[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 200310121213.1

[45] 授权公告日 2009 年 12 月 2 日

[11] 授权公告号 CN 100566243C

[22] 申请日 2003.12.15
[21] 申请号 200310121213.1
[30] 优先权
[32] 2002.12.16 [33] US [31] 10/321，751
[73] 专利权人 英特尔公司
地址 美国加利福尼亚州
[72] 发明人 戴维·W·克劳罗克
[56] 参考文献
EP1263164A1 2002.12.4
US6351813B1 2002.2.26
US6078920A 2000.6.20
Trusted Computing Platform Alliance (TCPA) MainSpecification Version 1.1b. TCPA Main Specification. 2002
审查员 郑晓双

[74] 专利代理机构 永新专利商标代理有限公司
代理人 王 英

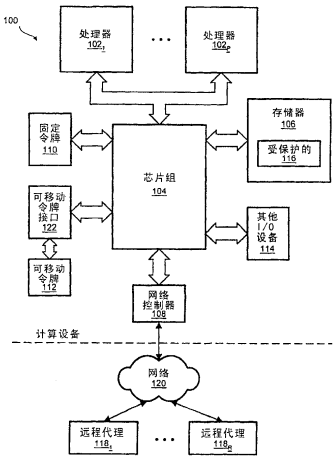
权利要求书 7 页 说明书 18 页 附图 6 页

[54] 发明名称

使用固定令牌和可移动令牌两者的计算设备及其方法

[57] 摘要

本发明描述了一种使用固定令牌和可移动令牌两者的计算设备及其方法，其中在授权使用所述受保护密钥二进制大对象的密钥之前要求出现特定的可移动令牌。 这样的受保护密钥二进制大对象可被用于在本地用户和计算设备之间建立一定水平的信任。



1. 一种方法，包括

请求固定令牌创建包括了第一密钥对和第一使用授权数据的被密封的密钥二进制大对象，其中为了使用所述第一密钥对的私有密钥需要对所述第一使用授权数据的知识，以及

请求可移动令牌创建包括了所述被密封的密钥二进制大对象和第二使用授权数据的受保护密钥二进制大对象，其中为了从所述受保护密钥二进制大对象获取所述被密封的密钥二进制大对象需要对所述第二使用授权数据的知识。

2. 如权利要求 1 所述的方法，包括

利用所述固定令牌和所述固定令牌的公共密钥，对所述第一密钥对的所述私有密钥以及所述第一使用授权数据加密，以及

利用所述加密的私有密钥和所述加密的第一使用授权数据，创建被密封的密钥二进制大对象。

3. 如权利要求 2 所述的方法，包括

利用所述可移动令牌和所述可移动令牌的公共密钥，对所述被密封的密钥二进制大对象和所述第二使用授权数据加密，以及

利用所述加密的被密封的密钥二进制大对象和所述加密的第二使用授权数据，创建所述受保护密钥二进制大对象。

4. 如权利要求 1 所述的方法，包括

请求所述可移动令牌从所述受保护密钥二进制大对象返回所述被密封的密钥二进制大对象，

向所述可移动令牌提供对拥有所述第二使用授权数据的证据，以及

仅当对拥有所述第二使用授权数据的所述证据是有效的时候，从所述可移动令牌获取所述被密封的密钥二进制大对象。

5. 如权利要求 4 所述的方法，包括

请求所述固定令牌从所述被密封的密钥二进制大对象加载所述第一密钥对，以及

向所述固定令牌提供对拥有所述第一使用授权数据的证据，以及

仅当对拥有所述第一使用授权数据的所述证据是有效的时候，获取存储于所述固定令牌中的对于所述第一密钥对的密钥句柄。

6. 如权利要求 1 所述的方法，包括

向所述可移动令牌发送请求以从所述受保护密钥二进制大对象返回所述被密封的密钥二进制大对象，所述请求包括对拥有所述第二使用授权数据的证据，以及

仅当所述可移动令牌存在并且对拥有所述第二使用授权数据的所述证据是有效的时候，从所述可移动令牌获取所述被密封的密钥二进制大对象。

7. 如权利要求 6 所述的方法，包括

向所述固定令牌发送请求以从所述被密封的密钥二进制大对象加载所述第一密钥对，所述请求包括对拥有所述第一使用授权数据的证据，以及

仅当所述对拥有所述第一使用授权数据的所述证据是有效的并且与所述请求相关的环境满足由所述被密封的密钥二进制大对象所规定的标准的时候，获取存储于所述固定令牌中的对于所述第一密钥对的密钥句柄。

