(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 109863770 B
(45)授权公告日 2021.08.17

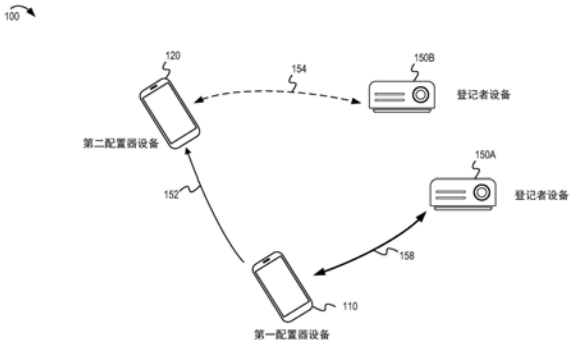
(21)申请号 201780064120.X
(22)申请日 2017.08.25
(65)同一申请的已公布的文献号
申请公布号 CN 109863770 A
(43)申请公布日 2019.06.07
(30)优先权数据
62/410,309 2016.10.19 US
15/648,437 2017.07.12 US
(85)PCT国际申请进入国家阶段日
2019.04.17
(86)PCT国际申请的申请数据
PCT/US2017/048560 2017.08.25
(87)PCT国际申请的公布数据
WO2018/075135 EN 2018.04.26
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚
(72)发明人 R·卡马罗塔 J·K·马利宁
P·丁娜功西素帕普
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 张扬 王英
(51)Int.Cl.
H04W 12/041(2021.01)
H04W 12/0433(2021.01)
H04L 9/08(2006.01)
(56)对比文件
WO 2015094326 A1,2015.06.25
US 2014258724 A1,2014.09.11
CN 105657785 A,2016.06.08
WO 2015094326 A1,2015.06.25
MORIARTY K ET AL.PERSONAL INFORMATION EXCHANGE SYNTAX V1.1.《RFC7292》.2014,
审查员 张长梅
权利要求书4页 说明书16页 附图10页

(54)发明名称

用于设备设定协议的配置器密钥包

(57)摘要

本公开内容提供了用于增强设备设定协议(DPP)以支持多个配置器的系统、方法和装置,包括编码在计算机存储介质上的计算机程序。在一个方面中,第一配置器设备可以导出配置器密钥包。在一个方面中,配置器密钥包可以用于对配置器密钥的备份和恢复。配置器密钥包可以包括配置器私有签名密钥,以及可选地,包括配置器公共验证密钥。第二配置器设备可以获得配置器密钥包,以及还可以获得能够用于解密配置器密钥包的解密信息。因此,在另一个方面中,第一配置器设备和第二配置器设备两者可以使用相同的配置器密钥与设备设定协议来将登记者配置到网络。



CN 109863770 B

1.一种由网络的第一配置器设备执行的方法,包括:

由所述第一配置器设备实现设备设定协议,在所述设备设定协议中,所述第一配置器设备被配置为使用配置器私有签名密钥来将登记者设备登记到所述网络;

生成配置器密钥包,所述配置器密钥包至少包括与所述第一配置器设备相关联的所述配置器私有签名密钥;

对所述配置器密钥包的至少一部分进行加密;以及

将所述配置器密钥包作为备份存储在存储位置处,以用于由第二配置器设备进行后续恢复,其中,相同的配置器私有签名密钥和相同的配置器公共验证密钥是在包括所述第二配置器设备的多个配置器之间共享的,所述第二配置器设备用于根据所述设备设定协议来将不同的登记者设备登记到所述网络。

2.根据权利要求1所述的方法,其中,所述配置器密钥包还包括与所述配置器私有签名密钥相关联的配置器公共验证密钥。

3.根据权利要求1所述的方法,其中,对所述配置器密钥包的所述至少一部分进行加密包括:使用与所述配置器私有签名密钥不同的加密密钥,来对所述配置器密钥包进行加密。

4.根据权利要求1所述的方法,其中,对所述配置器密钥包的至少所述部分进行加密包括:使用私钥加密技术,对所述配置器私有签名密钥进行加密,以及将对所述私钥加密技术的指示包括在所述配置器密钥包的报头中。

5.根据权利要求1所述的方法,其中,存储所述配置器密钥包包括:

生成包括所述配置器密钥包和解密信息的数字包络,其中,所述解密信息使所述第二配置器设备能够解密所述配置器密钥包的至少所述部分。

6.根据权利要求1所述的方法,其中,所述存储位置是从包括以下各项的组中选择的至少一个成员:所述第一配置器设备的存储器、网络共享位置、个人计算机、家庭服务器、基于云的存储服务、以及无线网络的接入点(AP)。

7.根据权利要求1所述的方法,还包括:

由所述第一配置器设备从所述存储位置取回所述配置器密钥包的所述备份;

对所述配置器密钥包的至少所述部分进行解密;以及

从所述配置器密钥包获得所述配置器私有签名密钥。

8.根据权利要求7所述的方法,还包括:

至少部分地基于从所述配置器密钥包获得的所述配置器私有签名密钥来确定配置器公共验证密钥。

9.根据权利要求1所述的方法,还包括:

确定所述配置器密钥包在所述存储位置处的位置地址;以及

向所述第二配置器设备提供所述位置地址。

10.根据权利要求1所述的方法,还包括:

向所述第二配置器设备提供解密信息,其中,所述解密信息使所述第二配置器设备能够解密所述配置器密钥包的至少所述部分以及获得所述配置器私有签名密钥。

11.根据权利要求10所述的方法,其中,所述解密信息包括从包括以下各项的组中选择的至少一个成员:所述配置器密钥包在所述存储位置处的位置地址、以及可用于解密所述配置器密钥包的至少所述部分的加密密钥。

12.根据权利要求10所述的方法,其中,提供所述解密信息包括在来自从包括以下各项的组中选择的至少一个成员的信号中传送所述解密信息:显示器、扬声器、光信号、传感器接口、和所述第一配置器设备的短程射频接口。

13.根据权利要求10所述的方法,其中,提供所述解密信息包括:显示具有编码在其中的所述解密信息的图像。

14.根据权利要求13所述的方法,其中,所述图像是条形码或快速响应(QR)码图像。

15.一种第一配置器设备,包括:

处理器;以及

存储器,其具有存储在其中的指令,当所述指令被所述处理器执行时,使得所述第一配置器设备进行以下操作:

实现设备设定协议,在所述设备设定协议中,所述第一配置器设备被配置为使用配置器私有签名密钥来将登记者设备登记到网络;

生成配置器密钥包,所述配置器密钥包至少包括与所述第一配置器设备相关联的所述配置器私有签名密钥;

对所述配置器密钥包的至少一部分进行加密;以及

将所述配置器密钥包作为备份存储在存储位置处,以用于第二配置器设备进行后续恢复,其中,相同的配置器私有签名密钥和相同的配置器公共验证密钥是在包括所述第二配置器设备的多个配置器之间共享的,所述第二配置器设备用于根据所述设备设定协议来将不同的登记者设备登记到所述网络。

16.根据权利要求15所述的第一配置器设备,其中,当所述指令被所述处理器执行时,还使所述第一配置器设备进行以下操作:

使用与所述配置器私有签名密钥不同的加密密钥,来对所述配置器密钥包进行加密。

17.根据权利要求15所述的第一配置器设备,其中,当所述指令被所述处理器执行时,还使所述第一配置器设备进行以下操作:

使用私钥加密技术,来对所述配置器私有签名密钥进行加密;以及

将对所述私钥加密技术的指示包括在所述配置器密钥包的报头中。

18.根据权利要求15所述的第一配置器设备,其中,当所述指令被所述处理器执行时,还使所述第一配置器设备进行以下操作:

生成包括所述配置器密钥包和解密信息的数字包络,其中,所述解密信息使所述第二配置器设备能够解密所述配置器密钥包的至少所述部分。

19.根据权利要求15所述的第一配置器设备,其中,当所述指令被所述处理器执行时,还使所述第一配置器设备进行以下操作:

从所述存储位置取回所述配置器密钥包的所述备份;

对所述配置器密钥包的至少所述部分进行解密;以及

从所述配置器密钥包获得所述配置器私有签名密钥。

20.根据权利要求15所述的第一配置器设备,其中,当所述指令被所述处理器执行时,还使所述第一配置器设备进行以下操作:

确定所述配置器密钥包在所述存储位置处的位置地址;以及

向所述第二配置器设备提供所述位置地址。

21.根据权利要求15所述的第一配置器设备，其中，当所述指令被所述处理器执行时，还使所述第一配置器设备进行以下操作：

向所述第二配置器设备提供解密信息，其中，所述解密信息使所述第二配置器设备能够解密所述配置器密钥包的至少所述部分以及获得所述配置器私有签名密钥。

22.根据权利要求21所述的第一配置器设备，其中，所述解密信息包括从包括以下各项的组中选择的至少一个成员：所述配置器密钥包在所述存储位置处的位置地址、以及可用于解密所述配置器密钥包的至少所述部分的加密密钥。

23.根据权利要求21所述的第一配置器设备，其中，当所述指令被所述处理器执行时，还使所述第一配置器设备进行以下操作：

使用从包括以下各项的组中选择的至少一个成员来提供所述解密信息：显示器、扬声器、光信号、传感器接口、和所述第一配置器设备的短程射频接口。

24.一种具有存储在其中的指令的计算机可读介质，当所述指令被第一配置器设备的处理器执行时，使得所述第一配置器设备进行以下操作：

实现设备设定协议，在所述设备设定协议中，所述第一配置器设备被配置为使用配置器私有签名密钥来将登记者设备登记到网络；

生成配置器密钥包，所述配置器密钥包至少包括与所述第一配置器设备相关联的配置器私有签名密钥；

对所述配置器密钥包的至少一部分进行加密；以及

将所述配置器密钥包存储在存储位置处，以用于由第二配置器设备进行后续取回，其中，相同的配置器私有签名密钥和相同的配置器公共验证密钥是在包括所述第二配置器设备的多个配置器之间共享的，所述第二配置器设备用于根据所述设备设定协议来将不同的登记者设备登记到所述网络。

25.一种由第二配置器设备执行的方法，包括：

在所述第二配置器设备处从存储位置获得配置器密钥包，其中，所述配置器密钥包的至少一部分被加密，以及所述配置器密钥包至少包括与第一配置器设备相关联的配置器私有签名密钥，其中，所述第一配置器设备实现设备设定协议，在所述设备设定协议中，所述第一配置器设备被配置为使用所述配置器私有签名密钥来将第一登记者设备登记到网络，并且相同的配置器私有签名密钥和相同的配置器公共验证密钥是在包括所述第一配置器设备和所述第二配置器设备的多个配置器之间共享的；

对所述配置器密钥包的至少所述部分进行解密；

从所述配置器密钥包获得所述配置器私有签名密钥；以及

根据所述设备设定协议，利用所述配置器私有签名密钥来针对所述网络设定与所述第一登记者设备不同的登记者设备。

26.根据权利要求25所述的方法，还包括：

从所述第一配置器设备获得解密信息，其中，所述解密信息使所述第二配置器设备能够解密所述配置器密钥包的至少所述部分。

27.根据权利要求26所述的方法，其中，所述解密信息包括从包括以下各项的组中选择的至少一个成员：所述配置器密钥包在所述存储位置处的位置地址、以及可用于解密所述配置器密钥包的至少所述部分的加密密钥。

28.根据权利要求26所述的方法，其中，获得所述解密信息包括使用从包括以下各项的组中选择的至少一个成员来获得所述解密信息：显示器、扬声器、光信号、传感器接口、和所述第一配置器设备的短程射频接口。

29.根据权利要求26所述的方法，其中，获得所述解密信息包括：

经由与所述第二配置器设备相关联的照相机，来获得具有编码在其中的所述解密信息的图像；以及

对所述图像进行解码以取回所述解密信息。

用于设备设定协议的配置器密钥包

[0001] 相关申请

[0002] 本申请要求享受于2017年7月12日提交的美国申请序列号15/648,437 的优先权权益，后一申请要求享受于2016年10月19日提交的标题为“DEVICE PROVISIONING PROTOCOL(DPP)WITH MULTIPLE CONFIGURATORS(具有多个配置器的设备设定协议(DPP))”的美国临时申请第62/410,309号的优先权权益，以及上述申请转让给本申请的受让人。所述在先申请的公开内容被认为是本专利申请的一部分，并且以引用方式并入本专利申请。

技术领域

[0003] 概括地说，本公开内容涉及通信系统领域，以及更具体地说，本公开内容涉及通信网络中的设备设定协议(DPP)。

背景技术

[0004] 网络包括经由通信介质彼此通信的设备。在设备可以与网络的其它设备通信之前，可以利用接入通信介质的参数来对设备进行配置。配置设备的过程可以称为设备设定，以及可以包括用于关联、注册、认证的操作或其它操作。尚未针对网络配置的新设备称为登记者设备。设备设定协议 (DPP)可以促进对被引入网络的登记者设备的配置。配置器设备是具有根据设备设定协议来针对网络配置登记者设备的能力的设备。

