[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200480040803.4

[43] 公开日 2007 年 1 月 31 日

[11] 公开号 CN 1906888A

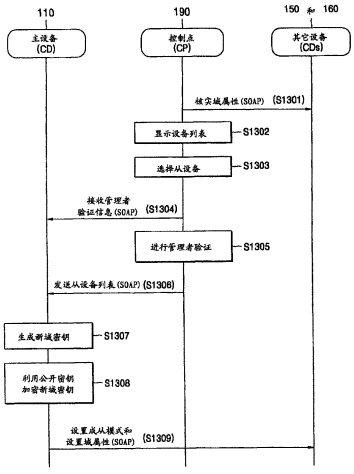
[22] 申请日 2004.11.25
[21] 申请号 200480040803.4
[30] 优先权
[32] 2003.12.1 [33] US [31] 60/525,701
[32] 2004.2.9 [33] KR [31] 10-2004-0008343
[86] 国际申请 PCT/KR2004/003062 2004.11.25
[87] 国际公布 WO2005/055521 英 2005.6.16
[85] 进入国家阶段日期 2006.7.21
[71] 申请人 三星电子株式会社
地址 韩国京畿道
[72] 发明人 张容珍 金明宣 南秀铉 李栽兴
[74] 专利代理机构 北京市柳沈律师事务所
代理人 郭定辉 黄小临
权利要求书 4 页 说明书 18 页 附图 15 页

[54] 发明名称

本地网络系统及其方法

[57] 摘要

一种允许用户利用用户界面直接控制域中成员设备的加入或移去和有效控制域的成员设备的状态变化的本地网络系统及其管理方法。本地网络系统包括：主设备，其与一个以上的受控设备形成域，将预定域密钥发送到包括在域中的受控设备，每当域的配置发生改变时生成新域密钥，并将新域密钥发送到余留在域中的受控设备和控制点，提供允许用户直接改变域的配置的用户界面。



1. 一种本地网络系统，包含:

主设备，其与一个以上的受控设备形成域，将预定域密钥发送到包括在域中的受控设备，每当域的配置发生改变时生成新域密钥，并将新域密钥发送到余留在域中的受控设备；和

控制点，用于提供允许用户直接改变域的配置的用户界面。

2. 根据权利要求 1 所述的本地网络系统，其中，形成域的一些设备提供预定内容。

3. 根据权利要求 2 所述的本地网络系统，其中，域密钥用于加密内容密钥，而内容密钥用于加密预定内容。

4. 根据权利要求 2 所述的本地网络系统，其中，利用接收预定内容的受控设备的公开密钥加密域密钥，和利用与公开密钥形成对的预定秘密密钥解密加密域密钥。

5. 根据权利要求 1 所述的本地网络系统，其中，根据 UPnP 构建本地网络系统。

6. 根据权利要求 1 所述的本地网络系统，其中，利用形成域的设备的设备信息生成域密钥。

7. 根据权利要求 1 所述的本地网络系统，其中，控制点将操作形成域的主设备和从设备所需的信息发送到形成域的主设备和从设备。

8. 根据权利要求 1 所述的本地网络系统，其中，形成域的成员设备共享随形成域的成员设备的改变而改变的会话 ID，如果与域连接的设备的会话 ID 与主设备的会话 ID 不相同，则主设备将存储在主设备中的域密钥发送到相连设备。

9. 根据权利要求 8 所述的本地网络系统，其中，每个受控设备具有作为设备模式的从状态或客状态，如果与域连接的设备的会话 ID 与主设备的会话 ID 不相同和相连设备存在于存储在主设备中的从设备列表之中，则主设备将存储在主设备中的域密钥发送到相连设备。

10. 根据权利要求 9 所述的本地网络系统，其中，如果相连设备未存在于存储在主设备中的从设备列表之中，则将相连设备的设备模式改变成客状态。

11. 根据权利要求 9 所述的本地网络系统，其中，如果与域连接的设备的域 ID 与存储在主设备中的域 ID 不相同，则主设备不将域密钥发送到相连设备。

12. 根据权利要求 9 所述的本地网络系统，其中，如果与域连接的设备的设备模式不是从状态，则主设备不将域密钥发送到相连设备。

13. 根据权利要求 8 所述的本地网络系统，其中，除了唯一 ID 之外，会话 ID 还包含日期信息和/或版本信息。

14. 一种管理本地网络系统的方法，该本地网络系统包含：主设备，其与一个以上的受控设备形成域，并将预定域密钥发送到包括在域中的受控设备；和控制点，用于提供用户界面，该方法包含：

（a）响应利用用户界面输入的用户命令，改变域的配置；

（b）在主设备中根据域的配置变化生成新域密钥；和

（c）将生成的域密钥发送到余留在域中的受控设备。

15. 根据权利要求 14 所述的方法，其中，根据 UPnP 构建本地网络系统。

16. 根据权利要求 14 所述的方法，其中，利用形成域的设备的设备信息生成域密钥。

17. 根据权利要求 14 所述的方法，还包含：

（d）与域的成员设备共享随形成域的成员设备的状态改变而改变的会话 ID；和

（e）如果与域连接的设备的会话 ID 与域的会话 ID 不相同，主设备将域的域密钥发送到相连设备。

18. 根据权利要求 17 所述的方法，其中，每个受控设备具有作为设备模式的从状态或客状态，和在步骤（e）中，如果与域连接的设备的会话 ID 与域的会话 ID 不相同和相连设备存在于存储在主设备中的从设备列表之中，将存储在主设备中的域密钥发送到相连设备。

19. 根据权利要求 18 所述的方法，其中，在步骤（e）中，如果与域连接的设备未存在于从设备列表之中，将相连设备的设备模式设置成客状态。

20. 根据权利要求 18 所述的方法，其中，步骤（e）包含：如果与域连接的设备的域 ID 与域的域 ID 不相同，则不将域密钥发送到相连设备。

21. 根据权利要求 18 所述的方法，其中，步骤（e）包含：如果与域连接的设备的设备模式不是从状态，则不将域密钥发送到相连设备。

22. 根据权利要求 17 所述的方法，其中，除了唯一 ID 之外，会话 ID 还包含日期信息和/或版本信息。

23. 一种本地网络系统中的本地网络管理控制装置，该本地网络系统包含与一个以上的受控设备形成域的主设备，该装置包含:

用户界面提供者，用于提供允许用户直接改变域的配置的用户界面；和

设备操作信息提供者，用于根据利用用户界面输入的用户命令，将操作域的成员设备所需的信息发送到域的成员设备。

24. 一种本地网络系统中的本地网络管理控制装置，该本地网络系统包含与一个以上的受控设备形成域的主设备，该装置包含:

用户界面提供者，用于提供允许用户直接改变域的配置的用户界面;

设备检测器，用于检测与本地网络管理控制装置连接的设备；和

设备操作信息提供者，用于将相连设备的信息发送到主设备和将主设备的处理结果发送到相连设备。

25. 一种与一个以上的受控设备形成域的主设备，该主设备包含:

受控设备管理器，用于对受控设备进行验证;

域 ID 管理器，用于生成标识域的域 ID，并将域 ID 发送到域的成员设备;

会话 ID 管理器，用于生成随域的配置改变而改变的会话 ID，并将会话 ID 发送到域的成员设备；和

域密钥管理器，用于生成随域的配置改变而改变的域密钥，并将域密钥发送到域的成员设备。

26. 一种由主设备管理受控设备的方法，该主设备与一个以上的受控设备形成域，该方法包含:

（a）对受控设备进行验证;

（b）生成标识域的域 ID 和将域 ID 发送到域的成员设备;

（c）生成随域的配置改变而改变的会话 ID，并将会话 ID 发送到域的成员设备；和

（d）生成随域的配置改变而改变的域密钥，并将域密钥发送到域的成员设备。

27. 一种记录着执行如权利要求 26 所述的方法的计算机可读程序的计算机可读媒体。

28. 一种与从设备形成域的主设备，每个从设备在作为设备模式的从状

态下工作，多个受控设备在作为设备模式的从状态或客状态下工作，该主设备包含:

受控设备管理器，用于对与域连接的受控设备进行验证和设备模式确定，生成和改变从设备列表，和确定相连设备是否存在于从设备列表之中;

域 ID 管理器，用于生成标识域的域 ID，并将主设备的域 ID 与相连设备的域 ID 相比较;

会话 ID 管理器，用于将随域的配置改变而改变的主设备的会话 ID 与相连设备的会话 ID 相比较; 和

域密钥管理器，用于生成随域的配置改变而改变的域密钥，如果作为域 ID 管理器的比较结果域 ID 相同，作为会话 ID 管理器的比较结果会话 ID 不相同，而作为受控设备管理器的确定结果相连设备存在于从设备列表之中，则将主设备的域密钥发送到相连设备。

29. 一种由主设备管理受控设备的方法，该主设备与受控设备形成域，每个从设备在作为设备模式的从状态下工作，多个受控设备在作为设备模式的从状态或客状态下工作，该方法包含:

（a）对与域连接的设备进行验证;

（b）如果验证成功，确定相连设备的设备模式;

（c）如果作为步骤（b）的确定结果，相连设备的设备模式是从状态，将主设备的会话 ID 与相连设备的会话 ID 相比较;

（d）如果作为步骤（c）的比较结果，会话 ID 不相同，确定相连设备是否存在于示出其各自设备模式是从状态的受控设备的从设备列表之中;和(e)如果作为步骤（d）的确定结果，相连设备存在于从设备列表之中，将随域的配置改变而改变的主设备的域密钥发送到相连设备。

30. 根据权利要求 29 所述的方法，还包含，至少在步骤（c）之前，将可以标识域的和域的成员设备共享的域 ID 与相连设备的域 ID 相比较，如果域 ID 不相同，不执行下一个步骤。

31. 一种记录着执行如权利要求 29 或 30 所述的方法的计算机可读程序的计算机可读媒体。

本地网络系统及其方法

技术领域

本发明涉及管理本地网络域中的设备的方法，尤其涉及允许用户利用用户界面直接连接或断开域中的成员设备和有效地控制域中成员设备的状态变化的本地网络系统及其管理方法。

背景技术

最近人们提出了一些在本地网络上保护内容的本地网络技术，譬如，Thomson 公司提出的“SmartRight”、Sysco 公司提出的“开放条件内容访问管理（OCCAM）”和 IBM 公司提出的“xCP 群集协议”。

SmartRight 是将包括公开密钥证书的智能卡放置在本地网络中的每个设备中，并且通过利用智能卡在设备之间交换证书，生成用于本地网络的密钥的方法。

OCCAM 是本地网络中的设备利用每个内容的唯一凭证使用内容的方法。

xCP 群集协议是一种基于广义加密的技术，它利用叫做群集的域概念和在包括在群集中的设备之间自由使用内容的方法。

图 1 是例示传统本地域结构的方块图。

参照图 1，已验证本地域 100 包括主设备 110 和多个从设备 120－140。在主设备 110 和多个从设备 120－140 之间管理一个域。

现在参照图 2 描述基于 xCP 群集协议的内容再现过程。

图 2 是例示根据传统主从结构的基于 xCP 群集协议的内容再现过程的流程图。

参照图 2，内容再现过程大体上划分成步骤 S200 中的群集生成过程、步骤 S210 中的设备验证过程、步骤 S220 中的内容加密过程和步骤 S230 中的内容解密过程，其操作如下。

最初与本地网络连接的服务器在步骤 S200 中生成本地网络的结合标识符（ID_b）。这里，ID_b 可以是制造服务器时设置的唯一标识符或由用户设置的唯一标识符。当生成 ID_b 时，生成由 ID_b 标识的群集。

打算使用存储在服务器中的内容的设备在步骤 S212 中利用它自己的设备密钥组从媒体密钥块（MKB）中提取媒体密钥（K_m）。该设备在步骤 S214 中利用提取的 K_m 和个人 ID（ID_p）生成个人密钥（K_p）。该设备在步骤 S216 中向服务器请求设备验证，以便使自己验证成成员设备。也就是说，该设备将作为个人唯一标识符的 ID_p、作为代表设备类型的类型标识符的‘tpye’和作为 ID_p 和 type 的散列值的值

$$h = MAC(ID_p \| type)K_p$$

发送到群集内或群集外的设备验证服务器。

服务器利用 K_m 和 ID_p 获取值 K_p'，将利用值 K_p' 获得的散列值

$$h' = MAC(ID_p \| type)K_p'$$

与从该设备接收的散列值 h 相比较，确定散列值 h′ 和散列值 h 是否相同。如果散列值 h′ 和散列值 h 相同，服务器将利用 K_p 加密 ID_b 的值 $E(ID_b)K_p$ 和 ID_p 发送到该设备，并将 ID_p 加入它自己的验证表（auth.tab）中。该设备从从服务器接收的值 $E(ID_b)K_p$ 中提取 ID_b，然后，在步骤 S218 中完成设备验证。

在设备验证完成之后，服务器在步骤 S220 中加密要发送到设备的内容。首先，服务器在步骤 S222 中利用 ID_b、auth.tab 和 K_m 生成结合密钥（K_b），其中，$K_b = H[ID_b?H[auth.tab], K_m]$。

服务器在步骤 S224 中利用标量密钥（K_t）加密内容以保护内容。包括复制控制信息、是否允许传送的信息、使用权限和许可证有效期限的使用规则（UR）信息包含在每个内容中。服务器在步骤 S226 中像 $E(K_t?H[UR])K_b$ 那样利用 K_b 加密 UR 信息和 K_t。

该设备从服务器接收 auth.tab，在步骤 S232 中利用提取的 K_m 从 $K_b = H[ID_b?H[auth.tab], K_m]$ 中提取 K_b，在步骤 S234 中从 $E(K_t?H[UR])K_b$ 中提取 K_t，和在步骤 S236 中利用提取的 K_t 解密从服务器接收的内容。

根据上述的 xCP 群集协议，通信范围内的所有设备可以自动加入域中，而无需对要包括在域中的设备作出选择或限定。此外，每当每个设备新生成 K_b 时，该设备必须从服务器接收 auth.tab 和进行计算。因此，有必要在用户的控制下确定本地域的成员设备，并且通过将本地域构建成与外界独立，更安全地保护内容。

