

(12) 发明专利申请

(10) 申请公布号 CN 103297224 A

(43) 申请公布日 2013. 09. 11

(21) 申请号 201210043852. X

(22) 申请日 2012. 02. 23

(71) 申请人 中国移动通信集团公司

地址 100032 北京市西城区金融大街 29 号

(72) 发明人 齐旻鹏 朱红儒 徐晖

(74) 专利代理机构 北京同达信恒知识产权代理有限公司 11291

代理人 郭润湘

(51) Int. Cl.

H04L 9/08 (2006. 01)

H04L 29/06 (2006. 01)

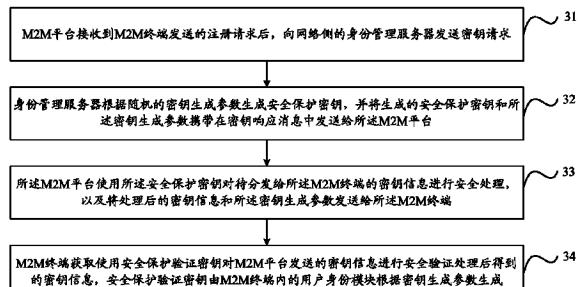
权利要求书5页 说明书14页 附图7页

(54) 发明名称

密钥信息分发方法及相关设备

(57) 摘要

本发明公开了一种密钥信息分发方法及相关设备，M2M 平台接收到注册请求后向身份管理服务器发送密钥请求；身份管理服务器根据密钥生成参数生成安全保护密钥，将安全保护密钥和密钥生成参数发送给 M2M 平台；M2M 平台使用安全保护密钥对密钥信息进行安全处理后将密钥信息和密钥生成参数发送给 M2M 终端；M2M 终端获取使用与安全保护密钥对应的安全保护验证密钥对密钥信息进行安全验证处理后得到的密钥信息，安全保护验证密钥由 M2M 终端内的用户身份模块根据密钥生成参数生成。采用本发明技术方案，能够解决现有技术中传输密钥信息的安全性较低，且 M2M 系统应用的灵活性较低的问题。



1. 一种密钥信息分发方法,其特征在于,包括:

机器对机器 M2M 平台接收到 M2M 终端发送的注册请求后,向网络侧的身份管理服务器发送密钥请求;

所述身份管理服务器根据随机的密钥生成参数生成安全保护密钥,并将生成的安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给所述 M2M 平台;

所述 M2M 平台使用所述安全保护密钥对待分发给所述 M2M 终端的密钥信息进行安全处理,以及将处理后的密钥信息和所述密钥生成参数发送给所述 M2M 终端;

所述 M2M 终端获取使用安全保护验证密钥对所述 M2M 平台发送的密钥信息进行安全验证处理后得到的密钥信息,其中,所述安全保护验证密钥由所述 M2M 终端内的用户身份模块根据所述密钥生成参数生成。

2. 如权利要求 1 所述的方法,其特征在于,所述 M2M 终端获取使用安全保护验证密钥对所述 M2M 平台发送的密钥信息进行安全验证处理后得到的密钥信息,具体包括:

所述 M2M 终端将接收到的密钥信息和所述密钥生成参数携带在密钥传输消息中发送给所述 M2M 终端内的用户身份模块;

所述用户身份模块根据接收到的所述密钥生成参数,生成与所述安全保护密钥对应的安全保护验证密钥,以及使用生成的安全保护验证密钥对 M2M 终端发送的密钥信息进行安全验证处理,并将通过安全验证处理的密钥信息发送给所述 M2M 终端。

3. 如权利要求 2 所述的方法,其特征在于,所述身份管理服务器根据随机的密钥生成参数生成安全保护密钥,并将生成的安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给所述 M2M 平台,具体包括:

所述处理服务器根据随机的密钥生成参数,生成至少两个安全保护密钥,并将生成的各安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给所述 M2M 平台,所述密钥生成参数中携带有处理服务器指示的、此次对密钥信息进行安全处理的安全保护密钥的标识;

所述 M2M 平台使用所述安全保护密钥对待分发给所述 M2M 终端的密钥信息进行安全处理,具体包括:

所述 M2M 平台根据密钥生成参数中携带的安全保护密钥的标识,在接收到的各安全保护密钥中选择出此次对密钥信息进行安全处理的安全保护密钥,并使用选择出的安全保护密钥对待分发给所述 M2M 终端的密钥信息进行安全处理;

所述用户身份模块根据接收到的所述密钥生成参数,生成与所述安全保护密钥对应的安全保护验证密钥,以及使用生成的安全保护验证密钥对 M2M 终端发送的密钥信息进行安全验证处理,具体包括:

所述用户身份模块根据接收到的所述密钥生成参数,生成与各安全保护密钥分别对应的至少两个安全保护验证密钥,以及根据所述密钥生成参数中携带的安全保护密钥的标识,在生成的各安全保护验证密钥中选择出此次对密钥信息进行安全验证处理的安全保护验证密钥,并使用选择出的安全保护验证密钥对接收到的密钥信息进行安全验证处理。

4. 如权利要求 1 所述的方法,其特征在于,所述 M2M 终端获取使用安全保护验证密钥对所述 M2M 平台发送的密钥信息进行安全验证处理后得到的密钥信息,具体包括:

所述 M2M 终端将接收到的密钥生成参数携带在密钥传输消息中发送给所述 M2M 终端内

的用户身份模块；

所述用户身份模块根据接收到的所述密钥生成参数，生成与所述安全保护密钥对应的安全保护验证密钥，并将生成的安全保护验证密钥发送给所述 M2M 终端；

所述 M2M 终端使用接收到的安全保护验证密钥对 M2M 平台发送的密钥信息进行安全验证处理，得到通过安全验证处理的密钥信息。

5. 如权利要求 4 所述的方法，其特征在于，所述身份管理服务器根据随机的密钥生成参数生成安全保护密钥，并将生成的安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给所述 M2M 平台，具体包括：

所述身份管理服务器根据随机的密钥生成参数，生成至少两个安全保护密钥，并将生成的各安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给所述 M2M 平台，所述密钥生成参数中携带有身份管理服务器指示的、此次对密钥信息进行安全处理的安全保护密钥的标识；

所述 M2M 平台使用所述安全保护密钥对待分发给所述 M2M 终端的密钥信息进行安全处理，具体包括：

所述 M2M 平台根据密钥生成参数中携带的安全保护密钥的标识，在接收到的各安全保护密钥中选择出此次对密钥信息进行安全处理的安全保护密钥，并使用选择出的安全保护密钥对待分发给所述 M2M 终端的密钥信息进行安全处理；

所述用户身份模块根据接收到的所述密钥生成参数，生成与所述安全保护密钥对应的安全保护验证密钥，并将生成的安全保护验证密钥发送给所述 M2M 终端，具体包括：

所述用户身份模块根据接收到的所述密钥生成参数，生成与各安全保护密钥分别对应的至少两个安全保护验证密钥，以及根据所述密钥生成参数中携带的安全保护密钥的标识，在生成的各安全保护验证密钥中选择出此次对密钥信息进行安全验证处理的安全保护验证密钥，并将选择出的安全保护验证密钥发送给所述 M2M 终端。

6. 如权利要求 1 所述的方法，其特征在于，所述密钥请求中携带有所述用户身份模块的标识；

所述身份管理服务器根据随机的密钥生成参数生成安全保护密钥，具体包括：

所述身份管理服务器根据接收到的密钥请求中携带的所述用户身份模块的标识，查找所述用户身份模块对应的根密钥；并

根据查找到的根密钥和随机的密钥生成参数，生成安全保护密钥；

所述 M2M 终端内的用户身份模块根据所述密钥生成参数生成安全保护验证密钥，具体包括：

所述 M2M 终端内的用户身份模块根据自身的根密钥以及所述密钥生成参数，生成与所述安全保护密钥对应的安全保护验证密钥。

7. 如权利要求 1 所述的方法，其特征在于，所述安全保护密钥中包含加密密钥和 / 或完整性保护密钥；

所述安全保护验证密钥中包含解密密钥和 / 或完整性保护验证密钥。

8. 如权利要求 1 所述的方法，其特征在于，所述身份管理服务器为归属位置寄存器 HLR 或归属用户服务器 HSS。

9. 一种机器对机器平台，其特征在于，包括：

注册请求接收单元,用于接收机器对机器 M2M 终端发送的注册请求;

密钥请求发送单元,用于在注册请求接收单元接收到 M2M 终端发送的注册请求后,向网络侧的身份管理服务器发送密钥请求;

密钥响应消息接收单元,用于接收所述身份管理服务器发送的携带有安全保护密钥和随机的密钥生成参数的密钥响应消息,所述安全保护密钥是所述身份管理服务器根据所述密钥生成参数生成的;

安全处理单元,用于使用所述安全保护密钥对待分发给所述 M2M 终端的密钥信息进行安全处理;

密钥信息发送单元,用于将安全处理单元处理后的密钥信息和所述密钥生成参数发送给所述 M2M 终端。

10. 如权利要求 9 所述的机器对机器平台,其特征在于,所述身份管理服务器根据所述密钥生成参数生成至少两个安全保护密钥,所述密钥响应消息接收单元接收到的密钥生成参数中携带有身份管理服务器指示的、此次对密钥信息进行安全处理的安全保护密钥的标识;

所述安全处理单元具体包括:

安全保护密钥选择子单元,用于根据密钥响应消息接收单元接收到的密钥生成参数中携带的安全保护密钥的标识,在密钥响应消息接收单元接收到的各安全保护密钥中选择出此次对密钥信息进行安全处理的安全保护密钥;

安全处理子单元,用于使用安全保护密钥选择子单元选择出的安全保护密钥,对待分发给所述 M2M 终端的密钥信息进行安全处理。

11. 一种身份管理服务器,其特征在于,包括:

密钥请求接收单元,用于接收机器对机器 M2M 平台发送的密钥请求;

安全保护密钥生成单元,用于在密钥请求接收单元接收到密钥请求后,根据随机的密钥生成参数生成安全保护密钥;

密钥响应消息发送单元,用于将安全保护密钥生成单元生成的安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给所述 M2M 平台。

12. 如权利要求 11 所述的身份管理服务器,其特征在于,安全保护密钥生成单元,具体用于在密钥请求接收单元接收到密钥请求后,根据随机的密钥生成参数,生成至少两个安全保护密钥;

密钥响应消息发送单元,具体用于将安全保护密钥生成单元生成的各安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给所述 M2M 平台,所述密钥生成参数中携带有所述身份管理服务器指示的、此次对密钥信息进行安全处理的安全保护密钥的标识。

13. 如权利要求 11 所述的身份管理服务器,其特征在于,密钥请求接收单元接收到的所述密钥请求中携带有用户身份模块的标识;

安全保护密钥生成单元具体包括:

