所述应用服务器包括：

票存储部件，用于存储从用户终端发送的票；

票检验部件，用于检验在从用户终端发送的票中的验证信息中是否存在任何伪造，并且在不存在伪造时将票存储在票存储部件中；

地址比较部件，用于确定在存储于票存储部件的票中包含的所分配的地址是否与通过所述会话从用户终端发送的服务请求分组的源地址一致；和

服务提供部件，用于当地址比较部件确定所述地址一致时向用户终端发送分组，所述分组向用户提供服务。

2. 根据权利要求 1 的验证系统，其中

用户终端具有与用户终端的公开密钥相关的密钥信息，

用户验证信息发送部件是用于将密钥信息和用户验证信息一起发送的部件，并且所述票发出部件是用于发出还包含从用户终端发送的密钥信息的所述票的部件，

用户终端还包括：

会话密钥产生部件，用于根据用户终端的私有密钥和应用服务器的公开密钥来计算与应用服务器共享的会话保密密钥；和

分组加密处理部件，用于通过会话保密密钥对要发送给应用服务器的分组进行加密处理，以保证分组中没有伪造；

所述应用服务器还包括：

会话密钥产生部件，用于根据应用服务器的私有密钥和用户终端的公开密钥来计算与用户终端共享的会话保密密钥；和

分组检验部件，用于使用会话保密密钥来确认从用户终端接收的分组是否被伪造；

其中，所述票检验部件被配置为检验在已被检验为未被伪造的分组的票中包含的密钥

信息是否是与用户终端的公开密钥相关的信息，并且如果不是，则防止所述票被存储在票存储部件中。

3. 根据权利要求 2 的验证系统，其中

所述应用服务器还包括 ：

地址核对部件，用于将从用户终端发送的票中的地址与包含所述票的分组的源地址进行核对，并且如果未发现一致则防止所述票被存储在票存储部件中。

4. 根据权利要求 2 的验证系统，其中验证服务器包括用户标识符分配部件，其用于响应于成功验证用户的验证请求而分配与已验证的用户对应的用户标识符，

所述票发出部件是用于发出包括用户标识符的票的部件。

5. 根据权利要求 1 至 4 中任一项权利要求的验证系统，其中

验证信息产生部件被配置为使用在验证服务器与应用服务器之间预先共享的共享保密密钥来处理包括所分配的地址的所述信息，

应用服务器的票检验部件还被配置为使用在验证服务器与应用服务器之间预先共享的共享保密密钥来检验包含在票中的验证信息。

6. 根据权利要求 1 至 4 中任一项权利要求的系统，其中，验证服务器具有用于数字签名的一对私有密钥和公开密钥，在验证服务器处的产生验证信息的步骤是使用用于数字签名的私有密钥对包括所分配的地址的信息计算数字签名的步骤，

在应用服务器处的票检验步骤是使用验证服务器的公开密钥检验在所述票中的验证信息中是否存在任何伪造的步骤。

7. 根据权利要求 1 或 4 的验证系统，其中，

应用服务器包括地址核对部件，其用于核对从用户终端发送的票中的地址与包括所述票的分组的源地址，并且用于在未发现一致时防止所述票被存储在票存储部件中。

8. 一种验证系统中的验证服务器，在该验证系统中，通过用户终端，验证服务器执行使用用户终端的用户的验证，并且根据所述验证，对应用服务器做出提供服务的请求，所述验证服务器包括 ：

用户验证信息接收部件，用于接收包括均从用户终端发送的用户验证信息以及与用户终端的公开密钥相关的密钥信息的验证请求 ；

验证部件，其中输入了接收到的验证请求的用户验证信息，并且根据用户验证信息来验证用户，并且一旦成功验证就提供表示成功验证的信号 ；

地址分配部件，用于响应于表示用户成功验证的信号的输入而向用户终端分配地址 ；

验证信息产生部件，用于根据包括至少所分配的地址和所述密钥信息的信息来产生验证信息 ；

票发出部件，用于向其用户被验证部件验证的用户终端发出包含由地址分配部件分配的所分配的地址、所述密钥信息以及所述验证信息的票 ；和

票发送部件，其中输入了由票发出部件发出的所述票，并且向用户终端发送所述票。

9. 根据权利要求 8 的验证服务器，其中，验证信息产生部件被配置为通过使用在验证服务器与应用服务器之间预先共享的共享保密密钥处理包括所分配的地址和所述密钥信息的信息，来产生所述验证信息。

10. 根据权利要求 8 的验证服务器，其中，验证服务器具有用于数字签名的一对私有密

钥和公开密钥，并且所述票发出部件包括：验证信息产生部件，使用用于数字签名的私有密钥对包括至少所分配的地址的信息计算数字签名以产生所述验证信息，使得应用服务器能够使用验证服务器的公开密钥检验在票中的验证信息中是否存在任何伪造。

11. 根据权利要求 8 的验证服务器，还包括：

用户标识符分配部件，用于当用户验证成功时，响应于验证请求而分配与已验证的用户对应的用户标识符，

其中，所述验证信息产生部件被配置为处理包括所分配的地址、所述密钥信息和所述用户标识符的信息以产生所述验证信息，并且票发出部件被配置为将至少所述验证信息、所分配的地址、所述密钥信息和所述用户标识符组合以形成所述票。

12. 根据权利要求 11 的验证服务器，其中用户标识符分配部件被配置为通过使用验证服务器的标识符产生保密密钥来加密直接识别用户的信息，以产生所述用户标识符。

13. 一种验证系统中的用户终端，在该验证系统中，验证服务器执行使用用户终端的用户的验证，并且根据所述验证对应用服务器做出提供服务的请求，所述用户终端包括：

票接收部件，用于接收从验证服务器发送的票，所述票包含分配给用户终端的地址、与用户终端的公开密钥相关的密钥信息、以及通过处理包括所分配的地址和所述密钥信息的信息而产生的验证信息；

源地址设定部件，其中输入了由票接收部件接收到的所述票，并且将所述票中包含的所分配的地址设定为用户终端的源地址；

会话建立部件，其中输入了由票接收部件接收到的所述票，并且向应用服务器发送包括所述票的分组，以建立与应用服务器的会话；

服务请求部件，用于通过所建立的会话向应用服务器发送表示服务请求的分组；

密钥信息产生部件，其中输入了用户终端的公开密钥，并且产生与用户终端的公开密钥相关的密钥信息；

会话密钥产生部件，其中输入了用户终端的私有密钥和应用服务器的公开密钥，并且计算与应用服务器共享的会话保密密钥；

分组加密处理部件，其中输入了要从用户终端发送的分组和会话保密密钥，并且使用会话保密密钥对所述分组施加加密处理以便保证在所述分组中没有伪造；以及

用户验证信息发送部件，其被配置为将所述密钥信息和用户验证信息一起发送给验证服务器。

14. 一种验证系统中的用户终端，在该验证系统中，验证服务器执行使用用户终端的用户的验证，并且根据所述验证对应用服务器做出提供服务的请求，所述用户终端包括：

票接收部件，用于接收从验证服务器发送的票，所述票包含分配给用户终端的地址、与用户终端的公开密钥相关的密钥信息、以及通过处理包括所分配的地址和所述密钥信息的信息而产生的验证信息；

源地址设定部件，其中输入了由票接收部件接收到的所述票，并且将所述票中包含的所分配的地址设定为用户终端的源地址；

会话建立部件，其中输入了由票接收部件接收到的所述票，并且向应用服务器发送包括所述票的分组，以建立与应用服务器的会话；

服务请求部件，用于通过所建立的会话向应用服务器发送表示服务请求的分组；

密钥信息产生部件，其中输入了与应用服务器共享的用于验证的共享保密密钥和每次建立会话时改变的会话相关信息，并且通过用于验证的共享保密密钥处理会话相关信息来产生密钥信息；以及

用户验证信息发送部件，其被配置为将密钥信息和用户验证信息一起发送给验证服务器。

15. 一种验证系统中的应用服务器，在该验证系统中，验证服务器执行使用用户终端的用户的验证，并且根据所述验证对应用服务器做出提供服务的请求，所述应用服务器包括：

会话建立部件，用于建立与用户终端的会话；

票存储部件，其中存储了从用户终端发送的票；

地址比较部件，其中输入了从用户终端发送并通过所建立的会话接收的服务请求分组的源地址，并且确定该源地址是否与在票存储部件中存储的票中包含的用户终端的所分配的地址一致；和

服务提供部件，其在地址比较部件的输出指示一致时，向用户终端发送用于向用户提供服务的分组；

其中，所述会话建立部件包括票检验部件，该票检验部件用于通过检查包含在所述票中的验证信息来检验通过来自用户终端的用于建立会话的分组接收的票的真实性，并且在检验不成功时防止所述票被存储在票存储部件中。

16. 根据权利要求 15 的应用服务器，还包括：

会话密钥产生部件，用于根据应用服务器的私有密钥和用户终端的公开密钥来计算与用户终端共享的会话保密密钥；和

分组检验部件，用于使用会话保密密钥来检验从用户终端接收的分组是否被伪造，并且响应于表示存在伪造的检验输出而防止所述票被存储。

17. 根据权利要求 16 的应用服务器，其中所述票检验部件包括核对部件，该核对部件用于在接收到被分组检验部件检验为未被伪造的分组时，检验包含在所述票中的密钥信息是否对应于在计算会话保密密钥中已被使用的用户终端的公开密钥。

18. 根据权利要求 15 的应用服务器，其中所述票检验部件包括终端验证部件，其中输入了与用户终端共享的用于验证的共享保密密钥和每次建立会话时改变的会话相关信息，并且使用该用于验证的共享保密密钥来处理会话相关信息，将处理结果与所述票中的密钥信息进行核对并通过查看处理结果与密钥信息之间是否匹配来检验所述票的真实性。

19. 根据权利要求 15、17 和 18 中任一项权利要求的应用服务器，其中票检验部件包括用于检验所接收的分组的源地址是否与分组内的所述票中包含的地址一致、以及响应于表示不一致的检测输出而防止所述票被存储的部件。

基于地址的验证系统及其装置和程序

技术领域

[0001] 本发明涉及一种用于用户终端从验证服务器接收用户验证并且根据接收到的验证来请求由应用服务器提供的服务的验证系统，尤其涉及这样一种验证系统及其装置和程序，即其中一旦用户验证成功时，验证服务器向用户终端分配源地址并且用户使用所分配的源地址请求应用服务器提供的服务。

背景技术

[0002] 当用户期望通过诸如因特网的网络从服务器获得服务时，通常的实践是，在用户的终端（用户终端）与服务器之间建立会话并且通过该会话将服务请求发送至服务器。由于服务器提供的服务要收费，所以服务器要求在提供服务之前验证用户，并且一旦验证成功，它就通过所建立的会话来提供服务。因此，每次对服务器进行服务请求时都发生用户验证，并且通过所建立的会话来提供服务。如果所提供的服务覆盖多个分组，则通过相同的会话来提供服务。

[0003] 鉴于如果响应每个服务请求执行用户验证而使每个应用服务器经历的吞吐量增加，提出了一种由验证服务器执行的用户验证的方法，其中一旦成功验证，就向用户分配 IP 地址，然后用户使用 IP 地址作为源地址来请求服务器提供服务。

[0004] 在现有的网络验证系统中，例如在专利文献中公开了如下所述的这种基于地址的验证方法。具体地，当用户利用连接服务时，网络接入验证服务器参考个人信息数据库，其中预先存储了客户信息与用户 ID（唯一识别用户的信息）之间的对应关系以便验证用户，并且一旦成功验证，就向用户的终端一起分配 IP（因特网协议）地址和连接许可，在存储器中存储 IP 地址与用户 ID 之间的关系的同时向用户终端发送所分配的 IP 地址，并且当利用商业交易服务时，用户终端在因特网上使用从网络接入验证服务器发送的 IP 地址向销售服务提供商装置提出购买货物，销售服务提供商地址获得货物购买提出 (proposal) 包的源 IP 地址并且向网络接入验证服务器发送该用于查询的 IP 地址以根据 IP 地址获取用户 ID，并且随后获取与所获取的用户 ID 对应的客户信息用以验证客户。

[0005] 专利文献 1 :公开的日本申请，公开号 :No. 2002-207929

发明内容

[0006] 然而，上述的现有技术的验证系统出现这样一个问题 :在用户的网络接入验证期间或者当提供服务时，第三方可能从在网络上发送或者接收的分组中窃取用户使用的 IP 地址，从而能够通过访问提供商业交易服务的服务器来进行假冒。换句话说，现有技术的基于地址的验证系统不能保证向用户分配的地址的真实性。应当注意，真实的地址是指诸如 ISP（因特网服务提供商）的组织根据正确过程向用户或用户终端分配的地址。

[0007] 本发明的一个目的是提供一种基于地址的验证系统、装置和程序，因此能够保证分配给用户的地址的真实性，从而克服了现有技术的这种问题。

[0008] 解决问题的手段

[0009] 根据本发明的一个方面，提供了一种基于地址的验证系统，在验证系统中，验证用户的验证服务器、发送用户验证信息的用户终端、以及通过用户终端向用户提供服务的应用服务器连接在一起，以便在它们之间能够通过网络进行通信，所述验证服务器包括：验证部件，用于根据作为验证请求而从用户终端发送的用户验证信息来验证用户；地址分配部件，用于向成功验证用户的用户终端分配地址；验证信息产生部件，用于根据包括所分配的地址的信息来产生验证信息；票发出（issuing）部件，用于发出包含由地址分配部件分配的所分配的地址和所述验证信息的票；和票发送部件，用于向用户终端发送由票发出部件发出的票；所述用户终端包括：用户验证信息发送部件，用于为了验证请求而向验证服务器发送用户验证信息；票接收部件，用于接收从验证服务器发送的包含所分配的地址的票；用于将票中包含的所分配的地址设定为将要从用户终端发送的分组的源地址的部件；用于向应用服务器发送包含票的分组以建立会话的部件；和服务请求部件，用于通过所述会话向应用服务器发送请求服务的分组；所述应用服务器包括：票存储部件，用于存储从用户终端发送的票；票检验部件，用于检验在从用户终端发送的票中的验证信息中是否存在任何伪造，并且在不存在伪造时将票存储在票存储部件中；地址比较部件，用于确定在存储于票存储部件的票中包含的所分配的地址是否与通过所述会话从用户终端发送的服务请求分组的源地址一致；和服务提供部件，用于当地址比较部件确定所述地址一致时向用户终端发送分组，所述分组向用户提供服务。

[0010] 根据本发明的另一方面，提供了一种验证系统中的验证服务器，在该验证系统中，通过用户终端，验证服务器执行使用用户终端的用户的验证，并且根据所述验证，对应用服务器做出提供服务的请求，所述验证服务器包括：用户验证信息接收部件，用于接收包括均从用户终端发送的用户验证信息以及与用户终端的公开密钥相关的密钥信息的验证请求；验证部件，其中输入了接收到的验证请求的用户验证信息，并且根据用户验证信息来验证用户，并且一旦成功验证就提供表示成功验证的信号；地址分配部件，用于响应于表示用户成功验证的信号的输入而向用户终端分配地址；验证信息产生部件，用于根据包括至少所分配的地址和所述密钥信息的信息来产生验证信息；票发出部件，用于向其用户被验证部件验证的用户终端发出包含由地址分配部件分配的所分配的地址、所述密钥信息以及所述验证信息的票；和票发送部件，其中输入了票，并且向用户终端发送票。

[0011] 根据本发明的另一方面，提供了一种验证系统中的用户终端，在该验证系统中，验证服务器执行使用用户终端的用户的验证，并且根据所述验证对应用服务器做出提供服务的请求，所述用户终端包括：票接收部件，用于接收从验证服务器发送的票，所述票包含分配给用户终端的地址、与用户终端的公开密钥相关的密钥信息、以及通过处理包括所分配的地址和所述密钥信息的信息而产生的验证信息；源地址设定部件，其中输入了接收到的票，并且将票中包含的所分配的地址设定为用户终端的源地址；会话建立部件，其中输入了票，并且向应用服务器发送包括票的分组，以建立与应用服务器的会话；服务请求部件，用于通过所建立的会话向应用服务器发送表示服务请求的分组；密钥信息产生部件，其中输入了用户终端的公开密钥，并且产生与用户终端的公开密钥相关的密钥信息；会话密钥产生部件，其中输入了用户终端的私有密钥和应用服务器的公开密钥，并且计算与应用服务器共享的会话保密密钥；和分组加密处理部件，其中输入了要从用户终端发送的分组和会话保密密钥，并且通过会话保密密钥对所发送的分组进行加密处理，其保证在分组中没有

伪造；用户验证信息发送部件，其被配置为将所述密钥信息和用户验证信息一起发送给验证服务器。

[0012] 根据本发明的另一方面，提供了一种验证系统中的应用服务器，在该验证系统中，验证服务器执行使用用户终端的用户的验证，并且根据所述验证对应用服务器做出提供服务的请求，所述应用服务器包括：会话建立部件，用于建立与用户终端的会话；票存储部件，其中存储了从用户终端发送的票；地址比较部件，其中输入了从用户终端发送并通过所建立的会话接收的服务请求分组的源地址，并且确定源地址是否与在票存储部件中存储的票中包含的用户终端的所分配的地址一致；和服务提供部件，其在地址比较部件的输出指示一致时，向用户终端发送用于向用户提供服务的分组；其中，所述会话建立部件包括票检验部件，该票检验部件用于通过检查包含在票中的验证信息来检验通过来自用户终端的用于建立会话的分组接收的票的真实性，并且在检验不成功时防止票被存储在票存储部件中。

[0013] 发明效果

[0014] 使用所述结构，通过相同的验证服务器来执行用户的验证和地址的分配，由此，保证地址仅被分配给有效的用户。由于相同的验证服务器执行地址的分配和票的发出，因此通过票能够保证地址的真实性。

[0015] 由于地址是根据用户验证来发出的，所以能够保证地址的真实性。另外，票到应用服务器的发送仅发生一次，并且由于该票中包含的地址是验证服务器向用户终端给出的有效用户正好请求其验证的地址，并且由于该票中的地址被作为源地址，因此如果通过对于票发送而建立的会话从用户终端发送的每个服务请求分组的源地址与所存储的票中包含的地址一致，则那个分组可以被认为是来自已验证的用户的分组。因此，服务请求分组的源地址通过在建立会话时期间仅发送一次的票中包含的地址而与已验证的用户相关联。如果第三方窃取了服务请求分组的源地址并且使用它对应用服务器进行服务请求，则在那个会话期间所存储的票中包含的地址不与源地址一致，从而防止提供服务。

