



[12] 发 明 专 利 说 明 书

[21] ZL 专利号 00103048.5

[45] 授权公告日 2005 年 7 月 6 日

[11] 授权公告号 CN 1209718C

[22] 申请日 2000.2.22 [21] 申请号 00103048.5

[30] 优先权

[32] 1999. 2. 23 [33] US [31] 09/256,432

[71] 专利权人 视听. com 联合公司

地址 美国宾夕法尼亚

[72] 发明人 阿瑟·R·海尔

审查员 袁丽颖

[74] 专利代理机构 永新专利商标代理有限公司

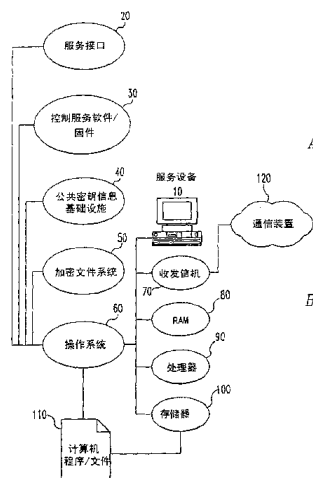
代理人 韩 宏

权利要求书 4 页 说明书 35 页 附图 12 页

[54] 发明名称 操纵计算机文件和/或程序的系统和
方法

[57] 摘要

操纵计算机文件和/或程序的系统和方法。该系统包括服务设备，能存取未加密的计算机文件和/或程序，并能够对未加密的计算机文件和/或程序加密；连接器，连接到服务设备，加密计算机文件和/或程序在该连接器上传播，并服务设备将加密计算机文件和/或程序传送到该连接器；客户机设备，接收加密计算机文件和/或程序，并将该加密计算机文件和/或程序解密。客户机设备在加密计算机文件和/或程序接收期内不允许干预加密计算机文件和/或程序。



1. 一种操纵计算机文件和/或程序的系统，包含：

一服务设备，该设备能够存取未加密的计算机文件和/或程序，并且能够对所述未加密的计算机文件和/或程序进行加密，以使其变成加密的计算机文件和/或程序并对其进行传送；

一连接器，连接到所述服务设备，所述加密的计算机文件和/或程序在该连接器上传播，并且所述服务设备将加密的计算机文件和/或程序传送到该连接器；和

一客户机设备，该设备接收所述加密的计算机文件和/或程序，并将该加密的计算机文件和/或程序解密回到未加密的计算机文件和/或程序，在根据与之相伴随的允许或权利接收所述加密的计算机文件和/或程序的时期内，所述客户机设备暂停存取所述加密的计算机文件和/或程序，所述服务设备与所述客户机设备分离、远离且截然不同。

2. 如权利要求1所述的系统，其中在所述客户机设备已接收所述加密的计算机文件和/或程序之后，或者在所述客户机设备已将所述加密的计算机文件和/或程序解密回到未加密的计算机文件和/或程序之后，所述服务设备将能够识别客户机设备能够如何处置未加密的或加密的计算机文件和/或程序的允许和/或权利分配给未加密的计算机文件和/或程序。

3. 如权利要求2所述的系统，其中所述服务设备对所述允许和/或权利进行加密，并将它们通过所述连接器传送给所述客户机设备，所述客户机设备对所述加密的允许和/或权利进行解密。

4. 如权利要求3所述的系统，其中所述服务设备包括控制服务器软件和/或固件，该控制服务器软件和/或固件使所述未加密的计算机文件和/或程序以及所述允许和/或权利被加密，并在所述客户机设

备接收所述加密的计算机文件和/或程序以及所述加密的允许和/或权利的时候指示所述客户机设备临时暂停用户存取。

5. 如权利要求4所述的系统, 其中所述客户机设备包括控制客户机软件和/或固件, 该控制客户机软件和/或固件使所述加密的计算机文件和/或程序被解密。

6. 如权利要求5所述的系统, 其中所述客户机设备具有向所述服务设备请求未加密的计算机文件和/或程序的机构。

7. 如权利要求6所述的系统, 其中所述控制客户机软件和/或固件使所述未加密的计算机文件和/或程序以及所述允许和/或权利被加密, 以被存储。

8. 如权利要求7所述的系统, 其中所述客户机设备具有一操作系统, 并且所述控制客户机软件和/或固件指示该操作系统在需要时重新建立用户存取。

9. 如权利要求8所述的系统, 其中所述服务设备具有一服务器公共密钥信息基础设施, 该服务器公共密钥信息基础设施利用加密通信协议对所述允许和/或权利以及所述未加密的计算机文件和/或程序进行加密。

10. 如权利要求9所述的系统, 其中所述客户机设备具有一客户机公共密钥信息基础设施, 该客户机公共密钥信息基础设施利用加密通信协议解密所述允许或权利以及从该服务设备发送的加密的计算机文件或程序。

11. 如权利要求10所述的系统, 其中所述客户机设备包括一加密文件系统, 该加密文件系统对所述未加密的计算机文件和/或程序以及所述允许和/或权利进行加密, 并允许手动选择用于加密或解密的未加密的计算机文件和/或程序。

12. 如权利要求11所述的系统, 其中所述客户机公共密钥信息基础设施具有一加密和/或解密密钥, 并且所述加密文件系统使用由

所述客户机公共密钥信息基础设施所利用的所述加密和/或解密密钥。

13. 如权利要求12所述的系统，包括通过所述连接器连接到所述客户机设备的下一个客户机设备。

14. 如权利要求13所述的系统，其中所述控制客户机软件和/或固件通过第二个连接器移动或复制所述加密的计算机文件和/或程序到所述下一个客户机设备，所述客户机设备具有一控制下一个客户机软件和/或固件，该控制下一个客户机软件和/或固件对所接收的加密的计算机文件和/或程序和所述加密的允许和/或权利进行解密，并在由所述下一个客户机设备接收所述加密的计算机文件和/或程序的时候临时暂停所述下一个客户机设备的用户存取。

15. 如权利要求14所述的系统，其中所述连接器包括一通信链路，所述服务设备包括连接到所述通信链路的一发送器，用于将所述加密的计算机文件和/或程序以及未加密的允许和/或权利传送到所述通信链路，并且所述客户机设备包括连接到所述通信链路的一接收器，该接收器从所述通信链路接收所述加密的计算机文件和/或程序以及加密的允许和/或权利。

16. 如权利要求15所述的系统，其中所述第一和第二连接器是因特网或者其它通信网络的一部分。

17. 一种操纵计算机文件和/或程序的方法，包括下列步骤：

由客户机设备端的用户暂停该客户机设备的存取；

对服务设备端的未加密的计算机文件和/或程序进行加密，以形成加密的计算机文件和/或程序；

将所述加密的计算机文件和/或程序沿着与所述客户机设备和所述服务设备连接的一连接器传送到所述客户机设备；和

由用户重新建立所述客户机设备的存取。

18. 如权利要求17所述的方法，包括在所述传送步骤之前的步

骤：对所述未加密的计算机文件和/或程序的允许和/或权利进行加密，并将加密的允许和/或权利沿所述连接器从所述服务设备传送到所述客户机设备。

19. 如权利要求18所述的方法，包括在对所述未加密的计算机文件和/或程序进行加密的步骤之前的步骤：由所述客户机设备请求所述服务设备的未加密的计算机文件和/或程序。

20. 如权利要求19所述的方法，包括在所述请求步骤之后的步骤：复制原始的未加密计算机文件和/或程序，以形成所述未加密的计算机文件和/或程序。

21. 如权利要求20所述的方法，包括在所述重新建立步骤之前的步骤：在所述客户机设备端将所述加密的计算机文件和/或程序解密回到未加密的计算机文件和/或程序。

22. 如权利要求21所述的方法，包括在所述解密步骤之后的步骤：在所述客户机设备端对所述未加密的计算机文件和/或程序以及允许和/或权利进行加密；并且将加密的计算机程序和/或文件及加密的允许和/或权利存储到所述客户机设备中。

23. 如权利要求22所述的方法，包括在所述存储步骤之后的步骤：将所述加密的计算机文件和/或程序传送到由第二连接器连接到所述客户机设备的下一个客户机设备。

操纵计算机文件和/或程序的系统和方法

技术领域

本发明涉及一种在从一个计算设备到另一个计算设备加密传送和加密存储计算机文件和/或计算机程序的过程中，自动调用一操作系统的功能体(functionality)的方法和系统。

背景技术

随着因特网在电子发行和电子商务方面的增殖，经通信装置安全传送计算机文件的重要性已经增长。随着因特网作为普遍存在的低成本网络的出现，开始了基于电子发送而进行的从计算机文件和/或计算机程序的物理传送到数字传送的根本转变。就象先前的从报纸到广播然后到电视的转变那样的技术创新，当代的中介公司被迫对付这些新媒体的出现。然而，与先前技术转变不同的是，因特网作为媒体支持所有的传统印刷、广播和电视工业这些功能体，同时也支持电子商务。当前，许多商家利用因特网，以经过因特网销售或分发它们的计算机文件和/或计算机程序，并且在多数情况下，计算机文件没有为保护免遭盗版或非法使用而被加密。此外，当前与安全传送和存储计算机文件有关的方法不能权衡计算设备操作系统的加密功能体。当前方法要求用作服务器(“服务设备”)的一个计算设备与用作客户机(“客户机设备”)的另一个计算设备进行通信，以传送要在客户机设备的应用级(例如，但不限于，Win32应用程序)解密的加密文件。客户机设备利用运行在应用级用于解密的计算机程序，该计算机程序被分配了唯一解密“密钥”。在发送处理过程中，服务设备利用客户机设备的加密“密钥”对用于存储的计算机文件进行加密。然后，加密的计算机文件经因特网发送并保存到客户机设备内或与客户机设备连接的存储器中。在对计算机文件

解密之后，解密计算机程序将解密信号发送到操作系统用于显示，或者在音频文件的情况下，通过声卡播放。解密信号在从解密应用程序发送到操作系统的过程中容易受到侵害，并且该信号可能被截取，有可能造成计算机文件的非法复制。

对于计算机文件和计算机程序加密的某些方面，微软公司于1998年出版了题为“Microsoft Windows NT version 5.0, Public Key Infrastructure(微软视窗NT版本5.0, 公共密钥信息基础设施)”的白皮书，在此以参考方式将其包含在此文中，(下文中称为“Windows 2000 PKI White Paper(视窗2000 PKI 白皮书)”），其中详细描述了Windows 2000操作系统家族(先前称为Windows NT 5.0)中的综合公共密钥信息基础设施(PKI)的加密功能体。Windows 2000 PKI白皮书在其封面陈述道：“微软Windows NT版本5.0对Windows平台引入了一种综合的公共密钥信息基础设施(PKI)。它利用并扩展了过去几年引入的基于Windows的公共密钥(PK)加密服务，提供了建立、部署和管理基于PK的应用程序的服务和管理工具的集成组。这就允许应用程序开发者适当利用Windows NT中的共享秘密安全机制或基于PK的安全机制的优势。同时，企业可获得能基于一致的工具和策略机制来管理其环境和应用程序的优势。”

此外，还着重强调了Windows 2000操作系统家族的公共密钥信息基础设施的加密功能体，在Windows PKI白皮书中陈述道：“在建立和部署用于基于万维网来有效交换信息的解决方案时，Web已迅速地变成一个关键因素。尤其是，用于商业目的的应用已急剧增长。对于许多应用，安全是一个要考虑的关键因素。特别是：服务器认证—使各个客户机确认正在与它们通信的服务器。客户机认证—允许各个服务器确认客户机的身份，并以此作为访问控制决策的基础。保密性—在客户机和服务器之间对数据加密，以防止通过公共的因特网链接使数据泄露。

安全套接层(Secure Sockets Layer, SSL)和出现的IETF标准传输层安全(Transport Layer Security, TLS)协议在满足这些需求方面起着

非常重要的作用。SSL和TLS是可以定位在其它的传输协议顶层之上的灵活的安全协议。它们依赖于基于PK的认证技术，并使用基于PK的密钥协商来为每一个客户和/或服务会话期产生唯一的加密密钥。它们大多与基于Web的应用程序和HTTP协议(称为HTTPS)有关。

在Windows平台上，由安全通道(schannel)SSPI提供者来支持SSL和TLS。微软因特网浏览器(Explorer)和因特网信息服务这两者都将安全通道用于这种功能。由于安全通道是与微软的SSPI体系结构集成在一起的，所以许多协议都可以用它来支持认证和/或加密通信。

要使用SSL和TLS协议的全部优势，要求客户机和服务器都具有由互相信任的CA签发的身份证书，允许各方间互相认证。在这种模式中，证书随同证明拥有对应的私人密钥的数据一起交换。然后，每一方都可以证实证书并利用该证书的公共密钥来核实拥有该私人密钥。然后，包含在证书中的身份信息可用于作出附加的访问控制决策。例如，客户可以确定服务器是否是他想要与其进行业务的服务器，并且服务器可以确定哪些数据可以允许客户机访问。

Windows NT 5.0 PKI把对后面的决策的支持集成为Windows NT服务器的标准特性。用户证书可以在一对一或多对一基础上与活动目录的安全主体(用户对象)进行映射。安全通道可以有利地利用此信息为客户机自动组合成安全权标，以使Windows NT ACL(访问控制列表)机制用于强制对资源的访问控制。这样做对服务是有利的，因为各种服务可以使用与曾使用的客户机认证机制(PK或Kerberos)无关的相同访问控制机制。

一旦客户机和服务器已相互认证，它们可继续协商会话密钥并开始安全地通信。SSL和TLS也经常用在不需要客户机认证的模式中。然而，由于相互认证允许使用基于Windows的访问控制机制，因而被推荐用在企事业环境中。此外，PKI大大简化了认证登记和管理，减小了客户机的负担。

微软公司于1998年9月出版了另一本题为“Windows NT Workstation 5.0 Key Benefits and Capabilities White paper (视窗NT工作站5.0密钥优点和性能白皮书)”的白皮书,在此以参考方式将其包含在此文中(“Windows 2000 Workstation White Paper(视窗2000工作站白皮书)”),在此文中,微软提供了对Windows 2000操作系统家族的加密功能的附加详细描述。Windows 2000工作站白皮书在其第30页中陈述道:“Windows NT工作站5.0提供对公共密钥安全协议的支持,该安全协议是用在比如因特网等公共网络上的一种工业标准认证协议。公共密钥的最重要的应用是用于数字签名,这能保证各个成份的认证,这些成份包括:来自发送者的E-mail(电子邮件);E-mail不能由其它用户观看或编辑;来自已知源的应用程序和驱动程序;软件在安装之后被保护免遭篡改;保证远程计算机的身份;允许安全因特网通信;允许比如对安全交易所需要的强加密。

