(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 103413086 B
(45)授权公告日 2016.08.10

(21)申请号 201310373030.2

(22)申请日 2013.08.23

(73)专利权人 杭州华三通信技术有限公司
地址 310053 浙江省杭州市高新技术产业开发区之江科技工业园六和路310号华为杭州生产基地

(72)发明人 罗友春

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
G06F 21/44(2013.01)

(56)对比文件
CN 1537374 A,2004.10.13,
CN 1697367 A,2005.11.16,
CN 1784911 A,2006.06.07,
US 6732277 B1,2004.05.04,
CN 102017577 A,2011.04.13,

审查员 彭苏

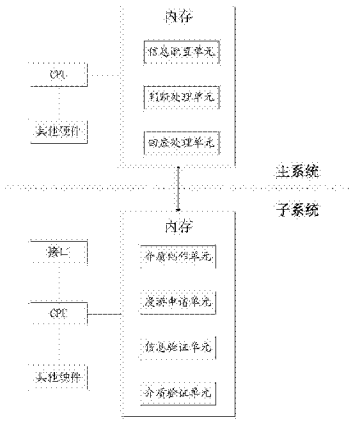
权利要求书3页 说明书6页 附图2页

(54)发明名称

一种解决可信移动存储介质安全漫游的方法及装置

(57)摘要

本发明提供一种解决可信移动存储介质安全漫游的方法及装置，在主系统装置上生成子系统唯一标识信息和安全漫游其他验证信息，在收到子系统装置发送来的漫游申请后，根据申请中的子系统唯一标识信息和安全漫游其他验证信息来判断该介质是否是本系统装置管理范围内能够进行漫游的介质，再根据判断结果做出相应处理；在子系统装置上制作可信移动存储介质，将子系统唯一标识信息、介质标识信息、加密后的子系统唯一标识信息写入介质，在非本子系统装置制作的介质插入后，向主系统装置发送漫游申请，根据主系统装置的回应做出处理。本发明能有效解决同一局点多套部署可信移动存储介质在多个系统装置间安全漫游的问题。



CN 103413086 B

1.一种实现可信介质安全漫游的装置，应用在可信移动存储介质管理系统的主系统上，该可信移动存储介质管理系统还包括若干子系统装置、子系统装置部署的客户端和可信移动存储介质，其特征在于，该实现可信介质安全漫游的装置包括信息配置单元、判断处理单元和回应处理单元；其中：

信息配置单元，用于为每一个子系统装置生成子系统唯一标识信息，以便子系统装置获取与之对应的子系统唯一标识信息后制作带有子系统唯一标识信息的可信移动存储介质；

判断处理单元，用于在收到漫游子系统装置发送来的漫游申请后，根据申请中的子系统唯一标识信息，判断该可信移动存储介质是否是其管理的子系统装置制作的，如果不是则回应漫游子系统装置该介质无法使用；

回应处理单元，用于在收到制作介质的子系统装置发送回来的验证结果后，如果验证结果是通过，则将制作介质的子系统装置发送来的解密参数转发给漫游子系统装置，如果验证结果不通过则回应漫游子系统装置该介质无法使用。

2.如权利要求1所述的装置，其特征在于，所述信息配置单元进一步用于，

配置每个子系统装置间的漫游关系，同时为每个子系统装置生成加密密钥，所述子系统装置从所述实现可信介质安全漫游的装置中获取密钥。

3.如权利要求1所述的装置，其特征在于，所述判断处理单元进一步用于，

在判断该可信移动存储介质是否是其管理的子系统装置制作的之后，进一步根据信息配置单元配置的子系统装置间漫游关系来判断，该可信移动存储介质是否能在漫游子系统装置上使用，如果不能则回应漫游子系统装置该介质无法使用，如果能则将介质标识信息发送给制作该介质的子系统装置。

4.如权利要求1所述的装置，其特征在于，所述回应处理单元进一步用于，

在验证通过后，将制作介质的子系统装置发送来的加密子系统唯一标识信息随同解密参数转发给漫游子系统装置，以供漫游子系统客户端根据漫游子系统装置转发来的加密子系统唯一标识信息、解密参数对该介质解密。

5.一种实现可信介质安全漫游的装置，应用在可信移动存储介质管理系统的子系统上，该可信移动存储介质管理系统还包括主系统装置、可信移动存储介质、子系统装置部署的客户端，其特征在于，该实现可信介质安全漫游的装置包括介质制作单元、漫游申请单元和信息验证单元；其中：

介质制作单元，用于从主系统装置中获取为本子系统装置生成的子系统唯一标识信息并将其保存，在制作可信移动存储介质时，为每个介质生成介质标识信息，将子系统唯一标识信息和介质标识信息写入介质中；