附图说明

[0016] 图 1 是示出根据执行本发明的第一和第二模式的验证系统的示例性系统结构的方框图；

[0017] 图 2 是示出根据执行本发明的第一模式的验证服务器的示例性功能结构的方框图；

[0018] 图 3 是示出根据执行本发明的第一模式的用户终端的示例性功能结构的方框图；

[0019] 图 4 是示出根据执行本发明的第一模式的应用服务器的示例性功能结构的方框图；

[0020] 图 5 是示出在执行本发明的第一模式中使用的票的构造的示例图；

[0021] 图 6 是示出包括在执行本发明的第一模式中使用的票的分组的构造的示例图；

[0022] 图 7 是示出根据执行本发明的第一模式的验证系统的示例处理过程的顺序图；

[0023] 图 8 是示出由根据执行本发明的第一模式的验证服务器处理的示例流程的流程图；

[0024] 图 9A 是示出在根据执行本发明的第一模式的用户终端在用户验证期间发生的处

理的示例流程的流程图；

[0025] 图 9B 是示出在服务请求期间发生的处理的示例流程的流程图；

[0026] 图 10 是示出由根据执行本发明的第一模式的应用服务器处理的示例流程的流程图；

[0027] 图 11A 和 11B 图解了图 2 所示的验证信息产生部件 151 的不同功能结构的示例；

[0028] 图 11C 图解了图 4 所示的验证信息检验器 320a 的不同功能结构的示例；

[0029] 图 12 是示出根据执行本发明的第二模式的验证服务器的示例性功能结构的方框图；

[0030] 图 13 是示出根据执行本发明的第二模式的用户终端的示例性功能结构的方框图；

[0031] 图 14 是示出根据执行本发明的第二模式的应用服务器的示例性功能结构的方框图；

[0032] 图 15 是示出在执行本发明的第二模式中使用的票的构造的示例图；

[0033] 图 16 是示出被添加有在执行本发明的第二模式中使用的验证头标的分组的构造的示例图；

[0034] 图 17 是示出根据执行本发明的第二模式的验证系统的示例处理过程的顺序图；

[0035] 图 18 是示出由根据执行本发明的第二模式的验证服务器处理的示例流程的流程图；

[0036] 图 19A 是示出在根据执行本发明的第二模式的用户验证期间在用户终端发生的处理的示例流程的流程图；

[0037] 图 19B 是示出服务请求期间的处理的示例流程的流程图；

[0038] 图 20 是示出由根据执行本发明的第二模式的应用服务器处理的示例流程的流程图；

[0039] 图 21A 是示出在使用密钥信息的另一个示例时验证系统中的示例处理过程的顺序图；

[0040] 图 21B 是示出被添加到图 12 所示的验证服务器的质询发生器 (challengegenerator) 的具体示例的方框图；

[0041] 图 21C 是示出图 13 的密钥信息发生器的另一具体示例的方框图；和

[0042] 图 21D 是示出图 14 的票检验部件 620 内的修改的具体示例的方框图。

具体实施方式

[0043] 现在将参考附图来详细描述执行本发明的几个模式。在下面的说明中，为了避免重复说明，相应的部件由相同的参考符号表示。

[0044] [第一模式] 系统结构

[0045] 图 1 是示出根据执行本发明的第一模式的基于地址的验证系统的系统结构图。根据本发明的基于地址的验证系统包括：验证用户的验证服务器 100；覆盖多个用户终端 200 的接入点 300，所述多个用户终端 200 发送用户验证信息；和多个应用服务器 300，其向用户终端 200 发送分组，所述分组向用户提供服务，所有这些部件连接在一起，以这种方式允许通过网络 10 在它们之间进行通信。

[0046] 验证服务器 100 与存储关于用户的信息（用户验证数据）的用户数据库 20 相连接。用户不限于操作用户终端 200 的用户，还可以是充当操作员的程序自身，例如其就可以是像在计算机的程序执行期间用户正在利用用户终端一样。基于地址的验证系统可以被构造成物理地保护用户终端 200 与应用服务器 300 之间的网络安全。在该示例中，不需要确认是否伪造了从用户终端 200 向应用服务器 300 发送的分组的处理。

[0047] 网络 10 可以包括无线和有线网络、LAN（局域网）或者因特网。可以对于每个给定区域提供接入点 30。用户终端 200 可以包括能够进行无线通信的蜂窝电话、手机、个人设备或个人计算机。应用服务器 300 可以包括提供内容分发服务的服务器，所述内容分发服务包括电影和体育节目、电子商务交易服务、电子邮件的通信服务、IP 电话和即时消息、或者诸如万维网的信息浏览器服务。另外，应用服务器 300 也可以包括网关服务器或防火墙，用于在独立的网络上提供服务的接入。

[0048] 用户终端 200 通过经由接入点 30 发送用户验证信息来请求用户的验证，所述用户验证信息被要求用于由验证服务器 100 来验证用户。在执行本发明的这种模式中，用户验证信息包括至少下列之一：用户标识符和口令、根据密钥对产生以验证用户的信息、用于验证用户的生物学测定特征 (biometrics)（例如指纹、虹膜、脉相、笔迹、语音印迹等）的信息、和在已知的各种用户验证技术中使用的其他信息。应当注意，密钥对表示一对基于公开密钥加密技术的公开密钥和私有密钥。

[0049] 验证服务器 100 根据从用户终端 200 发送的用户验证信息通过参考用户数据库 20 来验证用户，并且一旦用户验证成功，则分配与用户对应的用户标识符，并且分配能够唯一识别与所分配的用户标识符相对应的用户终端的地址，发出包括所分配的地址和用户标识符的票，并且将所发出的票发送至用户终端 200。

[0050] 用户终端 200 使用在从验证服务器 100 发送的票中包含的地址作为用于从用户终端 200 发送的分组的源地址，并且开始将票发送至应用服务器 100，随后发送请求服务的分组（以后称之为服务请求分组）。

[0051] 应用服务器 300 存储从用户终端 200 发送的票，确定包含在所存储的票中的地址是否与服务请求分组的源地址一致，并且一旦确定地址一致时，将向用户提供服务的分组发送至用户终端 200。

[0052] [第一模式] 验证服务器

[0053] 图 2 是在执行本发明的第一模式中使用的验证服务器的方框图。验证服务器 100 包括通信接口 101 和控制处理部件 102。通信接口 101 可以包括例如调制解调器或 LAN 接口，并且任何部件只要能够与连接到网络 10 的通信设备通信就可被用来构造该通信接口。

[0054] 控制处理部件 102 包括：具有执行程序的 CPU（中央处理单元）的控制单元 102a、存储程序等的存储器、用户验证信息接收部件 110、验证部件 120、用户标识符分配部件 130、地址分配部件 140、票发出部件 150 和票发送部件 160。应当理解，这些部件不必构造成硬件，而是通过程序执行实现的功能。

[0055] 上述的验证服务器 100 连接到存储了与用户相关的信息的用户数据库 20，并且用户数据库 20 存储有用户 ID 条目数据，包括在验证用户时使用的验证数据和用户 ID（例如用于唯一识别用户自身的名称或信息）。

[0056] 用户验证信息接收部件 110 通过通信接口 101 接收从用户终端 200 发送的包括用

户验证信息的验证请求。

[0057] 验证部件 120 根据由用户验证信息接收部件 110 接收的验证请求的用户验证信息来执行用户的验证。验证部件 120 通过检验用户验证信息与存储在用户数据库 20 中的验证数据之间的一致性来验证用户。

[0058] 一旦成功验证用户，用户标识符分配部件 130 响应验证请求而分配与那个用户对应的用户标识符 ID_U。应当理解，用户标识符是基于地址的验证系统中的唯一标识符。或者，用户标识符 ID_U 可以是世界上实现唯一性的扩展标识符，诸如“A@B”，其中 A 表示验证服务器内的唯一标识符，B 表示验证服务器的全球 IP 地址。因此，用户标识符唯一地对应于一对假设的用户中的一个用户。然而，单个用户可以同时对应于多个用户标识符。

[0059] 用户标识符分配部件 130 例如从存储在用户数据库 20 中的用户 ID 条目数据获取用户 ID，并且响应验证请求分配所获取的用户 ID 作为用户标识符 ID_U。或者，用户标识符分配部件 130 当其已获取用户 ID 时可以在加密部件 140a 中产生随机数，将所产生的随机数添加到所获取的用户 ID，并且可以用验证服务器 100 的标识符产生私有密钥对所得的结果（随机数 + 用户 ID）信息进一步加密以便分配为用户标识符 ID_U。当以这种方式安排时，只有知道标识符产生私有密钥的人（例如验证服务器 100）根据用户标识符 ID_U 能够知道用户 ID，从而即使用户标识符 ID_U 包含在将被发送至应用服务器的票中也可以实现用户的私密性保护。作为另一种替换，用户标识符分配部件 130 可以分配来自用户标识符信息的用户标识符 ID_U 或者可以从随机数、字符、序号中选择某物，通过数据库其唯一地与用户 ID 相关联。

[0060] 地址分配部件 140 将地址 A_U 分配给用户终端，该用户终端对应于由用户标识符分配部件 130 分配的用户标识符 ID_U。该地址 A_U 可以是 IP 地址并且另外还可以是邮件地址、在 SIP（会话起始协议）中使用的 URI（统一资源识别符）或者 IM（即时消息）的地址。

[0061] 如果可以假设在地址分配部件 140 的地址分配期间，不能出现相同地址与多个用户标识符同时对应，则一个地址唯一地对应一个用户标识符并且也唯一地对应一个用户。

[0062] 为了使分配给已验证用户的用户标识符 ID_U 与已分配地址 A_U 之间的对应关系可被容易地识别，那种对应或者包含那种对应信息的票本身被存储在分配存储器 102b 中或者与包含在用户数据库 20 中的用户信息相关联。每次发出验证请求时，可以改变用户标识符 ID_U 和分配给相同用户的地址 A_U。为此，根据发出票的日期和时间来区分相同用户的票。在适当的时间删除不使用的用户标识符 ID_U 和地址 A_U。以这种方式，根据用户标识符 ID_U 或者所提供服务的费用来进行调节，以便答复来自应用服务器 300 的关于用户信息的查询。

[0063] 在该示例中，票发出部件 150 包括验证信息产生部件 151，临时产生包含由用户标识符分配部件 130 分配的用户标识符 ID_U 和由地址分配部件 140 分配的地址 A_U 的临时票 (ID_U, A_U)，根据验证信息产生部件 151 产生的临时票来产生验证信息 IA，并且发出包含验证信息 IA、用户标识符信息 ID_U 和地址 A_U 的票 CK1。

[0064] 如图 5 所示，票 CK1 包括用户标识符、地址、验证信息以及表示发出票 CK1 的日期和时间的时间戳、表示票的有效期的信息、以及图 5 中未示出的表示分配给用户终端 200 的通信带宽的信息以及与覆盖用户终端 200 的接入点 30 相关的信息（例如位置信息等）。当包含时间戳时，票发出部件 150 包括时钟部分 150a，并且利用从时钟部分 150a 传递的时间戳。表示票的有效期的信息和表示分配给用户终端 200 的通信带宽的信息可以事先通过通

信企业或应用服务提供商与使用用户终端 200 的用户之间的接触来确定，通信企业或应用服务提供商操作接入点 30、验证服务器 100 和应用服务器 300。

[0065] 另外，例如，如图 5 所示，在票 CK1 中可以包含唯一识别验证服务器 100 的验证服务器标识符信息（例如地址 A_A）。或者，在验证服务器 100 内唯一的标识符 A 和验证服务器 100 的全球 IP 地址被组合成将被用作用户标识符 ID_U 的“A@B”形式，如先前所述，该 B 可被用作验证服务器标识符信息，如图 5 所示。

[0066] 验证信息产生部件 151 输入预先与应用服务器 300 共享的共享保密密钥 K_{CAS} 和临时票（ID_U，A_U），以便使用该共享保密密钥 K_{CAS} 来计算相对于临时票的单向散列函数以产生鉴别码 MAC（消息验证码），该鉴别码被作为验证信息 IA 传递。

[0067] 票发送部件 160 通过通信接口 101 向用户终端 200 发送由票发出部件 150 发出的票 51。

[0068] [第一模式]用户终端

[0069] 图 3 是在执行本发明的第一模式中使用的用户终端的方框图。用户终端 200 包括通信接口 201 和控制处理部件 202。通信接口 201 包括有线或无线 LAN 接口、调制解调器或诸如蜂窝电话（模块）等的通信工具，并且可以使用能够与通过接入点 30 连接到网络 10 的通信设备进行通信的任意接口。

[0070] 控制处理部件 202 包括：具有执行程序的 CPU 的控制单元 202a、存储程序等的存储器、验证请求部件 203 和服务请求部件 230。这些部件的功能可以通过程序模块或者如在验证服务器 100 中的程序执行来实现。验证请求部件 203 包括用户验证信息产生部件 210、用户验证信息发送部件 220 和票接收部件 231。

[0071] 用户验证信息产生部件 210 产生包括表示用户名和口令的信息的用户验证信息。用户验证信息产生部件 210 例如通过根据所输入的信息产生用户验证信息，而响应来自诸如键盘的输入工具 40 的用户名和口令的输入。可选地，代替用户名和口令，被验证服务器 100 请求来验证用户的下列信息中的至少一种信息也可用作用户验证信息：根据验证用于验证用户的生物学测定特征的用户信息的密钥对而产生的信息或者在用户验证的已知方法中使用的其他各种信息。

[0072] 为了验证请求，用户验证信息发送部件 220 通过通信接口 201 向验证服务器 100 发送由用户验证信息产生部件 210 产生的用户验证信息。

[0073] 票接收部件 231 接收包括通过通信接口 201 从验证服务器 100 发送的票 (CK1)51 的分组，并且包含在所接收的票 51 中的地址 A_U 被设定并作为源地址 A_S 被登记在通信接口 201，例如被源地址设定部件 231a 登记在寄存器 201a 中。或者，包含在由服务请求部件 230 中的源地址设定部件 230a 接收的票 51 中的地址可以被设定并作为源地址 A_S 被登记在通信接口 201 内的寄存器 201a 中。

[0074] 服务请求部件 230 包括会话建立部件 232，用于请求将由应用服务器 300 提供的服务。

[0075] 会话建立部件 232 根据用户采用的服务来建立应用服务器 300 与用户终端 200 之间的会话。例如，在建立会话的处理操作期间的某一步骤，会话建立部件 232 通过通信接口 201 向应用服务器 300 发送票接收部件 231 接收的票 (CK1)51 来建立会话。会话建立请求分组 52 包括具有源地址 A_S 的头标部分 52h 和具有票 51 的有效负荷部分 52p，例如如图 6

所示。

[0076] 例如，会话建立部件 232 通过通信接口 201 向应用服务器 300 发送分组 52。通信接口 201 将由票接收部件 231 的源地址设定部件 231a 登记的地址 A_S 设定为分组 52 的源地址，并且发送分组 52。在所建立的会话使用作为源地址 A_S 登记在通信接口 201 中的地址期间，服务请求部件 230 向应用服务器 300 发送表示服务请求的分组（服务请求分组）。

[0077] ［第一模式］应用服务器

[0078] 图 4 是执行本发明的第一模式中使用的应用服务器的方框图。应用服务器 300 包括通信接口 301 和控制处理部件 302。通信接口 301 可以例如包括调制解调器或 LAN 接口，并且可以使用只要能够与连接到网络 10 的通信设备进行通信的任意接口。

[0079] 控制处理部件 302 包括：具有处理程序的 CPU 的控制单元 302a、存储程序等的存储器、服务提供部件 310、会话建立部件 311 和票存储部件 330。以与应用服务器 100 类似的方式，这些部件可由程序模块来实现。

[0080] 服务提供部件 310 包括地址比较部件 312，并且提供由用户终端 200 请求的服务。

[0081] 会话建立部件 311 包括票检验部件 320，并且建立与用户终端 200 的会话。在建立会话的过程中，会话建立部件 301 接收包括从用户终端 200 发送的票 (CK1)51 的分组 52。

[0082] 票检验部件 320 检验包含在分组 52 中的票 (CK1)51 是否被伪造。例如，票检验部件 320 在验证信息检验器 320a 中检验包含在接收到的票 51 中的验证信息 IA。具体地，如果验证信息 IA 是鉴别码 (MAC：消息验证码)，则在验证检验器 320a 中使用与验证服务器 100 事先共享的共享保密密钥 K_{CAS} 来检验票 51 是否被伪造。另外，票检验部件 320 在地址核对器 320b 中将票 51 中包含的地址 A_U 与分组 52 中的源地址 A_S 进行核对，如果它们不一致，则检验失败。

[0083] 另外，如果票 (CK1)51 包含有效期 EPe，则票检验部件 320 可以根据来自时钟部分 320d 的时间信息在有效期鉴别器 320f 中检验票 51 是否在其有效期之内。票检验部件 320 可以通过选择共享保密密钥来执行检验，所述共享保密密钥是对于每个时段根据票 (CK1)51 中包含的时间戳 Tms 中的值而单独准备的。当时间戳 Tms 包含在票 (CK1)51 中时，票检验部件 320 可以根据来自时钟部分 320d 的时间信息以及票被产生时的、由时间戳表示的日期和时间来检验票 51 是否有效。或者，有效期检验器 320f 可以根据票 51 中包含的时间戳和表示有效期的信息来检验用户请求的服务是否在服务提供部件 310 的有效提供期之内。

[0084] 当由票检验部件 320 执行的包含在票 (CK1)51 中的地址 A_U 和分组 52 的源地址 A_S 的核对结果表示匹配并且确定票已经从具有验证地址的用户终端被发送时，该票 51 被存储在票存储部件 330 中。然而，如果其他检验和由票检验部件 320 执行的核对中的任何一个不成功时，防止将票 51 存储在票存储部件 330 中。例如，来自检验器 320a、320c 和 320f 以及核对器 (collator)320b 的输出被输入到存储命令单元 320g，并且如果任何一个输入表示未成功，则不产生存储票 51 的命令。

[0085] 地址比较部件 312 通过参考票存储部件 330 根据表示服务请求的分组的源地址 A_S 来检验源地址 A_S 是否与包含在票 51 中的对应地址 A_U 一致。当票 51 中包含的地址 A_U 与分组的源地址 A_S 一致时，服务提供部件 310 向用户终端 200 发送分组，该分组有效地向用户提供用户终端 200 请求的服务。

