(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102291715 A
(43)申请公布日 2011.12.21

(21)申请号 201010203847.1

(22)申请日 2010.06.18

(71)申请人 黄金富
地址 100035 北京市西城区桦皮厂胡同 2 号国际商会大厦 16 层

(72)发明人 黄金富

(51)Int.Cl.
H04W 12/02(2009.01)
H04W 12/06(2009.01)
H04W 88/02(2009.01)

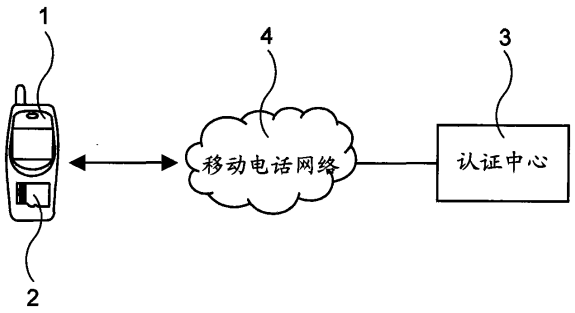
权利要求书 3 页 说明书 5 页 附图 1 页

(54)发明名称

保护手机内个人资料的方法和相应系统

(57)摘要

一种保护手机内个人资料的方法和相应系统，包括认证中心(3)、用户手机(1)及SD卡(2)，认证中心(3)设有各用户的认证帐户，认证帐户记录有用户手机(1)电话号码和SD卡(2)序列号及用于加密和解密的密码；SD卡(2)置于手机(1)内，并以密码加密，储存有用户的电话簿、短信息、电邮、备忘录、行事历、照片、影片等个人资料；手机(1)设有保安程式，保安程式于手机(1)启动接入移动电话网络(4)后，与认证中心(3)进行认证，认证成功后认证中心(3)才将密码传送给保安程式，由保安程式使用该密码将SD卡(2)解密，让用户可以通过手机(1)访问该SD卡(2)内所储存的个人资料。



CN 102291715 A

1. 一种保护手机内个人资料的系统，其特征在于，所述的系统包括认证中心 (3)、各用户的手机 (1) 及 SD 卡 (2)，

其中，

所述的认证中心 (3) 设有各用户的认证帐户，每一认证帐户记录有该认证帐户的用户的手机 (1) 电话号码和 SD 卡 (2) 序列号及用于将 SD 卡 (2) 加密和解密的密码；

所述的 SD 卡 (2) 置于用户的手机 (1) 内，储存有用户的个人资料，并使用用户的认证帐户的密码将该 SD 卡 (2) 加密；

所述的手机 (1) 设有用于控制 SD 卡 (2) 内容安全的保安程式；

以及，

手机 (1) 通过移动电话网络 (4) 与认证中心 (3) 相通讯，手机 (1) 内的保安程式于手机 (1) 启动接入移动电话网络 (4) 后，与认证中心 (3) 进行认证，认证成功后认证中心 (3) 才将该手机 (1) 的认证帐户的密码传送给保安程式，由保安程式使用该密码将 SD 卡 (2) 解密，让用户可以通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料。

2. 如权利要求 1 所述的保护手机内个人资料的系统，其特征在于，所述的认证帐户还设有确认码。

3. 一种保护手机内个人资料的方法，其特征在于，所述的方法包括如下步骤：

●每次手机 (1) 启动并接入移动电话网络 (4) 后，手机 (1) 内的保安程式读取手机 (1) 内的 SD 卡 (2) 的序列号，然后将包含该序列号的请求认证信息通过手机 (1) 及移动电话网络 (4) 传送到认证中心 (3)；

●认证中心 (3) 从信息的来源电话号码或信息内容的序列号找出对应的认证帐户，核对该来源电话号码和该序列号与该认证帐户的电话号码和序列号一致无误后，将该认证帐户的密码传回给手机 (1)，由保安程式使用该密码将手机内的 SD 卡 (2) 解密，让用户可以通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料。

4. 如权利要求 3 所述的保护手机内个人资料的方法，其特征在于，所述的认证帐户还设有一确认码，所述的方法还包括保安程式将请求认证信息传送到认证中心 (3) 前，通过手机 (1) 键盘接收用户输入确认码，以及，所述的请求认证信息内容还包含有该确认码，以及，认证中心 (3) 将认证帐户内的密码传送给手机 (1) 前，还核对请求认证信息内的确认码与对应的认证帐户的确认码是否一致无误，只有核对一致无误后认证中心 (3) 才将认证帐户的密码传送给手机 (1)。