8. 如权利要求 3 所述的方法，包括

向所述可移动令牌提供对所述受保护密钥二进制大对象的所述被密封的密钥二进制大对象的请求，所述请求提供了对拥有所述第二使用授权数据的证据，

利用所述可移动令牌使用所述可移动令牌的私有密钥，对所述受保护密钥二进制大对象的所述加密的被密封的密钥二进制大对象以及所述加密的第二使用授权数据解密，以及

响应于所述可移动令牌确定了对拥有所述第二使用授权数据的所述证据是有效的，从所述可移动令牌接收所述被密封的密钥二进制大对象。

9. 如权利要求 8 所述的方法，还包括

响应于确定了对拥有所述第二使用授权数据的所述证据是无效的，从所述可移动令牌擦去所述受保护密钥二进制大对象和相关的数据。

10. 如权利要求 9 所述的方法，还包括响应于确定了对拥有所述第二

使用授权数据的所述证据是无效的，停用所述可移动令牌。

11. 如权利要求 8 所述的方法，包括

向所述固定令牌提供请求以加载所述被密封的密钥二进制大对象的所述第一密钥对，所述请求提供了对拥有所述第一使用授权数据的证据，

利用所述固定令牌使用所述固定令牌的私有密钥，对所述被密封的密钥二进制大对象的所述加密的私有密钥和所述加密的第一使用授权数据解密，以及

响应于所述固定令牌确定了对拥有所述第一使用授权数据的所述证据是有效的，接收对于所述被密封的密钥二进制大对象的第一密钥对的密钥句柄。

12. 如权利要求 11 所述的方法，还包括

响应于确定了对拥有所述第一使用授权数据的所述证据是无效的，从所述固定令牌擦去所述被密封的密钥二进制大对象和相关的数据。

13. 如权利要求 12 所述的方法，还包括响应于确定了对拥有所述第一使用授权数据的所述证据是无效的，停用所述可移动令牌。

14. 一种由处理器执行的方法，包括

请求可移动令牌从包括第二使用授权数据的受保护密钥二进制大对象提供被密封的密钥二进制大对象，

向所述可移动令牌提供基于所述处理器具有的对于所述受保护密钥二进制大对象的第二使用授权数据的第二认证代码，

仅当所述第二认证代码表明所述处理器的所述第二使用授权数据与所述受保护密钥二进制大对象的所述第二使用授权数据具有预定关系时，从所述可移动令牌接收所述被密封的密钥二进制大对象，其中所述被密封的密钥二进制大对象包括第一使用授权数据，

请求固定令牌从所述被密封的密钥二进制大对象加载第一密钥对，

向所述固定令牌提供基于所述处理器具有的对于所述被密封的密钥二进制大对象的第一使用授权数据的第一认证代码，以及

仅当所述第一认证代码表明所述处理器的所述第一使用授权数据与所述被密封的密钥二进制大对象的所述第一使用授权数据具有预定关系时，

接收对于所述第一密钥对的第一密钥句柄。

15. 如权利要求 14 所述的方法，还包括

基于使用了第一共享秘密的第一 HMAC 计算，生成所述第一认证代码，所述第一共享秘密是基于所述处理器具有的对于所述被密封的密钥二进制大对象的所述第一使用授权数据，

基于使用了第二共享秘密的第二 HMAC 计算，生成所述第二认证代码，所述第二共享秘密是基于所述处理器具有的对于所述受保护密钥二进制大对象的所述第二使用授权数据。

16. 如权利要求 14 所述的方法，还包括

基于第一 HMAC 计算，生成所述第一认证代码，所述第一 HMAC 计算使用了基于所述处理器具有的对于所述被密封的密钥二进制大对象的所述第一使用授权数据的第一共享秘密以及与所述固定令牌相关的第一滚动现时标志，

基于第二 HMAC 计算，生成所述第二认证代码，所述第二 HMAC 计算使用了基于所述处理器具有的对于所述受保护密钥二进制大对象的所述第二使用授权数据的第二共享秘密以及与所述可移动令牌相关的第二滚动现时标志。

17. 如权利要求 14 所述的方法，还包括

响应于接收所述第一密钥句柄确定与所述可移动令牌相关的用户出现。

18. 如权利要求 14 所述的方法，还包括

响应于成功地使用由所述第一密钥句柄所标识的所述第一密钥对解密秘密，确定与所述可移动令牌相关的用户出现。

19. 如权利要求 14 所述的方法，还包括

向所述固定令牌提供对环境的至少一个量度，并且

其中，仅当所述第一认证代码表明所述处理器的所述第一使用授权数据与所述被密封的密钥二进制大对象的所述第一授权数据具有预定关系并且所述至少一个量度表明所述环境满足由所述被密封的密钥二进制大对象规定的标准的时候，接收对于所述第一密钥对的第一密钥句柄。