发明内容

[0005] 本公开内容的系统、方法和设备均具有若干创新性方面，这些方面中没有任何单个方面单独负责本文所公开的期望属性。

[0006] 本公开内容中描述的主题的一个创新性方面可以是在网络的第一配置器设备中实现的。第一配置器设备可以生成配置器密钥包，所述配置器密钥包至少包括与第一配置器设备相关联的配置器私有签名密钥。第一配置器设备可以对配置器密钥包的至少一部分进行加密。第一配置器设备可以将配置器密钥包作为备份存储在存储位置处，以用于由第一配置器设备或第二配置器设备进行后续恢复。

[0007] 在一些实现方式中，配置器密钥包还包括与配置器私有签名密钥相关联的配置器公共验证密钥。

[0008] 在一些实现方式中，第一配置器设备可以使用与配置器私有签名密钥不同的加密密钥，来对配置器密钥包进行加密。

[0009] 在一些实现方式中，第一配置器设备可以使用私钥加密技术，来对所述配置器私有签名密钥进行加密，以及可以将对私钥加密技术的指示包括在配置器密钥包的报头中。

[0010] 在一些实现方式中，第一配置器设备可以生成包括配置器密钥包和解密信息的数字包络。解密信息可以使第二配置器设备能够解密配置器密钥包的至少所述部分。

[0011] 在一些实现方式中，存储位置是从由以下各项构成的组中选择的至少一个成员：第一配置器设备的存储器、网络共享位置、个人计算机、家庭服务器、基于云的存储服务、以

及无线网络的接入点(AP)。

[0012] 在一些实现方式中,存储配置器密钥包包括存储配置器密钥包的备份。第一配置器设备可以从存储位置取回配置器密钥包的备份。第一配置器设备可以对配置器密钥包的至少所述部分进行解密,以及可以从配置器密钥包获得配置器私有签名密钥。

[0013] 在一些实现方式中,第一配置器设备可以至少部分地基于从配置器密钥包获得的配置器私有签名密钥来确定配置器公共验证密钥。

[0014] 在一些实现方式中,第一配置器设备可以确定配置器密钥包在存储位置的位置地址,以及可以向第二配置器设备提供位置地址。

[0015] 在一些实现方式中,第一配置器设备可以使用与设备设定协议相关联的引导技术来提供解密信息。

[0016] 在一些实现方式中,第一配置器设备可以向第二配置器设备提供解密信息。解密信息可以使第二配置器设备能够解密配置器密钥包的至少所述部分,以及可以获得配置器私有签名密钥和配置器公共验证密钥。

[0017] 在一些实现方式中,解密信息包括从由以下各项构成的组中选择的至少一个成员:配置器密钥包在存储位置的位置地址、密码、以及可用于解密配置器密钥包的至少所述部分的加密密钥。

[0018] 在一些实现方式中,提供解密信息包括使用从由以下各项构成的组中选择的至少一个成员来提供解密信息:显示器、扬声器、光信号、传感器接口和第一配置器设备的短程射频接口。

[0019] 在一些实现方式中,第一配置器设备可以通过显示具有编码在其中的解密信息的图像,来提供解密信息。

[0020] 在一些实现方式中,所述图像是条形码或快速响应(QR)码图像。

[0021] 在一些实现方式中,在第一网络的多个配置器之中共享配置器私有签名密钥和配置器公共验证密钥。多个配置器中的每一个配置器可以是能够根据用以针对第一网络配置登记者设备的设备设定协议,来使用配置器私有签名密钥和配置器公共验证密钥的。

[0022] 本公开内容中描述的主题的另一个创新性方面可以是在第二配置器设备中实现的。第二配置器设备可以从存储位置获得配置器密钥包。配置器密钥包的至少一部分可以是加密的,以及配置器密钥包可以至少包括配置器公共验证密钥和与第一配置器设备相关联的配置器私有签名密钥。第二配置器设备可以对配置器密钥包的至少所述部分进行解密。第二配置器设备可以从配置器密钥包获得所述配置器私有签名密钥。第二配置器设备可以根据设备设定协议,利用所述配置器私有签名密钥针对网络设定登记者设备。

[0023] 在一些实现方式中,第二配置器设备可以从第一配置器设备获得解密信息。解密信息可以使第二配置器设备能够解密配置器密钥包的至少所述部分。

[0024] 在一些实现方式中,第二配置器设备可以使用从由以下各项构成的组中选择的至少一个成员来获得解密信息:显示器、扬声器、光信号、传感器接口和第一配置器设备的短程射频接口。

[0025] 在一些实现方式中,第二配置器设备可以经由与第二配置器设备相关联的照相机,获得具有编码在其中的解密信息的图像。第二配置器设备可以对图像进行解码以取回解密信息。

[0026] 本公开内容中描述的主题的另一个创新性方面可以在一种方法中实现。所述方法可以是由网络的第一配置器设备执行的，以及可以包括：生成配置器密钥包，所述配置器密钥包至少包括与第一配置器设备相关联的配置器私有签名密钥。所述方法可以包括：对配置器密钥包的至少一部分进行加密。所述方法可以包括：将配置器密钥包作为备份存储在存储位置处，以用于由第一配置器设备或第二配置器设备进行后续恢复。

[0027] 在一些实现方式中，配置器密钥包还可以包括与配置器私有签名密钥相关联的配置器公共验证密钥。

[0028] 在一些实现方式中，对配置器密钥包的至少所述部分进行加密可以包括：使用与配置器私有签名密钥不同的加密密钥，来对配置器密钥包进行加密。

[0029] 在一些实现方式中，对配置器密钥包的至少所述部分进行加密可以包括：使用私钥加密技术，来对配置器私有签名密钥进行加密，以及将对私钥加密技术的指示包括在配置器密钥包的报头中。

[0030] 在一些实现方式中，存储配置器密钥包可以包括：生成包括配置器密钥包和解密信息的数字包络，其中，所述解密信息使第二配置器设备能够解密配置器密钥包的至少所述部分。

[0031] 在一些实现方式中，存储位置可以是从由以下各项构成的组中选择的至少一个成员：第一配置器设备的存储器、网络共享位置、个人计算机、家庭服务器、基于云的存储服务、以及无线网络的接入点(AP)。

[0032] 在一些实现方式中，存储配置器密钥包可以包括存储配置器密钥包的备份。所述方法可以包括：由第一配置器设备从存储位置取回配置器密钥包的备份。所述方法可以包括：对配置器密钥包的至少所述部分进行解密。所述方法可以包括：从配置器密钥包获得配置器私有签名密钥。

[0033] 在一些实现方式中，所述方法可以包括：至少部分地基于从配置器密钥包获得的配置器私有签名密钥来确定配置器公共验证密钥。

[0034] 在一些实现方式中，所述方法可以包括：确定配置器密钥包在存储位置处的位置地址。所述方法可以包括：向第二配置器设备提供位置地址。

[0035] 在一些实现方式中，所述方法可以包括：向第二配置器设备提供解密信息，其中，所述解密信息使第二配置器设备能够解密配置器密钥包的至少所述部分，以及获得配置器私有签名密钥。

[0036] 在一些实现方式中，解密信息可以包括从由以下各项构成的组中选择的至少一个成员：配置器密钥包在存储位置处的位置地址、以及可用于解密配置器密钥包的至少所述部分的加密密钥。

[0037] 在一些实现方式中，提供解密信息可以包括：使用从由以下各项构成的组中选择的至少一个成员来提供解密信息：显示器、扬声器、光信号、传感器接口和第一配置器设备的短程射频接口。

[0038] 在一些实现方式中，提供解密信息可以包括：显示具有编码在其中的解密信息的图像。

[0039] 在一些实现方式中，所述图像可以是条形码或快速响应(QR)码图像。

[0040] 在一些实现方式中，配置器公共验证密钥可以是根据配置器私有签名密钥导出

的，或者是从配置器密钥包获得的。配置器私有签名密钥和配置器公共验证密钥可以是在第一网络的多个配置器之间共享的。多个配置器中的每一个配置器可以是能够根据设备设定协议，使用配置器私有签名密钥和配置器公共验证密钥来针对第一网络配置登记者设备的。

[0041] 本公开内容中描述的主题的另一个创新性方面可以是在第一配置器设备中实现的，所述第一配置器设备包括处理器和具有存储在其上的指令的存储器。当所述指令被处理器执行时，可以使第一配置器设备生成配置器密钥包，所述配置器密钥包至少包括与第一配置器设备相关联的配置器私有签名密钥。当所述指令被处理器执行时，可以使第一配置器设备对配置器密钥包的至少一部分进行加密，以及将配置器密钥包作为备份存储在存储位置处，以用于由第一配置器设备或第二配置器设备进行后续恢复。

[0042] 在一些实现方式中，当所述指令被处理器执行时，可以使第一配置器设备使用与配置器私有签名密钥不同的加密密钥，来对配置器密钥包进行加密。

[0043] 在一些实现方式中，当所述指令被处理器执行时，可以使第一配置器设备使用私钥加密技术来对配置器私有签名密钥进行加密，以及将对私钥加密技术的指示包括在所述配置器密钥包的报头中。

[0044] 在一些实现方式中，当所述指令被处理器执行时，可以使第一配置器设备生成包括配置器密钥包和解密信息的数字包络，其中，所述解密信息使第二配置器设备能够解密配置器密钥包的至少所述部分。

[0045] 在一些实现方式中，用于存储配置器密钥包的指令包括用于存储配置器密钥包的备份的指令。当所述指令被处理器执行时，可以使第一配置器设备从存储位置取回配置器密钥包的备份，对配置器密钥包的至少所述部分进行解密，以及从配置器密钥包获得配置器私有签名密钥。

[0046] 在一些实现方式中，当所述指令被处理器执行时，可以使第一配置器设备确定配置器密钥包在存储位置处的位置地址，以及向第二配置器设备提供位置地址。

[0047] 在一些实现方式中，当所述指令被处理器执行时，可以使第一配置器设备向第二配置器设备提供解密信息，其中，所述解密信息使第二配置器设备能够解密配置器密钥包的至少所述部分，以及获得配置器私有签名密钥。

[0048] 在一些实现方式中，解密信息包括从由以下各项构成的组中选择的至少一个成员：配置器密钥包在存储位置处的位置地址、以及可用于解密配置器密钥包的至少所述部分的加密密钥。

[0049] 在一些实现方式中，当所述指令被处理器执行时，可以使第一配置器设备使用从由以下各项构成的组中选择的至少一个成员来提供解密信息：显示器、扬声器、光信号、传感器接口和第一配置器设备的短程射频接口。

[0050] 本公开内容中描述的主题的另一个创新性方面可以是在具有存储在其上的指令的计算机可读介质中实现的，当所述指令被第一配置器设备的处理器执行时，可以使第一配置器设备生成配置器密钥包，所述配置器密钥包至少包括与第一配置器设备相关联的配置器私有签名密钥。当所述指令被第一配置器设备的处理器执行时，可以使第一配置器设备对配置器密钥包的至少一部分进行加密，以及将配置器密钥包作为备份存储在存储位置处，以用于由第一配置器设备或第二配置器设备进行后续恢复。

[0051] 本公开内容中描述的主题的另一个创新性方面可以是在一种由第二配置器设备执行的方法中实现的。所述方法可以包括:在第二配置器设备处从存储位置获得配置器密钥包,其中,配置器密钥包的至少一部分是被加密的,以及配置器密钥包至少包括与第一配置器设备相关联的配置器私有签名密钥。所述方法可以包括:对配置器密钥包的至少所述部分进行解密,从配置器密钥包获得配置器私有签名密钥,以及根据设备设定协议,利用配置器私有签名密钥来针对网络设定登记者设备。

[0052] 在一些实现方式中,所述方法可以包括:从第一配置器设备获得解密信息,其中,所述解密信息使第二配置器设备能够解密配置器密钥包的至少所述部分。

[0053] 在一些实现方式中,解密信息可以包括从由以下各项构成的组中选择的至少一个成员:配置器密钥包在存储位置处的位置地址、以及可用于解密配置器密钥包的至少所述部分的加密密钥。

[0054] 在一些实现方式中,获得解密信息可以包括:使用从由以下各项构成的组中选择的至少一个成员来获得解密信息:显示器、扬声器、光信号、传感器接口和第一配置器设备的短程射频接口。

[0055] 在一些实现方式中,获得解密信息可以包括:经由与第二配置器设备相关联的照相机,获得具有编码在其中的解密信息的图像;以及对图像进行解码以取回解密信息。

[0056] 在附图和下文的描述中,阐述了本公开内容中描述的主题的一个或多个实现方式的细节。根据这些描述、附图和权利要求,其它特征、方面和优点将变得显而易见。注意的是,附图中的相对尺寸可能不是按比例描绘的。

