(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 101022613 B
(45)授权公告日 2010.05.12

(21)申请号 200610093507.1

(22)申请日 2006.06.23

(30)优先权数据
2006-036622 2006.02.14 JP

(73)专利权人 富士通株式会社
地址 日本神奈川县川崎市

(72)发明人 小野津崇之 箕轮雅春

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 黄纶伟

(51)Int.Cl.
H04W 8/24(2009.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)

(56)对比文件
CN 1407787 A,2003.04.02, 全文.
JP 特开2003-307061 A,2003.10.31, 全文.
JP 特开平11-275215 A,1999.10.08, 全文.
US 2005/0045731 A1,2005.03.03, 全文.

审查员 刘承恩

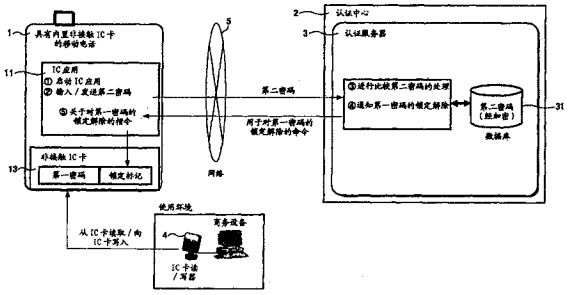
权利要求书 2 页 说明书 6 页 附图 4 页

(54)发明名称

移动通信设备、移动通信设备控制程序及移动通信设备控制方法

(57)摘要

移动通信设备、移动通信设备控制程序及移动通信设备控制方法。提供了一种移动通信设备，其具有如下功能：在非接触IC卡功能被具有内置该非接触IC卡的移动电话中的PIN认证错误锁定的情况下，能够通过除了PIN以外的认证密钥来解除对IC卡功能的锁定。当具有内置非接触IC的移动电话1中的PIN被锁定时，启动IC应用11以将除了PIN以外的第二密码发送到认证服务器3。认证服务器3将从移动电话1接收的第二密码与存储在数据库31中的另一第二密码相比较。如果这两个第二密码彼此一致，则将PIN锁定解除命令发送到移动电话1。此外，移动电话1通过所接收的命令将非接触IC卡13的锁定标记从开启切换到关闭。由此解除了IC卡功能的PIN锁定。



CN 101022613 B

1. 一种移动通信设备，使其靠近信息处理设备，以与该信息处理设备进行无线通信，所述移动通信设备包括：

锁定部分，如果所述移动通信设备的用户与所述信息处理设备进行无线通信以执行使用认证，并且如果该使用认证失败满足预定锁定条件，则其执行对关于使用认证的操作的锁定；

用户认证信息获得部分，如果通过所述锁定部分执行了所述锁定，则其获得用户认证信息作为关于对用户的认证的信息；

用户管理服务器无线通信部分，其将通过所述用户认证信息获得部分获得的用户认证信息无线地发送到用户管理服务器，并且无线地接收来自所述用户管理服务器的指令；以及

锁定解除部分，如果通过所述用户管理服务器无线通信部分无线地接收的指令是关于解除所述锁定的指令，则其解除所述锁定。

2. 根据权利要求 1 所述的移动通信设备，其中，所述锁定部分使用非接触 IC 卡的无线通信功能，并且所述信息处理设备使用所述非接触 IC 卡的读 / 写器的无线通信功能。

3. 根据权利要求 1 所述的移动通信设备，其中，所述用户管理服务器无线通信部分使用移动通信网络中的无线通信功能。

4. 根据权利要求 1 所述的移动通信设备，其中，基于来自用户的输入，所述用户认证信息获得部分获得与用于使用认证的第一密码不同的第二密码，并且将所获得的第二密码视为用户认证信息。

5. 根据权利要求 1 所述的移动通信设备，其中，所述用户认证信息获得部分获得用户的生物学信息，并且将根据所获得的生物学信息而计算出的信息视为用户认证信息。

6. 根据权利要求 4 所述的移动通信设备，其中，所述用户管理服务器将从所述用户管理服务器无线通信部分发送来的所述用户认证信息与事先登记的另一用户认证信息相比较，从而对用户进行认证，并且如果用户通过认证，则将关于解除所述锁定的指令发送到所述移动通信设备。

7. 根据权利要求 1 所述的移动通信设备，其中，基于来自用户的输入，所述用户认证信息获得部分获得与用于使用认证的第一密码不同的第二密码，将所获的第二密码与事先登记的另一第二密码相比较，从而对用户进行认证，并且如果用户通过认证，则将用户已经通过认证的事实视为用户认证信息。

8. 根据权利要求 1 所述的移动通信设备，其中，所述用户认证信息获得部分获得用户的生物学信息，将所获得的生物学信息与事先登记的其它用户生物学信息相比较，从而对用户进行认证，并且如果用户通过认证，则将用户已经通过认证的事实视为用户认证信息。

9. 根据权利要求 7 所述的移动通信设备，其中，所述用户管理服务器接收来自所述用户管理服务器无线通信部分的用户认证信息，并且如果对应于该用户认证信息的用户满足预定许可条件，则将关于解除所述锁定的指令发送到所述移动通信设备。

10. 根据权利要求 9 所述的移动通信设备，其中，所述预定许可条件是对应于用户认证信息的用户不是已经事先登记的并禁止对其解除锁定的用户。

11. 根据权利要求 1 所述的移动通信设备，其中，所述预定锁定条件是使用认证失败的次数达到预定值。

12. 一种控制移动通信设备的移动通信设备控制方法，使所述移动通信设备靠近信息处理设备，以与该信息处理设备进行无线通信，所述方法包括：

移动通信设备中的锁定步骤，如果所述移动通信设备的用户与所述信息处理设备进行无线通信以执行使用认证，并且如果使用认证失败满足预定锁定条件，则执行对关于使用认证的操作的锁定；