[0086] 如果需要，服务提供部件 310 可以根据票 51 中包含的用户标识符 ID_U 向验证服务器 100 进行关于用户信息的查询。另外，服务提供部件 310 可以通过验证服务器 100 发送与涉及向用户数据库 20 提供的服务收费相关的信息。在该示例中，如果票 CK1 包含验证服务器 100 的标识符信息，如图 5 所示，则如果存在多个验证服务器就可以指定验证服务器，并且如果验证服务器标识符信息是地址（例如地址 A_A），则该地址可被立即用来访问验证服务器 100。

[0087] [第一模式] 验证系统的处理过程

[0088] 现在将参考图 7 来描述根据执行本发明的第一模式的基于地址的验证系统的处理过程。

[0089] (1) 首先，当向验证服务器请求用户的验证时，用户终端 200 准备用户验证信息，该用户验证信息随后通过接入点 30 被发送至验证服务器 100。

[0090] (2) 一旦接收验证请求，验证服务器 100 就根据用户验证信息来执行用户的验证。一旦成功验证用户，验证服务器 100 向用户分配用户标识符 ID_U，向与用户对应的用户终端 200 分配地址 A_U，并且如果需要则发出包含对于所分配地址 A_U 的验证信息 IA、时间戳、和有效期等的票 51。以及

[0091] (3) 向用户终端 200 发送票 51。

[0092] (4) 一旦接收票 51，用户终端 200 将票 51 的地址设定为源地址 A_S，并且向应用服务器 300 发送包括票 51 的分组 52，从而请求建立与应用服务器 300 的会话。

[0093] (5) 一旦接收分组 52，应用服务器 300 根据验证信息来检验票的正确性，并且一旦成功检验，则比较分组的源地址 A_S 与票 51 中包含的地址 A_U，并且如果它们匹配，则存储票 51 并建立会话。

[0094] (6) 当建立会话时，用户终端 200 通过所建立的会话向应用服务器 300 发送服务请求分组。

[0095] (7) 一旦接收这些服务请求分组，应用服务器 300 确定服务请求分组的源地址 A_S 是否与所存储的票 51 中包含的地址 A_U 一致，一旦所述地址一致，则它向用户终端 200 发送分组，该分组有效地向用户提供服务。

[0096] [第一模式] 验证服务器的处理

[0097] 图 8 是示出在执行本发明的第一模式中使用的验证服务器 100 的处理的流程的流程图。

[0098] 首先，用户验证信息接收部件 110 通过通信接口 101 接收从用户终端 200 发送的验证信息 (S101)，并且验证部件 120 根据用户验证信息进行用户的验证，一旦成功验证用户，操作继续到 S103，而一旦未成功验证用户，则操作终止 (S102)。

[0099] 一旦成功验证用户，则向用户终端 200 分配地址 A_U。在该示例中，用户标识符分配部件 130 分配与用户对应的用户标识符 ID_U(S103)，并且通过地址分配部件向对应于用户标识符 ID_U 的用户终端分配地址 A_U(S104)。

[0100] 然后通过票发出部件 150 临时产生临时票，在该示例中该临时票包括用户标识符分配部件 130 分配的用户标识符 ID_U 和地址分配部件 140 分配的地址 A_U，并且使用预先与应用服务器 300 共享的共享保密密钥，鉴别码产部件 151 产生用于临时票的鉴别码 (MAC：消息验证码)(S105)。

[0101] 然后票发出部件 150 发出包含用户标识符 ID_U、地址 A_U、和鉴别码 (MAC :消息验证码) 等的票 51(S106),并且票发送部件 160 通过通信接口 101 向用户终端 200 发送票 51(S107)。

[0102] [第一模式] 用户终端的处理

[0103] 图 9A 和 9B 是示出在执行本发明的第一模式中使用的用户终端 200 的处理的流程的流程图。

[0104] 首先,如图 9A 所示,用户验证信息产生部件 210 产生包括表示用户标识符和口令的信息的用户验证信息 (S201),并且用户验证信息发送部件 220 通过通信接口 201 向验证服务器 100 发送用户验证信息 (S202)。

[0105] 票接收部件 231 接收从验证服务器 100 发送的票 51(S203)。

[0106] 如图 9B 所示,在已经接收到票 51 之后,会话建立部件 232 建立与应用服务器 300 的会话 (S204)。在已经建立了与应用服务器 300 的会话之后,服务请求部件 230 通过会话向应用服务器 300 发送表示服务请求的分组 (S205)。

[0107] [第一模式] 应用服务器的处理

[0108] 图 10 是示出在执行本发明的第一模式中使用的应用服务器 300 的处理的流程的流程图。

[0109] 首先,会话建立部件 311 开始用户终端 200 的会话的建立 (S301),并且应用服务器 300 接收包含在分组 52 中的票 51。票检验部件 320 检验票 51,并且当票 51 被检验为真实时,操作继续到 S303,而如果票 51 被检验为被伪造而不真实时,操作终止 (S302)。

[0110] 当票 51 被检验为真实时,会话建立部件 311 建立会话,并且票 51 被存储在票存储部件 330(S303) 中。接收从用户终端 200 发送的分组请求服务,地址比较部件 312 确定分组的源地址 A_S 是否与包含在所存储的票 51 中的地址 A_U 一致 (S304),当确定所述地址一致时,发送使服务提供部件 310 能够通过用户终端 200 向用户提供服务的分组 (S305)。如果源地址 A_S 和地址 A_U 不一致,则操作终止。

[0111] 如上所述,根据用户验证,执行本发明的第一模式的基于地址的验证系统发出地址,因此,保证了该地址已经被发向真实的用户 (用户标识符)。鉴于这种关系,验证服务器 100 发出包含所分配的地址和用户标识符的票 51,用户终端向应用服务器发送所发出的票 51,并且应用服务器 300 检验并存储所发送的票 51,并且将从用户终端 200 发送的服务请求分组的源地址与包含在所存储的票 51 中的地址进行比较,并且一旦发现它们之间一致,将认为服务请求分组为来自于已验证的用户的分组。以这种方式,能够进行基于地址的验证。

[0112] 换句话说,基于用户验证,由验证服务器发出的票保证了用户 (标识符) 与地址之间的对应关系,因此,通过将服务请求分组的源地址 A_S 与在存储的票中的地址 A_U 进行比较,能够确认该分组是否来自于已验证的用户。

[0113] 在该模式中,使用验证信息来检验票 51 的真实性,该验证信息是使用预先在应用服务器 300 与验证服务器 100 之间共享的共享保密密钥而产生的,因此,能够保证由验证服务器 100 发出的票 51 的真实性,特别地,能够保证其中包含的地址的真实性。

[0114] 同样在该模式中,验证服务器 100 发出包含表示票 51 的有效期的信息的票 51,并且应用服务器 300 根据有效期来检验票 51 的有效性,允许根据验证服务器 100 的操作原理来确定有效期。

[0115] [第一模式]修改

[0116] 在验证服务器 100 中不是一直需要用户标识符分配部件 130。用户标识符当作为发出的票 51 的一个组成元素时可以被省略。在该示例中，省略用户标识符分配部件 130，并且如图 8 中的虚线所示，一旦在 S102 成功验证，操作立即转到步骤 S104。然而，当使用用户标识符时，票 51 本身提供分配给用户终端 200 的地址 A_U 与用户之间的对应关系，从而应用服务器 300 可以使用用户标识符对验证服务器 100 进行关于用户信息的查询。当省略用户标识符时，必须使用地址 A_U 来进行这种查询并且要求验证服务器 100 存储分配给用户终端的地址 A_U 与用户 ID 之间的对应关系。

[0117] 验证信息产生部件 151 产生的验证信息 IA 不限于鉴别码 (MAC :消息验证码)。如图 11A 所示，例如，临时票 (ID_U, A_U) 可以被输入到签名计算器 151b 以使用验证服务器 100 的私有密钥 K_{SA} 基于公开密钥加密技术来执行相对于临时票 (ID_U,A_U) 的数字签名计算，来产生签名，所述签名可被用作验证信息 IA。或者，如图 11B 所示，在加密器 151c 中使用与应用服务器 300 共享的保密密钥 K_{CAS} 可以加密被输入到验证信息产生部件 151 的临时票 (ID_U, A_U)，并且所加密的临时票可被用作验证信息 IA。

[0118] 在签名被用作验证信息 IA 的情况下，应用服务器 300 内的验证信息检验器 320a 将是签名检验器而不是鉴别码检验器，如图 4 的括号中所示，并且作为验证信息 IA 的签名经受用验证服务器 100 的公开密钥 K_{PA} 的签名检验。如果整个票 51 被加密以用作验证信息 IA，则验证信息检验器 320a 如图 11C 构造，其中在解密部件 320a1 中使用与验证服务器 100 共享的保密密钥 K_{CAS} 来解密验证信息 IA，并且在核对器 320a2 中将所解密的结果与临时票 (IDU, A_U) 进行核对，从而导致对于它们之间一致性的成功检验。

[0119] 在用户标识符不被用作票 51 的一个元素的情况下，临时票仅包括地址 A_U。在包含时间戳等作为票 51 的元素的情况下，其被看作临时票，并且准备对于临时票的验证信息 IA。总之，除了票 51 中的验证信息 IA 以外的每个元素可以被作为临时票 51 对待以准备验证信息 IA。

[0120] 可以省略票 51 中的验证信息 IA。因此，如图 8 中的虚线所示，操作可以从步骤 S104 直接转到 S106。然而，当使用验证信息 IA 时，在步骤 S302 发生的 (图 10 中的虚线所示) 以及在应用服务器 300 中发生的票的验证首先检验验证信息 IA，以便检验临时票是否被伪造 (S302a)，并且当确认票未被伪造时，并且因此票 51 中包含的地址 A_U 未被伪造而是真实的，则比较源地址 A_S 与票中的地址 A_U，以便查看两个地址是否一致 (S302b)，一旦一致，则操作转到 S303，如果不一致则操作终止。

[0121] 作为票 51 中的元素，可以省略时间戳和有效期中的一个或两者。在应用服务器 300 中，每次建立与用户终端 200 的会话时，从用户终端 200 接收的分组的票 CK1 可以被立即存储在票存储部件 330 中。因此，可以省略图 4 所示的票检验部件 320，并且操作可以从处理 S301 直接到图 10 中虚线 31 所示的处理 S303。即使以这种方式进行改变，每次建立会话时票 CK1 的发送从用户终端到应用服务器 300 也仅发生一次，并且因为每次用户终端需要随后被分配至用户终端 200 的新的服务和地址 (包含在票 CK1 中的地址) 改变时验证服务器进行用户验证，因此第三方难以窃取源地址 A_S 和假冒该用户。

[0122] 用户数据库 20 不必总是连接到验证服务器 100。例如，当使用公开密钥加密技术进行用户验证时，不需要验证数据。然而，为了确认从用户终端 200 发送的用户公开密钥证

明是可靠的，对已经发出该公开密钥证明的公开密钥证明发出组织进行查询，如果是真实的，则获取公开密钥证明中包含的用户信息，如果不是充足的，则公开密钥证明发出组织内的数据库获取有关对应用户的信息。

[0123] 验证服务器 100 可以由通过安全网络连接在一起的一组服务器构成，该组服务器彼此具有依赖关系。例如，它可以包括通过安全网络连接在一起的专用验证服务器、地址发出服务器、票发出服务器等。

[0124] [第二模式] 验证系统的结构

[0125] 现在将描述执行本发明的第二模式，说明原则上针对与第一模式的不同之处。同样在第二模式中，提供验证服务器、用户终端和应用服务器，尽管它们具有与第一模式不同的功能，但是系统结构类似于图 1 所示的第一模式，因此，第二模式中使用的附图标记在图 1 中示于括号内。验证服务器 400、用户终端 500 和应用服务器 600 连接在一起，以这种方式允许通过网络 10 在它们之间进行通信。

[0126] 在第二模式中，用户终端 500 当其请求验证服务器 400 验证时除了发送用户验证信息以外还发送密钥信息。因此，用户终端 500 具有密钥信息。密钥信息包括关于下列的信息 :用户或者用户终端的公开密钥，诸如用户密钥对的公开密钥、终端密钥对的公开密钥、包括这种公开密钥的证明、或者通过向公开密钥或者包括该公开密钥的证明应用单向散列函数而获得的散列值。

[0127] 当一旦响应来自用户终端 500 的验证请求而成功验证用户从而发出票时，在第二模式中，除了用户标识符和地址外，验证服务器 400 还使从用户终端发送的密钥信息包含在该票中。

[0128] [第二模式] 验证服务器

[0129] 图 12 是在执行本发明的第二模式中使用的验证服务器的方框图。验证服务器 400 包括通信接口 101 和控制处理部件 402。

[0130] 控制处理部件 402 包括 :具有执行程序的 CPU(中央处理单元) 的控制单元 402a、存储程序等的存储器、用户验证信息接收部件 110、验证部件 420、用户标识符分配部件 130、地址分配部件 140、票发出部件 450 和票发送部件 160。应当理解，这些部件可以由程序模块构成。

[0131] 验证部件 420 根据由用户验证信息接收部件 110 接收的用户验证信息来执行用户的验证。例如，验证部件 420 在验证信息核对器 102a 中检验用户验证信息与存储在用户数据库 20 中的验证数据之间的匹配以用于验证用户。如果需要，验证服务器也可以确认用户终端是否保持与密钥信息 IK 相关的私有密钥。例如，可以确认具有与对应于密钥信息 IK 的公开密钥形成一对的私有密钥。

[0132] 票发出部件 450 包括验证信息产生部件 151，并且发出票，所述票包含地址分配部件 140 分配的地址 A_U、用户标识符分配部件 130 分配的用户标识符 ID_U、从用户终端 500 发送的密钥信息与用户验证信息、以及验证信息产生部件 151 产生的验证信息 IA。这样，所述票提供用户标识符与密钥信息之间的对应关系。因此，已验证的用户对应于保持与密钥信息相关联的私有密钥的用户终端。所述票可以包含发出票时的时间戳、票的有效期、分配给用户终端 500 的通信带宽以及与覆盖用户终端 500 的接入点 30 相关的信息。图 15 示出了票 53 的一个示例。该票 53 不同于在第一模式中使用的票 51，其中票 53 包含密钥信息。

[0133] 一旦响应验证请求而成功验证用户，验证服务器 400 向用户分配用户标识符，并且还向与用户标识符对应的用户终端分配地址。以与第一模式类似的方式在用户终端 500 中将该地址设定为源地址。由于密钥信息与用户终端 500 的公开密钥相关联，所以接着验证服务器 400 通过密钥信息来链接用户和用户使用的用户终端 500（作为一对）进行用户验证，并且，具有密钥信息的用户终端被分配有地址。

[0134] 根据第二模式，用户验证的用户密钥对不同于用于建立会话的终端密钥对，并且用户密钥对由连接到用户终端的验证设备持有，从而通过连接验证设备到用户终端，可以利用位于任何地方的用户终端。作为一种用户验证的方法，也可以采用不使用密钥对的方法。

[0135] ［第二模式］用户终端

[0136] 图 13 是在执行本发明的第二模式中使用的用户终端的方框图。用户终端 500 包括通信接口 201 和控制处理部件 502。控制处理部件 502 包括：具有处理程序的 CPU 的控制单元 502a、存储程序等的存储器、验证请求部件 503 和服务请求部件 530。应当理解，这些部件可以通过程序的模块来构成。验证请求部件 503 包括用户验证信息输入部件 510、用户验证信息发送部件 220 和票接收部件 231。

[0137] 用户验证信息输入部件 510 使验证设备 41 输入用户验证信息等。存储在验证设备 41 中的用户密钥对的私有密钥不能从验证设备 41 中取出。验证设备 41 可以包括智能卡、包括 USB（通用串行总线）密钥的硬件验证标记、或者生物学测定特征验证设备。或者可以通过输入工具 40 输入口令 / 用户标识符以便馈送到用户验证信息产生器 210 用以产生用户验证信息。在简化的结构中验证设备 41 未连接到用户终端 500 的情况下，可以使用存储在密钥存储器 502b 中的终端密钥对来代替用户密钥对以产生用户验证信息。

[0138] 密钥信息发生器 503a 使从密钥存储器 502b 输入用户终端 500 的公开密钥 K_{PU} 以产生密钥信息 IK。密钥信息发生器 503a 可以直接传递输入的公开密钥作为密钥信息。用户验证信息发送部件 220 不仅向验证服务器 400 发送用户验证信息还发送密钥信息，用以验证请求。

[0139] 服务请求部件 530 包括会话建立部件 532 和分组加密处理部件 533，并且该服务请求部件 530 被用来请求由应用服务器 600 提供的服务。依据 IKE（因特网密钥交换），根据与票 53 中包含的密钥信息相关联的公开密钥 K_{PU} 形成一对的私有密钥 K_{SU} 和应用服务器 600 的公开密钥 K_{PS}，会话建立部件 532 在会话密钥发生器 532a 中产生与应用服务器 600 共享的保密密钥作为会话保密密钥 K_{CUS}。

[0140] 在应用服务器 600 共享会话保密密钥之后，或者与用户终端 500 共享的保密密钥也作为应用服务器 600 中的会话保密密钥产生之后，分组加密处理部件 533 通过会话建立部件 532 使用与应用服务器 600 共享的会话保密密钥，依据 IPsec（因特网协议的安全结构）或者 TLS（传输层安全）在验证头标发生器 533a 中对所发送的分组信息计算验证头标，并且将验证头标 AH 添加到正在发送的分组。验证头标发生器 533a 通过计算相对于分组的单向散列函数而使用会话保密密钥产生验证头标，因此能够识别分组是否已经被伪造。分组加密处理部件 533 可以在如图 13 中的括号所示的加密器 533a′ 中依据 IPsec 或 TLS 来加密分组。或者，分组 54 可以被添加有验证头标 H，并且在加密器 533a′ 中可以加密得到的分组。验证头标 H 的添加以及分组的加密处理通常称作分组加密处理，并且执行这种处

理的结构称作分组加密处理部件。

[0141] 图 16 示出了分组加密处理部件 533 产生的分组 54 的构成的示例。作为与图 6 所示的分组 52 的区别，头标 54h 被添加有验证头标，并且有效负荷 54p 中的票 53 被添加有密钥信息。应当注意，分组可以在加密器 533a′ 中被加密并且被添加有验证头标 AH。