5. 如权利要求 3 所述的保护手机内个人资料的方法，其特征在于，所述的方法还包括遥控删除 SD 卡 (2) 内容的步骤，是用户遗失 SD 卡 (2) 后，向认证中心 (3) 挂失其 SD 卡 (2)，当认证中心 (3) 接收到包含该 SD 卡 (2) 序列号的请求认证信息时，认证中心 (3) 操控手机 (1) 删除 SD 卡 (2) 内所储存的个人资料的步骤，具体的步骤如下：

●用户向认证中心 (3) 挂失其 SD 卡 (2)，认证中心 (3) 将该 SD 卡 (2) 的序列号列入黑名单中；

●当认证中心 (3) 收到包含有黑名单内任一序列号的请求认证信息时，认证中心 (3) 立即向该手机 (1) 发出删除资料指令；

●发出该请求认证信息的手机 (1) 内的保安程式收到该删除资料指令后，将 SD 卡 (2) 内所储存的个人资料删除，以保障个人该资料不会泄露。

6. 如权利要求 3 所述的保护手机内个人资料的方法，其特征在于，所述的方法还包括遥控删除 SD 卡 (2) 内容的步骤，是用户遗失 SD 卡 (2)，向认证中心 (3) 挂失其 SD 卡 (2) 后，由认证中心 (3) 操控手机 (1) 删除 SD 卡 (2) 内所储存的个人资料的步骤，具体的步骤如下：

●用户向认证中心 (3) 挂失其 SD 卡 (2)；

●认证中心 (3) 立即向用户的手机 (1) 发出删除资料指令；

●用户手机 (1) 内的保安程式收到该删除资料指令后，将用户手机 (1) 内的 SD 卡 (2) 内所储存的个人资料删除，以保障该个人资料不会泄露。

7. 如权利要求 3 所述的保护手机内个人资料的方法，其特征在于，所述的认证帐户还设有一确认码，所述的方法还包括用户将其 SD 卡 (2) 加密的步骤，具体的步骤如下：

●用户使用内置 SD 卡 (2) 的手机 (1)，通过手机 (1) 的保安程式输入确认码，然后保安程式将包含该确认码和 SD 卡 (2) 序列号内容的请求加密信息通过移动电话网络 (4) 传送到认证中心 (3)；

●认证中心 (3) 从信息的内容找出确认码和序列号，从信息的来源电话号码或该序列号找出对应的认证帐户，核对该来源电话号码和该序列号及该确认码与该认证帐户的电话号码和序列号及确认码均一致无误后，将包含有该认证帐户的密码的加密指令通过移动电话网络 (4) 传送给该手机 (1)；

●手机 (1) 接收到该加密指令后，由保安程式使用该密码将手机内的 SD 卡 (2) 加密，以保护该 SD 卡 (2) 内所储存的个人资料。

8. 如权利要求 3 所述的保护手机内个人资料的方法，其特征在于，所述的认证帐户还设有一确认码，所述的方法还包括用户撤消其 SD 卡 (2) 加密的步骤，具体的步骤如下：

●用户使用内置 SD 卡 (2) 的手机 (1)，通过手机 (1) 的保安程式输入确认码，然后保安程式将包含该确认码和 SD 卡 (2) 序列号内容的请求撤消加密信息通过移动电话网络 (4) 传送到认证中心 (3)；

●认证中心 (3) 从信息的内容找出确认码和序列号，从信息的来源电话号码或该序列号找出对应的认证帐户，核对该来源电话号码和该序列号及该确认码与该认证帐户的电话号码和序列号及确认码均一致无误后，将包含有该认证帐户的密码的撤消加密指令通过移动电话网络 (4) 传送给该手机 (1)；

●手机 (1) 接收到该撤消加密指令后，由保安程式使用该密码将手机内的 SD 卡 (2) 撤消加密，让该 SD 卡 (2) 内所储存的个人资料可以随意被访问。

9. 如权利要求 3 所述的保护手机内个人资料的方法，其特征在于，所述的认证帐户还设有一确认码，所述的方法还包括用户将 SD 卡 (2) 用于不同电话号码的手机 (1) 时，认证中心 (3) 验证用户身份的步骤，具体的步骤如下：

