(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 1681238 B
(45)授权公告日 2010.12.08

(21)申请号 200410075235.3

(22)申请日 2004.09.13

(30)优先权数据
2004-113732 2004.04.08 JP

(73)专利权人 株式会社日立制作所
地址 日本东京都

(72)发明人 高田治 藤城孝宏 锻忠司 星野和义

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 胡建新

(51)Int.Cl.
H04L 9/00(2006.01)

(56)对比文件
CN 1299545 A,2001.06.13, 全文.
US 2003/0147536 A1,2003.08.07, 全文.
US 6094487 A,2000.07.25, 说明书第1栏第51行到第2栏第6行, 第2栏第57行到第5栏第44行、图1.

审查员 林牲

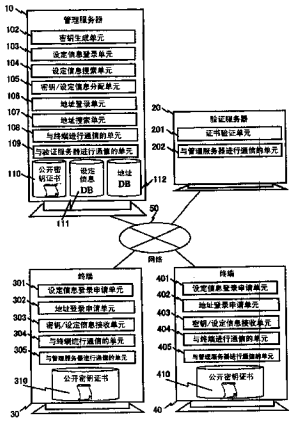
权利要求书 2 页 说明书 13 页 附图 12 页

(54)发明名称

用于加密通信的密钥分配方法及系统

(57)摘要

本发明提供一种将用于加密通信的密钥分配给通信源终端和通信对象终端的方法及系统。设置管理服务器(10)和验证服务器(20)。终端(30)和终端(40)预先将用于加密通信的、可以利用的设定信息登录到管理服务器(10)中。在进行加密通信时,管理服务器(10)从登录的设定信息中搜索一致的设定信息,终端(30)和终端(40)生成能够利用的、该加密通信用的密钥,与一致的设定信息一起分配。管理服务器(10)和验证服务器(20)一起认证终端(30)和终端(40)。终端(30)信赖管理服务器(10)认证终端(40)的结果,终端(40)信赖管理服务器(10)认证终端(30)的结果,由此不必分别认证通信对方的终端。



CN 1681238 B

1. 一种通信系统，包括通信源终端、通信对象终端和管理服务器，其特征在于，

上述通信源终端和上述通信对象终端，分别向多个加密通信用设定信息赋予优先顺序，登录到上述管理服务器中；

上述通信源终端向管理服务器发送与通信对象终端连接的请求；

上述管理服务器根据上述连接请求，参照上述优先顺序，从预先所登录的、上述通信源终端的上述加密通信用设定信息、和上述通信对象终端的上述加密通信用设定信息中，搜索一致的加密通信用设定信息；

当搜索到了一致的加密通信用设定信息时，上述通信源终端和上述通信对象终端使用根据上述一致的加密通信用设定信息所生成的加密通信用密钥，进行加密通信。

2. 如权利要求 1 所述的通信系统，其特征在于，

上述管理服务器将上述连接请求发送给上述通信对象终端，上述通信对象终端进行上述连接请求可否的判断。

3. 如权利要求 1 所述的通信系统，其特征在于，

上述管理服务器根据上述一致的加密通信用设定信息，生成上述加密通信用的密钥，

将生成的上述加密通信用密钥发送给上述通信源终端和上述通信对象终端。

4. 如权利要求 1 所述的通信系统，其特征在于，

上述管理服务器根据上述一致的加密通信用设定信息，生成作为上述加密通信用密钥的种子的信息；

将生成的作为上述加密通信用密钥的种子的信息发送给上述通信源终端和上述通信对象终端；

上述通信源终端和上述通信对象终端分别根据接收到的作为上述密钥的种子的信息，生成上述加密通信用的密钥。

5. 如权利要求 1 所述的通信系统，其特征在于，

上述通信源终端为了发送与上述通信对象终端连接的上述请求，与上述管理服务器之间建立加密通信信道；

上述管理服务器为了发送上述通信源终端发出的与上述通信对象终端的连接的上述请求，与上述通信对象终端之间建立加密通信信道。

6. 如权利要求 5 所述的通信系统，其特征在于，

还具有验证服务器；

上述通信源终端将上述通信源终端的公开密钥证书发送给上述管理服务器；

上述管理服务器请求上述验证服务器验证上述通信源终端的公开密钥证书；

上述验证服务器验证上述通信源终端的公开密钥证书，将验证结果向上述管理服务器应答；

上述管理服务器在上述通信源终端的公开密钥证书的验证成功时，与上述通信源终端之间建立上述加密通信信道。

7. 如权利要求 6 所述的通信系统，其特征在于，

上述通信对象终端将上述通信对象终端的公开密钥证书发送给上述管理服务器；

上述管理服务器请求上述验证服务器验证上述通信对象终端的公开密钥证书；

上述验证服务器验证上述通信对象终端的公开密钥证书，将验证结果向上述管理服务

器应答；

上述管理服务器在上述通信对象终端的公开密钥证书的验证成功时，与上述通信对象终端之间建立上述加密通信信道。

8. 如权利要求 7 所述的通信系统，其特征在于，

上述通信源终端或上述通信对象终端请求上述管理服务器发送公开密钥证书；

上述管理服务器将被请求的管理服务器的公开密钥证书发送给上述通信源终端或上述通信对象终端；

上述通信源终端或上述通信对象终端从上述管理服务器接收上述管理服务器的公开密钥证书，进行上述管理服务器的公开密钥证书的验证，在验证成功时，与上述管理服务器之间建立上述加密通信信道。

9. 如权利要求 5 所述的通信系统，其特征在于，

上述通信源终端和 / 或上述通信对象终端利用上述加密通信信道，将上述加密通信用设定信息登录到上述管理服务器中。

用于加密通信的密钥分配方法及系统

技术领域

[0001] 本发明涉及一种将用于加密通信的密钥分配给通信源终端和通信对象终端的方法及系统。

背景技术

[0002] 在通信源终端装置与通信对象终端装置（以下将“终端装置”称为“终端”）之间通过网络进行加密通信时，将数据加密进行接收和发送。通信源终端与通信对象终端预先共有用于在通信源终端与通信对象终端之间进行加密通信的设定信息和密钥，用共有的设定信息和密钥进行加密通信。

[0003] 例如，在使用公开密钥密码共有密钥时，如下这样地进行。

[0004] 通信源终端获取通信对象终端的公开密钥，生成用于与通信源终端进行加密通信的密钥，使用该公开密钥加密该加密通信的密钥，发送给通信对象终端。并且，通信对象终端从通信源终端接收用该公开密钥加密过的该加密通信用的密钥，用通信对象终端的专用密钥解码。

[0005] 在上述方法中，通信源终端为了与多个通信对象终端进行加密通信，有必要分别与各通信对象终端共有用于该加密通信的设定信息和密钥，存在通信源终端的负荷变大的问题。

[0006] 因此提出了在网络上设置将上述加密通信用的设定信息和密钥分配给通信源终端和通信对象终端的服务器装置（以下简称“服务器”），通信源终端和通信对象终端用该服务器分配给的上述加密通信用设定信息和密钥进行加密通信的方案。参照Mark Baugher及其他3人所著，“MSEC Group Key Management Architecture<draft-ietf-msec-gkmarch-07.txt>”、2003年1月30日；IETF(InternetEngineering Task Force)，P.3-13[日本平成16年4月2日检索]，<URL：http://www.

[0007] ietf.org/internet-drafts/draft-msec-gkmarch-07.txt>

[0008] 并且，在通过网络进行的通信中，为了确认通信对方的合法性，在进行通信之前有必要认证通信对方。认证通信对方的方法之一有使用电子签名的方法。具体为，进行通信的通信源终端和通信对象终端互相交换付与了电子签名的ID和公开密钥证书，验证获得的电子签名和公开密钥证书，由此认证通信对方。

[0009] 通信源终端为了与多个通信对象终端进行加密通信，有必要分别与各通信对象终端共有用于该加密通信的设定信息和密钥，通信源终端的负荷变大。

[0010] 例如，通信源终端为了用公开密钥密码与通信对象终端共有用于加密通信的密钥，通信源终端有必要进行获取通信对象终端的公开密钥、生成用于进行加密通信的密钥、加密使用了获得的公开密钥的加密通信的密钥的处理，通信源终端的负荷变大。

[0011] 为了解决这些问题，在使用上述非专利文献1的技术的情况下，服务器生成通信源终端与通信对象终端之间的加密通信用的设定信息和密钥，并分配给通信源终端和通信对象终端。但是，终端并不局限于支持分配到的设定信息和密钥。当通信源终端或通信对

象终端分配到不支持的设定信息或密钥时，在通信源终端与通信对象终端之间不能进行加密通信。

[0012] 并且，为了确认通信对方的合法性，通信源终端与通信对象终端进行认证各通信对方的处理。但是，在通信源终端进行与多个通信对象终端的加密通信时，有必要分别认证各通信对象终端，确认通信对方的合法性，通信源终端的处理负荷变大。

发明内容

[0013] 本发明提供一种在网络上管理终端间的通信、配置了管理服务器的通信系统。

[0014] 本发明的通信系统通过进行以下的步骤，通信源终端和通信对象终端共有在进行通信源终端与通信对象终端之间的加密通信时使用的密钥。

[0015] 通信源终端和通信对象终端分别预先将能够利用的用于进行上述加密通信的设定信息登录到管理服务器中。

[0016] 通信源终端在与通信对象终端连接时通知管理服务器，管理服务器从通信源终端与通信对象终端的设定信息中搜索一致的设定信息。

[0017] 管理服务器根据一致的设定信息生成加密通信用的密钥或密钥的种子的信息，根据一致的设定信息分配给通信源终端和通信对象终端。通信源终端和通信对象终端在管理服务器分配了设定信息和密钥的种子信息的情况下根据密钥种类信息生成密钥，使用管理服务器分配的设定信息和生成或发送来的密钥进行加密通信。

[0018] 并且，上述通信系统的特征在于，管理服务器利用电子签名认证通信源终端和通信对象终端，认为通信源终端和通信对象终端互相认证对方。

[0019] 在通信源终端请求与通信对象终端进行通信时，管理服务器认证两终端，在认证成功时许可两终端间的通信。在管理服务器许可该通信后，通信源终端可以与通信对象终端连接。