[0142] [第二模式] 应用服务器

[0143] 图 14 是执行本发明的第二模式中使用的应用服务器的方框图。应用服务器 600 包括通信接口 301 和控制处理部件 602。控制处理部件 602 包括 :具有处理程序的 CPU 的控制单元 602a、存储程序等的存储器、服务提供部件 610、会话建立部件 611 和票存储部件 330。应当注意，这些部件可由程序的模块来实现。

[0144] 服务提供部件 610 包括地址比较部件 312 和票验证部件 612，并且提供用户终端 500 请求的服务。

[0145] 会话建立部件 611 包括票检验部件 620，并且建立与用户终端 500 的会话。在建立会话的过程中，它与用户终端 500 依据 IKE 等共享会话保密密钥。因此，会话建立部件 611 在会话密钥发生器 611a 中使用存储在密钥存储器 602b 中的应用服务器 600 的私有密钥 K_{SS} 和用户终端 500 的公开密钥 K_{PU} 来产生与用户终端 500 共享的保密密钥作为会话保密密钥 K_{CUS}。

[0146] 在与用户终端 500 共享会话保密密钥之后，分组验证部件 612 使用会话保密密钥 K_{CUS} 来检验被添加到所接收的分组 54 的验证头标 AH。如果被添加到分组 54 的验证头标的验证结果正确，则分组验证部件 612 将分组 54 中的票 (CK2)53 传递到票检验部件 620。当通过用户终端 500 加密所接收的分组 54 时，使用括号中表示的分组解密部件 612′ 来代替分组验证部件 612，并且用会话保密密钥 K_{CUS} 来解密分组 54。当正常解密时或者当分组 54 未被伪造时，将所解密的分组 54 传递到票检验部件 620。验证头标 AH 的验证或分组 54 的解密处理通常称作分组检验，并且执行这种检验的结构称作分组检验部件。

[0147] 票检验部件 620 检验分组验证部件 612 所传递的票 53 的真实性。例如，票检验部件 620 在密钥核对器 620a 中将票 53 中包含的密钥信息 IK 与用户方的公开密钥进行核对，该公开密钥是当共享会话保密密钥 K_{CUS} 时使用的，如果它们之间匹配，并且在该示例中，如果当在地址核对器 320b 中核对时票 53 中包含的地址 A_U 被发现与分组 54 的源地址 A_S 一致，则通过存储器命令单元 620c 来检测这一事实，允许票 (CK2)53 被存储在票存储部件 330 中。在已经建立了与用户终端 500 的会话并且将票 (CK2)53 存储在票存储部件 330 中之后，当通过会话从用户终端 500 接收服务请求分组时，在地址比较部件 312 确定被分组验证部件 612(或者分组解密部件 612′) 依据 IPsec 或 TLS 等确认 (或解密) 为未被伪造的分组 54 的源地址与存储在票存储部件 330 中的对应票 (CK2)53 中包含的地址一致的条件下，服务提供部件 610 通过用户终端 500 的会话发送为用户终端 500 提供其所请求的服务的分组。如果需要，票检验部件 620 可以包括各种检验器，例如以在第一模式中使用的应用服务器 300 类似的方式，可以在图 4 所示的票检验部件 320 中提供的验证信息检验器 320a。

[0148] [第二模式] 验证系统的处理过程

[0149] 现在将参考图 17 来描述根据执行本发明的第二模式的基于地址的处理系统的处理过程。

[0150] (1) 首先，用户终端 500 产生用户验证信息和密钥信息 IK，并且通过接入点 30 向

验证服务器 400 发送验证请求。

[0151] (2) 一旦接收验证请求，验证服务器 400 就根据用户验证信息来执行用户的验证，并且一旦成功验证了用户，就分配用户标识符 ID_U 并向与 ID_U 对应的用户终端分配地址 A_U，并且如果需要则产生验证信息，发出包含用户标识符 ID_U、地址 A_U、和密钥信息 IK 的票 53。

[0152] (3) 向用户终端 500 发送票。

[0153] (4) 用户终端 200 将接收到的票的地址 A_U 设定为源地址。

[0154] (5) 用户终端 500 使用其自己的私有密钥 K_{SU} 和应用服务器 600 的公开密钥 K_{PS} 依据诸如 IKE 的密钥交换过程来计算与应用服务器 600 共享的会话保密密钥 K_{CUS}。然后它使用会话保密密钥 K_{CUS} 来产生对于将被发送至应用服务器 600 的分组的验证头标 AH，允许该头标被添加到分组。在建立会话的处理中，它向应用服务器 600 发送包括验证头标和票的分组。通过上述的过程，它请求应用服务器 600 建立会话。

[0155] (6) 在建立会话的处理中，应用服务器 600 使用其自己的私有密钥 K_{SS} 和用户终端的公开密钥 K_{PU} 来计算会话保密密钥 K_{CUS}，并且使用会话保密密钥 K_{CUS} 来检验被添加到分组的验证头标 AH，如果需要，还使用与验证服务器 400 共享的保密密钥 K_{CAS} 来检验包含在建立会话的过程中接收到的票 (CK2)53 中的验证信息 IA。它还检验接收到的票 53 中包含的密钥信息是否对应于用户方的公开密钥（用户公开密钥或终端公开密钥）K_{PU}，该 K_{PU} 在会话保密密钥 K_{CUS} 的计算中被使用，并且将接收到的分组 54 的源地址 A_S 与票 (CK2)53 中包含的地址 A_U 进行比较，如果这些检验都成功，则它存储票 (CK2)53 从而建立会话。

[0156] (7) 为了保护源地址 A_S，用户终端 500 执行使用会话保密密钥 K_{CUS} 的加密处理和验证头标添加处理中的至少一个，并且通过所建立的会话向应用服务器 600 发送表示服务请求的分组。

[0157] (8) 应用服务器 600 用会话保密密钥 K_{CUS} 来解密服务请求分组或者检验验证头标，确定所存储的票 53 中包含的地址是否与表示服务请求的分组的源地址 A_S 一致，并且一旦地址一致，将向用户终端 500 发送有效地向用户提供服务的分组。

[0158] [第二模式] 验证服务器的处理

[0159] 图 18 是示出在执行本发明的第二模式中使用的验证服务器的处理的流程的流程图。

[0160] 一旦从用户终端 500 接收验证请求 (S101)，验证部件 120 就根据用户验证信息执行用户的验证，并且一旦成功验证用户，操作继续到 S103，如果用户的验证失败，则操作终止 (S102)。票发出部件 450 发出包含地址 A_U、用户标识符 ID_U 和密钥信息 IK 的票 53(S402)。其他处理保持与根据第一模式的验证服务器的处理过程类似。

[0161] [第二模式] 用户终端的处理

[0162] 图 19 是示出在执行本发明的第二模式中使用的用户终端的处理的流程的流程图。

[0163] 在图 19A 所示的用户验证请求的处理中，用户验证信息输入部件 510 输入用户验证信息和密钥信息 IK(S501)，并且用户验证信息发送部件 220 通过通信接口 201 向验证服务器 400 发送用户验证信息和密钥信息 IK(S202)。票接收部件 231 接收从验证服务器 400 发送的票 (CK2)53(S203)。

[0164] 如图 9B 所示的后续处理，其中建立了与应用服务器 600 的会话，该处理由会话建

立部件 532 启动，共享用户终端 500 与应用服务器 600 之间的会话保密密钥。通过分组处理部件 533 将验证头标添加处理和 / 或加密处理应用于包括票 53 的分组 54，并且将分组发送至应用服务器 600(S502)。

[0165] 在已经建立了与应用服务器 600 的会话之后，服务请求部件 530 通过建立会话向应用服务器 600 发送表示服务请求的分组，从而向应用服务器 600 请求服务 (S205)。

[0166] [第二模式] 应用服务器的处理

[0167] 图 20 是示出在执行本发明的第二模式中使用的应用服务器的处理的流程的流程图。

[0168] 首先，会话建立部件 611 开始与用户终端 500 的建立会话，并且在用户终端 500 与应用服务器 600 之间共享通过根据自己的私有密钥和另一方的公开密钥依据诸如 IKE 的密钥交换过程计算获得的会话保密密钥 (S601)。现在，包括从用户终端 500 发送的票 53 的分组 54 由应用服务器 600 接收。

[0169] 分组验证部件 612 使用会话保密密钥来检验被添加到所接收的分组 54 的验证头标，并且如果检验表明该分组 54 未被伪造而是真实的，则操作继续到 S603。然而，当验证表明分组 54 由于被伪造而不真实时，操作终止 (S602)。如果对分组 54 加密，则由分组解密部件 612′ 使用会话保密密钥对其进行解密，并且当其被正确解密时，操作继续到 S603。

[0170] 当检验票 53 的验证或者检验至少在票 53 中包含的密钥信息与在共享会话保密密钥中使用的用户方的公开密钥之间的匹配时，分组 54 的源地址 A_S 与票中包含的地址 A_U 一致 (S603)，票 53 被确定为真实的并且被存储在票存储部件 330(S303) 中。

[0171] 在建立了会话之后，分组检验部件检验从用户终端 500 发送的、请求服务的分组是否被伪造并且是否真实 (S604)，并且如果其是真实的，确定分组的源地址是否与所存储的票 53 中包含的地址一致。一旦所述地址一致 (S304)，服务提供部件 610 通过用户终端 500 向用户提供服务 (S305)。

[0172] 用户终端 500 向应用服务器 600 发送包括票 53 的分组 54 时的时序可以在诸如 IKE 的密钥交换过程的完成之前。在该示例中，在密钥交换过程之前，票检验部件 620 通过检验从用户终端 500 发送的票 53，能够预先确定是否要执行密钥交换过程。这样，获得的优点是，在早期阶段可以排除对来自不具有票的用户终端的不适当服务请求的处理。然而，因为在用户终端 500 与应用服务器 600 之间共享会话保密密钥之前发生包括票 53 的分组 54 的发送，从而分组检验部件不起作用，所以它不能进行分组 54 的任意伪造的检测并且存在诸如票的替换的侵权行为的可能性。然而，由于票 53 中包含的验证信息使得票检验部件 620 能够检测票 53 本身的任意伪造，当这与检验在密钥交换期间使用的用户方的公开密钥与票 53 中包含的密钥信息之间的匹配相组合时，可以对票是从真实的用户终端发送的进行确认。换句话说，如果用户终端 500 在 (刚刚) 完成密钥交换过程之前 (或期间) 向应用服务器 600 发送票 53，可以最终保持安全性。

[0173] 如上所述，在根据执行本发明的第二模式的基于地址的验证系统中，验证服务器根据通过用户终端进行的用户验证的结果向用户终端发送保证用户标识符、地址和密钥信息之间的对应关系的票。用户终端向应用服务器发送票并通过共享会话保密密钥来建立与其的会话，并且通过该会话向应用服务器请求服务。应用服务器在确认接收到的票的真实性之后存储票，通过将接收到的服务请求分组的源地址与所存储的票中包含的地址进行比

较来检验服务请求并且当其被正常检验时提供服务。

[0174] 具体地，因为当用户终端500向应用服务器600发送分组时，诸如验证头标的信息被添加到所发送的分组，所述验证头标是使用会话保密密钥等来计算的并且其用于检测任意伪造，并且应用服务器600确认从用户终端500发送的分组没有被伪造，从而能够保证在会话期间没有从用户终端500向应用服务器600发送的伪造的分组54。换句话说，保证了在分组包含的源地址中没有伪造。

[0175] 在上述的示例中，为了使应用服务器检验从用户终端接收的信息（例如用户方的公开密钥）与在建立会话时票中包含的密钥信息之间的匹配，所建立的会话可以与票相关。另外，验证服务器根据通过用户终端进行的用户验证来发出票，从而保证用户标识符、地址与密钥信息之间的联系，保证了具有与密钥信息相关的密钥的用户终端与用户标识符指定的用户之间的对应关系。因此，所建立的会话和票保证了源地址与用户之间的对应关系。

[0176] 另外，由于根据如上所述的用户验证发出票，因此可以保证票中包含的地址真实性。而且，将应用服务器中存储的票中包含的地址与分组的源地址进行比较并确保在所建立的会话中分组的源地址没有伪造保证了分组的源地址的真实性。因此，保证了分组的源地址的真实性和源地址与用户之间的对应关系，因此能够进行基于地址的验证。

[0177] 应当注意，因为验证用户的功能、发出地址的功能和保证其间的联系的票产生功能可以通过相同的验证服务器来实现，因此能够通过票来保证地址的真实性，或者通过正确的过程来保证将地址发给正常经过验证的用户。因为在通过用户终端进行用户验证的同时，用户与终端之间的对应关系是通过从用户终端将密钥信息发送至验证服务器的这样的过程和结构来确定的，所以通过票能够保证用户与终端之间的对应关系。

[0178] 可以通过清除与来自终端的密钥信息相关的私有密钥来使用户、终端与地址之间的对应关系无效。这是因为在没有私有密钥的情况下不能进行密钥交换，并且如果使用不同的密钥，则不能应用与票中包含的密钥信息的匹配，从而导致建立会话失败的情况。

[0179] [第二模式]修改

[0180] 在与利用密钥信息IK的处理相关的部分，第二模式与第一模式不同。因此，上述结合第一模式的修改在第二模式中可能相似。

[0181] 在应用服务器600中，可以省略地址核对器320b，并且当密钥核对器620a确认匹配时，票CK2可被存储在票存储部件330中。

[0182] 密钥信息IK不限于与用户终端的公开密钥相关的信息。例如，在用户终端500与应用服务器600之间预先共享用于验证的共享保密密钥(authentication purpose shared secret key)K_{US}的情况下，可以使用能够证实拥有用于验证的共享保密密钥K_{US}的信息。例如，如图21A的顺序图所示，一旦成功验证用户，验证服务器400就可以在质询发生器460(图21B)中产生质询b，并且将其发送至用户终端500。

[0183] 用户终端500使用验证请求部件503中的密钥信息发生器503a′（图21C)来计算对于输入b的单向散列函数h的值r和用于验证的共享保密密钥K_{US}，$r = h(K_{US}, b)$作为对接收到的b的响应，并且产生一对质询b和响应r作为密钥信息$IK = \{b, r\}$。该密钥信息IK被发送至验证服务器400。应当注意，作为质询b，而不是明显从验证服务器400发送的值，可以使用诸如产生响应的时间（时间戳）或者会话中的序号之类的隐式(implicit)

质询，并且在该示例中，可以省略质询的发送和接收。

[0184] 验证服务器 400 确认所接收的密钥信息 IK 中包含的质询 b 的真实性，并且当它确认正确时，它发出包含密钥信息 IK 的票 CK2。可以这样的方式来确认质询的真实性：即如果质询 b 是显式 (explicit) 质询或者是根据用户终端 500 与验证服务器 400 之间的会话唯一确定的，则确认其间的一致性，或者如果质询 b 是诸如当计算响应 r 时的时间 t1 之类的隐式质询，则通过要求 t1 与发出票时的时间 t2 之间的差在容许范围 d（即，$t2-t1 \leqslant d$）来确认真实性。使用共享保密密钥在质询和响应方面的验证是公知的，因此不再给出详细描述。

[0185] 当建立用于服务请求的会话时，已接收到票 CK2 的用户终端 500 以上述方式向应用服务器 600 发送票 CK2。

[0186] 在应用服务器 600 中，还在票检验部件 620 中提供终端验证器 620d（图 21D），其输入密钥信息 IK = {b, r}，在单向散列计算器中使用共享保密密钥 K_{US} 来重新计算质询 b 的散列后的值 $h(K_{US},b)$，并且在核对判定单元中核对该散列后的值是否与密钥信息 IK 内的响应 r 一致。如果比较结果表示一致，则从终端验证器 620d 的核对判定单元向存储命令单元 620c（图 14）发出命令以便允许存储，从而存储了票。

[0187] 或者，应用服务器 600 中的终端验证器 620d（图 21D）可以在建立与用户终端 500 的会话的处理中向用户终端发送附加质询 b'，如图 21A 中的虚线所示，并且从用户终端 500 接收对应的响应 $r' = h(K_{US}, b')$ 以确认 r' 的真实性。（在该示例中，b' 可以用隐式质询来代替）

[0188] 通过上面的过程，通过根据密钥信息 IK 确认对质询 b(b')（该质询是基于会话的信息）的响应 r(r') 是正确的，应用服务器 600 可以识别：在用户验证的时侯（以及在服务请求的时侯），用户终端 100 已经拥有该共享的保密密钥 K_{US}。

[0189] 另外，由于根据用户验证发出票 CK2，所以保证了密钥信息 IK、地址 A_U 以及用户标识符 ID_U 之间的对应关系，并且由此能够保证地址 A_U 已经颁发给具有由密钥信息指示的共享保密密钥 K_{US} 的用户终端。还能够保证使用作为源的地址 A_U 产生的服务请求是来自于已验证的用户。而且其能够与已验证的用户的 ID、名字以及地址等相关。

[0190] 密钥信息 IK 可以是如第一示例所述的、与用户终端的公开密钥 K_{PU} 相关的信息，并且也可以是证明拥有用户终端 500 与应用服务器 600 之间的用于验证的共享保密密钥的信息。总之，密钥信息 IK 可以是这样的密钥信息 IK，即，使应用服务器 600 能够根据密钥信息 IK 来检验用户终端 500 拥有使普通应用服务器或者接收到服务请求的应用服务器唯一识别用户终端 500 的保密密钥，该保密密钥是应用服务器 600 的用户终端的密钥对的私有密钥 K_{SU}，并且是用户终端 500 的用于验证的共享保密密钥 K_{US}。

[0191] 图 2 和 12 所示的验证服务器、图 3 和 13 所示的用户终端、以及图 4 和 14 所示的应用服务器中的每一个都可由计算机来实现。例如，使计算机充当图 2 所示的验证服务器的验证服务器程序可以被从诸如 CD-ROM、磁盘、半导体存储介质等的记录介质安装到计算机或者可以通过通信网络下载以使计算机执行服务器程序。相同的应用也适于其他示例。