同时,其它平台,比如运行Internet Explorer 4.0(因特网浏览器4.0)的Windows平台,也支持公共密钥的使用,Windows NT工作站5.0还能够对建立证书提供鲁棒性(robust)更好的信息基础设施,“信任(trusts)”其它系统,并提供对证书的安全存储。

Windows 2000工作站白皮书扩展了安全的虚拟专用网络服务,在其第31页中陈述道:“除当前最通用的方法即PPTP之外,Windows NT工作站5.0还支持几种新的、更安全的建立虚拟专用网络的方法,这些方法包括:L2PT(Layer 2 Tunneling Protocol,第2层隧道协议),是一种更安全的PPTP版本,用于隧道、地址分配及认证;IPSEC(IP Security Protocol,IP安全协议),是一种基于标准的协议,提供最高级的VPN安全性。利用IPSEC,实际网络层之上的任何物都可被加密。这就通过公共网络提供了端对端的专用性、集成性和认证性。IPSEC方法对于应用程序和协议来说是透明的。微软正在与各零销商紧密合作,以通过NDIS接口支持对IPSEC的硬件加速。

Windows NT工作站5.0还提供增强的网络连接对话,能使用户

容易地建立VPN(参见“简单性”部分)。”

此外，微软还在Windows 2000 PKI白皮书中讨论了Windows 2000操作系统家族内的存储加密功能，描述了驻留在Windows 2000内核中的加密文件系统(encrypting file system, EFS)。微软在Windows 2000 PKI白皮书的第21页和22页中陈述道：“Windows NT 5.0加密文件系统(EFS)支持对存储在Windows NT文件系统(NT file system, NTFS)的磁盘上的文件的透明加密和解密。用户能单独指定要加密的各文件，或者其内容要以加密形式保持的文件夹。应用程序能以与访问未加密文件同样的方式来访问一用户的加密文件。然而，它们不能解密任何其它用户的加密文件。

EFS扩展使用基于PK的技术来提供对多个用户加密文件并且支持文件恢复的机制。为做到这点，它利用了PK的能在不用事先共享秘密而支持成批加密的能力。在操作中，每个EFS用户产生一公共密钥对，并获得一个EFS证书。该证书是由Windows NT 5.0领域内的企业CA签发的，尽管EFS也将产生自签名的用于没有数据共享问题的单机数据操作中的证书。此外，Windows NT 5.0支持EFS恢复策略，其中可指定其信任的代理。这些代理产生EFS恢复公共密钥对，并且由企业CA签发EFS恢复证书。通过组策略对象(Group Policy Object)公布EFS恢复代理的证书给领域中的各客户。

在操作中，对要加密的每一个文件，EFS产生用于加密文件的随机密钥。然后，用户的EFS公共密钥用于加密此秘密的密钥并将它与此文件相关联。此外，用每一个恢复代理的EFS公共密钥来加密此秘密密钥的复制件，并且该复制件与此文件相关联。没有该秘密密钥的明文复制件存于系统之中。

当重新获得文件时，EFS利用用户的私人密钥对用用户的公共密钥加密的秘密密钥的复制件进行透明解包。然后，这将用于在文件的读和写操作过程中实时地对文件进行解密。类似地，恢复代理还可以通过利用私人密钥来取得秘密密钥而对文件进行解密。

为提供对微软的加密文件系统的安全级的附加详细描述，

Windows 2000工作站白皮书在其第28页中陈述道：“加密文件系统(EFS)对硬盘上的文件进行加密。利用随机产生的与用户的公共和/或私人密钥对无关的密钥来对每个文件加密。EFS驻留在Windows NT内核中，并利用未分页的缓冲池来存储文件加密密钥，保证它们绝不会进入对换文件中。在文件或目录基础上支持EFS。加密和解密对用户来说是透明的”。

一般认为计算功能(function)的不稳定性(例如，但不限于，造成计算系统崩溃的功能)在应用程序级比在操作系统级更大。离操作系统的内核越近的计算功能，通常越稳定。如果应用级解密程序被损害或破坏并且需要重新安装另一个解密程序，则产生一新的“解密密钥”，并且先前加密的计算机文件是相对于旧的“解密密钥”进行的加密，则不能由新安装的解密程序来解密。为避免应用级程序固有的加密和/或解密弱点，微软已采取一些措施来对在Windows 2000 PKI中的“加密和/或解密密钥”的丢失进行保护。微软在Windows 2000 PKI白皮书的第14页中陈述道：“公共密钥对和证书趋向于具有很高的价值。如果由于系统失败而丢失，则对它们进行替换会很费时，并且会造成金钱上的浪费。为对付这些问题，Windows NT 5.0 PKI通过证书维护和管理工具来支持证书和相关密钥对的备份和恢复能力”。

发明内容

本发明提供了一种新的改进的方法和系统来自动调用操作系统的公共密钥基础设施和加密文件系统的某些功能体，以便对用于在各个计算设备之间电子传送的计算机文件或计算机程序进行加密，并对用于后续存储的那些计算机文件或计算机程序进行加密，并且还限制使用允许和/或权利。本发明指示计算设备的操作系统临时暂停用户存取，直到结束加密发送和加密存储处理，用以防止未授权使用计算机文件或计算机程序复制品。本发明指示一服务设备的公共密钥信息基础设施对存储在其中或者连接到服务设备的的计算机

文件或计算机程序(以及由服务设备建立的任何伴随的允许和/或权利)进行加密以便发送,然后将所述计算机文件或计算机程序发送到客户机设备。一旦由客户机设备接收到所述计算机文件或计算机程序(以及由服务设备建立的任何伴随的允许和/或权利),则本发明自动指示客户机设备的公共密钥信息基础设施从发送信息中解密由服务设备发送的所述计算机文件或计算机程序(以及由服务设备建立的任何伴随的允许和/或权利)。然后,本发明指示客户机设备的加密文件系统根据如由服务设备建立并伴随计算机文件或计算机程序的任何允许和/或权利进行加密以便存储,并存储计算机文件或计算机程序。本发明将存储加密处理过程与发送加密处理过程分离开来,以使运行不同的操作系统的计算设备之间能使用工业标准通信协议进行加密传输,并使用不同的操作系统来执行它们的唯一的或专有的存储加密处理。此外,最广泛使用的操作系统支持因特网的加密发送标准,然而,对操作系统来说,不存在基于加密存储的标准。本发明的独特好处是,本发明采用了多种加密和/或解密处理,以对在运行不同操作系统的计算机之间的计算机文件和/或程序的加密传送和存储提供端对端方案。本发明不是对计算机文件和/或程序进行永久加密以用在一种特定的解密设备或计算机上,而是将允许和/或权利分配给计算机文件和/或程序,然后给拥有计算机文件和/或程序的操作系统分派加密功能,以强制实施允许和/或权利。以这种方式,将灵活的允许和/或权利分配给计算机文件和/或程序,所述允许和/或权利从计算机到计算机、从操作系统到操作系统都跟随着所述计算机文件和/或程序,并且在必要时以所述方式被加密或解密。

本发明还提供一种新的改进的方法和系统来激活客户机设备的公共密钥基础设施和加密文件系统的某些功能体,以便执行伴随着给定计算机文件或计算机程序的任何允许和/或权利。然后,由加密文件系统结合本发明强制实现允许和/或权利(例如,但不限于,播放、打印输出、观看、使用、复制、移动、再定位次数、使用期限、用户数目等)。例如,由客户机设备接收的计算机文件或计算机

程序可能伴随有比如由服务设备建立的允许或权利，允许客户机设备的用户将所述计算机文件或计算机程序移动到另一个计算设备(“下一个客户机设备”)。在本例中，本发明指示客户机设备和下一个客户机设备的操作系统防止用户存取，直到移动结束。本发明指示客户机设备的加密文件系统对所述计算机文件或计算机程序进行解密。然后，本发明指示客户机设备的公共密钥信息基础设施对所述计算机文件或计算机程序(以及由服务设备建立的允许和/或权利)进行加密以便发送，然后经通信装置将计算机文件或计算机程序发送到下一个客户机设备。一旦由下一个客户机设备接收到所述计算机文件或计算机程序(以及由服务设备建立的任何允许和/或权利)，则本发明自动指示下一个客户机设备的公共密钥信息基础设施从发送信息中解密由客户机设备发送的所述计算机文件或计算机程序(以及由服务设备建立的允许和/或权利)。然后，本发明指示下一个客户机设备的加密文件系统根据由服务设备建立并伴随所述计算机文件或计算机程序的任何允许和/或权利进行加密以便存储，并存储所述计算机文件或计算机程序。

本发明涉及一种操纵计算机文件和/或程序的系统。该系统包括一服务设备，该设备能够存取未加密的计算机文件和/或程序，并且能够对所述未加密的计算机文件和/或程序进行加密，以使其变成加密的计算机文件和/或程序并对其进行传送。所述系统包含连接到所述服务设备的一连接器，所述加密的计算机文件和/或程序在该连接器上传播，并且所述服务设备将加密的计算机文件和/或程序传送到该连接器。所述系统包含一客户机设备，该设备接收所述加密的计算机文件和/或程序，并将该加密的计算机文件和/或程序解密回到未加密的计算机文件和/或程序，在根据与之相伴随的允许或权利接收所述加密的计算机文件和/或程序的时期内，所述客户机设备暂停存取所述加密的计算机文件和/或程序，所述服务设备与所述客户机设备分离、远离且截然不同。

本发明涉及一种操纵计算机文件和/或程序的方法。该方法包括

步骤：由客户机设备端的用户暂停客户机设备的存取。之后是步骤：对服务器设备端的未加密的计算机文件和/或程序进行加密，以形成加密的计算机文件和/或程序。接着是步骤：将加密的计算机文件和/或程序沿着与客户机设备和服务器设备相连的连接器传送到客户机设备。然后是步骤：由用户重新建立客户机设备的存取。

附图说明

图1是可用于实施本发明的教导的用于自动调用服务设备10的操作系统60的功能体的目的的示意图。

图2是可用于实施本发明的教导的用于自动调用客户机设备11的操作系统61的功能体的目的的示意图。

图3是可用于实施本发明的教导的用于自动调用服务设备10的操作系统60的功能体的目的的计算机编程流程图。

图4是可用于实施本发明的教导的用于自动调用客户机设备11的操作系统61的功能体的目的的计算机编程流程图。

具体实施方式。

在下面的附图中，示出了本发明的优选实施例和实现本发明的优选方法，其中：

图1是可用于实施本发明的教导的用于自动调用服务设备10的操作系统60的功能体的目的的示意图，用于：通过利用与通信装置120连接的收发信机70加密和发送计算机文件和/或程序110及其相关的允许和/或权利到客户机设备11。图1也是可用于实施本发明的教导的用于自动调用客户机设备11的操作系统61的功能体的目的的示意图，用于：通过利用与通信装置120连接的收发信机71从服务设备10的发送信息中接收和解密计算机文件和/或程序110及其相关的允许和/或权利，并将它们的电子复制件存储在RAM 81中；利用所述相关的允许和/或权利加密并存储RAM 81中的所述计算机文件和/或

程序110到存储器101中，然后从RAM 81中擦除所述计算机文件和/或程序110的任何电子复制件；和

图2是可用于实施本发明的教导的用于自动调用客户机设备11的操作系统61的功能体的目的的示意图，用于：对来自存储器101的计算机文件和/或程序110进行解密，并在RAM 81中存储其电子复制件并存储相关的允许和/或权利；并且，通过利用与通信装置120连接的收发信机71加密和发送计算机文件和/或程序110及其相关的允许和/或权利到下一个客户机设备12；然后，从RAM 81中擦除所述计算机文件和/或程序110的任何电子复制件；以及，在从存储器101移动所述计算机文件和/或程序110到存储器102的情况下，则会从存储器101中擦除所述计算机文件和/或程序110的任何电子复制件。图2也是可用于实施本发明的教导的用于自动调用客户机设备12的操作系统62的功能体的目的的示意图，用于：通过利用与通信装置120连接的收发信机72从客户机设备11的发送信息中接收和解密计算机文件和/或程序110及其相关的允许和/或权利，并将它们的电子复制件存储在RAM 82中；利用所述相关的允许和/或权利加密并存储RAM 82中的所述计算机文件和/或程序110到存储器102中，然后从RAM 82中擦除所述计算机文件和/或程序110的任何电子复制件；和

图3是可用于实施本发明的教导的用于自动调用服务设备10的操作系统60的功能体的目的的计算机编程流程图，用于：通过利用与通信装置120连接的收发信机70加密和发送计算机文件和/或程序110及其相关的允许和/或权利到客户机设备11。图3也是可用于实施本发明的教导的用于自动调用客户机设备11的操作系统61的功能体的目的的计算机编程流程图，用于：通过利用与通信装置120连接的收发信机71从服务设备10的发送信息中接收和解密计算机文件和/或程序110及其相关的允许和/或权利，并将它们的电子复制件存储在RAM 81中；利用所述相关的允许和/或权利加密并存储RAM 81中的所述计算机文件和/或程序110到存储器101中，然后从RAM 81中擦

除所述计算机文件和/或程序110的任何电子复制件；和

图4是可用于实施本发明的教导的用于自动调用客户机设备11的操作系统61的功能体的目的的计算机编程流程图，用于：对来自存储器101的计算机文件和/或程序110进行解密，并在RAM 81中存储其电子复制件并存储相关的允许和/或权利；并且，通过利用与通信装置120连接的收发信机71加密和发送计算机文件和/或程序110及其相关的允许和/或权利到下一个客户机设备12；然后，从RAM 81中擦除所述计算机文件和/或程序110的任何电子复制件；以及，在从存储器101移动所述计算机文件和/或程序110到存储器102的情况下，则会从存储器101中擦除所述计算机文件和/或程序110的任何电子复制件。图4也是可用于实施本发明的教导的用于自动调用客户机设备12的操作系统62的功能体的目的的计算机编程流程图，用于：通过利用与通信装置120连接的收发信机72从客户机设备11的发送信息中接收和解密计算机文件和/或程序110及其相关的允许和/或权利，并将它们的电子复制件存储在RAM 82中；利用所述相关的允许和/或权利加密并存储RAM 82中的所述计算机文件和/或程序110到存储器102中，然后从RAM 82中擦除所述计算机文件和/或程序110的任何电子复制件。

现在参照附图，其中在几幅附图中相似的标号表示类似或等同的部分，具体到附图中的图1和2，其中示出了一种操纵计算机文件和/或程序的系统。该系统包括一服务设备10，该设备10能够存取未加密的计算机文件和/或程序，并且能够对所述未加密的计算机文件和/或程序进行加密，以使其变成加密的计算机文件和/或程序并对其进行传送。所述系统还包括连接到服务设备10的一连接器，所述加密的计算机文件和/或程序在该连接器上传播，并且服务设备10将加密的计算机文件和/或程序传送到该连接器。该连接器可以是通信装置120。所述系统还包括一客户机设备11，该设备11接收所述加密的