●手机 (1) 启动并接入移动电话网络 (4) 后，手机 (1) 内的保安程式读取手机 (1) 内的 SD 卡 (2) 的序列号，然后将包含该序列号的请求认证信息通过手机 (1) 及移动电话网络 (4) 传送到认证中心 (3)；

●认证中心 (3) 从信息内容的序列号找出对应的认证帐户，核对该信息的来源电话号码与该认证帐户的电话号码发现两者不相同后，通过移动电话网络 (4) 向手机 (1) 内的保安程式发出请求确认信息；

●手机 (1) 内的保安程式接收到该请求确认信息后，显示提示信息，请用户在手机 (1) 输入确认码，用户核对无误后在手机上输入确认码 ；

●手机 (1) 内的保安程式将该确认码通过手机 (1) 及移动电话网络 (4) 传送到认证中心 (3) ；

●认证中心 (3) 核对该确认码与该认证帐户的确认码一致无误后，将该认证帐户的密码传回给手机 (1)，由保安程式使用该密码将手机内的 SD 卡 (2) 解密，让用户可以通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料。

10. 如权利要求 3 所述的保护手机内个人资料的方法，其特征在于，所述的认证帐户还设有一确认码，所述的方法还包括用户通过遥控方式禁止访问 SD 卡 (2) 内容的步骤，具体的步骤如下 ：

●用户向认证中心 (3) 请求临时暂停其认证帐户，认证中心 (3) 根据用户的请求暂停该用户的认证帐户 ；

●认证中心 (3) 立即向该认证帐户的电话号码的手机 (1) 发出暂停指令 ；

●该手机 (1) 内的保安程式收到该暂停指令后，取消手机 (1) 内 SD 卡 (2) 的解密状态，使该 SD 卡 (2) 回复式加密状态，使不能通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料。

保护手机内个人资料的方法和相应系统

【技术领域】

[0001] 本发明涉及个人资料保安技术，特别是涉及一种保护手机内个人资料的方法和相应系统。

【背景技术】

[0002] 一般的手机通常设有包括电话簿，部分人还会将短信息、电邮、备忘录、行事历、照片、影片等个人资料储存于手机内。如果遗失了手机，这些电话簿、电邮、备忘录、行事历、照片、影片等个人资料就可能会外泄，给用户造成损害。如何保护手机内的个人资料的安全，是一个有待解决的问题。

【发明内容】

[0003] 本发明的目的，在于提供一种保护手机内个人资料的方法和相应系统，以实现保护手机内的个人资料安全的应用。

[0004] 本发明的目的是这样实现的，采用这样一种保护手机内个人资料的系统，其特征在于，所述的系统包括认证中心 (3)、各用户的手机 (1) 及 SD 卡 (2)，其中，所述的认证中心 (3) 设有各用户的认证帐户，每一认证帐户记录有该认证帐户的用户的手机 (1) 电话号码和 SD 卡 (2) 序列号及用于将 SD 卡 (2) 加密和解密的密码；所述的 SD 卡 (2) 置于用户的手机 (1) 内，储存有用户的个人资料，包括电话簿、短信息、电邮、备忘录、行事历、照片、影片等等个人资料，并使用用户的认证帐户的密码将该 SD 卡 (2) 加密；所述的手机 (1) 设有用于控制 SD 卡 (2) 内容安全的保安程式；以及，手机 (1) 通过移动电话网络 (4) 与认证中心 (3) 相通讯，手机 (1) 内的保安程式于手机 (1) 启动接入移动电话网络 (4) 后，与认证中心 (3) 进行认证，认证成功后认证中心 (3) 才将该手机 (1) 的认证帐户的密码传送给保安程式，由保安程式使用该密码将 SD 卡 (2) 解密，让用户可以通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料。