根密钥查找子单元,用于根据密钥请求接收单元接收到的密钥请求中携带的用户身份模块的标识,查找所述用户身份模块对应的根密钥;

安全保护密钥生成子单元,用于根据根密钥查找子单元查找到的根密钥和随机的密钥生成参数,生成安全保护密钥。

14. 一种机器对机器终端，其特征在于，包括：

密钥信息接收单元，用于接收机器对机器 M2M 平台发送的、使用安全保护密钥对待发送给所述 M2M 终端的密钥信息进行安全处理后的密钥信息和密钥生成参数；

密钥信息获取单元，用于获取使用安全保护验证密钥对密钥信息接收单元接收到的密钥信息进行安全验证处理后得到的密钥信息，其中，所述安全保护验证密钥由所述 M2M 终端内的用户身份模块根据所述密钥生成参数生成；

密钥信息确认单元，用于将密钥信息获取单元获取到的密钥信息确认为 M2M 平台分发的密钥信息。

15. 如权利要求 14 所述的机器对机器终端，其特征在于，密钥信息获取单元具体包括：

第一密钥传输消息发送子单元，用于将密钥信息接收单元接收到的密钥信息和密钥生成参数携带在密钥传输消息中发送给所述 M2M 终端内的用户身份模块；

密钥信息接收子单元，用于接收通过安全验证处理的密钥信息，通过安全验证处理的密钥信息是所述用户身份模块根据接收到的密钥生成参数，生成与所述安全保护密钥对应的安全保护验证密钥，以及使用生成的安全保护验证密钥对第一密钥传输消息发送子单元发送的密钥信息进行安全验证处理后发送的。

16. 如权利要求 15 所述的机器对机器终端，密钥信息获取单元具体包括：

第二密钥传输消息发送子单元，用于将密钥信息接收单元接收到的密钥生成参数携带在密钥传输消息中发送给所述 M2M 终端内的用户身份模块；

安全保护验证密钥接收子单元，用于接收所述用户身份模块发送的与所述安全保护密钥对应的安全保护验证密钥，所述安全保护验证密钥是所述用户身份模块根据接收到的所述密钥生成参数生成的；

安全验证处理子单元，用于使用安全保护验证密钥接收子单元接收到的安全保护验证密钥，对密钥信息接收单元接收到的密钥信息进行安全验证处理，得到通过安全验证处理的密钥信息。

17. 一种用户身份模块，置于机器对机器 M2M 终端内，其特征在于，包括：

密钥生成参数获取单元，用于获取生成安全保护密钥的随机的安全生成参数，安全保护密钥用于 M2M 平台对待发送给所述 M2M 终端的密钥信息进行安全处理；

安全保护验证密钥生成单元，用于根据密钥生成参数获取单元获取到的所述密钥生成参数，生成与所述安全保护密钥对应的安全保护验证密钥，所述安全保护验证密钥用于对安全处理后的密钥信息进行安全验证处理。

18. 如权利要求 17 所述的用户身份模块，其特征在于，密钥生成参数获取单元，具体用于接收所述 M2M 终端发送的密钥传输消息，所述密钥传输消息中携带有生成安全保护密钥的随机的安全生成参数、以及 M2M 平台使用安全保护密钥对待发送给所述 M2M 终端的密钥信息进行安全处理后得到的密钥信息；

安全保护验证密钥生成单元，具体用于根据密钥生成参数获取单元接收到的所述密钥生成参数，生成与所述安全保护密钥对应的安全保护验证密钥；

所述用户身份模块还包括：

安全验证处理单元，用于使用安全保护验证密钥生成单元生成的安全保护验证密钥，对密钥生成参数获取单元接收到的密钥信息进行安全验证处理；

密钥信息发送单元，用于将通过安全验证处理单元进行安全验证处理后的密钥信息发送给所述 M2M 终端。

19. 如权利要求 18 所述的用户身份模块，其特征在于，密钥生成参数获取单元接收到的密钥生成参数中携带有此次对密钥信息进行安全处理的安全保护密钥的标识；

安全保护验证密钥生成单元，具体用于根据密钥生成参数获取单元接收到的所述密钥生成参数，生成与各安全保护密钥分别对应的至少两个安全保护验证密钥；

安全验证处理单元，具体用于根据密钥生成参数获取单元接收到的密钥生成参数中携带的安全保护密钥的标识，在安全保护验证密钥生成单元生成的各安全保护验证密钥中选择出此次对密钥信息进行安全验证处理的安全保护验证密钥，并使用选择出的安全保护验证密钥对接收到的密钥信息进行安全验证处理。

20. 如权利要求 17 所述的用户身份模块，其特征在于，密钥生成参数获取单元，具体用于接收所述 M2M 终端发送的密钥传输消息，所述密钥传输消息中携带有生成安全保护密钥的随机的安全生成参数；

安全保护验证密钥生成单元，具体用于根据密钥生成参数获取单元接收到的所述密钥生成参数，生成与所述安全保护密钥对应的安全保护验证密钥；

所述用户身份模块还包括：

安全保护验证密钥发送单元，用于将安全保护验证密钥生成单元生成的安全保护验证密钥发送给所述 M2M 终端，所述安全保护验证密钥用于所述 M2M 终端对使用安全保护密钥对密钥信息进行安全处理后的密钥信息进行安全验证处理。

21. 如权利要求 20 所述的用户身份模块，其特征在于，密钥生成参数获取单元接收到的密钥生成参数中携带有此次对密钥信息进行安全处理的安全保护密钥的标识；

安全保护验证密钥生成单元，具体用于根据密钥生成参数获取单元接收到的所述密钥生成参数，生成与各安全保护密钥分别对应的至少两个安全保护验证密钥；

安全保护验证密钥发送单元，具体用于根据密钥生成参数获取单元接收到的密钥生成参数中携带的安全保护密钥的标识，在安全保护验证密钥生成单元生成的各安全保护验证密钥中选择出此次对密钥信息进行安全验证处理的安全保护验证密钥，并将选择出的安全保护验证密钥发送给所述 M2M 终端。

22. 如权利要求 17 所述的用户身份模块，其特征在于，安全保护验证密钥生成单元，具体用于根据自身的根密钥以及密钥生成参数获取单元获取到的所述密钥生成参数，生成与所述安全保护密钥对应的安全保护验证密钥。

## 密钥信息分发方法及相关设备

### 技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种密钥信息分发方法及相关设备。

### 背景技术

[0002] 机器对机器 (M2M, Machine-to-Machine) 是一种以机器终端智能交互为核心的、网络化的应用与服务。M2M 终端与 M2M 平台建立通信时需要通过接入密码完成 M2M 终端在 M2M 平台的登录过程，并需要基于基础密钥对数据进行加密，因此 M2M 终端接入 M2M 系统前必须从 M2M 平台上获取其上、下行接入密码和基础密钥，M2M 终端的接入密码和基础密钥是 M2M 安全机制的基础，接入密码和基础密钥也可以统称为密钥信息。

[0003] 目前，M2M 终端获取接入密码和基础密钥的方法一般包含下述两种，下面分别进行介绍。

[0004] 第一种获取方法，通过预配置的方法将 M2M 终端的终端序列号、接入密码和基础密钥预先存储在 M2M 终端中，同时将预配置的终端序列号、接入密码和基础密钥保存在 M2M 平台上。M2M 终端向 M2M 平台注册时，将接入密码和基础密钥进行摘要处理后，和终端序列号一起上报给 M2M 平台，M2M 平台根据 M2M 终端上报的终端序列号及经过摘要处理后的接入密码和基础密钥的相关信息进行核对，若核对结果为无效，则 M2M 平台将禁止该 M2M 终端注册。

[0005] 第二种获取方法，M2M 终端首次向 M2M 平台注册时，M2M 平台通过短消息将接入密码和基础密钥下发给 M2M 终端，如图 1 所示，其具体处理流程如下：

[0006] 步骤 11，M2M 终端通过注册 (REGISTER) 报文向 M2M 平台发起注册请求；

[0007] 步骤 12，M2M 平台通过 M2M 终端的注册请求之后，向该 M2M 终端发送注册确认 (REGISTER\_ACK ;ACK, Acknowledge) 报文回复注册成功，并要求该 M2M 终端进入短消息通信模式，准备接收 M2M 平台下发的接入密码和基础密钥；

[0008] 步骤 13，M2M 终端接收到 REGISTER\_ACK 报文之后，立即进入短消息通信模式；

[0009] 步骤 14，M2M 平台经过一定的时延之后，生成接入密码和基础密钥，通过短消息向 M2M 终端发送安全设置 (SECURITY\_CONFIG) 报文，SECURITY\_CONFIG 报文中携带有该 M2M 终端的上行接入密码、上行接入密码的有效期、下行接入密码、下行接入密码的有效期，若 M2M 终端支持并启用了数据加密功能，则 M2M 平台还会在 SECURITY\_CONFIG 报文中携带该 M2M 终端的基础密钥和基础密钥的有效期，由于接入密码和基础密钥是首次分发，因此 M2M 平台必须采用短消息明文发送的方式进行下发，在 M2M 系统支持短消息加密传输的情况下，携带接入密码和基础密钥的报文的传输安全性可以由短消息的安全传输机制来保证；

[0010] 步骤 15，M2M 终端成功接收到 M2M 平台下发的接入密码和基础密钥之后，立即将其存储，并向 M2M 平台返回安全设置确认 (SECURITY\_CONFIG\_ACK) 报文；

[0011] 步骤 16，M2M 终端使用接收到的接入密码向 M2M 平台发送登录 (LOGIN) 报文，即发起登录请求，若 M2M 终端支持并启用了数据加密功能，则还需要携带基础密钥的相关信息摘要；

[0012] 步骤 17, M2M 平台接收到 M2M 终端的 LOGIN 报文之后, 对其进行鉴权, 并在鉴权通过后回复登录确认 (LOGIN\_ACK) 报文, 并在 M2M 平台生成首次下发密码成功日志, 同时保存接入密码以及基础密钥。

[0013] 由上可见, 现有技术中第一种获取接入密码和基础密钥的方法需要人为地将密钥信息配置到每个 M2M 终端, 增加了用户使用终端设备时操作的复杂性, 此外, 由于不确定 M2M 终端初始接入 M2M 系统的确切时间, 为了确保 M2M 终端接入时密钥信息不过期, 预置的接入密码和基础密钥的有效期都必须设置为最长时间, 这就给网络攻击者留下了获取并使用密码信息的网络安全隐患, 使得传输密钥信息的安全性较低; 而现有技术第二种获取接入密码和基础密钥的方法虽然能够实现密钥信息自动配置和分发, 但是由于缺乏对密钥信息的保护机制, M2M 终端的密钥信息只能以明文的形式下发, 这就使密钥信息很容易地被网络攻击者获取, 使得传输密钥信息的安全性较低, 此外在 M2M 系统支持短消息加密传输的情况下, 采用短消息传输的方法虽然能够对密钥信息进行传输安全保护, 但是必须要通过短消息的方式进行发送, 这就使原本可支持多种数据通信方式的 M2M 系统在密钥信息分发环节只能采取短消息的方式传输, 在很大程度上限制了 M2M 系统应用的灵活性。