[0020] 而且，管理服务器可以委托验证公开密钥证书的验证服务器（以下简称“验证服务器”）验证通信源终端和通信对象终端的公开密钥证书。

[0021] 通过验证服务器验证该公开密钥证书，能够更确实地认证通信源终端和通信对象终端。

[0022] 发明效果

[0023] 如果采用本发明，通信源终端不必进行与通信对象终端共有用于在通信源终端与通信对象终端之间进行加密通信的设定信息或密钥的处理。

[0024] 而且，通信源终端与通信对象终端能够确实地进行加密通信。

[0025] 并且，如果采用本发明，通信源终端与通信对象终端不必直接认证通信对方，减轻了处理负担。

附图说明

[0026] 图 1 表示本发明的一个实施形态的通信系统的结构的图

[0027] 图 2 表示终端 30 和管理服务器 10 共有用于在终端 30 与管理服务器 10 之间进行加密通信的参数，交换公开密钥证书的处理过程的流程图

[0028] 图 3 表示管理服务器 10 请求验证服务器 20 验证终端 30 的公开密钥证书，验证服

务器 20 应答验证结果的处理过程的流程图

[0029] 图 4 表示终端 30 和管理服务器 10 用电子签名互相认证对方，分别生成终端 30 与管理服务器 10 之间的加密通信用的密钥的处理过程的流程图

[0030] 图 5 表示到终端 30 与管理服务器 10 建立连接进行加密通信之前的处理过程的流程图

[0031] 图 6 表示终端 30 与管理服务器 10 结束连接的处理过程的流程图

[0032] 图 7 表示终端 30 将终端 30 的地址、与其他终端进行加密通信用的设定信息登录到管理服务器 10 中的处理过程的流程图

[0033] 图 8 表示在终端 30 进行与终端 40 的连接处理时管理服务器 10 从终端 30 和终端 40 所登录的设定信息中搜索一致的设定信息的处理过程的流程图

[0034] 图 9 表示管理服务器 10 生成终端 30 和终端 40 之间的加密通信用的密钥并将其分配给终端 30 和终端 40 的处理过程的流程图

[0035] 图 10 表示终端 30 结束通过管理服务器 10 与终端 40 的连接的处理过程的流程图

[0036] 图 11 表示管理服务器 10、验证服务器 20、终端 30 和终端 40 各硬件的结构示例的图

[0037] 图 12 管理服务器 10 所保持的地址 DB112 的内容的示例

[0038] 图 13 管理服务器 10 所保持的设定信息 DB111 的示例

具体实施方式

[0039] 下面详细说明本发明的实施形态。另外，本发明并不局限于此。

[0040] 图 1 为表示本发明的实施形态 1 的密钥分配系统的结构的方框图。

[0041] 在图 1 的密钥分配系统中，网络 50 上连接着终端 30、终端 40、管理服务器装置（以下简称“管理服务器”）10 和验证服务器装置（以下简称“验证服务器”）20。

[0042] 终端 30 和终端 40 分别将委托的认证局各自发行的公开密钥证书 310、410 保管在终端内。而且包括：用于在该终端之间进行加密通信的设定信息登录申请单元 301、401，用于登录确定该终端在网络上的位置的地址的地址登录申请单元 302、402，请求该终端之间进行加密通信、从管理服务器 10 接收必要的密钥或设定信息的密钥 / 设定信息接收单元 303、403，在该终端之间进行加密通信的终端通信单元 304、404，管理服务器通信单元 305、405。

[0043] 管理服务器 10 保管由委托的认证局发行的公开密钥证书 110、终端 30 与终端 40 进行加密通信的设定信息 DB111、确定终端 30 和终端 40 在网络上的位置的地址 DB112。在本实施例中，用 IP 地址作为上述终端地址。

[0044] 而且，管理服务器 10 包括：生成用于在终端 30 与终端 40 之间进行加密通信的密钥的密钥生成单元 102；接受终端 30 或终端 40 提出的设定信息的登录申请，登录设定信息的设定信息登录单元 103；当终端 30 与终端 40 连接时，从终端 30 和终端 40 所登录的设定信息中搜索一致的设定信息的设定信息搜索单元 104；分配用于在终端 30 与终端 40 之间进行加密通信的密钥或设定信息的密钥 / 设定信息分配单元 105；接受终端 30 或终端 40 提出的登录地址的申请，将地址登录到地址 DB112 中的地址登录单元 106；在地址 DB112 中搜索终端的地址的地址搜索单元 107；进行终端的认证和通信的对终端通信单元 108；以及与

验证服务器 20 进行通信的与验证服务器进行通信的单元 109。

[0045] 验证服务器 20 包括：在管理服务器 10 认证终端 30 或终端 40 时确认公开密钥证书的有效性的证书验证单元 201、和与管理服务器 10 进行通信的对管理服务器通信单元 202。

[0046] 另外，图 1 所示的管理服务器 10 和验证服务器 20、终端 30、终端 40 等各种装置以及具备这些装置的各单元例如图 11 所示那样具备 CPU61、存储器 62、硬盘等外部存储装置 63、通过因特网等网络或 LAN（以下简称“网络”）50 与其他装置进行通信的通信装置 64、键盘或鼠标等输入装置 65、监视器或打印机等输出装置 66、从可移动的记忆媒体 68 中读取信息的读取装置 67、在这些装置之间进行数据的传输的接口 60，在电子计算机中，通过 CPU61 执行装入存储器 62 中的预定的程序能够实现。

[0047] 这些程序也可以预先保存在上述电子计算机内的存储器 62 或者外部存储装置 63 中，必要时可以通过上述电子计算机能够利用的、可以插拔的记忆媒体 68 或者通信媒体（网络或 LAN50 等或者在其上传送的载波或数字信号等）导入。

[0048] 另外，在本实施例中，终端可以用图 11 所示那样的结构实现，但本发明并不局限于此。图 1 所示的终端 30 和终端 40 各设备也可以是具备能够与网络 50 相连接的通信装置的设备。例如，路由器、PC、移动电话机、PDA、电视机和冰箱等也可以成为终端。

[0049] 下面就本实施形态的通信系统的动作进行说明。

[0050] 本实施形态的通信系统首先建立终端 30 通过网络 50 与管理服务器 10 的保密通信信道。

[0051] 这里描述终端 30 建立与管理服务器 10 之间进行加密通信的信道进行加密通信，直到结束通信时的动作。在建立该通信信道时，终端 30 将终端 30 的公开密钥证书发送给管理服务器 10，管理服务器 10 请求验证服务器 20 验证该公开密钥证书的有效性，管理服务器 10 根据验证服务器 20 验证该公开密钥证书的有效性的结果，来认证终端 30。

[0052] 首先，终端 30 和管理服务器 10 按照图 2 所示的流程交换公开密钥证书 310 和公开密钥证书 110。

[0053] 对管理服务器通信单元 305 将用于与管理服务器 10 之间进行加密通信的 1 个以上的参数的候补发送给管理服务器 10（步骤 1000）。用于加密通信的参数中包含加密通信数据时使用的加密算法的种类、密钥的长度、用于检测通信数据是否篡改了的散列函数的种类等。

[0054] 对终端通信单元 108 接收终端 30 传送来的加密通信参数的候补（步骤 1002）。

[0055] 管理服务器 10 从接收到的参数的候补中选择 1 个管理服务器能够利用的参数，对终端通信单元 108 将选择的参数发送给终端 30（步骤 1004）。

[0056] 对管理服务器通信单元 305 接收管理服务器 10 选择的参数（步骤 1006）。

[0057] 经过上述步骤 1000 到步骤 1006，终端 30 和管理服务器 10 共有参数。

[0058] 对管理服务器通信单元 305 将管理服务器 10 的公开密钥证书 110 的请求发送给管理服务器 10（步骤 1008）。

[0059] 对终端通信单元 108 接收终端 30 发送来的公开密钥证书 110 的请求（步骤 1010）。

[0060] 当管理服务器 10 保持有在步骤 1010 中接受了请求的公开密钥证书 110 时（步骤 1012 中为 YES 时），对终端通信单元 108 将管理服务器 10 的公开密钥证书 110 和终端 30 的公开密钥证书请求发送给终端 30（步骤 1014）。

[0061] 对管理服务器通信单元 305 从管理服务器 10 中接收管理服务器 10 的公开密钥证书 110 和终端 30 的公开密钥证书请求（步骤 1016）。

[0062] 当终端 30 保持有在步骤 1016 中接受了请求的公开密钥证书 310（在步骤 1018 中为 YES）时，通过对管理服务器通信单元 305 将终端 30 的公开密钥证书 310 发送给管理服务器 10（步骤 1020）。

[0063] 对终端通信单元 108 从终端 30 中接收终端 30 的公开密钥证书 310（步骤 1022）。

[0064] 对终端通信单元 108 将终端 30 的公开密钥证书 310 的接收通知发送给终端 30（步骤 1024）。

[0065] 对管理服务器通信单元 305 从管理服务器 10 中接收终端 30 的公开密钥证书 310 的接收通知（步骤 1026）。

[0066] 对终端通信单元 304 通过验证在步骤 1016 中接收到的公开密钥证书 110 的有效性和签名验证公开密钥证书 110（步骤 1028）。

[0067] 终端 30 在公开密钥证书 110 的验证成功（在步骤 1030 中为 YES）时，进入图 3 的处理。

[0068] 在上述步骤 1012 或者步骤 1018 或者步骤 1030 为 NO 的情况下，进入图 6 的步骤 1316(A)，进行结束终端 30 与管理服务器 10 的通信的处理。但是，图 6 表示终端 30 请求结束通信时的情况，在从步骤 1012 进入时，由于管理服务器 10 发出了结束通信的请求，因此替换成终端 30 和管理服务器 10 的动作。

[0069] 接着，管理服务器 10 按照图 3 所示的流程请求验证服务器 20 验证终端 30 的公开密钥证书，获取验证结果。

[0070] 与验证服务器进行通信的单元 109 将终端 30 的公开密钥证书 310 发送给验证服务器 20（步骤 1100）。

[0071] 对管理服务器通信单元 202 接收公开密钥证书 310（步骤 1102）。

[0072] 验证服务器 20 通过证书验证单元 201 验证接收到的公开密钥证书 310。在公开密钥证书 310 的验证中，验证有效期限、签名和公开密钥证书的失效状态（步骤 1104）。

[0073] 当公开密钥证书 310 的验证 1104 不成功（步骤 1106 为 NO）时，通过对管理服务器通信单元 202 付与验证服务器 20 的签名，将验证失败的通知发送给管理服务器 10（步骤 1108）。

[0074] 当公开密钥证书 310 的验证 1104 成功（步骤 1106 为 YES）时，通过对管理服务器通信单元 202 付与验证服务器 20 的签名，将验证成功的通知发送给管理服务器 10（步骤 1110）。

[0075] 管理服务器 10 通过与验证服务器进行通信的单元 109 接收在步骤 1108 或步骤 1110 中发送来的验证失败的通知或验证成功的通知，验证付给到通知中的验证服务器 20 的签名，由此确认通知是否确实地从验证服务器 20 中发送、是否未被篡改（步骤 1112）。