移动通信设备中的用户认证信息获得步骤，如果通过所述锁定步骤执行了所述锁定，则获得用户认证信息作为关于对用户的认证的信息；

移动通信设备中的用户认证信息发送步骤，其将通过所述用户认证信息获得步骤获得的用户认证信息无线地发送到所述用户管理服务器；

用户管理服务器中的移动通信设备指令发送步骤，其基于通过所述用户认证信息发送步骤无线地发送的信息，将指令发送到所述移动通信设备；

移动通信设备中的用户管理服务器无线接收步骤，其无线地接收通过所述移动通信设备指令发送步骤无线发送的指令；以及

移动通信设备中的锁定解除步骤，如果通过所述用户管理服务器无线接收步骤接收到关于解除所述锁定的指令，则解除所述锁定。

13. 根据权利要求 12 所述的移动通信设备控制方法，其中，锁定步骤使用非接触 IC 卡的无线通信功能，并且所述信息处理设备使用所述非接触 IC 卡的读 / 写器的无线通信功能。

14. 根据权利要求 12 所述的移动通信设备控制方法，其中，所述用户认证信息发送步骤、所述移动通信设备指令发送步骤以及所述用户管理服务器无线接收步骤使用移动通信网络中的无线通信功能。

15. 根据权利要求 12 所述的移动通信设备控制方法，其中，所述用户认证信息获得步骤基于来自用户的输入，获得与用于使用认证的第一密码不同的第二密码，并且将所获得的第二密码视为用户认证信息。

16. 根据权利要求 12 所述的移动通信设备控制方法，其中，所述用户认证信息获得步骤获得用户的生物学信息，并且将根据所获得的生物学信息而计算出的信息视为用户认证信息。

17. 根据权利要求 15 所述的移动通信设备控制方法，其中，所述移动通信设备指令发送步骤将通过所述用户认证信息发送步骤发送的用户认证信息与事先登记的用户认证信息相比较，由此对用户进行认证，并且如果用户通过认证，则将关于解除所述锁定的指令发送到所述移动通信设备。

18. 根据权利要求 12 所述的移动通信设备控制方法，其中，所述用户认证信息获得步骤基于来自用户的输入，获得与用于使用认证的第一密码不同的第二密码，将所获得的第二密码与事先登记的另一第二密码进行比较，由此对用户进行认证，并且如果用户通过认证，则将用户已经通过认证的事实视为用户认证信息。

19. 根据权利要求 12 所述的移动通信设备控制方法，其中所述用户认证信息获得步骤获得用户的生物学信息，将所获得的生物学信息与事先登记的其他用户生物学信息相比较，由此对用户进行认证，并且如果用户通过认证，则将用户已经通过认证的事实视为用户认证信息。

移动通信设备、移动通信设备控制程序及移动通信设备控制方法

技术领域

[0001] 本发明涉及诸如内置有非接触 IC 卡的移动电话的移动通信设备、移动通信设备控制程序以及移动通信设备控制方法。具体地，本发明涉及如下一种移动通信设备、移动通信设备控制程序以及移动通信设备控制方法，所述移动通信设备具有如下功能：当在使用非接触 IC 卡的情况下，在用于授权使用的密码被锁定时，解除对该密码的锁定。

背景技术

[0002] 存在一种常规非接触 IC 卡（以下在一些情况下将其简称为 IC 卡）或者一种其中内置有非接触 IC 卡的移动电话。还存在多种情况，例如：在购物时使用 IC 卡来利用信用卡支付奢侈品的情况，和出于商业目登录个人计算机（以下称为 PC）的情况。在这些情况下，如果错误地输入密码（PIN：个人识别码）达到特定次数（比如 3 次），则将 PIN 锁定并且禁止 IC 卡的使用。即，如果重复 PIN 认证错误，则保护起 IC 卡功能以便维持安全性。

[0003] 另选地，如果由于移动电话的用户的过失而无意地重复了 PIN 认证错误，并且如果 PIN 被锁定以保护 IC 卡功能，则移动电话的用户请求系统管理员解除该锁定，即解除该保护。

[0004] 已公开了一种用于通过使用移动电话解除 PIN 的锁定的技术，虽然公开的既不是非接触 IC 卡也不是具有内置非接触 IC 卡的移动电话。现在描述这种技术作为参考。例如，事先从用户标识模块将锁定解除码设置在移动电话中。在解除锁定的情况下，从移动电话向用户标识模块发送随机数。于是，用户标识模块利用所接收的随机数和锁定解除码来计算锁定解除计算值，并且将锁定解除计算值发送到移动电话。另一方面，仅当移动电话所接收的锁定解除计算值与该移动电话内部计算出的锁定解除计算值相一致时，该移动电话执行解锁（参见，例如日本专利申请特开平 11-275215 号公报，第 0019 到 0037 段，和图 1）。

[0005] 然而，如果在锁定了内置于移动电话中的非接触 IC 卡的 PIN 的情况下执行锁定解除（保护解除），则系统管理员在通过如下方式对请求锁定解除的客户进行识别之后，即通过会见或者电话呼叫来识别该客户是移动电话的真实用户还是“冒充”的恶意第三方之后，才解除 PIN 的锁定。然而，这种确认方法需要系统管理员的大量劳动和时间来解除 PIN 的锁定。

[0006] 根据上述特开平 11-275215 号公报的技术需要通过操作员的人工操作，并且因此需要系统管理员的大量劳动和时间。

发明内容

[0007] 提出本发明来解决上述问题，并且本发明的目的是提供一种移动通信设备、移动通信设备控制程序以及移动通信设备控制方法，其具有如下功能：如果在具有内置非接触 IC 卡的移动电话中，因 PIN 认证错误而锁定（或者保护）了 IC 卡功能，则能够通过使用除了正常使用的 PIN 以外的认证密码，在线地解除对 IC 卡功能的锁定（保护），而不需要花费