20. 如权利要求 19 所述的方法，还包括

响应于接收所述第一密钥句柄，确定所述环境满足由所述被密封的密钥二进制大对象所规定的所述标准。

21. 如权利要求 19 所述的方法，还包括

响应于成功地利用由所述第一密钥句柄所标识的所述第一密钥对解密秘密，确定所述环境满足了由所述被密封的密钥二进制大对象规定的所述标准。

22. 一种计算设备，包括

固定令牌，所述固定令牌包括第一处理单元和第一受保护存储器，所述第一处理单元响应于确定了第一认证代码与被密封的密钥二进制大对象的第一使用授权数据具有预定关系，将所述被密封的密钥二进制大对象的第一密钥对加载到所述第一受保护存储器中，其中所述被密封的密钥二进制大对象包括所述第一密钥对，

可移动令牌，所述可移动令牌包括第二处理单元和第二受保护存储器，所述第二处理单元响应于确定了第二认证代码与受保护密钥二进制大对象的第二使用授权数据具有预定关系，从所述受保护密钥二进制大对象返回所述被密封的密钥二进制大对象，其中所述受保护密钥二进制大对象包括所述被密封的密钥二进制大对象，

可移动令牌接口，所述可移动令牌接口使得所述可移动令牌能够被耦合到所述计算设备并能够从所述计算设备移除，

处理器，所述处理器向所述可移动令牌提供对所述被密封的密钥二进制大对象的请求，所述请求包括所述受保护密钥二进制大对象和所述第二认证代码，并且所述处理器向所述固定令牌提供加载所述第一密钥对的请求，所述请求包括所述被密封的密钥二进制大对象和所述第一认证代码。

23. 如权利要求 22 所述的计算设备，其中

所述固定令牌将响应于成功地加载所述第一密钥对，提供对于所述第一密钥对的第一密钥句柄，并且

所述处理器将响应于接收所述第一密钥句柄，确定与所述可移动令牌相关的用户出现。

24. 如权利要求 22 所述的计算设备，其中

所述固定令牌将响应于成功地加载了所述第一密钥对，提供对于所述第一密钥对的第一密钥句柄，并且

所述处理器将响应于成功地使用由所述第一密钥句柄标识的所述第一密钥对解密秘密，确定与所述可移动令牌相关的用户出现。

25. 如权利要求 22 所述的计算设备，其中

所述固定令牌的所述第一受保护存储器包括用于存储对环境的量度的寄存器，

所述处理器将向所述固定令牌提供所述环境的多个量度，并且

所述第一处理单元将仅当存储于所述寄存器中的所述量度表明所述环境满足了所述被密封的密钥二进制大对象的标准的时候，将所述第一密钥对加载到所述第一受保护存储器中。

26. 如权利要求 25 所述的计算设备，其中

所述固定令牌将响应于成功地加载所述第一密钥对，提供对于所述第一密钥对的第一密钥句柄，并且

所述处理器将响应于接收所述第一密钥句柄，确定所述环境满足了由所述被密封的密钥二进制大对象规定的所述标准。

27. 如权利要求 25 所述的计算设备，其中

所述固定令牌将响应于成功地加载所述第一密钥对，提供对于所述第一密钥对的第一密钥句柄，并且

所述处理器将响应于成功地使用由所述第一密钥句柄标识的所述第一密钥对解密秘密，确定所述环境满足了由所述被密封的密钥二进制大对象规定的所述标准。

28. 如权利要求 25 所述的计算设备，其中

所述第一处理单元将响应于确定了所述环境没有满足所述被密封的密钥二进制大对象的所述标准，从所述固定令牌擦去所述被密封的密钥二进制大对象和相关的数据。

29. 如权利要求 22 所述计算设备，其中

所述固定令牌包括用于创建所述被密封的密钥二进制大对象的密钥

对，

所述第一处理单元只响应于通过为被用来创建所述被密封的密钥二进制大对象的所述密钥对而建立的第一会话而接收的请求，加载所述被密封的密钥二进制大对象的所述第一密钥对，并且

所述处理器将在向所述固定令牌提供加载所述第一密钥对的所述请求之前，建立所述第一会话。

30. 如权利要求 29 所述的计算设备，其中

所述可移动令牌包括用于创建所述受保护密钥二进制大对象的密钥对，

所述第二处理单元将只响应于通过为用于创建所述受保护密钥二进制大对象的所述密钥对而建立的第二会话而接收的请求，从所述受保护密钥二进制大对象获得所述被密封的密钥二进制大对象，并且