近来，人们提出了利用通用即插即用（UPnP）基础设施管理本地网络的方法。一般说来，UPnP 是识别与通用计算机连接的计算机外设的标准化功能。

并且，人们正在将 UPnP 改进成网络中间件标准，据此，除了计算机外设之外的本地联合体和无线设备在它们与网络连接时可以自动得到识别。此外，由于 UPnP 使用了传统标准因特网协议，UPnP 可以顺利地整合到传统网络中，不依赖于特定操作系统或物理媒体。但是，由于利用 UPnP 管理域的方法还不是著名的，有必要开发出利用 UPnP 有效管理域的方法。

发明内容

技术解决方案

本发明提供了管理允许用户直接控制域的形成和更安全地将域构建成与外界独立的本地网络的方法。

本发明还提供了基于可以利用传统因特网协议顺利整合到网络中的 UPnP 的本地网络系统。

本发明还提供了通过允许用户直接控制本地网络中域的成员设备的状态变化，允许主设备负责根据成员设备的变化生成新域密钥，和允许从设备接收主设备生成的域密钥，简化根据域的配置变化的域密钥改变过程的方法和装置。

本发明还提供了通过除了域 ID 和域密钥之外还引入会话 ID 作为域共享信息，防止域密钥被频繁改变的方法和装置。

有益效果

根据本发明，用户可以直接控制域的形成和更安全地构建域。

此外，根据本发明，可以开发出可以利用传统标准因特网协议顺利整合到网络中的 UPnP 基础设施的本地网络系统。

此外，根据本发明，通过允许用户直接控制本地网络域的成员设备的变化，允许主设备根据成员设备的变化生成新域密钥，和允许从设备接收主设备生成的域密钥，可以简化根据域配置变化改变域密钥的过程。

此外，根据本发明，通过除了域 ID 和域密钥之外还引入会话 ID 作为域共享信息，和当从设备发生频繁连接/断开时不改变域密钥，可以防止域密钥被频繁改变。

附图说明

图 1 是例示传统本地域结构的方块图;

图 2 是例示根据传统主从结构的基于“xCP 群集协议”的内容再现过程的流程图;

图 3 是例示构建公开密钥基础设施（PKI）的域的方法的流程图;

图 4 是例示采用根据本发明一个实施例构建域的方法的 UPnP 的方块图;

图 5 例示了在控制点和受控设备之间进行的典型 UPnP 操作;

图 6 是例示根据本发明一个实施例确定主设备的过程的流程图;

图 7 是例示与如图 6 所示的过程平行的设备验证过程的流程图;

图 8 是例示与如图 7 所示的过程平行的确定从设备的过程的流程图;

图 9A－9C 例示了控制点提供的用户界面表示;

图 10 是例示根据本发明一个示范性实施例确定主设备的另一个过程的流程图;

图 11 是例示与如图 10 所示的过程平行的设备验证过程的流程图;

图 12 是例示与如图 11 所示的过程平行的确定从设备的过程的流程图;

图 13 是例示根据本发明一个实施例生成域密钥的过程的流程图;

图 14 例示了根据从设备的连接/断开的域状态;

图 15 例示了根据从设备的连接/断开的另一种域状态;

图 16 是例示根据本发明一个实施例管理与域新连接的设备的过程的流程图;

图 17 是根据本发明一个实施例的控制点的方块图; 和

图 18 是根据本发明一个实施例的主设备的方块图。

具体实施方式

根据本发明的一个方面，提供了包括如下的本地网络系统: 主设备，其与一个以上的受控设备形成域，将预定域密钥发送到包括在域中的受控设备，每当域的配置发生改变时生成新域密钥，并将新域密钥发送到余留在域中的受控设备; 和控制点，用于提供允许用户直接改变域的配置的用户界面。

根据一个实施例，形成域的一些设备提供预定内容。

根据另一个实施例，域密钥用于加密内容密钥，而内容密钥用于加密预定内容。

根据又一个实施例，利用接收预定内容的受控设备的公开密钥加密域密

钥，和利用与公开密钥形成对的预定秘密密钥解密加密域密钥。

根据又一个实施例，根据 UPnP 构建本地网络系统。

根据又一个实施例，利用形成域的设备的设备信息生成域密钥。

根据又一个实施例，控制点将操作形成域的主设备和从设备所需的信息发送到形成域的主设备和从设备。

根据另一个实施例，形成域的成员设备共享随形成域的成员设备的改变而改变的会话 ID,如果与域连接的设备的会话 ID 与主设备的会话 ID 不相同，则主设备将存储在主设备中的域密钥发送到相连设备。

根据另一个实施例，每个受控设备具有作为设备模式的从状态或客状态，如果与域连接的设备的会话 ID 与主设备的会话 ID 不相同和相连设备存在于存储在主设备中的从设备列表之中，则主设备将存储在主设备中的域密钥发送到相连设备。

根据另一个实施例，如果相连设备未存在于存储在主设备中的从设备列表之中，则将相连设备的设备模式改变成客状态。

根据另一个实施例，如果与域连接的设备的域 ID 与存储在主设备中的域 ID 不相同，则主设备不将域密钥发送到相连设备。

根据另一个实施例，如果与域连接的设备的设备模式不是从状态，则主设备不将域密钥发送到相连设备。

根据另一个实施例，除了唯一 ID 之外，会话 ID 还包含日期信息和/或版本信息。

根据本发明的另一个方面，提供了管理本地网络系统的方法，该本地网络系统包含：主设备，其与一个以上的受控设备形成域，并将预定域密钥发送到包括在域中的受控设备；和控制点，用于提供用户界面，该方法包含：（a)响应利用用户界面输入的用户命令，改变域的配置；（b）在主设备中根据域的配置变化生成新域密钥；和（c）将生成的域密钥发送到余留在域中的受控设备。

根据一个实施例，根据 UPnP 构建本地网络系统。

根据一个实施例，利用形成域的设备的设备信息生成域密钥。

根据一个实施例，该方法还包含：（d）与域的成员设备共享随形成域的成员设备的状态改变而改变的会话 ID；和（e）如果与域连接的设备的会话 ID 与域的会话 ID 不相同，主设备将域的域密钥发送到相连设备。

根据一个实施例，每个受控设备具有作为设备模式的从状态或客状态，和在步骤（e）中，如果与域连接的设备的会话 ID 与域的会话 ID 不相同和相连设备存在于存储在主设备中的从设备列表之中，将存储在主设备中的域密钥发送到相连设备。

根据一个实施例，在步骤（e）中，如果与域连接的设备未存在于从设备列表之中，将相连设备的设备模式设置成客状态。

根据一个实施例，步骤（e）包含：如果与域连接的设备的域 ID 与域的域 ID 不相同，则不将域密钥发送到相连设备。

根据另一个实施例，步骤（e）包含：如果与域连接的设备的设备模式不是从状态，则不将域密钥发送到相连设备。

根据另一个实施例，除了唯一 ID 之外，会话 ID 还包含日期信息和/或版本信息。

根据本发明的另一个方面，提供了本地网络系统的本地网络管理控制装置，该本地网络系统包含与一个以上的受控设备形成域的主设备，该装置包含：用户界面提供者，用于提供允许用户直接改变域的配置的用户界面；和设备操作信息提供者，用于根据利用用户界面输入的用户命令，将操作域的成员设备所需的信息发送到域的成员设备。

根据本发明的另一个方面，提供了本地网络系统中的本地网络管理控制装置，该本地网络系统包含与一个以上的受控设备形成域的主设备，该装置包含：用户界面提供者，用于提供允许用户直接改变域的配置的用户界面；设备检测器，用于检测与本地网络管理控制装置连接的设备；和设备操作信息提供者，用于将相连设备的信息发送到主设备和将主设备的处理结果发送到相连设备。

根据本发明的另一个方面，提供了与一个以上的受控设备形成域的主设备，该主设备包含：受控设备管理器，用于对受控设备进行验证；域 ID 管理器，用于生成标识域的域 ID，并将域 ID 发送到域的成员设备；会话 ID 管理器，用于生成随域的配置改变而改变的会话 ID，并将会话 ID 发送到域的成员设备；和域密钥管理器，用于生成随域的配置改变而改变的域密钥，并将域密钥发送到域的成员设备。

根据本发明的另一个方面，提供了由主设备管理受控设备的方法，该主设备与一个以上的受控设备形成域，该方法包含：（a）对受控设备进行验证；

（b）生成标识域的域 ID 和将域 ID 发送到域的成员设备；（c）生成随域的配置改变而改变的会话 ID，并将会话 ID 发送到域的成员设备；和（d）生成随域的配置改变而改变的域密钥，并将域密钥发送到域的成员设备。

根据本发明的另一个方面，提供了记录着执行管理受控设备的方法的计算机可读程序的计算机可读媒体。

根据本发明的另一个方面，提供了与从设备形成域的主设备，每个从设备在作为设备模式的从状态下工作，多个受控设备在作为设备模式的从状态或客状态下工作，该主设备包含：受控设备管理器，用于对与域连接的受控设备进行验证和设备模式确定，生成和改变从设备列表，和确定相连设备是否存在于从设备列表之中；域 ID 管理器，用于生成标识域的域 ID，并将主设备的域 ID 与相连设备的域 ID 相比较；会话 ID 管理器，用于将随域的配置改变而改变的主设备的会话 ID 与相连设备的会话 ID 相比较；和域密钥管理器，用于生成随域的配置改变而改变的域密钥，如果作为域 ID 管理器的比较结果域 ID 相同，作为会话 ID 管理器的比较结果会话 ID 不相同，而作为受控设备管理器的确定结果相连设备存在于从设备列表之中，则将主设备的域密钥发送到相连设备。

根据本发明的另一个方面，提供了由主设备管理受控设备的方法，该主设备与从设备形成域，每个从设备在作为设备模式的从状态下工作，多个受控设备在作为设备模式的从状态或客状态下工作，该方法包含：（a）对与域连接的设备进行验证；（b）如果验证成功，确定相连设备的设备模式；（c）如果作为步骤（b）的确定结果，相连设备的设备模式是从状态，将主设备的会话 ID 与相连设备的会话 ID 相比较；（d）如果作为步骤（c）的比较结果，会话 ID 不相同，确定相连设备是否存在于示出其各自设备模式是从状态的受控设备的从设备列表之中；和（e）如果作为步骤（d）的确定结果，相连设备存在于从设备列表之中，将随域的配置改变而改变的主设备的域密钥发送到相连设备。

根据另一个实施例，至少在步骤（c）之前，该方法还包含将可以标识域的和域的成员设备共享的域 ID 与相连设备的域 ID 相比较，如果域 ID 不相同，不执行下一个步骤。

根据本发明的另一个方面，提供了记录着执行管理受控设备的方法的计算机可读程序的计算机可读媒体。

本发明的实施方式

在下文中，将参照示出本发明的示范性实施例的附图更全面地描述本发明。在附图中相同的标号自始至终用于表示相同的单元。

图 3 是例示构建公开密钥基础设施（PKI）的域的方法的流程图。假设向内容供应服务器请求内容的每个设备具有唯一秘密密钥组和在生产设备时生成公开密钥组的公开密钥或函数。这里秘密密钥组用于从通过广播加密方法提供的秘密信息块（SIB）中提取秘密值。SIB 是核实设备是否被拒绝的信息。被拒设备不能从 SIB 中提取秘密值，并且接受设备可以从 SIB 中提取公用秘密值。

为了构建域，服务器 320 在步骤 S332 中通过广播加密方法从外部服务器 310 接收 SIB。在步骤 S334 中，关于设备 330，服务器 320 通过经由有线或无线网络从设备 330 接收信息，或通过检测设备 330，识别设备 330 是否存在。

服务器 320 将识别设备 330 显示在显示装置上，和用户在步骤 S336 中从显示在显示装置上的设备当中选择要加入域中的设备 330。服务器 320 在步骤 S338 中将从外部服务器 310 接收的 SIB 发送到用户选择的设备 330。已经接收到 SIB 的每个设备 SIB 在步骤 S340 中从 SIB 中提取秘密值，并且在步骤 S342 中利用提取的秘密值生成自身公开密钥的证书。

当每个设备 330 在步骤 S344 中将每个设备拥有的证书、设备唯一标识符（ID）和公开密钥发送到服务器 320 时，服务器 320 在步骤 S346 中通过核实证书来检验设备 330，和在步骤 S348 中生成写入已验证设备的唯一 ID 和公开密钥的验证列表。这里，可验证设备的数量可以由用户随意限制。

在生成验证列表之后，服务器 320 在步骤 S350 中利用验证列表中的设备信息和服务器 320 生成的随机数生成唯一域 ID 和唯一域密钥。此时，每当包括在域中的成员设备发生改变时，改变作为只由包括在用户构建的域中的设备共享的秘密密钥的域密钥，和域 ID 用作将域标识成与其它域区分开的标识符。

服务器 320 在步骤 S352 中利用设备 330 的公开密钥加密域 ID 和域密钥，并将加密域 ID 和域密钥发送到已验证设备 330。设备 330 在步骤 S354 中利用它们自己的秘密密钥解密域密钥。然后，构建使用内容的域。当已构建起

使用内容的域时，服务器 320 利用内容密钥加密内容和利用域密钥加密内容密钥。打算使用内容的设备可以通过用域密钥解密加密内容来使用内容。

图 4 是例示采用根据本发明一个实施例构建域的方法的 UPnP 的方块图。

受控设备（CD）110－160 接收来自控制点（CP）190 的命令和向控制点（CP）190 提供服务。通过将受控设备 110－160 的一个设备 110 设置成主设备和将用户选择的设备 120－140 设置成从设备可以构建起一个域。

受控设备 110－160 当中未设置成主设备或从设备的设备 150 和 160 被叫做客设备。主设备 110 和从设备 120－140 形成已验证本地域 100，而 CP 190 和所有受控设备 110－160 形成本地网络 200。

图 5 例示了在控制点和受控设备 120－160 之间进行的典型 UPnP 操作。首先，执行寻址过程。UPnP 网络的基础设施是 TCP/IP 协议，和协议的关键功能是寻址功能。每个设备必须是动态主机配置协议（DHCP）客户机，和当一个设备最初与 UPnP 连接时，该设备搜索 DHCP 服务器。如果找到 DHCP 服务器，则该设备使用分配的 IP 地址。如果未找到 DHCP 服务器，则该设备使用自动 IP（auto IP）来保证地址。