系统管理员的劳动和时间。

[0008] 根据本发明，提供了一种移动通信设备，使其靠近信息处理设备以与该信息处理设备进行无线通信，所述移动通信设备包括：锁定部分，如果移动通信设备的用户与信息处理设备进行无线通信以执行用户认证，并且如果用户认证失败满足预定锁定条件，其执行对关于使用认证的操作的锁定；用户认证信息获得部分，如果通过锁定部分执行了该锁定，则其获得用户认证信息作为关于对用户的认证的信息；用户管理服务器无线通信部分，其将通过用户认证信息获得部分获得的用户认证信息无线地发送到用户管理服务器，并且无线地接收来自用户管理服务器的指令；以及锁定解除部分，如果通过用户管理服务器无线通信部分无线地接收的指令是关于解除所述锁定的指令，则其解除所述锁定。

[0009] 在根据本发明的移动通信设备中，优选地，锁定部分使用非接触 IC 卡的无线通信功能，并且信息处理设备使用非接触 IC 卡的读 / 写器的无线通信功能。

[0010] 在根据本发明的移动通信设备中，优选地，用户管理服务器无线通信部分使用移动通信网络中的无线通信功能。

[0011] 在根据本发明的移动通信设备中，优选地，基于来自用户的输入，用户认证信息获得部分获得与用于使用认证的第一密码不同的第二密码，并且将所获得的第二密码视为用户认证信息。

[0012] 在根据本发明的移动通信设备中，优选地，用户认证信息获得部分获得用户的生物学信息，并且将根据所获得的生物学信息而计算出的信息视为用户认证信息。

[0013] 在根据本发明的移动通信设备中，优选地，用户管理服务器将从用户管理服务器无线通信部分发送来的用户认证信息与事先登记的其它用户认证信息相比较，由此对用户进行认证，并且如果用户通过认证，则将关于解除所述锁定的指令发送到移动通信设备。

[0014] 在根据本发明的移动通信设备中，优选地，基于来自用户的输入，用户认证信息获得部分获得与用于使用认证的第一密码不同的第二密码，将所获得的第二密码与事先登记的另一第二密码相比较，由此对用户进行认证，并且如果用户通过认证，则将用户已经通过认证的事实视为用户认证信息。

[0015] 在根据本发明的移动通信设备中，优选地，用户认证信息获得部分获得用户的生物学信息，并且将所获得的生物学信息与事先登记的其它用户生物学信息相比较，由此对用户进行认证，并且如果用户通过认证，则将用户已经通过认证的事实视为用户认证信息。

[0016] 在根据本发明的移动通信设备中，优选地，用于管理服务器接收来自用户管理服务器无线通信部分的用户认证信息，并且如果对应于用户认证信息的用户满足预定许可条件，则将关于解除所述锁定的指令发送到移动通信设备。

[0017] 在根据本发明的移动通信设备中，优选地，预定许可条件是对应于用户认证信息的用户不是已经事先登记的，并且对其禁止解除锁定的用户。

[0018] 在根据本发明的移动通信设备中，优选地，预定锁定条件是使用认证失败的次数达到预定值。

[0019] 此外，根据本发明，提供了一种移动通信设备控制程序，其使得移动通信设备的计算机对靠近信息处理设备以与该信息处理设备进行无线通信的移动通信设备执行控制，所述程序包括：锁定步骤：如果移动通信设备的用户执行与信息处理设备的无线通信来执行使用认证，并且如果使用认证失败满足预定锁定条件，则对关于使用认证的操作执行锁定；

用户认证信息获得步骤，如果通过锁定步骤执行锁定，则获得用户认证信息作为关于用户的认证的信息；用户管理服务器无线通信步骤，将通过用户认证信息获得步骤获得的用户认证信息无线地发送到用户管理服务器，并且无线地接收来自用户管理服务器的指令；以及锁定解除步骤，如果通过用户管理服务器无线通信步骤无线地接收的指令是关于解除所述锁定的指令，则其解除所述锁定。

[0020] 此外，根据本发明，提供了一种移动通信设备控制方法，其对靠近信息处理设备以便与信息处理设备进行无线通信的移动通信设备进行控制，所述方法包括：移动通信设备中的锁定步骤，如果移动通信设备的用户与信息处理设备进行无线通信以执行使用认证，并且如果使用认证失败满足预定锁定条件，则对关于使用认证的操作执行锁定；移动通信设备中的用户认证信息获得步骤，如果通过锁定步骤执行了锁定，则获得用户认证信息作为关于对用户的认证的信息；移动通信设备中的用户认证信息发送步骤，将通过用户认证信息获得步骤获得的用户认证信息无线地发送到用户管理服务器；用户管理服务器中的移动通信设备指令发送步骤，基于通过用户认证信息发送步骤无线地发送的信息，将指令发送到移动通信设备；移动通信设备中的用户管理服务器无线接收步骤，无线地接收通过移动通信设备指令发送步骤无线地发送的指令；以及移动通信设备中的锁定解除步骤，如果通过用户管理服务器无线接收步骤接收到关于解除所述锁定的指令，则解除所述锁定。

[0021] 在根据本发明的移动通信设备控制方法中，优选地，锁定步骤使用非接触 IC 卡的无线通信功能，并且信息处理设备使用非接触 IC 卡的读 / 写器的无线通信功能。

[0022] 在根据本发明的移动通信设备控制方法中，优选地，用户认证信息发送步骤、移动通信设备指令发送步骤、以及用户管理服务器无线接收步骤使用移动通信网络中的无线通信功能。

[0023] 在根据本发明的移动通信设备控制方法中，优选地，基于来自用户的输入，用户认证信息获得步骤获得与用于使用认证的第一密码不同的第二密码，并且将所获得的第二密码视为用户认证信息。

[0024] 在根据本发明的移动通信设备控制方法中，优选地，用户认证信息获得步骤获得用户的生物学信息，并且将根据所获得的生物学信息而计算出的信息视为用户认证信息。

[0025] 在根据本发明的移动通信设备控制方法中，优选地，移动通信设备指令发送步骤将通过用户认证信息发送步骤发送的用户认证信息与事先登记的用户认证信息进行比较，由此对用户进行认证，并且如果用户通过认证，则将关于解除所述锁定的指令发送到移动通信设备。