计算机文件和/或程序，并将该加密的计算机文件和/或程序解密回到未加密的计算机文件和/或程序。客户机设备11在所述加密的计算机文件和/或程序被接收的时期内不允许干预该加密的计算机文件和/或程序。服务设备10与客户机设备11分离、远离且截然不同。

最好，在所述客户机设备11已接收所述加密的计算机文件和/或程序之后，或者在所述客户机设备11已将所述加密的计算机文件和/或程序解密回到未加密的计算机文件和/或程序之后，所述服务器设备将允许和/或权利分配给能够识别客户机设备11能够如何处置未加密的或加密的计算机文件和/或程序的未加密的计算机文件和/或程序。所述服务器设备最好对所述允许和/或权利进行加密，并将它们通过所述连接器传送给客户机设备11。客户机设备11对未加密的允许和/或权利进行解密。

最好，所述服务设备10包括控制服务器软件和/或固件30，可以使得当所述客户机设备11接收所述加密的计算机文件和/或程序以及所述加密的允许和/或权利的时候所述未加密的计算机文件和/或程序以及所述允许和/或权利的加密使客户机设备11临时暂停用户干预。最好，客户机设备11具有向所述服务器设备请求未加密的计算机文件和/或程序的机制。

最好，控制客户机软件和/或固件31能使未加密的计算机文件和/或程序以及允许和/或权利被加密，以便存储。最好，客户机设备11具有一操作系统，并且控制客户机软件和/或固件51指示该操作系统在需要时重新建立用户干预。所述服务器设备最好具有一服务器公共密钥信息基础设施41，该服务器公共密钥信息基础设施41利用加密的通信协议对所述允许和/或权利以及所述未加密的计算机文件和/或程序进行加密。

最好，所述客户机设备11具有一客户机公共密钥信息基础设施42，该客户机公共密钥信息基础设施42利用加密的通信协议从发送

信息中解密所述允许和/或权利以及所述加密的计算机文件和/或程序。所述客户机设备11最好包括一加密文件系统51，该加密文件系统51对所述未加密的计算机文件和/或程序以及所述允许和/或权利进行加密，并允许手动选择用于加密或解密的未加密的计算机文件和/或程序。最好，所述客户机公共密钥信息基础设施42具有一加密和/或解密密钥，并且所述加密文件系统51使用由所述客户机公共密钥信息基础设施42所利用的所述加密和/或解密密钥。

所述系统最好还包括通过所述连接器连接到客户机设备11的下一个客户机设备20。最好，所述控制客户机软件和/或固件31通过第二个连接器移动或复制所述加密的计算机文件和/或程序到所述下一个客户机设备20，所述客户机设备11具有一控制下一个客户机软件和/或固件，该控制下一个客户机软件和/或固件对所接收的加密的计算机文件和/或程序和所述加密的允许和/或权利进行解密，并在由所述下一个客户机设备20接收所述加密的计算机文件和/或程序的时候临时暂停用户干预。最好，所述连接器包括一通信链路，所述服务器设备包括连接到所述通信链路的一发送器，用于将所述加密的计算机文件和/或程序以及未加密的允许和/或权利传送到所述通信链路，并且所述客户机设备11包括连接到所述通信链路的一接收器，该接收器从所述通信链路接收所述加密的计算机文件和/或程序以及加密的允许和/或权利。所述连接器最好是因特网或者其它通信网络的一部分。

本发明还涉及一种操纵计算机文件和/或程序的方法。该方法包括步骤：由客户机设备11端的用户暂停客户机设备11的干预。之后是步骤：对服务器设备端的未加密的计算机文件和/或程序进行加密，以形成加密的计算机文件和/或程序。接着是步骤：将所述加密的计算机文件和/或程序沿着与客户机设备11和服务器设备连接的一连接器传送到客户机设备11。然后是步骤：由用户重新建立客户机

设备11的干预。

在所述传送步骤之前，最好有下列步骤：对所述未加密的计算机文件和/或程序的允许和/或权利进行加密，并将加密的允许和/或权利沿所述连接器从所述服务器设备传送到客户机设备11。最好，在对所述未加密的计算机文件和/或程序进行加密的步骤之前，包括下列步骤：由客户机设备11请求所述服务器设备的未加密的计算机文件和/或程序。在所述请求步骤之后，最好包括下列步骤：复制原始的未加密计算机文件和/或程序，以形成所述未加密的计算机文件和/或程序。

最好，在所述重新建立步骤之前，包括下列步骤：在客户机设备11端将所述加密的计算机文件和/或程序解密回到未加密的计算机文件和/或程序。在所述解密步骤之后，最好包括下列步骤：在所述客户机设备11端对所述未加密的计算机文件和/或程序以及允许和/或权利进行加密；并且将加密的计算机程序和/或文件及加密的允许和/或权利存储到所述客户机设备11中。最好，在所述存储步骤之后，包括下列步骤：将所述加密的计算机文件和/或程序传送到由所述连接器连接到客户机设备11的下一个客户机设备20。

现在参照附图，其中在几幅附图中相似的标号表示类似或等同的部分，具体到附图中的图1和3，其中示出了用于分别调用计算机设备的服务设备10和客户机设备11的操作系统60和61的功能体的装备30和31。装备30和31分别连接到计算机设备的服务设备10和客户机设备11的操作系统60和61。装备30包括用于调用服务设备10的操作系统60的功能体的一装置或机构，用于：在执行装备30和31的功能体的期间，指示装备31去指示操作系统61临时暂停客户机设备11的用户干预；通过利用连接到通信装置120的收发信机70进行加密通信；通过利用与通信装置120连接的收发信机70加密和发送计算机文件和/或程序110及其相关的允许和/或权利到客户机设备11。装备31

包括用于调用客户机设备11的操作系统61的功能体的一装置或机构，用于：在执行装备30和31的功能体的期间，指示操作系统61临时暂停客户机设备11的用户干预；通过利用连接到通信装置120的收发信机70执行加密通信；通过利用连接到通信装置120的收发信机71从服务设备10的发送信息中接收和解密计算机文件和/或程序110及其相关的允许和/或权利，并将它们的电子复制件存储在RAM 81中；利用所述相关的允许和/或权利加密并存储RAM 81中的所述计算机文件和/或程序110到存储器101中，然后从RAM 81中擦除所述计算机文件和/或程序110的任何电子复制件；在结束执行装备30和31的功能体时，指示操作系统61恢复客户机设备11的用户干预。

现在参照附图，其中在几幅附图中相似的标号表示类似或等同的部分，具体到附图中的图2和4，其中示出了用于分别调用计算机设备的客户机设备11和下一个客户机设备12的操作系统61和62的功能体的装备31和32。装备31和32分别连接到计算机设备的客户机设备11和下一个客户机设备12的操作系统61和62。装备31包括用于调用客户机设备11的操作系统61的功能体的一装置或机构，用于：在执行装备31和32的功能体的期间，指示操作系统61临时暂停客户机设备11的用户干预；在执行装备31和32的功能体的期间，指示装备32去指示操作系统62临时暂停下一个客户机设备12的用户干预；通过利用连接到通信装置120的收发信机71进行加密通信；对存储器101的计算机文件和/或程序110进行解密，并将其电子复制件以及相关的允许和/或权利存储在RAM 81中；通过利用与通信装置120连接的收发信机71加密和发送计算机文件和/或程序110及其相关的允许和/或权利到下一个客户机设备12；然后从RAM 81中擦除所述计算机文件和/或程序110的任何电子复制件；以及，在从存储器101移动所述计算机文件和/或程序110到存储器102的情况下，则会从存储器101中擦除所述计算机文件和/或程序110的任何电子复制件；在结束执

行装备31的功能体时，指示操作系统61恢复客户机设备11的用户干预。

装备32包括用于调用下一个客户机设备12的操作系统62的功能体的一装置或机构，用于：在执行装备31和32的功能体的期间，指示操作系统62临时暂停下一个客户机设备12的用户干预；通过利用连接到通信装置120的收发信机71进行加密通信；通过利用连接到通信装置120的收发信机72从客户机设备11的发送信息中接收和解密计算机文件和/或程序110及其相关的允许和/或权利，并将它们的电子复制件存储在RAM 82中；利用所述相关的允许和/或权利加密并存储RAM 82中的所述计算机文件和/或程序110到存储器102中，然后从RAM 82中擦除所述计算机文件和/或程序110的任何电子复制件；在结束执行装备32的功能体时，指示操作系统62恢复下一个客户机设备12的用户干预。

参照图1和图3，本发明的一个优选实施例包括下列部分或部件：

- 10 服务设备
- 11 客户机设备
- 20 服务接口
- 21 客户机接口
- 30 控制服务软件和/或固件(也称为“服务CSS和/或F”)
- 31 控制客户机软件和/或固件(也称为“客户机CCS和/或F”)
- 40 公共密钥信息基础设施
- 41 公共密钥信息基础设施
- 50 加密文件系统
- 51 加密文件系统
- 60 操作系统
- 61 操作系统

- 70 收发信机
- 71 收发信机
- 80 随机存取存储器(也称为“RAM”)
- 81 随机存取存储器(也称为“RAM”)
- 90 处理器
- 91 处理器
- 100 存储器
- 101 存储器
- 110 计算机文件和/或程序(也称为“文件和/或程序”)
- 120 通信装置

在图1和图3中, 下列部件已是可用商品: 服务设备10、客户机设备11、服务接口20、客户机接口21、公共密钥信息基础设施40、公共密钥信息基础设施41、加密文件系统50、加密文件系统51、操作系统60、操作系统61、收发信机70、收发信机71、随机存取存储器80(也称为“RAM 80”)、随机存取存储器81(也称为“RAM 81”)、处理器90、处理器91、存储器100、存储器101、计算机文件和/或程序110(也称为“文件和/或程序 110”)以及通信装置120。控制服务软件和/或固件30(也称为“服务CSS和/或F 30”)及控制客户机软件和/或固件31(也称为“客户机CCS和/或F 31”)是在本发明中新教导的。

参照图2和图4, 本发明的一个优选实施例包括下列部分或部件:

- 11 客户机设备
- 12 下一个客户机设备
- 21 客户机接口
- 22 下一个客户机接口
- 31 控制客户机软件和/或固件(也称为“客户机CCS和/或F”)

- 32 控制客户机软件和/或固件(也称为“下一个客户机CCS和/或F”)
- 41 公共密钥信息基础设施
- 42 公共密钥信息基础设施
- 51 加密文件系统
- 52 加密文件系统
- 61 操作系统
- 62 操作系统
- 71 收发信机
- 72 收发信机
- 81 随机存取存储器(也称为“RAM”)
- 82 随机存取存储器(也称为“RAM”)
- 91 处理器
- 92 处理器
- 101 存储器
- 102 存储器
- 110 计算机文件和/或程序(也称为“文件和/或程序”)
- 120 通信装置

在图2和/或图4中，下列部件已是可用商品：客户机设备11、下一个客户机设备12、客户机接口21、下一个客户机接口22、公共密钥信息基础设施41、公共密钥信息基础设施42、加密文件系统51、加密文件系统52、操作系统61、操作系统62、收发信机71、收发信机72、随机存取存储器81(也称为“RAM 81”)、随机存取存储器82(也称为“RAM 82”)、处理器91、处理器92、存储器101、存储器102、计算机文件和/或程序110(也称为“文件和/或程序110”)以及通信装置120。控制客户机软件和/或固件31(也称为“客户机CCS和/或F 31”)及控制客户机软件和/或固件32(也称为“客户机CCS和

/或F 32”)是在本发明中新教导的。

服务设备10(例如,但不限于,Web服务器、PC、Mac、PalmPC、Laptop等)是能够与其它计算设备电通信的装置或机构。服务设备10也是可以用来将计算机文件发送到其它计算设备的装置或机构。服务设备10可包括视频显示器、音频扬声器和其它计算外设。

客户机设备11(例如,但不限于,Web服务器、PC、Mac、PalmPC、Laptop等)是可以用来使计算机文件发送到其它计算设备或从其它计算设备发送来的装置或机构。客户机设备11也是可以用来从其它计算设备接收计算机文件的装置或机构。客户机设备11可包括视频显示器、音频扬声器和其它计算外设。

下一个客户机设备12(例如,但不限于,Web服务器、PC、Mac、PalmPC、Laptop等)是可以用来使计算机文件发送到其它计算设备或从其它计算设备发送来的装置或机构。下一个客户机设备12也是可以用来从其它计算设备接收计算机文件的装置或机构。下一个客户机设备12可包括视频显示器、音频扬声器和其它计算外设。

服务接口20(例如,但不限于,web服务器商业软件,比如微软的商用服务器)是能够接收和执行从另一个计算装置发送来的请求的装置或机构。

客户机接口21(例如,但不限于,web浏览器软件,比如微软的因特网浏览器)是能够发送请求到另一个计算设备并能够显示服务接口20和下一个客户机接口22的内容的装置或机构。

下一个客户机接口22(例如,但不限于,web浏览器软件,比如微软的因特网浏览器)是能够发送请求到另一个计算设备并能够显示客户机接口21的内容的装置或机构。

控制服务软件和/或固件30是用于指示操作系统60或者其通信程序经通信装置120与客户机设备11通信的装置或机构。控制服务软件

和/或固件30也是用于在执行控制服务软件和/或固件30和控制客户机软件和/或固件31的功能体的期间，指示控制客户机软件和/或固件31去指示操作系统61临时暂停客户机设备11的用户干预的装置或机构。控制服务软件和/或固件30也是用于经通信装置120从控制客户机软件和/或固件31接收指令的装置或机构。控制服务软件和/或固件30也是能够使服务设备10的用户建立与计算机文件和/或程序110有关的第三方使用允许和/或权利，从而由客户机设备11或下一个客户机设备12限制计算机文件和/或程序110的使用的装置或机构。控制服务软件和/或固件30也是用于自动指示服务设备10的公共密钥信息基础设施40经通信装置120加密和发送与计算机文件和/或程序110有关的使用允许和/或权利，以及加密和发送计算机文件和/或程序110到客户机设备11的装置或机构。控制服务软件和/或固件30可体现在计算机编码软件中(例如，但不限于，以计算机语言C++编写的程序)，用于执行上述功能。