接着，执行发现过程。如果设备与网络连接和得到适当寻址，可以执行搜索操作。搜索操作是利用简单服务发现协议（SSDP）进行的。如果其它设备加入网络中，利用 SSDP 将这些设备提供的服务发送到网络中的控制点。

此后，执行描述过程。即使已经将设备提供的服务通知控制点，控制点仍然没有多少有关设备的信息。为了使控制点利用设备的信息和设备的功能与每个设备交互，控制点必须从每个设备提供的搜索消息和统一资源定位符（URL）中确认每个设备的描述。每个设备的 UPnP 描述用可扩充标记语言（XML）表示，和包括唯一制造信息（型号名、序号、制造者名称、制造者 URL 等）。除了用于控制、事件处理和展示的 URL 之外，该描述还包括多个内置设备和服务列表

最后，执行 UPnP 操作过程。UPnP 操作过程通过控制、事件处理和演示操作来进行。在控制操作中，控制点保证每个设备的描述，然后进行与设备控制有关的基本操作。为了控制设备，控制点将服务操作命令发送到设备。也就是说，为了相应服务，控制点将适当控制消息发送到控制 URL（描述在设备手册中）。控制消息也利用简单对象访问协议（SOAP）用 XML 表示。相应服务是相对于控制消息的响应和提供特定操作值或错误码。

在事件处理中，每个设备都接收命令，如果设备的状态发生改变，该设备利用事件消息将状态变化通知控制点。事件消息包括至少一个状态变量名和变量的当前值。此外，事件消息也用 XML 表示和利用通用事件通知结构（GENA）格式化。事件的细节被定期更新和不断地通知控制点。此外，可以利用 GENA 取消加入。

在展示操作中，如果设备拥有用于展示的 URL，控制点可以通过 URL 搜索网页和将网页装载到浏览器上，用户可以利用网页控制设备或查询设备的状态。功能执行得好不好取决于设备的展示网页和特定功能。

图 6 例示了在构建 UPnP 基础设施的本地网络的过程中确定主设备的过程。

参照图 6，首先，所有受控设备 110－160 在步骤 S601 中利用 SSDP 将它们已与本地网络连接通知控制点 190。控制点 190 在步骤 S602 中利用超文本传输协议（HTTP）接收来自设备 110－160 的设备信息和数字权限管理（DRM）信息。设备信息包括用在 UPnP 中的典型设备信息，和 DRM 信息包括设备属性和设备模式。这里，作为确定受控设备是否可以是主设备的值的设备属性是告知受控设备是否可以起域主设备作用的信息。设备模式是确定受控设备当前起主设备，从设备、还是客设备作用的值。最初，所有受控设备都被设置成客设备，此后，如果受控设备被设置成主设备或从设备，改变受控设备的设备模式。

控制点 190 确定 DRM 信息的设备模式是主状态的受控设备是否存在，如果起主设备作用的受控设备不存在，则控制点 190 在步骤 S603 中选择可以成为主设备的受控设备之一作为主设备。主设备选择由用户利用控制点 190 的用户界面完成。用户界面的例子显示在图 9A 中。在用户界面中，显示了非主设备‘main nexus’和‘sub nexus’，它们当前被设置成客设备。用户可以从设备当中选择用户打算设置成主设备的设备。在本实施例中，第 1 受控设备被设置成主设备。

控制点 190 在步骤 S604 中利用 SOAP 从设置成主设备的第 1 受控设备 110 接收管理者验证信息。管理者验证信息可以从例如主设备的智能卡中获得。此外，管理者验证信息对于确认已经确定主设备的用户是管理者的过程是必不可少的。控制点 190 在步骤 S605 中通过由用户利用管理者验证信息输出用户界面和输入管理者 ID 和口令进行管理者验证。用户界面的例子显示在图

9B 中。

控制点 190 在步骤 S606 中将第 1 受控设备 110 设置成主设备和将存储在控制点 190 中的设备列表发送到第 1 受控设备 110。然后，第 1 受控设备 110 的设备模式变成主状态。设置成主设备的第 1 受控设备 110 在步骤 S607 中生成最初只有自身设备是成员设备的域。

图 7 是例示与如图 6 所示的确定主设备的过程平行的设备验证过程的流程图。

参照图 7，首先，域主设备 110 在步骤 S711 中通过如图 3 所示的方法接收来自外部服务器的新 SIB。于是，控制点 190 在步骤 S712 中利用 SOAP 将存储 SIB 的 URL 的信息发送到其它受控设备 120－160。其它受控设备 120－160 在步骤 S713 中利用 HTTP 接收存储在 URL 中的 SIB。其它受控设备 120－160 的每一个在步骤 S714 中利用 SIB 提取秘密值，并利用秘密值、个人设备 ID 和个人公开密钥生成证书。证书用于将设备与非法设备区分开。例如，如果坚持只有特定制造者生产的设备才被接纳为合法设备的验证政策，由其它制造者生产的设备将被当作非法设备对待。

接着，当控制点 190 在步骤 S715 中利用 SOAP 将存储证书的 URL 的信息发送到主设备 110 时，主设备 110 在步骤 S716 中利用 HTTP 从其它受控设备 120－160 接收证书、设备 ID 和公开密钥。此外，控制点 190 在步骤 S717 中核实接收的证书和生成已验证设备的列表。将作为证书验证的结果当作非法设备对待的设备排除在域之外，不可能将这些设备指定成从设备。

图 8 是例示与如图 7 所示的设备验证过程平行的确定从设备的过程的流程图。

参照图 8，首先，控制点 190 在步骤 S821 中利用 SOAP 核实作为验证核实的结果验证为合法设备的设备 120－140 的域属性。域属性包括域密钥、域中的设备名称和域中的设备数量。如果在设备中不存在域属性，控制点 190 在步骤 S822 中利用用户界面显示设备的列表，和在步骤 S823 中允许用户利用用户界面选择从设备。显示合法设备 120－140 的列表的用户界面的例子显示在图 9C 中。用户可以通过检验要包含在域中的设备选择从设备。用户可以选择与选择主设备的情形不同的多个从设备。控制点 190 在步骤 S824 中接收来自主设备的管理者验证信息，和像如图 6 所示的方法那样在步骤 S825 中进行管理者验证。

接着，控制点 190 在步骤 S826 中利用 SOAP 将所选从设备的列表发送到主设备 110，和在步骤 S827 中将所选设备的设备模式设置成从状态。主设备 110 在步骤 S828 中利用从设备生成域 ID 和域密钥。主设备 110 在步骤 S829 中利用从设备的公开密钥加密域 ID 和域密钥。此外，主设备 110 存储选为从设备的设备的从设备列表。

最后，控制点 190 在步骤 S830 中利用 SOAP 将存储域属性的主设备 110 的 URL 信息发送到选为从设备的设备。然后，选为从设备的设备在步骤 S831 中利用 HTTP 接收来自 URL 的域属性。如上所述，域属性包括域密钥、域中的设备名称和域中的设备数量的信息。

图 10－12 与图 6－8 不同，是例示将控制点 190 的重要功能移到主设备 110 中时的操作过程的流程图。这里，控制点 190 的功能只局限于管理与用户界面有关的操作。也就是说，主设备 110 除了作为受控设备的功能之外，还包括除了控制点 190 的限制功能之外其它作为控制点的功能。于是，控制点 190 执行的操作减少了，即使控制点 190 是非法设备，也不会出现安全问题。此外，即使在主设备 110 中没有用户界面，也不存在操作问题。

图 10 是例示根据本发明一个示范性实施例确定主设备的另一个过程的流程图。由于第 1 受控设备 110 在该过程中只起受控设备的作用，如图 10 所示的过程与如图 6 所示的过程相同。

图 11 是例示与如图 10 所示的确定主设备过程平行的设备验证过程的流程图。

参照图 11，首先，控制点 190 在步骤 S1101 中利用 SOAP 通知主设备 110 设备验证过程已开始。在步骤 S1101 中，主设备 110 作为 CD 运行。然后，主设备 110（作为 CP 运行）在步骤 S1102 中利用 SOAP 直接将 SIB 发送到其它受控设备 120－160。其它受控设备 120－160 的每一个在步骤 S1103 中利用 SIB 提取秘密值，和利用秘密值、个人设备 ID 和个人公开密钥生成证书。

接着，其它受控设备 120－160 在步骤 S1104 中利用 SOAP 直接将证书、设备 ID 和公开密钥发送到主设备 110。然后，主设备 110 在步骤 S1105 中核实接收的证书和生成受控设备的验证列表。将作为证书验证的结果当作非法设备对待的设备排除在域之外，不可能将这些设备指定成从设备。主设备 110（作为 CD 运行）在步骤 S1106 中利用 GENA 用事件消息将核实设备的 ID 通知控制点 190。控制点 190 在步骤 S1107 中利用 SOAP 从主设备 110（作为 CD 运

行）接收设备的核实结果，然后，在步骤 S1108 中利用用户界面显示核实设备是否是非法的。

图 12 是例示与如图 11 所示的设备验证过程平行的确定从设备的过程的流程图。

参照图 12，首先，控制点 190 在步骤 S1201 中利用 SOAP 核实作为验证核实的结果验证为合法设备的设备 120－140 的域属性。如果在设备中不存在域属性，控制点 190 在步骤 S1202 中利用用户界面显示设备的列表，并在步骤 S1203 中允许用户利用用户界面选择从设备。显示合法设备的列表的用户界面的例子显示在图 9C 中。用户可以通过检验要包含在域中的设备选择从设备。控制点 190 在步骤 S1204 中接收来自主设备 110 的管理者验证信息，和像如图 6 所示的方法那样在步骤 S1205 中进行管理者验证。

接着，控制点 190 在步骤 S1206 中利用 SOAP 将所选从设备 120－140 的列表发送到主设备 110（作为 CD 运行）。主设备 110 在步骤 S1207 中生成域 ID 和域密钥。这里，域 ID 用于将自身域与其它域区分开，如果域 ID 对于该域是唯一的，不执行生成方法。因此，域 ID 可以是随机数发生器生成的随机数，或合并从设备的设备 ID 和某个随机数的值的散列值。也就是说，通过使生成方法局限于特定方法不生成域 ID。同样，域密钥可以是随机数发生器生成的随机数，或合并从设备的设备 ID 和某个随机数的值的散列值。但是，由于域密钥随域的成员设备的状态改变而改变，最好利用从设备的设备 ID 生成域密钥。

当生成域 ID 和域密钥时，主设备 110 在步骤 S1208 中利用从设备的公开密钥加密域 ID 和域密钥。主设备 110（作为 CP 运行）在步骤 S1209 中直接将所选设备的设备模式设置成从状态和将设置设备的域属性发送到设置设备。此外，主设备 110 存储选为从设备的设备的从设备列表。

图 13 是例示根据本发明一个实施例的在当前验证域中已经是客设备的受控设备 150 和 160 作为从设备加入时的过程的流程图。图 13 例示了将控制点的重要功能移到主设备中和控制点只主要执行用户界面功能的情况。

为了加入从设备，如果用户利用控制点 190 提供的用户界面选择从设备加入菜单，控制点 190 在步骤 S1301 中利用 SOAP 核实作为验证核实的结果验证为合法设备的设备 120－160 的域属性。如果设备 120－160 当中的设备 150 和 160 没有域属性，控制点 190 在步骤 S1302 中利用用户界面显示设备 150

和 160 的列表，和在步骤 S1303 中允许用户利用用户界面选择从设备。用户可以在如图 9C 所示的用户界面屏幕上，在合法验证设备当中通过检验客设备选择从设备。控制点 190 在步骤 S1304 中接收来自主设备 110 的管理者验证信息，和像如图 6 所示的方法那样在步骤 S1305 中进行管理者验证。

控制点 190 在步骤 S1306 中利用 SOAP 将所选从设备 150 和 160 的列表发送到主设备 110。主设备 110 在步骤 S1307 中利用以前选为从设备的设备 120－140 的列表和新选为从设备的设备 150 和 160 的设备信息（例如，设备 ID）生成新域密钥。也就是说，由于域密钥是域的成员设备必须共享的秘密密钥，最好利用域的成员设备的信息生成域密钥。因此，根据域的成员设备的状态变化生成新域密钥。这里，由于域 ID 是将自身域与其它域区分开的标识符，只要主设备 110 不改变，域 ID 就不改变。主设备 110 在步骤 S1308 中利用从设备的公开密钥加密新域密钥。主设备 110 在步骤 S1309 中直接将所选设备的设备模式设置成从状态，并将包括新域密钥的新域属性发送到从设备。

上面已经描述了新从设备加入已验证域中的过程，同样，用户可以利用用户界面屏幕从已验证域中移去设置成从设备的设备。主设备 110 也从主设备 110 的从设备列表中删除移去从设备，和以与如图 13 所示相似的方式利用移去从设备的信息生成新域密钥。

诸如加入或移去之类的术语用在通过控制点经用户许可地在主设备中通过改变从设备列表改变域的配置的时候。也就是说，加入和移去分别指的是像通过控制点未经用户许可地在物理上将从设备加入控制点中的情况或打开从设备的情况那样，将从设备与域连接的状况，和像通过控制点未经用户许可地在物理上从控制点中取消从设备的情况或关闭从设备的情况那样，将从设备与域断开的状况。

同时，当从域中移去已验证域的从设备（例如，120－140）当中的从设备 120，和其它客设备（例如，150 和 160）当中的客设备 150 作为从设备加入域中时，通过如图 13 所示的过程生成新域密钥。如果移去的从设备 120 重新加入已验证域中，通过反映从设备 120 的设备信息生成新域密钥。从设备的加入或移去由用户决定，不会频繁发生。但是，例如，在从设备是家用电器的情况下，会频繁发生打开/关闭（即，连接/断开）它们的状况。在这种情况下，域密钥被频繁地改变，这会使用户感到烦恼，另外，会加重系统负担。

因此，在本发明中，当连接/断开从设备时，将会话 ID 用作区分从设备的加入/移去的标识符。会话 ID 随从设备的加入/移去而改变，而不是随从设备的连接/断开而改变，和由主设备和从设备共享。此外，可以随机地或利用域的成员设备的信息生成会话 ID，最好利用从设备的公开密钥加密会话 ID 和将会话 ID 发送到从设备。会话 ID 可以包括唯一 ID、日期信息和版本信息。