[0026] 在根据本发明的移动通信设备控制方法中，优选地，基于来自用户的输入，用户认证信息获得步骤获得与用于使用认证的第一密码不同的第二密码，将所获得的第二密码与事先登记的另一第二密码相比较，由此对用户进行认证，并且如果用户通过认证，则将用户已经通过认证的事实视为用户认证信息。

[0027] 在根据本发明的移动通信设备控制方法中，优选地，用户认证信息获得步骤获得用户的生物学信息，将所获得的生物学信息与事先登记的其它用户生物学信息相比较，由此对用户进行认证，并且如果用户通过认证，则将用户已经通过认证的事实视为用户认证信息。

[0028] 根据本发明的移动通信设备，可通过网络从移动通信设备具有的 IC 应用来实施

对 PIN 的锁定解除。另外，通过使用仅能够被用户得知的第二密码可防止通过“冒充”进行的欺骗性锁定解除。因此，系统管理员不必通过进行会见或者电话呼叫来执行用户识别。由此 PIN 的解除不需要花费系统管理员的时间和劳力，这样使得能够实现实时的 PIN 锁定解除。因此，根据本发明的移动通信设备能够显示出对 PIN 锁定解除的即时性和安全性。

附图说明

[0029] 图 1 是示出应用于本发明的第一实施例的内置于移动电话中的非接触 IC 卡的 PIN 锁定解除功能的概念图；

[0030] 图 2 是示出图 1 所示的第一实施例中的通过 PIN 锁定解除功能的系统所执行的 PIN 锁定解除处理的流程的流程图；

[0031] 图 3 是示出应用于本发明的第二实施例的内置于移动电话中的非接触 IC 卡的 PIN 锁定解除功能的概念图；以及

[0032] 图 4 是示出在图 3 所示的第二实施例中，通过 PIN 锁定解除功能的系统所执行的 PIN 锁定解除处理的流程的流程图。

[0033] 具体实施例方式

[0034] 现在参照附图描述根据本发明的移动通信设备的实施例。首先描述根据本发明的移动通信设备的梗概。

[0035] 根据本发明的移动通信设备，当具有内置非接触 IC 卡的移动通信设备（即移动电话）的 IC 卡功能由于 PIN 认证错误而被锁定（或者被保护起来）时，移动电话启动应用（IC 应用程序）来解除 PIN 锁定，并且通过网络请求认证服务器解除锁定。接着，认证服务器要求用户输入与正常使用的 PIN（即第一密码）不同的第二密码，以对用户进行识别。例如，第二密码可以是诸如指纹、声波纹、虹膜、血脉等的生物学信息。接着，如果用户识别通过，则认证服务器解除移动电话的 PIN 的锁定。随后，移动电话解除在内置于其中的非接触 IC 卡中的芯片上记录的锁定信息。于是，关于非接触 IC 卡的 PIN 的锁定得以解除。

[0036] 现在将具体描述根据本发明的移动通信设备的优选实施例，以移动电话作为示例。

[0037] 实施例 1

[0038] 图 1 是示出应用于本发明的第一实施例的内置于移动电话中的非接触 IC 卡的 PIN 锁定解除功能的概念图。该概念图示出了实现 IC 卡的 PIN 锁定解除功能的组成部分和 PIN 锁定解除的处理流程。

[0039] 图 1 所示的第一实施例中的 PIN 锁定解除功能的系统是由具有内置非接触 IC 卡的移动电话 1（以下简称为移动电话）、认证服务器 3、以及 IC 卡读 / 写器 4 构成。用于商务设备的使用认证的非接触 IC 卡内置于移动电话 1 内。将认证服务器 3 包括在认证中心 2 中。IC 卡读 / 写器 4 非接触地从 IC 卡读取 / 向 IC 卡写入信息。移动电话 1 和认证服务器 3 连接到网络 5。注意，由认证服务器 3 对用于用户识别的第二密码进行管理。

[0040] 现在更详细地描述图 1 所示的锁定解除功能的系统配置。移动电话 1 具有实现密码锁定解除功能的 IC 应用 11，和执行外部设备的使用认证的非接触 IC 卡 13。注意，非接触 IC 卡被置于其中卡 13 能够通过 IC 卡读 / 写器 4 非接触地从其自己的 IC 芯片读取信息 / 向其自己的芯片写入信息的使用环境中。

[0041] 包括在认证中心 2 中的认证服务器 3 具有数据库 31。数据库 31 对移动电话 1 的拥有者已经为用户识别而登记的第二密码进行加密并且存储。

[0042] 图 2 是示出在图 1 所示的第一实施例中，通过 PIN 锁定解除功能的系统执行的 PIN 锁定解除处理的流程的流程图。现在参照图 1 所示的系统配置和处理流程来描述根据图 2 所示的流程图的 PIN 锁定解除处理的操作。

[0043] 移动电话 1 连续监控 PIN（第一密码）是否被锁定（步骤 S1）。第一密码是例如在通过支付终端使用信用卡的支付处理中或者在商务 PC 的登录处理中，正常用于执行使用认证的秘密号码。

[0044] 如果重复三次不正确地输入第一密码（即 PIN），则 PIN 被锁定（步骤 S1，是），并且在非接触 IC 卡 13 的 IC 芯片上的锁定标记开启（步骤 S2）。接下来，移动电话 1 根据用户的操作启动 IC 应用 11（步骤 S3）。IC 应用 11 要求用户输入第二密码。在输入第二密码之后（步骤 S4），移动电话 1 将第二密码发送到认证服务器 3（步骤 S5）。

[0045] 接下来，认证服务器 3 接收到来自移动电话 1 的第二密码（步骤 S6），并且将所接收的第二密码与事先存储在认证服务器 3 本身中的数据库 31 中的另一经加密的第二密码进行比较（步骤 S7）。认证服务器 3 确定这两个第二密码是否彼此一致（步骤 S8）。