控制客户机软件和/或固件31是用于自动指示操作系统61或者其通信程序经通信装置120与服务设备10或下一个客户机设备12通信的装置或机构。控制客户机软件和/或固件31也是用于经通信装置120接收来自控制服务软件和/或固件30的指令的装置或机构。控制客户机软件和/或固件31也是用于在执行控制服务软件和/或固件30和控制客户机软件和/或固件31的功能体的期间，指示操作系统61临时暂停客户机设备11的用户干预的装置或机构。控制客户机软件和/或固件31也是用于自动指示客户机设备11的公共密钥信息基础设施41经通信装置120从发送信息中接收和解密与计算机文件和/或程序110有关的使用允许和/或权利，以及从发送信息中接收和解密从服务设备10发送的计算机文件和/或程序110，并将它们的电子复制件放置于RAM 81中的装置或机构。控制客户机软件和/或固件31也是用于利用与所述计算机文件和/或程序110有关并且由服务设备10发送的所

述使用允许和/或权利，自动指示客户机设备11的加密文件系统51从RAM 81中再调用计算机文件和/或程序110，并对其电子复制件进行加密并且保存到存储器101中的装置和机构。控制客户机软件和/或固件31也是用于在结束执行控制服务软件和/或固件30和控制客户机软件和/或固件31的功能体时，指示操作系统61恢复客户机设备11的用户干预的装置或机构。控制客户机软件和/或固件31是用于在执行控制客户机软件和/或固件31和控制客户机软件和/或固件32的功能体的期间，指示操作系统61临时暂停客户机设备11的用户干预的装置或机构。控制客户机软件和/或固件31是用于在执行控制客户机软件和/或固件31和控制客户机软件和/或固件32的功能体的期间，指示操作系统62临时暂停下一个客户机设备12的用户干预的装置或机构。控制客户机软件和/或固件31也是用于经通信装置120从下一个客户机设备12的控制客户机软件和/或固件32接收指令的装置或机构。控制客户机软件和/或固件31也是用于自动指示客户机设备11的加密文件系统51对存储器101中的计算机文件和/或程序110进行解密，并将其电子复制件放置于RAM 81中的装置和机构。控制客户机软件和/或固件31也是用于自动指示客户机设备11的公共密钥信息基础设施41经通信装置120加密和发送计算机文件和/或程序110到下一个客户机设备12的装置或机构。控制客户机软件和/或固件31也是用于在结束执行控制客户机软件和/或固件31的功能体时，指示操作系统61恢复客户机设备11的用户干预的装置或机构。控制客户机软件和/或固件31可体现在计算机编码软件中(例如，但不限于，以计算机语言C++编写的程序)，用于执行此处的上述功能。控制客户机软件和/或固件31可具有许多类似于控制客户机软件和/或固件32的体现形式。

控制客户机软件和/或固件32是用于自动指示操作系统62或者其通信程序经通信装置120与客户机设备12进行电子通信的装置或机构。控制客户机软件和/或固件32也是用于经通信装置120接收来自

客户机设备11的控制客户机软件和/或固件31的指令的装置或机构。控制客户机软件和/或固件32也是用于在执行控制客户机软件和/或固件31和控制客户机软件和/或固件32的功能体的期间，指示操作系统62临时暂停下一个客户机设备12的用户干预的装置或机构。控制客户机软件和/或固件32也是用于自动指示下一个客户机设备12的公共密钥信息基础设施42经通信装置120从发送信息中接收和解密与计算机文件和/或程序110有关的使用允许和/或权利，以及从发送信息中接收和解密从客户机设备11发送的计算机文件和/或程序110，并将它们的电子复制件放置于RAM 82中的装置或机构。控制客户机软件和/或固件32也是用于利用与所述计算机文件和/或程序110有关并且由客户机设备11发送的所述使用允许和/或权利，自动指示下一个客户机设备12的加密文件系统52从RAM 82中再调用计算机文件和/或程序110，并对其电子复制件进行加密并且保存到存储器102中的装置和机构。控制客户机软件和/或固件32也是用于在结束执行控制客户机软件和/或固件31和控制客户机软件和/或固件32的功能体时，指示操作系统62恢复下一个客户机设备12的用户干预的装置或机构。控制客户机软件和/或固件32可体现在计算机编码软件中(例如，但不限于，以计算机语言C++编写的程序)，用于执行此处的上述功能。控制客户机软件和/或固件32可具有许多类似于控制客户机软件和/或固件31的体现形式。

服务设备10的公共密钥信息基础设施40(例如，但不限于，先前称为Microsoft Windows NT服务器版本5.0的Microsoft Windows 2000服务器家族的公共密钥信息基础设施)是用于提供能使服务设备10利用加密通信协议(例如，但不限于，安全套接层(SSL)、传输层安全性(TLS)和虚拟专用网络(VPN)等)经通信装置120进行加密通信的公共加密和私人解密密钥的密码装置或机构。服务设备10的公共密钥信息基础设施40也是用于向操作系统60的其它部件或者运行在操作

系统60上的应用程序提供公共加密和私人解密密钥的密码装置或机构。

客户机设备11的公共密钥信息基础设施41(例如,但不限于,先前称为Microsoft Windows NT工作站版本5.0的Microsoft Windows 2000专业版的公共密钥信息基础设施)是用于提供能使客户机设备11利用加密通信协议(例如,但不限于,安全套接层(SSL)、传输层安全性(TLS)和虚拟专用网络(VPN)等)经通信装置120进行加密通信的公共加密和私人解密密钥的密码装置或机构。客户机设备11的公共密钥信息基础设施41也是用于向操作系统61的其它部件或者运行在操作系统61上的应用程序提供公共加密和私人解密密钥的密码装置或机构。

下一个客户机设备12的公共密钥信息基础设施42(例如,但不限于,先前称为Microsoft Windows NT工作站版本5.0的Microsoft Windows 2000专业版的公共密钥信息基础设施)是用于提供能使所述下一个客户机设备12利用加密通信协议(例如,但不限于,安全套接层(SSL)、传输层安全性(TLS)和虚拟专用网络(VPN)等)经通信装置120进行加密通信的公共加密和私人解密密钥的密码装置或机构。下一个客户机设备12的公共密钥信息基础设施42也是用于向操作系统62的其它部件或者运行在操作系统62上的应用程序提供公共加密和私人解密密钥的密码装置或机构。

加密文件系统50(例如,但不限于,先前称为Microsoft Windows NT服务器版本5.0的Microsoft Windows 2000服务器的加密文件系统)是允许服务设备的用户手动选择要加密或解密的计算机文件或文件夹的装置或机构。加密文件系统50也是利用随机产生且秘密的加密和/或解密密钥对计算机文件和/或程序110进行加密的装置或机构。加密文件系统50也是利用公共密钥信息基础设施40的公共加密密钥对所述随机产生的秘密的加密和/或解密密钥进行加密,并将其存储

到存储器100，并且使所述随机产生的秘密的加密和/或解密密钥与所述计算机文件和/或程序110相关的装置或机构。加密文件系统50也是利用公共密钥信息基础设施40的私人解密密钥对与所述计算机文件和/或程序110相关的所述随机产生的秘密的加密和/或解密密钥的复制件进行解密，然后在服务设备10的读和写操作期间，利用所述随机产生的秘密的加密和/或解密密钥对所述计算机文件和/或程序110进行实时解密的装置或机构。

加密文件系统51(例如，但不限于，先前称为Microsoft Windows NT工作站版本5.0的Microsoft Windows 2000专业版的加密文件系统)是允许客户机设备的用户手动选择要加密或解密的计算机文件或文件夹的装置或机构。加密文件系统51也是利用随机产生且秘密的加密和/或解密密钥对计算机文件和/或程序110进行加密的装置或机构。加密文件系统51也是利用公共密钥信息基础设施41的公共加密密钥对所述随机产生的秘密的加密和/或解密密钥进行加密，并将其存储到存储器101，并且使所述随机产生的秘密加密和/或解密密钥与所述计算机文件和/或程序110相关的装置或机构。加密文件系统51也是利用公共密钥信息基础设施41的私人解密密钥对与所述计算机文件和/或程序110相关的所述随机产生的秘密加密和/或解密密钥的复制件进行解密，然后在客户机设备11的读和写操作期间，利用所述随机产生的秘密加密和/或解密密钥对所述计算机文件和/或程序110进行实时解密的装置或机构。

加密文件系统52(例如，但不限于，先前称为Microsoft Windows NT工作站版本5.0的Microsoft Windows 2000专业版的加密文件系统)是允许下一个客户机设备12的用户手动选择要加密或解密的计算机文件或文件夹的装置或机构。加密文件系统52也是利用随机产生且秘密的加密和/或解密密钥对计算机文件和/或程序110进行加密的装置或机构。加密文件系统52也是利用公共密钥信息基础设施42的公

共加密密钥对所述随机产生的秘密加密和/或解密密钥进行加密，并将其存储到存储器102，并且使所述随机产生的秘密加密和/或解密密钥与所述计算机文件和/或程序110相关的装置或机构。加密文件系统52也是利用公共密钥信息基础设施42的私人解密密钥对与所述计算机文件和/或程序110相关的所述随机产生的秘密加密和/或解密密钥的复制件进行解密，然后在下一个客户机设备12的读和写操作期间，利用所述随机产生的秘密加密和/或解密密钥对所述计算机文件和/或程序110进行实时解密的装置或机构。

操作系统60(例如，但不限于，先前称为Microsoft Windows NT 服务器版本5.0的Microsoft Windows 2000服务器)是允许服务设备10的计算功能的装置或机构。

操作系统61(例如，但不限于，先前称为Microsoft Windows NT 工作站版本5.0的Microsoft Windows 2000专业版)是允许客户机设备11的计算功能的装置或机构。

操作系统62(例如，但不限于，先前称为Microsoft Windows NT 工作站版本5.0的Microsoft Windows 2000专业版)是允许下一个客户机设备12的计算功能的装置或机构。

收发信机70(例如，但不限于，modem、cable modem(电缆调制解调器)、网络接口卡，等)是用于经通信装置120电子发送和接收通信信号的装置或机构。收发信机70是由服务设备10和/或操作系统60的软件和/或固件使用或者与服务设备10和/或操作系统60连接，以便通过通信装置120进行电子通信的装置或机构。收发信机70连接到服务设备10并连接到通信装置120。

收发信机71(例如，但不限于，modem、cable modem、网络接口卡，等)是用于经通信装置120电子发送和接收通信信号的装置或机构。收发信机71是由客户机设备11和/或操作系统61的软件和/或固件使用或者与客户机设备11和/或操作系统61连接，以便通过通信装

置120进行电子通信的装置或机构。收发信机71连接到客户机设备11并连接到通信装置120。

收发信机72(例如,但不限于, modem、cable modem、网络接口卡,等)是用于经通信装置120电子发送和接收通信信号的装置或机构。收发信机72是由下一个客户机设备12和/或操作系统62的软件和/或固件使用或者与下一个客户机设备12和/或操作系统62连接,以便通过通信装置120进行电子通信的装置或机构。收发信机72连接到下一个客户机设备12并连接到通信装置120。

随机存取存储器80(也称为“RAM 80”)是由服务设备10的操作系统60使用的装置或机构,用于临时存储要由操作系统60使用的计算机文件、计算机程序或者其它计算机信息、运行在所述服务设备10的操作系统60或其它计算机外设上的计算机程序。

随机存取存储器81(也称为“RAM 81”)是由客户机设备11的操作系统61使用的装置或机构,用于临时存储要由操作系统61使用的计算机文件、计算机程序或者其它计算机信息、运行在所述客户机设备11的操作系统61或其它计算机外设上的计算机程序。

随机存取存储器82(也称为“RAM 82”)是由下一个客户机设备12的操作系统62使用的装置或机构,用于临时存储要由操作系统62使用的计算机文件、计算机程序或者其它计算机信息、运行在所述下一个客户机设备12的操作系统62或其它计算机外设上的计算机程序。

处理器90是服务设备10的用于电子处理操作系统60的指令、运行在所述服务设备10的所述操作系统60或其它计算机外设上的其它计算机程序的装置或机构。处理器90也是服务设备10的用于电子处理所述服务设备10的其它外围软件和/或固件设备的指令的装置或机构。

处理器91是客户机设备11的用于电子处理操作系统61的指令、

运行在所述客户机设备11的所述操作系统61或其它计算机外设上的其它计算机程序的装置或机构。处理器91也是客户机设备11的用于电子处理所述客户机设备11的其它外围软件和/或固件设备的指令的装置或机构。

处理器92是下一个客户机设备12的用于电子处理操作系统62的指令、运行在所述下一个客户机设备12的所述操作系统62或其它计算机外设上的其它计算机程序的装置或机构。处理器92也是下一个客户机设备12的用于电子处理所述下一个客户机设备12的其它外围软件和/或固件设备的指令的装置或机构。

存储器100是服务设备10内部或与该服务设备10连接的装置或机构，能够用于电子保存来自所述服务设备10的RAM 80的计算机程序或计算机文件的数字代码的电子复制件。

存储器101是客户机设备11内部或与该客户机设备11连接的装置或机构，能够用于电子保存来自所述客户机设备11的RAM 81的计算机程序或计算机文件的数字代码的电子复制件。

存储器102是下一个客户机设备12内部或与该下一个客户机设备12连接的装置或机构，能够用于电子保存来自所述下一个客户机设备12的RAM 82的计算机程序或计算机文件的数字代码的电子复制件。

计算机文件和/或程序110是一计算机文件或一计算机程序(例如，但不限于，字处理文件(即MS Word、Lotus WordPro)、电子表格(spreadsheet)文件(例如，但不限于，Lotus 1-2-3、MS Excel)、音频文件(例如，但不限于，MP3、WAV、AUI)、视频文件(例如，但不限于，AVI、MPEG)、可执行程序(例如，但不限于，EXE)，等)。

通信装置120(例如，但不限于，电话线、有线电视线、同轴电缆、光纤设备、无线设备、蜂窝设备、卫星设备、串行电缆、并行

电缆、红外线通信设备、通用串行总线(USB)电缆、因特网、LAN、以太网、通用网络,等)是可以使与其连接的计算设备能够进行电子通信的装置或机构。通信装置120也是可以使与其连接的计算设备能够调用加密通信协议(例如,但不限于,安全套接层(SSL)、传输层安全性(TLS)和虚拟专用网络(VPN)等)以发送和接收加密信号的装置或机构。通信装置120分别连接到服务设备10、客户机设备11和下一个客户机设备12的收发信机70、71和72。

服务设备10的用户将计算机文件和/或程序110保存到服务设备10内部或与该服务设备10连接的存储器100中。服务设备10的用户在服务接口20和存储器100中的所述计算机文件和/或程序110的位置之间建立链路、连接或其它形式的电子关联(例如,但不限于,建立一TCP和/或IP超链接)(集合地称为“超链接”)。服务设备10的收发信机70连接到通信装置120。服务设备10的用户输入(例如,但不限于,通过键盘、鼠标等输入)要通过控制服务软件和/或固件30与计算机文件和/或程序110相关联的允许和/或权利。所述允许包括,但不限于,移动或复制等,而所述权利包括,但不限于,使用号码、使用截止日期、分配允许和/或权利到第三方等。