同时，必须根据从设备与域连接还是断开的状况考虑几个项目。

如图 14 所示，在自从从设备 S1 与控制点 CP 断开以来经过了预定时间之后从设备 S1 重新与控制点 CP 连接的情况下，当连接或断开从设备 S1 时，不改变主设备 M 和从设备 S1、S2 和 S3 共享的会话 ID 和域密钥。因此，从设备 S1 可以在断开之前用域密钥使用内容。

但是，如图 15 所示，在当从设备 S1 与控制点 CP 断开时另一个从设备 S4 加入域中的情况下，改变主设备 M 和从设备 S1、S2、S3 和 S4 共享的会话 ID 和域密钥。因此，在从设备 S1 重新与控制点 CP 连接的情况下，从设备 S1 不能顺利地使用或再现在域中共享的内容。于是，主设备 M 将主设备 M 的会话 ID 与与域新连接的设备的会话 ID 相比较，如果两个会话 ID 不相同，主设备 M 将从设备 S4 加入域中时新生成的域密钥 DK2 发送到从设备 S1。此外，由于在当从设备 S1 断开时移去从设备 S2 的情况下，主设备 M 的会话 ID 和域密钥也发生改变，所以要执行如图 15 所示的过程。控制点（CP）感测要连接的预定设备，将相连设备的会话 ID 发送到主设备 M，并将主设备的信息发送到域的成员设备。

当连接或断开从设备时，不改变存储在主设备 M 中的从设备，直到用户通过控制点（CP）改变从设备列表。因此，如果用户在从设备 S1 已经断开时从从设备列表中删除从设备 S1，从设备 S1 丧失作为从设备的资格。但是，由于断开从设备的设备模式仍然被设置成从状态，如果重新连接从设备 S1，主设备 M 除了检查会话 ID 之外，必须检查从设备 S1 是否存在于从设备列表之中，并将不存在于从设备列表之中的设备的设备模式改变成客状态。否则，由于实际处在客状态的从设备 S1 未经用户许可地共享新域密钥，使整个系统的结构崩溃。

图 16 是例示根据本发明一个实施例管理与域新连接的设备的过程的流程图。

参照图 16，当控制点在步骤 S1601 中发现域中新连接的新设备时，在步

骤 S1603 中执行如图 7 所示的设备验证过程。如果验证失败，通过将相连设备当作非法设备终止该过程，如果验证成功，在步骤 S1605 中确定相连设备的设备模式是否是从状态。

如果相连设备的设备模式是客状态，终止该过程，如果相连设备的设备模式是从状态，在步骤 S1607 中确定相连设备的会话 ID 是否与主设备的会话 ID 相同。如果相连设备的会话 ID 与主设备的会话 ID 相同，由于域密钥也未改变，终止该过程。如果相连设备的会话 ID 与主设备的会话 ID 不相同，由于主设备的域密钥与相连设备的域密钥不相同，有必要将新域密钥发送到相连设备。但是，即使相连设备的会话 ID 与主设备的会话 ID 不相同，如果立刻将新域密钥发送到相连设备，设备模式实际上是客状态的设备也有可能被接纳为从设备。因此，在步骤 S1609 中必须确定相连设备是否存在于存储在主设备 M 中的从设备列表之中。

如果相连设备存在于从设备列表之中，由于认为相连设备将设备模式保持在从状态上，在步骤 S1611 中将新域密钥发送到相连设备，如果相连设备未存在于从设备列表之中，在步骤 S1613 中将相连设备的设备模式改变成客状态。通过执行如图 8 所示的过程，可以将设备模式改变成客状态的相连设备选为从设备。

如果采用从设备可以加入多个域中的多域政策，可以在通过在比较会话 ID 之前比较域 ID，对没有适当域 ID 的相连设备执行接着的步骤（S1605 到 S1611）之前终止该过程。此外，即使由于未采用多域政策，从设备只能拥有一个域 ID，也可以在对由于加入另一个域改变了域 ID 的设备执行接着的步骤（S1605 到 S1611）之前终止该过程。因此，对于上面两种情况，最好至少在步骤 S1607 之前将相连设备的域 ID 与当前域的域 ID 相比较。

如上所述，会话 ID 除了包括唯一 ID 之外，还可以包括日期信息和/或版本信息。如果使日期信息或版本信息包括在会话 ID 中，可以更清楚地区分旧会话 ID 和当前会话 ID。于是，可以利用信息提供多种服务。例如，当主设备断开时，控制点确认从设备的会话 ID 的日期信息和版本信息，如果域 ID 相同，但会话 ID 不同，可以知道，当从设备断开时，域的配置发生了改变。因此，即使主设备与域断开，也可以利用日期信息或版本信息和利用含有最近会话 ID 和域密钥改变其余从设备的会话 ID 和域密钥。

图 17 是根据本发明一个实施例的如图 4 所示的控制点 190 的方块图。

参照图 17，控制点 190 包括用户界面提供者 192，用于提供如图 9A－9C 所示的用户界面；设备操作信息提供者 194，用于将操作与控制点 190 连接的设备所需的信息提供给主设备和从设备；和设备检测器，用于检测与控制点 190 连接的设备。

用户界面提供者 192 将设备列表或设备验证结果显示在用户界面屏幕上。根据设备验证结果，用户可以选择主设备和从设备和改变从设备列表，还可以将非法设备列表存储在主设备中。设备操作信息提供者 194 像图 6－8 和 10－12 所示的那样将操作设备所需的信息发送到设备。设备检测器 196 感测与控制点 190 连接或断开的设备，并将相应设备的信息发送到设备操作信息提供者 194。设备操作信息提供者 194 将该信息发送到设备，然后，例如，可以执行如图 6 所示的过程。

图 18 是根据本发明一个实施例的如图 4 所示的主设备 110 的方块图。

参照图 18，主设备 110 包括受控设备管理器 113，用于对通过控制点 190 与主设备 110 连接的受控设备进行验证、设备模式确定和从设备列表管理；域 ID 管理器 115，用于生成域 ID 和检查域中相连设备的域 ID；会话 ID 管理器，用于生成会话 ID，改变会话 ID，和检查域中相连设备的会话 ID；和域密钥管理器 119，用于生成域密钥，改变域密钥，并将域密钥发送到从设备。

受控设备管理器 113 根据图 7 或 11 的流程图对域中相连的受控设备进行验证，和在图 16 的步骤 S1603 中确定受控设备的验证是否成功。此时，如果验证失败，受控设备管理器 113 可以将相连受控设备当作非法设备和将其名称分开存储在非法设备列表中。此外，受控设备管理器 113 在图 16 的步骤 S1605 中确定域中相连的受控设备的设备模式是从状态还是客状态。此时，如果设备模式不是处在从状态，受控设备管理器 113 输出错误信号，用户可以通过正常过程将相连受控设备登记成从设备，或根据错误信号移去相连受控设备。此外，受控设备管理器 113 可以通过控制点 190 根据用户命令生成和改变从设备列表，和在图 16 的步骤 S1609 中确定会话 ID 与主设备 110 的会话 ID 不相同的受控设备是否存在于从设备列表之中，如果受控设备不存在，受控设备管理器 113 控制受控设备，以便将受控设备的设备模式改变成客状态。

域 ID 管理器 115 生成域 ID 和将域 ID 发送到域的成员设备，如果新的受控设备与域连接，域 ID 管理器 115 至少在图 16 的步骤 S1607 之前，将主设

备 110 的域 ID 与域中相连的受控设备的域 ID 相比较，如果两个域 ID 不相同，域 ID 管理器 115 输出错误信号，和用户根据错误信号进行预定处理。

会话 ID 管理器 117 生成会话 ID，根据从设备列表的变化生成新会话 ID，和在图 16 的步骤 S1607 中将主设备 110 的会话 ID 与域中相连的受控设备的会话 ID 相比较，如果两个会话 ID 不相同，会话 ID 管理器 117 将主设备的会话 ID 发送到受控设备。

域密钥管理器 119 生成域密钥，根据域的配置的变化生成新域密钥，并将生成的域密钥发送到从设备。

虽然通过参照本发明的示范性实施例已经对本发明进行了具体图示和描述，但本领域的普通技术人员应该明白，可以在形式上和细节上对其作各种各样的改变，而不偏离所附权利要求书限定的本发明的精神和范围。应该认为这些示范性实施例是描述性的，而不是限制性的。因此，本发明的范围不是由本发明的详细描述限定，而是由所附权利要求书限定，在这个范围内的所有差异都应该理解为包括在本发明之中。

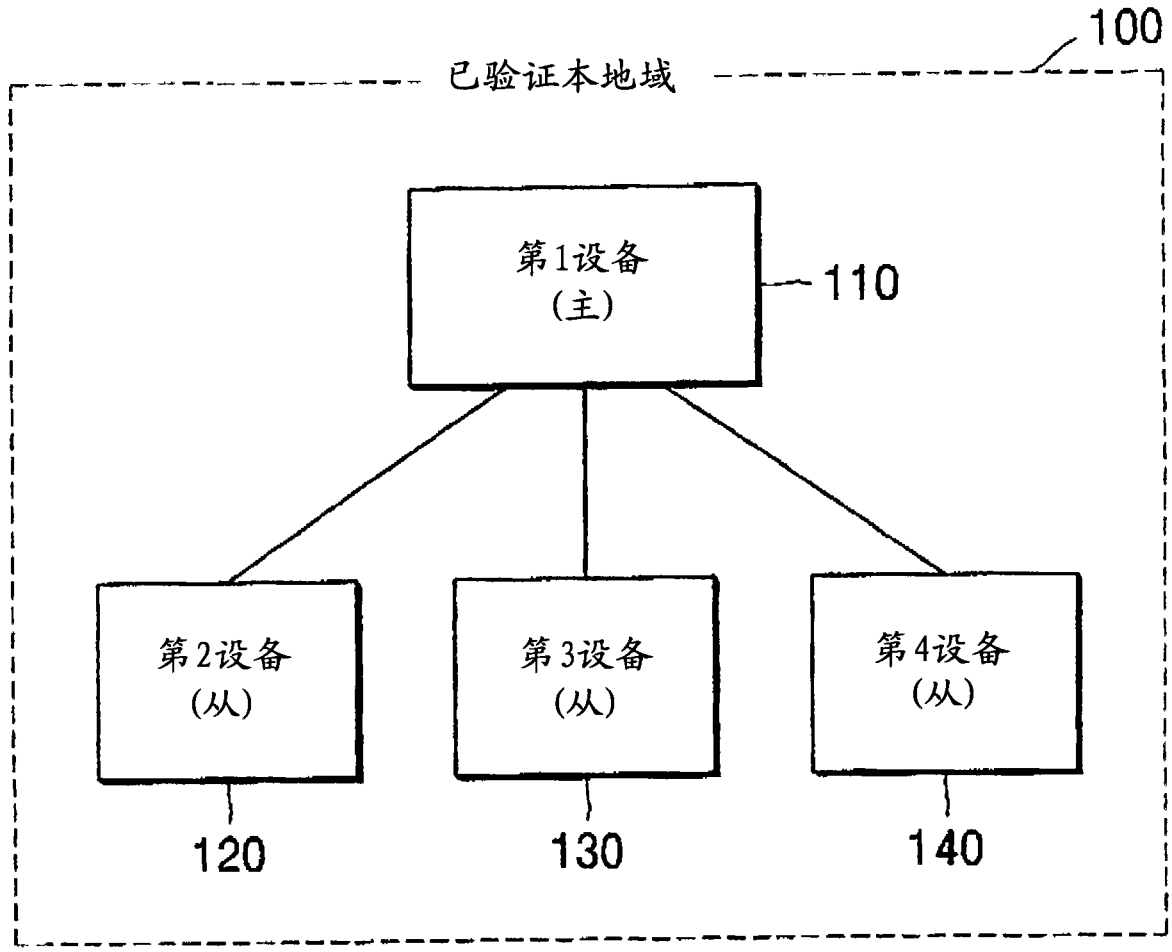


图 1

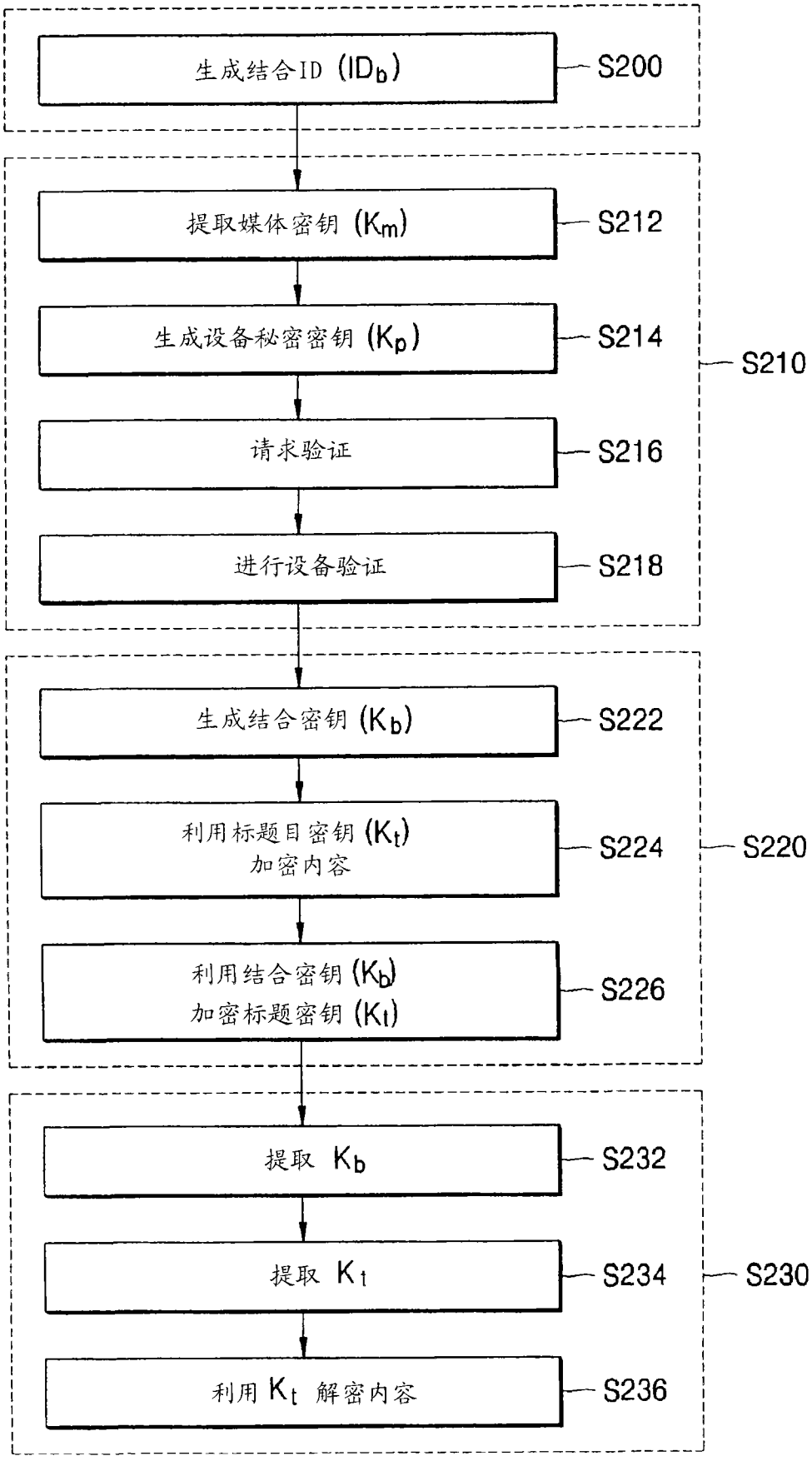

生成结合ID (ID_b)
S200
提取媒体密钥 (K_m)
S212
生成设备秘密密钥 (K_p)
S214
请求验证
S216
进行设备验证
S218
S210
生成结合密钥 (K_b)
S222
利用标题目密钥 (K_t)
加密内容
S224
利用结合密钥 (K_b)
加密标题密钥 (K_t)
S226
S220
提取 K_b
S232
提取 K_t
S234
利用 K_t 解密内容
S236
S230