漫游申请单元，用于在收到从本子系统部署的客户端发送来的可信移动存储介质的子系统唯一标识信息、介质标识信息时，根据子系统唯一标识信息判断该介质是否是本系统装置制作的，如果是则可直接使用，如果不是则发送漫游申请给主系统装置，主系统装置在收到漫游申请后，将根据漫游申请中的信息做出相应处理；

信息验证单元，用于在收到主系统装置发送来的介质标识信息时，对其进行验证，如果验证是自己制作的介质，则向主系统装置返回解密参数；如果验证未通过，则向主系统装置返回失败的验证结果。

6.如权利要求5所述的装置，其特征在于，所述介质制作单元进一步用于，

从主系统装置中获取为本子系统装置生成的密钥，并进一步将子系统唯一标识信息进行加密，然后再将其写入所制作的介质中。

7.如权利要求5所述的装置，其特征在于，所述信息验证单元进一步用于，

当验证是自己所制作的可信移动存储介质后，在返回解密参数的同时，返回加密的子系统唯一标识信息给主系统装置，以供主系统装置将该加密的子系统唯一标识信息发送给漫游子系统装置。

8.如权利要求5所述装置，其特征在于，还包括：

介质验证单元，用于在收到主系统装置发送来的加密子系统唯一标识信息和解密参数后，将其发送给客户端，客户端将加密子系统唯一标识信息与介质中携带的子系统唯一标识信息进行对比验证，对比一致则验证通过，接着将解密参数按照预定算法进行计算，用计算出的结果对介质中加密的数据进行解密，即可使用介质；如果对比不一致则说明验证未通过，则无法使用该介质。

9.如权利要求5所述装置，其特征在于，所述介质标识信息为经过加密的该介质的唯一标识信息。

10.一种实现可信介质安全漫游的方法，应用在可信移动存储介质管理系统的主系统上，该可信移动存储介质管理系统还包括若干子系统装置、子系统装置部署的客户端和可信移动存储介质，其特征在于，该方法包括如下步骤：

为每一个子系统装置生成子系统唯一标识信息，以便子系统装置获取与之对应的子系统唯一标识信息后制作带有子系统唯一标识信息的可信移动存储介质；

在收到漫游子系统装置发送来的漫游申请后，根据申请中的子系统唯一标识信息，判断该可信移动存储介质是否是其管理的子系统装置制作的，如果不是则回应漫游子系统装置该介质无法使用；

在收到制作介质的子系统装置发送回来的验证结果后，如果验证结果是通过，则将制作介质的子系统装置发送来的解密参数转发给漫游子系统装置，如果验证结果不通过则回应漫游子系统装置该介质无法使用。

11.如权利要求10所述的方法，其特征在于，所述步骤进一步包括，

配置每个子系统装置间的漫游关系，同时为每个子系统装置生成加密密钥，所述子系统装置从主系统装置上获取该加密密钥。

12.如权利要求10所述的方法，其特征在于，所述步骤进一步包括，

在判断该可信移动存储介质是否是其管理的子系统装置制作的之后，进一步根据信息配置单元配置的子系统装置间漫游关系来判断，该可信移动存储介质是否能在漫游子系统装置上使用，如果不能则回应漫游子系统装置该介质无法使用，如果能则将介质标识信息发送给制作该介质的子系统装置。

13.如权利要求10所述的方法，其特征在于，所述步骤进一步包括，

在验证通过后，将制作介质的子系统装置发送来的加密子系统唯一标识信息随同解密参数转发给漫游子系统装置，以供漫游子系统客户端根据漫游子系统装置转发来的加密子系统唯一标识信息、解密参数对该介质解密。

14.一种实现可信介质安全漫游的方法，应用在可信移动存储介质管理系统的子系统

上，该可信移动存储介质管理系统还包括主系统装置、可信移动存储介质、子系统装置部署的客户端，其特征在于，该方法包括如下步骤：

从主系统装置中获取为本子系统装置生成的子系统唯一标识信息，并将其保存，在制作可信移动存储介质时，为每个介质生成介质标识信息，将子系统唯一标识信息和介质标识信息写入介质中；

在收到从本子系统装置部署的客户端发送来的可信移动存储介质的子系统唯一标识信息、介质标识信息时，根据子系统唯一标识信息判断该介质是否是本系统装置制作的，如果是则可直接使用，如果不是则发送漫游申请给主系统装置，主系统装置在收到漫游申请后，将根据漫游申请中的信息做出相应处理；

在收到主系统装置发送来的介质标识信息时，对其进行验证，如果验证是自己制作的介质，则向主系统装置返回解密参数；如果验证未通过，则向主系统装置返回失败的验证结果。

15.如权利要求14所述的方法，其特征在于，所述步骤进一步包括，

从主系统装置中获取为本子系统装置生成的密钥，并进一步将子系统唯一标识信息进行加密，然后再将其写入所制作的介质中。

16.如权利要求14所述的方法，其特征在于，所述步骤进一步包括，

当验证是自己所制作的可信移动存储介质后，在返回解密参数的同时，返回加密的子系统唯一标识信息给主系统装置，以供主系统装置将该加密的子系统唯一标识信息发送给漫游子系统装置。