## 发明内容

[0014] 本发明实施例提供一种密钥信息分发方法及相关设备, 用以解决现有技术中传输密钥信息的安全性较低, 且 M2M 系统应用的灵活性较低的问题。

[0015] 本发明实施例技术方案如下:

[0016] 一种密钥信息分发方法, 该方法包括步骤: 机器对机器 M2M 平台接收到 M2M 终端发送的注册请求后, 向网络侧的身份管理服务器发送密钥请求; 所述身份管理服务器根据随机的密钥生成参数生成安全保护密钥, 并将生成的安全保护密钥和所述密钥生成参数携带有在密钥响应消息中发送给所述 M2M 平台; 所述 M2M 平台使用所述安全保护密钥对待分发给所述 M2M 终端的密钥信息进行安全处理, 以及将处理后的密钥信息和所述密钥生成参数发送给所述 M2M 终端; 所述 M2M 终端获取使用安全保护验证密钥对所述 M2M 平台发送的密钥信息进行安全验证处理后得到的密钥信息, 其中, 所述安全保护验证密钥由所述 M2M 终端内的用户身份模块根据所述密钥生成参数生成。

[0017] 一种机器对机器平台, 包括: 注册请求接收单元, 用于接收 M2M 终端发送的注册请求; 密钥请求发送单元, 用于在注册请求接收单元接收到 M2M 终端发送的注册请求后, 向网络侧的身份管理服务器发送密钥请求; 密钥响应消息接收单元, 用于接收所述身份管理服务器发送的携带有安全保护密钥和随机的密钥生成参数的密钥响应消息, 所述安全保护密钥是所述身份管理服务器根据所述密钥生成参数生成的; 安全处理单元, 用于使用所述安全保护密钥对待分发给所述 M2M 终端的密钥信息进行安全处理; 密钥信息发送单元, 用于将安全处理单元处理后的密钥信息和所述密钥生成参数发送给所述 M2M 终端。

[0018] 一种身份管理服务器, 包括: 密钥请求接收单元, 用于接收机器对机器 M2M 平台发送的密钥请求; 安全保护密钥生成单元, 用于在密钥请求接收单元接收到密钥请求后, 根据随机的密钥生成参数生成安全保护密钥; 密钥响应消息发送单元, 用于将安全保护密钥生成单元生成的安全保护密钥和所述密钥生成参数携带有在密钥响应消息中发送给所述 M2M 平台。

[0019] 一种机器对机器终端,包括:密钥信息接收单元,用于接收机器对机器 M2M 平台发送的、使用安全保护密钥对待发送给所述 M2M 终端的密钥信息进行安全处理后的密钥信息和密钥生成参数;密钥信息获取单元,用于获取使用安全保护验证密钥对密钥信息接收单元接收到的密钥信息进行安全验证处理后得到的密钥信息,其中,所述安全保护验证密钥由所述 M2M 终端内的用户身份模块根据所述密钥生成参数生成;密钥信息确认单元,用于将密钥信息获取单元获取到的密钥信息确认为 M2M 平台分发的密钥信息。

[0020] 一种用户身份模块,置于机器对机器 M2M 终端内,包括:密钥生成参数获取单元,用于获取生成安全保护密钥的随机的安全生成参数,安全保护密钥用于 M2M 平台对待发送给所述 M2M 终端的密钥信息进行安全处理;安全保护验证密钥生成单元,用于根据密钥生成参数获取单元获取到的所述密钥生成参数,生成与所述安全保护密钥对应的安全保护验证密钥,所述安全保护验证密钥用于对安全处理后的密钥信息进行安全验证处理。

[0021] 本发明实施例技术方案中,M2M 平台接收到 M2M 终端发送的注册请求后,向网络侧的身份管理服务器发送密钥请求,身份管理服务器根据随机的密钥生成参数生成安全保护密钥,并将生成的安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给 M2M 平台,M2M 平台使用所述安全保护密钥对待分发给 M2M 终端的密钥信息进行安全处理,以及将处理后的密钥信息和密钥生成参数发送给 M2M 终端,M2M 终端内的用户身份模块根据密钥生成参数生成与安全保护密钥对应的安全保护验证密钥,M2M 终端获取使用安全保护验证密钥对 M2M 平台发送的密钥信息进行安全验证处理后得到的密钥信息,获取到的密钥信息即为 M2M 平台分发的密钥信息。由此可见,本发明实施例技术方案与现有技术第一种获取密钥信息的方法相比,能够在 M2M 终端注册至 M2M 系统时自动实现 M2M 终端的密钥信息的分发,免除了用户对 M2M 终端进行密钥配置操作的复杂性,提高了用户体验,同时在 M2M 终端发起注册时将密钥信息分发给 M2M 终端,因此 M2M 平台可以在接收到 M2M 终端的注册请求时动态生成密钥信息,有效地提高了传输密钥信息的安全性;本发明实施例技术方案与现有技术第二种获取密钥信息的方法相比,通过网络侧的身份管理服务器生成安全保护密钥,M2M 平台使用安全保护密钥对密钥信息进行安全处理后以密文的形式发送给 M2M 终端,从而有效地提高了传输密钥信息的安全性,此外,密钥信息以密文的形式发送给 M2M 终端时不依赖于底层通信网络,也就不限于短消息的形式,从而使可支持多种数据通信方式的 M2M 系统能够采取各种数据通信方式进行传输,因此有效地提高了 M2M 系统应用的灵活性。

## 附图说明

[0022] 图 1 为现有技术中,M2M 终端获取接入密码和基础密钥的方法流程示意图;

[0023] 图 2 为本发明实施例一中,密钥信息分发方法网络架构示意图;

[0024] 图 3 为本发明实施例二中,密钥信息分发方法流程示意图;

[0025] 图 4 为本发明实施例三中,当安全验证处理的执行主体为用户身份模块时的密钥信息分发方法具体实现流程示意图;

[0026] 图 5 为本发明实施例四中,当安全验证处理的执行主体为 M2M 终端时的密钥信息分发方法具体实现流程示意图;

[0027] 图 6 为本发明实施例五中,M2M 平台结构示意图;

[0028] 图 7 为本发明实施例六中,身份管理服务器结构示意图;

- [0029] 图 8 为本发明实施例七中, M2M 终端结构示意图 ;  
[0030] 图 9 为本发明实施例八中, 用户身份模块结构示意图。

## 具体实施方式

[0031] 下面结合各个附图对本发明实施例技术方案的主要实现原理、具体实施方式及其对应能够达到的有益效果进行详细地阐述。

### [0032] 实施例一

[0033] 本发明实施例一提出一种密钥信息分发方法网络架构示意图, 其结构如图 2 所示, 主要包括 M2M 平台、网络侧的身份管理服务器、M2M 终端和 M2M 终端内的用户身份模块。

[0034] 其中, M2M 平台主要用于在接收到 M2M 终端发送的注册请求后, 向网络侧的身份管理服务器发送密钥请求, 以及接收身份管理服务器发送的密钥响应消息, 密钥响应消息中携带有安全保护密钥和随机的密钥生成参数, 使用安全保护密钥对待分发给 M2M 终端的密钥信息进行安全处理, 并将处理后的密钥信息和上述密钥生成参数发送给 M2M 终端 ;

[0035] 网络侧的身份管理服务器主要用于在接收到密钥请求后, 根据随机的密钥生成参数生成安全保护密钥, 并将生成的安全保护密钥和上述密钥生成参数携带在密钥响应消息中发送给 M2M 平台 ;

[0036] M2M 终端内的用户身份模块主要用于根据上述密钥生成参数生成与上述安全保护密钥对应的安全保护验证密钥 ;

[0037] M2M 终端主要用于获取使用用户身份模块生成的安全保护验证密钥对 M2M 平台发送的密钥信息进行安全验证处理后得到的密钥信息, 获取到的密钥信息即为 M2M 平台分发的密钥信息。

[0038] 本发明实施例中, M2M 终端内的用户身份模块可以为用户身份模块 (SIM, Subscriber Identity Module) 卡, 也可以为用户识别模块 (UIM, User Identity Model) 卡, 还可以为全球用户识别 (USIM, Universal Subscriber Identity Module) 卡 ; 上述身份管理服务器可以但不限于为归属位置寄存器 (HLR, Home Location Register) 或归属用户服务器 (HSS, Home Subscriber Server) 。

### [0039] 实施例二

[0040] 基于本发明实施例一提出的网络架构, 本发明实施例二提出一种密钥信息分发方法, 如图 3 所示, 其具体处理过程如下 :

[0041] 步骤 31, M2M 平台接收到 M2M 终端发送的注册请求后, 向网络侧的身份管理服务器发送密钥请求。

[0042] 当 M2M 平台接收到 M2M 终端发送的注册请求后, 需要将接入密码下发给该 M2M 终端, 如果该 M2M 终端支持并启用了数据加密功能, 则 M2M 平台还需要将基础密钥下发给该 M2M 终端。

[0043] 本发明实施例二提出, 运营商在 M2M 系统中增加一种用于产生安全保护密钥和安全保护验证密钥的密钥生成机制以及用于在分发密钥信息时对密钥信息进行安全保护的安全处理算法和对密钥信息进行安全保护验证的安全验证处理算法。在网络侧, 新增加的密钥生成机制在身份管理服务器上实现, 新增加的安全处理算法在 M2M 平台实现 ; 在终端侧, 新增加的密钥生成机制在用户身份模块中实现, 新增加的安全验证处理算法即可在 M2M

终端上实现，也可以在 M2M 终端内的用户身份模块上实现。

[0044] M2M 接收到 M2M 终端发送的注册请求后，向网络侧的身份管理服务器发送密钥请求，请求身份管理服务器为其生成用于保护密钥信息的安全保护密钥。

[0045] 步骤 32，身份管理服务器根据随机的密钥生成参数生成安全保护密钥，并将生成的安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给所述 M2M 平台。

[0046] 身份管理服务器接收到 M2M 平台发送的密钥请求后，确认需要生成安全保护密钥，此时身份管理服务器可以按照下述两种方式生成安全保护密钥：

[0047] 第一种生成方式：身份管理服务器根据随机的密钥生成参数生成安全保护密钥，身份管理服务器先生成随机的密钥生成参数，然后基于新增的密钥生成机制，根据随机生成的密钥生成参数生成安全保护密钥；

[0048] 第二种生成方式，身份管理服务器根据用户身份模块的根密钥和随机的密钥生成参数生成安全保护密钥，此时 M2M 平台向身份管理服务器发送的密钥请求中携带有该 M2M 终端内的用户身份模块的标识，身份管理服务器接收到密钥请求后，根据密钥请求中携带的用户身份模块的标识，查找该用户身份模块对应的根密钥，身份管理服务器还需要生成随机的密钥生成参数，然后身份管理服务器基于新增的密钥生成机制，根据查找到的根密钥和随机生成的密钥生成参数生成安全保护密钥。