所述处理器将在向所述可移动令牌提供对于所述被密封的密钥二进制大对象的所述请求之前，建立所述第二会话。

使用固定令牌和可移动令牌两者的计算设备及其方法

技术领域

本发明一般地涉及用于创建和使用受保护密钥二进制大对象的方法和装置。

背景技术

2002年2月22日1.1b版的可信计算平台联盟（TCPA）主规范（以下称为“TCPA SPEC”）描述了被附加于计算设备或平台和/或要不然不能从计算设备或平台上被移除的令牌或者可信平台模块（TPM）。这种固定令牌支持对软件进程、平台引导完整性、文件完整性以及软件授权的审计和日志记录。另外，固定令牌提供受保护存储器，其中项目能够受到保护而免遭暴露或不适当的使用，固定令牌还提供可以被用于证明的标识。这些特征促进了第三方准许计算设备或者平台访问信息，而这在其他情况下是会被拒绝的。

第三方可以利用远程计算设备来与使用固定令牌证明机制的计算设备建立一定水平的信任。但是，用以建立这种水平的信任的处理一般要求第三方的远程计算设备进行复杂的计算并且参与和该固定令牌有关的复杂协议。但是，平台的本地用户可能还希望与本地平台或计算设备建立类似水平的信任。然而，对于本地用户要象远程计算设备一样进行同样的复杂计算并参与和固定令牌有关的同样的复杂协议以便建立对该计算设备的信任，这是不切实际的。

发明内容

根据本发明的一个方面，提出了一种方法，包括请求固定令牌创建包括了第一密钥对和第一使用授权数据的被密封的密钥二进制大对象，其中为了使用所述第一密钥对的私有密钥需要对所述第一使用授权数据的知

识，以及请求可移动令牌创建包括了所述被密封的密钥二进制大对象和第二使用授权数据的受保护密钥二进制大对象，其中为了从所述受保护密钥二进制大对象获取所述被密封的密钥二进制大对象需要对所述第二使用授权数据的知识。

根据本发明的另一个方面，提出了一种由处理器执行的方法，包括：请求可移动令牌从包括第二使用授权数据的受保护密钥二进制大对象提供被密封的密钥二进制大对象，向所述可移动令牌提供基于所述处理器具有的对于所述受保护密钥二进制大对象的第二使用授权数据的第二认证代码，仅当所述第二认证代码表明所述处理器的所述第二使用授权数据与所述受保护密钥二进制大对象的所述第二使用授权数据具有预定关系时，从所述可移动令牌接收所述被密封的密钥二进制大对象，其中所述被密封的密钥二进制大对象包括第一使用授权数据，请求固定令牌从所述被密封的密钥二进制大对象加载第一密钥对，向所述固定令牌提供基于所述处理器具有的对于所述被密封的密钥二进制大对象的第一使用授权数据的第一认证代码，以及仅当所述第一认证代码表明所述处理器的所述第一使用授权数据与所述被密封的密钥二进制大对象的所述第一使用授权数据具有预定关系时，接收对于所述第一密钥对的第一密钥句柄。

根据本发明的另一个方面，提出了一种计算设备，包括固定令牌、可移动令牌、可移动令牌接口和处理器，所述固定令牌包括第一处理器单元和第一受保护存储器，所述第一处理器单元响应于确定了第一认证代码与被密封的密钥二进制大对象的第一使用授权数据具有预定关系，将所述被密封的密钥二进制大对象的第一密钥对加载到所述第一受保护存储器中，其中所述被密封的密钥二进制大对象包括所述第一密钥对，所述可移动令牌包括第二处理单元和第二受保护存储器，所述第二处理单元响应于确定了第二认证代码与受保护密钥二进制大对象的第二使用授权数据具有预定关系，从所述受保护密钥二进制大对象返回所述被密封的密钥二进制大对象，其中所述受保护密钥二进制大对象包括所述被密封的密钥二进制大对象，所述可移动令牌接口使得所述可移动令牌能够被耦合到所述计算设备并能够从所述计算设备移除，所述处理器向所述可移动令牌提供对所述被密封的密钥二进制大对象的请求，所述请求包括所述受保护密钥二进制大