客户机设备11的用户经通信装置120与服务设备10进行通信。客户机设备11的收发信机71连接到通信装置120。客户机设备11的用户在客户机设备11的视频显示器上观看服务接口20,并识别与所需计算机文件和/或程序110相关联的超链接。客户机设备11的用户利用客户机接口21经通信装置120启动超链接发送请求(例如,但不限于,在与所述计算机文件和/或程序110相关联的超链接上双击鼠标),以便从服务设备10获取所述计算机文件和/或程序110。该请求通过控制服务软件和/或固件30,之后通过控制客户机软件和/或固件31启动一系列自动操作。首先,控制服务软件和/或固件30指示控制客户机软件和/或固件31去指示客户机设备11的操作系统61临时暂停

用户干预，以防止任何形式的未授权数据或指令通过服务设备10或客户机设备11内部或外部的装置或机构输入或贯穿服务设备10或客户机设备11，例如，但不限于，用户通过使用键盘、鼠标或其它物理装置或机构；计算机程序；宏；或者可以任何方式影响本发明的软件和/或固件的功能体或者以任何方式影响由本发明使用的任何软件和/或固件的功能体的任何其它装置，来进行输入或控制，以及防止在执行发送请求期间的任何形式的访问、使用或控制计算机文件和/或程序110。然后，控制客户机软件和/或固件31指示客户机设备11的操作系统61临时暂停用户干预。然后，控制客户机软件和/或固件31指示控制服务软件和/或固件30发送计算机文件和/或程序110到客户机设备11。然后，控制服务软件和/或固件30指示服务设备10的操作系统60的公共密钥信息基础设施40利用加密通信协议(例如，但不限于，安全套接层(SSL)、传输层安全性(TLS)和虚拟专用网络(VPN)等)加密和发送计算机文件和/或程序110及其相关的允许和/或权利到客户机设备11。然后，服务设备10的操作系统60从存储器100中再调用计算机文件和/或程序110；将计算机文件和/或程序110的电子复制件放置在RAM 80中；并且经通信装置120加密和发送计算机文件和/或程序110到客户机设备11。然后，客户机设备11的操作系统61的公共密钥信息基础设施41利用加密通信协议(例如，但不限于，安全套接层(SSL)、传输层安全性(TLS)和虚拟专用网络(VPN)等)从发送信息中接收和解密所述计算机文件和/或程序110，并将所述计算机文件和/或程序110的电子复制件放置到RAM 81中。然后，控制客户机软件和/或固件31自动指示客户机设备11的加密文件系统51利用由服务设备10发送的相关的允许和/或权利对RAM 81中的计算机文件和/或程序110的所述电子复制件进行加密并保存到存储器101中，然后从RAM 81中擦除计算机文件和/或程序110的任何电子复制件。然后，客户机设备11的操作系统61的控制客户机软件和/或固件31

指示客户机设备11的操作系统61重新建立用户干预。

客户机设备11的用户在得到与计算机文件和/或程序110相关的允许和/或权利的条件下可使用保存在存储器101中的计算机文件和/或程序110，就好象所述计算机文件和/或程序110没有被加密一样。没有由加密文件系统51执行过的计算机文件和/或程序110的复制或移动将不会被正确加密，以便只用在计算设备上而不是客户机设备11上。按照所述允许和/或权利，客户机设备11的用户可利用控制客户机软件和/或固件31来激活加密文件系统51的功能，以执行从存储器101到下一个客户机设备12的存储器102的计算机文件和/或程序110的移动或复制。客户机设备12的收发信机72连接到通信装置120。客户机设备11的用户观察客户机接口21和下一个客户机接口22的视窗(例如，但不限于，由Windows 2000操作系统所使用的视窗)，该视窗在客户机设备11的视频显示器上分别显示存储器101到存储器102的相关内容。用户识别与从存储器101移动到存储器102的计算机文件和/或程序110相关的对象(例如，但不限于，图标)(下文中称为“图标”)。客户机设备11的用户利用他们的计算机鼠标来从客户机接口21视窗到下一个客户机接口22视窗移动与计算机文件和/或程序110相关的图标(例如，但不限于，图形用户接口的drag-n-drop(拖放)移动)。与所述计算机文件和/或程序110相关的所述图标的drag-n-drop可通过控制服务软件和/或固件30，然后通过控制客户机软件和/或固件31来启动一系列自动操作。首先，控制客户机软件和/或固件31指示客户机设备11的操作系统61临时暂停用户干预，以防止任何形式的未授权数据或指令通过客户机设备11或下一个客户机设备12内部或外部的装置或机构输入或贯穿客户机设备11或下一个客户机设备12，例如，但不限于，用户通过使用键盘、鼠标或其它物理装置或机构；计算机程序；宏；或者可以任何方式影响本发明的软件和/或固件的功能体或者以任何方式影响由本发明使用的任何

软件和/或固件的功能体的任何其它装置，来进行输入或控制，以及防止在执行发送请求期间的任何形式的访问、使用或控制计算机文件和/或程序。然后，控制客户机软件和/或固件31指示控制客户机软件和/或固件32去指示下一个客户机设备12的操作系统62临时暂停在执行发送请求期间的用户干预(例如，但不限于，键盘或鼠标干预、程序或宏指令等)。然后，控制客户机软件和/或固件32去指示下一个客户机设备12的操作系统62临时暂停用户干预。然后，控制客户机软件和/或固件31指示加密文件系统51从存储器101再调用且解密所述计算机文件和/或程序110及其相关的允许和/或权利，并将它们的电子复制件保存在RAM 81中。然后，控制客户机软件和/或固件31指示客户机设备11的操作系统61的公共密钥信息基础设施41经通信装置120加密和发送来自RAM 81的所述计算机文件和/或程序110及其相关的允许和/或权利的电子复制件到下一个客户机设备12。然后，控制客户机软件和/或固件32指示下一个客户机设备12的公共密钥信息基础设施42从发送信息中接收和解密所述所述计算机文件和/或程序110及其相关的允许和/或权利，并将它们的电子复制件放置在RAM 82中。在从存储器101到存储器102移动所述计算机文件和/或程序110的情况下，一旦由下一个客户机设备12将计算机文件和/或程序110接收到RAM 82中，则下一个客户机设备12的控制客户机软件和/或固件32自动指示客户机设备11的控制客户机软件和/或固件31去指示客户机设备11的操作系统61删除存储器101或RAM 81中的计算机文件和/或程序110的所有复制件。然后，控制客户机软件和/或固件31指示操作系统61重新建立客户机设备11的用户干预。然后，控制客户机软件和/或固件32自动指示下一个客户机设备12的操作系统62的加密文件系统52利用从客户机设备11发送的相关的允许和/或权利对来自RAM 82的所述计算机文件和/或程序110的电子复制件进行加密并保存到存储器102中，然后从RAM 82中擦除计算机文

件和/或程序110的所有电子复制件。然后，控制客户机软件和/或固件32指示操作系统62重新建立下一个客户机设备12的用户干预。

下一个客户机设备12的用户在得到由服务设备10原始建立并发送到客户机设备11再到下一个客户机设备12的允许和/或权利的条件下可使用计算机文件和/或程序110，就好像该计算机文件和/或程序110没有被加密一样。没有由下一个客户机设备12的加密文件系统52以及下一个客户机设备12的控制客户机软件和/或固件32执行过的计算机文件和/或程序110的复制或移动将不会被正确加密，以便只用在计算设备上而不是下一个客户机设备11上。

举例来说，服务设备10的用户将服务设备10的收发信机70连接到通信装置120并随后与因特网通信连接。服务设备10的用户将作为计算机文件和/或程序110的音频文件(例如，但不限于，处于MP3制式)保存到存储器100，并为其分配到服务接口20(例如，但不限于，一web页)的一链路(例如，但不限于，TCP和/或IP超链接)。客户机设备11的用户将客户机设备11的收发信机71连接到通信装置120并随后与因特网通信连接。客户机设备11的用户能够在客户机设备11的视频显示器上观察客户机接口21内的服务接口20的复制件。客户机设备11的用户通过使用其计算机鼠标双击与MP3音频文件相关的超链接来选择MP3音频文件，以便下载到客户机设备11，所述超链接显示在客户机设备11的视频显示器上的客户机接口21上。所述双击动作指示客户机接口21经通信装置120发送电子请求，以请求从服务设备10下载MP3音频文件到客户机设备11。一旦接收到该发送请求，则服务接口指令控制服务软件和/或固件30开始各种自动功能。控制服务软件和/或固件30首先指示(经通信装置120)控制客户机软件和/或固件31去指示客户机设备11的操作系统61临时暂停用户干预。然后，控制客户机软件和/或固件31指示(经通信装置120)控制服务软件和/或固件30发送MP3音频文件。控制服务软件和/或固件30指示操

作系统60从存储器100再调用MP3音频文件及其相关的允许和/或权利，并将它们的电子复制件放置在随机存取存储器80中。然后，控制服务软件和/或固件30指示公共密钥信息基础设施40对MP3音频文件及其相关的允许和/或权利的电子复制件进行加密并经通信装置120发送到客户机设备11。此时，控制服务软件和/或固件30已完成其发送处理部分以及与控制服务软件和/或固件30有关的程序结束。一旦客户机设备11接收到MP3音频文件及其相关的允许和/或权利，则公共密钥信息基础设施41从发送信息中解密MP3音频文件及其相关的允许和/或权利，并将其电子复制件存储在随机存取存储器81中。然后，控制客户机软件和/或固件31指示客户机设备11的加密文件系统51利用由服务设备10发送的相关的允许和/或权利对来自随机存取存储器81的MP3音频文件的所述电子复制件保存到存储器101中。然后。控制客户机软件和/或固件31指示及指令加密文件系统51或操作系统61从随机存取存储器81中擦除MP3音频文件的任何电子复制件。然后，客户机设备11的操作系统61的控制客户机软件和/或固件31指示客户机设备11的操作系统61重新建立用户干预。此时，控制客户机软件和/或固件31已确定其发送及加密处理部分以及与控制客户机软件和/或固件31有关的程序结束。客户机设备11的用户在得到由加密文件系统51对MP3音频文件加密时使用的允许和/或权利的条件下，能够播放MP3音频文件并使用加密文件系统51。

此外，客户机设备11的用户然后可决定传送MP3音频文件到下一个客户机设备12，并且在本例中，用户可基于与MP3音频文件相关的允许和/或权利来进行上述行为。客户机设备11的用户将客户机设备11的收发信机71连接到通信装置120并随后与因特网通信连接。下一个客户机设备12的用户将下一个客户机设备12的收发信机72连接到通信装置120并随后与因特网通信连接。客户机设备11的用户在客户机设备11的视频显示器上观察分别显示存储器101和102的相关

内容的客户机接口21和下一个客户机接口22的复制件。用户识别与要从存储器101移动到存储器102的MP3音频文件相关的对象(例如,但不限于,图标)(下文中称为“图标”)。客户机设备11的用户使用其计算机鼠标将与MP3音频文件相关的图标从客户机接口21视窗移动(例如,但不限于,用户图形接口的drag-n-drop移动)到下一个客户机接口22视窗。与MP3音频文件相关的所述图标的drag-n-drop可通过控制客户机软件和/或固件31,然后通过控制客户机软件和/或固件32来启动一系列自动操作。首先,控制客户机软件和/或固件31指示客户机设备11的操作系统61临时暂停在执行发送请求期间的用户干预(例如,但不限于,键盘或鼠标干预、程序或宏指令等)。然后,控制客户机软件和/或固件31指示控制客户机软件和/或固件32去指示下一个客户机设备12的操作系统62临时暂停在执行发送请求期间的用户干预(例如,但不限于,键盘或鼠标干预、程序或宏指令等)。然后,控制客户机软件和/或固件32指示下一个客户机设备12的操作系统62临时暂停用户干预。然后,控制客户机软件和/或固件32指示控制客户机软件和/或固件31发送MP3音频文件到下一个客户机设备12。然后,控制客户机软件和/或固件31再调用与MP3音频文件相关并且由加密文件系统51使用的允许和/或权利,并指示加密文件系统51从存储器101再调用和解密MP3音频文件,并将其电子复制件保存在随机存取存储器81中。然后,控制客户机软件和/或固件31指示客户机设备11的操作系统61的公共密钥信息基础设施41对来自随机存取存储器81的MP3音频文件的电子复制件及其相关的允许和/或权利进行加密并通过通信装置120将其发送到下一个客户机设备12。然后,控制客户机软件和/或固件32指示下一个客户机设备12的公共密钥信息基础设施42从发送信息中接收和解密MP3音频文件及其相关的允许和/或权利,并将其电子复制件放置在随机存取存储器82中。在从存储器101移动MP3音频文件到存储器102的情况下,一旦由下

一个客户机设备12将MP3音频文件接收到随机存取存储器82中，则下一个客户机设备12的控制客户机软件和/或固件32自动指示客户机设备11的控制客户机软件和/或固件31去指示客户机设备11的操作系统61和/或加密文件系统51删除存储器101或随机存取存储器81中的MP3音频文件的所有复制件。然后，控制客户机软件和/或固件31指示操作系统61重新建立客户机设备11的用户干预。然后控制客户机软件和/或固件32自动指示下一个客户机设备12的操作系统62的加密文件系统52利用从客户机设备11发送的相关的允许和/或权利对来自随机存取存储器82的所述MP3音频文件的电子复制件进行加密并保存到存储器102中，然后从随机存取存储器82中擦除MP3音频文件的所有电子复制件。然后，控制客户机软件和/或固件32指示操作系统62重新建立下一个客户机设备12的用户干预。此时，控制客户机软件和/或固件32已完成其用于存储处理的发送及加密部分且与控制客户机软件和/或固件32有关的程序结束。下一个客户机设备12此时能够播放MP3音频文件，然而，在本例中，客户机设备11的用户不能播放MP3音频文件，因为该文件被“移动”，并且在“移动”处理期间，在“移动”处理结束时从客户机设备11删除了MP3的所有复制件。此外，由于MP3音频文件已由加密文件系统51加密以用在下一个客户机设备12上，传统的对MP3音频文件的移动或复制不会被加密文件系统51授权，只有采用控制客户机软件和/或固件32的MP3音频文件的移动或复制才会被加密文件系统51授权。