[0049] 其中，身份管理服务器查找用户身份模块对应的根密钥的过程可以但不限于为：身份管理服务器根据密钥请求中携带的用户身份模块的标识，检索该用户身份模块的签约信息，签约信息中包含该用户身份模块在签约时运营商为其分配的根密钥，身份管理服务器可以从检索到的签约信息中获取该用户身份模块对应的根密钥，因此身份管理服务器可以为保存用户身份模块的签约信息的 HLR 或 HSS。

[0050] 身份管理服务器生成安全保护密钥后，将生成的安全保护密钥和上述随机的密钥生成参数携带在密钥响应消息中发送给 M2M 平台，其中上述随机的密钥生成参数为密钥生成机制在产生安全保护密钥时使用的一些参数，例如随机数因子等。

[0051] 本发明实施例二提出，身份管理服务器可以根据随机的密钥生成参数生成一个安全保护密钥，此时身份管理服务器可以将生成的该安全保护密钥和密钥生成参数携带在密钥响应消息中发送给 M2M 平台；此外，身份管理服务器也可以根据随机的密钥生成参数生成至少两个安全保护密钥，其中，生成的安全保护密钥的个数可以预先设置，身份管理服务器将生成的各安全保护密钥和密钥生成参数携带在密钥响应消息中发送给 M2M 平台，其中，密钥生成参数中需要携带有身份管理服务器指示的、此次对密钥信息进行安全处理的安全保护密钥的标识，用于指示 M2M 平台使用各安全保护密钥中的第几个安全保护密钥来对密钥信息进行安全处理，本发明实施例二中，处理服务器可以在生成的安全保护密钥中随机选取此次对密钥信息进行安全处理的安全保护密钥，也可以按照预先设定的选取规则，在生成的安全保护密钥中选取此次对密钥信息进行安全处理的安全保护密钥，例如第一次选取第一个安全保护密钥，第二次选择第二个安全保护密钥。

[0052] 本发明实施例二中，安全保护密钥中可以包含加密密钥和 / 或完整性保护密钥，即安全保护密钥中可以包含加密密钥或完整性保护密钥，还可以既包含加密密钥，也包含完整性保护密钥。安全保护密钥中的加密密钥用于对密钥信息进行加密处理，完整性保护密钥用于对密钥信息进行完整性保护处理，不管是加密处理还是完整性保护处理，均可以

理解为对密钥信息进行安全处理。

[0053] 步骤 33,所述 M2M 平台使用所述安全保护密钥对待分发给所述 M2M 终端的密钥信息进行安全处理,以及将处理后的密钥信息和所述密钥生成参数发送给所述 M2M 终端。

[0054] M2M 平台接收到身份管理服务器发送的密钥响应消息后,从密钥响应消息中提取出安全保护密钥和密钥生成参数,根据提取出的安全保护密钥对待分发给上述 M2M 终端的密钥信息进行安全处理,然后将处理后的密钥信息和接收到的密钥生成参数发送给该 M2M 终端,例如 M2M 平台可以将处理后的密钥信息和接收到的密钥生成参数携带在注册响应消息中发送给该 M2M 终端。其中,密钥信息可以为接入密码,还可以为接入密码和基础密钥。

[0055] 若身份管理服务器生成一个安全保护密钥,则 M2M 平台可以直接根据该安全保护密钥对待分发给 M2M 终端的密钥信息进行安全处理;若身份管理服务器生成至少两个安全保护密钥,则 M2M 平台根据安全保护密钥对密钥信息进行安全处理时,先根据接收到的密钥生成参数中的安全保护密钥的标识,在身份管理服务器发送的各安全保护密钥中,选择出此次对密钥信息进行安全处理的安全保护密钥,身份管理服务器根据选择出的该安全保护密钥,对待分发给 M2M 终端的密钥信息进行安全处理。

[0056] 若安全保护密钥中包含加密密钥,则 M2M 平台根据安全保护密钥对密钥信息进行安全处理时,直接根据加密密钥对密钥信息进行加密处理;若安全保护密钥中包含完整性保护密钥,则 M2M 平台根据安全保护密钥对密钥信息进行安全处理时,直接根据完整性保护密钥对密钥信息进行完整性保护处理;若安全保护密钥中包含加密密钥和完整性保护密钥,则 M2M 平台根据安全保护密钥对密钥信息进行安全处理时,可以先根据加密密钥对密钥信息进行加密处理,然后根据完整性保护密钥对加密后的密钥信息进行完整性保护处理,也可以先根据完整性保护密钥对密钥信息进行完整性保护处理,然后再根据加密密钥对完整性保护后的密钥信息进行加密处理。

[0057] 步骤 34,所述 M2M 终端获取使用安全保护验证密钥对所述 M2M 平台发送的密钥信息进行安全验证处理后得到的密钥信息,其中,所述安全保护验证密钥由所述 M2M 终端内的用户身份模块根据所述密钥生成参数生成。

[0058] 所述 M2M 终端获取到的密钥信息即为 M2M 平台分发的密钥信息。

[0059] 若 M2M 平台将处理后的密钥信息和接收到的密钥生成参数携带在注册响应消息中发送给 M2M 终端,则该 M2M 终端在接收到注册响应消息后,以注册完成消息进行应答。

[0060] 本发明实施例二中, M2M 终端获取安全验证处理后的密钥信息的方式可以但不限于包含下述两种:

[0061] 第一种获取方式:M2M 终端将接收到的密钥信息和密钥生成参数携带在密钥传输消息中发送给该 M2M 终端内的用户身份模块,用户身份模块接收到密钥传输消息后,向 M2M 终端发送密钥确认消息进行应答,用户身份模块根据接收到的密钥生成参数生成安全保护验证密钥,安全保护验证密钥用于对安全处理后的密钥信息进行安全验证处理,用户身份模块使用生成的安全保护验证密钥对 M2M 终端发送的密钥信息进行安全验证处理,并将通过安全验证处理的密钥信息发送给 M2M 终端,例如将通过安全验证处理的密钥信息携带在密钥传输消息中发送给 M2M 终端,M2M 终端返回密钥确认消息进行应答。

[0062] 若身份管理服务器生成一个安全保护密钥,则用户身份模块根据 M2M 终端发送的密钥生成参数生成一个与安全保护密钥对应的安全保护验证密钥,此时,用户身份模块可

以直接使用生成的该安全保护验证密钥对 M2M 终端发送的密钥信息进行安全验证处理；此外，若身份管理服务器生成至少两个安全保护密钥，则用户身份模块根据 M2M 终端发送的密钥生成参数生成至少两个安全保护验证密钥，生成的安全保护验证密钥的数量和身份管理服务器生成的安全保护密钥的数量一致，且生成的各安全保护验证密钥和身份管理服务器生成的各安全保护密钥分别对应，用户身份模块生成至少两个安全保护验证密钥之后，根据 M2M 终端发送的密钥生成参数中的安全保护密钥的标识，在生成的各安全保护验证密钥中，选择出此次对密钥信息进行安全验证处理的安全保护验证密钥，用户身份模块根据选择的该安全保护验证密钥，对 M2M 终端发送的密钥信息进行安全验证处理。

[0063] 第二种获取方式：M2M 终端将接收到的密钥生成参数携带在密钥传输消息中发送给该 M2M 终端内的用户身份模块，用户身份模块接收到密钥传输消息后，向 M2M 终端发送密钥确认消息进行应答，用户身份模块根据接收到的密钥生成参数生成安全保护验证密钥，并将生成的安全保护验证密钥发送给该 M2M 终端，例如将生成的安全保护验证密钥携带在密钥传输消息中发送给该 M2M 终端，该 M2M 终端接收到密钥传输消息后返回密钥确认消息进行应答，M2M 终端使用接收到的安全保护验证密钥，对 M2M 平台发送的密钥信息进行安全验证处理，得到通过安全验证处理的密钥信息。

[0064] 若身份管理服务器生成一个安全保护密钥，则用户身份模块根据 M2M 终端发送的密钥生成参数生成一个与该安全保护密钥对应的安全保护验证密钥，此时，用户身份模块将该安全保护验证密钥发送给 M2M 终端，M2M 终端可以直接使用该安全保护验证密钥对 M2M 平台发送的密钥信息进行安全验证处理；此外，若身份管理服务器生成至少两个安全保护密钥，则用户身份模块根据 M2M 终端发送的密钥生成参数生成至少两个安全保护验证密钥，生成的安全保护验证密钥的数量和身份管理服务器生成的安全保护密钥的数量一致，且生成的各安全保护验证密钥和身份管理服务器生成的各安全保护密钥分别对应，用户身份模块生成至少两个安全保护验证密钥之后，根据 M2M 终端发送的密钥生成参数中的安全保护密钥的标识，在生成的各安全保护验证密钥中，选择出此次对密钥信息进行安全验证处理的安全保护验证密钥，用户身份模块将选择出的该安全保护验证密钥发送给 M2M 终端，M2M 终端直接使用该安全保护验证密钥对 M2M 平台发送的密钥信息进行安全验证处理。

[0065] 其中，用户身份模块可以按照下述两种方式生成安全保护验证密钥：

[0066] 与身份管理服务器生成安全保护密钥的第一种生成方式对应：用户身份模块基于新增的密钥生成机制，根据 M2M 终端发送的密钥生成参数生成安全保护验证密钥；

[0067] 与身份管理服务器生成安全保护密钥的第二种生成方式对应：用户身份模块根据自身的根密钥和密钥生成参数生成安全保护验证密钥，用户身份模块中存储有自身的根密钥，用户身份模块接收到密钥生成参数后，基于新增的密钥生成机制，根据自身存储的根密钥和 M2M 终端发送的密钥生成参数生成安全保护验证密钥。

[0068] 本发明实施例二中，安全保护验证密钥中可以包含解密密钥和 / 或完整性保护验证密钥，即安全保护验证密钥中可以包含解密密钥或完整性保护验证密钥，还可以既包含解密密钥，也包含完整性保护验证密钥。安全保护验证密钥中的解密密钥用于对加密后的密钥信息进行解密处理，完整性保护验证密钥用于对完整性保护后的密钥信息进行完整性保护验证处理，不管是解密处理还是完整性保护验证处理，均可以理解为对密钥信息进行安全验证处理。