图 2

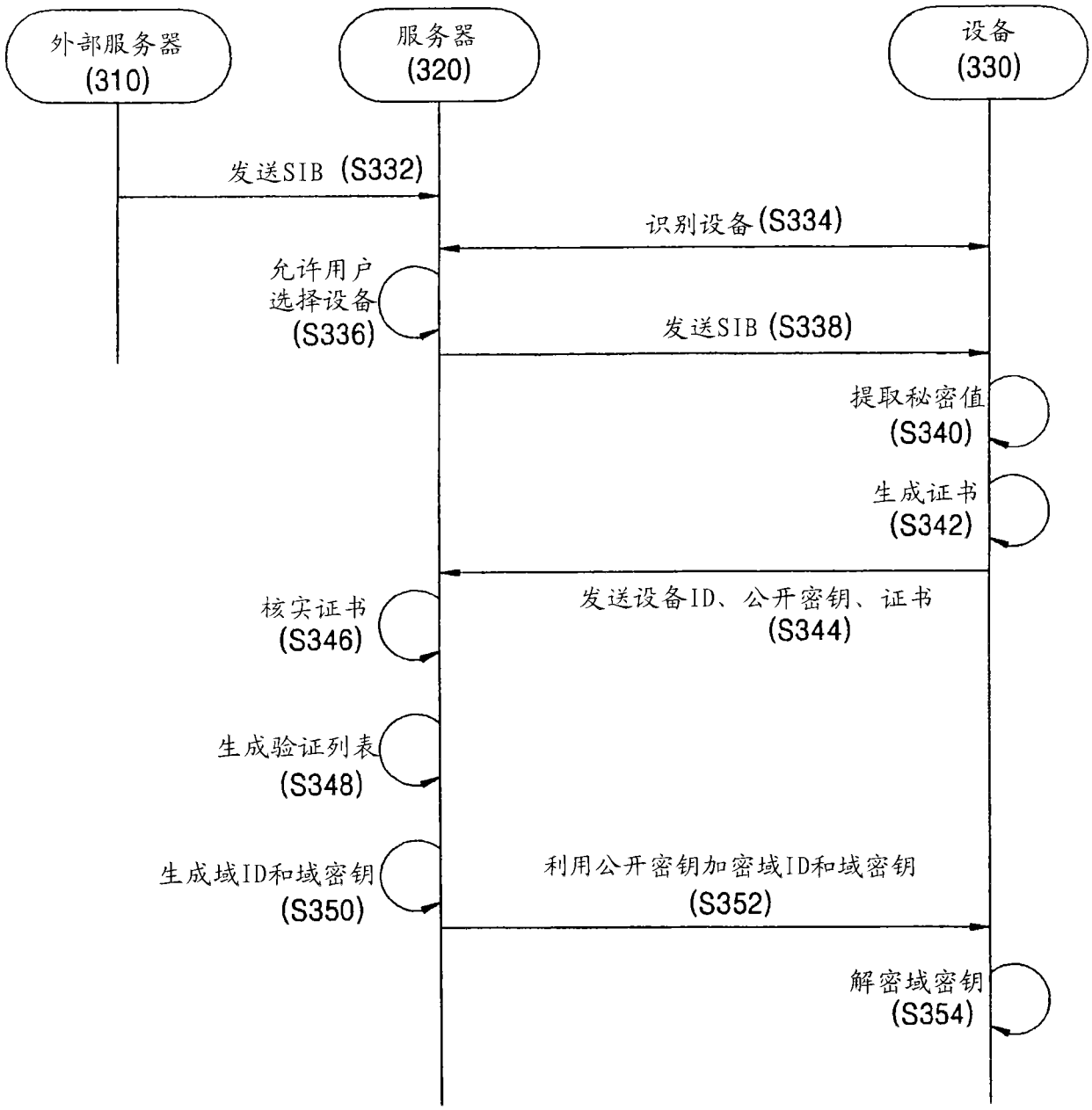

外部服务器
(310)
服务器
(320)
设备
(330)
发送SIB (S332)
识别设备(S334)
允许用户
选择设备
(S336)
发送SIB (S338)
提取秘密值
(S340)
生成证书
(S342)
发送设备ID、公开密钥、证书
(S344)
核实证书
(S346)
生成验证列表
(S348)
生成域ID和域密钥
(S350)
利用公开密钥加密域ID和域密钥
(S352)
解密域密钥
(S354)

图 3

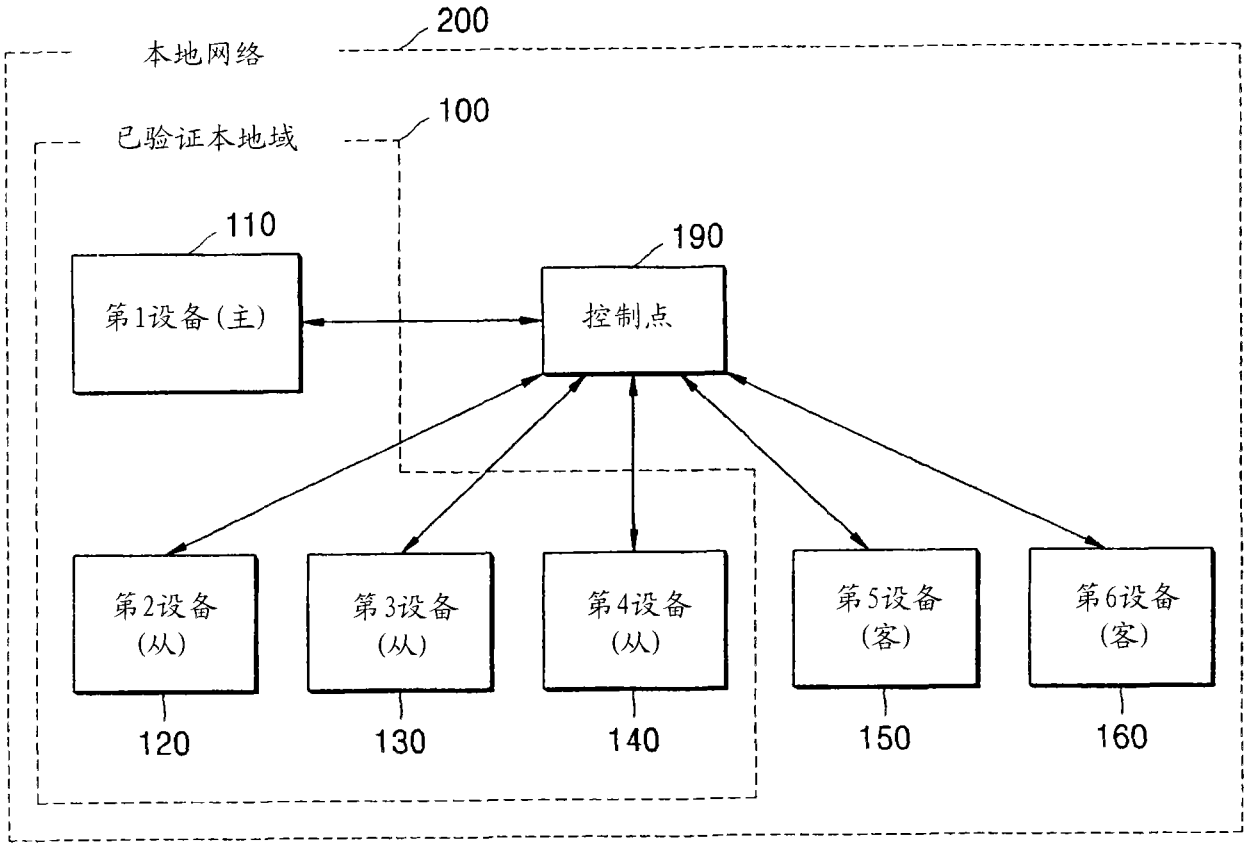

200
本地网络
100
已验证本地域
110
第1设备(主)
190
控制点
第2设备
(从)
第3设备
(从)
第4设备
(从)
第5设备
(客)
第6设备
(客)
120
130
140
150
160

图 4

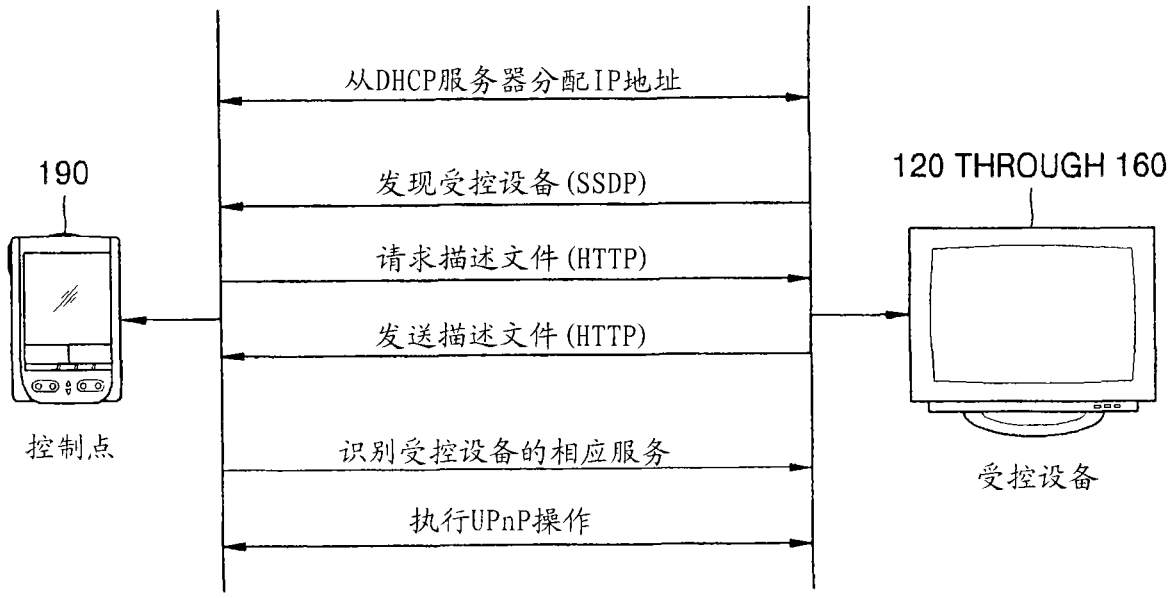

从DHCP服务器分配IP地址
190
发现受控设备(SSDP)
120 THROUGH 160
请求描述文件(HTTP)
发送描述文件(HTTP)
控制点
识别受控设备的相应服务
受控设备
执行UPnP操作