[0076] 当在步骤 1112 中接收到验证成功的通知时，管理服务器 10 进入图 4 的 (D) 处理。而当在步骤 1112 中接收到验证失败的通知时，为了结束与终端 30 的连接，管理服务器 10 进入图 6 的步骤 1316(A)。另外，由于管理服务器 10 发出了结束通信的请求，因此替换成图 6 的终端 30 和管理服务器 10 的动作。

[0077] 接着，终端 30 和管理服务器 10 如图 4 所示那样将电子签名添加到图 2 的步骤中

共有的信息中并更换，验证更换过的电子签名，由此认证对方，此后进行密钥共有。另外，可以利用在图 2 的步骤中交更换的信息中的任意的信息作为共有信息。

[0078] 首先，终端 30 对共有信息生成电子签名，将电子签名添加到共有信息中，然后通过对管理服务器通信单元 305 发送到管理服务器 10 中（步骤 1200）。

[0079] 对终端通信单元 108 从终端 30 接收共有信息和电子签名（步骤 1202）。

[0080] 管理服务器 10 用在步骤 1022 中接收到的终端 30 的公开密钥证书 310 的公开密钥验证接收到的电子签名（步骤 1204）。

[0081] 当电子签名的验证成功（步骤 1206 为 YES）时，对共有信息生成电子签名，将电子签名添加到共有信息中，通过对终端通信单元 108 发送给终端 30（步骤 1208）。

[0082] 对管理服务器通信单元 305 从管理服务器 10 中接收共有信息和电子签名（步骤 1210）。

[0083] 终端 30 用在步骤 1016 中接收到的管理服务器 10 的公开密钥证书 110 的公开密钥验证接收到的电子签名（步骤 1212）。

[0084] 当电子签名的验证成功（步骤 1214 为 YES）时，终端 30 前进到生成终端 30 与管理服务器 10 之间的加密通信用的密钥的步骤 1216。

[0085] 终端 30 根据步骤 1000 到步骤 1006 共有的参数生成用于与管理服务器 10 进行加密通信的密钥（步骤 1216）。

[0086] 管理服务器 10 也根据步骤 1000 到步骤 1006 共有的参数生成用于与终端 30 进行加密通信的密钥（步骤 1218）。

[0087] 如果步骤 1206 或步骤 1214 为 NO（电子签名的验证失败），则为了结束连接，前进到图 6 的步骤 1316(A)。但是，图 6 表示终端 30 请求结束通信时的情况，从步骤 1206 进入时，由于管理服务器 10 发出了结束通信的请求，因此替换到终端 30 与管理服务器 10 的动作。

[0088] 通过以上的处理，终端 30 认证管理服务器 10，管理服务器 10 认证终端 30。并且，终端 30 和管理服务器 10 共有用于在终端 30 与管理服务器 10 之间进行加密通信的密钥。

[0089] 如果终端 30 和管理服务器 10 能够互相认证对方，则建立通信连接，进行加密通信。

[0090] 图 5 为表示建立用于进行上述加密通信，进行上述加密通信的步骤的顺序图。

[0091] 对管理服务器通信单元 305 将数据传输许可请求发送给管理服务器 10（步骤 1300），对终端通信单元 108 接收该请求（步骤 1302）。

[0092] 对终端通信单元 108 将数据传输许可和对终端 30 的数据传输许可请求发送给终端 30（步骤 1304），对管理服务器通信单元 305 接收它们（步骤 1306）。

[0093] 对管理服务器通信单元 305 将数据传输许可发送给管理服务器 10（步骤 1308），对终端通信单元 108 接收该许可（步骤 1310）。

[0094] 通过以上的处理，由于终端 30 和管理服务器 10 互相发出数据传输许可，因此建立连接（步骤 1312）。

[0095] 在建立连接后，终端 30 和管理服务器 10 用在图 2 的步骤 1000 到步骤 1006 中共有的、用于上述加密通信的参数和在步骤 1216 和步骤 1218 中生成的上述加密通信用的密钥进行加密通信（步骤 1314）。

[0096] 如果不要加密通信信道，则终端 30 和管理服务器 10 按照图 6 所示的顺序结束连接。在结束上述加密通信时，首先，对管理服务器通信单元 305 将结束与管理服务器 10 的通信的请求，发送给管理服务器 10（步骤 1316）。

[0097] 对终端通信单元 108 接收该请求（步骤 1318）。

[0098] 对终端通信单元 108 将结束通信的许可和结束通信的许可请求发送给终端 30（步骤 1320），对管理服务器通信单元 305 接收它们（步骤 1322）。

[0099] 对管理服务器通信单元 305 将结束通信的许可发送给管理服务器 10（步骤 1324），对终端通信单元 108 接收该许可（步骤 1326）。

[0100] 通过以上的处理，由于终端 30 和管理服务器 10 互相发出结束通信的许可，因此结束连接（步骤 1328）。

[0101] 如上所述，通过图 2 到图 6 的动作，终端 30 和管理服务器 10 能够互相认证，能够建立终端 30 与管理服务器 10 之间的加密通信信道，进行加密通信，能够结束通信。

[0102] 在本实施形态中，管理服务器 10 为了严密地认证终端 30，通过图 3 所示的处理请求验证服务器 20 验证公开密钥证书 310。

[0103] 而且，终端 30 为了严密地认证管理服务器 10，也请求验证服务器 20 验证公开密钥证书 110。通过进行图 3 的替换终端 30 和管理服务器 10 的处理取代步骤 1028 和步骤 1030 所示的处理，终端 30 能够请求验证服务器 20 验证公开密钥证书 110。

[0104] 在图 7 所示的流程中，终端 30 用通过图 2 到图 5 的动作顺序建立的加密通信信道，将地址和用于与其他的终端进行加密通信的设定信息登录到管理服务器 10 中。

[0105] 首先，终端 30 和管理服务器 10 通过上述步骤 1000 到步骤 1030，步骤 1100 到步骤 1114，步骤 1200 到步骤 1218 以及步骤 1300 到步骤 1312 建立上述加密通信的信道（合并地描述为步骤 2000）。

[0106] 接着，终端 30 的地址登录申请单元 302 和设定信息登录申请单元 301 请求管理服务器 10，采用对管理服务器通信单元 305，登录终端 30 的地址和用于与其他的终端进行加密通信的设定信息（步骤 2002）。步骤 2002 发送 1 个以上的登录设定信息的请求。在设定信息中包含例如加密通信数据时使用的加密算法的种类、密钥的长度和用于检测通信数据是否篡改了的散列函数的种类等。

[0107] 对终端通信单元 108 接收该地址和加密通信用的设定信息（步骤 2004）。

[0108] 管理服务器 10 的地址登录单元 106，用图 1 的地址登录单元 106 将接收到的该地址登录道地址 DB112 中（步骤 2006）。后面详细叙述。

[0109] 设定信息登录单元 103 将接收到的该设定信息登录道设定信息 DB111 中（步骤 2008）。

[0110] 为了将登录了该地址和该设定信息的情况通知终端 30，管理服务器 10 采用对终端通信单元 108，将登录完了的通知发送给终端 30（步骤 2010），对管理服务器通信单元 305 接收该通知（步骤 2012）。

[0111] 终端 30 和管理服务器 10 通过上述步骤 1316 到步骤 1326，结束连接（合并地描述为 2014）。

[0112] 通过进行上述图 7 的处理，终端 30 能够将自身的地址和用于与其他的终端进行加密通信的设定信息登录到管理服务器 10 中。

[0113] 通过进行与图 7 相同的处理，终端 40 也可以用地址登录申请单元 402 和设定信息登录申请单元 401 将终端 40 的地址和用于与其他的终端进行加密通信的设定信息登录到管理服务器 10 中。

[0114] 在终端 40 登录时，终端 40 和管理服务器 10 进行将图 7 的终端 30 替换成终端 40 的流程。

[0115] 另外，终端 30 和终端 40 也可以删除登录到管理服务器 10 中的地址或设定信息。在删除时，进行将图 7 的“登录”替换成“删除”的处理。

[0116] 在图 7 的处理中，终端 30、40 将终端自身分配到的地址登录到管理服务器 10 中。在终端自身分配到的地址改变时，为了登录新的地址，终端 30、40 有必要再次进行图 7 的处理。

[0117] 例如，在地址为 IP 地址，终端自动地接受 IP 地址分配的情况下，如果开关终端的电源或者复位终端，则 IP 地址有可能改变。并且，在终端结束与网络的连接、移动到别处与别的网络连接时，IP 地址也可能改变。在终端具有改变 IP 地址的可能性的情况下，通过进行图 7 的处理，将最新的 IP 地址登录到管理服务器中。

[0118] 当终端 30 和终端 40 按图 7 的顺序将在网络上的位置（IP 地址）和与其他的终端之间进行加密通信用的设定信息登录到管理服务器 10 中时，终端 30 按图 8 和图 9 的流程进行通过管理服务器 10 与终端 40 连接的处理。

[0119] 终端 30 和管理服务器 10 通过上述步骤 1000 到步骤 1030、步骤 1100 到步骤 1114、步骤 1200 到步骤 1218 以及步骤 1300 到步骤 1312 建立加密通信信道（合并地描述为步骤 2100）。

[0120] 终端 30 的密钥 / 设定信息接收单元 303 通过对管理服务器通信单元 305，将与终端 40 的连接请求发送给管理服务器 10（步骤 2102），对终端通信单元 108 接收该请求（步骤 2104）。连接请求中包含确定连接对象（终端 40）的 ID 之类的信息（以下称为终端 ID）。终端 ID 在域内使用固定的就可以了。例如可以使用终端名、终端的 MAC 地址。并且，在公司内部之类的封闭的域内，也可以使用终端的使用者的 E-mail 地址、终端的 SIP-URI 或终端的 FQDN（全限定域名，Fully QualifiedDomain Name）之类的信息。

[0121] 管理服务器 10 为了获取作为终端 30 的连接目的地的终端 40 的地址，通过图 1 的地址搜索单元 107 以终端 ID 为口令搜索图 1 的地址 DB112（步骤 2106）。

[0122] 管理服务器 10 搜索图 1 的设定信息 DB111，获取终端 30 和终端 40 的设定信息的候补。并且通过图 1 的设定信息搜索单元 104 从获得的设定信息中搜索一致的设定信息（步骤 2108）。

[0123] 如果终端 30 的设定信息与终端 40 的设定信息有一个以上一致（步骤 2110 为 YES），则管理服务器 10 通过步骤 1000 到步骤 1030、步骤 1100 到步骤 1114、步骤 1200 到步骤 1218 以及步骤 1300 到步骤 1312 建立与终端 40 之间的加密通信信道（合并地描述为步骤 2112）。

[0124] 但是，为了建立管理服务器 10 与终端 40 之间的加密通信信道，进行将图 2、图 4 和图 5 的终端 30 替换成管理服务器 10，将管理服务器 10 替换成终端 40 的处理，管理服务器 10 和终端 40 分别具有这些处理所必须的上述功能。