对象和所述第二认证代码，并且所述处理器向所述固定令牌提供加载所述第一密钥对的请求，所述请求包括所述被密封的密钥二进制大对象和所述第一认证代码。

附图说明

这里所描述的本发明是通过示例而不是限制的方式图示于附图中的。为了说明的简洁和清楚，图中所示部件不一定按比例绘制。例如，为了清

晰，一些部件的尺寸可能相对于其他部件被夸大。另外，在认为合适的地方，在图之间重复标号以表示对应或者类似的元素。

图 1 图示了包括有固定令牌和可移动令牌的示例计算设备；

图 2 图示了图 1 的示例固定令牌和示例可移动令牌；

图 3 图示了可利用图 1 的计算设备实现的示例可信环境；

图 4 图示了可以被图 1 的计算设备用于本地证明的示例的被密封的密钥二进制大对象和示例的受保护的密钥二进制大对象；

图 5 图示了创建图 4 的受保护的密钥二进制大对象的示例方法；

图 6 图示了加载图 4 的受保护的密钥二进制大对象的密钥的示例方法。

具体实施方式

在以下详细描述中，描述了很多具体细节以便提供对本发明的全面的理解。但是，本发明可以在不采用这些具体细节的条件下实现。在其他情况中，没有详细描述已知的方法、程序、组成部分以及电路以避免使本发明不清晰。另外，示例尺寸/模块/值/范围可能被给出，虽然一些实施例可以不限于这些具体示例。

说明书中提到的“一个实施例”、“实施例”、“示例实施例”等表示所描述的实施例可以包括具体特征、结构或者特性，但是每个实施例未必包括该具体特征、结构或者特性。而且，这样的措词未必指的是同一个实施例。另外，虽然具体特征、结构或者特性是结合一个实施例描述的，但是应该认为不论是否被明确地描述，本领域技术人员都知道如何使这样的特征、结构或者特性结合其他实施例起作用。

另外，术语“二进制大对象”（binary large object，blob）常用于数据库领域，指以数据库本身不能解释的形式需要被存储于数据库中的任何随机的大块二进制数字。但是，术语“二进制大对象”用在这里意思是具有更广的范围。具体而言，术语“二进制大对象”被规定为广义的术语，它包含了不论结构、格式、表示法或者大小的一个或者多个二进制数字的任何分组。

此外，动词“散列”以及相关形式在这里被用来指基于操作数或者消息进行操作以产生值或者“散列”。理论上，散列操作生成散列，由该散列不能推算找出与该散列相关的消息，并且不能由其判断出有关与该散列相关消息的任何有用信息。另外，散列操作理论上生成散列，使得不可能通过推算判断出产生同样的散列的两个消息。尽管散列操作理论上具有以上性质，但是实际上例如消息摘要 5 算法（MD5）和安全散列算法 1（SHA-1）的单向函数生成从其还原消息是困难的、计算上繁复并且/或者实际上不可行的散列值。

此外，术语“第一”、“第二”、“第三”等用在这里作为标记以区别类似地命名的组成部分和/或操作。具体而言，这样的术语不用来表示也不意图要表示组成部分和/或操作的顺序。另外，这样的术语不用来表示也不意图要表示一个组成部分和/或操作具有比另一个更高的重要性。

现在参照图 1，示出了示例计算设备 100。计算设备 100 可以包括一个或多个处理器 $102_1...102_P$。处理器 $102_1...102_P$ 可支持一个或者多个操作模式，例如，实模式、保护模式、虚拟 8086 模式以及虚拟机扩展模式（VMX 模式）。另外，处理器 $102_1...102_P$ 可以在每个所支持的操作模式中支持一个或者多个特权等级或环。一般而言，处理器 $102_1...102_P$ 的操作模式和特权等级确定了可以用于执行的指令以及执行这样的指令的效果。更具体地说，仅当处理器 $102_1...102_P$ 处于合适的模式和/或特权等级的时候，处理器 $102_1...102_P$ 才可以被允许执行某些被授予特权的指令。

芯片组 104 可以包括一个或者多个集成电路组件或者芯片，将处理器 $102_1...102_P$ 耦合到存储器 106、网络接口 108、固定令牌 110、可移动令牌 112 以及该计算设备 100 的其他 I/O 设备 114，例如，鼠标、键盘、磁盘驱动器、视频控制器等。芯片组 104 可以包括用于向存储器 106 写入数据或者从中读取数据的存储器控制器（未示出）。另外，芯片组 104 和/或处理器 $102_1...102_P$ 可以将存储器 106 的某些区域确定为受保护存储器 116。在一个实施例中，处理器 $102_1...102_P$ 仅当处于特定操作模式（例如，保护模式）和特权等级（例如，0P）时才可以访问受保护存储器 116。