图 5

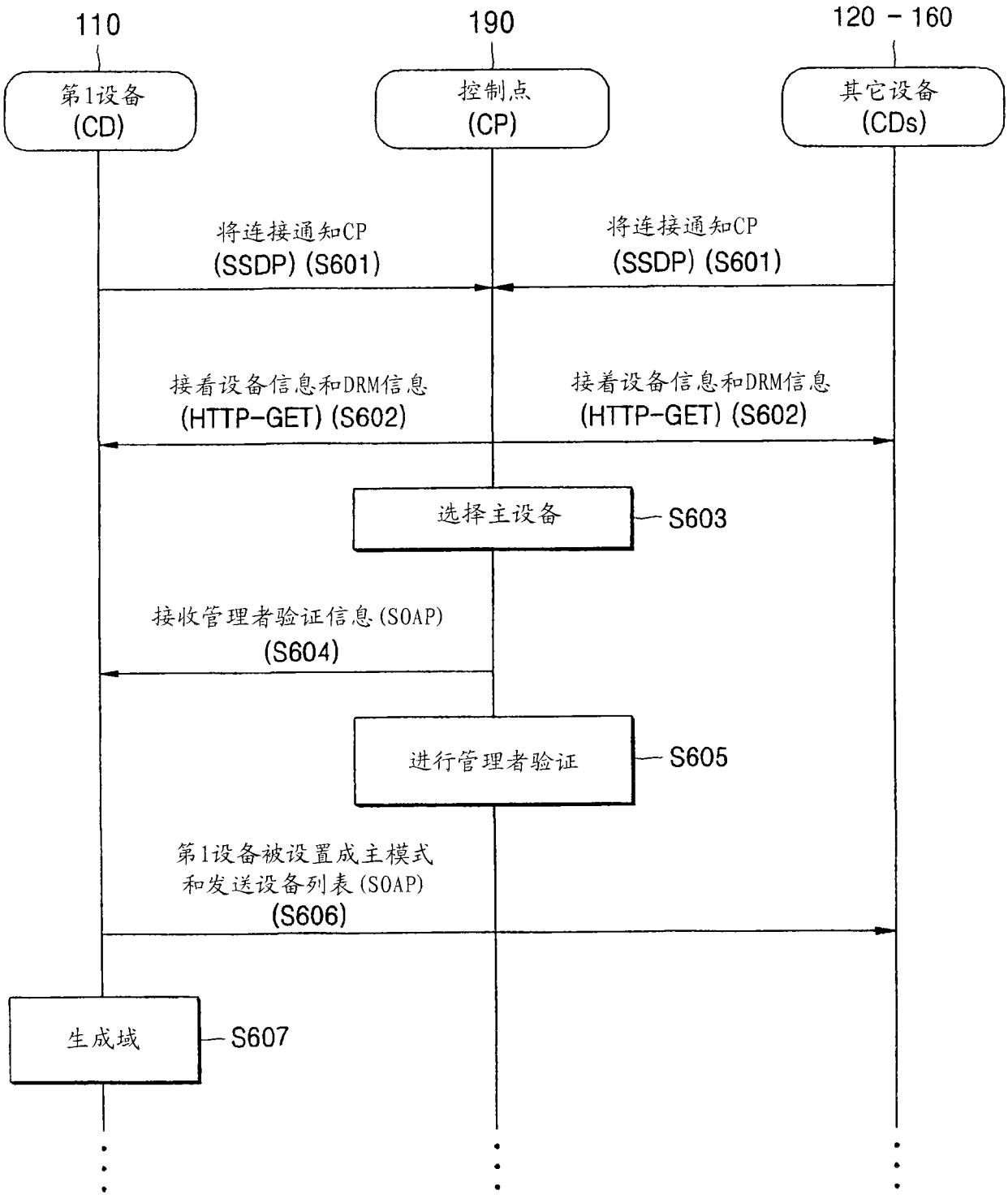

110
190
120 - 160
第1设备
(CD)
控制点
(CP)
其它设备
(CDs)
将连接通知CP
(SSDP) (S601)
将连接通知CP
(SSDP) (S601)
接着设备信息和DRM信息
(HTTP-GET) (S602)
接着设备信息和DRM信息
(HTTP-GET) (S602)
选择主设备
S603
接收管理者验证信息(SOAP)
(S604)
进行管理者验证
S605
第1设备被设置成主模式
和发送设备列表(SOAP)
(S606)
生成域
S607

图 6

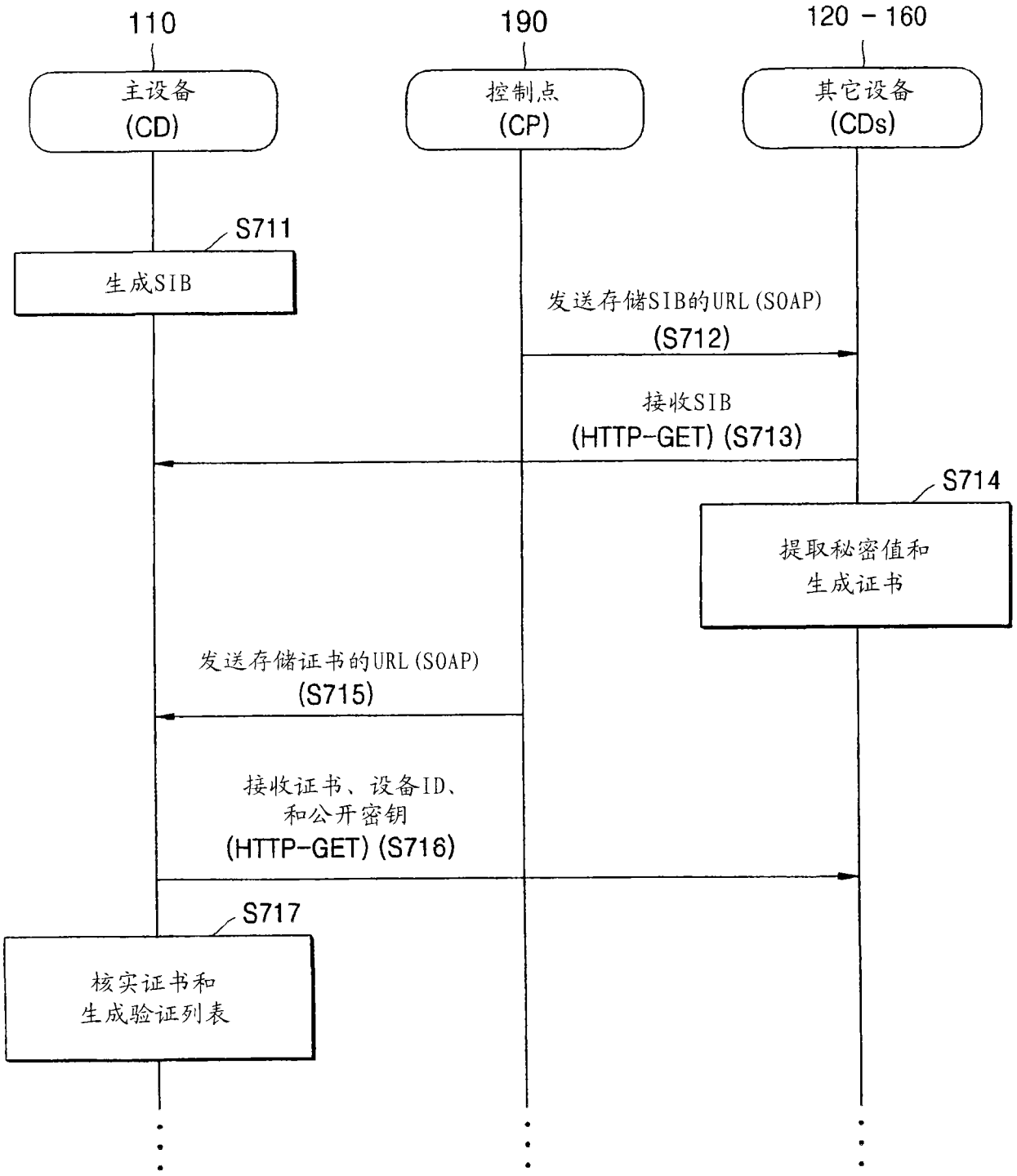

110
主设备
(CD)
190
控制点
(CP)
120 - 160
其它设备
(CDs)
S711
生成SIB
发送存储SIB的URL(SOAP)
(S712)
接收SIB
(HTTP-GET) (S713)
S714
提取秘密值和
生成证书
发送存储证书的URL(SOAP)
(S715)
接收证书、设备ID、
和公开密钥
(HTTP-GET) (S716)
S717
核实证书和
生成验证列表

图 7

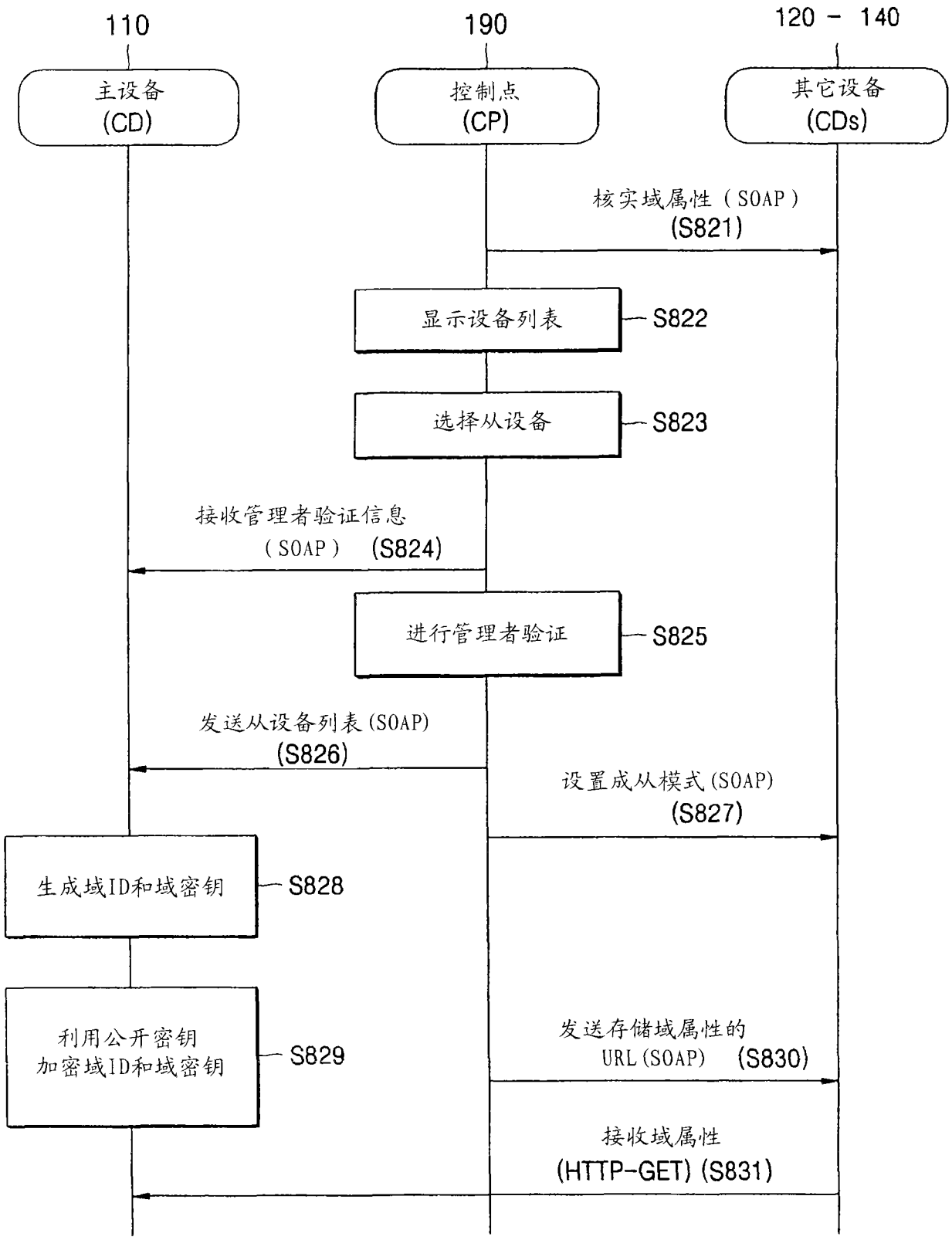

110
主设备
(CD)
190
控制点
(CP)
120 - 140
其它设备
(CDs)
核实域属性（SOAP）
(S821)
显示设备列表
S822
选择从设备
S823
接收管理者验证信息
（SOAP） (S824)
进行管理者验证
S825
发送从设备列表(SOAP)
(S826)
设置成从模式(SOAP)
(S827)
生成域ID和域密钥
S828
利用公开密钥
加密域ID和域密钥
S829
发送存储域属性的
URL(SOAP) (S830)
接收域属性
(HTTP-GET) (S831)

图 8

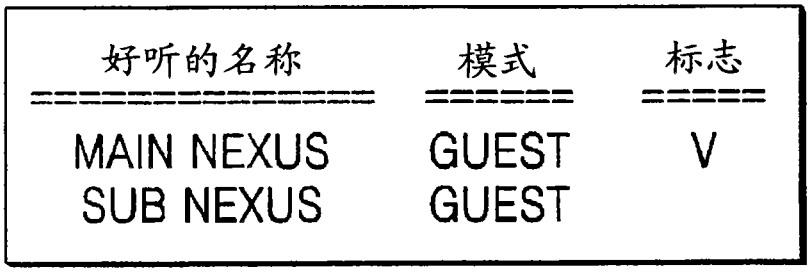

好听的名称
模式
标志
MAIN NEXUS
GUEST
V
SUB NEXUS
GUEST

图 9A


管理者验证
ID:0314620157
PASSWORD: ....