[0125] 而且，由于在步骤 2112 中管理服务器 10 请求验证服务器 20 验证终端 40 的公开

密钥证书，因此管理服务器 10 从图 2 的步骤 1026 进入图 3 的 C，从图 3 的 D 进入图 4 的 B，终端 40 从图 2 的 C 进入图 4 的 D。

[0126] 如果在步骤 2110 中设定信息不一致，则进入图 6 的 A，将由于设定信息不一致而不能连接的意思记载在图 6 的处理中的信息中并通知终端 30，结束终端 30 与管理服务器 10 的连接。但是，图 6 表示终端 30 请求结束通信时的情况，当从步骤 2110 进入时，由于管理服务器 10 已发出了结束通信的请求，因此替换为终端 30 和管理服务器 10 的动作。

[0127] 在步骤 2112 之后，对终端通信单元 108 用建立的加密通信，将在步骤 2104 中接收到的、终端 30 与终端 40 的连接请求发送给终端 40（步骤 2114），与管理服务器进行通信的单元 405 接收这些请求（步骤 2116）。

[0128] 终端 40 根据现在能否通信之类的终端自身或其使用者的状态或者终端 40 独自的策略进行的过滤功能，判断是许可还是拒绝接收到的连接请求（步骤 2118）。

[0129] 与管理服务器进行通信的单元 405 将上述判断结果发送给管理服务器 10（步骤 2120），对终端通信单元 108 接收这些结果（步骤 2122）。

[0130] 对终端通信单元 108 将接收到的判断结果传输给终端 30（步骤 2124），对管理服务器通信单元 305 接收这些结果（步骤 2126）。

[0131] 通过以上的处理，能够达成在终端 30 与终端 40 之间能否用在终端 30 与管理服务器 10 之间、管理服务器 10 与终端 40 之间建立的加密通信信道连接的协议。

[0132] 接着，管理服务器 10 按照图 9 所示的流程，根据在图 8 的步骤 2108 中搜索到的一致的设定信息生成终端 30 与终端 40 之间进行加密通信用的密钥，将该加密通信用的密钥和设定信息分配给终端 30 和终端 40。终端 30 和终端 40 用分配到的密钥和设定信息建立加密通信信道。

[0133] 终端 30、管理服务器 10 和终端 40 判断在步骤 2118 中判断的能否连接的结果（步骤 2128、步骤 2130 和步骤 2132）。为了在步骤 2128、步骤 2130 和步骤 2132 的判定中反映步骤 2118 的判断结果，所有的结果相同，同时为 YES 或 NO。

[0134] 在判定结果为 NO 的情况下，终端 30、管理服务器 10 和终端 40 结束处理。

[0135] 在判定结果为 YES 的情况下，管理服务器 10 的密钥生成单元 102 根据在步骤 2108 中搜索到的一致的设定信息，生成终端 30 与终端 40 之间进行加密通信用的密钥（步骤 2134）。另外，在步骤 2134 中也可以生成该加密通信用的密钥的种子信息取代该加密通信用的密钥。

[0136] 管理服务器 10 用密钥 / 设定信息分配单元 105，将在步骤 2134 中生成的密钥或密钥的种子信息和在步骤 2108 中搜索到的一致的设定信息发送给终端 30 和终端 40（步骤 2138），终端 30 和终端 40 用密钥 / 设定信息接收单元 303、403 接收这些信息（步骤 2136、步骤 2140）。

[0137] 终端 30 和终端 40 的对终端通信单元 304、404，用接收到的终端 30 与终端 40 之间进行加密通信用的密钥和设定信息建立加密通信信道（步骤 2142）。

[0138] 另外，在管理服务器 10 在步骤 2134 中生成终端 30 与终端 40 之间进行加密通信用的密钥的种子信息，在步骤 2138 中分配的情况下，密钥 / 设定信息接收单元 303、403 用分配到的该加密通信用的密钥的种子信息生成该加密通信用的密钥，对终端通信单元 304、404 用生成的密钥和接收到的设定信息建立加密通信信道。

[0139] 终端 30 和终端 40 通过对终端通信单元 304、404 用建立的上述加密通信信道进行加密通信（步骤 2144）。

[0140] 通过以上的处理，管理服务器 10 将终端 30 与终端 40 之间进行加密通信所必需的密钥或密钥的种子信息以及设定信息分配给终端 30 和终端 40，终端 30 和终端 40 进行加密通信。

[0141] 当加密通信（步骤 2144）结束时，终端 30 和终端 40 按照图 10 所示的流程结束通信。

[0142] 对管理服务器通信单元 305 将结束请求发送给管理服务器 10（步骤 2146），对终端通信单元 108 接收这些请求（步骤 2148）。

[0143] 对终端通信单元 108 将接收到的结束请求传输给终端 40（步骤 2150），与管理服务器进行通信的单元 405 接收该请求（步骤 2152）。

[0144] 与管理服务器进行通信的单元 405 将结束许可发送给管理服务器 10（步骤 2154），对终端通信单元 108 接收该许可（步骤 2156）。

[0145] 对终端通信单元 108 将接收到的结束许可传输给终端 30（步骤 2158），对管理服务器通信单元 305 接收该许可（步骤 2160）。

[0146] 通过图 10 的以上的处理，终端 30 和管理服务器 10 结束在图 8 的步骤 2100 中建立的终端 30 与管理服务器 10 之间的加密通信信道的连接（步骤 2162），管理服务器 10 和终端 40 结束在图 8 的步骤 2112 中建立的管理服务器 10 与终端 40 之间的加密通信信道的连接（步骤 2164）。

[0147] 并且，终端 30 和终端 40 结束在图 9 的步骤 2142 中建立的终端 30 与终端 40 之间的加密通信信道的连接（步骤 2166）。

[0148] 另外，终端 30 和终端 40 也不必为了结束通信而非要进行图 10 所示的流程不可，也可以不进行图 10 的流程而结束通信。

[0149] 在不进行图 10 的流程的情况下，由于终端 30、管理服务器 10 和终端 40 不必进行图 10 的处理，因此处理负担变小。并且，如果在步骤 2142 之前结束步骤 2100 和步骤 2112 建立的加密通信信道的话，则能够节约终端 30 与管理服务器之间的、管理服务器 10 与终端 40 之间的通信资源。

[0150] 并且，终端 30 和管理服务器 10 也可以在步骤 2136 和步骤 2138 之后结束在步骤 2100 中建立的加密通信信道，在步骤 2144 之后再次建立加密通信信道；管理服务器 10 和终端 40 也可以在步骤 2138 和步骤 2140 之后结束在步骤 2112 中建立的加密通信信道，在步骤 2144 之后再次建立加密通信信道。

[0151] 此时，在步骤 2144 中不必预先建立终端 30 与管理服务器 10 之间的或者管理服务器 10 与终端 40 之间的加密通信信道，能够节省通信资源。

[0152] 在上述图 8 的处理中，由于当在步骤 2100 中建立加密通信信道时终端 30 和管理服务器 10 互相认证，当在步骤 2112 中建立加密通信信道时管理服务器 10 和终端 40 互相认证，因此终端 30 能够通过管理服务器 10 确认终端 40 的合法性，终端 40 能够通过管理服务器 10 确认终端 30 的合法性。

[0153] 并且，由于通过进行上述图 8、9 的处理管理服务器 10 能够从终端 30 和终端 40 预先登录的，终端 30 与终端 40 之间的加密通信用设定信息中搜索一致的设定信息，并且分配

该加密通信用的密钥或密钥的种子信息以及设定信息，因此终端 30 和终端 40 能够用分配到的密钥和设定信息进行加密通信。

[0154] 在本实施形态中，当管理服务器 10 附加了处理终端 30、40 的使用者个人信息的功能时，为了防止泄露终端 30、40 发送给管理服务器 10 的使用者的个人信息，通过进行图 7 的步骤 2000，具体为进行图 2 到图 6 的处理来建立加密通信信道，但在管理服务器 10 不处理个人信息的情况下，也可以不加密通信信道。在没有加密通信信道的情况下，在图 2、图 3、图 4、图 5 和图 6 的建立加密通信信道的步骤中省略图 4 的步骤 1216 和步骤 1218，在图 5 的步骤 1314 中不加密通信。

[0155] 下面详细叙述以上描述的流程的一部分。

[0156] 在图 7 的步骤 2006 中将终端 30 的地址登录道图 1 的地址 DB112 中。图 12 的表 700 表示了地址 DB112 的示例。

[0157] 下面说明地址 DB112 的登录和检索。

[0158] 终端 30 的地址登录申请单元 302 在图 2 的步骤 2002 的发送登录请求步骤中将地址发送给管理服务器 10。

[0159] 管理服务器 10 的地址登录单元 106 在步骤 2006 中将在步骤 2004 中接收到的终端 30 的地址登录到地址 DB112 中。

[0160] 地址 DB112 可以像例如图 12 所示的表 700 那样地构成。表 700 保管管理服务器 10 在步骤 2104 中接收的连接请求中所包含的、确定终端的信息（终端 ID）和地址对。

[0161] 在表 700 的示例中，登记项 702 和登记项 704 中分别保管着终端 30 和终端 40 的终端 ID 和 IP 地址。并且，每 1 个终端保管 1 个登记项。在表 700 的示例中描述的信息已经登录到地址 DB112 内的情况下，当终端再次进行 IP 地址的登录时，地址登录单元 106 通过步骤 2006 更新与该终端有关的登记项的 IP 地址。

[0162] 并且，管理服务器 10 的地址搜索单元 107 在图 8 的步骤 2106 中检索终端 30 的连接请求目的地即终端 40 的地址。

[0163] 在步骤 2106 中，参照图 12 的登记项 704 获取终端 40 的 IP 地址信息。

[0164] 在图 7 的步骤 2008 中，将终端 30、40 与其他的终端进行加密通信时可以利用的、1 个以上的该加密通信用的设定信息登录到图 1 的设定信息 DB111 中，在图 8 的步骤 2108 中，参照设定信息 DB111 从设定信息中搜索一致的设定信息。

[0165] 下面叙述设定信息 DB111 的登录和对 DB111 搜索一致的设定信息时的情况。

[0166] 终端的设定信息登录申请单元 301 在步骤 2002 的发送设定信息登录请求步骤中，将与其他的终端进行加密通信用的设定信息的候补发送给 1 个以上的管理服务器 10。另外，在登录 2 个以上的设定信息时，将优先顺序付与设定信息的候补并发送。

[0167] 管理服务器 10 的设定信息登录单元 103 在步骤 2008 中将在步骤 2004 中接收到的、终端的上述加密通信用的设定信息的候补登录到设定信息 DB111 中。