17.如权利要求14所述方法，其特征在于，还包括：

在收到主系统装置发送来的加密子系统唯一标识信息和解密参数后，将其发送给客户端，客户端将加密子系统唯一标识信息与介质中携带的子系统唯一标识信息进行对比验证，对比一致则验证通过，接着将解密参数按照预定算法进行计算，用计算出的结果对介质中加密的数据进行解密，即可使用介质；如果对比不一致则说明验证未通过，则无法使用该介质。

18.如权利要求14所述方法，其特征在于，所述介质标识信息为经过加密的该介质的唯一标识信息。

一种解决可信移动存储介质安全漫游的方法及装置

技术领域

[0001] 本发明涉及计算机通信领域，尤其涉及一种解决可信移动存储介质安全漫游的方法及装置。

背景技术

[0002] 随着移动存储介质越来越轻便、存储容量越来越大，在企业信息安全建设中移动存储介质安全性越来越重要。因此，当前企业迫切需要一套完整的移动存储介质管理方案，从根本上解决移动存储介质的安全使用的问题。

[0003] 现有可信移动存储介质的管理方案是：为企业购买新的移动存储介质后，通过该移动存储介质的注册(打标签)完成授权，在使用时需要可信移动存储介质和可信移动存储介质管理服务器双方在线完成互信后才能使用。也就是说，当可信移动存储介质接入客户端后，客户端会将可信移动存储介质中的标签信息发送给可信移动存储介质管理服务器验证；服务器验证该接入的可信移动存储介质是本系统中授权的可信移动存储介质后，服务器根据验证结果将服务器标识下发给客户端；客户端拿到服务器标识后，将服务器标识和可信移动存储介质中的服务器标识进行比对，以此验证服务器是否为本系统中部署的服务器，而非第三方部署的服务器；双方完成互信后，客户端才会成功加载可信移动存储介质，进而实现数据安全读写。如此一来，企业信息资产、涉密信息就不会被移动存储介质非法拷贝，进而实现对移动存储介质标识信息安全管理。

[0004] 但现有技术无法解决同一局点部署多套可信移动存储介质管理系统时，可信移动存储介质在多个管理系统间安全漫游的问题。

发明内容

[0005] 有鉴于此，本发明提供一种解决可信移动存储介质安全漫游的方法及装置，以解决现有技术中存在的问题。

[0006] 具体地，本发明是通过以下技术方案实现的：

[0007] 一种实现可信介质安全漫游的装置，应用在可信移动存储介质管理系统的主系统上，该可信移动存储介质管理系统还包括若干子系统装置、子系统装置部署的客户端和可信移动存储介质，该装置包括信息配置单元、判断处理单元和回应处理单元；其中：

[0008] 信息配置单元，用于为每一个子系统装置生成子系统唯一标识信息，以便子系统装置获取与之对应的子系统唯一标识信息后制作带有子系统唯一标识信息的可信移动存储介质；

[0009] 判断处理单元，用于在收到漫游子系统装置发送来的漫游申请后，根据申请中的子系统唯一标识信息，判断该可信移动存储介质是否是其管理的子系统装置制作的，如果不是则回应漫游子系统装置该介质无法使用。

[0010] 回应处理单元，用于在收到制作介质的子系统装置发送回来的验证结果后，如果验证结果是通过，则将制作介质的子系统装置发送来的解密参数转发给漫游子系统装置，

如果验证结果不通过则回应漫游子系统装置该介质无法使用。

[0011] 本发明还同时提供一种实现可信介质安全漫游的装置，应用在可信移动存储介质管理系统的子系统上，该可信移动存储介质管理系统还包括主系统装置、可信移动存储介质、子系统装置部署的客户端，该装置包括介质制作单元、漫游申请单元和信息验证单元；其中：

[0012] 介质制作单元，用于从主系统装置中获取为本子系统装置生成的子系统唯一标识信息并将其保存，在制作可信移动存储介质时，为每个介质生成介质标识信息，将子系统唯一标识信息和介质标识信息写入介质中；

[0013] 漫游申请单元，用于在收到从本子系统部署的客户端发送来的可信移动存储介质的子系统唯一标识信息、介质标识信息时，根据子系统唯一标识信息判断该介质是否是本系统装置制作的，如果是则可直接使用，如果不是则发送漫游申请给主系统装置，主系统装置在收到漫游申请后，将根据漫游申请中的信息做出相应处理；

[0014] 信息验证单元，用于在收到主系统装置发送来的介质标识信息时，对其进行验证，如果验证是自己制作的介质，则向主系统装置返回解密参数；如果验证未通过，则向主系统装置返回失败的验证结果。