本文中的“装置或机构”指35 U.S.C.部分112的第6段。“装置或机构”中的术语“装置”涉及35 U.S.C.部分112的第6段，但“装置或机构”中的术语“机构”不涉及35 U.S.C.部分112的第6段。

尽管在上面的实施例中为示例目的详细描述了本发明，但应当理解，这些细节仅仅是为所述示例目的，本领域普通技术人员在不脱离由所附权利要求书所描述的本发明的精神和范围的情况下，可对本发明做出多种变化。

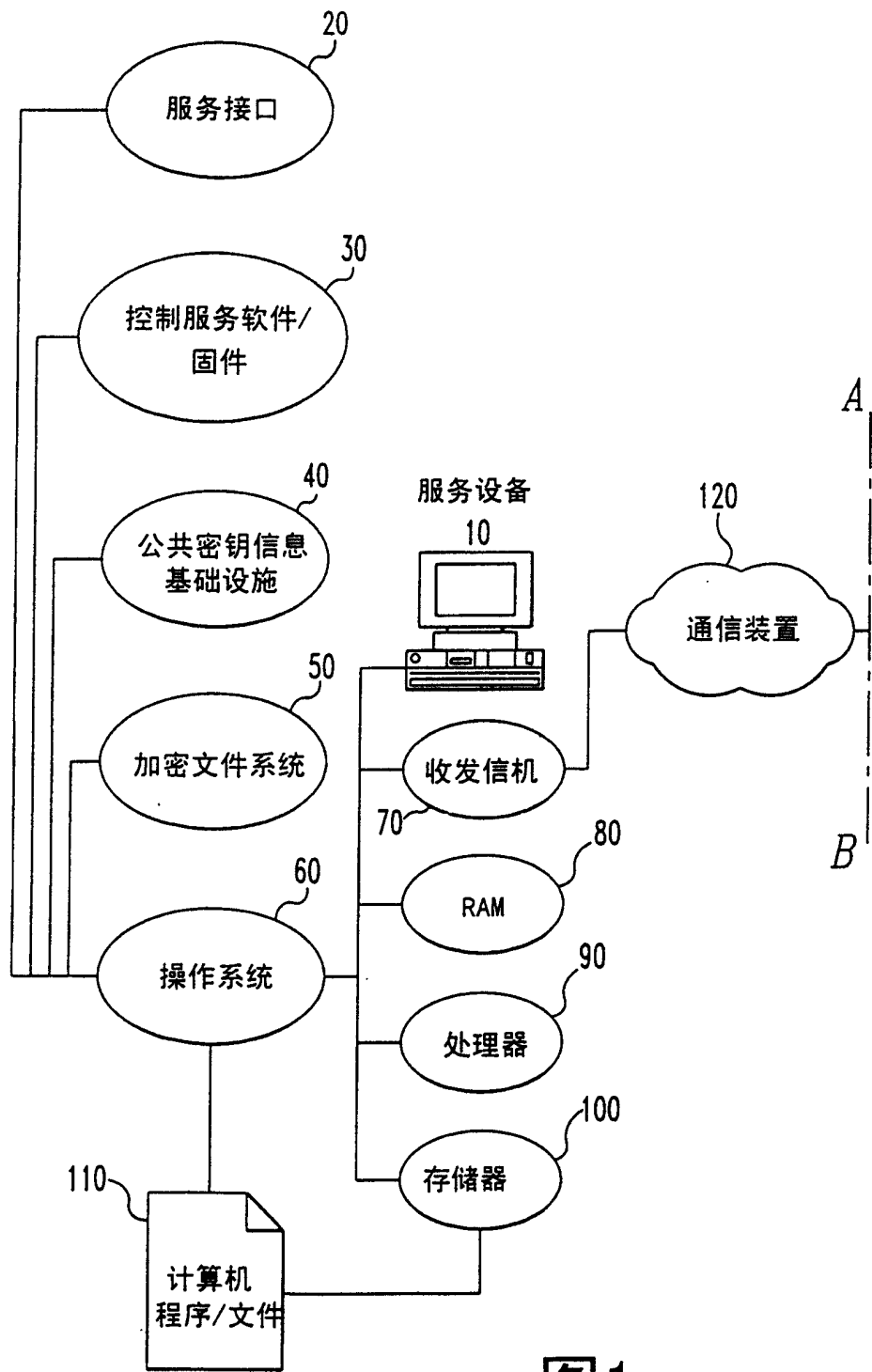


图1a