附图说明

[0057] 图1示出了用于介绍具有多个配置器的设备设定协议的概念的示例系统图。

[0058] 图2示出了设备设定协议的示例消息流程图。

[0059] 图3示出了用于第一配置器设备存储配置器密钥的示例流程图。

[0060] 图4示出了用于描述由第一配置器设备进行的对配置器密钥的备份和恢复的示例系统图。

[0061] 图5示出了用于描述从第一配置器设备向第二配置器设备共享配置器密钥的示例系统图。

[0062] 图6示出了具有多个配置器的设备设定协议的示例消息流程图。

[0063] 图7示出了用于操作第一配置器设备的示例流程图。

[0064] 图8示出了用于操作第二配置器设备的示例流程图。

[0065] 图9示出了用于操作配置器设备以备份和恢复配置器密钥的示例流程图。

[0066] 图10示出了用于实现本公开内容的方面的示例电子设备的方块图。

[0067] 各个附图中的相似附图标记和名称指示相似的元件。

具体实施方式

[0068] 出于描述本公开内容的创新性方面的目的,下面的描述针对某些实现方式。然而,本领域普通技术人员将容易认识到,可以以多种不同方式来应用本文中的教导。可以在能够根据以下标准来发送和接收射频(RF)信号的任何设备、系统或网络中实现所描述的实现

方式:电气和电子工程师协会(IEEE)16.11标准中的任何一种标准、或者IEEE 802.11标准中的任何一种标准、蓝牙®标准、码分多址(CDMA)、频分多址(FDMA)、时分多址(TDMA)、全球移动通信系统(GSM)、GSM/通用分组无线电服务 (GPRS)、增强型数据GSM环境(EDGE)、地面集群无线电(TETRA)、宽带CDMA(W-CDMA)、演进数据优化(EV-DO)、1xEV-DO、EV-DO版本A、EV-DO版本B、高速分组接入(HSPA)、高速下行链路分组接入 (HSDPA)、高速上行链路分组接入(HSUPA)、演进高速分组接入 (HSPA+)、长期演进(LTE)、AMPS、或者用于在无线、蜂窝或物联网(IOT) 网络内通信的其它已知信号(诸如,利用3G、4G或5G技术、或其进一步的实现方式的系统)。

[0069] 如上所述,设备设定协议(DPP,诸如Wi-Fi设备设定协议)可以促进对被引入网络的登记者设备的配置。例如,DPP可以提供在登记者设备与配置器设备之间的认证和认证密钥建立。在一些实现方式中,DPP使用与典型用于认证协议的消息相比较少的消息。例如,DPP认证协议可以将“引导出的(bootstrapped)”公钥用于第一认证,以及用于在进一步设定之前生成短暂的协议密钥。引导指代的是使用受信任的带外技术来获得公钥。带外技术基于设备的接近度来提供一定程度的信任。例如,引导可以包括使用第一设备上的相机来扫描和解码通过第二设备显示(或附加于第二设备) 的图像。

[0070] 在DPP中,配置器设备负责支持对登记者的设置。典型地,引导密钥可以用于在配置器设备与新登记者之间的第一次认证。在认证完成之后,配置器设备可以设定登记者用于经由网络进行的通信。作为该设定的一部分,配置器设备使登记者能够与网络中的其它对等体建立安全关联。配置器设备使用配置器密钥来生成“连接符”(其还可以称为“配置对象”)。连接符携带对登记者的配置,并且授权在登记者设备与对等设备(例如,接入点或对等邻居)之间的连接性。配置器密钥包括由配置器私有签名密钥 (其可以称为“c-sign-key”)和配置器公共验证密钥(其可以称为“C-sign-key”)组成的签名密钥对。配置器使用配置器私有签名密钥 (c-sign-key)来对连接符进行签名,而经设定的设备使用配置器公共验证密钥(C-sign-key)来验证其它设备的连接符是否由相同的配置器进行签名。如下面所进一步描述的,配置器密钥在数学上相对应,以及可以用于验证由配置器设备签名的消息的真实性。可以使用配置器设备的配置器私有签名密钥来对每一个连接符进行签名。配置器设备可以针对该配置器设备配置的每一个登记者产生一个或多个连接符。在使用配置器设备的配置器私用签名密钥已经对连接符进行了签名之后,网络中的任何对等体可以对连接符进行验证。例如,可以使用配置器公共验证密钥来验证使用配置器私有签名密钥已经进行了签名的连接符的真实性。因为配置器密钥可以是设备设定协议的基本方面,所以可能存在以下情况:可以将配置器密钥安全地存储为备份或者与另一个配置器设备共享。

[0071] 在一个方面中,配置器设备可以将配置器密钥包准备成对配置器密钥的安全备份。可以将配置器密钥包存储成备份以便以后恢复。例如,可以将配置器密钥包导出到由该配置器设备以及潜在地由其它配置器设备可访问的位置。在另一个方面中,多个配置器设备可以共享相同的配置器密钥。例如,可以与第二配置器设备共享配置器密钥,使得第二配置器设备可以使用该配置器密钥。作为假设情景,考虑当两个室友共享住所的示例,以及每一个室友操作配置器设备(诸如,他们的个人移动电话)来配置访客登记者设备。本公开内容中描述的实现方式增强了设备设定协议,使得配置器密钥可以是由多个配置器设备使用的。

[0072] 第一配置器设备可以生成配置器密钥包，所述配置器密钥包至少包括与第一配置器设备相关联的配置器私有签名密钥。配置器密钥包还可以包括与配置器私有签名密钥相关联的配置器公共验证密钥。第一配置器设备可以对配置器密钥包的至少一部分进行加密，以及将配置器密钥包存储在存储位置处，以便由第一配置器设备或第二配置器设备进行后续取回。可以使用加密密钥来对配置器密钥包进行加密，所述加密密钥可以是从第一配置器设备共享到第二配置器设备的。在一些实现方式中，设备设定协议使用引导来获得登记者设备的公共引导密钥。类似的引导技术可以用于在配置器设备之间共享加密密钥。引导提供了对加密密钥的信任，这是因为带外技术典型地涉及与对等设备的接近度或物理关联。

[0073] 可以实现在本公开内容中描述的主题的特定实现方式，以实现以下潜在优点中的一个或多个优点。使用本公开内容中的实现方式，设备设定协议可以支持对配置器密钥的备份/恢复或者导出/导入。在一些实现方式中，设备设定协议可以受益于具有用于网络的多个配置器设备。多个配置器设备可以使用相同的共享配置器密钥，这可以改善在针对网络配置的对等体之间的兼容性。例如，可以使用相同的配置器密钥来对连接符进行签名和验证，而不管哪个配置器设备针对网络配置登记者设备。与依赖于不同配置器密钥用于每一个配置器设备的方法相比，本公开内容中的用于共享配置器密钥的技术可以提供用于向设备设定协议添加更多配置器设备的可扩展且不太复杂的方法。通过定义用于存储或共享配置器密钥的安全存储格式，设备设定协议可以受益于在配置器设备之间增加的互操作性。

[0074] 图1示出了用于介绍具有多个配置器的设备设定协议的概念的示例系统图。示例系统100包括第一配置器设备110、第二配置器设备120和登记者设备150A和150B。登记者设备可以是还未曾被配置在由第一配置器设备110或第二配置器设备120中的任何一者管理的网络中使用的任何类型的设备。第一配置器设备110可以具有一对配置器密钥，其包括配置器私有签名密钥和配置器公共验证密钥。配置器私有签名密钥可以用于创建数字签名消息。配置器公共验证密钥可以用于验证使用配置器私有签名密钥进行签名的数字签名消息。

[0075] 如图1中所示，第一配置器设备110可以实现设备设定协议(如箭头 158所示)以配置登记者设备150A用于在网络中使用。为了在具有多个配置器设备的情况下使用设备设定协议，第一配置器设备110可以与第二配置器设备120共享(如箭头152所示)其配置器密钥对。如下面所进一步论述的，可以不是直接地将配置器密钥发送给第二配置器设备120。确切地说，第一配置器设备110可以生成配置器密钥包。可以使用加密密钥来对配置器密钥包的一些或所有内容进行加密。可以将配置器密钥包导出到由第二配置器设备120可访问的在网络中的某个位置。在一些实现方式中，第一配置器设备110可以向第二配置器设备120提供解密信息，使得第二配置器设备120可以获得并解密配置器密钥包。例如，解密信息可以包括存储配置器密钥包的位置地址。在一些实现方式中，解密信息可以包括加密密钥。可以使用类似的引导技术来提供解密信息，配置器设备使用所述引导技术来获得登记者设备的公共引导密钥。在图2的描述中更详细地描述了引导技术。在一些其它实现方式中，解密信息可以包括：能够手动地输入到第二配置器设备120中以解密配置器密钥包的密码或其它信息。

[0076] 一旦第二配置器设备120已经获得解密信息和配置器密钥包，第二配置器设备120就可以对配置器密钥包进行解密(诸如，使用加密密钥)并且取回配置器密钥。第二配置器设备120可以存储配置器密钥，并且在配置其它登记者设备时使用该共享的配置器密钥。例如，第二配置器设备120 可以实现设备设定协议(如箭头154所示)以配置登记者设备150B。即使登记者设备150A和150B是由不同的配置器设备来进行配置的，登记者设备150A和150B中的每一者也可以使用相同的配置器公共验证密钥来验证 (授权它们经由网络进行通信的)签名的连接符。

[0077] 图2示出了设备设定协议的示例消息流程图。图2中的DPP 200是在一对设备(登记者设备250和配置器设备210)之间的。DPP 200包括三个操作：引导技术、DPP认证和DPP配置。DPP认证依赖于通过引导技术(诸如，下面进一步描述的那些)已经获得的认证方的引导密钥。

[0078] 引导指代的是用于从另一个设备获得共享密钥的带外技术。登记者设备250和配置器设备210中的每一者可以具有公共引导密钥(有时也称为“公共标识密钥”)，其被信任用于初始认证和用于生成临时设定密钥。引导是可以用于共享公共引导密钥的各种技术之一。例如，引导可以包括扫描快速响应®(QR)码，所述QR码对公共引导密钥进行编码。对这种形式的认证的支持允许缺少用户接口的某些设备(诸如，IOT设备、可穿戴配件、家庭自动化设备等)利用配置器设备来进行认证。

[0079] 在205处，配置器设备210可以从登记者设备250获得登记者引导数据。例如，登记者设备250可以具有在其上(或者在包装上、或者插入在包装中)的视觉标签。该视觉标签可以是条形码、矩阵码、二维码等。条形码的常见示例可以是QR码。配置器设备210可以使用照相机和相应的软件来检测条形码(或者类似的视觉标签)。配置器设备210可以通过对条形码进行解码，来获得登记者引导数据。在一种实现方式中，登记者引导数据可以包括用于登记者设备250的公共引导密钥。除了公共引导密钥之外，其它信息也可以包括在登记者引导数据中。例如，登记者引导数据可以包括公共引导密钥以及全局操作类和信道号列表。全局操作类和信道号列表可以用于确定登记者设备250将使用哪些无线电参数或哪些无线信道来进行DPP认证。例如，全局操作类和信道号列表一起可以指示登记者设备250 将针对哪个无线信道来监听(或发送)DPP认证请求消息。在207处，在一些实现方式中，登记者设备250还可以从配置器设备210获得配置器引导数据。当双方获得彼此的引导数据时，DPP认证可以利用相互双向认证。

[0080] 除了图2中所示的引导技术之外，还可以使用各种其它引导技术。引导技术允许接收者信任属于特定设备的引导数据。如图1中所述，扫描二维矩阵条形码(诸如，QR码)是一种用于获得引导数据的技术。作为对扫描条形码的替代方案，配置器设备210可以使用邻居感知网络(NAN)(未示出)。NAN在无需具有设备之间的关联的情况下提供发现能力和通过无线介质的服务信息交换。另一种引导技术是通过其它介质来传送引导数据，所述其它介质可以提供对所传送内容的完整性的某种程度的信任。例如，在一些实现方式中，引导可以包括使用通用串行总线(USB)、近场通信 (NFC)或短程无线电通信(诸如，蓝牙™通信)。另一种引导技术是利用共享的码/密钥/短语/词(下文称为“码”)来遮罩引导数据，并且依赖于对共享的码的知识来对引导密钥进行去遮罩。如果对等体能够证明它知道并且可以使用共享的码，则可以信任对等体的引导数据。

[0081] DPP认证阶段使用引导数据来强认证配置器和登记者，所述引导数据是使用引导技术获得的。DPP认证包括3个消息交换，并且生成共享秘密和经认证的密钥。在215处，配置器设备210生成第一随机数，生成协议密钥对，执行登记者公共引导密钥的散列函数，并且基于从经散列的引导数据导出的共享秘密来生成第一对称密钥。配置器设备210经由信道列表中的一个或多个信道来发送DPP认证请求消息217。DPP认证请求消息217 包括共享秘密和通过第一对称密钥加密的第一随机数。