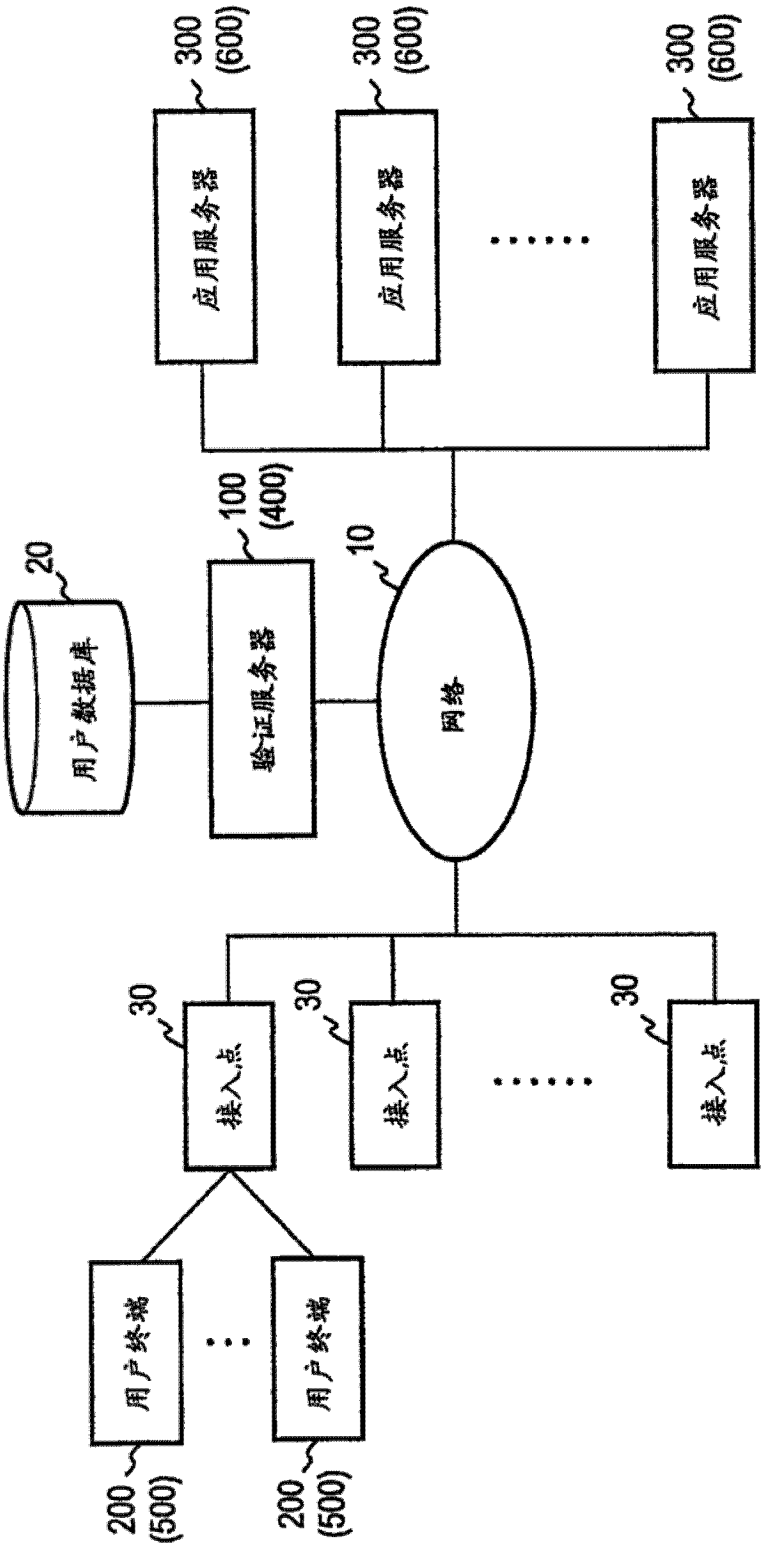

300
(600)
应用服务器
300
(600)
应用服务器
300
(600)
应用服务器
100
(400)
20
用户数据库
验证服务器
10
网络
30
接入点
30
接入点
30
接入点
用户终端
用户终端
200
(500)
200
(500)

图 1

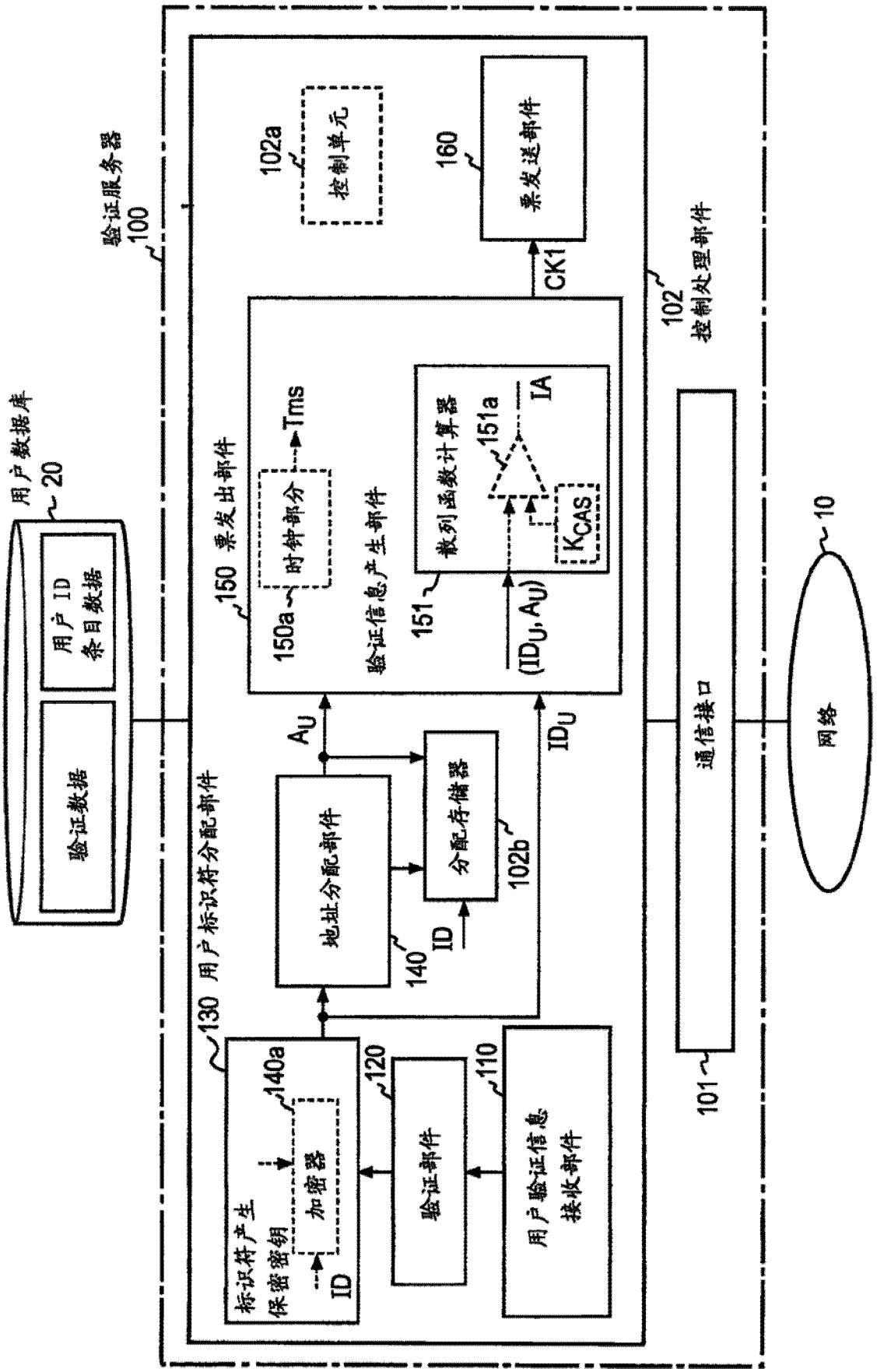

验证服务器
100
用户数据库
20
用户 ID
条目数据
验证数据
130 用户标识符分配部件
标识符产生
保密密钥
ID
140a
加密器
120
验证部件
110
用户验证信息
接收部件
140
地址分配部件
ID
分配存储器
102b
A_U
ID_U
150 乘发出部件
150a
时钟部分
Tms
验证信息产生部件
151
散列函数计算器
151a
IA
K_{CAS}
(ID_U, A_U)
102a
控制单元
160
乘发送部件
CK1
102
控制处理部件
通信接口
101
网络
10

图 2

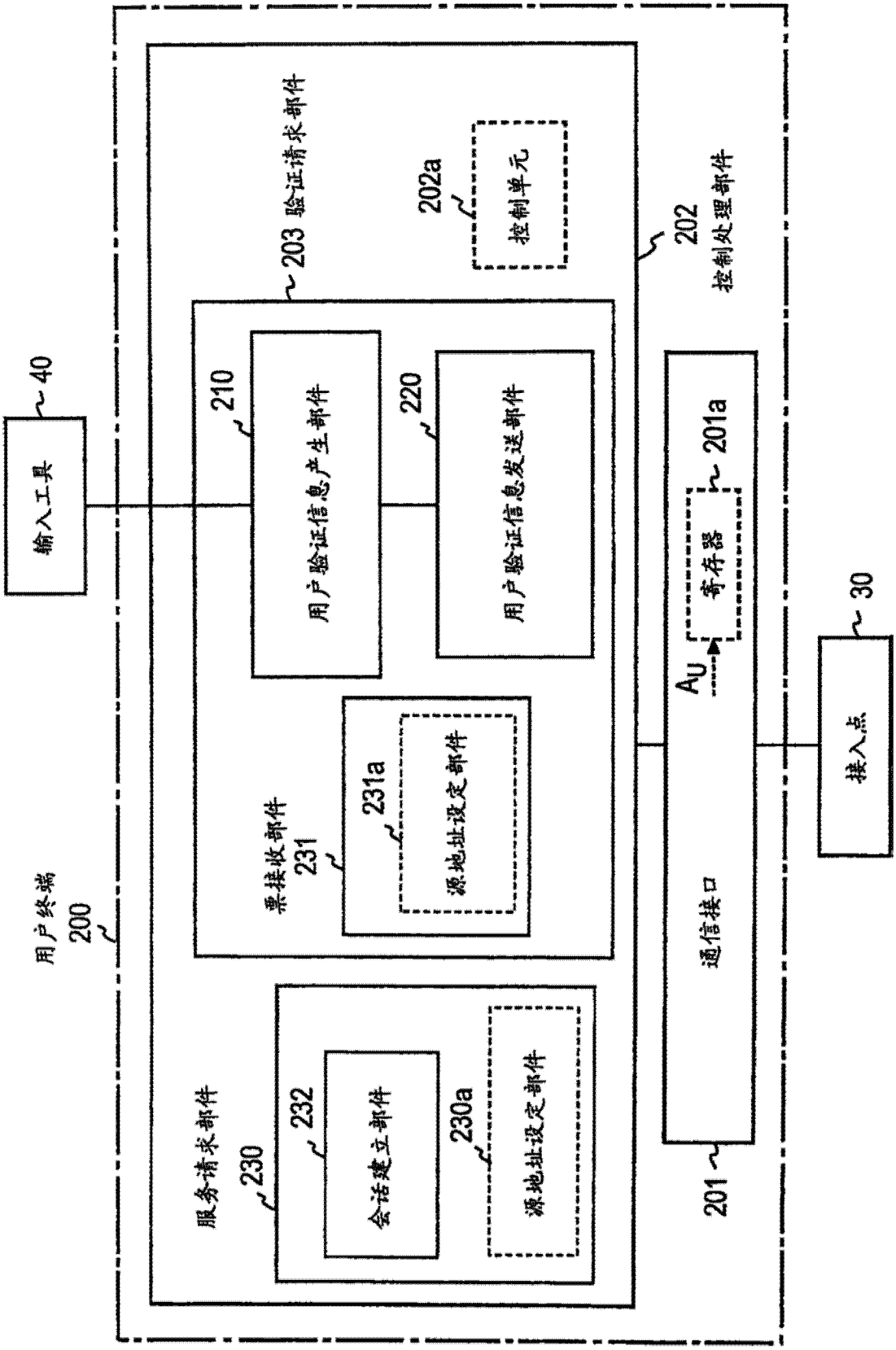

用户终端
200
输入工具
40
服务请求部件
230
会话建立部件
232
源地址设定部件
230a
乘接收部件
231
源地址设定部件
231a
用户验证信息产生部件
210
用户验证信息发送部件
220
验证请求部件
203
控制单元
202a
控制处理部件
202
寄存器
201a
通信接口
201
接入点
30

图 3

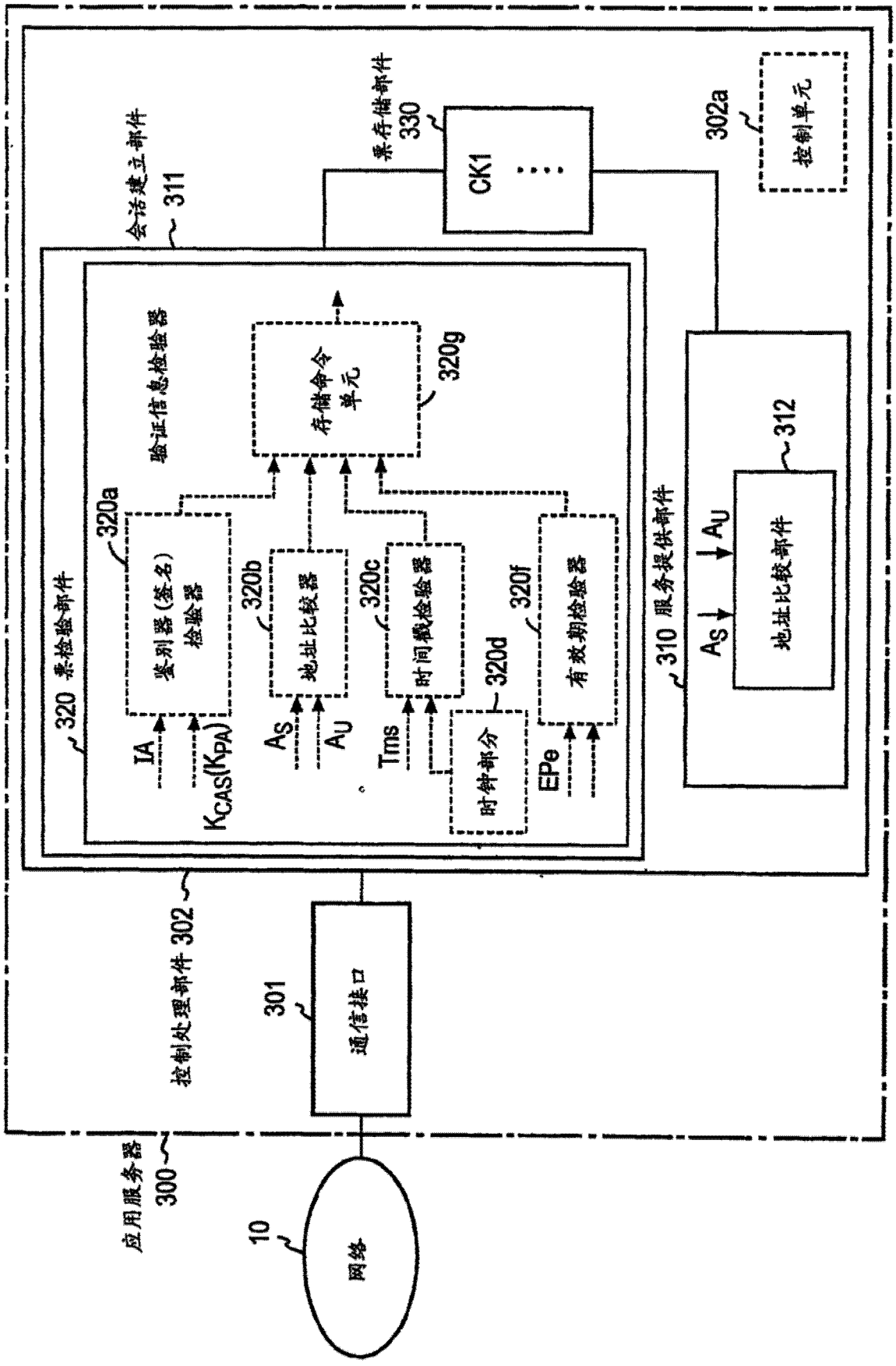

应用服务器 300
网络 10
通信接口 301
控制处理部件 302
会话建立部件 311
乘检验部件 320
鉴别器（签名）检验器 320a
地址比较器 320b
时间戳检验器 320c
时钟部分 320d
有效期检验器 320f
验证信息检验器
存储命令单元 320g
乘存储部件 330
CK1
服务提供部件 310
地址比较部件 312
控制单元 302a
IA
$K_{CAS}(K_{PA})$
A_S
A_U
Tms
EPe