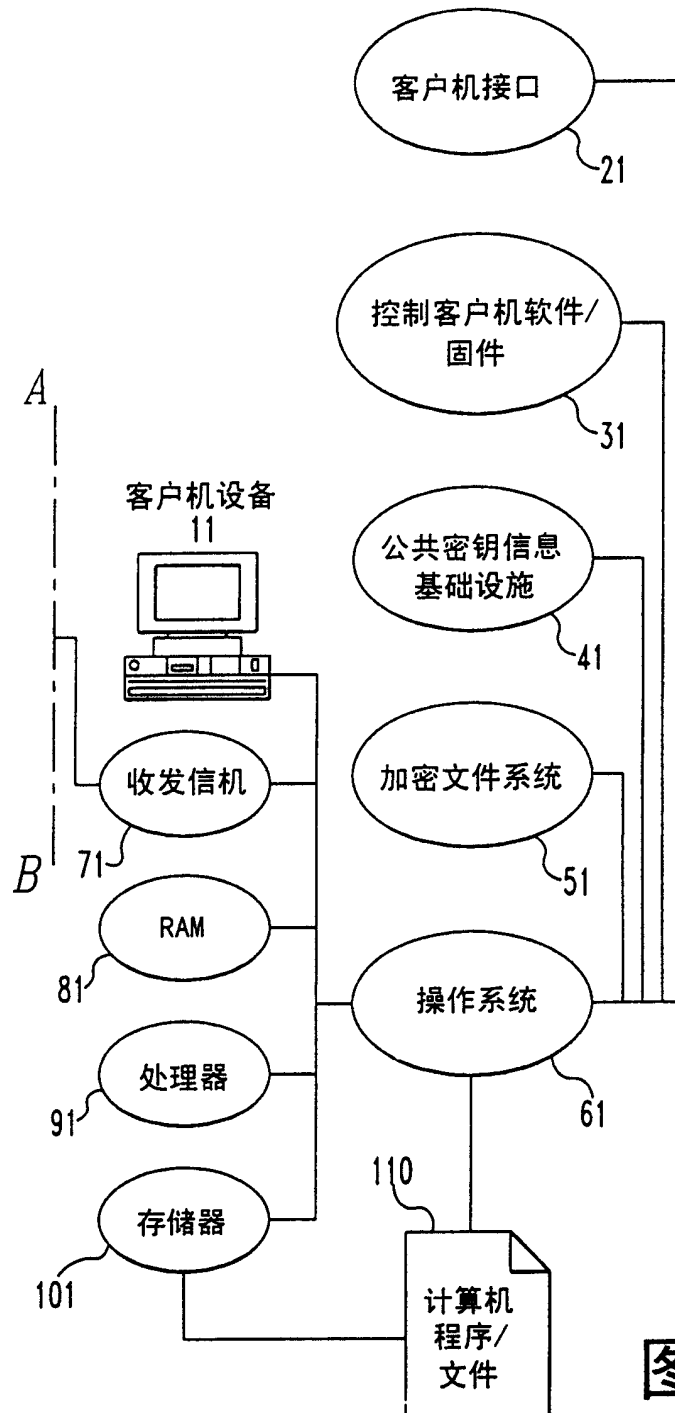


图1b

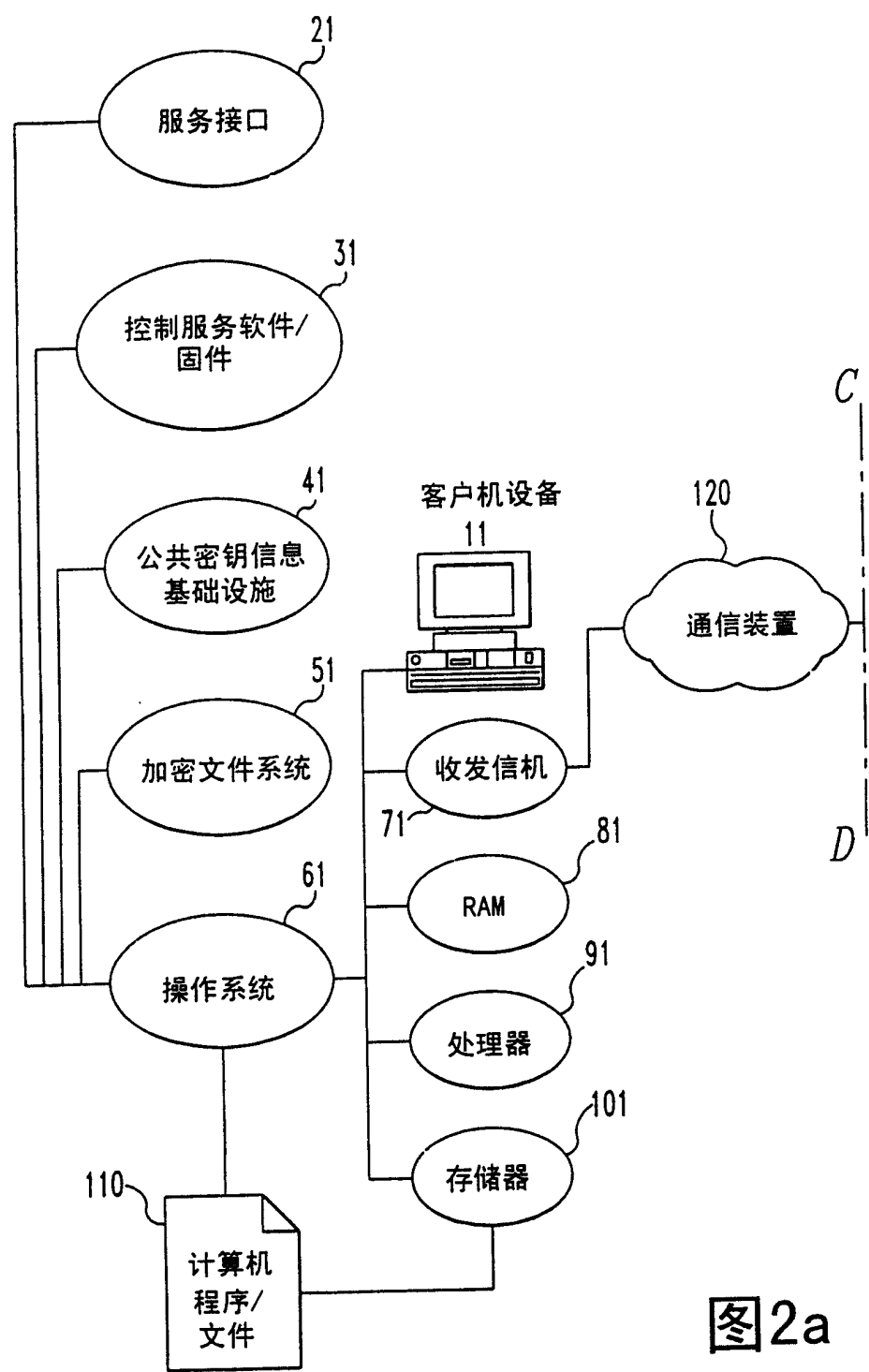


图2a

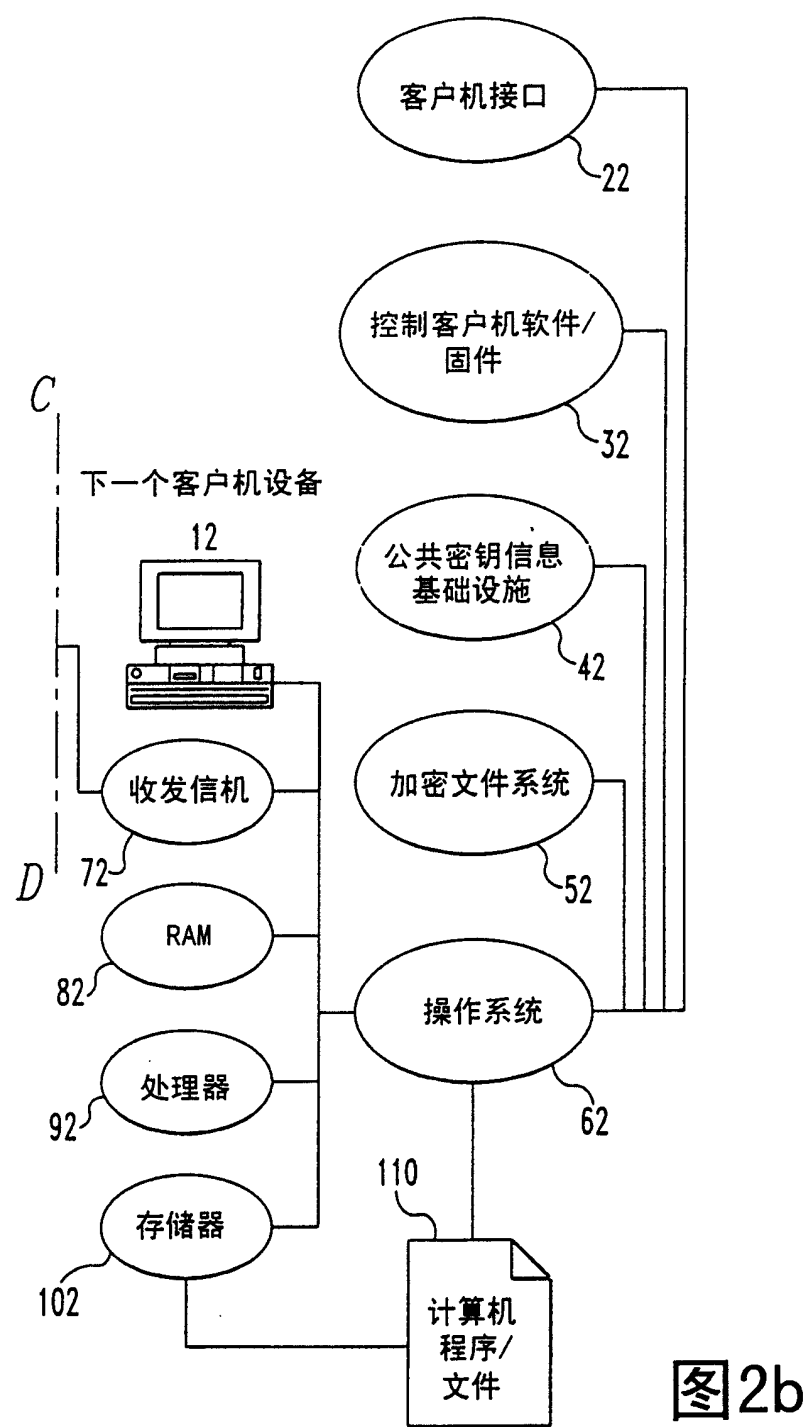
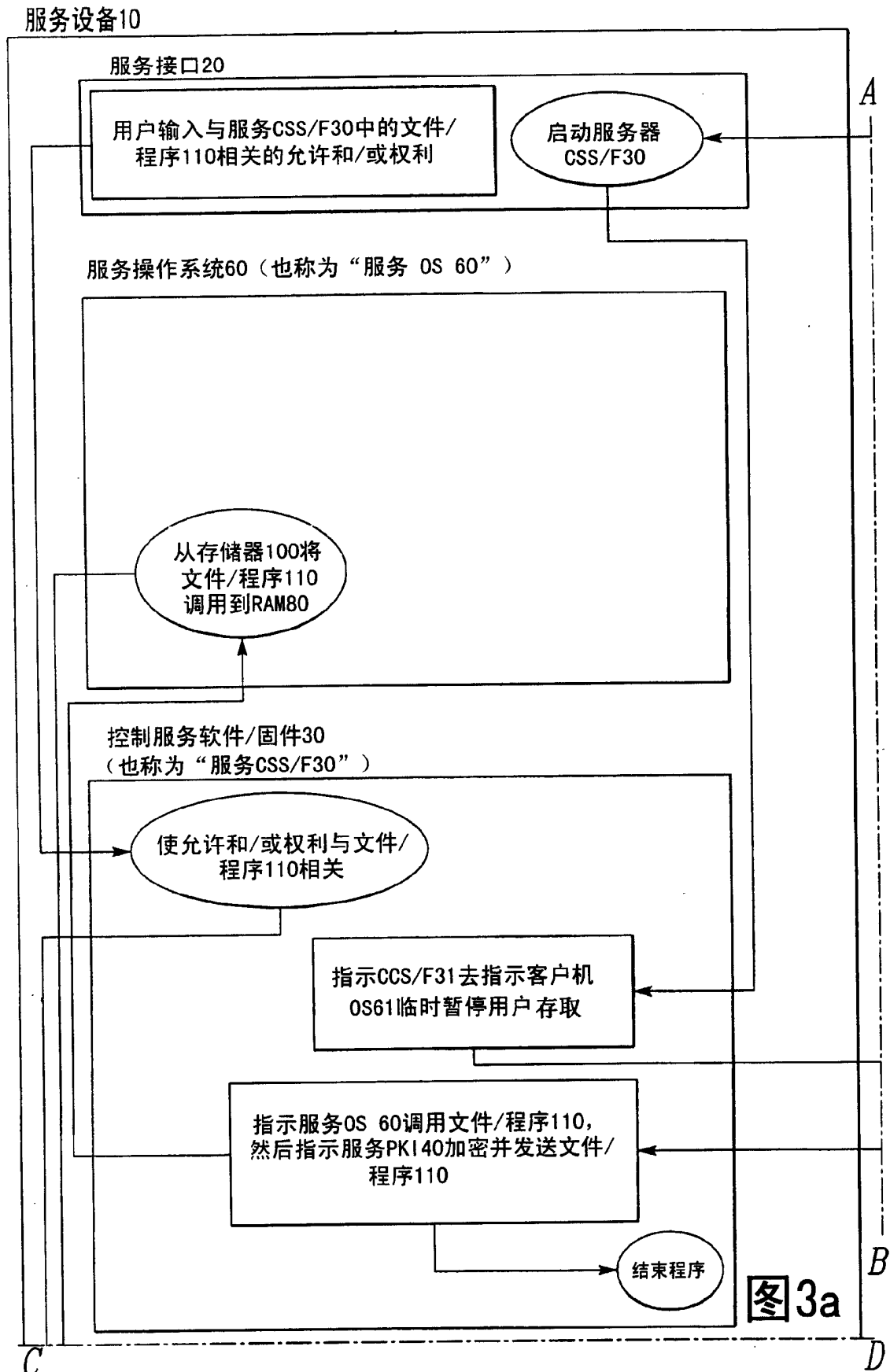


图2b



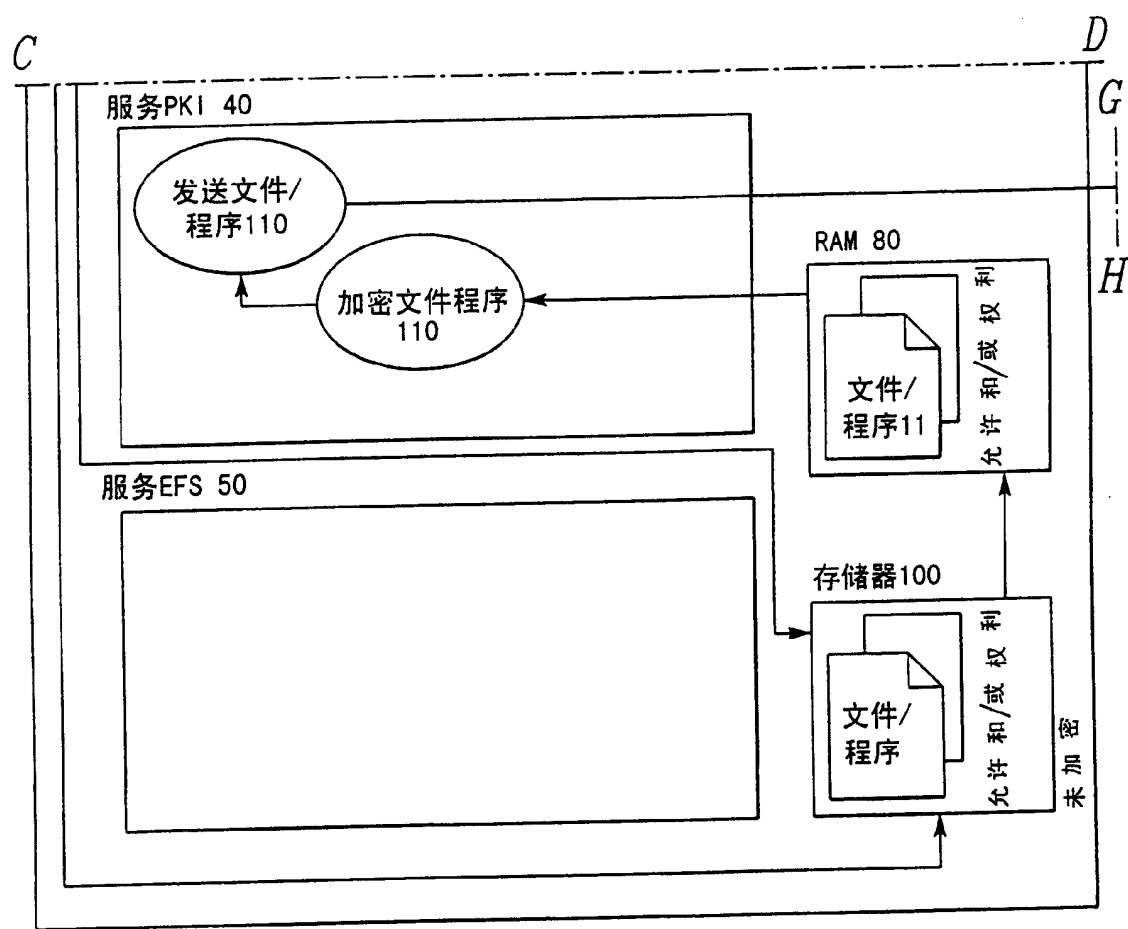
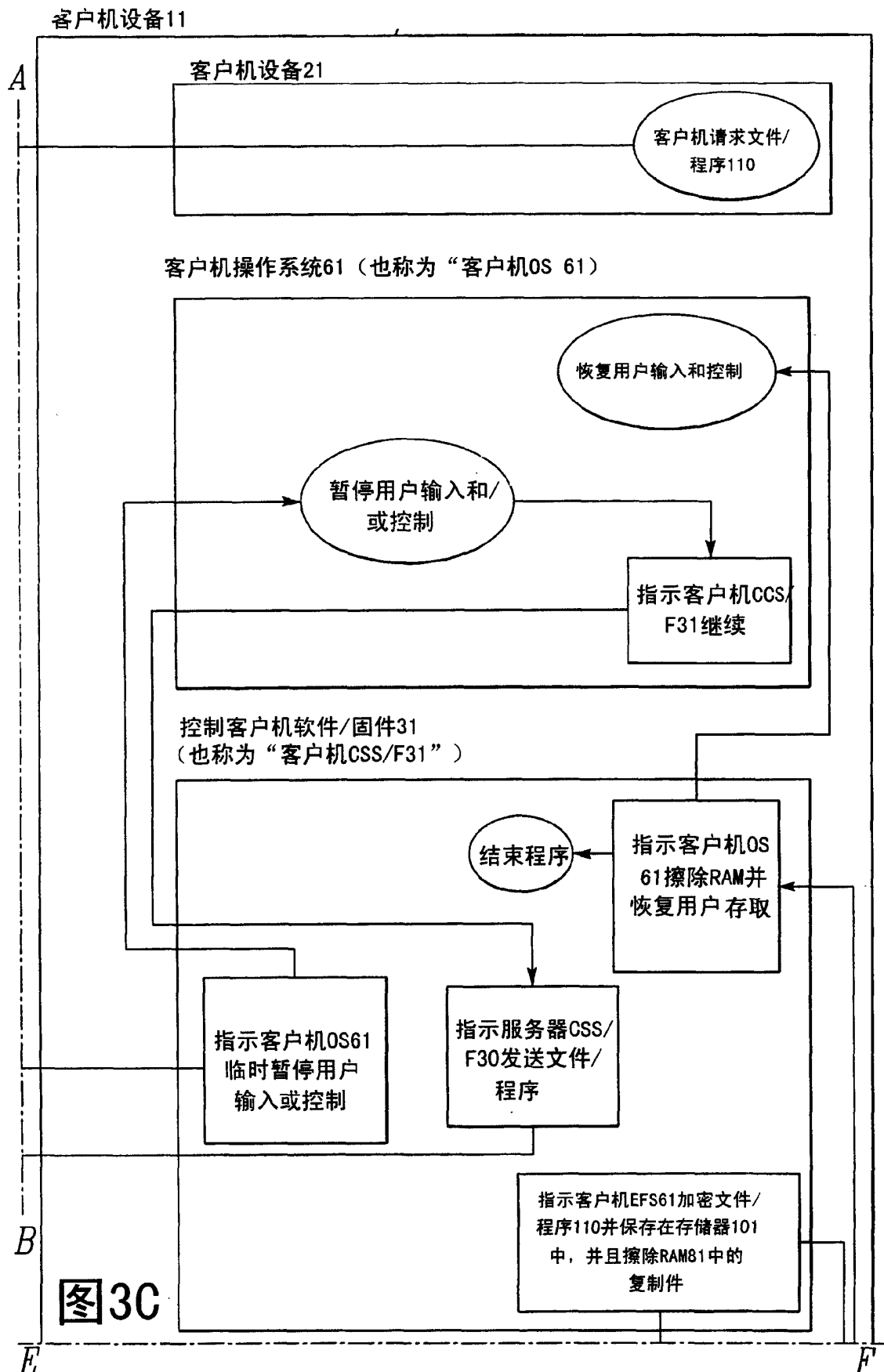