[0082] 登记者设备250接收DPP认证请求消息217。在225处，登记者设备 250检查其公共引导密钥的散列是否在该消息中。如果其公共引导密钥的散列在该消息中，则登记者设备250生成共享秘密并且导出第一对称密钥。登记者设备250尝试使用第一对称密钥来打开第一随机数。接着，登记者设备250生成第二随机数、共享秘密和第二对称密钥。登记者设备250将两个随机数及其能力包装在第一对称密钥中，并且将认证标签包装在第二对称密钥中。然后，登记者设备250将其公共引导密钥的散列(以及可选地如果其正在进行相互认证的话则包括配置器公共引导密钥的散列)、其公共协议密钥、所包装的随机数、连同其包装的网络公钥和所包装的认证标签放置在在DPP认证响应消息227中。向配置器设备210发送DPP认证响应消息227。

[0083] 在成功地接收到响应之后，在235处，配置器设备210验证结果并且发送DPP认证确认消息237以完成DPP认证阶段。在成功完成这些帧交换之后，在245处，建立在启动器/配置器与响应者/登记者之间的安全信道。

[0084] 在DPP认证完成之后，配置器设备210设定登记者设备250用于设备到设备通信或基础设施通信。作为该设定的一部分，配置器设备210使登记者设备250能够与网络中的其它对等体建立安全关联。登记者设备250 通过发送DPP配置请求消息263来发起配置阶段，并且是利用在DPP配置响应消息267中的配置信息来设定的。在成功接收到DPP配置响应消息267 之后，登记者设备250是利用可用于建立到网络的安全接入的配置信息来设定的。

[0085] 在一些实现方式中，配置器设备210还可以是无线局域网(WLAN) 的接入点。替代地，配置器设备210可以是与接入点分离的。例如，登记者设备250可以使用由配置器设备210提供的配置信息，来与接入点280 建立安全无线连接。在另一种实现方式中，配置器设备210可以是对等(P2P) 组所有者或P2P组成员。

[0086] 在DPP配置阶段结束时，配置器设备210可以创建连接符(由箭头277 表示)。连接符是签名的介绍，其使得登记者设备250能够获得准许网络上的其它设备与其进行通信的受信任声明。每一个连接符可以包括组标识符、网络角色和网络接入设定密钥的元组，所有这些内容使用配置器设备的配置器私有签名密钥进行了签名。该标识符可以指示特定的对等体或通配符 (其指示所有对等体)。如上所述，连接符是通过配置器设备210的配置器私有签名密钥(c-sign-key)来签名的，并且可以是使用配置器设备210的配置器公共验证密钥(C-sign-key)来进行验证的。

[0087] 如果配置器设备210与接入点280分离，则登记者设备250可以将配置信息和连接符用作针对与接入点280的无线关联287的证书。登记者设备250可以发现接入点280，发送对等体发现请求帧(未示出)，以及然后等待对等体发现响应帧(未示出)。在成功地验证对等体发现帧之后，登记者设备250和接入点280相互导出成对主密钥(PMK)，并且遵循正常的IEEE 802.11过程。例如，可以在登记者设备250与接入点280之间执行4 次握手过程，以完

成登记者设备250与接入点280的认证和无线关联。成对主密钥(PMK)可以用于后续的Wi-Fi™保护接入(WPA)握手和配置消息。替代地,如果接入点280是旧有接入点,则配置信息可以包括预共享密钥(PSK)或PSK密码凭证以允许登记者设备250连接到接入点280。在该实现方式中,登记者设备250将使用该配置信息以采用IEEE 802.11和 WPA2-个人网络接入过程来发现AP并与AP进行关联。

[0088] 图3示出了用于第一配置器设备存储配置器密钥的示例流程图。流程图300开始于方块310。在方块310处,第一配置器设备可以生成配置器密钥包,所述配置器密钥包至少包括与第一配置器设备相关联的配置器私有签名密钥。在一些实现方式中,配置器密钥包可以包括配置器私有签名密钥和配置器公共验证密钥两者。

[0089] 在方块320处,第一配置器设备可以对配置器密钥包的至少一部分进行加密。例如,配置器密钥包可以是使用与配置器私有签名密钥不同的加密密钥来加密的。在一些实现方式中,第一配置器设备可以使用私钥加密技术来对配置器私有签名密钥(以及可选地,配置器公共验证密钥)进行加密。在一些实现方式中,配置器密钥包可以包括报头,所述报头描述了用于准备配置器密钥包的结构、内容或加密技术。

[0090] 在方块330处,第一配置器设备可以将配置器密钥包作为备份存储在存储位置处,用以由第一配置器设备或第二配置器设备进行后续恢复。例如,存储位置可以是第一配置器设备的存储器、网络共享位置、个人计算机、家庭服务器、基于云的存储服务、或者无线网络的接入点(AP)。

[0091] 在已经存储了配置器密钥包之后,可以存在使用所存储的配置器密钥包的不同方式。例如,在方快340处,第一配置器设备可以从存储位置取回配置器密钥包的备份。第一配置器设备可以对配置器密钥包进行解密,并且从配置器密钥包获得配置器私有签名密钥。在另一个示例中,在方块 350处,第一配置器设备可以向第二配置器设备提供解密信息。该解密信息可以使第二配置器设备能够对由第一配置器设备进行加密的配置器密钥包的至少一部分进行解密。第二配置器设备可以从配置器密钥包中获得配置器私有签名密钥。如果配置器密钥包包括配置器公共验证密钥,则第二配置器设备可以从配置器密钥包中恢复配置器公共验证密钥。如果配置器密钥包不包括配置器公共验证密钥,则第二配置器设备可以至少部分地基于配置器私有签名密钥来确定配置器公共验证密钥。

[0092] 图4示出了用于描述由第一配置器设备进行的对配置器密钥的备份和恢复的示例系统图。示例系统400包括第一配置器设备110和存储位置410。第一配置器设备110具有配置器密钥412,并且能够使用加密技术416对配置器密钥412的至少一部分进行加密。可以存在能够容易地应用于本公开内容的实现方式的多种加密技术。下面将进一步描述不同加密技术的示例。

[0093] 第一配置器设备110可以生成配置器密钥包427,所述配置器密钥包 427包括配置器密钥412并且已经使用加密技术416进行了至少部分地加密 (通过大括号表示)。第一配置器设备110还具有备份/恢复模块455。备份 /恢复模块455可以使配置器密钥包427存储(在箭头467处示出)在存储位置410处。例如,存储配置器密钥包427的动作可以称为备份。

[0094] 在已经存储了配置器密钥包427之后,备份/恢复模块455可以是能够恢复配置器密钥的。备份/恢复模块455可以从存储位置410取回(在箭头 477处示出)配置器密钥包427。例如,备份/恢复模块455可以从存储位置410访问或下载配置器密钥包427。备份/恢复

模块455可以通过逆转加密技术并且从配置器密钥包427获得配置器密钥，来恢复配置器密钥。

[0095] 图5示出了用于描述从第一配置器设备向第二配置器设备共享配置器密钥的示例系统图。示例系统500包括第一配置器设备110、第二配置器设备120和存储位置410。存储位置410可以是网络共享存储器、网络驱动器、接入点的资源、基于云的存储位置、或者第二配置器设备120经由通信网络可访问的任何其它资源。如上所述，第一配置器设备110具有配置器密钥412，所述配置器密钥412可以包括配置器私有签名密钥和配置器公共验证密钥。为了向第二配置器设备120提供配置器密钥，第一配置器设备110 可以将配置器密钥导出在配置器密钥包427中。在517处表示，第一配置器设备110可以(使用加密密钥)来加密配置器密钥和创建配置器密钥包 427。

[0096] 在一些实现方式中，第一配置器设备110可以根据称为公钥加密标准 (PKCS)的标准族，来生成配置器密钥包。例如，PKCS#8是标准中的一种标准，以及定义了用于存储私钥信息的标准语法。PKCS#8中的加密指定了数字包络，所述数字包络由(具有关于配置的信息的)非对称密钥包和加密密钥组成。加密密钥可以是使用密钥管理、密钥协议、利用共享密码导出的对称密钥、或者通过共享信息的对称密钥加密来保护的。因此，只有能够导出加密密钥的设备才能够对配置器密钥包进行解密。在一种实现方式中，第一配置器设备110可以在网络中创建公共连接符简档，使得任何配置器设备都可以从存储位置410获得配置器密钥包427(以PKCS# 8二进制大物件(blob)的形式)。

[0097] 公共连接符简档可以包括例如，位置地址，诸如，针对可以下载配置器密钥包的存储位置410的统一资源定位符(URL)或统一资源标识符(URI)。虽然配置器密钥包可以是由多个设备可访问的，但是只有授权的配置器设备(诸如，第二配置器设备120)将具有为了对配置器密钥包进行解密而需要的解密信息。例如，解密信息可以是为了从与配置器密钥包相关联的数字包络中导出加密密钥的共享密码。替代地，解密信息可以是用于设备获得用于对配置器密钥包进行加密的加密密钥的任何其它方式。在另一种实现方式中，可以将位置地址维护成仅提供给授权配置器的秘密。

[0098] 在547处，将配置器密钥包427存储在存储位置410处以供后续取回。在一些实现方式中，第一配置器设备110可以经由网络向第二配置器设备120 发送配置器密钥包427，并且使配置器密钥包427存储在共置于第二配置器设备120的存储位置处。

[0099] 第二配置器设备120可以从第一配置器设备110获得(由箭头537表示)解密信息。在一些实现方式中，解密信息可以包括为了对配置器密钥包进行解密而需要的加密密钥。在一些实现方式中，解密信息可以包括：用于指示配置器密钥包存储在存储位置410处的何处的位置地址。第一配置器设备110可以有多种方式向第二配置器设备120提供解密信息(包括引导)。例如，可以将加密密钥编码在条形码图像中，该条形码图像可以由第二配置器设备120扫描。在一些实现方式中，条形码图像可以是静态的或短暂的。例如，第一配置器设备110可以配备有显示器，以及可以创建利用加密密钥编码的条形码图像(或其它编码图像)。加密密钥可以是通过利用照相机、智能电话、扫描仪或第二配置器设备120的另一种机器可读代码读取器来扫描和解码机器可读图像(诸如，QR码)来确定的。除了加密密钥之外，条形码图像还可以是利用第二配置器设备120能够下载配置器密钥包427的位置地址来进行编码的。

[0100] 第二配置器设备120可以从网络位置下载(由箭头557表示)配置器密钥包427。一旦第二配置器设备120已经获得了配置器密钥包427和加密密钥,第二配置器设备120就可以对经加密的私钥包进行解密以获得配置器密钥,并且将配置器密钥存储在第二配置器设备120的存储器中以结合设备设定协议进行使用。

[0101] 图6示出了具有多个配置器的设备设定协议的示例消息流程图。消息流程图600包括在第一配置器设备110、第二配置器设备120与存储位置 410之间的消息。在605处,第一配置器设备110可以生成包括第一配置器设备110的配置器密钥(c-sign-key和C-sign-key)的配置器密钥包。使用加密密钥来对配置器密钥包进行加密。在611处,第一配置器设备110将配置器密钥包导出,并且将其存储在存储位置410处。第一配置器设备110 还可以确定用于指示配置器密钥包存储在何处的位置地址。可以将加密密钥和位置地址编码成条形码图像或其它类型的数据结构。

[0102] 在613处,第二配置器设备120可以获得配置器密钥包(以及可选地,位置地址)。例如,第二配置器设备120可以获得条形码图像或其它数据结构,并对其进行解码。在619处,第二配置器设备120可以确定配置器密钥包的位置地址。第二配置器设备120可以经由来自第一配置器设备110 的另一个消息(未示出),使用公共连接符简档,或者通过用于共享位置地址的任何其它机制,来根据条形码图像确定位置地址。基于该位置地址,第二配置器设备120可以向存储位置410发送针对配置器密钥包的请求(在 621处)。在623处,第二配置器设备120可以从存储位置410接收配置器密钥包。在625处,第二配置器设备120可以对配置器密钥包(使用加密密钥)进行解密并且取回配置器密钥。一旦第二配置器设备120具有了配置器密钥,第二配置器设备120就可以使用第一配置器设备110将使用的相同配置器密钥,来配置登记者设备250。

[0103] 可以如前所述地继续设备设定(其包括引导、认证和配置)(参见对图 2中的消息205、207、217、227、237、263、267和277的相应描述)。

[0104] 图7示出了用于操作第一配置器设备的示例流程图。流程图700开始于方块710。在方块710处,第一配置器设备可以生成配置器密钥包,其具有使用加密密钥加密了的至少一部分。配置器密钥包可以至少包括用于第一配置器设备的配置器私有签名密钥。在方块720处,第一配置器设备可以将配置器密钥包存储在由第二配置器设备可访问的存储位置处。在方块 730处,第一配置器设备可以向第二配置器设备提供加密密钥,以使第二配置器设备能够对来自存储位置的配置器密钥包进行解密。在方块740处,第一配置器设备可以可选地向第二配置器设备提供位置地址。该位置地址可以指示配置器密钥包存储在存储位置的何处。