[0168] 设定信息 DB111 可以像例如图 13 的终端 30 的设定信息表 800 和终端 40 的设定信息表 810 那样，用每个终端的表构成。

[0169] 在表 800 的示例中，登记项 802、登录项 804 和登录项 806 保管终端 30 的设定信息的候补和优先顺序对。

[0170] 在表 800 所示的信息已经登录在设定信息 DB111 中的情况下，如果终端再次进行

设定信息的候补的登录，则管理服务器 10 的设定信息登录单元 103 通过步骤 2008 更新与该终端有关的表。

[0171] 并且，管理服务器 10 的设定信息搜索单元 104 在图 8 的步骤 2108 中从终端 30 与终端 40 的加密通信用设定信息中搜索一致的设定信息。

[0172] 在步骤 2108 中，参照图 13 的表 800 和表 810 从设定信息中搜索一致的设定信息。

[0173] 首先，从表 800 和表 810 的登录项中抽出设定信息的内容一致的登录项。在图 13 的示例中，抽出登录项 802 和登录项 814，登录项 804 和登录项 812。

[0174] 在没有设定信息一致的登录项的情况下，搜索失败。

[0175] 在表 800 和表 810 的各设定信息的登录项中记载有在步骤 2002 中发送的信息（设定值）。在步骤 2108 中，抽出登录项中记载的所有设定值一致的登录项。例如，在 1 个登录项内记载有加密通信数据时使用的加密算法的种类、密钥的长度以及检测通信数据是否篡改了时使用的散列函数的种类的情况下，在步骤 2108 中抽出 3 个设定值完全一致的登录项。

[0176] 登录项内记载的设定值也可以记载例如加密算法 :算法 A，密钥的长度 :64 比特以上，散列函数 :函数 A 或函数 B 这样的可以调节的设定值。此时，如果在步骤 2108 中与加密算法 :算法 A，密钥的长度 :128 比特以上，散列函数 :函数 B 或函数 C 的设定信息相比较，虽然两者不完全相同，但由于各可以设定的范围重叠，因此可以使例如加密算法 :算法 A，密钥的长度 :128 比特，散列函数 :函数 B 为一致的登录项。

[0177] 在多个项目的可以设定的范围重叠的情况下，可以根据预先确定的设定项目之间的优先度决定设定值。

[0178] 在有多个一致的登录项的情况下，根据使接收连接请求的终端优先于发出连接请求的终端这样的预先确定的终端的优先顺序，选择一组设定信息。

[0179] 在图 13 的示例中，在预先决定接收连接请求的终端 40 优先于发出连接请求的终端 30 的情况下，管理服务器 10 参照一致的登录项中的终端 40 的优先顺序（登录项 812 的优先顺序为 1，登录项 814 的优先顺序为 2）选择优先顺序高的设定 B，步骤 2108 的设定信息的搜索成功。

[0180] 并且，管理服务器可以根据预定的选择基准从一致的登录项中选择一组设定信息。

[0181] 此时，设定信息 DB（表 800 或表 810）中没有优先顺序栏也可以。终端将 1 个以上的设定信息登录到设定信息 DB111 中，管理服务器 10 从设定信息中搜索一致的设定信息，根据预定的选择基准选择一组设定信息。

[0182] 在例如追求高保密性的通信中，可以将加密算法的密码强度作为选择基准或将加密通信数据时使用的密钥的长度作为选择基准。并且，在追求通信性能时，也可以将加密算法的加密处理的简便程度或用于检测篡改的散列函数的计算处理的简便程度作为选择基准。

[0183] 虽然在本实施形态中以指定了终端 ID 的通信作为示例，但也可以将利用终端的使用者作为通信对象指定。

[0184] 在将利用终端的使用者作为通信对象指定时，可以预先将使用者拥有的公开密钥证书和用户 ID 输入可移动的记忆媒体 68 中，通过将记忆媒体 68 插入终端的读取装置 67

中，将使用者的属性反映在终端上。

[0185] 当使用者将可移动的记忆媒体 68 从读取装置 67 上拔下时，使用者的属性不反映在终端上。

[0186] 在使用者的属性反映到终端上的同时进行图 7 的处理，将用户 ID 和终端的地址登录到管理服务器 10 中；如果在不反映的同时进行将图 7 的“登录”替换成“删除”的处理的话，在与其他的终端连接时，能够判断使用者是否正在使用终端，如果使用者正在使用终端，则不必在意使用者正在使用哪个终端就能连接。

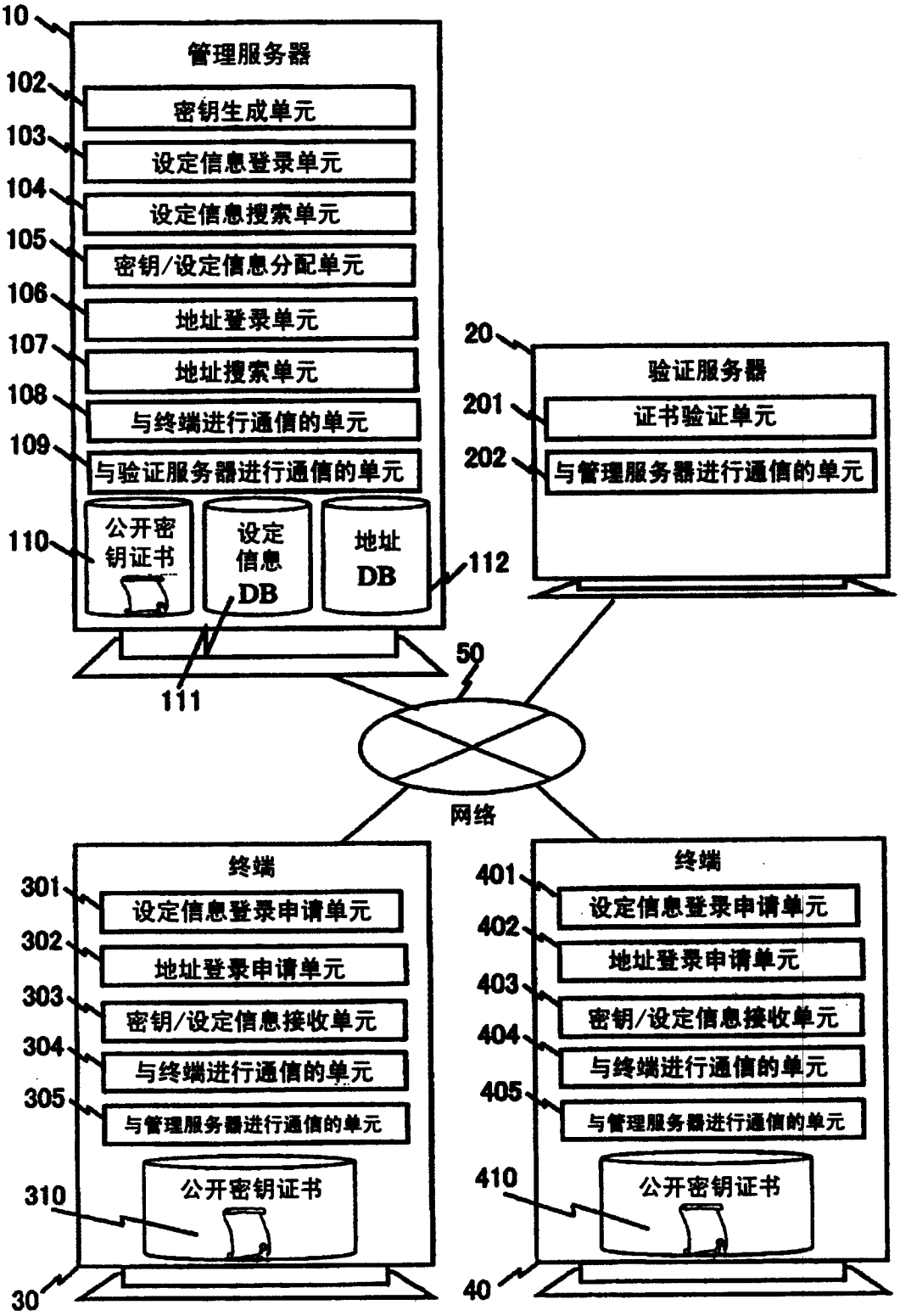

10
管理服务器
102
密钥生成单元
103
设定信息登录单元
104
设定信息搜索单元
105
密钥/设定信息分配单元
106
地址登录单元
107
地址搜索单元
108
与终端进行通信的单元
109
与验证服务器进行通信的单元
公开密钥证书
设定信息DB
地址DB
110
112
111
20
验证服务器
201
证书验证单元
202
与管理服务器进行通信的单元
50
网络
终端
301
设定信息登录申请单元
302
地址登录申请单元
303
密钥/设定信息接收单元
304
与终端进行通信的单元
305
与管理服务器进行通信的单元
公开密钥证书
310
30
终端
401
设定信息登录申请单元
402
地址登录申请单元
403
密钥/设定信息接收单元
404
与终端进行通信的单元
405
与管理服务器进行通信的单元
公开密钥证书
410
40