[0015] 本发明还提供一种实现可信介质安全漫游的方法，应用在可信移动存储介质管理系统的主系统上，该可信移动存储介质管理系统还包括若干子系统装置、子系统装置部署的客户端和可信移动存储介质，其中该方法包括如下步骤：

[0016] 为每一个子系统装置生成子系统唯一标识信息，以便子系统装置获取与之对应的子系统唯一标识信息后制作带有子系统唯一标识信息的可信移动存储介质；

[0017] 在收到漫游子系统装置发送来的漫游申请后，根据申请中的子系统唯一标识信息，判断该可信移动存储介质是否是其管理的子系统装置制作的，如果不是则回应漫游子系统装置该介质无法使用。

[0018] 在收到制作介质的子系统装置发送回来的验证结果后，如果验证结果是通过，则将制作介质的子系统装置发送来的解密参数转发给漫游子系统装置，如果验证结果不通过则回应漫游子系统装置该介质无法使用。

[0019] 本发明还提供一种实现可信介质安全漫游的方法，应用在可信移动存储介质管理系统的子系统上，该可信移动存储介质管理系统还包括主系统装置、可信移动存储介质、子系统装置部署的客户端，其中该方法包括如下步骤：

[0020] 从主系统装置中获取为本子系统装置生成的子系统唯一标识信息，并将其保存，在制作可信移动存储介质时，为每个介质生成介质标识信息，将子系统唯一标识信息和介质标识信息写入介质中；

[0021] 在收到从本子系统装置部署的客户端发送来的可信移动存储介质的子系统唯一标识信息、介质标识信息时，根据子系统唯一标识信息判断该介质是否是本系统装置制作的，如果是则可直接使用，如果不是则发送漫游申请给主系统装置，主系统装置在收到漫游申请后，将根据漫游申请中的信息做出相应处理；

[0022] 在收到主系统装置发送来的介质标识信息时，对其进行验证，如果验证是自己制作的介质，则向主系统装置返回解密参数；如果验证未通过，则向主系统装置返回失败的验证结果。

[0023] 与现有技术相比，本发明能有效解决同一局点部署多套可信移动存储介质管理系统时，可信移动存储介质在多个管理系统间安全漫游的问题。

附图说明

[0024] 图1是本发明装置逻辑结构及其硬件环境的示意图。

[0025] 图2是本发明方法一种示例性实施方式的流程框图。

具体实施方式

[0026] 本发明提供的在同一局点解决可信移动存储介质在多个管理系统间安全漫游的解决方案，在优选的实施方案中，本发明采用主系统装置与子系统装置交互的方式来解决可信移动存储介质在多个管理系统间安全漫游的问题。在子系统装置与主系统装置交互的过程中，可信移动存储介质中保存的相关信息被加密/解密，并被多次验证，任何一次验证未通过，该可移动存储介质都无法使用，从而实现了可移动存储介质的安全漫游。

[0027] 请参考图1，为本发明示例性实施方式中提供的分别应用在主系统和子系统上实现可信移动存储介质安全漫游的装置及其基本硬件环境，其中应用在可信移动存储介质管理系统的主系统上的装置包括信息配置单元、判断处理单元和回应处理单元。应用在可信移动存储介质管理系统的子系统上的装置包括介质制作单元、漫游申请单元、信息验证单元和介质验证单元。以上两个装置彼此相互配合执行如下处理流程，如图2所示。

[0028] 步骤1、主系统装置上的信息配置单元为每一个子系统装置生成该子系统装置唯一标识信息和一对不对称密钥。

[0029] 优选实施方式中，在进行可信移动存储介质漫游之前，首先要由主系统装置上的信息配置单元为主系统装置进行相关配置，主系统装置的配置主要包括：

[0030] 1)配置主系统装置是否启用漫游，在不启用漫游功能时，不支持可信移动存储介质在各子系统装置间漫游。

[0031] 2)在启用漫游时，配置其管理的子系统装置，完成配置后即可为每一子系统装置生成种子信息。

[0032] 其中，为主系统装置配置其管理的子系统装置的方法是，将确定作为子系统装置(通常为子系统服务器)的MAC地址和/或IP地址与主系统装置(通常为主系统服务器)进行绑定。优选地，种子信息包括：子系统唯一标识信息和一对不对称加密密钥。其中，在具体实现过程中，所述不对称加密密钥也可以是对称密钥，或者是其他加密验证实现方式。

[0033] 3)配置每个子系统装置间漫游关系。

[0034] 子系统装置间漫游关系是指各个子系统装置对不同子系统装置制作的可信移动存储介质的使用权限。例如，某主系统装置管理了A、B、C三个子系统装置，规定它们之间的漫游关系为：A可以使用B、C制作的介质；B、C无法使用A制作的介质；B、C可以相互使用对方制作的介质等。