[0105] 图8示出了用于操作第二配置器设备的示例流程图。流程图800开始于方块810。在方块810处,第二配置器设备可以在第二配置器设备处,从第一配置器设备获得解密信息。例如,解密信息可以是先前用于对配置器密钥包进行加密的加密密钥。在方块820处,第二配置器设备可以在第二配置器设备处,从存储位置获得配置器密钥包。配置器密钥包可以至少包括用于第一配置器设备的配置器私有签名密钥。在方块830处,第二配置器设备可以使用解密信息来对配置器密钥包进行解密,以取回配置器私有签名密钥。如果配置器密钥包包括配置器公共验证密钥,则第二配置器设备可以从配置器密钥包中恢复配置器公共验证密钥。如果配置器密钥包不包括配置器公共验证密钥,则第二配置器设备可以至少部分

地基于配置器私有签名密钥来确定配置器公共验证密钥。在方块840处，第二配置器设备可以根据设备设定协议，使用配置器私有签名密钥和配置器公共验证密钥来针对网络配置登记者设备。

[0106] 图9示出了用于操作配置器设备以备份和恢复配置器密钥的示例流程图。流程图900开始于方块910。在方块910处，配置器设备可以生成配置器密钥包，配置器密钥包至少包括配置器私有签名密钥的加密副本。加密副本可以是使用私钥加密技术来进行加密的。例如，私钥加密技术可以是在互联网工程任务组(IETF)请求注释(RFC)5958和RFC 5208中的至少一项中定义的。在一些实现方式中，私有密钥加密技术可以是在配置器密钥包的报头中标识的。

[0107] 在方块920处，配置器设备可以将配置器密钥包作为备份存储在由配置器设备可访问的存储位置处。存储位置可以是可用于配置器设备的任何存储设备。存储位置的示例包括配置器设备的本地存储器、存储位置、个人计算机、家庭服务器、基于云的存储服务等。在一些实现方式中，存储位置可以用于使用不同的配置器密钥来存储来自不同配置器设备的备份。

[0108] 在方块930处，配置器设备可以随后通过获得配置器密钥包，并且使用私钥加密技术来解密配置器密钥包，来恢复备份。

[0109] 以下是可以与本文所描述的任何实现方式一起使用的配置器密钥包的示例。该示例配置器密钥包是非对称密钥包，是RFC5958中(使用PKCS #8)定义的一个非对称密钥的ASN.1序列：

[0110]
```
AsymmetricKeyPackage ::= SEQUENCE SIZE (1) OF OneAsymmetricKey

OneAsymmetricKey ::= SEQUENCE {
    version                   Version,
    privateKeyAlgorithm       PrivateKeyAlgorithmIdentifier,      privateKey
PrivateKey,
    [[publicKey               PublicKey OPTIONAL,]]
```

[Optional Information as needed]（按需的可选信息）

}

PrivateKey ::= SEQUENCE {

encryptionAlgorithm EncryptionAlgorithmIdentifier,

encryptedData EncryptedData }

[0111] EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier

{ CONTENT-ENCRYPTION,

{ KeyEncryptionAlgorithms } }

EncryptedData ::= OCTET STRING containing the encrypted version of the configurator private signing key（包括配置器私有签名密钥的加密版本的八位位组串）

[0112] 图10示出了用于实现本公开内容的方面的示例电子设备1000的方块图。在一些实现方式中，电子设备1000可以类似于第一配置器设备110或第二配置器设备120。电子设备1000可以是膝上型计算机、平板计算机、移动电话、游戏控制台、智能手表、虚拟或增强现实设备、无人机、或者另一种电子系统。电子设备1000包括处理器1002(其可能包括多个处理器、多个内核、多个节点、或者实现多线程等)。电子设备1000包括存储器1006。存储器1006可以是系统存储器或者机器可读介质或者计算机可读介质的下面所描述的可能实现中的任何一种或多种。电子设备1000还可以包括总线 1001(诸如，PCI、ISA、PCI-Express、HyperTransport®、InfiniBand®、NuBus、 AHB、AXI等)。电子设备可以包括一个或多个网络接口1004，网络接口 1004可以是无线网络接口(诸如，WLAN接口、Bluetooth®接口、WiMAX 接口、ZigBee®接口、无线USB接口等)或者有线网络接口(诸如，电力线通信接口、以太网接口等)。在一些实现方式中，电子设备1000可以支持多个网络接口1004，每一个网络接口1004可以被配置为将电子设备1000 耦合到不同的通信网络。

[0113] 存储器1006包括用于支持上面所描述的各种实现方式的功能。存储器 1006可以包括有助于实现设备设定协议的一个或多个功能。例如，存储器1006可以实现如上所述的第一配置器设备110或第二配置器设备120的一个或多个方面。存储器1006可以体现用于实现上面在图1-9中所描述的实现方式的功能。在一些实现方式中，存储器1006可以包括有助于生成、存储或取回配置器密钥包的一个或多个功能。电子设备1000可以包括加密/ 解密模块1016或者备份/恢复模块1055。例如，加密/解密模块1016可以有助于对配置器密钥包的至少一部分进行加密或者对配置器密钥包进行解密。备份/恢复模块1055可以有助于存储配置器密钥包，以及从存储位置取回配置器密钥包。电子设备1000还可以包括其它组件1020，诸如传感器单元、用户接口组件或者另一个输入/输出组件。在一些其它实现方式中，电子设备1000可以具有用于使用引导技术来获得解密信息的其它适当的传感器(诸如，照相机、麦克风、NFC检测器、条形码扫描仪等)。

[0114] 这些功能中的任何一个功能可以部分地(或完全地)实现在硬件中(诸如，在处理

器1002上)。例如,该功能可以是利用专用集成电路来实现的,在处理器1002中实现的逻辑中实现的,在外围设备或卡上的协处理器中实现的等。此外,实现可以包括图10中未示出的更少的或额外的组件(诸如,视频卡、音频卡、另外的网络接口、外围设备等)。处理器1002和存储器 1006可以耦合到总线1001。虽然示出为耦合到总线1001,但是存储器1006 可以直接耦合到处理器1002。

[0115] 如本文所使用的,指代列表项目“中的至少一个”的短语是指这些项的任意组合,包括单个成员。举例而言,“a、b或c中的至少一个”旨在覆盖:a、b、c、a-b、a-c、b-c、以及a-b-c。

[0116] 结合本文所公开的实现方式描述的各种说明性的逻辑、逻辑块、模块、电路和算法过程可以实现成电子硬件、计算机软件或二者的组合。对硬件和软件之间的可交换性已经按照功能进行了一般描述,并且上文在各种说明性的组件、方块、模块、电路和过程中进行了说明。至于这种功能是实现成硬件还是实现成软件,取决于特定应用和施加于整个系统的设计约束。

[0117] 用于实现结合本文所公开的方面描述的各种说明性的逻辑、逻辑块、模块和电路的硬件和数据处理装置,可以是利用被设计为执行本文所述功能的通用单芯片或多芯片处理器、数字信号处理器(DSP)、专用集成电路 (ASIC)、现场可编程门阵列(FPGA)或其它可编程逻辑设备、分立门或者晶体管逻辑、分立硬件组件、或其任意组合来实现或者执行的。通用处理器可以是微处理器,或者,任何常规的处理器、控制器、微控制器或者状态机。处理器也可以实现为计算设备的组合,诸如,DSP和微处理器的组合、多个微处理器、一个或多个微处理器与DSP内核的结合,或者任何其它这样的配置。在一些实现方式中,特定的过程和方法可以是由特定于给定功能的电路来执行的。

[0118] 在一个或多个方面中,所描述的功能可以是用硬件、数字电子电路、计算机软件、固件(包括本说明书中所公开的结构及其结构等效物)、或其任意组合来实现的。本说明书中描述的主题的实现方式还可以实现成一个或多个计算机程序,即,编码在计算机存储介质上的、用于由数据处理装置执行或控制数据处理装置的操作的计算机程序指令的一个或多个模块。

[0119] 当用软件来实现时,功能可以作为一个或多个指令或代码存储在计算机可读介质上,或者在其上发送。本文所公开的方法或算法的过程可以是用存在于计算机可读介质上的处理器可执行软件模块来实现的。计算机可读介质包括计算机存储介质和通信介质两者,所述通信介质包括可以被实现为将计算机程序从一处传送到另一处的任何介质。存储介质可以是计算机能够存取的任何可用介质。举例而言但非限制,这种计算机可读介质可以包括高速缓冲存储器、RAM(包括SRAM、DRAM、零电容RAM、双晶体管RAM、eDRAM、EDO RAM、DDR RAM、EEPROM、NRAM、RRAM、 SONOS、PRAM等)、ROM、EEPROM、CD-ROM或其它光盘存储器、磁盘存储器或其它磁存储设备、或者能够用于以指令或数据结构形式存储期望的程序代码并能够由计算机进行存取的任何其它介质。此外,可以将任何连接适当地称作计算机可读介质。如本文所使用的,磁盘和光盘包括压缩光盘(CD)、激光光盘、光学光盘、数字通用光盘(DVD)、软盘和蓝光™光盘,其中磁盘通常磁性地复制数据,而光盘则用激光来光学地复制数据。上述的组合也可以包括在计算机可读介质的保护范围之内。另外地,方法或算法的操作可以作为代码和指令中的一项或其任意组合或其集合而存在于机器可读介质和计算机可

读介质上，所述机器可读介质和计算机可读介质可以并入到计算机程序产品中。

[0120] 对本公开内容所描述的实现方式的各种修改，对于本领域技术人员来说可以是显而易见的，并且，本文定义的总体原理也可以在不脱离本公开内容的精神或保护范围的基础上适用于其它实现方式。因此，权利要求不旨在限于本文所示出的实现方式，而是要符合与本公开内容、原理和新颖性特征相一致的最宽泛的保护范围。

[0121] 另外地，本领域普通技术人员将容易地理解，有时将术语“较上”和“较下”用于便于描述附图，以及指示与适当取向的页面上的图形的方向相对应的相对位置，并且可能不反映如所实现的任何装置的正确取向。

[0122] 本说明书中在分开的实现方式的背景下所描述的某些特征，也可以组合到单个实现方式中来实现。相反地，在单个实现方式的背景下所描述的各种特征，也可以分开地或者以任何适当的子组合在多个实现方式中实现。此外，虽然上面将一些特征描述成在某些组合下进行工作，以及即使最初按此要求保护，但在一些情况下，可以将所要求保护的组合中的一个或多个特征从该组合中切割，以及所要求保护的组合可以是针某种子组合或者子组合的变形的。

[0123] 类似地，虽然在附图中以特定顺序描绘了操作，但这不应当被理解为：为了实现期望的结果，需要以所示的特定顺序或者序列顺序来执行这些操作，或者执行示出的所有操作。此外，附图以流程图的形式示意性地描绘了一个或多个示例过程。然而，未描绘的其它操作可以并入到示意性示出的示例过程中。例如，一个或多个额外的操作可以在所示出的操作之前、之后、同时或者之间执行。在某些环境下，多任务处理和并行处理是有利的。此外，不应当将对上面描述的实现方式中的各个系统组件的划分，理解为在所有实现方式中都需要这种划分，以及应当理解的是，所描述的程序组件和系统通常可以一起集成到单个软件产品中，或者封装到多个软件产品中。另外的，其它实现方式也在所附权利要求的保护范围之内。在一些情况下，可以按不同的顺序执行权利要求中记载的动作，并且仍然实现期望的结果。