图1

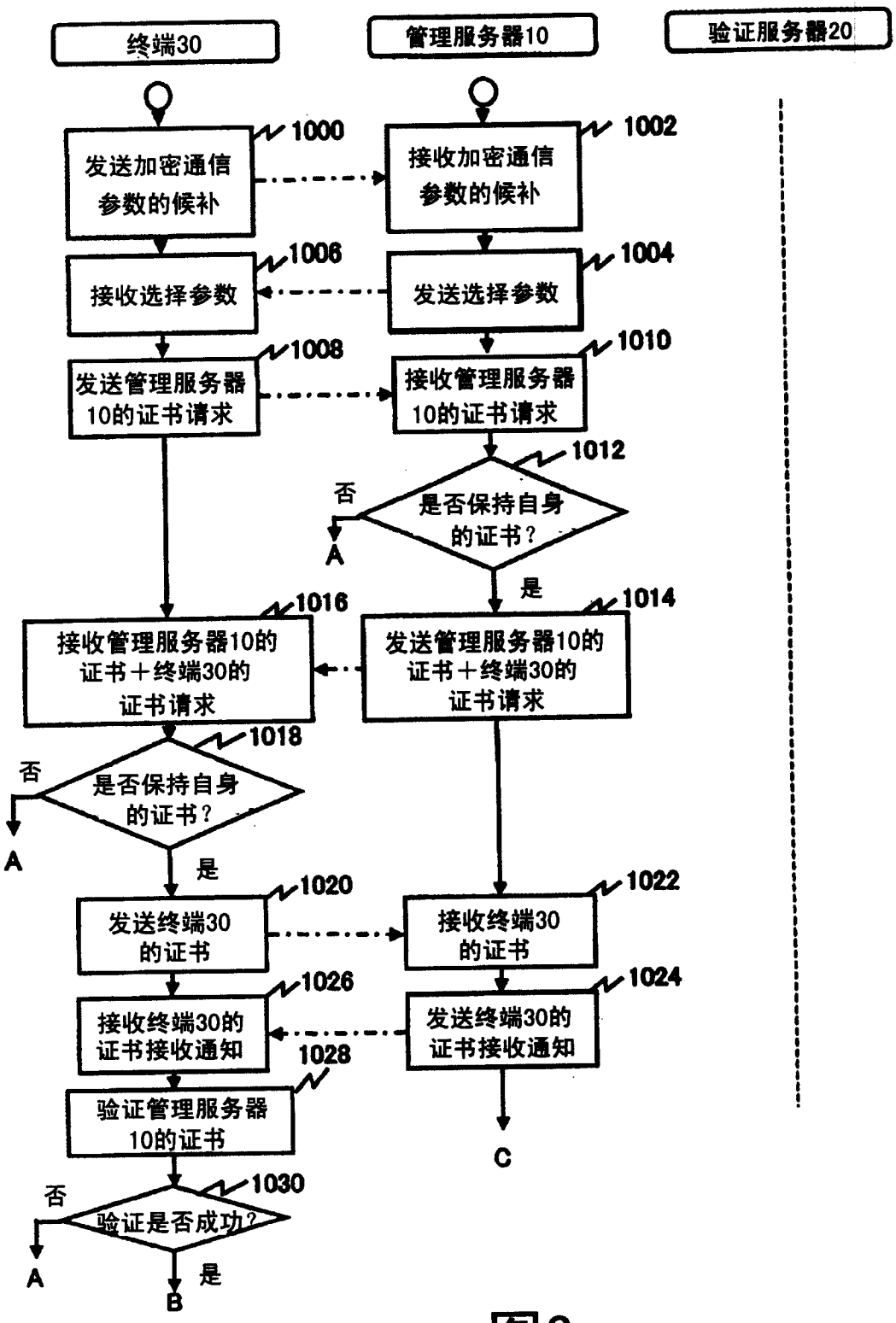

终端30
管理服务器10
验证服务器20
发送加密通信参数的候补
1000
接收加密通信参数的候补
1002
接收选择参数
1006
发送选择参数
1004
发送管理服务器10的证书请求
1008
接收管理服务器10的证书请求
1010
是否保持自身的证书？
1012
否
A
是
接收管理服务器10的证书＋终端30的证书请求
1016
发送管理服务器10的证书＋终端30的证书请求
1014
是否保持自身的证书？
1018
否
A
是
发送终端30的证书
1020
接收终端30的证书
1022
接收终端30的证书接收通知
1026
发送终端30的证书接收通知
1024
验证管理服务器10的证书
1028
C
验证是否成功？
1030
否
A
是
B

图2

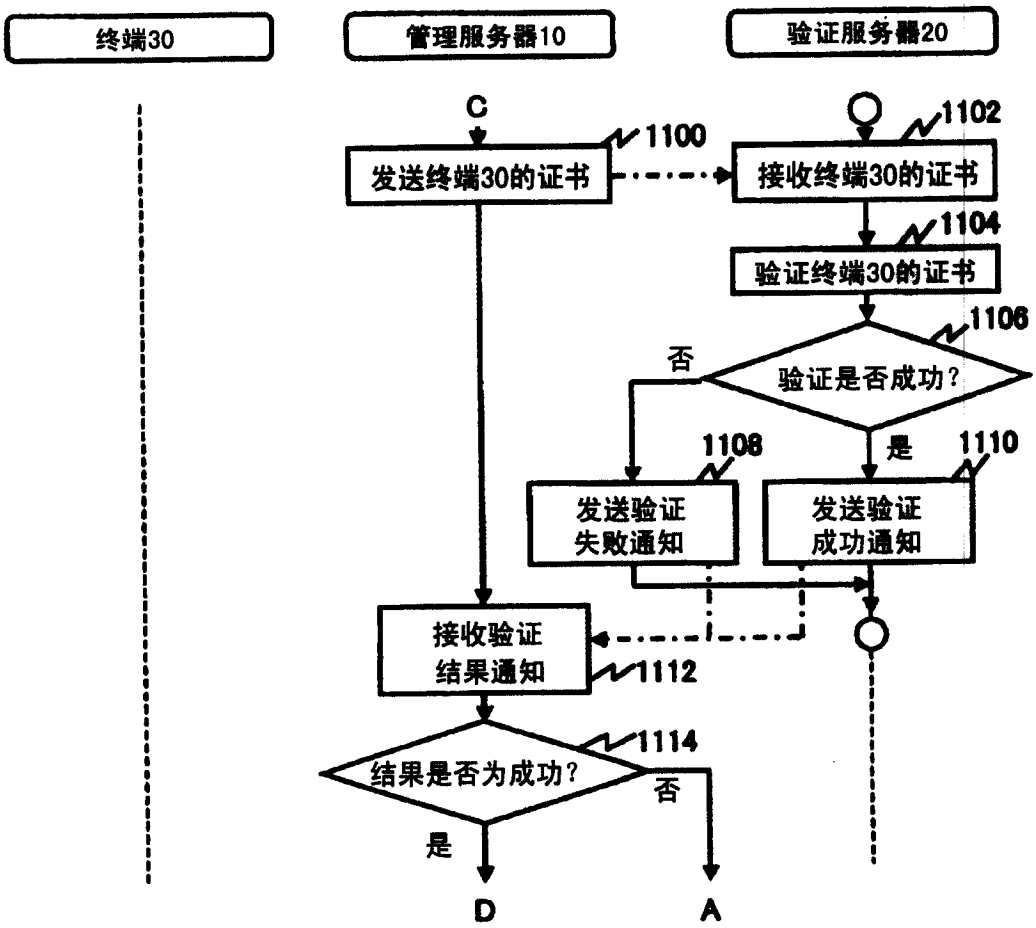

终端30
管理服务器10
验证服务器20
C
1100
发送终端30的证书
1102
接收终端30的证书
1104
验证终端30的证书
1106
验证是否成功?
否
是
1108
发送验证失败通知
1110
发送验证成功通知
接收验证结果通知
1112
1114
结果是否为成功?
否
是
D
A

图3

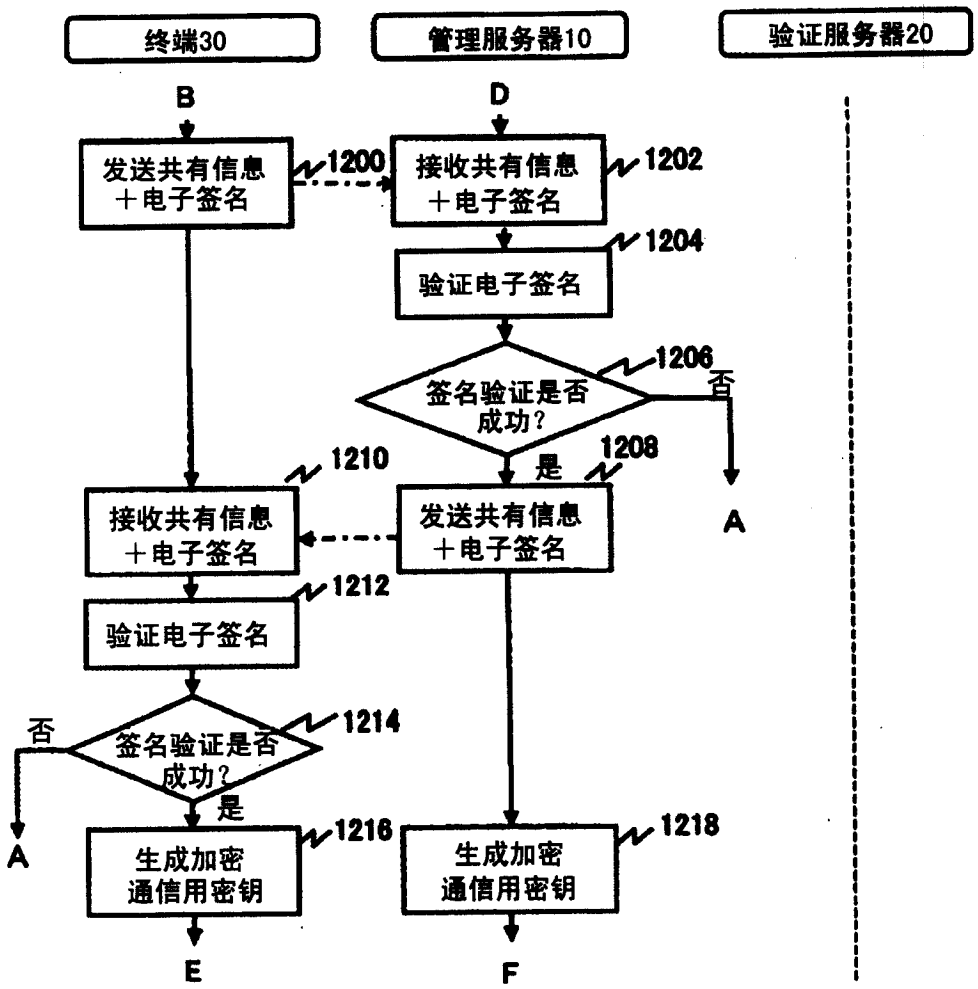

终端30
管理服务器10
验证服务器20
B
D
发送共有信息
＋电子签名
1200
接收共有信息
＋电子签名
1202
验证电子签名
1204
签名验证是否
成功?
1206
否
是
1208
A
接收共有信息
＋电子签名
1210
发送共有信息
＋电子签名
验证电子签名
1212
否
签名验证是否
成功?
1214
是
A
生成加密
通信用密钥
1216
生成加密
通信用密钥
1218
E
F