[0046] 如果这两个第二密码彼此不一致（步骤 S8 中，否），则认证服务器 3 将指示第二密码之间不一致的通知发送给移动电话 1（步骤 S9）。此后，移动电话 1 接收到第二密码不一致的通知（步骤 S10）并且显示不能进行 (NG)PIN 的锁定解除的指示（步骤 S11）。

[0047] 另一方面，如果认证服务器 3 确定从移动电话 1 接收的第二密码与存储在认证服务器 3 中的数据库 31 中的另一第二密码彼此一致，作为步骤 S8 的确定结果（步骤 S8 中，是）。则认证服务器 3 向移动电话 1 发送用于 PIN 锁定解除的命令，以通知移动电话 1 执行 PIN 锁定解除（步骤 S12）。为了提高安全性，用于 PIN 锁定解除的命令可以与加密密钥一起从认证服务器 3 发送到移动电话 1。

[0048] 另一方面，移动电话 1 从认证服务器 3 接收用于 PIN 锁定解除的命令（如果必要还有加密密钥）（步骤 S13），并且指令非接触 IC 卡 13 解除 PIN 锁定。随后，非接触 IC 卡 13 关闭 IC 芯片上的锁定标记（步骤 S14）。于是解除了 PIN（即第一密码）的锁定。

[0049] 实施例 2

[0050] 接下来，将描述根据第二实施例的 PIN 锁定解除功能的系统和锁定解除处理的流程。图 3 是示出应用于本发明的第二实施例的内置于移动电话 1 中的非接触 IC 卡的 PIN 锁定解除功能的概念图。在图 1 所示的第一实施例中，认证服务器 3 管理用于用户识别的第二密码。然而，在图 3 所示的第二实施例中，移动电话 1 管理用于用户识别的第二密码。

[0051] 因此，在根据图 3 所示的第二实施例的 PIN 锁定解除功能的系统中，对第二密码 14 进行加密并且将其存储在具有内置非接触 IC 卡的移动电话 1（简称为移动电话）的 IC 应用 11 中，并且认证服务器 3 没有用于存储第二密码的数据库。该系统配置的其它部分与根据图 1 所示的第一实施例的 PIN 锁定解除功能的相同。该系统配置中的不同导致图 3 所示的 PIN 锁定解除处理的流程与图 1 所示的 PIN 锁定解除处理的流程之间的轻微差别。现在将在下文中根据流程图的流程来具体描述图 3 所示的 PIN 锁定解除处理的流程。省略关于图 3 所示的第二实施例的系统配置中的与第一实施例相同的组成元件的重复描述。

[0052] 图 4 是示出根据图 3 所示的第二实施例的通过 PIN 锁定解除功能的系统执行的

PIN 锁定解除处理的流程的流程图。因此，参照图 3 中的系统配置描述图 4 的流程图中所示的 PIN 锁定解除处理的操作。

[0053] 移动电话 1 连续监控作为第一密码的 PIN 是否被锁定（步骤 S21）。如果错误地输入第一密码（即 PIN）重复三次，则 PIN 被锁定（步骤 S21 中为是），并且将非接触 IC 卡 13 的 IC 芯片上的锁定标记开启（步骤 S22）。

[0054] 接下来，移动电话 1 根据用户的操作启动 IC 应用 11（步骤 S23）。IC 应用 11 要求用户输入第二密码。在输入第二密码之后（步骤 S24）。移动电话 1 将所输入的第二密码与事先存储在移动电话 1 自身的 IC 应用 11 中的另一第二密码 14 相比较（步骤 S25）。

[0055] 移动电话 1 随后确定刚刚输入的第二密码与事先存储在其自身的 IC 应用 11 中的另一第二密码是否彼此一致（步骤 S26）。如果这两个第二密码彼此不一致（步骤 S26 中为否），则移动电话 1 显示不能进行 PIN 的锁定解除 (NG) 的指示（步骤 S27）。

[0056] 否则，如果作为步骤 S26 的确定结果，输入的第二密码与事先存储在移动电话 1 自身的 IC 应用 11 中的另一第二密码彼此一致（步骤 S26 中为是），则移动电话 1 将表示这两个第二密码一致的确定信息发送给认证服务器 3（步骤 S28）。

[0057] 认证服务器 3 接收确认信息（步骤 S29），向移动电话 1 发送用于 PIN 锁定解除的命令，并且通知移动电话 1 解除 PIN 锁定（步骤 S30）。为了提高安全性，认证服务器 3 可以将该命令与加密密钥一起发送给移动电话 1。

[0058] 此外，移动电话 1 接收来自认证服务器 3 的用于 PIN 锁定解除的命令（如果需要还接收加密密钥）（步骤 S31），并且指示非接触 IC 卡 13 关闭 IC 芯片上的锁定标记（步骤 S32）。于是，PIN（即，第一密码）锁定得以解除。

[0059] 参照移动电话作为优选示例描述了上述实施例。然而，根据本发明，移动通信设备不限于上述实施例中描述的移动电话。

[0060] 此外，构成移动通信设备的计算机可以提供程序来执行上述步骤。如果将这种程序存储在可从计算机读取的记录介质上，则可通过构成移动通信设备的计算机执行该程序。可从计算机读取的记录介质包括：内置于计算机中的诸如 ROM 或者 RAM 的内部存储设备；诸如 CD-ROM、软盘、DVD 盘、磁光盘、或者 IC 卡的便携式记录介质；用于存储计算机程序的数据库；另一计算机及其数据库；或者在线传输介质。

[0061] 接下来描述本发明与实施例的组成元件之间的对应。本发明中的移动通信设备对应于实施例中具有内置非接触 IC 卡的移动电话 1、本发明中的信息处理设备对应于实施例中的 IC 卡读 / 写器 4。

[0062] 本发明中的锁定部分对应于实施例中的非接触 IC 卡 13。本发明的用户管理服务器无线通信部分对应于实施例中的移动电话 1 的通信功能。本发明的用户认证信息获得部分对应于在实施例中通过 IC 应用 11 实现的功能。本发明的用户管理服务器对应于实施例中的认证服务器 3。此外，本发明中的锁定解除部分对应于实施例中的非接触 IC 卡 13 的锁定标记。