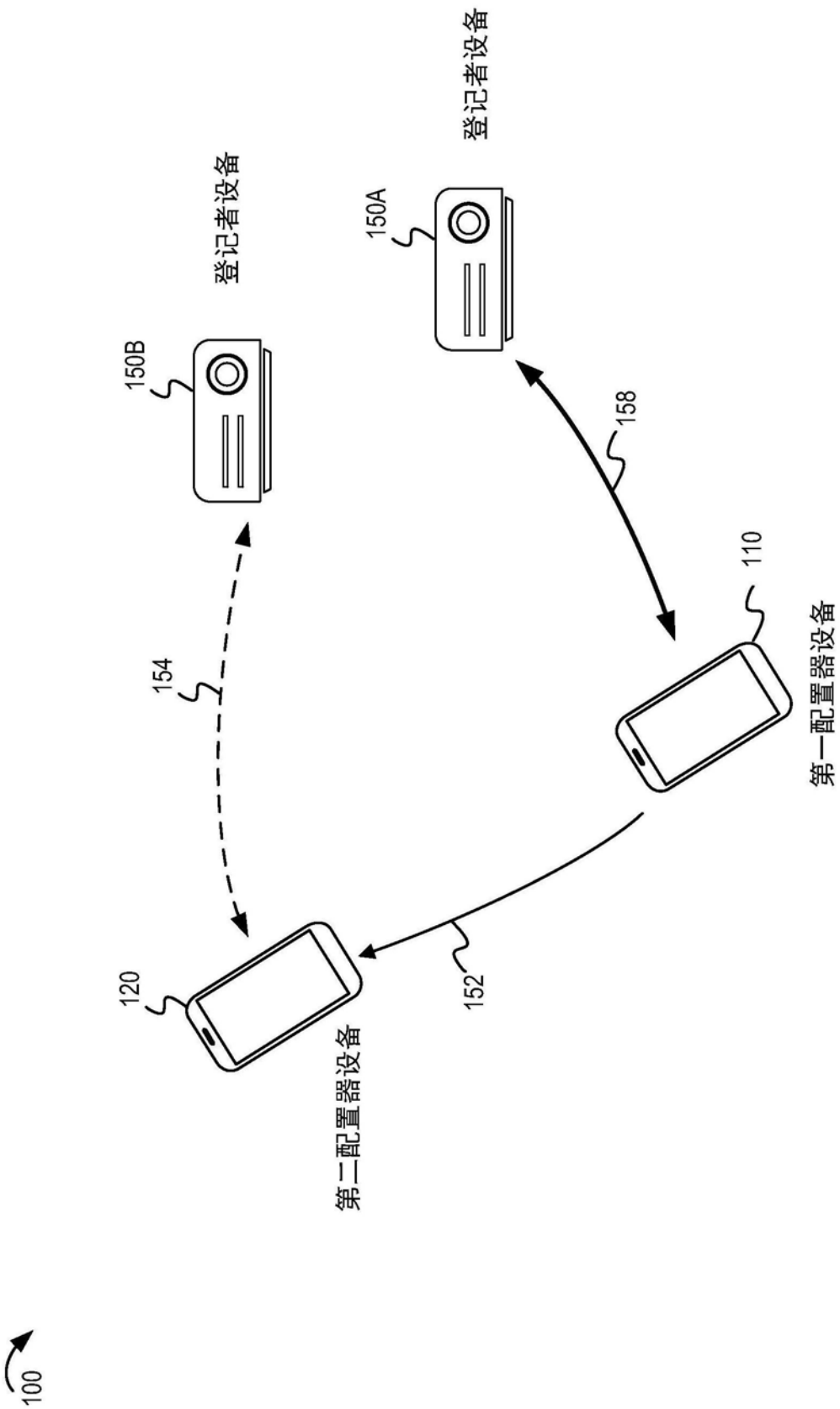

登记者设备
登记者设备
150A
150B
158
110
第一配置器设备
154
120
152
第二配置器设备
100

图1

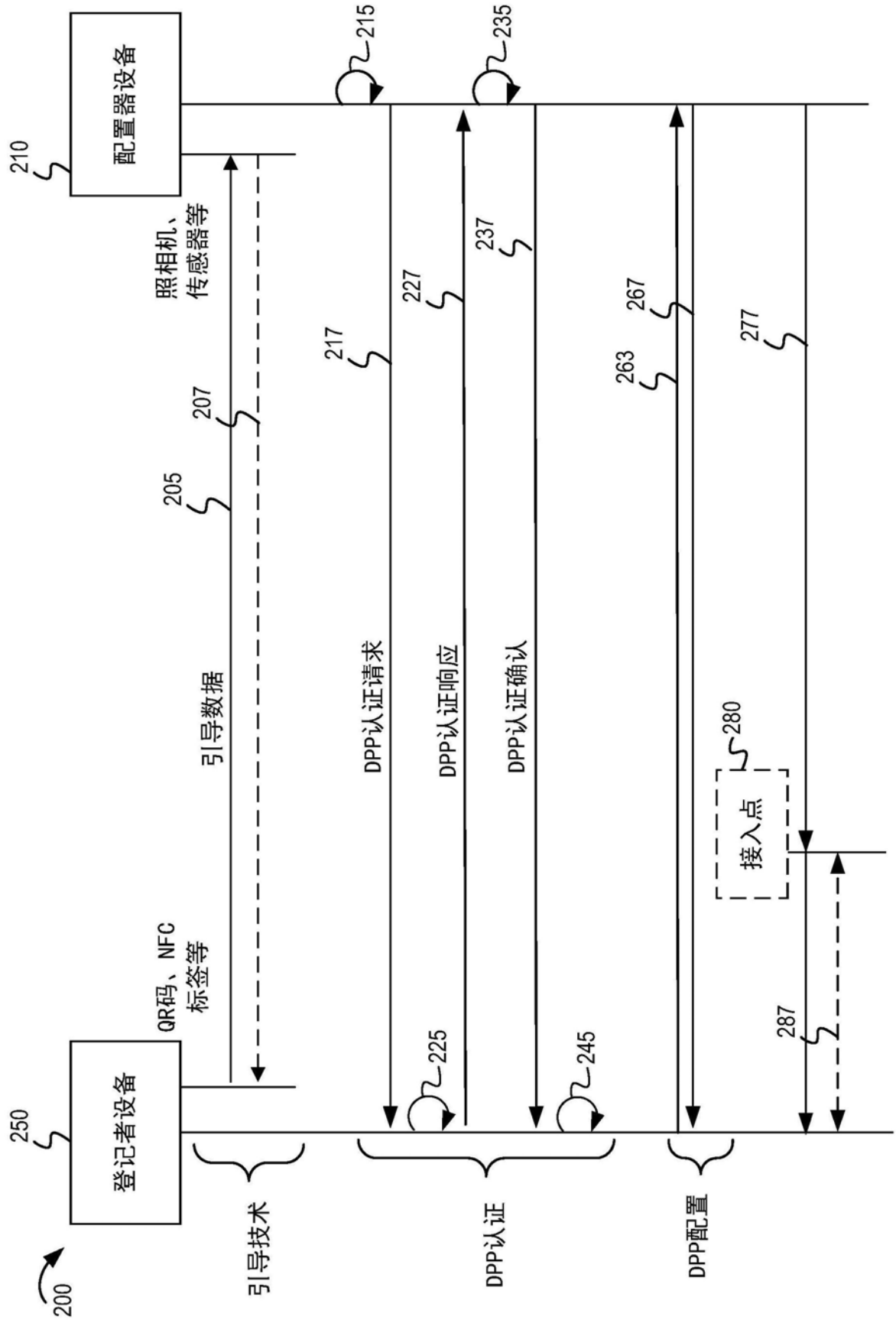

配置器设备
210
215
235
照相机、
传感器等
207
237
227
217
267
263
277
205
引导数据
DPP认证请求
DPP认证响应
DPP认证确认
280
接入点
QR码、NFC
标签等
225
245
287
登记者设备
250
引导技术
DPP认证
DPP配置
200

图2

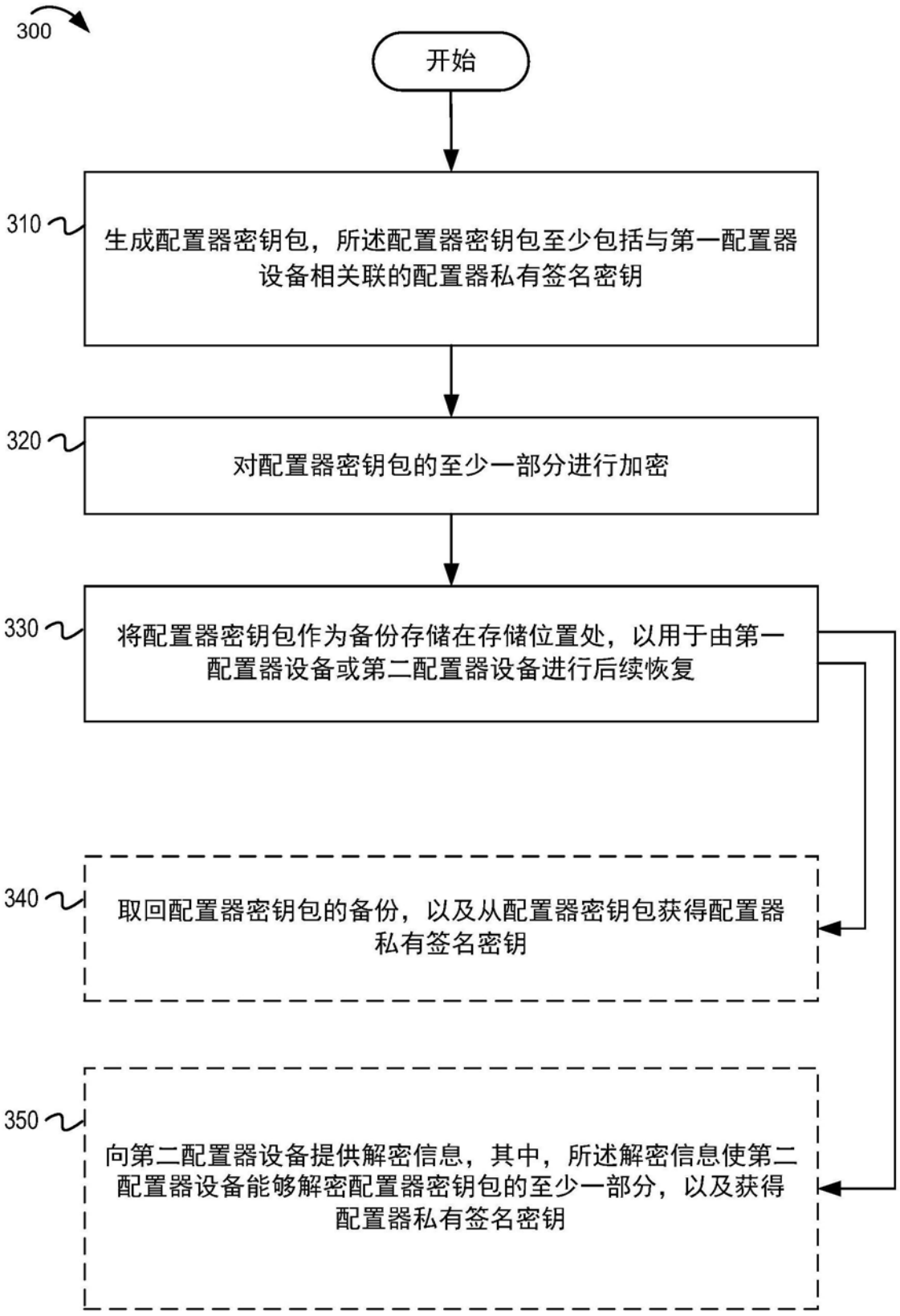

300
开始
310
生成配置器密钥包，所述配置器密钥包至少包括与第一配置器设备相关联的配置器私有签名密钥
320
对配置器密钥包的至少一部分进行加密
330
将配置器密钥包作为备份存储在存储位置处，以用于由第一配置器设备或第二配置器设备进行后续恢复
340
取回配置器密钥包的备份，以及从配置器密钥包获得配置器私有签名密钥
350
向第二配置器设备提供解密信息，其中，所述解密信息使第二配置器设备能够解密配置器密钥包的至少一部分，以及获得配置器私有签名密钥

图3

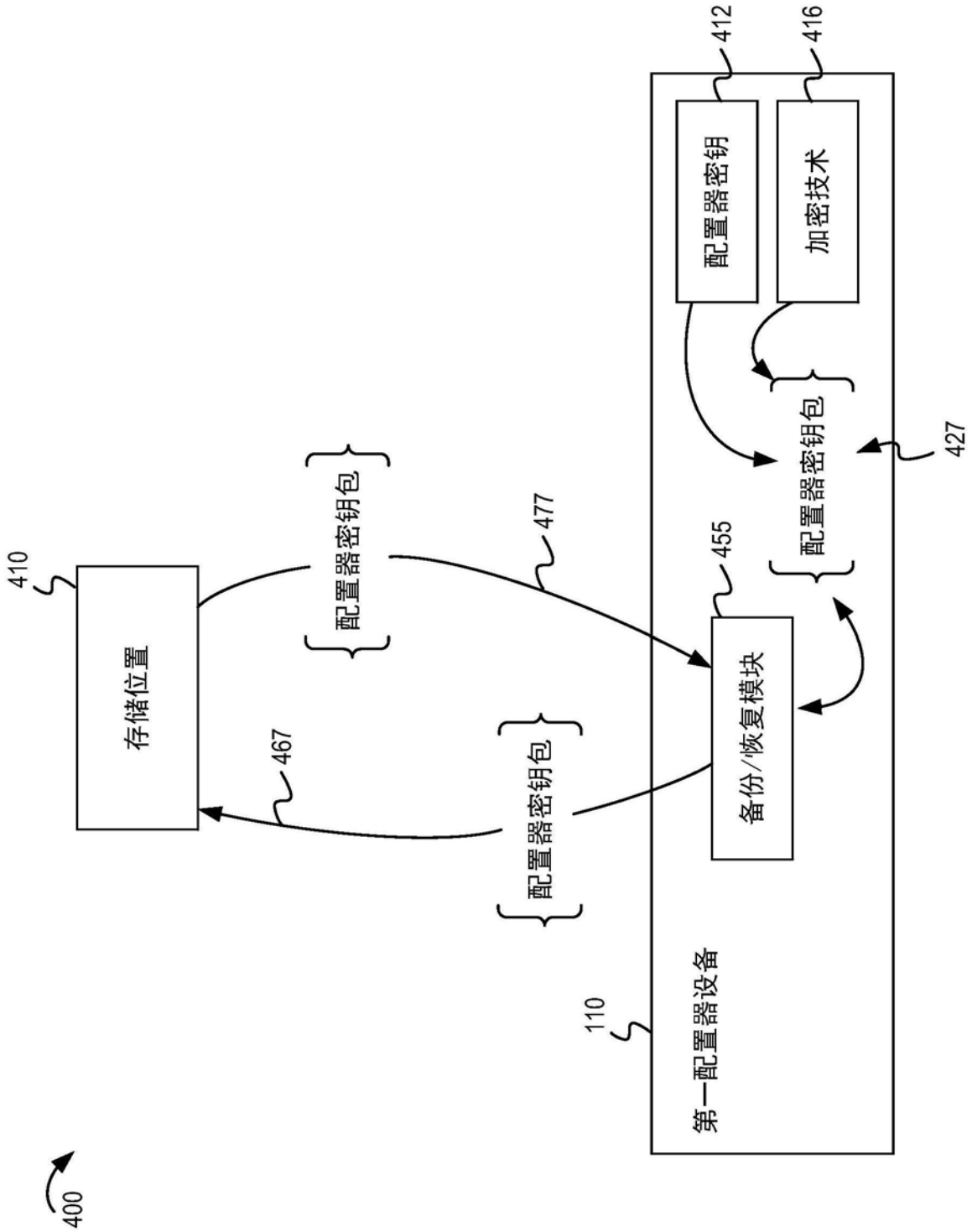

400
410
存储位置
配置器密钥包
467
477
配置器密钥包
110
第一配置器设备
412
配置器密钥
416
加密技术
427
配置器密钥包
455
备份/恢复模块