图3b



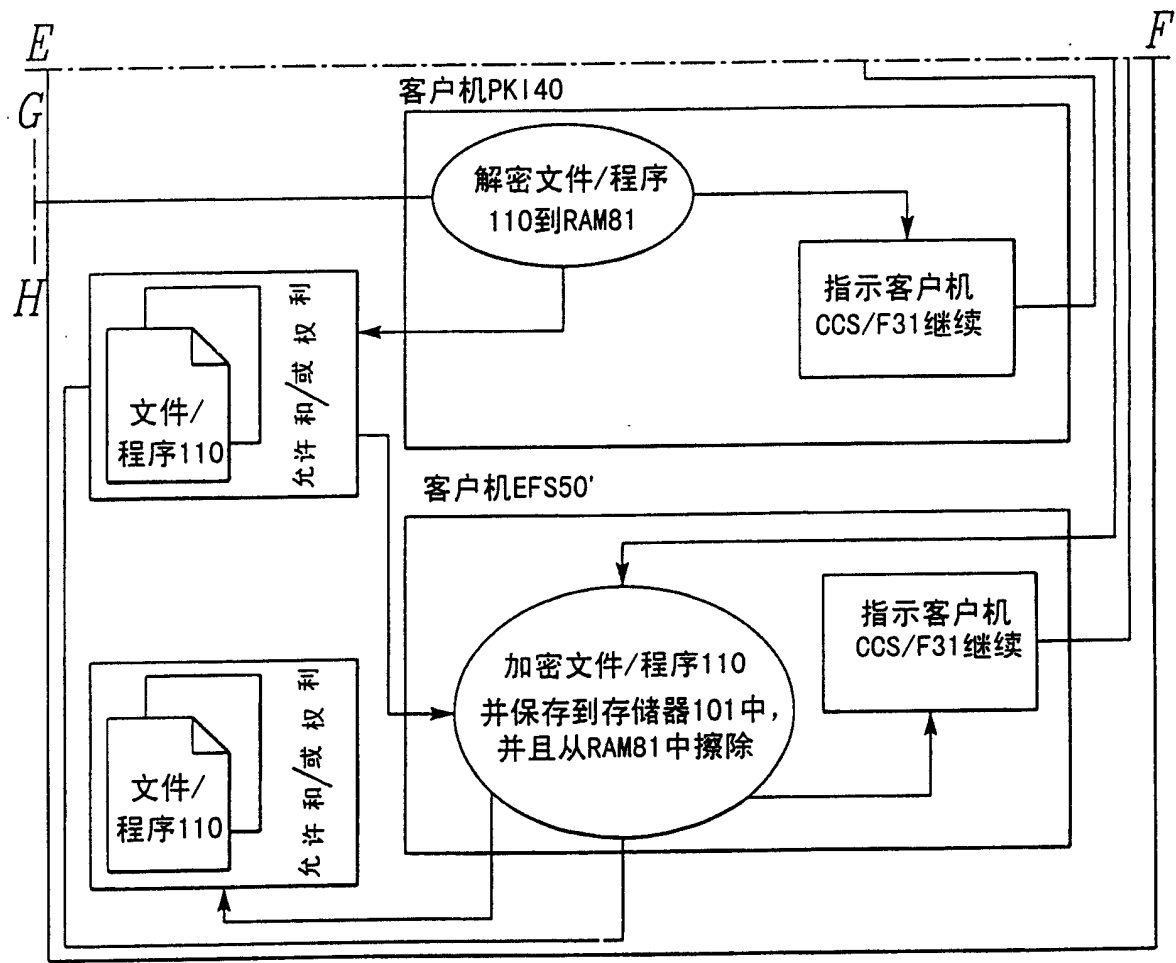
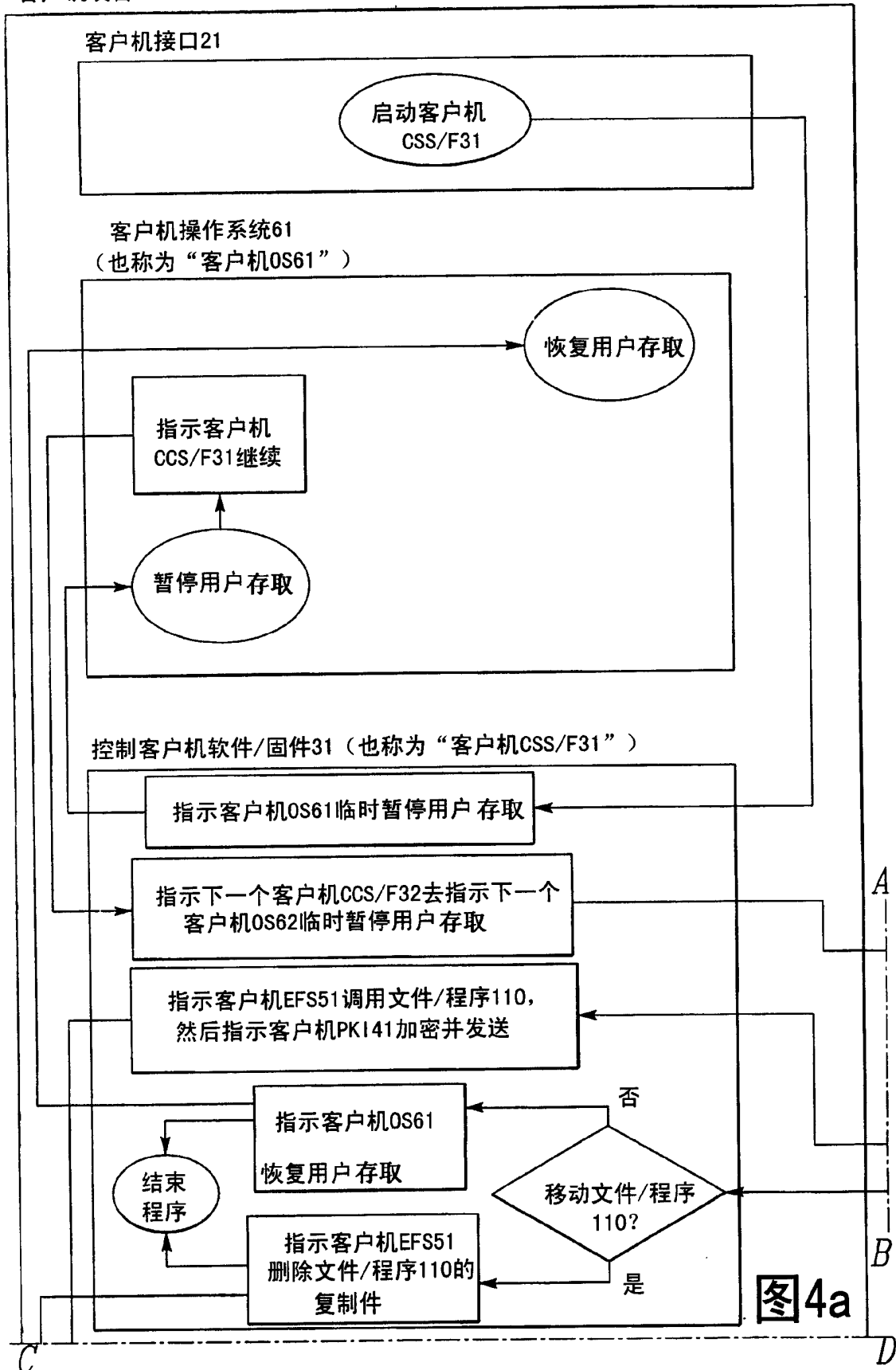


图3d

客户机设备11



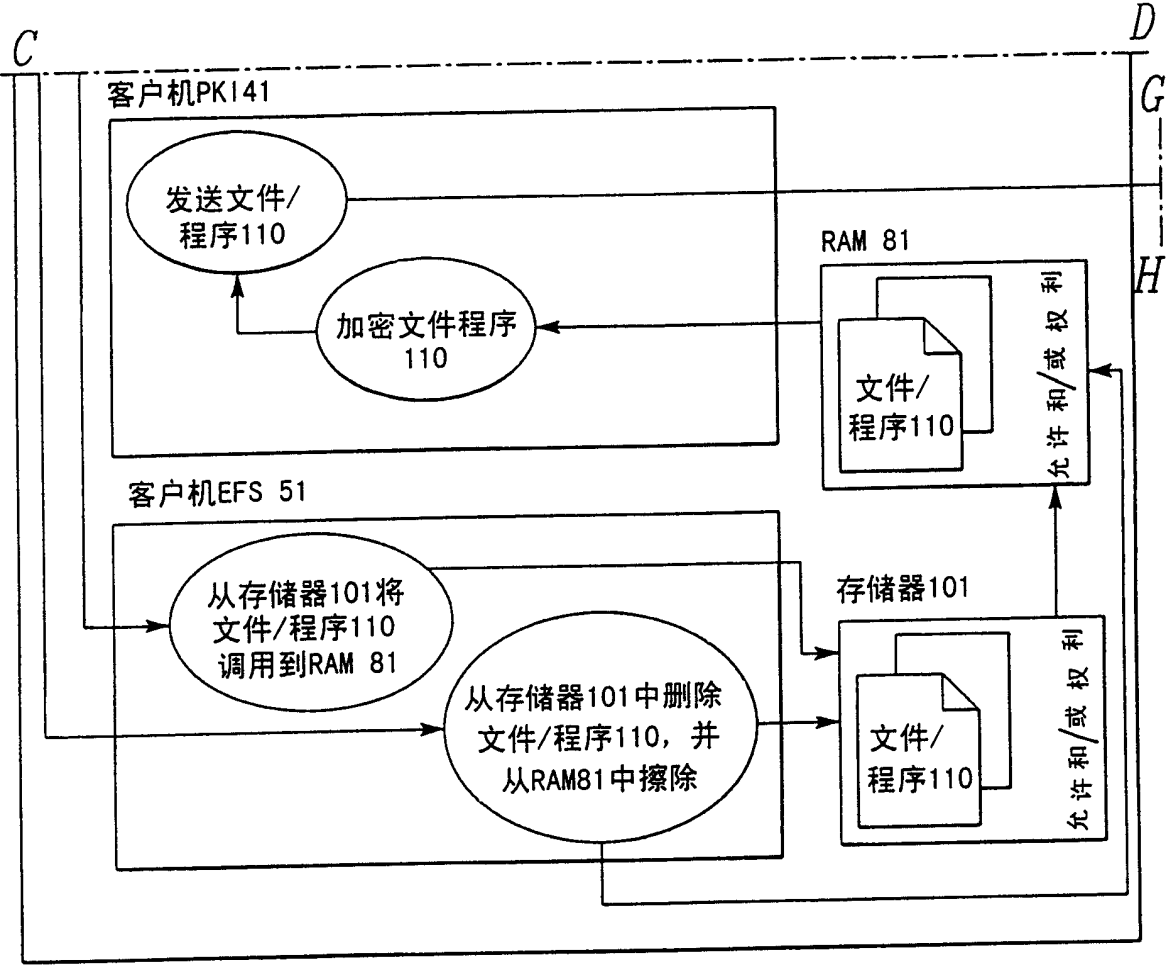
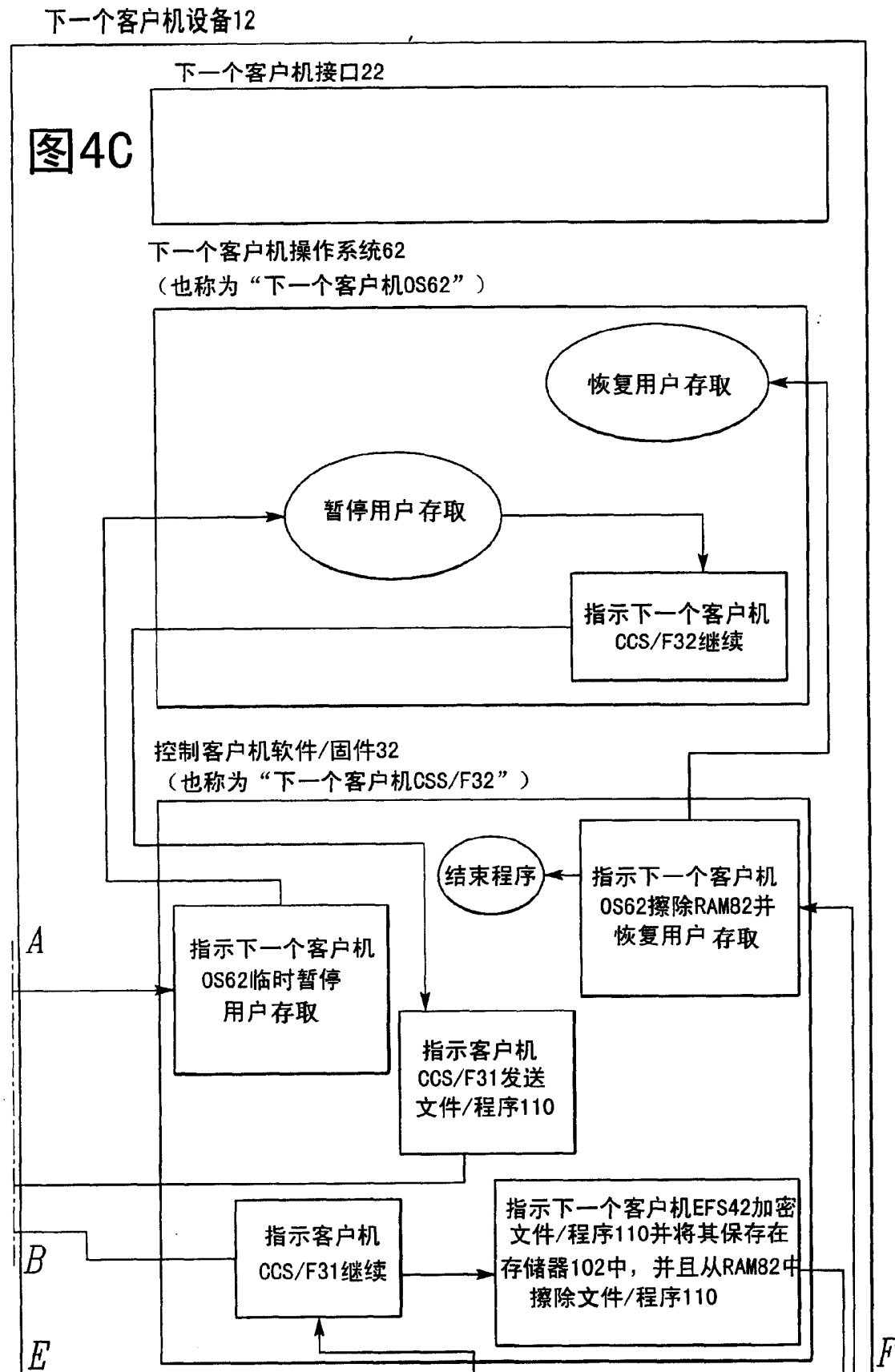


图4b



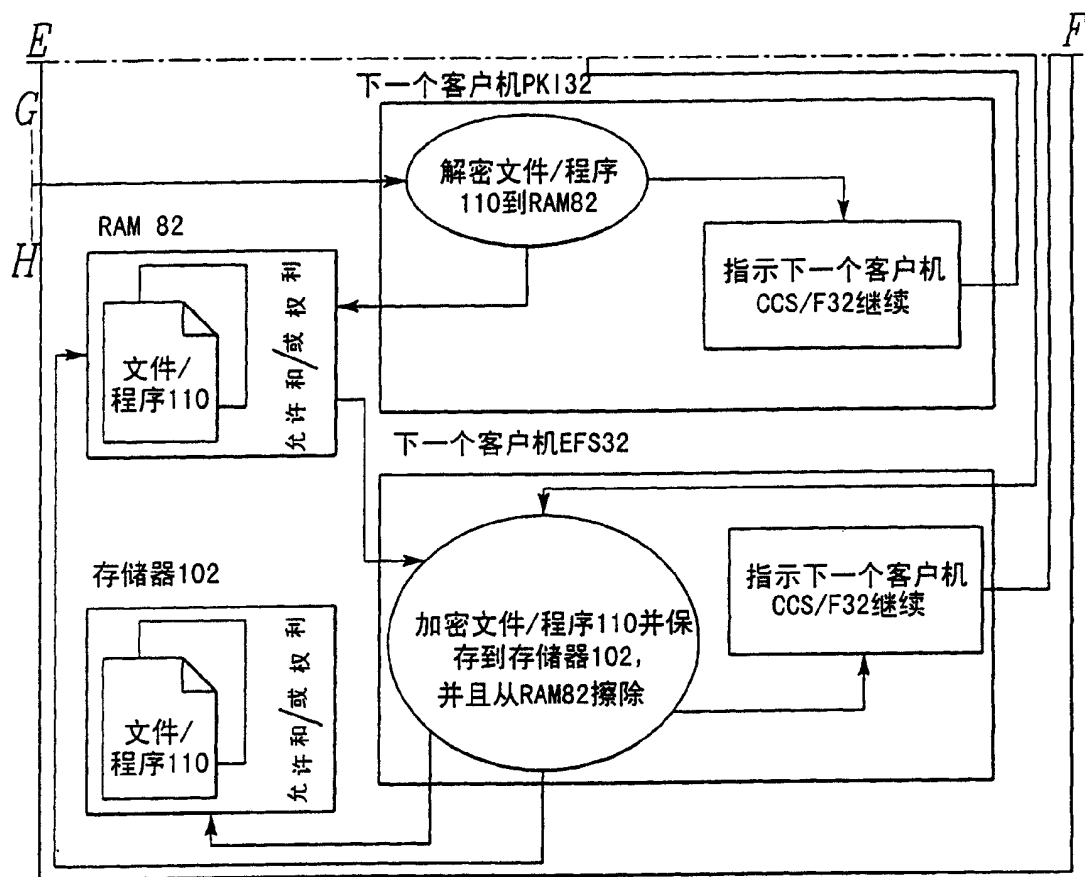


图4d