网络接口 108 一般为计算设备 100 提供通信机构以通过网络 120 与一

个或者多个远程代理 $118_1...118_R$（例如，认证中心、零售商、金融机构）通信。例如，网络接口 108 可包括千兆位以太网控制器、有线调制解调器、数字用户线路（DSL）调制解调器、普通老式电话服务（POTS）调制解调器等来将计算设备 100 耦合到一个或者多个远程代理 $118_1...118_R$。

固定令牌 110 可被附加或者结合到计算设备 100 中以向远程代理 $118_1...118_R$ 和/或本地用户保证固定令牌 110 只与计算设备 100 相关联。例如，固定令牌 110 可被结合到芯片组 104 的一个芯片中和/或被表面贴装到计算设备 100 的主板（未示出）。一般而言，固定令牌 110 可包括对量度（metric）、密钥和秘密的受保护存储，并可响应于来自处理器 $102_1...102_P$ 以及芯片组 104 的请求进行各种完整性功能。在一个实施例中，固定令牌 110 可以以可信方式存储量度，可以以可信方式引用量度，可以将秘密密封到特定环境（当前或者将来）中，并可对密封秘密的环境解封秘密。另外，固定令牌 110 可以加载被密封的密钥二进制大对象的密钥并可以建立会话，使得请求者能够使用与所建立的会话相关的密钥进行操作。

可移动令牌 112 可通过计算设备 100 的可移动令牌接口 122 建立到处理器 $102_1...102_P$ 的链接。可移动接口 122 可包括端口（例如，USB 端口、IEEE 1394 端口、串行端口、并行端口）、插槽（例如，读卡器、PC 卡插槽等）、收发器（例如，射频收发器、红外收发器等）和/或使得可移动令牌 112 能够方便地被耦合到计算设备 100 并从其上被移除的一些其他接口机构。与固定令牌类似，可移动令牌 112 可以包括对密钥和秘密的受保护存储器，并可以响应于来自处理器 $102_1...102_P$ 和芯片组 104 的请求完成各种完整性功能。在一个实施例中，可移动令牌 112 可以加载被密封的密钥二进制大对象的密钥，并可以建立会话，使得请求者能够使用与所建立的会话相关的密钥进行操作。另外，可移动令牌 112 可以改变与被密封的密钥二进制大对象相关的使用授权数据，并可以在确定请求者被授权接收被密封的密钥二进制大对象之后返回受保护密钥二进制大对象的被密封的密钥二进制大对象。

如图 2 所示，固定令牌 110 可以包括一个或者多个处理单元 200、随

机数生成器 202 以及受保护存储器 204，其中受保护存储器 204 可以包括密钥 206、秘密 208 和/或一个或多个用于量度的平台配置寄存器（PCR）寄存器 210。类似地，可移动令牌 112 可包括一个或多个处理单元 212、随机数生成器 214 和受保护存储器 216，其中受保护存储器 216 可以包括密钥 218 和/或秘密 220。处理单元 200、212 可以为计算设备 100 完成完整性功能，例如，生成和/或计算对称和非对称的密钥。在一个实施例中，处理单元 200、212 可以使用所生成的密钥来加密和/或标记信息。另外，处理单元 200、212 可基于 AES（先进加密标准）、DES（数据加密标准）、3DES（三倍数据加密标准）或者以由随机数生成器 202、214 所生成的随机数为种子的一些其他的对称密钥生成算法来生成对称密钥。类似地，处理单元 200、212 可基于 RSA（Rivest-Shamir-Adleman）、EC（椭圆曲线）或者以由随机数生成器 202、214 所生成的随机数为种子的一些其他的非对称密钥对生成算法来生成非对称密钥对。

在一个实施例中，固定令牌 110 和可移动令牌 112 都可从以其各自的随机数生成器 202、214 所生成的随机数为种子的对称和非对称密钥生成算法生成不可改变的对称密钥和/或非对称密钥对。一般而言，这些不可改变的密钥一旦被令牌 110、112 激活之后就不能被改变。由于不可改变的密钥在激活之后不能被改变，所以不可改变的密钥可被用于唯一地标识各自令牌 110、112 的机制的一部分。除了不可改变的密钥，处理单元 200、212 还可以按照非对称密钥生成算法生成一个或者多个补充的非对称密钥对。在一个示例的实施例中，尽管不可改变的非对称密钥对一旦被激活就不可被改变，计算设备 100 可根据需要生成补充的非对称密钥对。为了减少将不可改变的非对称密钥暴露给外界攻击，对于大多数加密、解密以及标记操作，计算设备 100 一般都使用其补充的非对称密钥对。具体而言，计算设备 100 一般仅向一组小规模的可信实体，例如，认证中心提供不可改变的公共密钥。另外，在一个实施例中计算设备 100 的固定令牌 110 从不向请求者提供不可改变的私有密钥，在利用它的一个不可改变的公共密钥和/或它的一个其他补充的非对称密钥对其加密之后，仅向请求者提供可改变的私有密钥。