图 9B

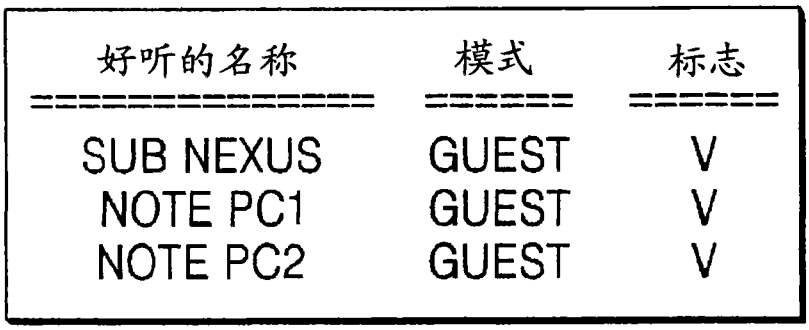

好听的名称
模式
标志
SUB NEXUS
GUEST
V
NOTE PC1
GUEST
V
NOTE PC2
GUEST
V

图 9C

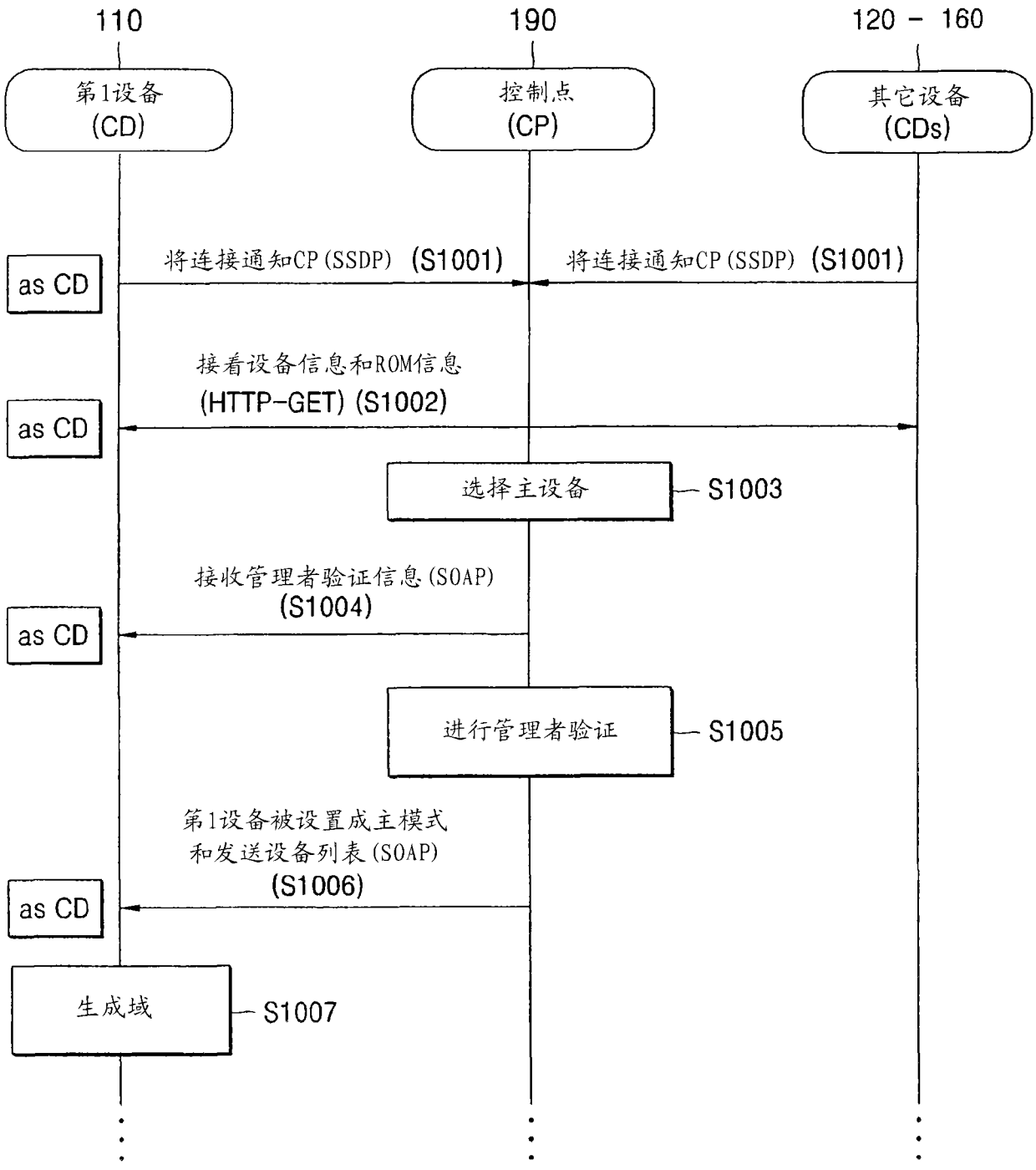

110
190
120 - 160
第1设备
(CD)
控制点
(CP)
其它设备
(CDs)
as CD
将连接通知CP(SSDP) (S1001)
将连接通知CP(SSDP) (S1001)
as CD
接看设备信息和ROM信息
(HTTP-GET) (S1002)
选择主设备
S1003
as CD
接收管理者验证信息(SOAP)
(S1004)
进行管理者验证
S1005
as CD
第1设备被设置成主模式
和发送设备列表(SOAP)
(S1006)
生成域
S1007

图 10

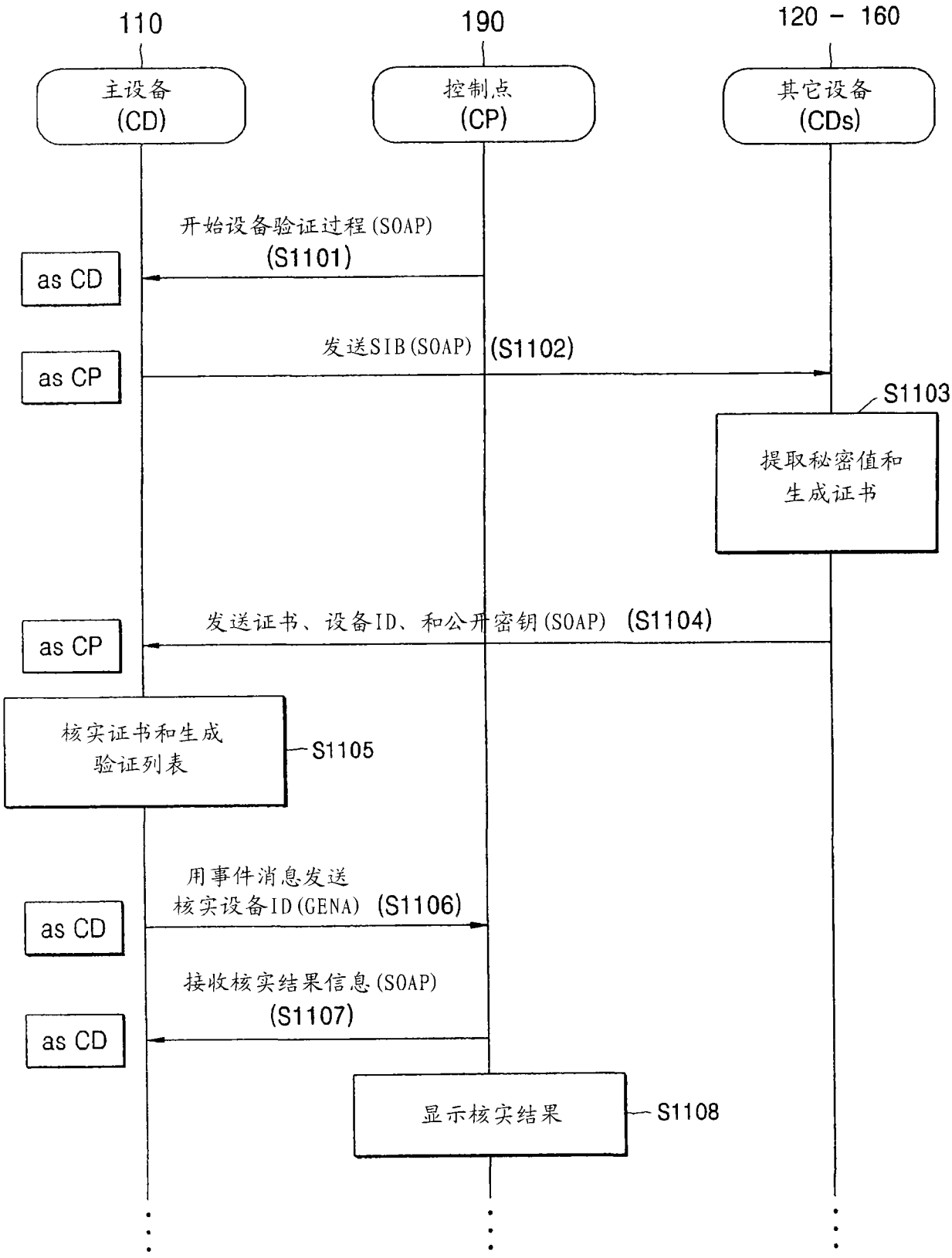

110
190
120 - 160
主设备
(CD)
控制点
(CP)
其它设备
(CDs)
开始设备验证过程(SOAP)
(S1101)
as CD
发送SIB(SOAP) (S1102)
as CP
S1103
提取秘密值和
生成证书
发送证书、设备ID、和公开密钥(SOAP) (S1104)
as CP
核实证书和生成
验证列表
S1105
用事件消息发送
核实设备ID(GENA) (S1106)
as CD
接收核实结果信息(SOAP)
(S1107)
as CD
显示核实结果
S1108

图 11

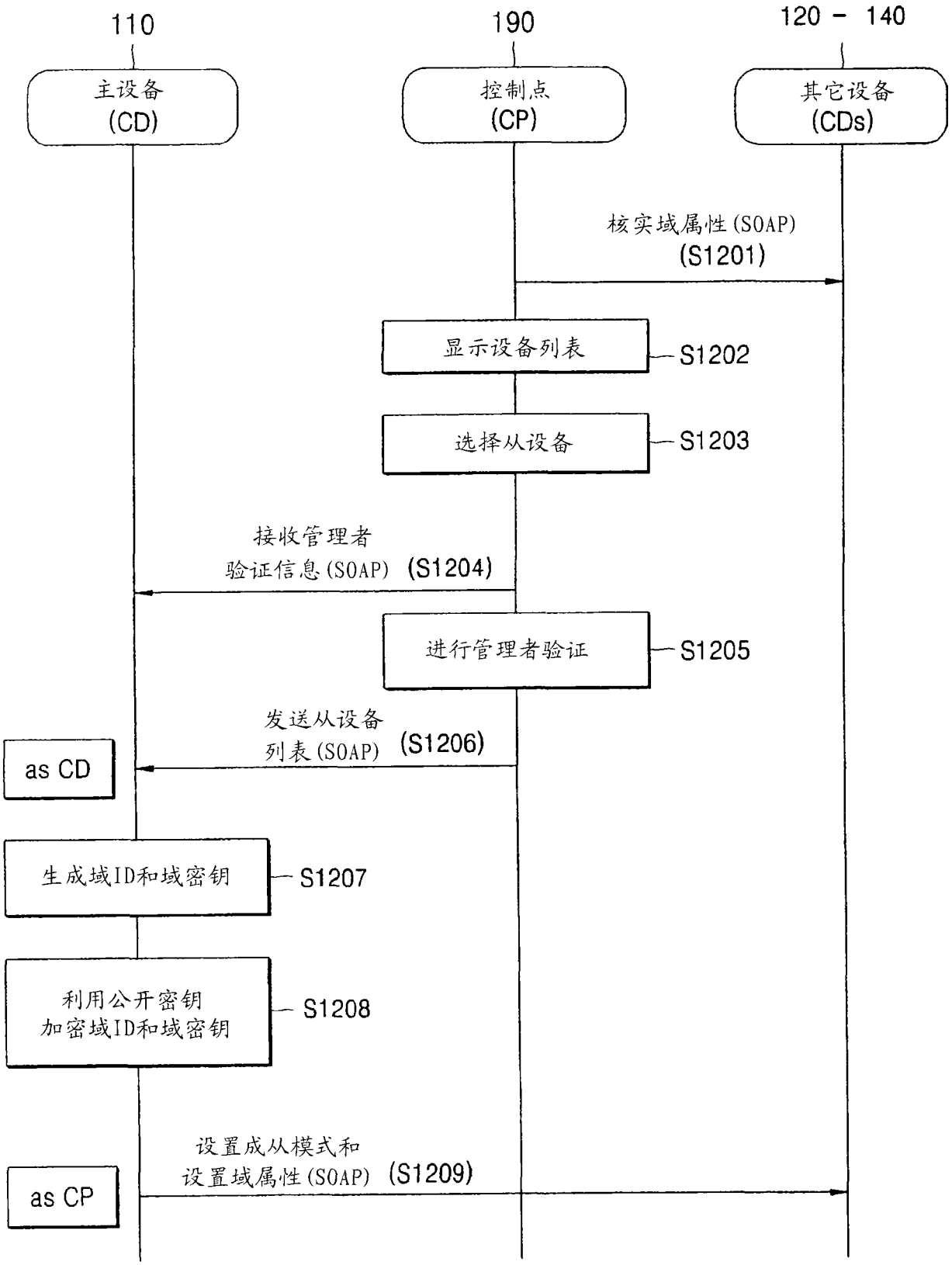

110
190
120 - 140
主设备
(CD)
控制点
(CP)
其它设备
(CDs)
核实域属性(SOAP)
(S1201)
显示设备列表
S1202
选择从设备
S1203
接收管理者
验证信息(SOAP) (S1204)
进行管理者验证
S1205
发送从设备
列表(SOAP) (S1206)
as CD
生成域ID和域密钥
S1207
利用公开密钥
加密域ID和域密钥
S1208
设置成从模式和
设置域属性(SOAP) (S1209)
as CP

图 12

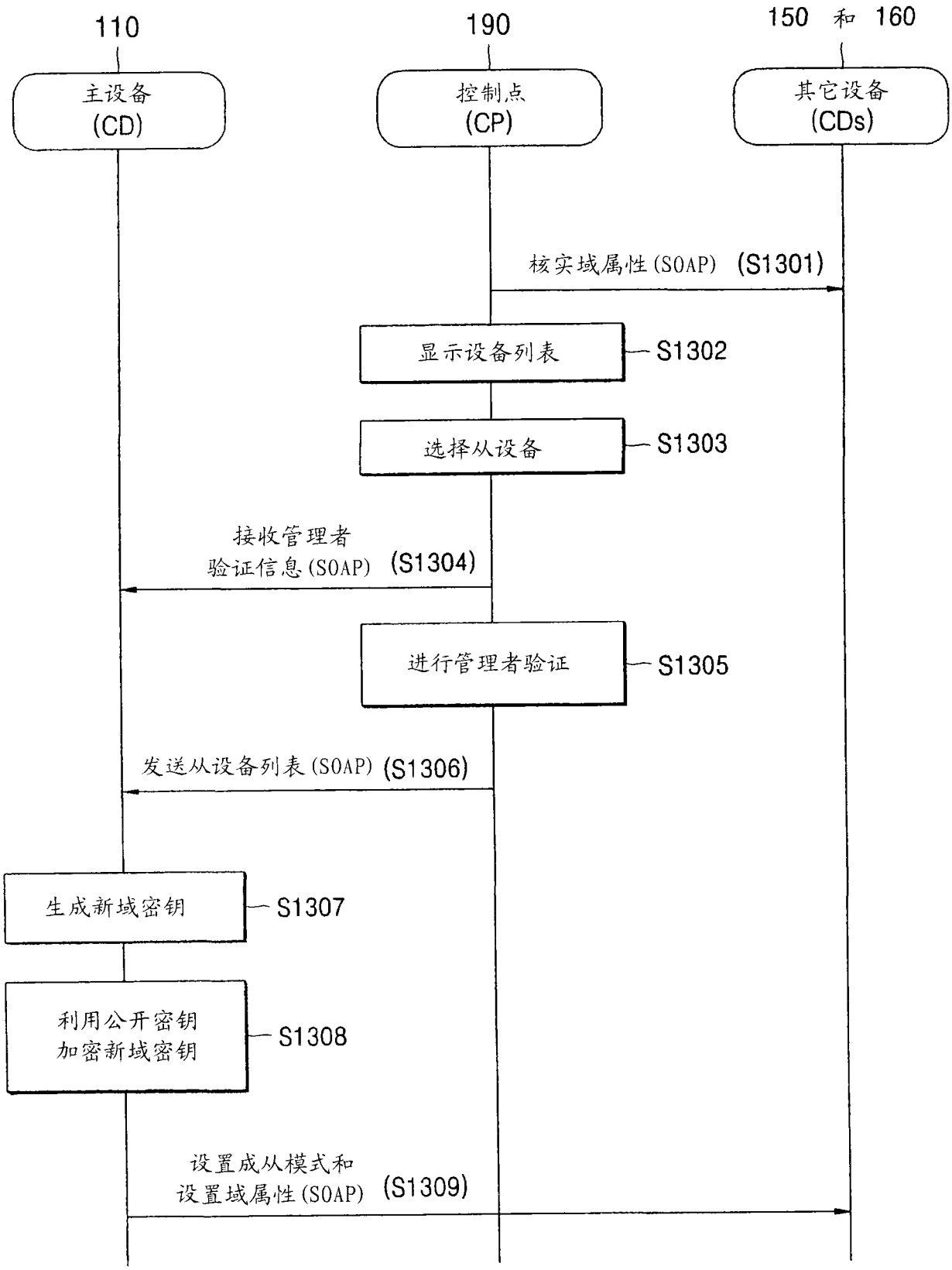

110
主设备
(CD)
190
控制点
(CP)
150 和 160
其它设备
(CDs)
核实域属性(SOAP) (S1301)
显示设备列表
S1302
选择从设备
S1303
接收管理者
验证信息(SOAP) (S1304)
进行管理者验证
S1305
发送从设备列表(SOAP) (S1306)
生成新域密钥
S1307
利用公开密钥
加密新域密钥
S1308
设置成从模式和
设置域属性(SOAP) (S1309)