[0035] 步骤2、子系统装置上的介质制作单元从主系统装置中获取唯一标识信息和公钥并将所述信息保存起来。

[0036] 子系统装置在与主系统装置进行绑定后，会与主系统装置进行通信，从而从主系统装置上获取本子系统装置对应的子系统唯一标识信息和不对称密钥的公钥，并将获取到

的信息保存到子系统装置中。由于子系统装置中只保存了公钥，因此，子系统装置只能对数据信息进行加密，而不能进行解密。

[0037] 步骤3、子系统装置上的介质制作单元在制作可信移动存储介质时，为其生成介质标识信息，再用公钥对子系统唯一标识信息进行加密，然后将子系统唯一标识信息、介质标识信息、加密子系统唯一标识信息写入可信移动存储介质中。

[0038] 具体地，本发明中，子系统装置在制作可信移动存储介质时，需要写入如下信息：

[0039] a)子系统唯一标识信息

[0040] 子系统装置从主系统装置那里获取了子系统唯一标识信息后，会将其写入自己所制作的可信移动存储介质中，便于以后判断该介质是哪个子系统装置制作的，且该子系统唯一标识信息是没有加密的。

[0041] b)介质标识信息

[0042] 子系统装置在制作介质时，还会为每个可信移动存储介质生成该介质的唯一信息(例如制作流水号，或者制作时间)，并用从主系统装置上获取的密钥(例如：从主系统装置上获取的公钥、对称密钥或其他加密密钥)对其进行加密，从而形成介质标识信息。介质标识信息还可以包括该介质的使用权限等内容。

[0043] c)加密后的子系统唯一信息

[0044] 在本步骤中，优选地，还需写入子系统装置用公钥加密过的子系统唯一标识信息，这是为了提高可信移动存储介质漫游过程中客户端验证相关信息的可靠性，防止在此过程中泄密，当然，对于保密要求不高的可信移动存储介质，也可以使用没有加密的子系统唯一信息。

[0045] 步骤4、当子系统装置部署的客户端接入了一个可信移动存储介质时，客户端获取该可信移动存储介质中的子系统唯一标识信息和所述可信移动存储介质的介质标识信息，并将该二信息发送给当前子系统装置。

[0046] 其中，客户端获取的该可信移动存储介质中的子系统唯一标识信息和所述移动存储介质的介质标识信息，就是上述步骤3中a和b项对应的信息。

[0047] 步骤5、当前子系统装置上的漫游申请单元根据接收的子系统唯一标识信息判断该可信移动存储介质是否是本系统装置制作的，如果是则可直接使用；如果不是则发送漫游申请给主系统装置。

[0048] 本发明中，可信移动存储介质中的子系统唯一标识信息，也就是上述步骤3中的a项对应的信息，是由主系统装置为每个子系统装置生成的，是唯一的，并且是由制作该介质的子系统装置写入该可信移动存储介质中的，同时制作该介质的子系统装置中保存了子系统唯一标识信息，所以子系统装置可以根据该接收到的子系统唯一标识信息来判断该可信移动存储介质是不是自己制作的介质。

[0049] 如果经过判断是由本子系统装置制作的可信移动存储介质，则进一步比对其接收的可信移动存储中的介质标识信息(也就是上述步骤3中的b项对应的信息)与其自身保留的对应介质标识信息是否一致，来判断是否为其制作的合法可信移动存储介质。具体地，当该介质标识信息是用不对称密钥中的公钥进行加密时，子系统装置虽然没有解密的私钥，但由于制作该可信移动存储介质上也保存有公钥加密过的相同介质标识信息，因此无需解密而通过直接比较该加密的介质标识信息是否一致即可判断是否为其制作的合法可信移

动存储介质；当该介质标识信息是用对称密钥或其他加密密钥进行加密时，则直接通过比较解密后的介质标识信息是否一致即可判断是否为其制作的合法可信移动存储介质。

[0050] 如果是其制作的介质，则通过介质验证单元将其保存的子系统唯一标识信息、介质标识信息、解密参数发送给客户端，客户端根据当前子系统装置发送的子系统唯一标识信息、介质标识信息与介质中携带的子系统唯一标识信息、介质标识信息进行对比验证，对比一致则验证通过，接着将解密参数按照预定算法进行计算，用计算出的结果对可信移动存储介质中加密的数据进行解密，即可使用该介质；如果对比不一致则无法使用该介质。在具体实现过程中，也可以不发送所述介质标识信息而仅发送子系统唯一标识信息、该介质的解密参数，所述客户端直接根据接收的子系统唯一标识信息、解密参数完成对该介质的使用认证。

[0051] 如果经过判断不是由本子系统装置制作的可信移动存储介质，则通过漫游申请单元向主系统装置发送漫游申请。其中，漫游申请携带的信息包括子系统唯一标识信息和介质标识信息，也就是之前客户端从可信移动存储介质中获取的a和b项对应的信息。