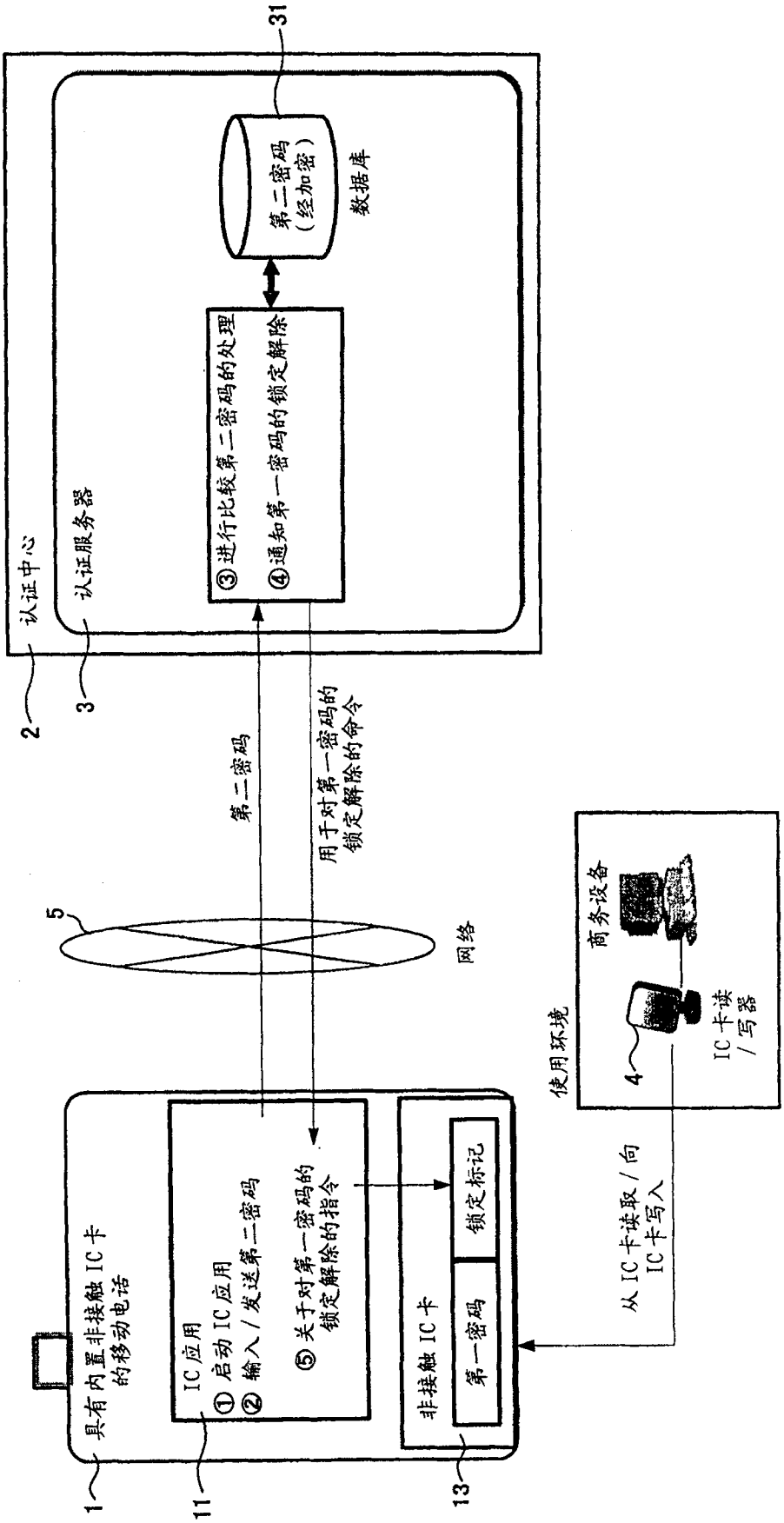

认证中心
2
认证服务器
3
31
第二密码
(经加密)
数据库
③进行比较第二密码的处理
④通知第一密码的锁定解除
第二密码
用于对第一密码的
锁定解除的命令
5
网络
使用环境
商务设备
4
IC卡读
/写器
具有内置非接触IC卡
的移动电话
1
IC应用
①启动IC应用
②输入/发送第二密码
⑤关于对第一密码的
锁定解除的指令
11
非接触IC卡
第一密码
锁定标记
13
从IC卡读取/向
IC卡写入