[0069] 若安全保护验证密钥中包含解密密钥，则用户身份模块或 M2M 终端根据安全保护验证密钥对密钥信息进行安全验证处理时，直接根据该解密密钥对加密后的密钥信息进行解密处理，解密后的密钥信息即为通过安全验证处理的密钥信息；若安全保护验证密钥中包含完整性保护验证密钥，则用户身份模块或 M2M 终端根据安全保护验证密钥对密钥信息进行安全验证处理时，直接根据该完整性保护验证密钥对完整性保护后的密钥信息进行完整性保护验证处理，若验证通过，则完整性保护验证后的密钥信息即为通过安全验证处理的密钥信息；若安全保护验证密钥中包含解密密钥和完整性保护验证密钥，且 M2M 平台对密钥信息进行安全处理时先进行加密处理再进行完整性保护处理，则用户身份模块或 M2M 终端先根据安全保护验证密钥对密钥信息进行安全验证处理时，先根据完整性保护验证密钥，对密钥信息进行完整性保护验证处理，若验证通过，再根据解密密钥对密钥信息进行解密处理，解密后的密钥信息即为通过安全验证处理的密钥信息；若安全保护验证密钥中包含解密密钥和完整性保护验证密钥，且 M2M 平台对密钥信息进行安全处理时先进行安全保护处理再进行加密处理，则用户身份模块或 M2M 终端先根据安全保护验证密钥对密钥信息进行安全验证处理时，先根据解密密钥，对密钥信息进行解密处理，然后根据完整性保护验证密钥对密钥信息进行完整性保护验证处理，若验证通过，则完整性保护验证后的密钥信息即为通过安全验证处理的密钥信息。

[0070] 其中，安全保护密钥中的加密密钥和安全保护验证密钥中的解密密钥可以但不限于相同，安全保护密钥中的完整性保护密钥和安全保护验证密钥中的完整性保护验证密钥可以但不限于相同。

[0071] 本发明实施例二中，若身份管理服务器生成至少两个安全保护密钥，则身份管理服务器无需在后续每次接收到 M2M 平台发送的密钥请求后均生成安全保护密钥，只要在密钥生成参数中携带指示此次对密钥信息进行安全处理的安全保护密钥即可，因此有效地节省了身份管理服务器的处理资源。

[0072] M2M 终端获取到 M2M 平台分发的密钥信息后，使用获取到的密钥信息中的接入密码登录至 M2M 平台，并在登录成功后，使用获取到的密钥信息中的基础密钥实现数据加密并与 M2M 平台进行数据交互。

[0073] 此外，本发明实施例二提出的密钥信息分发方法可以但不限于应用于无线机器通信协议 (WMMP, Wireless M2M Protocol) 场景。

[0074] 由上述处理过程可知，本发明实施例技术方案中，M2M 平台接收到 M2M 终端发送的注册请求后，向网络侧的身份管理服务器发送密钥请求，身份管理服务器根据随机的密钥生成参数生成安全保护密钥，并将生成的安全保护密钥和所述密钥生成参数携带有密钥响应消息中发送给 M2M 平台，M2M 平台使用所述安全保护密钥对待分发给 M2M 终端的密钥信息进行安全处理，以及将处理后的密钥信息和密钥生成参数发送给 M2M 终端，M2M 终端内的用户身份模块根据密钥生成参数生成与安全保护密钥对应的安全保护验证密钥，M2M 终端获取使用安全保护验证密钥对 M2M 平台发送的密钥信息进行安全验证处理后得到的密钥信息，获取到的密钥信息即为 M2M 平台分发的密钥信息。由上可见，本发明实施例技术方案与现有技术第一种获取密钥信息的方法相比，能够在 M2M 终端注册至 M2M 系统时自动实现 M2M 终端的密钥信息的分发，免除了用户对 M2M 终端进行密钥配置操作的复杂性，提高了用户体验，同时在 M2M 终端发起注册时将密钥信息分发给 M2M 终端，因此 M2M 平台可以在接

收到 M2M 终端的注册请求时动态生成密钥信息,有效地提高了传输密钥信息的安全性;本发明实施例技术方案与现有技术第二种获取密钥信息的方法相比,通过网络侧的身份管理服务器生成安全保护密钥,M2M 平台使用安全保护密钥对密钥信息进行安全处理后以密文的形式发送给 M2M 终端,从而有效地提高了传输密钥信息的安全性,此外,密钥信息以密文的形式发送给 M2M 终端时不依赖于底层通信网络,也就不限于短消息的形式,从而使可支持多种数据通信方式的 M2M 系统能够采取各种数据通信方式进行传输,因此有效地提高了 M2M 系统应用的灵活性。

[0075] 下面给出更为详细的实施方式。

[0076] 根据安全验证处理的执行主体不同,下面分别以实施例三和实施例四分别详细介绍本发明实施例中的密钥信息分发方法。

[0077] 实施例三

[0078] 如图 4 所示,为本发明实施例三提出的当安全验证处理的执行主体为用户身份模块时的密钥信息分发方法具体实现流程示意图,其具体处理流程如下:

[0079] 步骤 41, M2M 终端向 M2M 平台发起注册请求;

[0080] 步骤 42, M2M 平台向 HLR/HSS 发送密钥请求,请求 HLR/HSS 为其生成用于保护密钥信息(接入密码和基础密钥)的安全保护密钥(加密密钥和完整性保护密钥),密钥请求中携带有 M2M 终端内的(U)SIM 卡的标识,SIM 卡或 USIM 卡可以称为(U)SIM 卡;

[0081] 步骤 43, HLR/HSS 根据(U)SIM 卡的标识检索 M2M 终端的签约信息,以获取(U)SIM 卡在签约时运营商为其分配的根密钥,基于此根密钥和随机的密钥生成参数,HLR/HSS 依照新增加的密钥生成机制生成一套或多套安全保护密钥;

[0082] 步骤 44, HLR/HSS 向 M2M 平台发送密钥响应消息,其中携带有步骤 43 生成的加密密钥、完整性保护密钥以及密钥生成参数,在身份管理服务器生成多套密钥信息的情况下,密钥生成参数中还将包含此次使用的安全保护密钥的标识;

[0083] 步骤 45, M2M 平台使用从 HLR/HSS 接收到的安全保护密钥对密钥信息进行安全处理(先使用加密密钥对密钥信息进行加密,然后使用完整性保护密钥进行完整性保护处理),之后通过注册响应消息将安全处理后的密钥信息以及从 HLR/HSS 接收到的密钥生成参数发送给 M2M 终端,在身份管理服务器生成多套密钥信息的情况下,M2M 平台先根据密钥生成参数中携带的安全保护密钥的标识,在接收到的各安全保护密钥中选择进行安全处理的安全保护密钥,然后使用选择出的安全保护密钥对密钥信息进行安全处理;

[0084] 步骤 46, M2M 终端以注册完成消息对 M2M 平台进行响应;

[0085] 步骤 47, M2M 终端通过密钥传输消息将接收到的密钥信息以及密钥生成参数传递给(U)SIM 卡;

[0086] 步骤 48, (U)SIM 卡向 M2M 终端发送密钥确认消息进行应答;

[0087] 步骤 49, (U)SIM 卡根据卡内存储的根密钥以及接收到的密钥生成参数,依照新增加的密钥生成机制生成一套或多套安全保护验证密钥,安全保护验证密钥包含解密密钥和完整性保护验证密钥,且安全保护验证密钥和安全保护密钥对应;

[0088] 步骤 410, (U)SIM 卡根据生成的安全保护验证密钥对接收到的密钥信息进行安全验证处理(先使用完整性保护验证密钥进行完整性保护验证处理,在完整性保护验证正确通过的情况下,使用解密密钥进行解密),若(U)SIM 卡生成多套安全保护验证密钥,则根据

密钥生成参数提供的安全保护密钥的标识选择出此次进行安全验证处理的安全保护验证密钥；

- [0089] 步骤 411, (U) SIM 卡通过密钥传输消息将密钥信息发送给 M2M 终端；
- [0090] 步骤 412, M2M 终端返回密钥确认消息进行应答；
- [0091] 步骤 413, M2M 终端使用接入密码登录至 M2M 平台；
- [0092] 步骤 414, 登录成功后, M2M 终端使用基础密钥实现数据加密并与 M2M 平台进行数据交互。

#### [0093] 实施例四

[0094] 如图 5 所示, 为本发明实施例四提出的当安全验证处理的执行主体为 M2M 终端时的密钥信息分发方法具体实现流程示意图, 其具体处理流程如下：

- [0095] 步骤 51, M2M 终端向 M2M 平台发起注册请求；
- [0096] 步骤 52, M2M 平台向 HLR/HSS 发送密钥请求, 请求 HLR/HSS 为其生成用于保护密钥信息(接入密码和基础密钥)的安全保护密钥(加密密钥和完整性保护密钥), 密钥请求中携带有 M2M 终端内的 (U) SIM 卡的标识, SIM 卡或 USIM 卡可以称为 (U) SIM 卡；
- [0097] 步骤 53, HLR/HSS 根据 (U) SIM 卡的标识检索 M2M 终端的签约信息, 以获取 (U) SIM 卡在签约时运营商为其分配的根密钥, 基于此根密钥和随机的密钥生成参数, HLR/HSS 依照新增加的密钥生成机制生成一套或多套安全保护密钥；
- [0098] 步骤 54, HLR/HSS 向 M2M 平台发送密钥响应消息, 其中携带有步骤 43 生成的加密密钥、完整性保护密钥以及密钥生成参数, 在身份管理服务器生成多套密钥信息的情况下, 密钥生成参数中还将包含此次使用的安全保护密钥的标识；
- [0099] 步骤 55, M2M 平台使用从 HLR/HSS 接收到的安全保护密钥对密钥信息进行安全处理(先使用加密密钥对密钥信息进行加密, 然后使用完整性保护密钥进行完整性保护处理), 之后通过注册响应消息将安全处理后的密钥信息以及从 HLR/HSS 接收到的密钥生成参数发送给 M2M 终端, 在身份管理服务器生成多套密钥信息的情况下, M2M 平台先根据密钥生成参数中携带的安全保护密钥的标识, 在接收到的各安全保护密钥中选择进行安全处理的安全保护密钥, 然后使用选择出的安全保护密钥对密钥信息进行安全处理；
- [0100] 步骤 56, M2M 终端以注册完成消息对 M2M 平台进行响应；
- [0101] 步骤 57, M2M 终端通过密钥传输消息将接收到的密钥生成参数传递给 (U) SIM 卡；
- [0102] 步骤 58, (U) SIM 卡向 M2M 终端发送密钥确认消息进行应答；
- [0103] 步骤 59, (U) SIM 卡根据卡内存储的根密钥以及接收到的密钥生成参数, 依照新增加的密钥生成机制生成一套或多套安全保护验证密钥, 安全保护验证密钥包含解密钥和完整性保护验证密钥, 且安全保护验证密钥和安全保护密钥对应；
- [0104] 步骤 510, (U) SIM 卡通过密钥传输消息将生成的安全保护验证密钥发送给 M2M 终端, 若 (U) SIM 卡生成多套安全保护验证密钥, 则根据密钥生成参数提供的安全保护密钥的标识选择出此次进行安全验证处理的安全保护验证密钥；
- [0105] 步骤 511, M2M 终端返回密钥确认消息进行应答；
- [0106] 步骤 512, M2M 终端使用 (U) SIM 卡提供的安全保护验证密钥, 对接收到的密钥信息进行安全验证处理(先使用完整性保护验证密钥进行完整性保护验证处理, 在完整性保护验证正确通过的情况下, 使用解密密钥进行解密)；