[0052] 步骤6、主系统装置上的判断处理单元在收到漫游子系统装置发送来的漫游申请后，根据发送来的漫游申请中携带的子系统唯一标识信息，判断该可信移动存储介质是否是其管理的子系统装置，如果不是则回应漫游子系统装置该可信移动存储介质无法使用；如果是则将可信移动存储介质的介质标识信息发送给制作该可信移动存储介质的初始子系统装置。

[0053] 需要说明的是，这里的漫游子系统装置即步骤5中发送漫游申请给主系统装置的子系统装置。

[0054] 主系统装置在收到漫游子系统装置发送来的漫游申请后，所述判断处理单元首先对漫游申请中的子系统唯一标识信息进行判断，看该可信移动存储介质是不是自己管理的子系统装置制作的。因为子系统唯一标识信息是由主系统装置生成的，且该子系统唯一标识信息是唯一的，所以主系统装置上的判断处理单元可以根据子系统唯一标识信息来判断是不是主系统装置管理的子系统装置制作的可信移动存储介质，以及是哪个子系统装置制作的。

[0055] 在所述判断处理单元判断出该可信移动存储介质所携带的子系统唯一标识信息是属于自己管理的某个子系统装置之后，会进一步用与该子系统装置对应的私钥对介质标识信息中包含的加密可信移动存储介质唯一信息进行解密。因为主系统装置会为每一个由其管理的子系统装置生成一对不对称密钥，子系统装置会获取对应的公钥，用于信息加密，但子系统装置没有私钥，只有主系统装置有私钥，所以主系统装置可以用对应的私钥进行解密。

[0056] 需要说明的是，在实际实现过程中，为了保证介质标识信息传输过程中的安全性，也可以不对介质标识信息进行解密，而直接将该加密的介质标识信息发送给制作介质的初始子系统装置。

[0057] 另外，判断处理单元判断子系统唯一标识后，证实该可信移动存储介质是其所在的主系统装置管理的子系统装置制作的，还会进一步根据配置的子系统装置间漫游关系，也就是步骤1中的3，来判断漫游子系统装置和制作该介质的子系统装置之间的漫游关系。例如，A为漫游子系统装置，B为制作介质的子系统装置，如果B制作的可信移动存储不能在A

上漫游，则回应A该介质无法使用；如果B制作的可信移动存储介质可以在A上漫游，则将解密出来的可信移动存储介质唯一信息或者未解密的介质标识信息发送给B。

[0058] 步骤7、制作该可信移动存储介质的初始子系统装置上的信息验证单元在收到主系统装置发送来的可信移动存储介质唯一信息或者未解密的介质标识信息时，对其进行验证，如果验证通过，则返回解密参数、加密子系统装置唯一标识信息；如果验证未通过，则通知主系统装置验证失败。

[0059] 本发明中，由于可信移动存储介质携带的可信移动存储介质唯一信息或者未解密的介质标识信息是由制作该可信移动存储介质的初始子系统装置生成的，且是唯一的，所以制作该可信移动存储介质的初始子系统装置能够从该等信息中得知此介质是不是自己制作的。具体地，由制作该介质的初始子系统装置将接收到的可信移动存储介质唯一信息或者未解密的介质标识信息与自身保存的该可信移动存储介质唯一信息或者未解密的介质标识信息进行比较，如果一致，则验证通过，如果不一致，则验证未通过。

[0060] 所述解密参数是用来对可信移动存储介质中的数据信息进行解密的。由于为了保证数据信息安全，可信移动存储介质中的数据都是经由制作该可信移动存储介质的初始子系统装置加密后再写入的，因此无法直接使用，而且每个子系统装置对数据进行加密的算法不一样，所以只有获取了制作该可信移动存储介质的初始子系统装置的解密参数，才将介质中的数据进行解密，进而使用该介质。

[0061] 步骤8、主系统装置上的回应处理单元在收到制作可信移动存储介质的初始子系统装置发送回来的验证结果后，如果初始子系统装置验证成功，则将制作可信移动存储介质的子系统装置发送来的解密参数、加密子系统唯一标识信息转发给当前子系统装置；如果初始子系统装置验证失败则回应当前子系统装置该可信移动存储介质无法使用。

[0062] 步骤9、当前子系统装置介质验证单元在收到主系统装置发送来的解密参数、加密子系统唯一标识信息后，将该信息发送给客户端，客户端将加密子系统唯一标识信息与介质中携带的子系统唯一标识信息进行对比验证，对比一致则验证通过，接着将解密参数按照预定算法进行计算，用计算出的结果对可信移动存储介质中加密的数据进行解密，即可使用该介质；如果对比不一致则无法使用该介质。