因此，可以有理由向实体保证用一个补充公共密钥或一个不可改变的公共密钥加密的信息只能用相应的令牌 110、112 解密或者由在相应的令牌 110、112 授权下的实体解密。另外，可移动令牌 112 可向计算设备 100 和/或远程代理 $118_1...118_R$ 提供一些保证，确保与可移动令牌 112 相关的用户出现在或者位于或者邻近计算设备 100。由于可移动令牌 112 的唯一性以及因为假设了该用户正控制着该可移动令牌 112，计算设备 100 和/或远程代理 $118_1...118_R$ 可以有理由假设可移动令牌 112 的用户出现了或者该用户已经授权了其他人使用该可移动令牌 112。

固定令牌 110 的一个或者多个 PCR 寄存器 210 可被用来以可信方式记录和报告量度。为此，处理单元 200 可支持 PCR 引用操作，该操作返回被标识的 PCR 寄存器 210 的引用或者其内容。处理单元 200 还可支持 PCR 扩展操作，该操作在被标识的 PCR 寄存器 210 中记录所接收的量度。具体而言，PCR 扩展操作可以（1）将接收到的量度连接或者添加到被存储在被标识的 PCR 寄存器 210 中的量度上以获取被添加的量度，（2）散列该被添加的量度以获取代表了所接收的量度和先前由被识别的 PCR 寄存器 210 所记录的量度的更新的量度，并且（3）将该更新的量度存储在 PCR 寄存器 210 中。

在一个实施例中固定令牌 110 和可移动令牌 112 都提供对于在请求者和令牌 110、112 之间建立会话的支持。具体而言，在一个实施例中固定令牌 110 和可移动令牌 112 都履行了 TCPA SPEC 中所描述的针对对象的认证协议（Object-Specific Authentication Protocol，OS-AP）以建立会话。另外，固定令牌 110 和可移动令牌 112 都履行了 TCPA SPEC 的 TPM_OSAP 操作，结果使令牌 110、112 按照 OS-AP 协议建立了会话。一般，OS-AP 协议要求请求者提供标识令牌 110、112 的密钥的密钥句柄。密钥句柄仅仅是表明密钥被加载的标签以及用来定位被加载的密钥的机制。令牌 110、112 然后向请求者提供授权句柄，该授权句柄标识了密钥和从与该密钥相关的使用授权数据计算出的共享秘密。当使用会话时，请求者向令牌 110、112 提供授权句柄和消息认证代码（MAC），这两者都提供了拥有与密钥相关的使用授权数据的证据和对消息/请求的参数的证

明。在一个实施例中，请求者和令牌 110、112 还基于滚动现时标志（nonce）范例计算认证代码，其中请求者和令牌 110、112 都生成了被包括在请求及其应答中的随机值或者现时标志，以便帮助防止重放攻击。

固定令牌 110 的处理单元 200 还可以支持密封操作。密封操作一般使得固定令牌 110 将二进制大对象密封到规定的环境，并向请求部件，例如，监视器 302、内核 312、可信小应用程序 314、操作系统 308 和/或应用程序 310 提供被密封的二进制大对象。具体而言，请求部件可以建立对于固定令牌 110 的非对称密钥对的会话。请求部件还可通过所建立的会话向固定令牌 110 提供要被密封的二进制大对象、一个或多个标识了对其密封二进制大对象的 PCR 寄存器 210 的索引以及被标识的 PCR 寄存器 210 的期望的量度。固定令牌 110 可生成密封记录、证据值以及还可能生成二进制大对象对其密封的敏感数据，其中所述密封记录规定了环境标准（例如，对被标识 PCR 寄存器 210 的引用），所述证据值以后可被固定令牌 110 用来验证该固定令牌 110 创建了被密封的二进制大对象。固定令牌 110 还可以散列二进制大对象的一个或者多个部分以获取证明该二进制大对象的一个或多个被散列部分的完整性的摘要值。固定令牌 110 然后可以使用非对称加密算法和所建立的会话的公共密钥，通过对例如使用授权数据、私有密钥以及摘要值的二进制大对象敏感部分进行加密，来生成被密封的二进制大对象。固定令牌 110 然后可向请求部件提供被密封的二进制大对象。