图 13

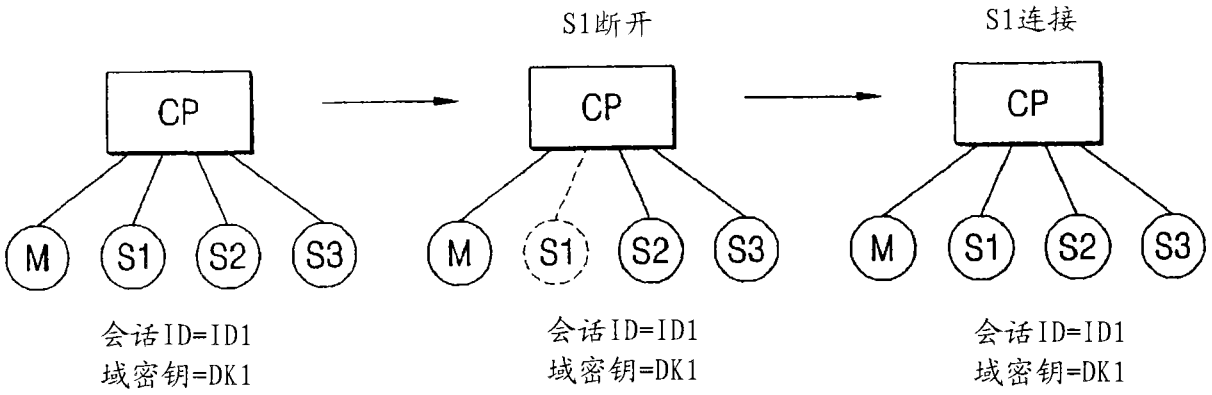

S1断开
S1连接
CP
CP
CP
M
S1
S2
S3
M
S1
S2
S3
M
S1
S2
S3
会话ID=ID1
域密钥=DK1
会话ID=ID1
域密钥=DK1
会话ID=ID1
域密钥=DK1

图 14

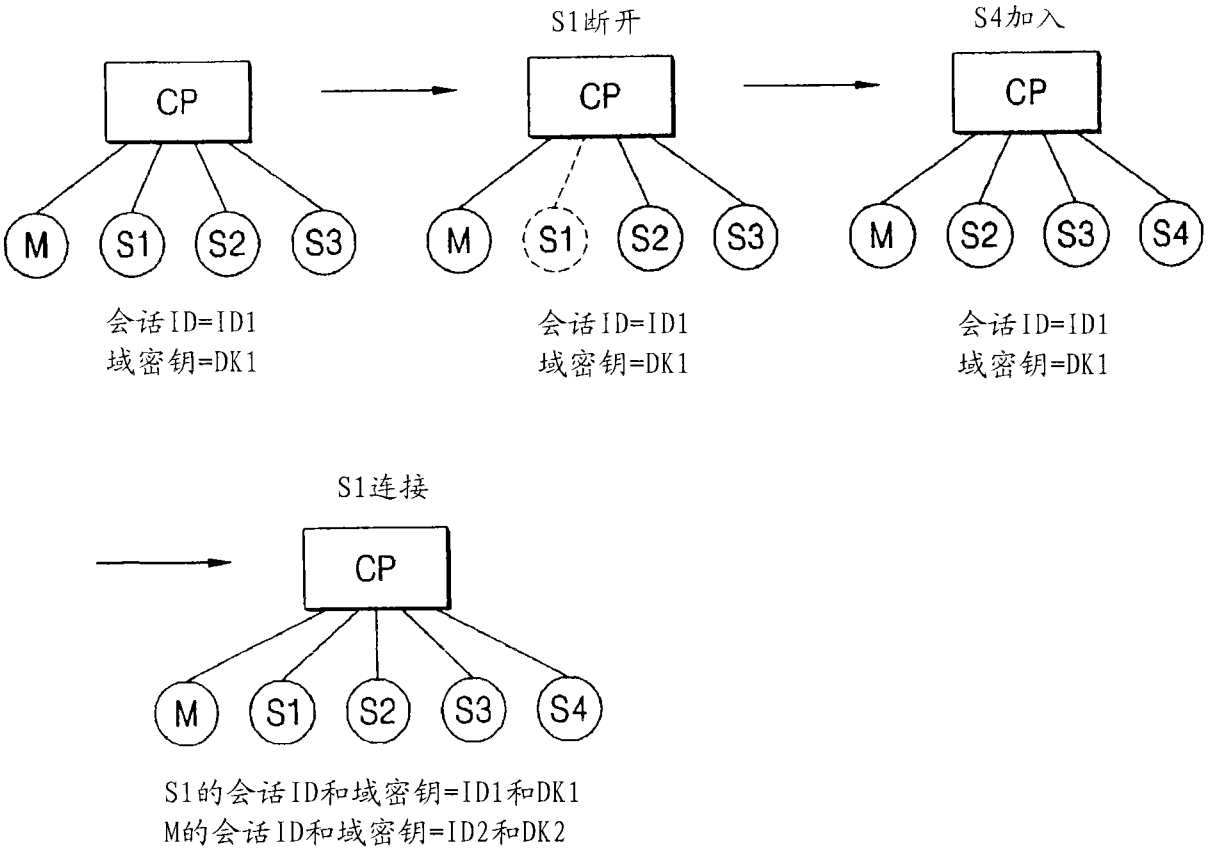

S1断开
S4加入
S1连接
CP
CP
CP
CP
M
S1
S2
S3
M
S1
S2
S3
M
S2
S3
S4
M
S1
S2
S3
S4
会话ID=ID1
域密钥=DK1
会话ID=ID1
域密钥=DK1
会话ID=ID1
域密钥=DK1
S1的会话ID和域密钥=ID1和DK1
M的会话ID和域密钥=ID2和DK2

图 15

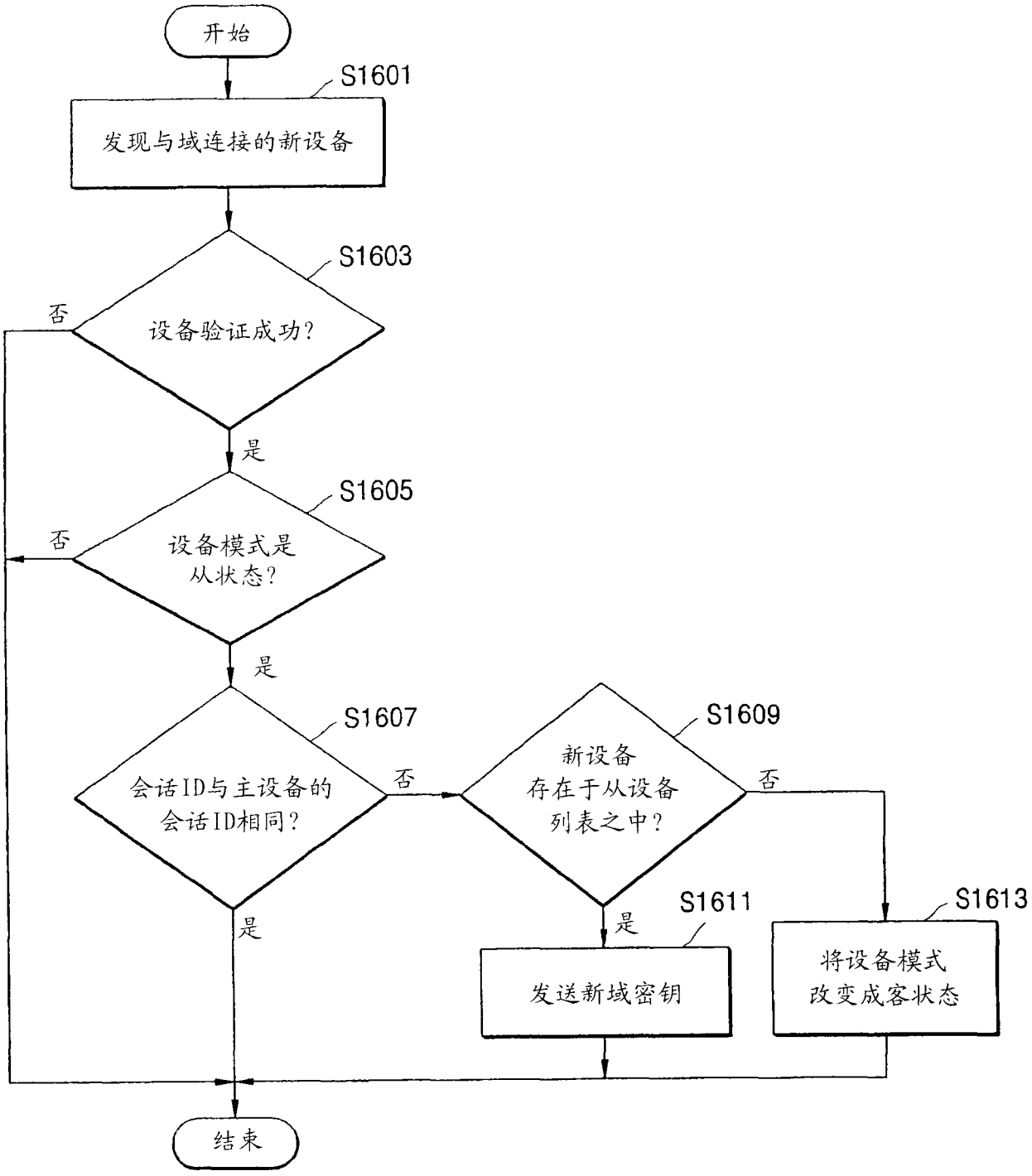

开始
S1601
发现与域连接的新设备
S1603
设备验证成功?
否
是
S1605
设备模式是
从状态?
否
是
S1607
会话ID与主设备的
会话ID相同?
否
是
S1609
新设备
存在于从设备
列表之中?
否
是
S1611
发送新域密钥
S1613
将设备模式
改变成客状态
结束

图 16

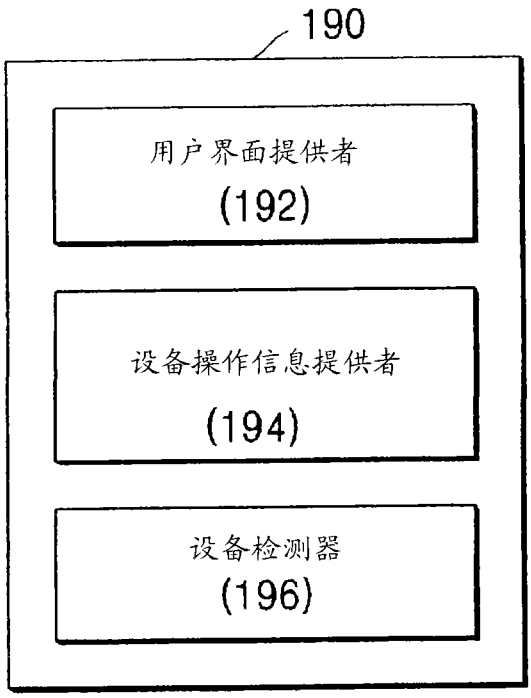

190
用户界面提供者
(192)
设备操作信息提供者
(194)
设备检测器
(196)

图 17

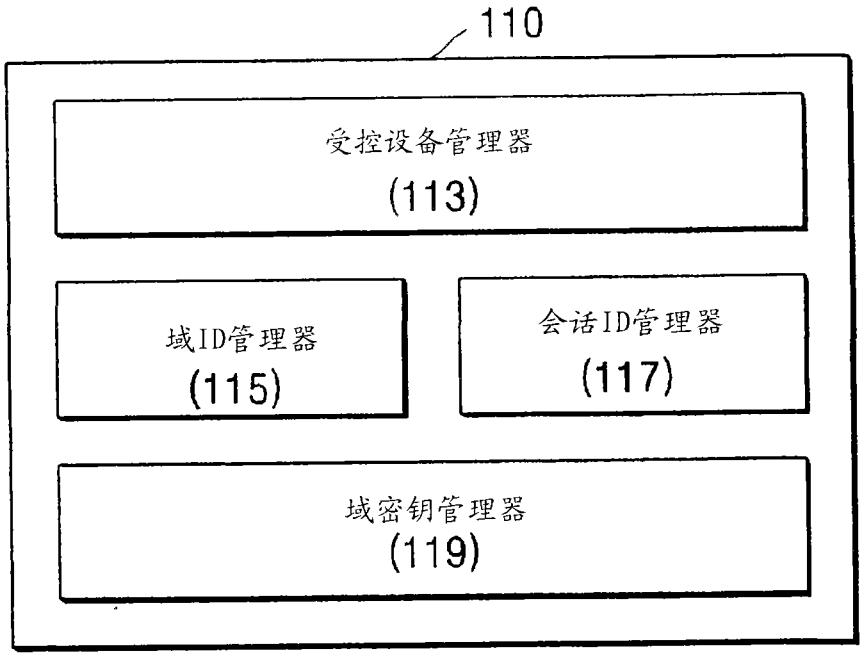

110
受控设备管理器
(113)
域ID管理器
(115)
会话ID管理器
(117)
域密钥管理器
(119)

图 18