[0107] 步骤 513, M2M 终端使用接入密码登录至 M2M 平台；  
[0108] 步骤 514, 登录成功后, M2M 终端使用基础密钥实现数据加密并与 M2M 平台进行数据交互。

[0109] 实施例五

[0110] 基于本发明实施例二提出的密钥信息分发方法, 本发明实施例五提出一种 M2M 平台, 其结构如图 6 所示, 包括 :

[0111] 注册请求接收单元 61, 用于接收 M2M 终端发送的注册请求；  
[0112] 密钥请求发送单元 62, 用于在注册请求接收单元 61 接收到 M2M 终端发送的注册请求后, 向网络侧的身份管理服务器发送密钥请求；  
[0113] 密钥响应消息接收单元 63, 用于接收所述身份管理服务器发送的携带有安全保护密钥和随机的密钥生成参数的密钥响应消息, 所述安全保护密钥是所述身份管理服务器根据所述密钥生成参数生成的；  
[0114] 安全处理单元 64, 用于使用所述安全保护密钥对待分发给所述 M2M 终端的密钥信息进行安全处理；  
[0115] 密钥信息发送单元 65, 用于将安全处理单元 64 处理后的密钥信息和所述密钥生成参数发送给所述 M2M 终端。

[0116] 较佳地, 所述身份管理服务器根据所述密钥生成参数生成至少两个安全保护密钥, 所述密钥响应消息接收单元 63 接收到的密钥生成参数中携带有身份管理服务器指示的、此次对密钥信息进行安全处理的安全保护密钥的标识；

[0117] 所述安全处理单元 64 具体包括 :

[0118] 安全保护密钥选择子单元, 用于根据密钥响应消息接收单元 63 接收到的密钥生成参数中携带的安全保护密钥的标识, 在密钥响应消息接收单元 63 接收到的各安全保护密钥中选择出此次对密钥信息进行安全处理的安全保护密钥；

[0119] 安全处理子单元, 用于使用安全保护密钥选择子单元选择出的安全保护密钥, 对待分发给所述 M2M 终端的密钥信息进行安全处理。

[0120] 实施例六

[0121] 基于本发明实施例二提出的密钥信息分发方法, 本发明实施例六提出一种身份管理服务器, 其结构如图 7 所示, 包括 :

[0122] 密钥请求接收单元 71, 用于接收 M2M 平台发送的密钥请求；  
[0123] 安全保护密钥生成单元 72, 用于在密钥请求接收单元 71 接收到密钥请求后, 根据随机的密钥生成参数生成安全保护密钥；  
[0124] 密钥响应消息发送单元 73, 用于将安全保护密钥生成单元 72 生成的安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给所述 M2M 平台。  
[0125] 较佳地, 安全保护密钥生成单元 72, 具体用于在密钥请求接收单元 71 接收到密钥请求后, 根据随机的密钥生成参数, 生成至少两个安全保护密钥；  
[0126] 密钥响应消息发送单元 73, 具体用于将安全保护密钥生成单元 72 生成的各安全保护密钥和所述密钥生成参数携带在密钥响应消息中发送给所述 M2M 平台, 所述密钥生成参数中携带有所述身份管理服务器指示的、此次对密钥信息进行安全处理的安全保护密钥的标识。

[0127] 较佳地，密钥请求接收单元 71 接收到的所述密钥请求中携带有用户身份模块的标识；

[0128] 安全保护密钥生成单元 72 具体包括：

[0129] 根密钥查找子单元，用于根据密钥请求接收单元 71 接收到的密钥请求中携带的用户身份模块的标识，查找所述用户身份模块对应的根密钥；

[0130] 安全保护密钥生成子单元，用于根据根密钥查找子单元查找到的根密钥和随机的密钥生成参数，生成安全保护密钥。

[0131] 实施例七

[0132] 基于本发明实施例二提出的密钥信息分发方法，本发明实施例七提出一种 M2M 终端，其结构如图 8 所示，包括：

[0133] 密钥信息接收单元 81，用于接收 M2M 平台发送的、使用安全保护密钥对待发送给所述 M2M 终端的密钥信息进行安全处理后的密钥信息和密钥生成参数；

[0134] 密钥信息获取单元 82，用于获取使用安全保护验证密钥对密钥信息接收单元 81 接收到的密钥信息进行安全验证处理后得到的密钥信息，其中，所述安全保护验证密钥由所述 M2M 终端内的用户身份模块根据所述密钥生成参数生成；

[0135] 密钥信息确认单元 83，用于将密钥信息获取单元 82 获取到的密钥信息确认为 M2M 平台分发的密钥信息。

[0136] 较佳地，密钥信息获取单元 82 具体包括：

[0137] 第一密钥传输消息发送子单元，用于将密钥信息接收单元 81 接收到的密钥信息和密钥生成参数携带在密钥传输消息中发送给所述 M2M 终端内的用户身份模块；

[0138] 密钥信息接收子单元，用于接收通过安全验证处理的密钥信息，通过安全验证处理的密钥信息是所述用户身份模块根据接收到的密钥生成参数，生成与所述安全保护密钥对应的安全保护验证密钥，以及使用生成的安全保护验证密钥对第一密钥传输消息发送子单元发送的密钥信息进行安全验证处理后发送的。

[0139] 更佳地，密钥信息获取单元 82 具体包括：

[0140] 第二密钥传输消息发送子单元，用于将密钥信息接收单元 81 接收到的密钥生成参数携带在密钥传输消息中发送给所述 M2M 终端内的用户身份模块；

[0141] 安全保护验证密钥接收子单元，用于接收所述用户身份模块发送的与所述安全保护密钥对应的安全保护验证密钥，所述安全保护验证密钥是所述用户身份模块根据接收到的所述密钥生成参数生成的；

[0142] 安全验证处理子单元，用于使用安全保护验证密钥接收子单元接收到的安全保护验证密钥，对密钥信息接收单元 81 接收到的密钥信息进行安全验证处理，得到通过安全验证处理的密钥信息。

[0143] 实施例八

[0144] 基于本发明实施例二提出的密钥信息分发方法，本发明实施例八提出一种用户身份模块，置于 M2M 终端内，其结构如图 9 所示，包括：

[0145] 密钥生成参数获取单元 91，用于获取生成安全保护密钥的随机的安全生成参数，安全保护密钥用于 M2M 平台对待发送给所述 M2M 终端的密钥信息进行安全处理；

[0146] 安全保护验证密钥生成单元 92，用于根据密钥生成参数获取单元 91 获取到的所

述密钥生成参数,生成与所述安全保护密钥对应的安全保护验证密钥,所述安全保护验证密钥用于对安全处理后的密钥信息进行安全验证处理。

[0147] 较佳地,密钥生成参数获取单元 91,具体用于接收所述 M2M 终端发送的密钥传输消息,所述密钥传输消息中携带有生成安全保护密钥的随机的安全生成参数、以及 M2M 平台使用安全保护密钥对待发送给所述 M2M 终端的密钥信息进行安全处理后得到的密钥信息;

[0148] 安全保护验证密钥生成单元 92,具体用于根据密钥生成参数获取单元 91 接收到的所述密钥生成参数,生成与所述安全保护密钥对应的安全保护验证密钥;

[0149] 所述用户身份模块还包括:

[0150] 安全验证处理单元,用于使用安全保护验证密钥生成单元 92 生成的安全保护验证密钥,对密钥生成参数获取单元 91 接收到的密钥信息进行安全验证处理;

[0151] 密钥信息发送单元,用于将通过安全验证处理单元进行安全验证处理后的密钥信息发送给所述 M2M 终端。

[0152] 更佳地,密钥生成参数获取单元 91 接收到的密钥生成参数中携带有此次对密钥信息进行安全处理的安全保护密钥的标识;

[0153] 安全保护验证密钥生成单元 92,具体用于根据密钥生成参数获取单元 91 接收到的所述密钥生成参数,生成与各安全保护密钥分别对应的至少两个安全保护验证密钥;

[0154] 安全验证处理单元,具体用于根据密钥生成参数获取单元 91 接收到的密钥生成参数中携带的安全保护密钥的标识,在安全保护验证密钥生成单元 92 生成的各安全保护验证密钥中选择出此次对密钥信息进行安全验证处理的安全保护验证密钥,并使用选择出的安全保护验证密钥对接收到的密钥信息进行安全验证处理。

[0155] 较佳地,密钥生成参数获取单元 91,具体用于接收所述 M2M 终端发送的密钥传输消息,所述密钥传输消息中携带有生成安全保护密钥的随机的安全生成参数;

[0156] 安全保护验证密钥生成单元 92,具体用于根据密钥生成参数获取单元 91 接收到的所述密钥生成参数,生成与所述安全保护密钥对应的安全保护验证密钥;

[0157] 所述用户身份模块还包括:

[0158] 安全保护验证密钥发送单元,用于将安全保护验证密钥生成单元 92 生成的安全保护验证密钥发送给所述 M2M 终端,所述安全保护验证密钥用于所述 M2M 终端对使用安全保护密钥对密钥信息进行安全处理后的密钥信息进行安全验证处理。

[0159] 更佳地,密钥生成参数获取单元 91 接收到的密钥生成参数中携带有此次对密钥信息进行安全处理的安全保护密钥的标识;

[0160] 安全保护验证密钥生成单元 92,具体用于根据密钥生成参数获取单元 91 接收到的所述密钥生成参数,生成与各安全保护密钥分别对应的至少两个安全保护验证密钥;

[0161] 安全保护验证密钥发送单元,具体用于根据密钥生成参数获取单元 91 接收到的密钥生成参数中携带的安全保护密钥的标识,在安全保护验证密钥生成单元 92 生成的各安全保护验证密钥中选择出此次对密钥信息进行安全验证处理的安全保护验证密钥,并将选择出的安全保护验证密钥发送给所述 M2M 终端。

[0162] 较佳地,安全保护验证密钥生成单元 92,具体用于根据自身的根密钥以及密钥生成参数获取单元 91 获取到的所述密钥生成参数,生成与所述安全保护密钥对应的安全保