图 4

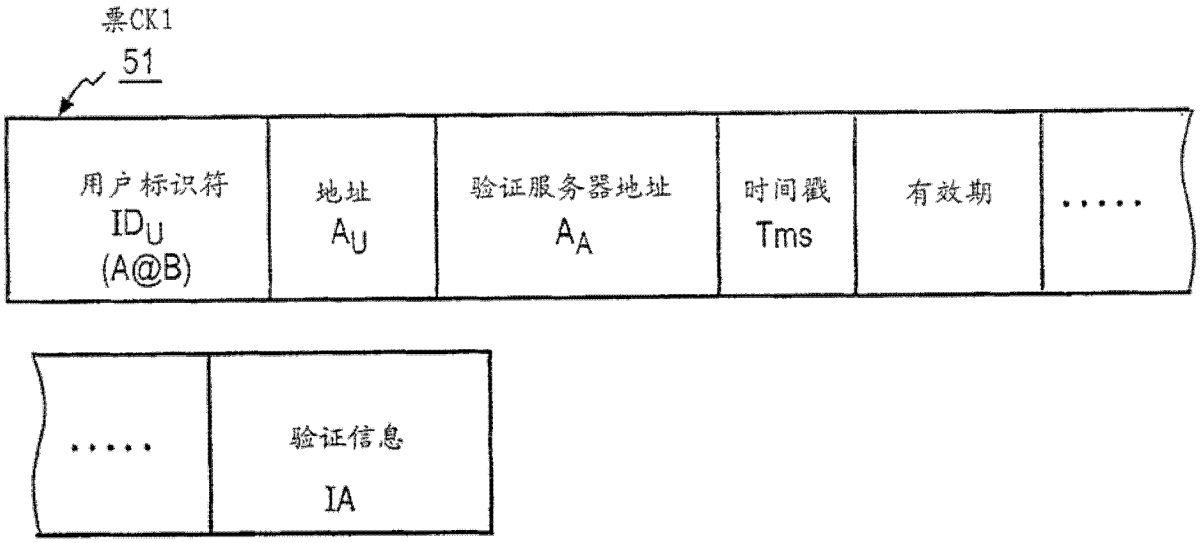

票CK1
51
用户标识符
ID_U
(A@B)
地址
A_U
验证服务器地址
A_A
时间戳
Tms
有效期
.....
.....
验证信息
IA

图 5

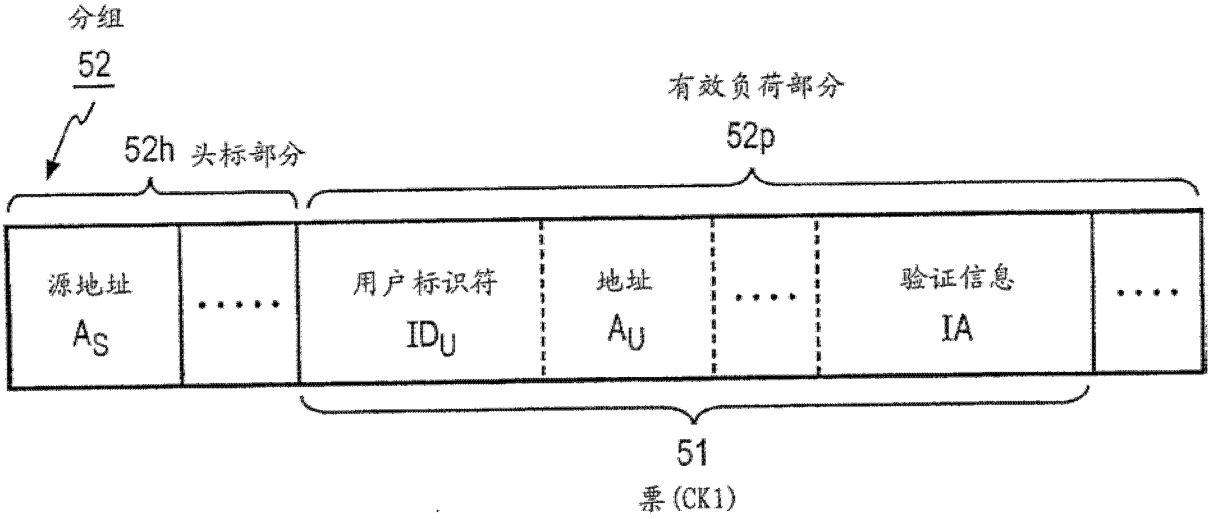

分组
52
52h 头标部分
有效负荷部分
52p
源地址
A_S
.....
用户标识符
ID_U
地址
A_U
....
验证信息
IA
....
51
票(CK1)

图 6

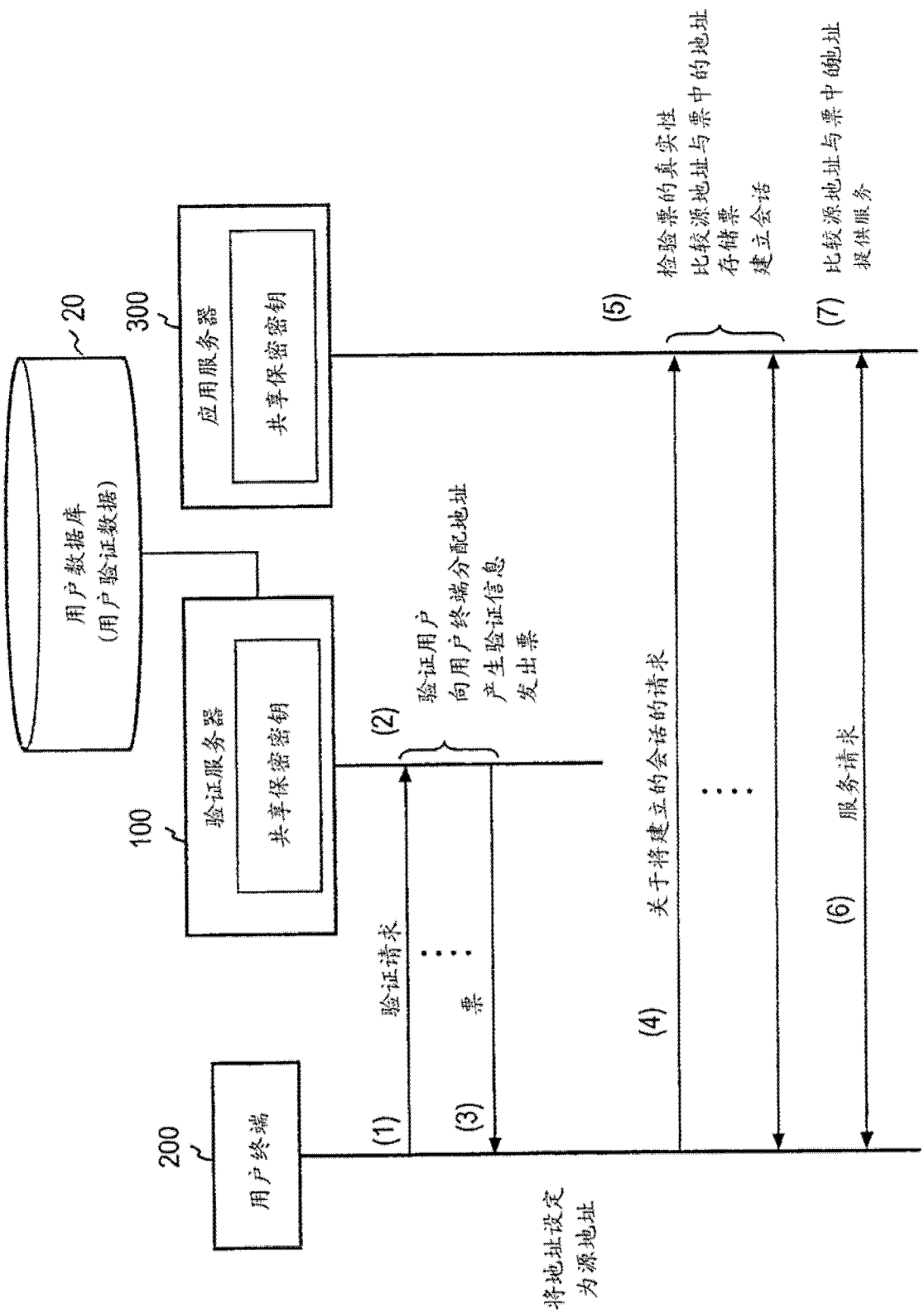

用户数据库
(用户验证数据)
20
应用服务器
300
共享保密密钥
验证服务器
共享保密密钥
100
用户终端
200
(1) 验证请求
(2) 验证用户
向用户终端分配地址
产生验证信息
发出票
(3) 票
(4) 关于将建立的会话的请求
(5) 检验票的真实性
比较源地址与票中的地址
存储票
建立会话
(6) 服务请求
(7) 比较源地址与票中的地址
提供服务
将地址设定
为源地址

图 7

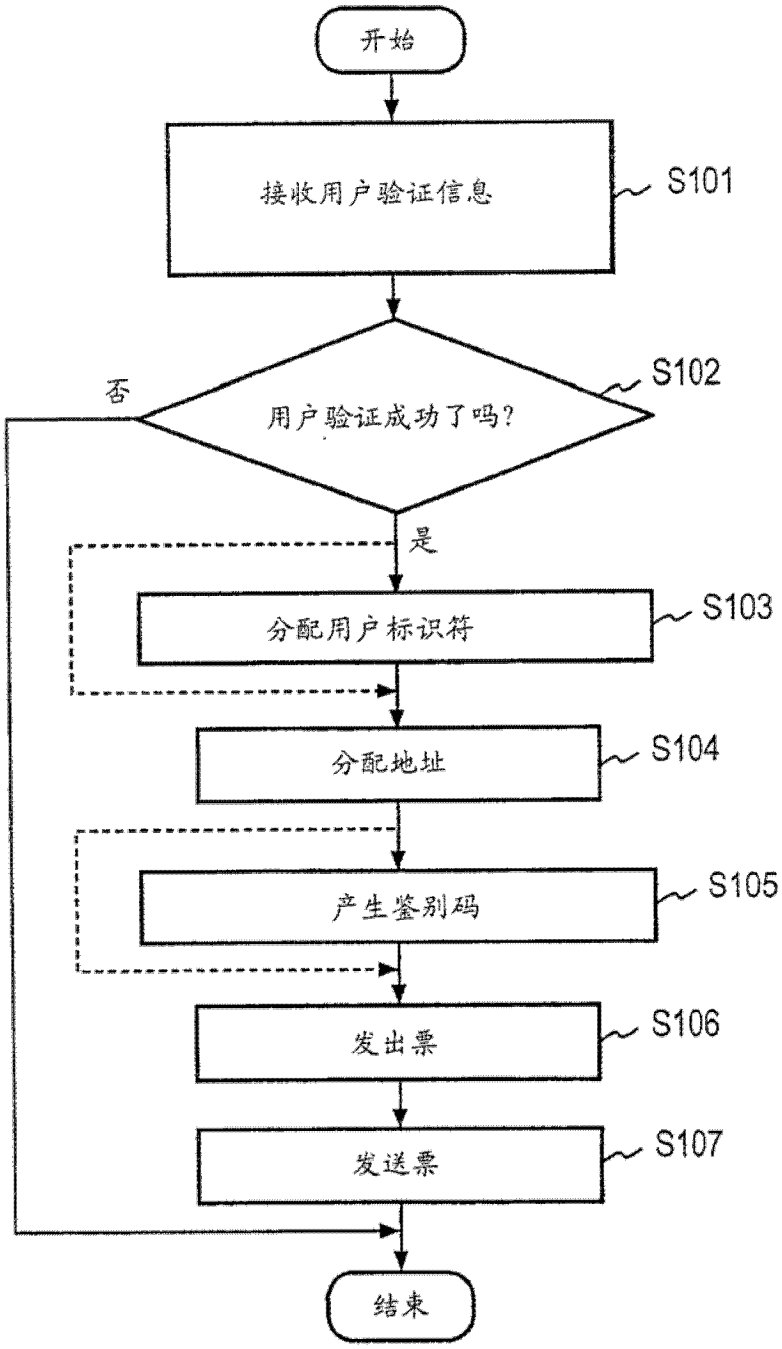

开始
接收用户验证信息
S101
用户验证成功了吗?
S102
否
是
分配用户标识符
S103
分配地址
S104
产生鉴别码
S105
发出票
S106
发送票
S107
结束

图 8

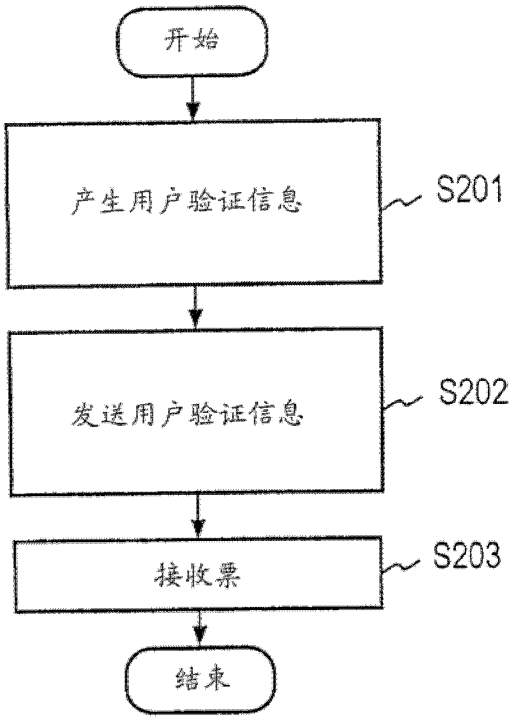

开始
产生用户验证信息
S201
发送用户验证信息
S202
接收票
S203
结束

图 9A

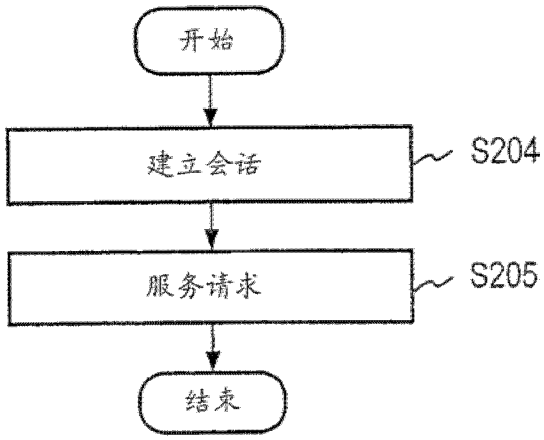

开始
建立会话
S204
服务请求
S205
结束

图 9B

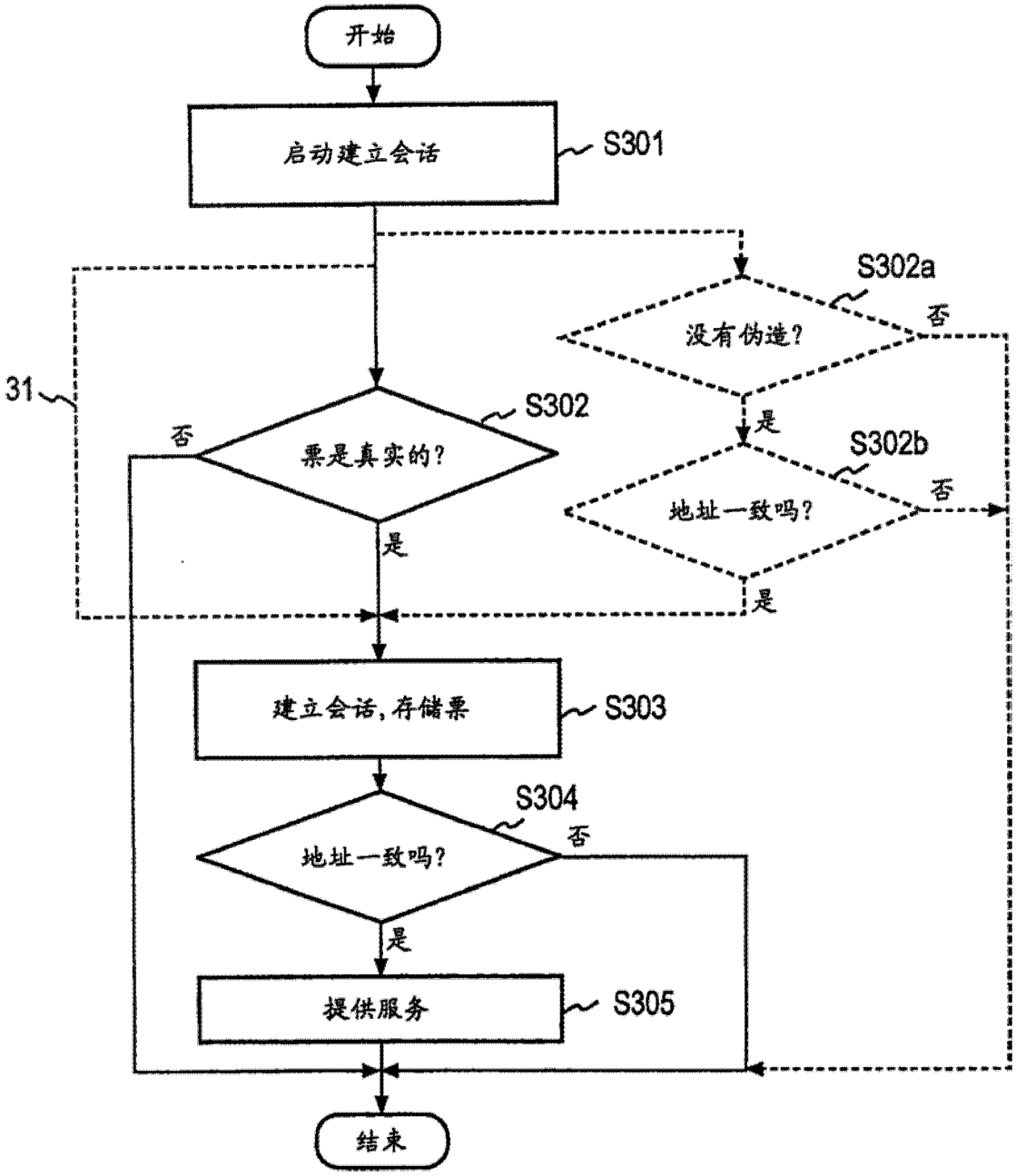

开始
启动建立会话
S301
S302a
没有伪造?
否
是
31
S302
否
票是真实的?
S302b
地址一致吗?
否
是
是
建立会话,存储票
S303
S304
地址一致吗?
否
是
提供服务
S305
结束