[0063] 正常情况下，客户端收到的加密子系统唯一标识信息和介质中携带的加密子系统唯一标识信息，都是由公钥对制作介质的子系统唯一标识信息进行加密后得到的，以此两者会一致。

[0064] 另外，这里的加密子系统唯一标识信息也可以是未加密的子系统唯一标识信息，或者是其他可用于对比验证的信息。

[0065] 在本发明优选的实施方式中，可信移动存储介质中携带的验证信息被多次验证，有效的保证了该可信移动存储介质中数据信息的安全。

[0066] 与现有技术相比，本发明可以有效解决同一局点多套部署可信移动存储介质在多个系统间安全漫游的问题。

[0067] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

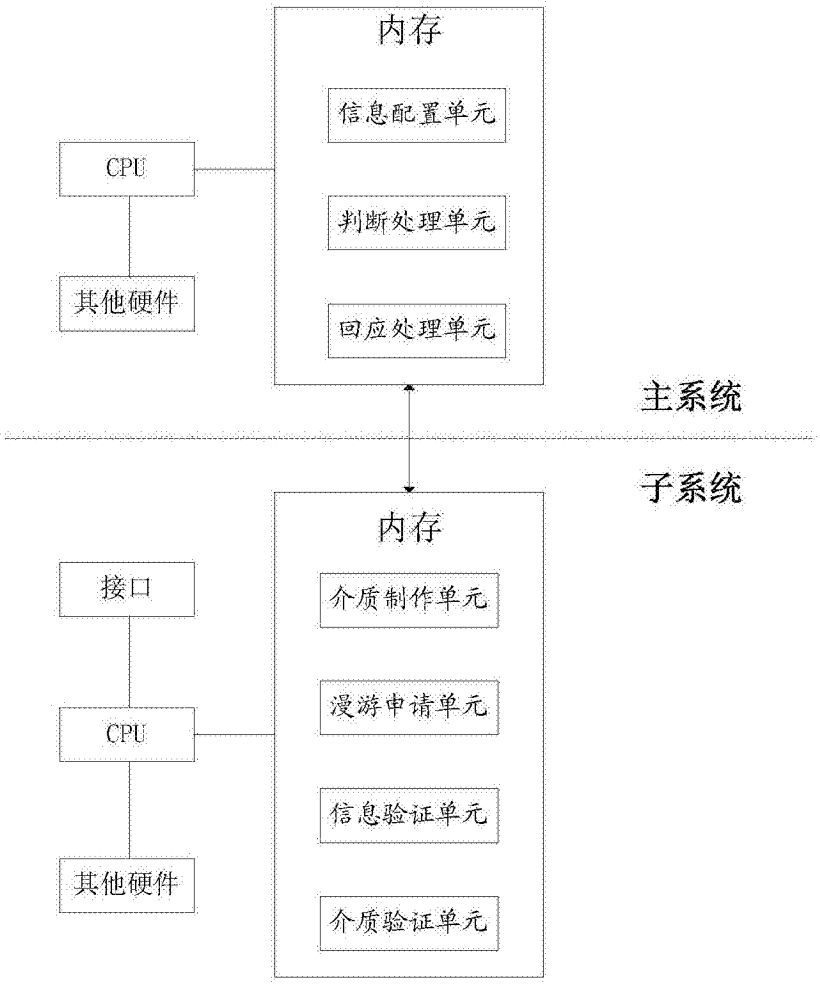

内存
信息配置单元
CPU
判断处理单元
其他硬件
回应处理单元
主系统
子系统
内存
接口
介质制作单元
CPU
漫游申请单元
信息验证单元
其他硬件
介质验证单元