图4

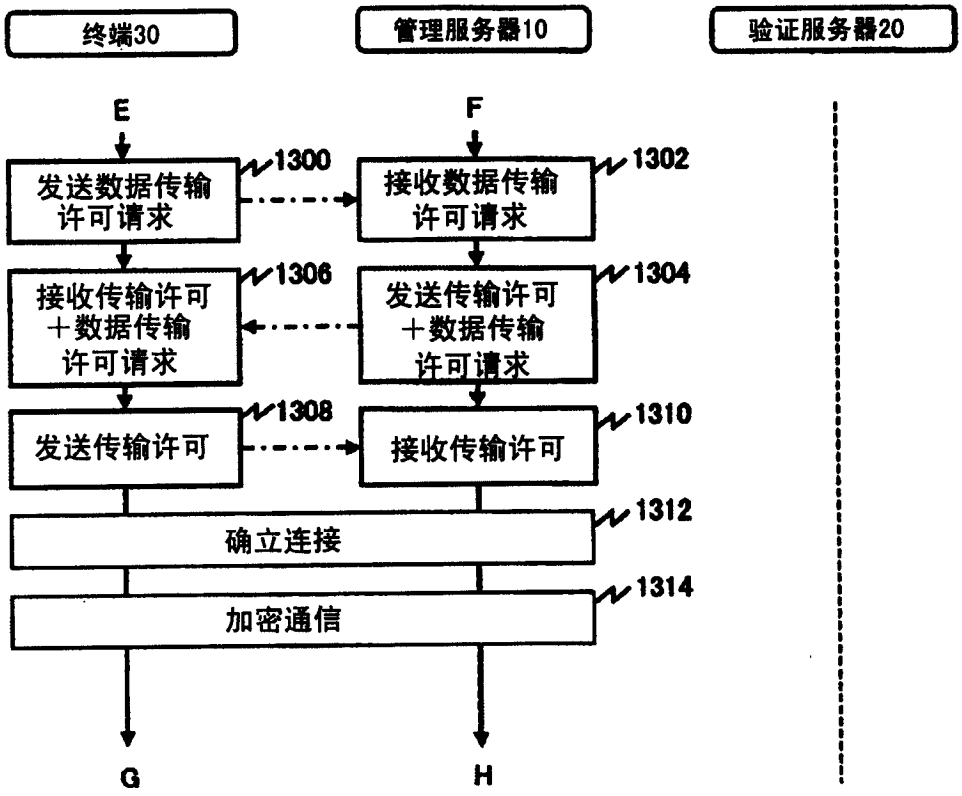

终端30
管理服务器10
验证服务器20
E
F
发送数据传输许可请求
1300
接收数据传输许可请求
1302
接收传输许可+数据传输许可请求
1306
发送传输许可+数据传输许可请求
1304
发送传输许可
1308
接收传输许可
1310
确立连接
1312
加密通信
1314
G
H

图5

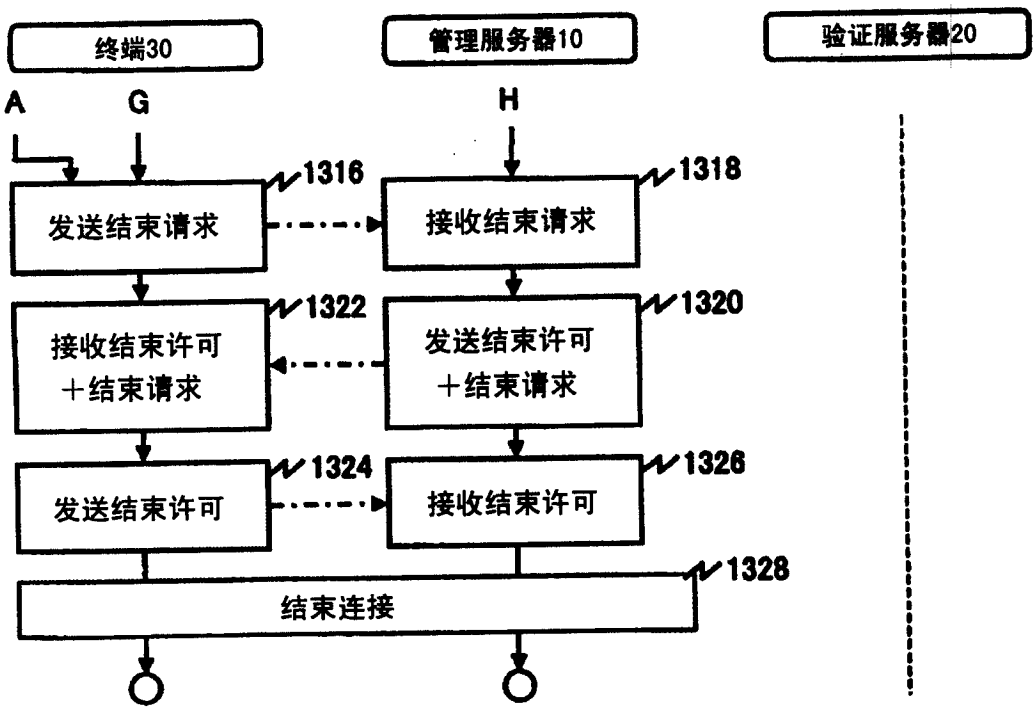

终端30
管理服务器10
验证服务器20
A
G
H
1316
发送结束请求
1318
接收结束请求
1322
接收结束许可
＋结束请求
1320
发送结束许可
＋结束请求
1324
发送结束许可
1326
接收结束许可
1328
结束连接

图6

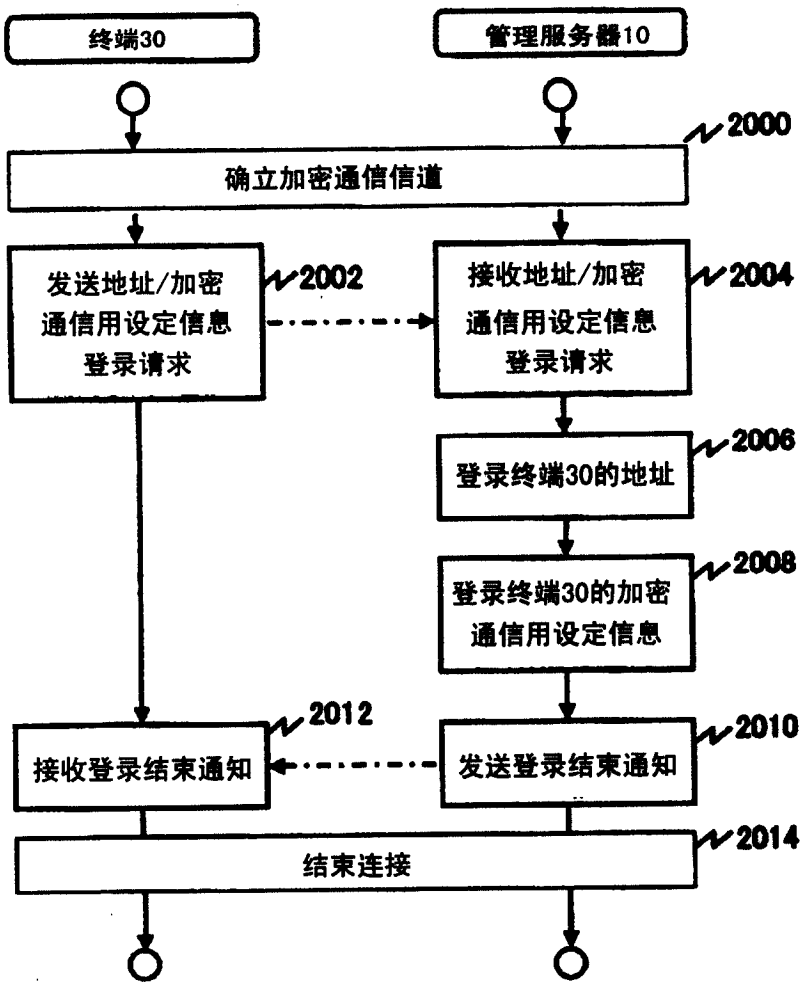

终端30
管理服务器10
2000
确立加密通信信道
发送地址/加密通信用设定信息登录请求
2002
接收地址/加密通信用设定信息登录请求
2004
登录终端30的地址
2006
登录终端30的加密通信用设定信息
2008
接收登录结束通知
2012
发送登录结束通知
2010
结束连接
2014

图7

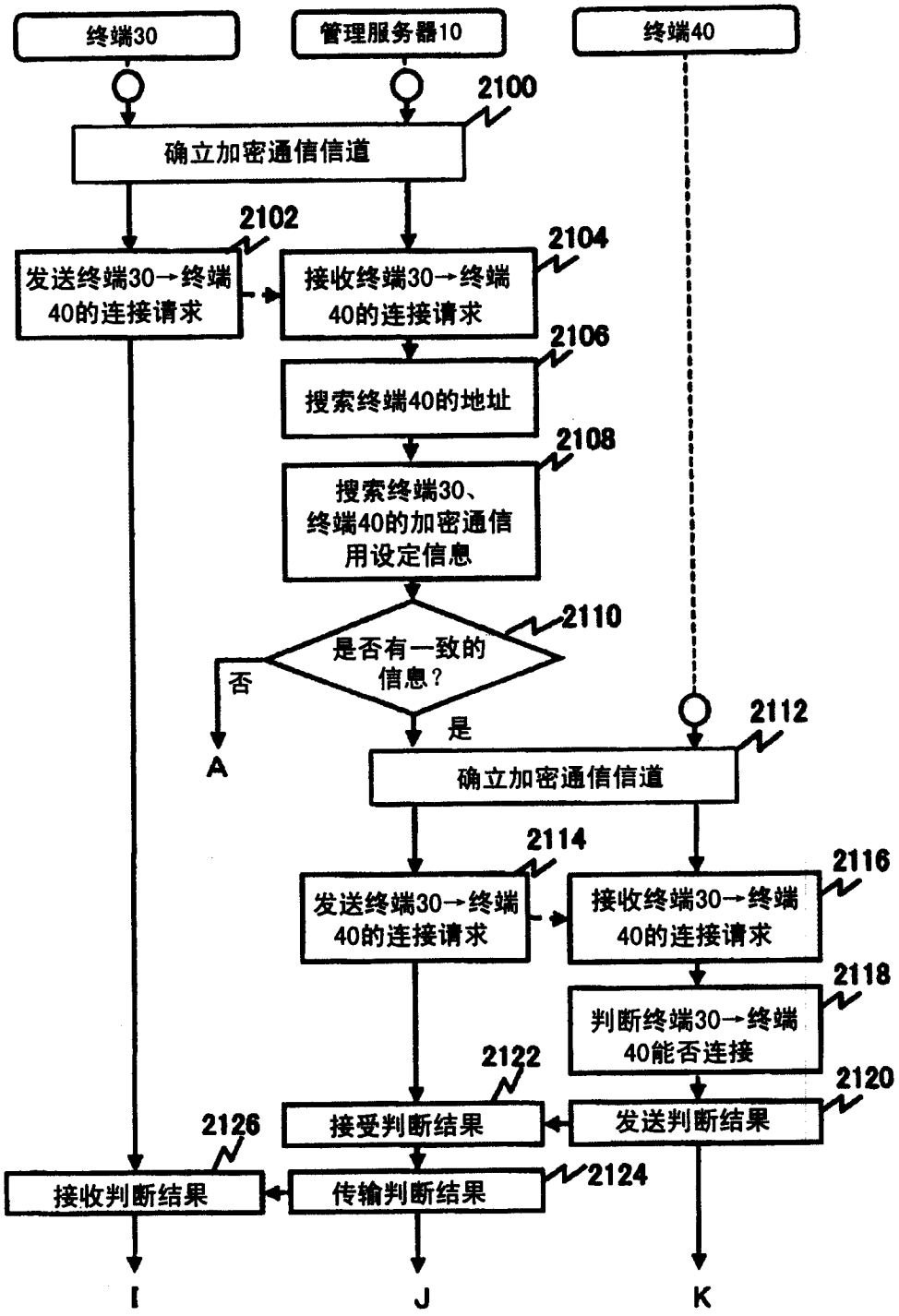

终端30
管理服务器10
终端40
2100
确立加密通信信道
2102
发送终端30→终端40的连接请求
2104
接收终端30→终端40的连接请求
2106
搜索终端40的地址
2108
搜索终端30、终端40的加密通信用设定信息
2110
是否有一致的信息？
否
是
A
2112
确立加密通信信道
2114
发送终端30→终端40的连接请求
2116
接收终端30→终端40的连接请求
2118
判断终端30→终端40能否连接
2120
发送判断结果
2122
接受判断结果
2124
传输判断结果
2126
接收判断结果
I
J
K