图 10

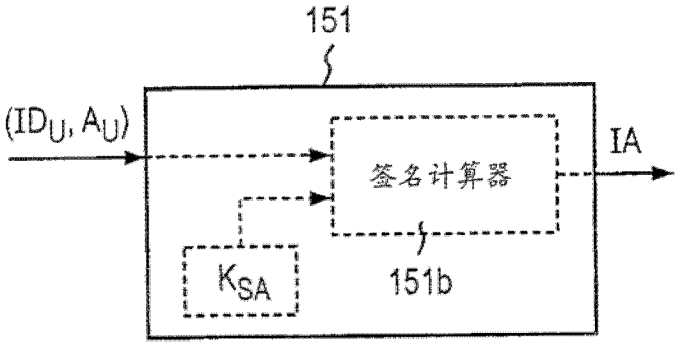


图 11A

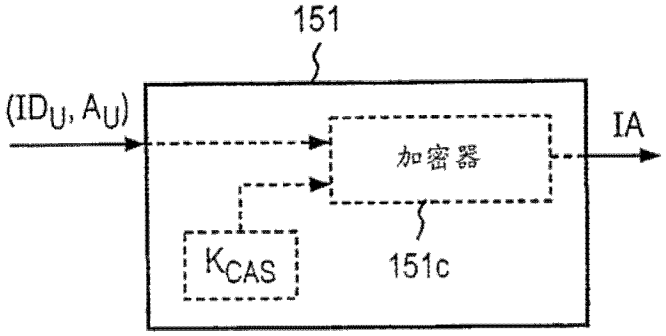


图 11B

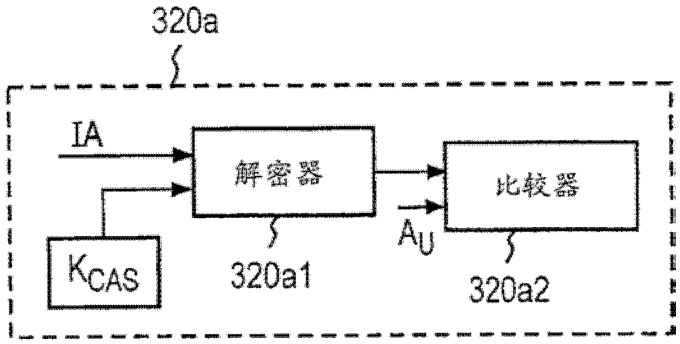


图 11C

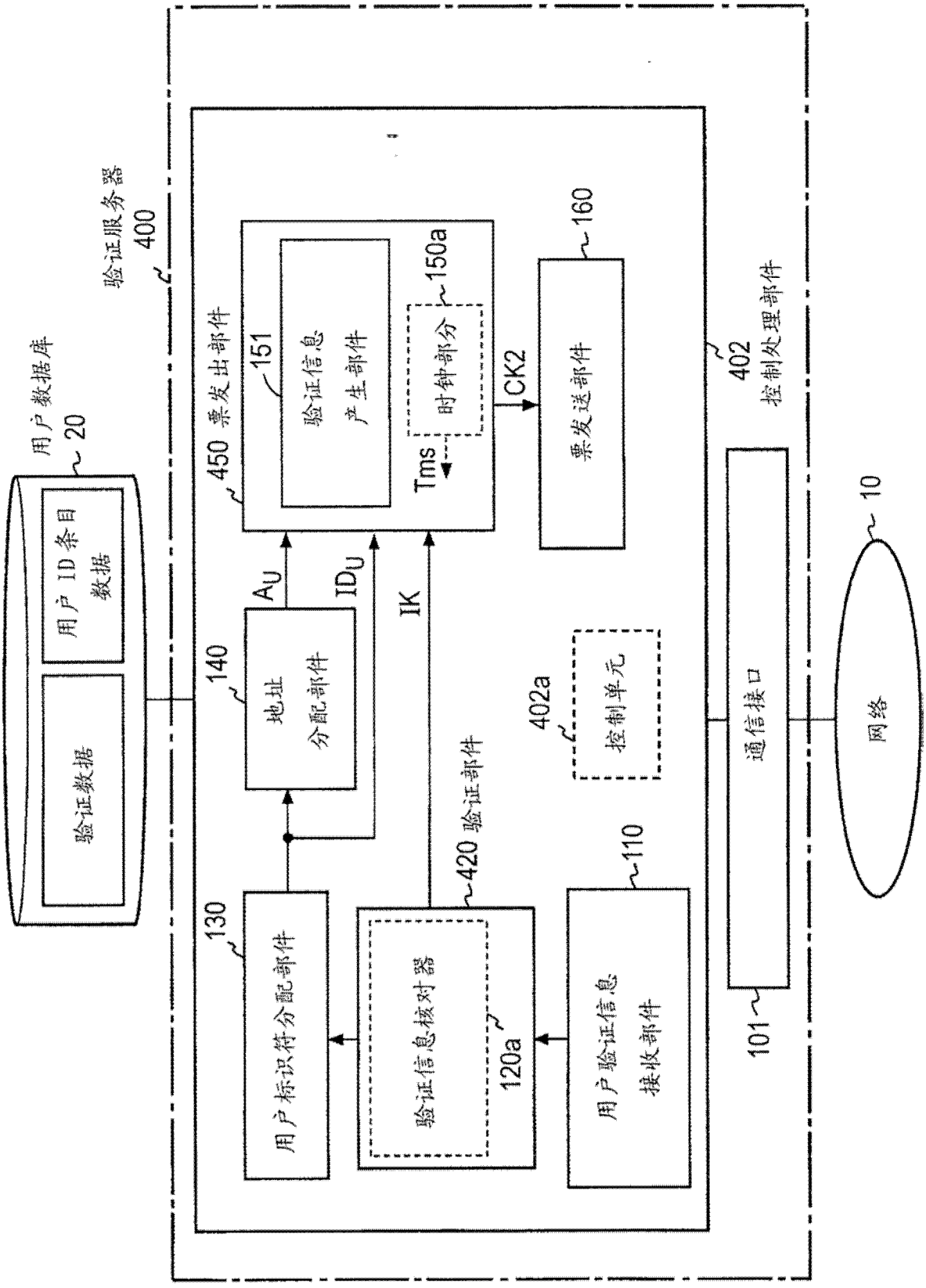

验证服务器
400
用户数据库
20
用户 ID 条目数据
验证数据
140
地址分配部件
A_U
ID_U
IK
450 票发出部件
151
验证信息产生部件
150a
时钟部分
Tms
CK2
160
票发送部件
402
控制处理部件
402a
控制单元
通信接口
101
网络
10
420 验证部件
130
用户标识符分配部件
验证信息核对器
120a
110
用户验证信息接收部件

图 12

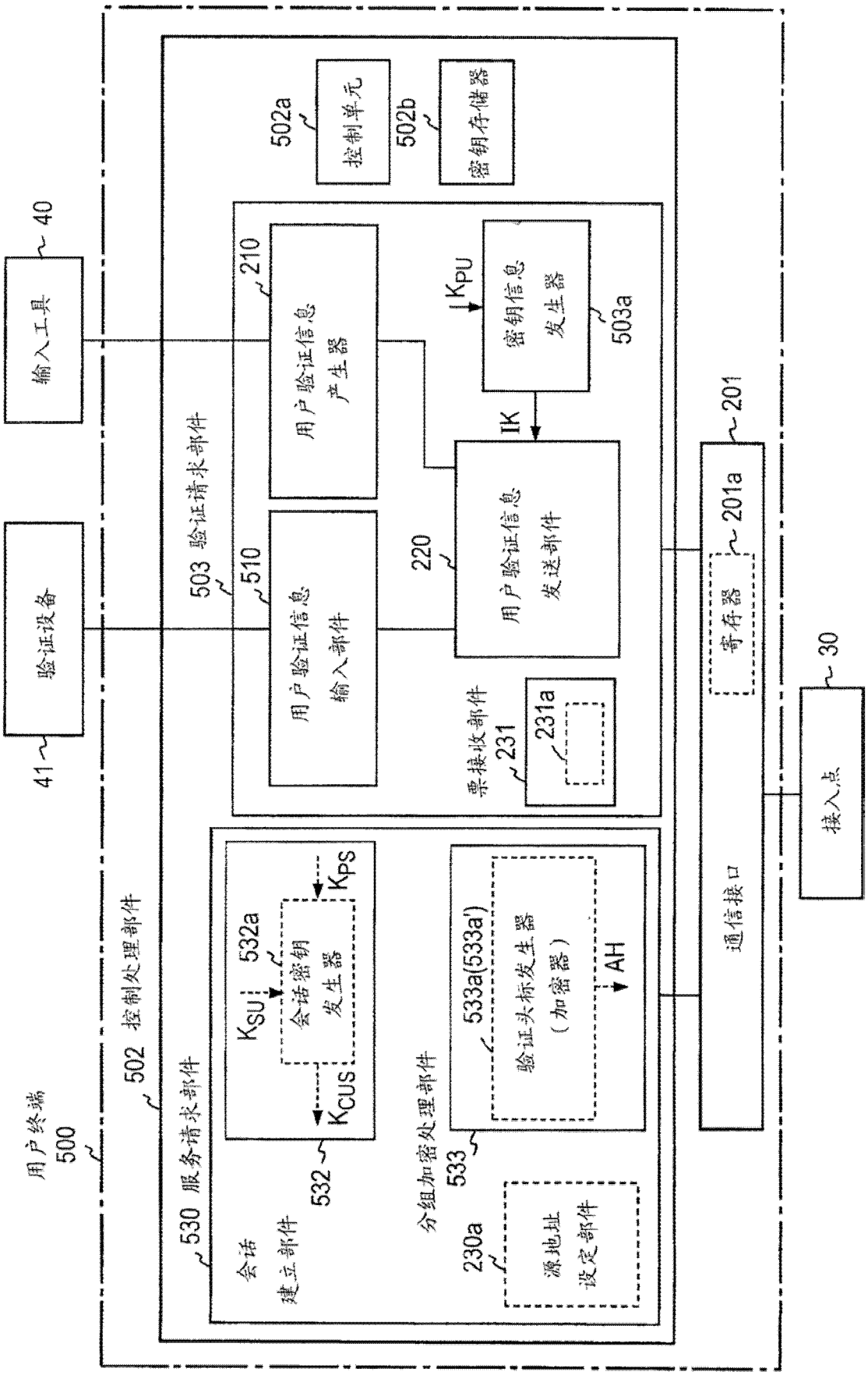

用户终端
500
控制处理部件
502
服务请求部件
530
会话
建立部件
532
K_{SU}
532a
会话密钥
发生器
K_{PS}
K_{CUS}
分组加密处理部件
533
533a(533a')
验证头标发生器
(加密器)
AH
230a
源地址
设定部件
验证请求部件
503
510
用户验证信息
输入部件
220
用户验证信息
发送部件
210
用户验证信息
产生器
K_{PU}
密钥信息
发生器
503a
IK
票接收部件
231
231a
502a
控制单元
502b
密钥存储器
输入工具
40
验证设备
41
通信接口
201
寄存器
201a
接入点
30

图 13

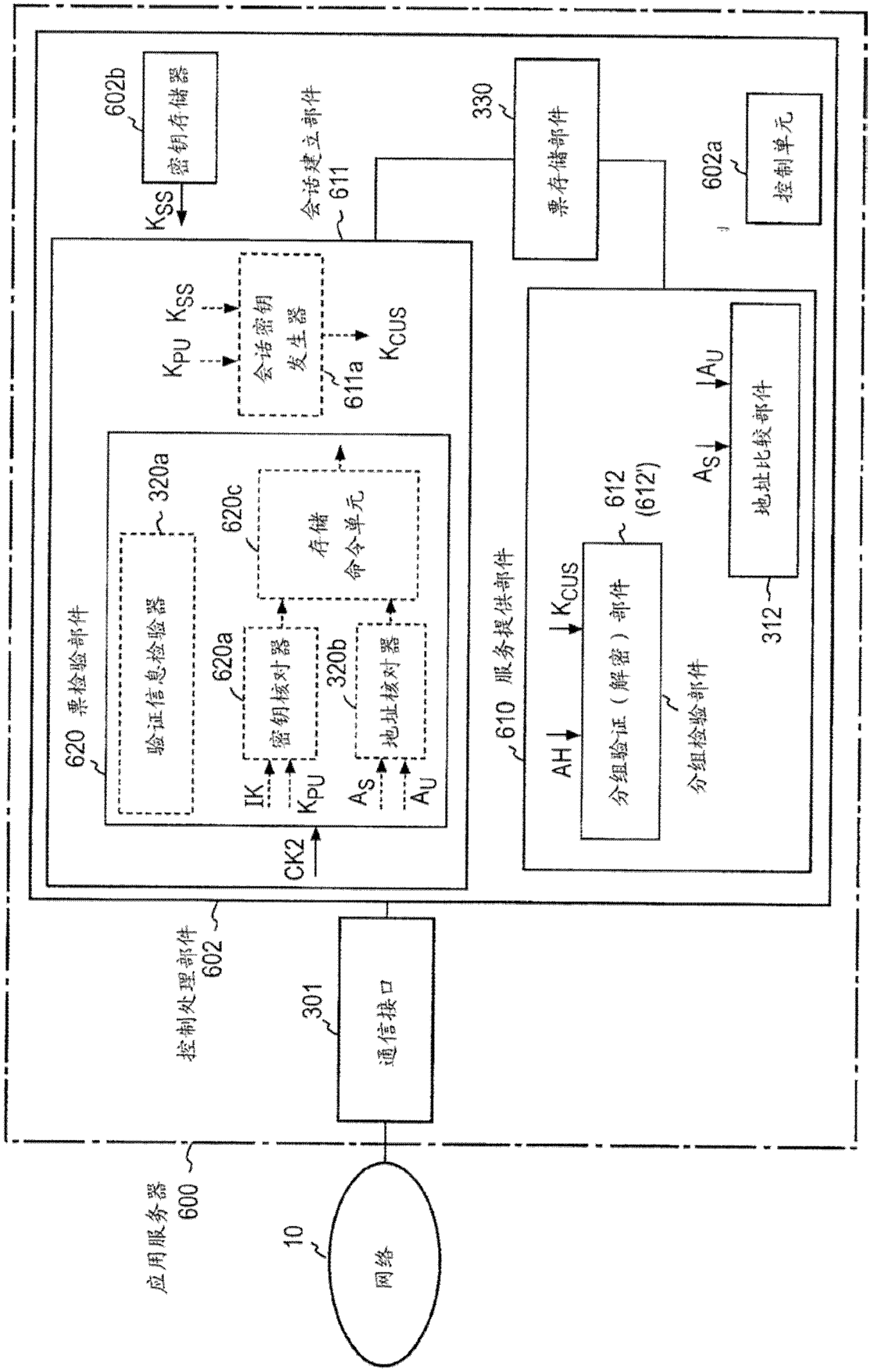

应用服务器
600
网络
10
通信接口
301
控制处理部件
602
票检验部件
620
验证信息检验器
320a
密钥核对器
620a
地址核对器
320b
存储
命令单元
620c
IK
KPU
AS
AU
CK2
会话建立部件
611
会话密钥
发生器
611a
KSS
KPU
KCUS
602b
密钥存储器
KSS
服务提供部件
610
分组验证（解密）部件
612
(612')
分组检验部件
AH
KCUS
地址比较部件
312
AS
AU
票存储部件
330
控制单元
602a

图 14

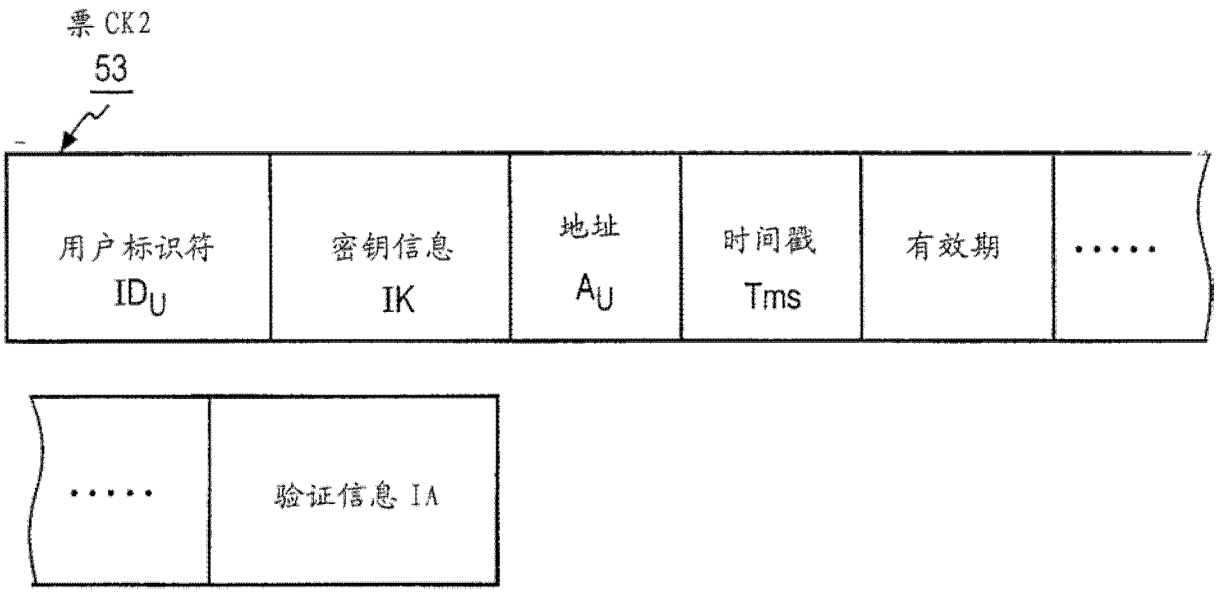

票 CK2
53
用户标识符
ID_U
密钥信息
IK
地址
A_U
时间戳
Tms
有效期
.....
.....
验证信息 IA

图 15

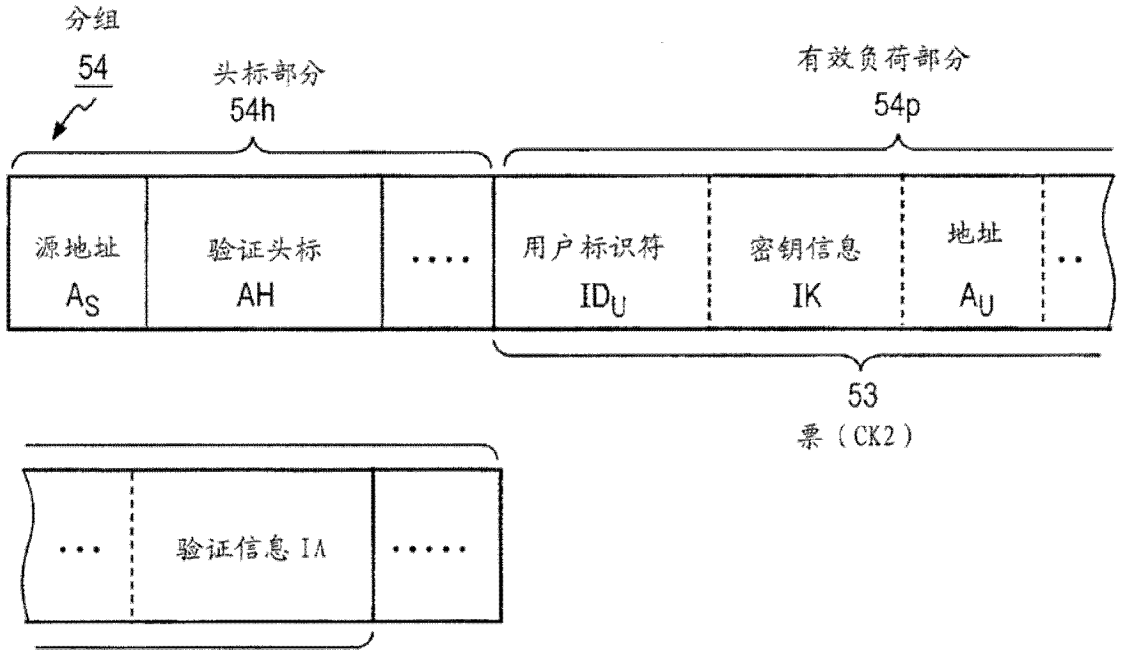

分组
54
头标部分
54h
有效负荷部分
54p
源地址
A_S
验证头标
AH
....
用户标识符
ID_U
密钥信息
IK
地址
A_U
..
53
票（CK2）
...
验证信息 IA
.....