[0005] 以及，采用这样一种保护手机内个人资料的方法，其特征在于，所述的方法包括如下步骤：

[0006] ●将用于手机 (1) 的用户个人资料储存在用户的 SD 卡 (2) 内，并使用密码将该 SD 卡 (2) 加密；

[0007] ●在用户的手机 (1) 上设置用于控制 SD 卡 (2) 内容安全的保安程式，并将用户的 SD 卡 (2) 设置于手机 (1) 内；

[0008] ●用户在认证中心 (3) 开设一认证帐户，将用户的手机 (1) 电话号码和 SD 卡 (2) 的序列号及密码登记到该认证帐户中；

[0009] 以及，

[0010] ●每次手机 (1) 启动并接入移动电话网络 (4) 后，手机 (1) 内的保安程式读取手机 (1) 内的 SD 卡 (2) 的序列号，然后将包含该序列号的请求认证信息通过手机 (1) 及移动电话网络 (4) 传送到认证中心 (3)；

[0011] ●认证中心 (3) 从信息的来源电话号码或信息内容的序列号找出对应的认证帐户，核对该来源电话号码和该序列号与该认证帐户的电话号码和序列号一致无误后，将该认证帐户的密码传回给手机 (1)，由保安程式使用该密码将手机内的 SD 卡 (2) 解密，让用户可以通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料。

[0012] 以上是用户在正常状况下使用手机 (1) 时，手机 (1) 内的保安程式将 SD 卡 (2) 解密，让用户可以通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料的步骤。当用户遗失 SD 卡 (2) 时，可以向认证中心 (3) 挂失其 SD 卡 (2)，然后暂停用户的认证帐户。当手机 (1) 向认证中心 (3) 发出请求认证信息时，由于用户的认证帐户已经暂停，认证中心 (3) 就不会将密码传给手机 (1)，使手机 (1) 无法将 SD 卡 (2) 解密，保障了 SD 卡 (2) 内所储存的个人资料的安全。

[0013] 这样就实现了本发明的目的。

[0014] 本发明的保护手机内个人资料的方法和相应系统，由认证中心 (3) 控制是否允许访问手机 (1) 内的个人资料，当用户遗失手机 (1) 时，就可以立即向认证中心 (3) 挂失手机 (1)，以防止其他人访问该手机 (1) 内的 SD 卡 (2) 所储存的个人资料，从而保障个人资料的安全。

【附图说明】

[0015] 图 1 是本发明的保护手机内个人资料的系统的示意说明图；

[0016] 图中，相同的数字代表相同的装置、部件器件附图是示意性的，用以说明本发明的系统的主要特征。

【具体实施方式】

[0017] 下面结合附图，对本发明的方法作进一步详细说明。

[0018] 参阅图 1，图 1 是本发明的保护手机内个人资料的系统的示意说明图，图 1 中示出的系统包括认证中心 (3)、各用户的手机 (1) 及 SD 卡 (2)，其中，所述的认证中心 (3) 设有各用户的认证帐户，每一认证帐户记录有该认证帐户的用户的手机 (1) 电话号码和 SD 卡 (2) 序列号及用于将 SD 卡 (2) 加密和解密的密码；所述的 SD 卡 (2) 置于用户的手机 (1) 内，储存有用户的个人资料，包括电话簿、短信息、电邮、备忘录、行事历、照片、影片等等个人资料，并使用用户的认证帐户的密码将该 SD 卡 (2) 加密；所述的手机 (1) 设有用于控制 SD 卡 (2) 内容安全的保安程式；以及，手机 (1) 通过移动电话网络 (4) 与认证中心 (3) 相通讯，手机 (1) 内的保安程式于手机 (1) 启动接入移动电话网络 (4) 后，与认证中心 (3) 进行认证，认证成功后认证中心 (3) 才将该手机 (1) 的认证帐户的密码传送给保安程式，由保安程式使用该密码将 SD 卡 (2) 解密，让用户可以通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料。

[0019] 在设置方面，认证中心 (3) 设有与移动电话网络 (4) 相连线的设备，可以通过移动电话网络 (4) 与各用户的手机 (1) 通讯交换信息，例如可以采用 GPRS 通讯交换信息、或采用短信息等等之类不同方式交换信息。在用户方面，用户要在认证中心 (3) 开设一个认证帐户，将用户的手机 (1) 电话号码和 SD 卡 (2) 的序列号及密码登记到该认证帐户中，用户在其手机 (1) 上设置用于控制 SD 卡 (2) 内容安全的保安程式，及将用户的 SD 卡 (2) 设置