图 1

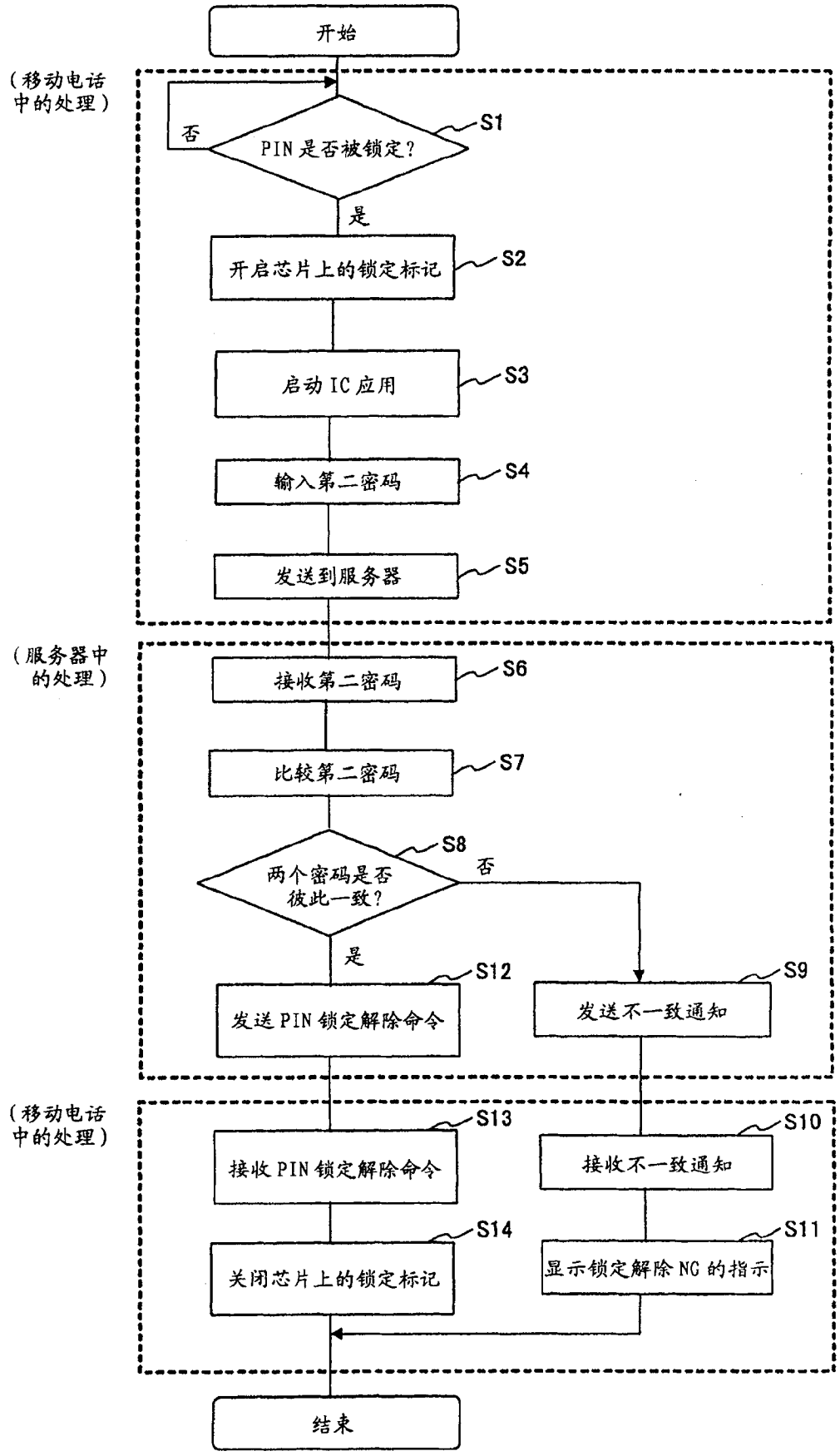

开始
（移动电话中的处理）
否
PIN 是否被锁定？
S1
是
开启芯片上的锁定标记
S2
启动 IC 应用
S3
输入第二密码
S4
发送到服务器
S5
（服务器中的处理）
接收第二密码
S6
比较第二密码
S7
两个密码是否彼此一致？
S8
否
是
发送 PIN 锁定解除命令
S12
发送不一致通知
S9
（移动电话中的处理）
接收 PIN 锁定解除命令
S13
接收不一致通知
S10
关闭芯片上的锁定标记
S14
显示锁定解除 NG 的指示
S11
结束