图 16

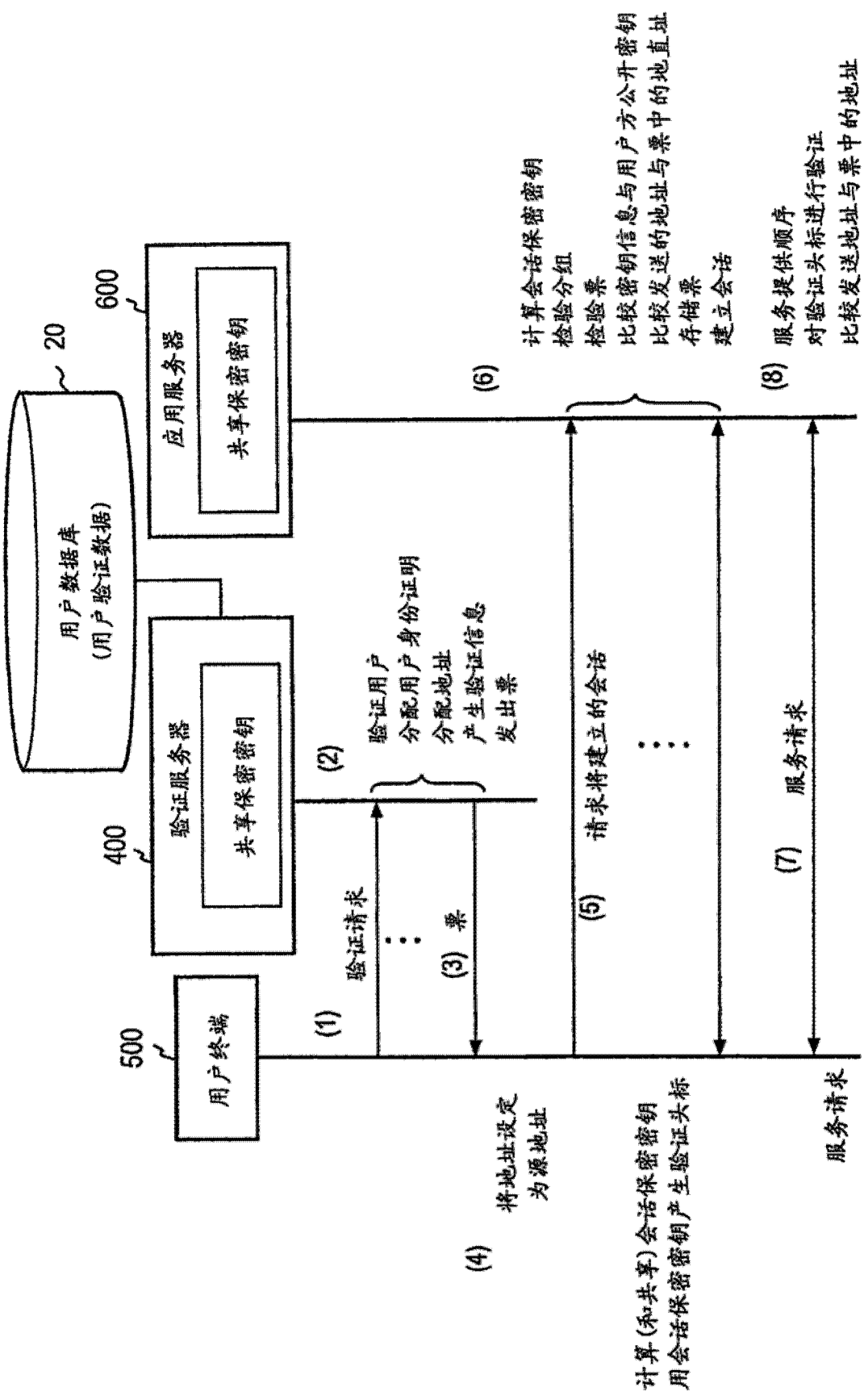

用户终端
500
验证服务器
共享保密密钥
400
用户数据库
(用户验证数据)
20
应用服务器
共享保密密钥
600
(1) 验证请求
(2) 验证用户
分配用户身份证明
分配地址
产生验证信息
发出票
(3) 票
(4) 将地址设定为源地址
(5) 请求将建立的会话
(6) 计算会话保密密钥
检验分组
检验票
比较密钥信息与用户方公开密钥
比较发送的地址与票中的地址
存储票
建立会话
(7) 服务请求
(8) 服务提供顺序
对验证头标进行验证
比较发送地址与票中的地址
提供服务
计算(和共享)会话保密密钥
用会话保密密钥产生验证头标
服务请求

图 17

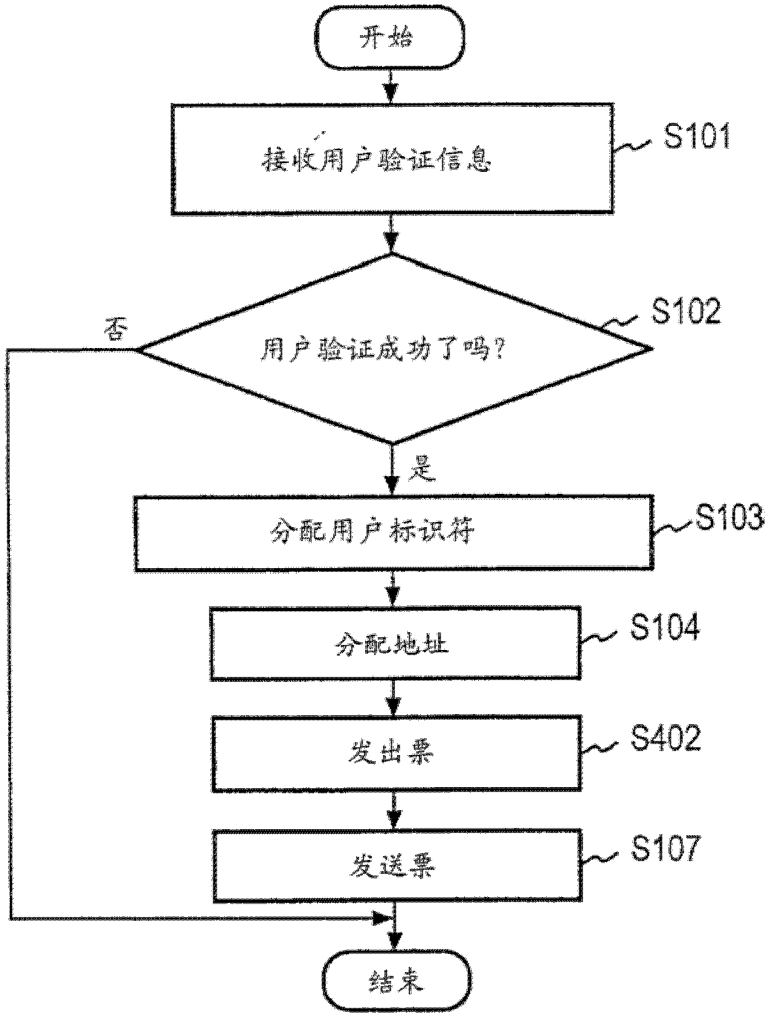


图 18

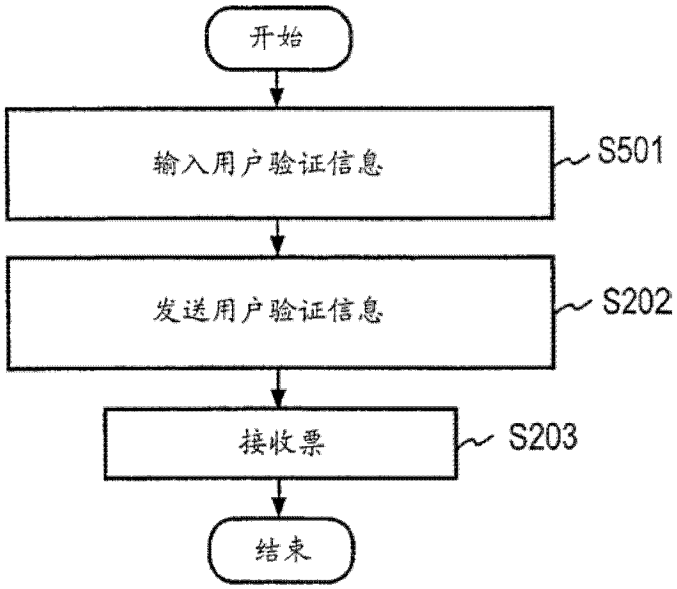


图 19A

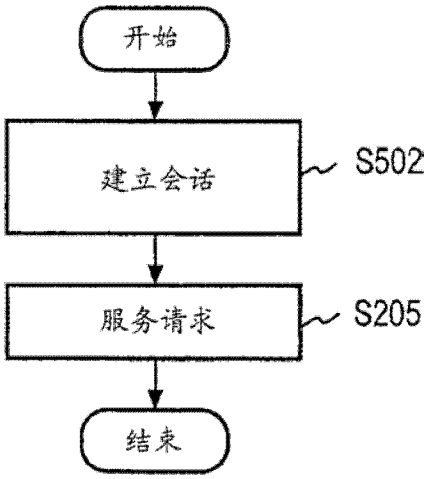


图 19B

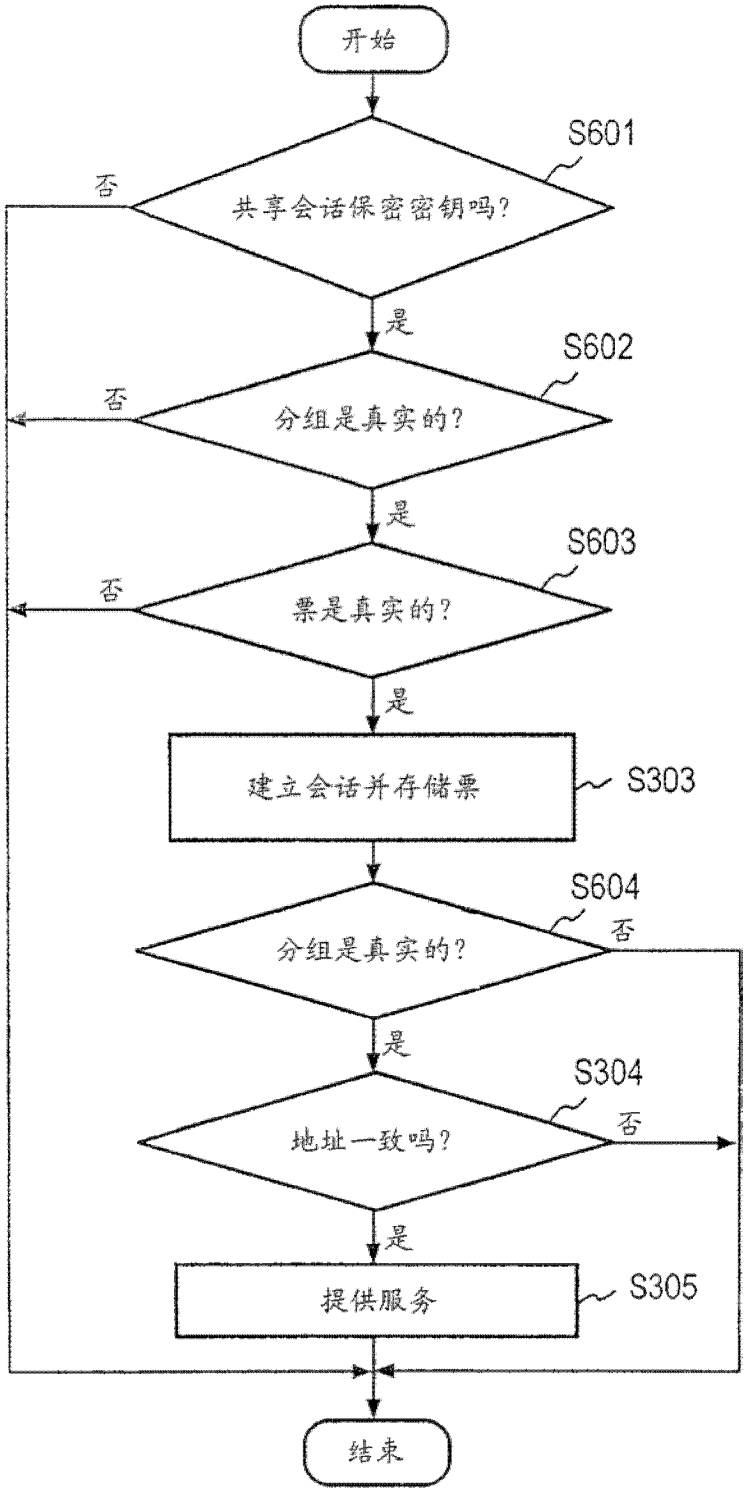

开始
S601
共享会话保密密钥吗?
否
是
S602
分组是真实的?
否
是
S603
票是真实的?
否
是
建立会话并存储票
S303
S604
分组是真实的?
否
是
S304
地址一致吗?
否
是
提供服务
S305
结束

图 20

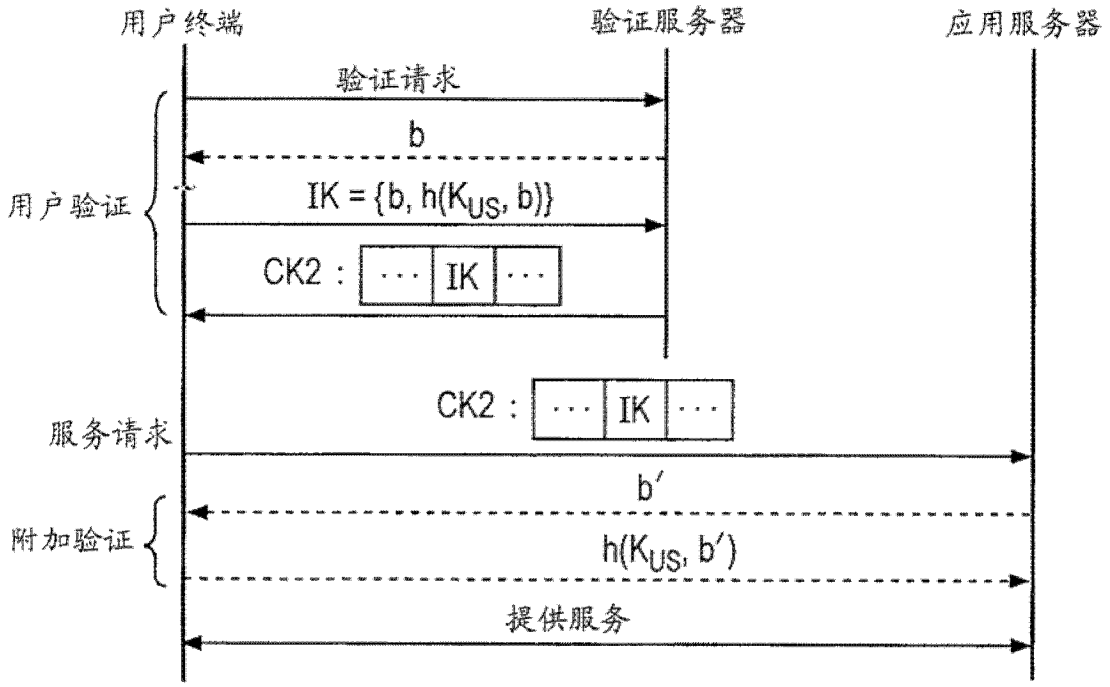


图 21A

图 21B

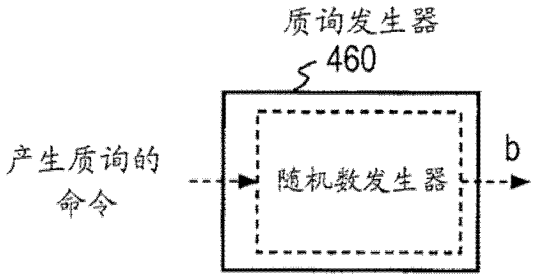
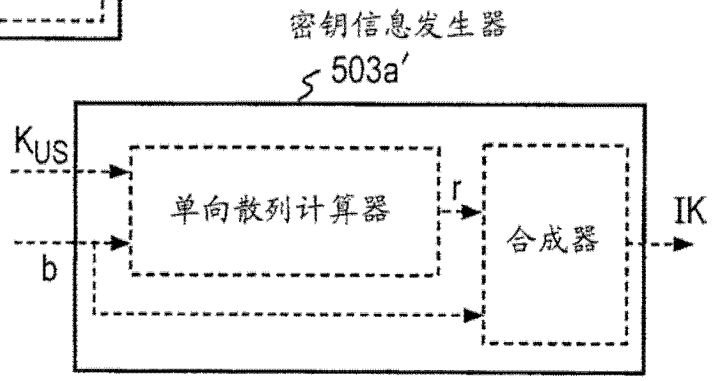


图 21C



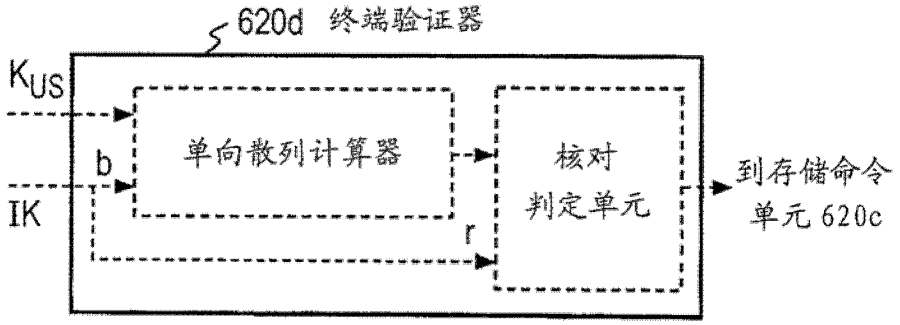


图 21D