于手机 (1) 内，用户还要将原来储存于手机 (1) 内的个人资料，例如电话簿、短信息、电邮、备忘录、行事历、照片、影片等等个人资料，转移到 SD 卡 (2) 内，并使用用户在认证帐户登记的密码将该 SD 卡 (2) 加密，使 SD 卡 (2) 在没有密码的情况下，不可以被人访问其内容。此外，所述的密码可以由用户自己选定然后将密码登记到其认证帐户内，也可以由认证中心 (3) 采用随机方式产生，然后通过保安程式使用该密码将 SD 卡 (2) 加密。在本发明中，手机 (1) 内的保安程式可以通过手机 (1) 与认证中心 (3) 相通讯，并执行认证中心 (3) 发出的指令，将 SD 卡 (2) 进行加密、解密、删除内容等任务。

[0020] 在本发明中，所述的保护手机内个人资料的方法，包括如下步骤：

[0021] ●每次手机 (1) 启动并接入移动电话网络 (4) 后，手机 (1) 内的保安程式读取手机 (1) 内的 SD 卡 (2) 的序列号，然后将包含该序列号的请求认证信息通过手机 (1) 及移动电话网络 (4) 传送到认证中心 (3)；

[0022] ●认证中心 (3) 从信息的来源电话号码或信息内容的序列号找出对应的认证帐户，核对该来源电话号码和该序列号与该认证帐户的电话号码和序列号一致无误后，将该认证帐户的密码传回给手机 (1)，由保安程式使用该密码将手机内的 SD 卡 (2) 解密，让用户可以通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料。

[0023] 本发明的更进一步改进，是在认证帐户增设确认码，所述的确认码用于验证用户的身份，从而进行 SD 卡 (2) 的加密、解密、删除内容等操作。通过这改进，可以进一步加强本发明的方法的保安功效。即在本发明的保护手机内个人资料的方法中，保安程式将请求认证信息传送到认证中心 (3) 前，通过手机 (1) 键盘接收用户输入确认码，以及，所述的请求认证信息内容还包含有该确认码，以及，认证中心 (3) 将认证帐户内的密码传送给手机 (1) 前，还核对请求认证信息内的确认码与对应的认证帐户的确认码是否一致无误，只有核对一致无误后认证中心 (3) 才将认证帐户的密码传送给手机 (1)。

[0024] 当用户更换新的 SD 卡 (2) 时，可以通过确认码来验证用户的身份，然后才将新的 SD 卡 (2) 加密，以下是用户将其 SD 卡 (2) 加密的步骤，具体的步骤如下：

[0025] ●用户使用内置 SD 卡 (2) 的手机 (1)，通过手机 (1) 的保安程式输入确认码，然后保安程式将包含该确认码和 SD 卡 (2) 序列号内容的请求加密信息通过移动电话网络 (4) 传送到认证中心 (3)；

[0026] ●认证中心 (3) 从信息的内容找出确认码和序列号，从信息的来源电话号码或该序列号找出对应的认证帐户，核对该来源电话号码和该序列号及该确认码与该认证帐户的电话号码和序列号及确认码均一致无误后，将包含有该认证帐户的密码的加密指令通过移动电话网络 (4) 传送给该手机 (1)；

[0027] ●手机 (1) 接收到该加密指令后，由保安程式使用该密码将手机内的 SD 卡 (2) 加密，以保护该 SD 卡 (2) 内所储存的个人资料。此外，认证中心 (3) 更可于核对电话号码和序列号及确认码均一致无误后，随机产生一新密码，并将该密码替换认证帐户原来的密码，然后才将密码传送给手机 (1) 将 SD 卡 (2) 加密。

[0028] 用户更换新的 SD 卡 (2) 前，还可以撤消旧有的 SD 卡 (2) 的加密，使旧有的 SD 卡 (2) 可以用被其他手机 (1) 或计算机访问其内容。进行这撤消加密的步骤时，同样需要通过确认码来验证用户的身份，以下是用户撤消其 SD 卡 (2) 加密的步骤，具体的步骤如下：