图1

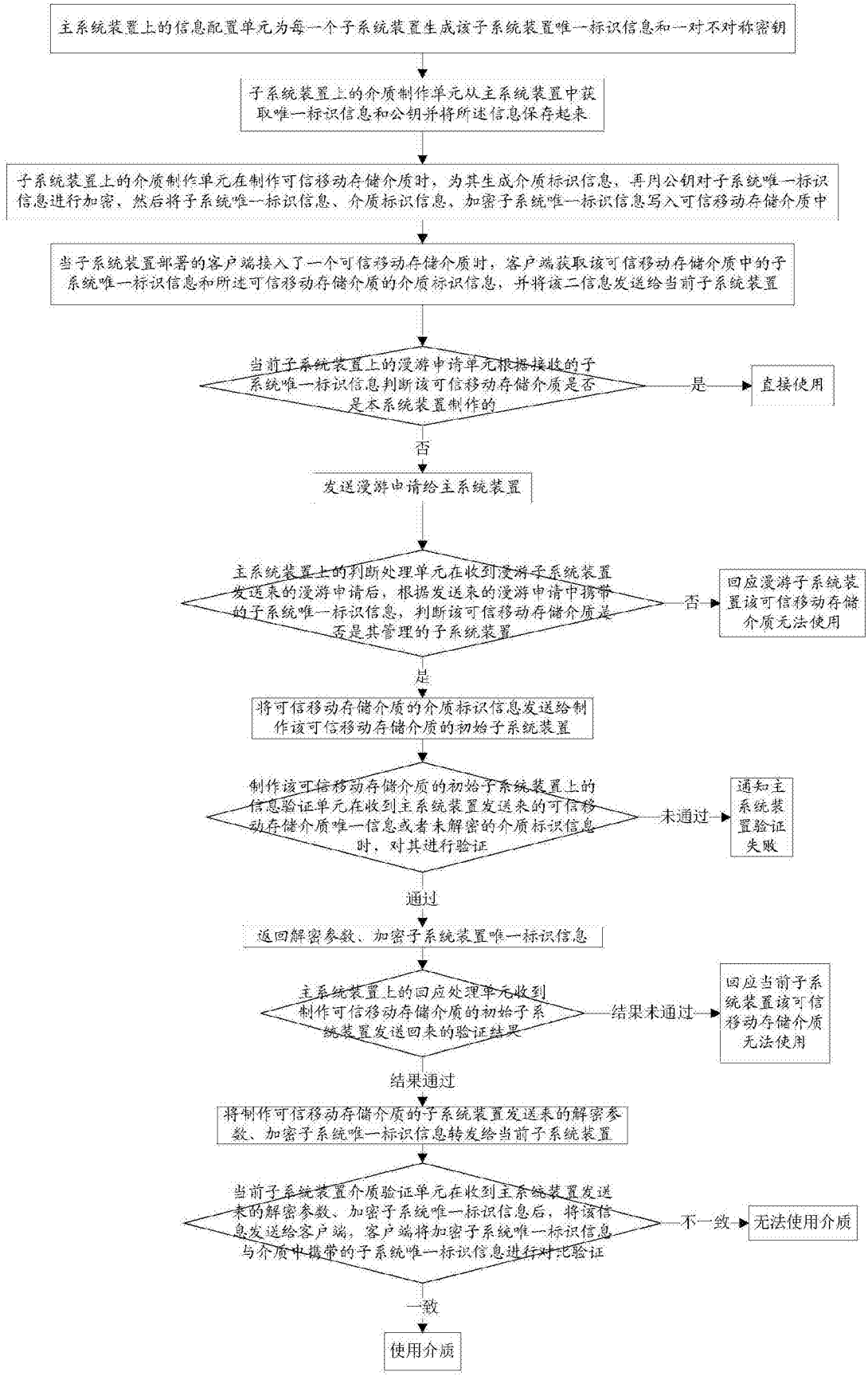

主系统装置上的信息配置单元为每一个子系统装置生成该子系统装置唯一标识信息和一对不对称密钥
子系统装置上的介质制作单元从主系统装置中获取唯一标识信息和公钥并将所述信息保存起来
子系统装置上的介质制作单元在制作可信移动存储介质时，为其生成介质标识信息，再用公钥对子系统唯一标识信息进行加密，然后将子系统唯一标识信息、介质标识信息、加密子系统唯一标识信息写入可信移动存储介质中
当子系统装置部署的客户端接入了一个可信移动存储介质时，客户端获取该可信移动存储介质中的子系统唯一标识信息和所述可信移动存储介质的介质标识信息，并将该二信息发送给当前子系统装置
当前子系统装置上的漫游申请单元根据接收的子系统唯一标识信息判断该可信移动存储介质是否是本系统装置制作的
是
直接使用
否
发送漫游申请给主系统装置
主系统装置上的判断处理单元在收到漫游子系统装置发送来的漫游申请后，根据发送来的漫游申请中携带的子系统唯一标识信息，判断该可信移动存储介质是否是其管理的子系统装置
否
回应漫游子系统装置该可信移动存储介质无法使用
是
将可信移动存储介质的介质标识信息发送给制作该可信移动存储介质的初始子系统装置
制作该可信移动存储介质的初始子系统装置上的信息验证单元在收到主系统装置发送来的可信移动存储介质唯一信息或者未解密的介质标识信息时，对其进行验证
未通过
通知主系统装置验证失败
通过
返回解密参数、加密子系统装置唯一标识信息
主系统装置上的回应处理单元收到制作可信移动存储介质的初始子系统装置发送回来的验证结果
结果未通过
回应当前子系统装置该可信移动存储介质无法使用
结果通过
将制作可信移动存储介质的子系统装置发送来的解密参数、加密子系统唯一标识信息转发给当前子系统装置
当前子系统装置介质验证单元在收到主系统装置发送来的解密参数、加密子系统唯一标识信息后，将该信息发送给客户端，客户端将加密子系统唯一标识信息与介质中携带的子系统唯一标识信息进行对比验证
不一致
无法使用介质
一致
使用介质

图2