图8

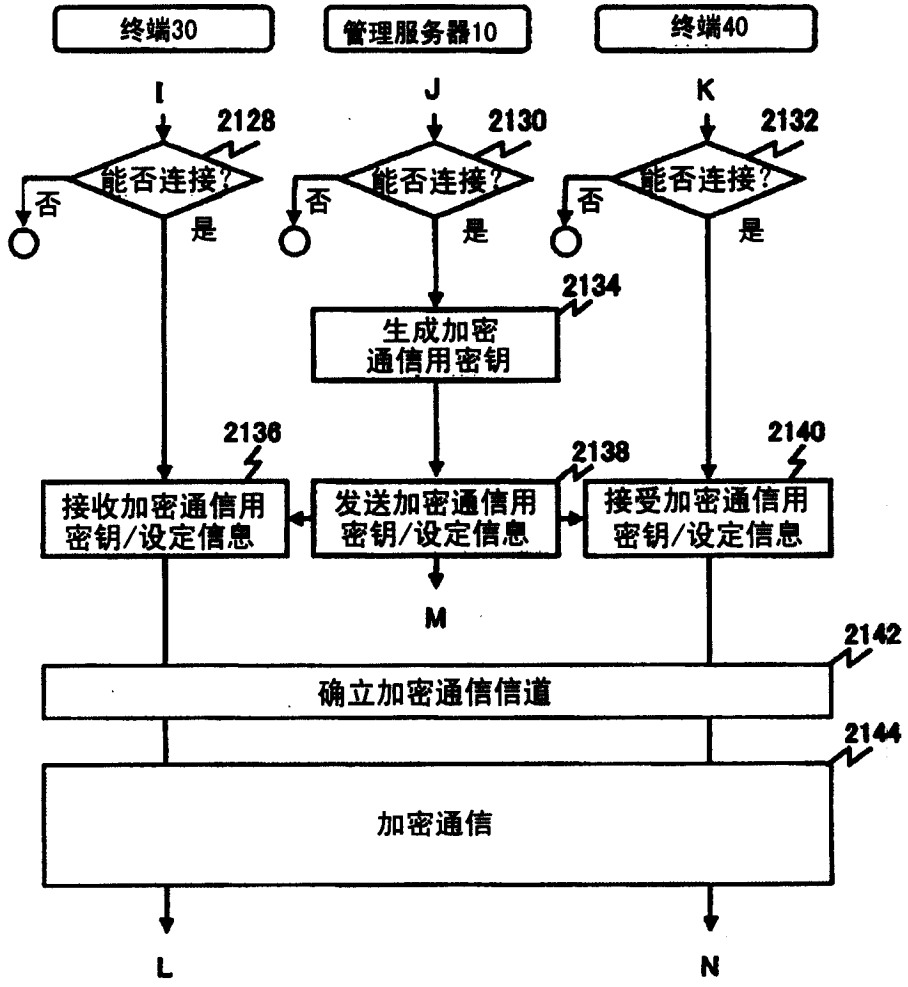

终端30
管理服务器10
终端40
I
J
K
2128
2130
2132
能否连接?
否
是
2134
生成加密通信用密钥
2136
2138
2140
接收加密通信用密钥/设定信息
发送加密通信用密钥/设定信息
接受加密通信用密钥/设定信息
M
2142
确立加密通信信道
2144
加密通信
L
N

图9

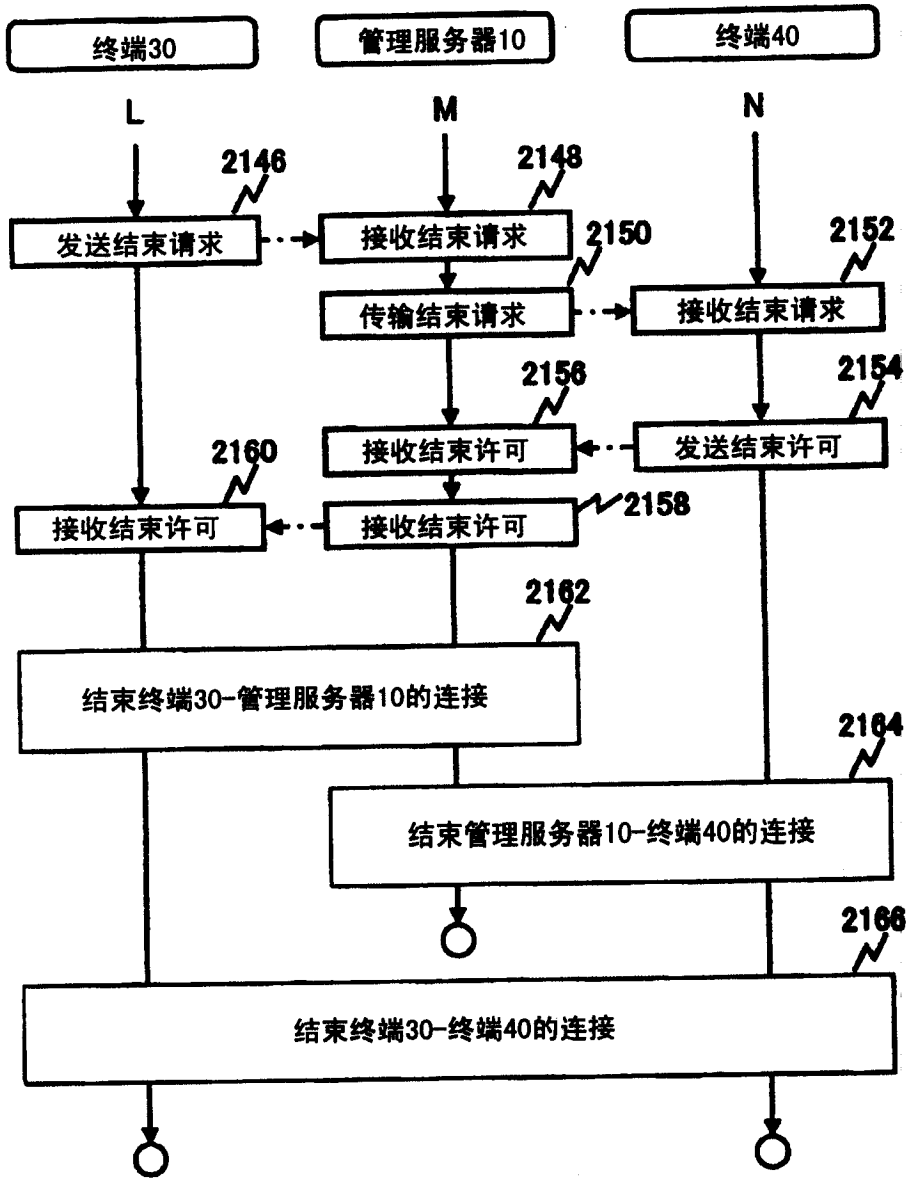

终端30
管理服务器10
终端40
L
M
N
2146
2148
2150
2152
2154
2156
2158
2160
2162
2164
2166
发送结束请求
接收结束请求
传输结束请求
接收结束请求
发送结束许可
接收结束许可
接收结束许可
结束终端30-管理服务器10的连接
结束管理服务器10-终端40的连接
结束终端30-终端40的连接

图10

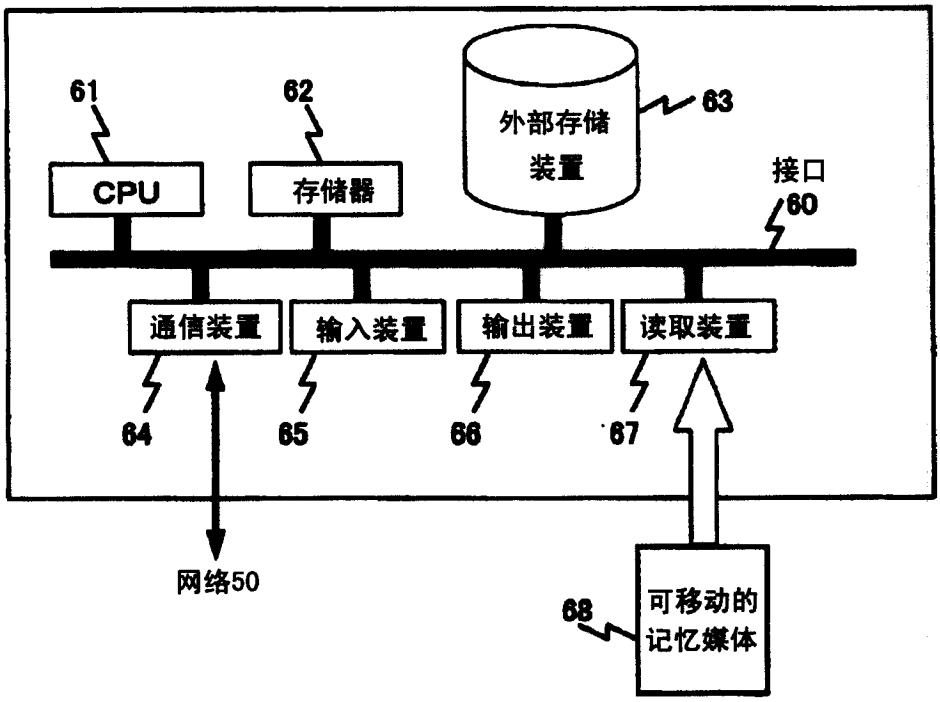


图11

地址DB112的示例

终端名	IP地址	700
终端30	10.0.0.1	702
终端40	10.1.0.1	704
…	…	

图12

设定信息DB111的示例

终端30的设定信息

设定信息	优先顺序	
设定A	1	802
设定B	2	804
设定C	3	806

800

终端40的设定信息

设定信息	优先顺序	
设定B	1	812
设定A	2	814

810

图13