图4

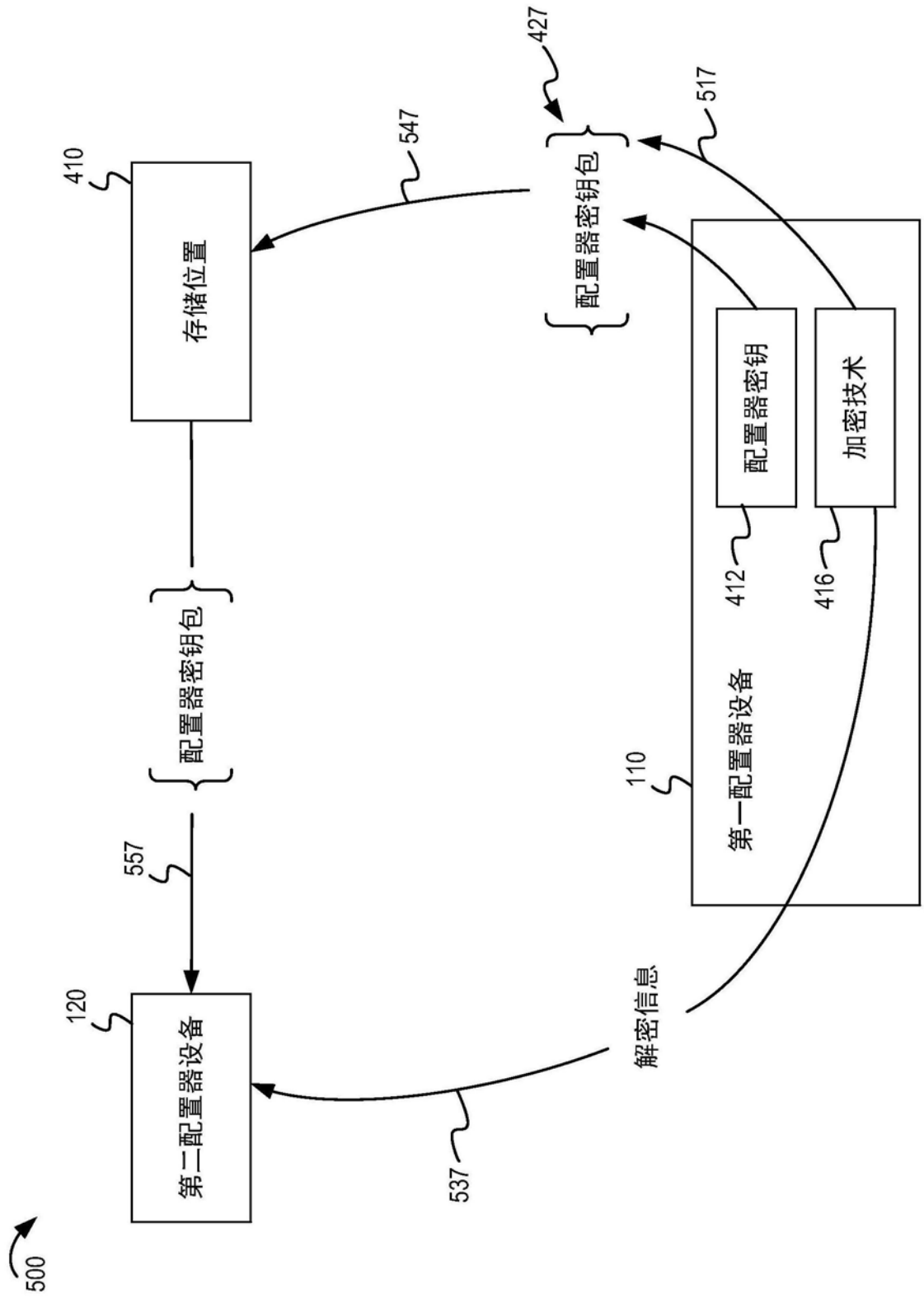

500
410
存储位置
547
427
517
配置器密钥包
配置器密钥包
557
120
第二配置器设备
537
110
第一配置器设备
配置器密钥
412
加密技术
416
解密信息

图5

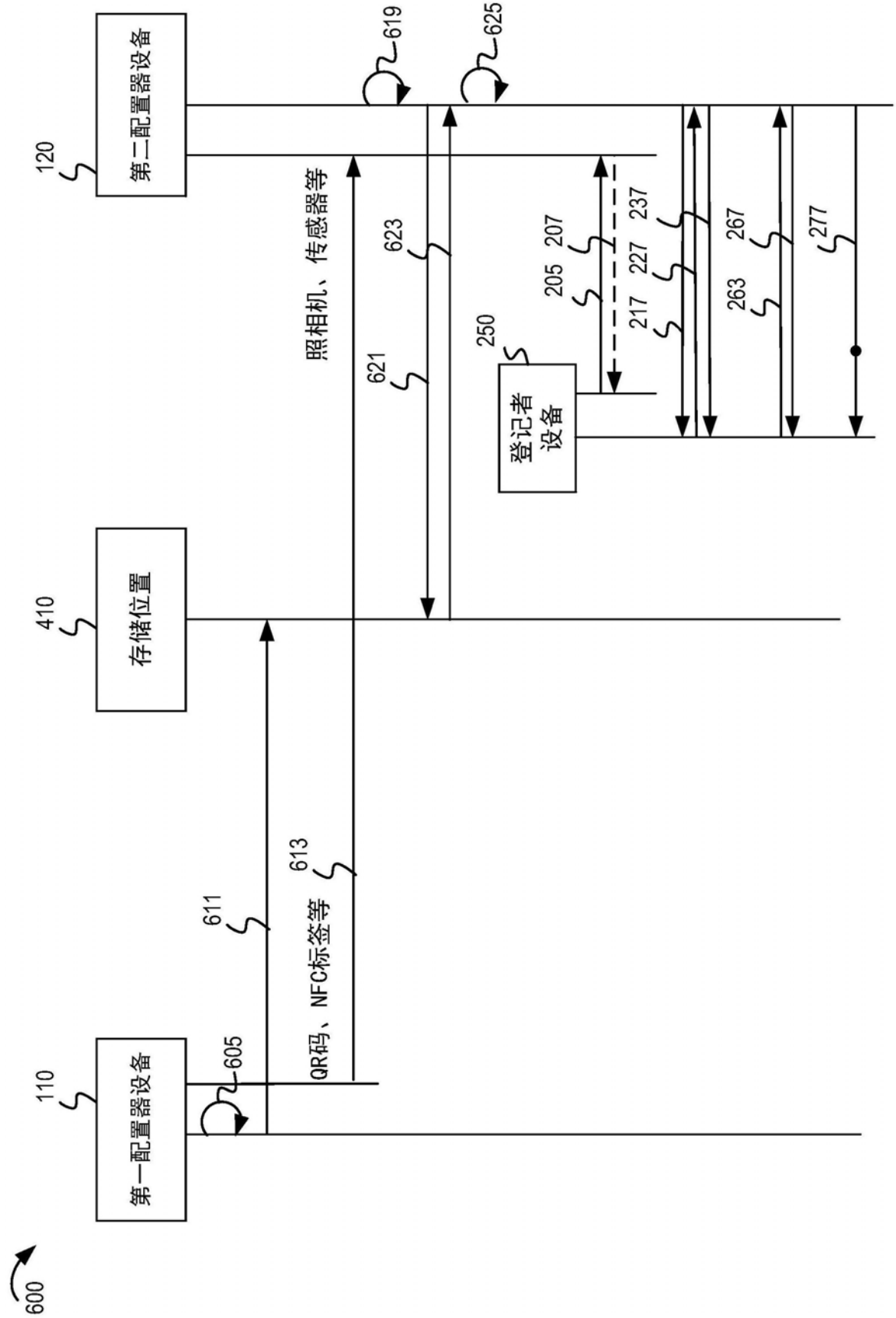

600
第一配置器设备
110
第二配置器设备
120
存储位置
410
登记者设备
250
605
611
613
QR码、NFC标签等
619
621
623
625
照相机、传感器等
205
207
217
227
237
263
267
277

图6

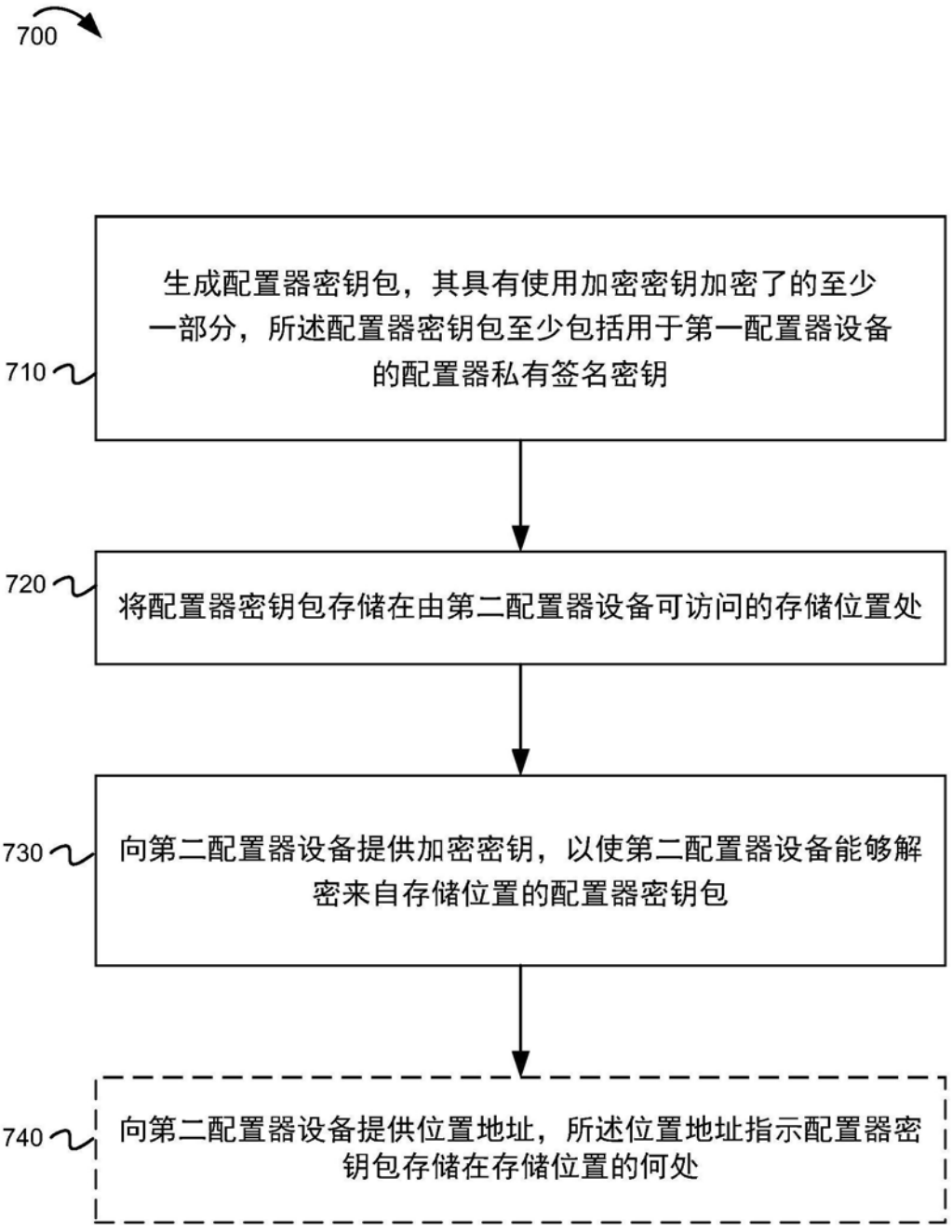

700
生成配置器密钥包，其具有使用加密密钥加密了的至少一部分，所述配置器密钥包至少包括用于第一配置器设备的配置器私有签名密钥
710
将配置器密钥包存储在由第二配置器设备可访问的存储位置处
720
向第二配置器设备提供加密密钥，以使第二配置器设备能够解密来自存储位置的配置器密钥包
730
向第二配置器设备提供位置地址，所述位置地址指示配置器密钥包存储在存储位置的何处
740