护验证密钥。

[0163] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

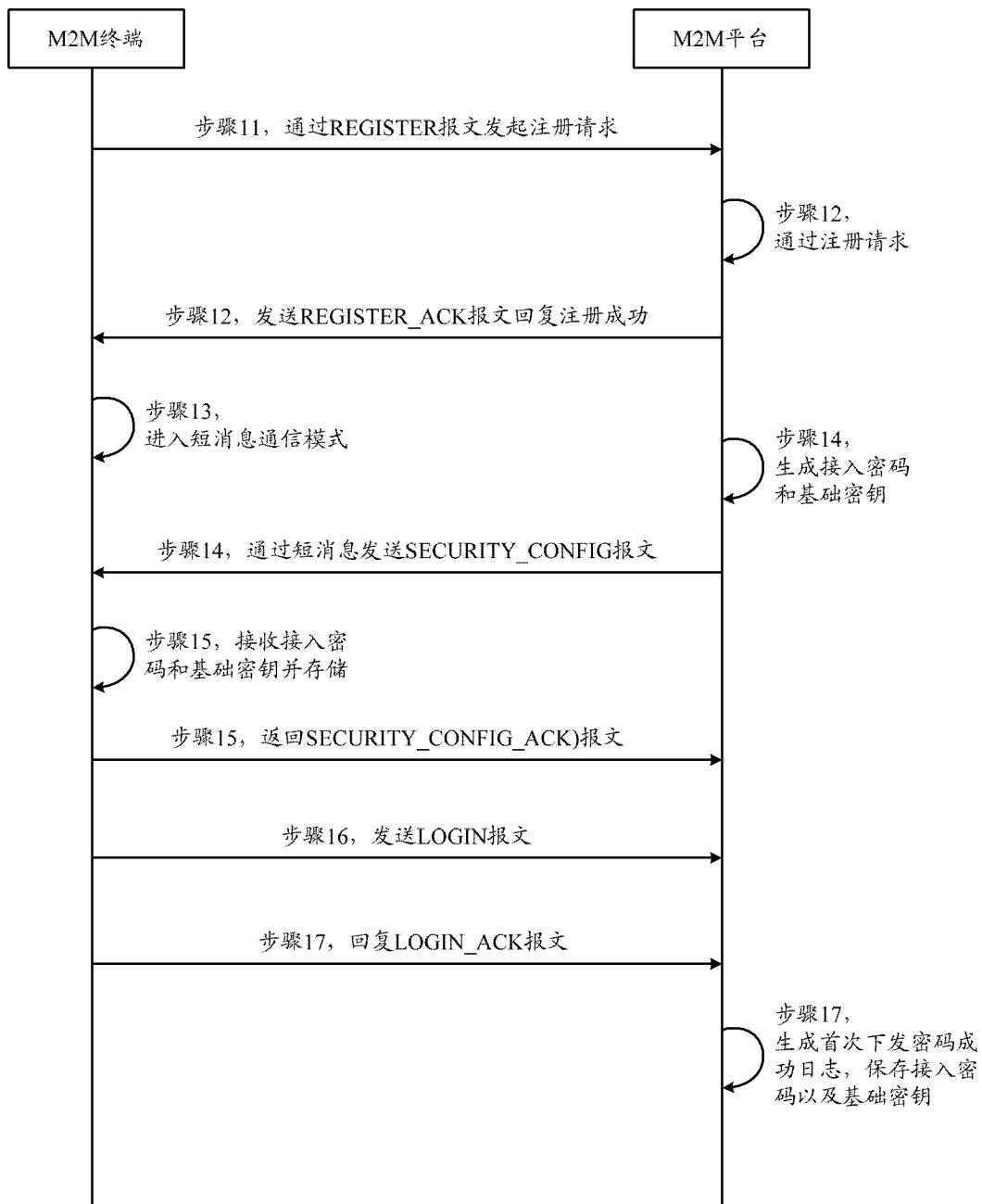


图 1

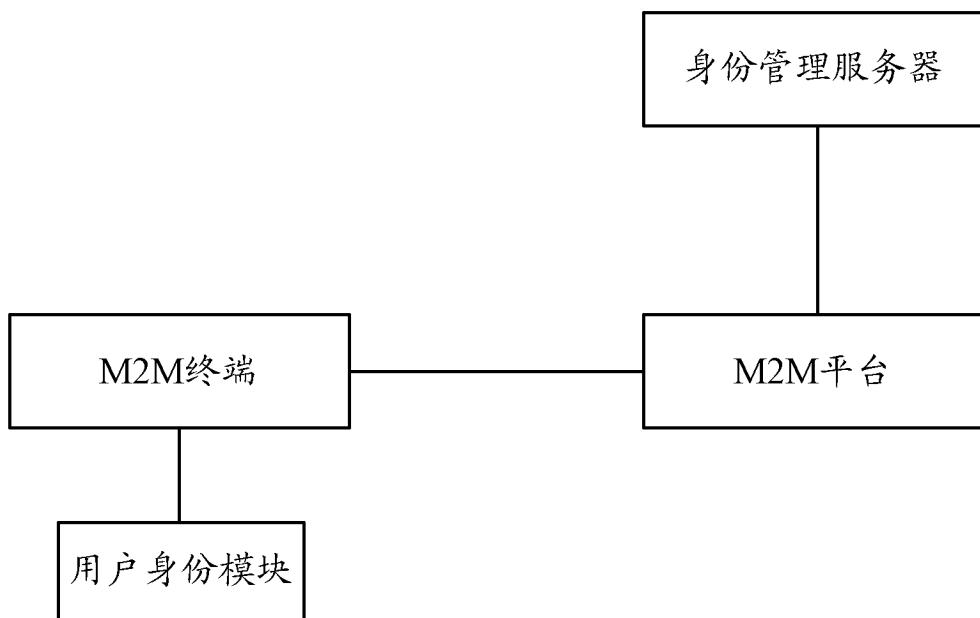


图 2

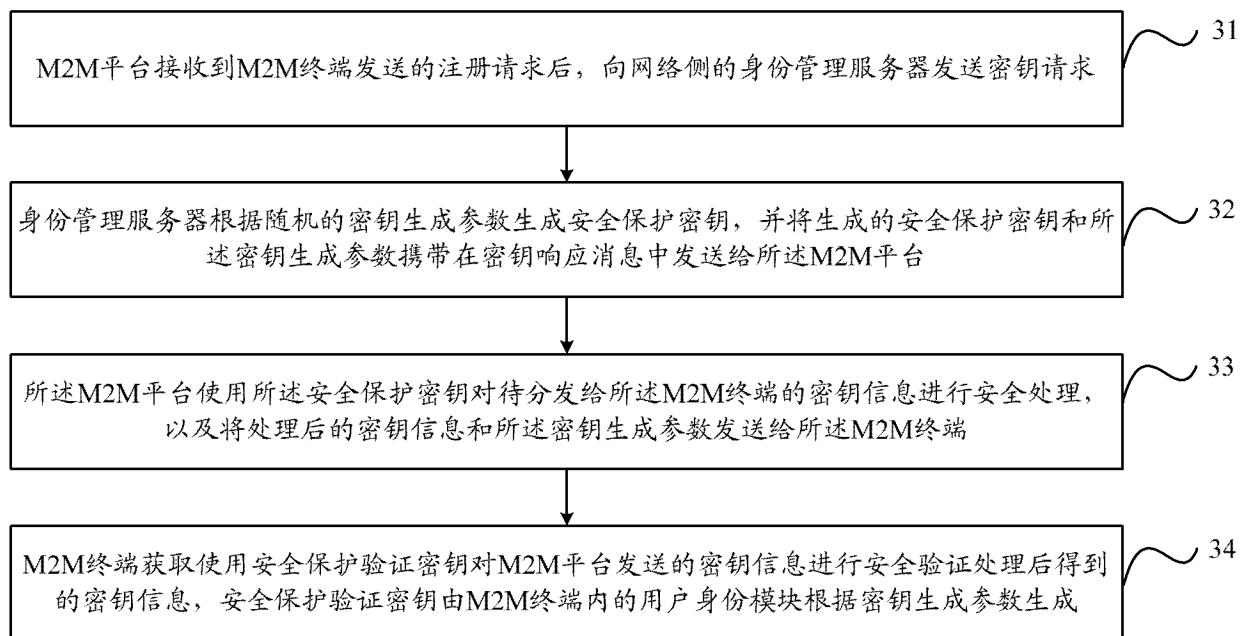


图 3

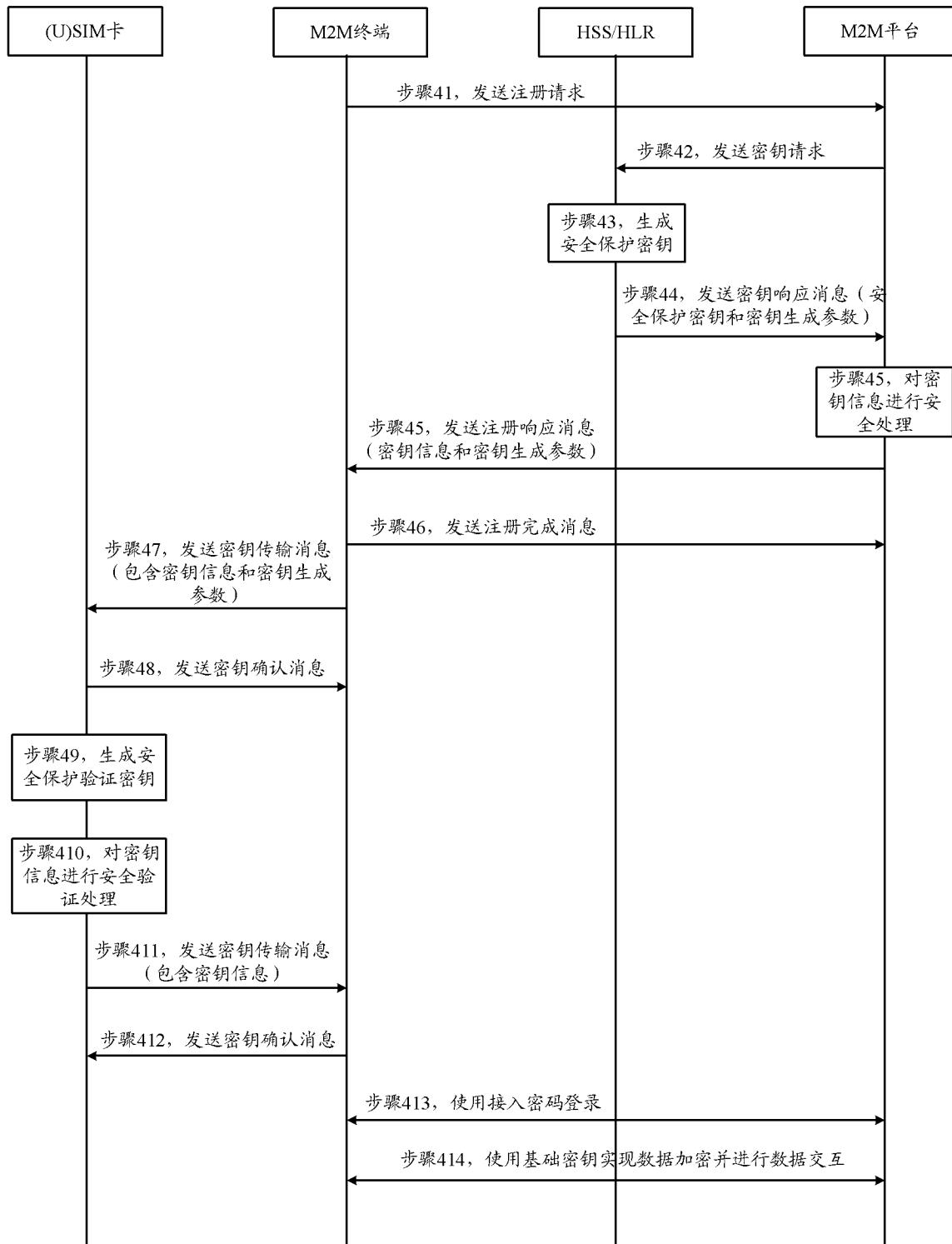