图 2

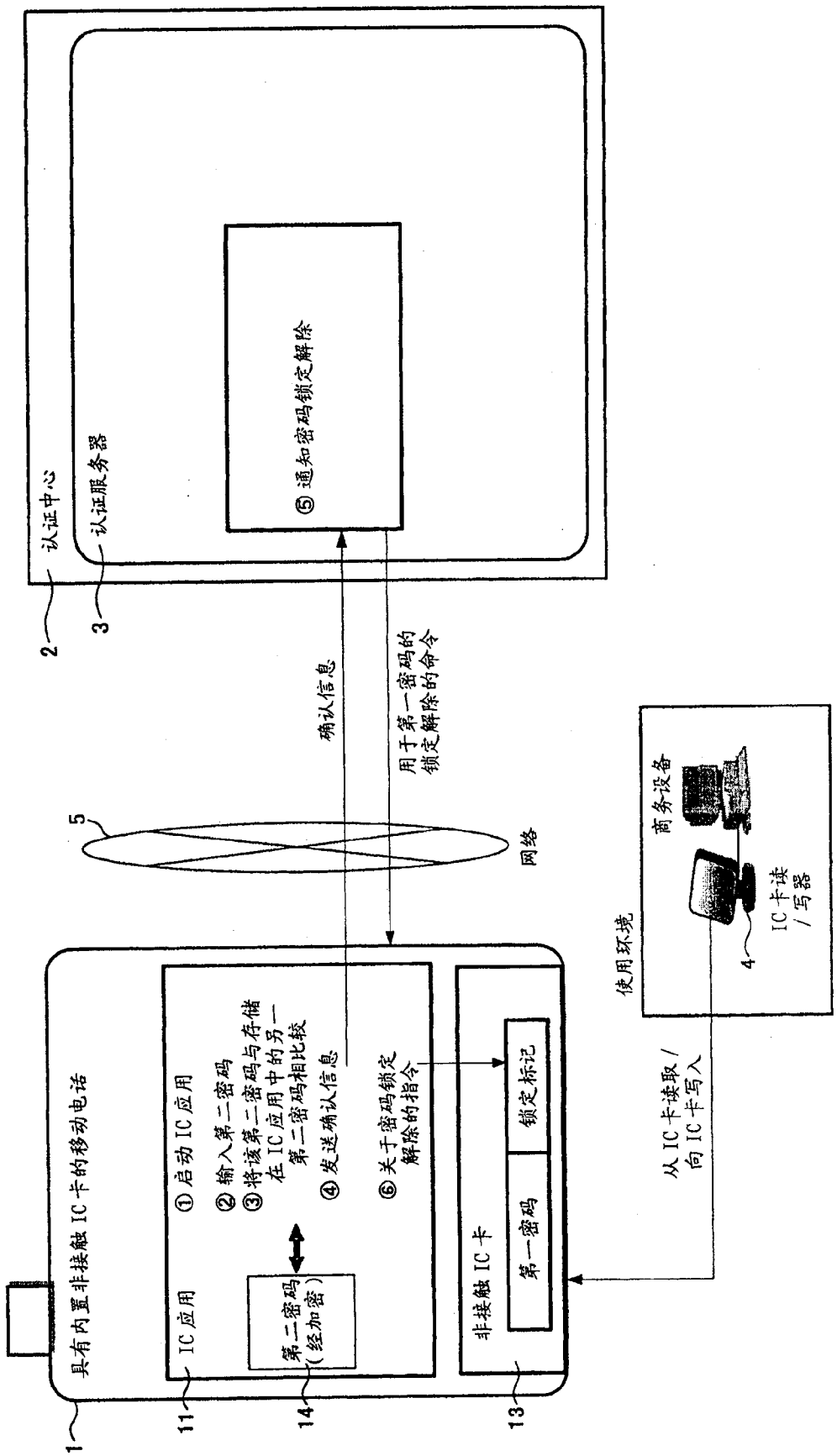

认证中心
认证服务器
⑤通知密码锁定解除
2
3
确认信息
用于第一密码的
锁定解除的命令
5
网络
使用环境
商务设备
IC卡读
/写器
4
从IC卡读取/
向IC卡写入
具有内置非接触IC卡的移动电话
IC应用
①启动IC应用
②输入第二密码
③将该第二密码与存储
在IC应用中的另一
第二密码相比较
④发送确认信息
⑥关于密码锁定
解除的指令
第二密码
(经加密)
非接触IC卡
第一密码
锁定标记
1
11
14
13

图 3

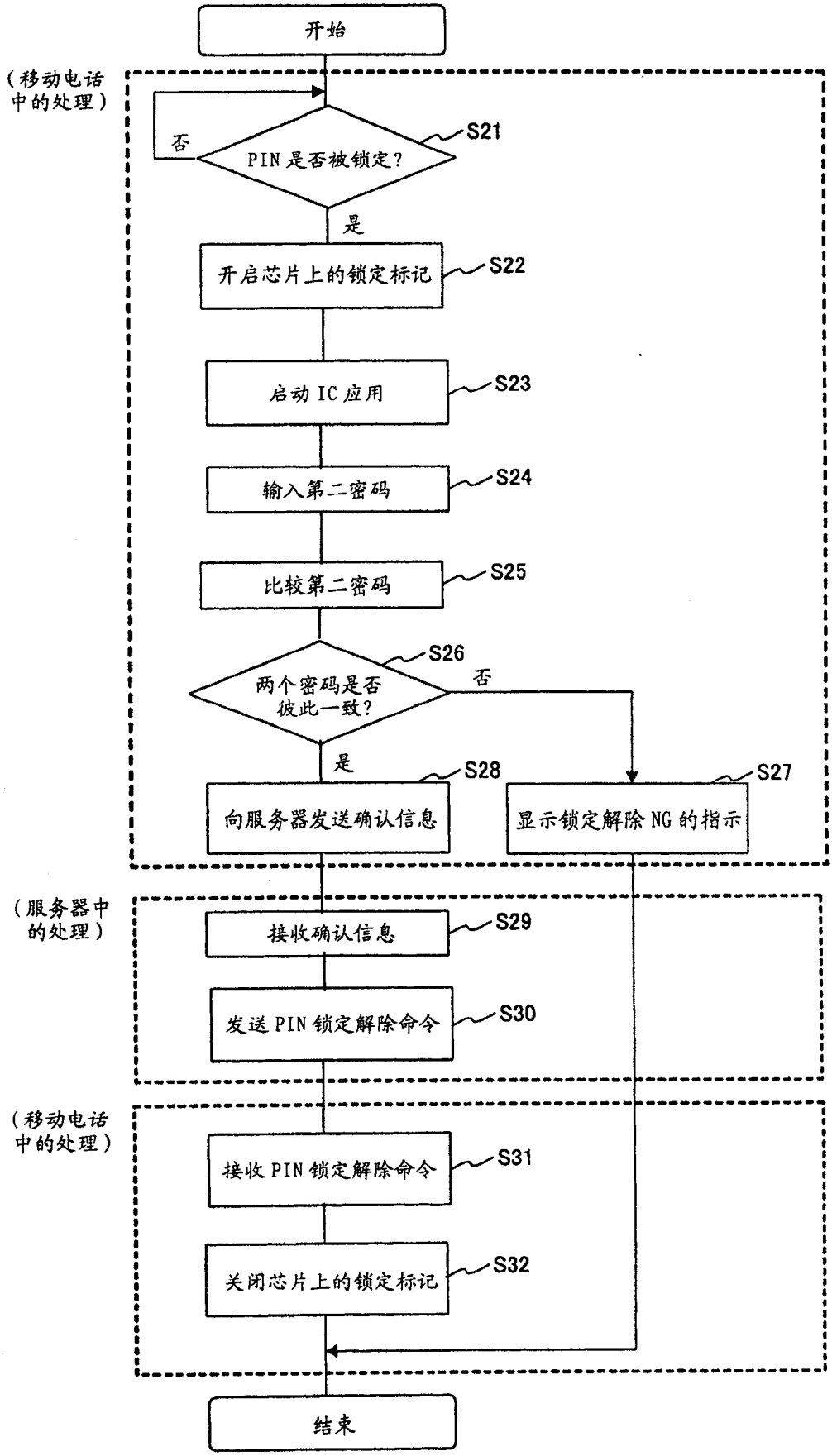

开始
（移动电话中的处理）
否
PIN 是否被锁定？
S21
是
开启芯片上的锁定标记
S22
启动 IC 应用
S23
输入第二密码
S24
比较第二密码
S25
两个密码是否彼此一致？
S26
否
是
向服务器发送确认信息
S28
显示锁定解除 NG 的指示
S27
（服务器中的处理）
接收确认信息
S29
发送 PIN 锁定解除命令
S30
（移动电话中的处理）
接收 PIN 锁定解除命令
S31
关闭芯片上的锁定标记
S32
结束

图 4