图7

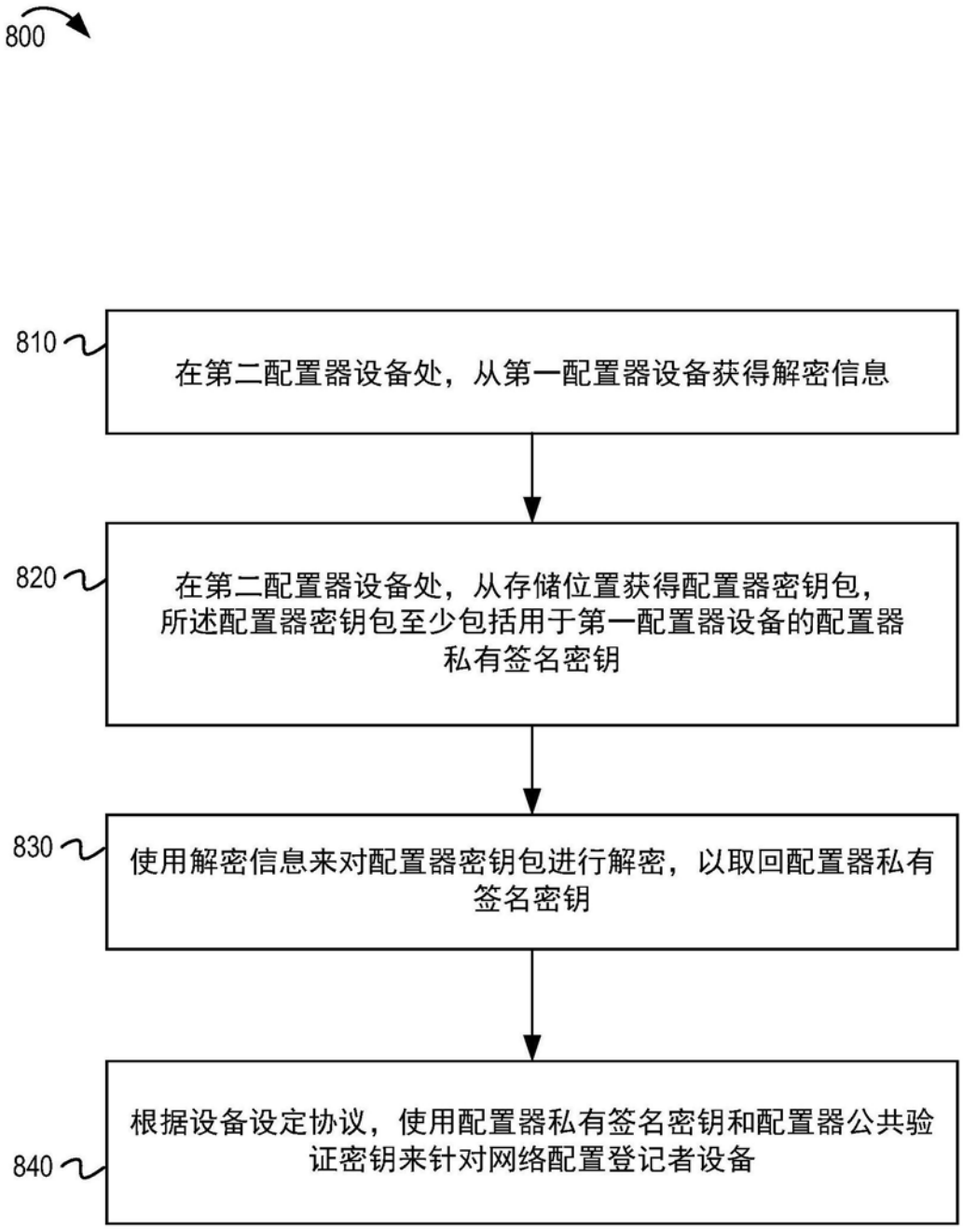

800
810
在第二配置器设备处，从第一配置器设备获得解密信息
820
在第二配置器设备处，从存储位置获得配置器密钥包，所述配置器密钥包至少包括用于第一配置器设备的配置器私有签名密钥
830
使用解密信息来对配置器密钥包进行解密，以取回配置器私有签名密钥
840
根据设备设定协议，使用配置器私有签名密钥和配置器公共验证密钥来针对网络配置登记者设备

图8

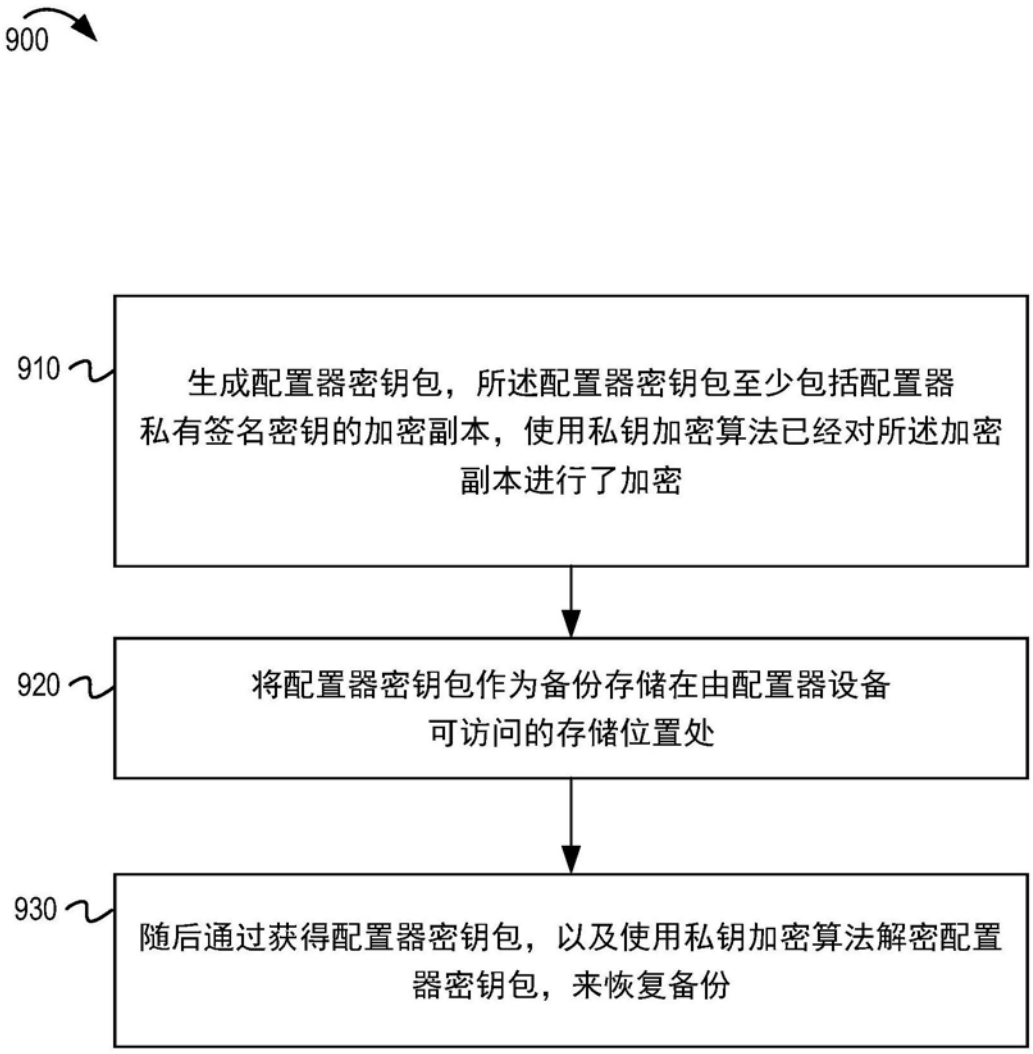

900
910
生成配置器密钥包，所述配置器密钥包至少包括配置器私有签名密钥的加密副本，使用私钥加密算法已经对所述加密副本进行了加密
920
将配置器密钥包作为备份存储在由配置器设备可访问的存储位置处
930
随后通过获得配置器密钥包，以及使用私钥加密算法解密配置器密钥包，来恢复备份

图9

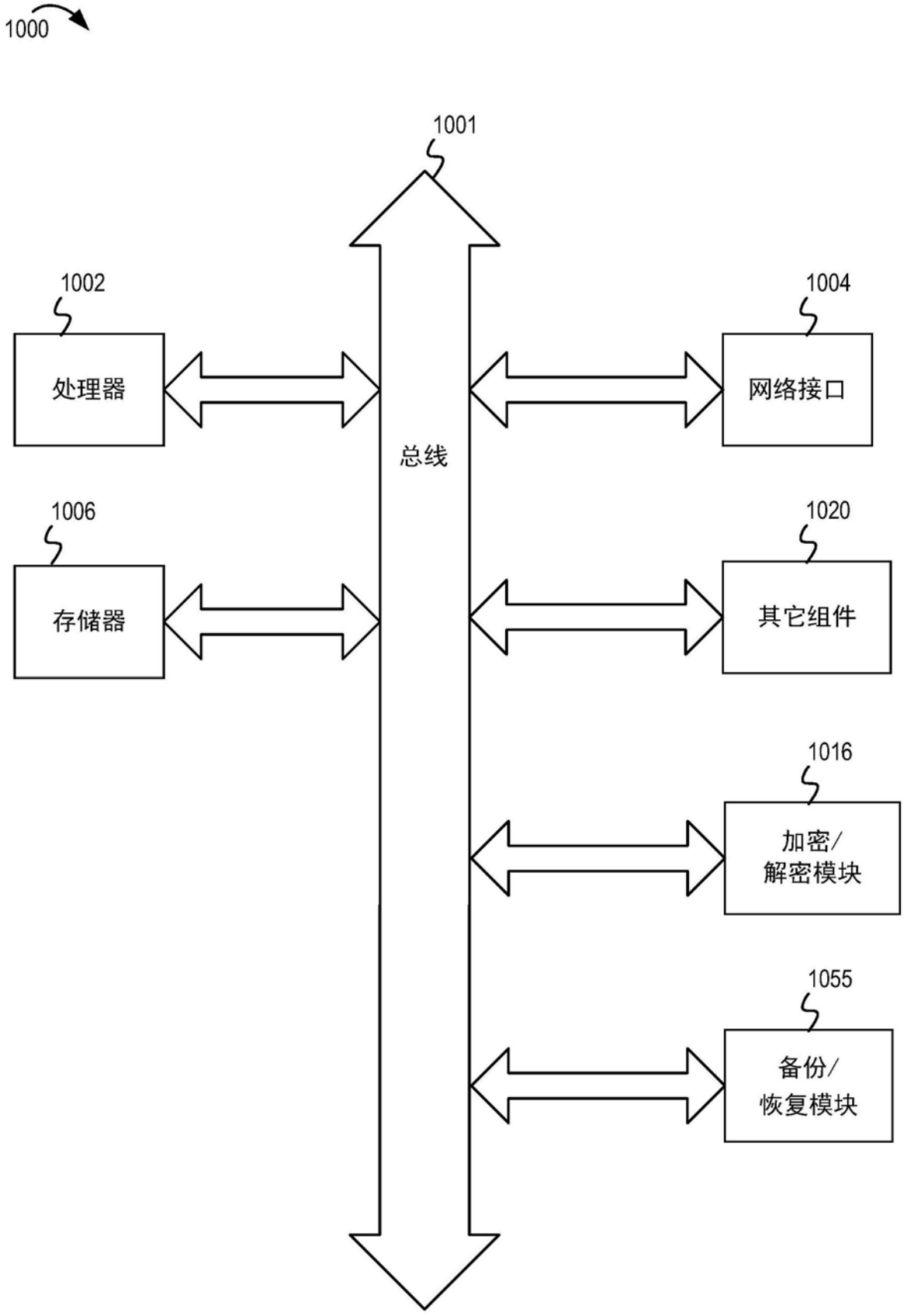

1000
1001
1002
处理器
1004
网络接口
总线
1006
存储器
1020
其它组件
1016
加密/
解密模块
1055
备份/
恢复模块

图10