图 4

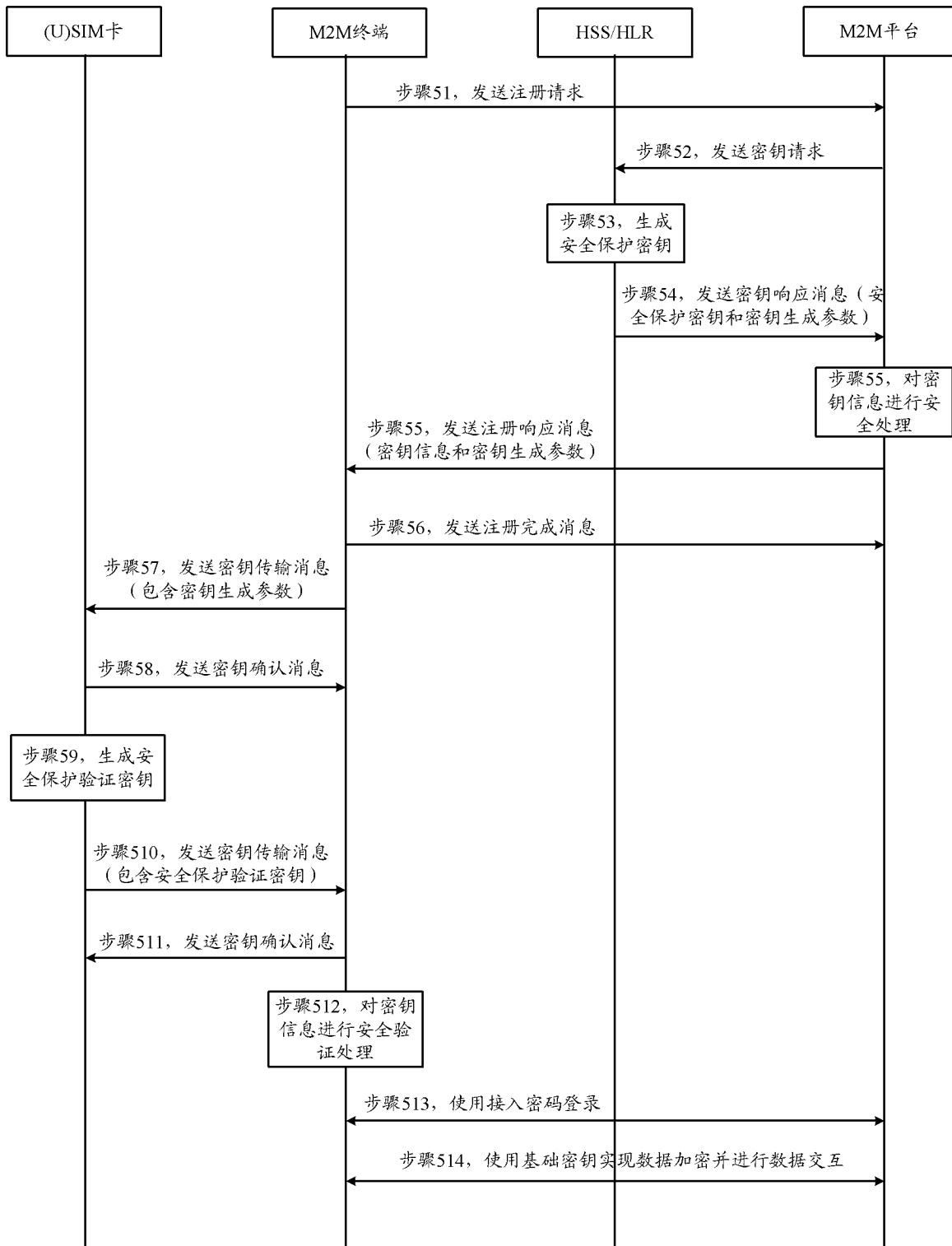


图 5

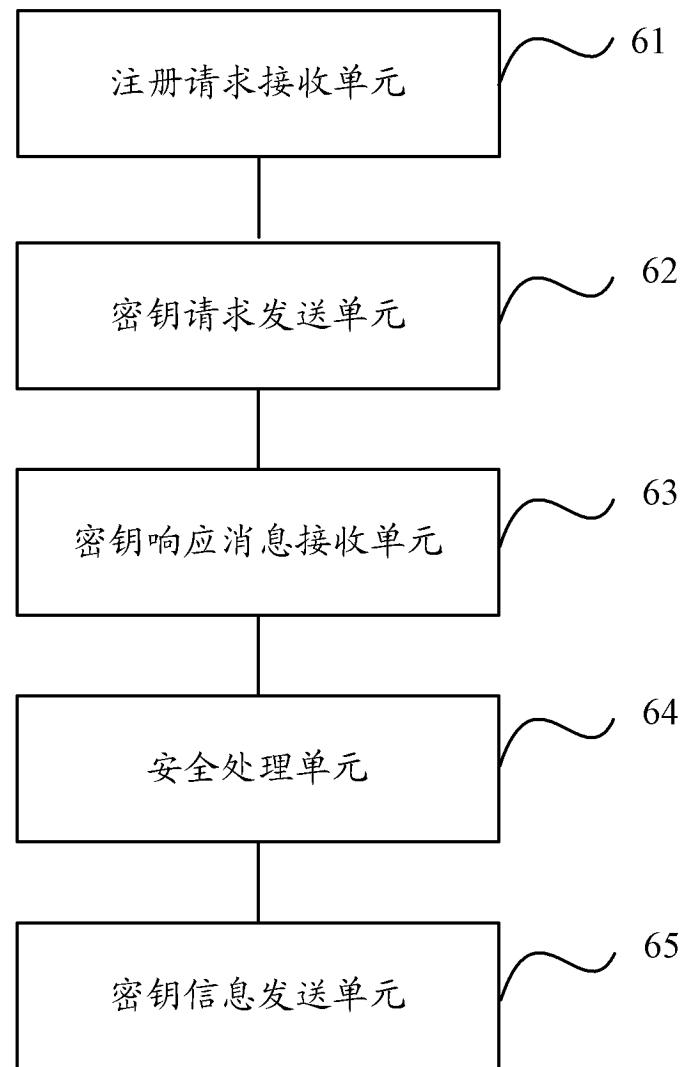


图 6

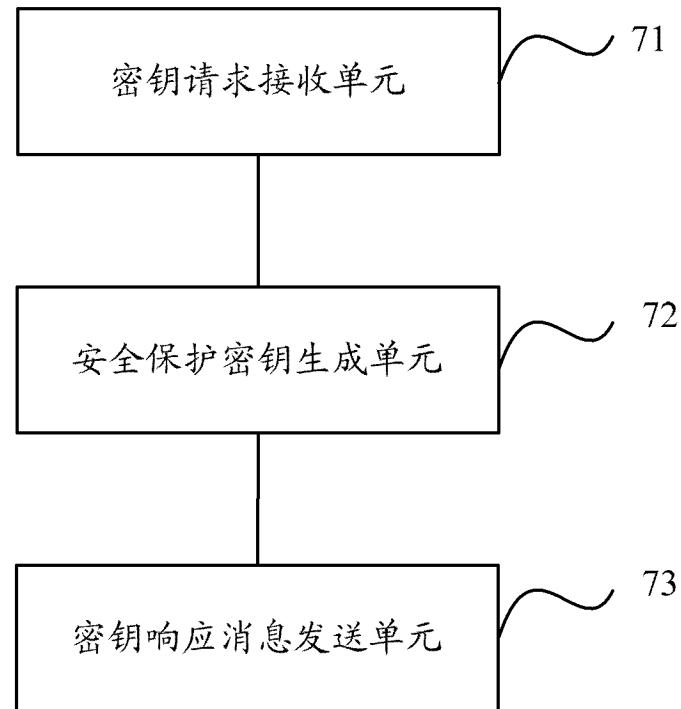


图 7

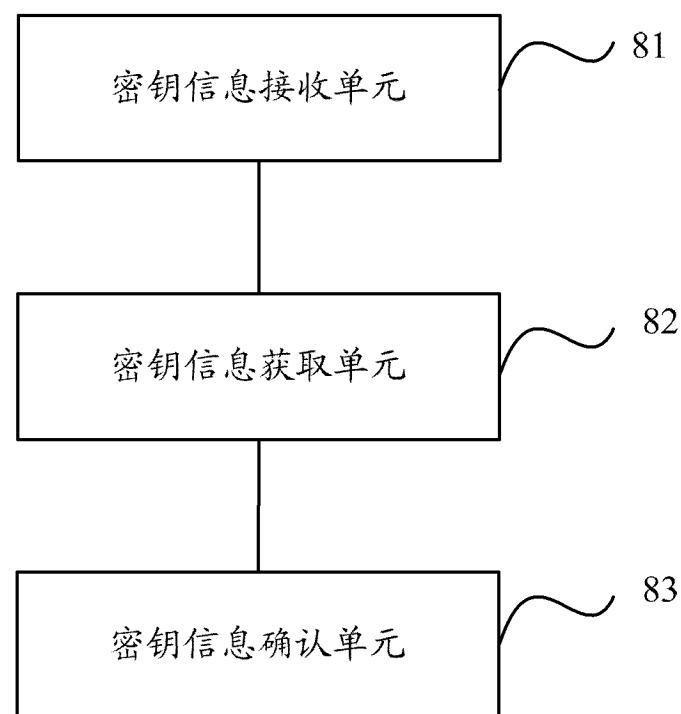


图 8

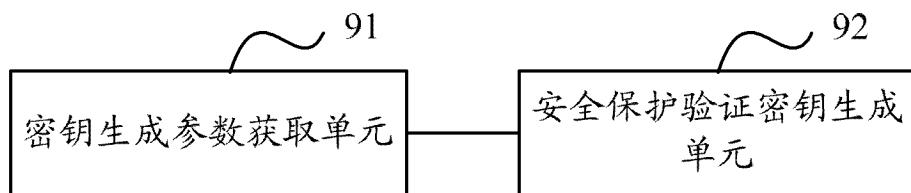


图 9