[0029] ●用户使用内置 SD 卡 (2) 的手机 (1)，通过手机 (1) 的保安程式输入确认码，然后

保安程式将包含该确认码和 SD 卡 (2) 序列号内容的请求撤消加密信息通过移动电话网络 (4) 传送到认证中心 (3)；

[0030] ●认证中心 (3) 从信息的内容找出确认码和序列号，从信息的来源电话号码或该序列号找出对应的认证帐户，核对该来源电话号码和该序列号及该确认码与该认证帐户的电话号码和序列号及确认码均一致无误后，将包含有该认证帐户的密码的撤消加密指令通过移动电话网络 (4) 传送给该手机 (1)；

[0031] ●手机 (1) 接收到该撤消加密指令后，由保安程式使用该密码将手机内的 SD 卡 (2) 撤消加密，让该 SD 卡 (2) 内所储存的个人资料可以随意被访问。

[0032] 当用户的手机 (1) 损坏时，或用户的手机 (1) 没电时，可以将手机 (1) 内已加密的 SD 卡 (2) 转移到其他的手机 (1) 上使用，即用户将 SD 卡 (2) 用于不同电话号码的手机 (1) 时，认证中心 (3) 验证用户身份的步骤，具体的步骤如下：

[0033] ●手机 (1) 启动并接入移动电话网络 (4) 后，手机 (1) 内的保安程式读取手机 (1) 内的 SD 卡 (2) 的序列号，然后将包含该序列号的请求认证信息通过手机 (1) 及移动电话网络 (4) 传送到认证中心 (3)；

[0034] ●认证中心 (3) 从信息内容的序列号找出对应的认证帐户，核对该信息的来源电话号码与该认证帐户的电话号码发现两者不相同后，通过移动电话网络 (4) 向手机 (1) 内的保安程式发出请求确认信息；

[0035] ●手机 (1) 内的保安程式接收到该请求确认信息后，显示提示信息，请用户在手机 (1) 输入确认码，用户核对无误后在手机上输入确认码；

[0036] ●手机 (1) 内的保安程式将该确认码通过手机 (1) 及移动电话网络 (4) 传送到认证中心 (3)；

[0037] ●认证中心 (3) 核对该确认码与该认证帐户的确认码一致无误后，将该认证帐户的密码传回给手机 (1)，由保安程式使用该密码将手机内的 SD 卡 (2) 解密，让用户可以通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料。

[0038] 当用户忘记携带手机 (1) 时，例如将手机 (1) 还留在办公室，用户还可以临时暂停其认证帐户，以免 SD 卡 (2) 内容被其他人访问查看。进行这临时暂停认证帐户的步骤时，同样需要通过确认码来验证用户的身份，以下是用户通过遥控方式禁止访问 SD 卡 (2) 内容的步骤，具体的步骤如下：

[0039] ●用户向认证中心 (3) 请求临时暂停其认证帐户，认证中心 (3) 根据用户的请求暂停该用户的认证帐户；

[0040] ●认证中心 (3) 立即向该认证帐户的电话号码的手机 (1) 发出暂停指令；

[0041] ●该手机 (1) 内的保安程式收到该暂停指令后，取消手机 (1) 内 SD 卡 (2) 的解密状态，使该 SD 卡 (2) 回复式加密状态，使不能通过手机 (1) 访问该 SD 卡 (2) 内所储存的个人资料。

[0042] 本发明的保护手机内个人资料的方法中，除了采用上述的方法来保护个人资料外，还包括遥控删除 SD 卡 (2) 内容的步骤，是用户遗失 SD 卡 (2) 后，向认证中心 (3) 挂失其 SD 卡 (2)，当认证中心 (3) 接收到包含该 SD 卡 (2) 序列号的请求认证信息时，认证中心 (3) 操控手机 (1) 删除 SD 卡 (2) 内所储存的个人资料的步骤，具体的步骤如下：

[0043] ●用户向认证中心 (3) 挂失其 SD 卡 (2)，例如用户使用另一预先登记了电话号码

用于挂失的手机，拨打认证中心 (3) 的挂失热线，并在接通电话通话后输入其挂失的手机 (1) 电话号码或 SD 卡 (2) 的序列号，认证中心 (3) 核对来电的主叫方电话号码和挂失的手机 (1) 电话号码或 SD 卡 (2) 的序列号无误后，认证中心 (3) 将该 SD 卡 (2) 的序列号列入黑名单中；

[0044] ●当认证中心 (3) 收到包含有黑名单内任一序列号的请求认证信息时，认证中心 (3) 立即向该手机 (1) 发出删除资料指令；

[0045] ●发出该请求认证信息的手机 (1) 内的保安程式收到该删除资料指令后，将 SD 卡 (2) 内所储存的个人资料删除，以保障该个人资料不会泄露。

[0046] 当用户将手机 (1) 连同 SD 卡 (2) 一起遗失时，还可以在用户向认证中心 (3) 挂失其 SD 卡 (2) 后，由认证中心 (3) 操控手机 (1) 删除 SD 卡 (2) 内所储存的个人资料的步骤，具体的步骤如下：

[0047] ●用户向认证中心 (3) 挂失其 SD 卡 (2)，例如用户使用另一预先登记了电话号码用于挂失的手机，拨打认证中心 (3) 的挂失热线，并在接通电话通话后输入其挂失的手机 (1) 电话号码或 SD 卡 (2) 的序列号，认证中心 (3) 核对来电的主叫方电话号码和挂失的手机 (1) 电话号码或 SD 卡 (2) 的序列号无误后；

[0048] ●认证中心 (3) 立即向用户的手机 (1) 发出删除资料指令；

[0049] ●用户手机 (1) 内的保安程式收到该删除资料指令后，将用户手机 (1) 内的 SD 卡 (2) 内所储存的个人资料删除，以保障该个人资料不会泄露。

[0050] 在本说明书中，所述的 SD 卡 (2) 可以是如下的其中任一规格的记忆卡：

[0051] ● SD(Secure Digital) 卡；

[0052] ● miniSD(Mini Secure Digital) 卡；

[0053] ● mircoSD(Micro Secure Digital) 卡；

[0054] ● SDHC(Secure Digital High Capaciy) 卡；

[0055] ● miniSDHC(Mini Secure Digital High Capacity) 卡；

[0056] ● mircoSDHC(Micro Secure Digital High Capacity) 卡；

[0057] ● SDXC(Secure Digital eXtended Capacity) 卡；

[0058] ● miniSDXC(Mini Secure Digital eXtended Capacity) 卡；

[0059] ● mircoSDXC(Micro Secure Digital eXtended Capacity) 卡。

[0060] 无论采用以上任一规格的记忆卡作为本发明的 SD 卡 (2)，都可很好地实现本发明的目的，都是属于本发明的保护范围。

[0061] 以上已经详细说明了本发明的保护手机内个人资料的方法和相应系统，虽然本发明以上述的实施例加以说明，但是本发明并不仅限于此，在不离开本发明的精神和所附权利要求书的范围的情况下，可以作多种改变和变化。

[0062] 本发明的保护手机内个人资料的方法和相应系统，除了可以保障用户的个人资料的安全，更可以方便用户转换手机，只要将储存了个人资料的 SD 卡 (2) 插到新的手机 (1) 上，就可以通过新的手机 (1) 访问 SD 卡 (2) 内所储存的个人资料，例如电话簿、短信息、电邮、备忘录、行事历、照片、影片等等。本发明的实施，会为用户带来良好安全效益。

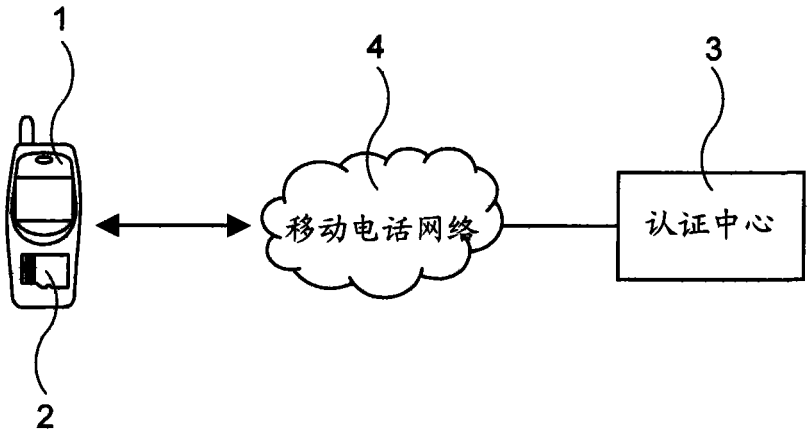


图 1