固定令牌 110 的处理单元 200 还可支持解封操作。解封操作一般使得固定令牌 110 仅当二进制大对象是利用该固定令牌 110 的密钥被密封的，并且当前环境满足了对该被密封的二进制大对象规定的标准的时候，才解封二进制大对象。具体而言，请求部件可以对固定令牌 110 的非对称密钥对建立会话，并可以通过所建立的会话向固定令牌 110 提供被密封的二进制大对象。固定令牌 110 可以使用所建立的会话的私有密钥对该被密封的二进制大对象的一个或者多个部分解密。如果私有密钥对应被用来密封被密封的二进制大对象的公共密钥，则固定令牌 110 可从该二进制大对象获取被加密的数据的纯文本译文。否则，固定令牌会遇到出错状态并且/或者

会得到被加密的数据的被破坏的表达。固定令牌还可散列二进制大对象的一个或者多个部分以得到该二进制大对象的计算的摘要值。响应于确定了计算的摘要值等于从被密封的二进制大对象获取的摘要值、PCR 寄存器 210 的量度满足了由从被密封的二进制大对象获取的密封记录所规定的标准并且证据值表明固定令牌创建了被密封的二进制大对象，固定令牌 110 然后可以将该二进制大对象返回到请求部件。否则，固定令牌 110 可以放弃解封操作并从固定令牌 110 上擦除二进制大对象、密封记录、摘要值以及计算的摘要值。

以上示例的密封和解封操作通过非对称密码算法使用公共密钥来密封二进制大对象并使用私有密钥来解封二进制大对象。但是，固定令牌可以使用对称密码算法用单个密钥来密封二进制大对象和解封二进制大对象。例如，固定令牌 110 可包括被用来通过例如 DES、3DES、AES 和/或其他算法的对称密码算法来密封和解封二进制大对象的嵌入的密钥。

应该认识到，固定令牌 110 和可移动令牌 112 可以若干不同的方式来实现。例如，固定令牌 110 和可移动令牌 112 可以类似于 TCPA SPEC 中所详细描述的可信平台模块（TPM）的方式实现。但是，特征和功能显著少于 TCPA SPEC 的 TPM 的可移动令牌的低成本实现可能适于一些使用模型，例如本地证明。另外，固定令牌 110 和可移动令牌 112 可以以超出以上所描述的 OS-AP 协议的若干不同的方式来建立会话和/或授权其密钥的使用。

图 3 示出了一个示例的可信环境 300。计算设备 100 可利用处理器 $102_1 \ldots 102_P$ 的操作模式和特权等级来建立该可信环境 300。如所示的，可信环境 300 可以包括可信虚拟机内核或者监视器 302、一个或者多个标准虚拟机（标准 VM）304 以及一个或者多个可信虚拟机（可信 VM）306。可信环境 300 的监视器 302 在最高特权处理器环（例如 0P）上在保护模式中执行，以管理虚拟机 304、306 之间的安全和特权屏障。

标准 VM 304 可包括在 VMX 模式的最高特权处理器环（例如，0D）上执行的操作系统 308 和在 VMX 模式的较低的特权处理器环（例如，3D）上执行的一个或者多个应用程序 310。由于监视器 302 执行于其中的

处理器环具有比操作系统 308 执行于其中的处理器环具有更高的特权，所以操作系统 308 并不具有对计算设备 100 的绝对控制权，而是受到监视器 302 的控制和约束。具体而言，监视器 302 可防止操作系统 308 及其应用程序 310 访问受保护存储器 116 以及固定令牌 110。

监视器 302 可对内核 312 进行一种或者多种测量，例如对内核代码的散列，以获取一个或者多个量度，监视器 302 可以使固定令牌利用可信内核 312 的量度扩展被标识的 PCR 寄存器 210，以及可以将量度记录在存储于受保护存储器 116 内的相关的 PCR 的日志中。另外，监视器 302 可以在受保护存储器 116 中建立可信 VM 306 并在所建立的可信 VM 306 中装入可信内核 312。

类似地，可信内核 312 可以对小应用程序或应用程序 314 进行一种或者多种测量，例如对小应用程序代码的散列，以获取一个或者多个量度。通过监视器 302，可信内核 312 然后可以使固定令牌 110 利用小应用程序 314 的量度扩展被标识 PCR 寄存器 210。可信内核 312 还可以将量度记录在存储于受保护存储器 116 内的相关的 PCR 的日志中。另外，可信内核 312 可以在受保护存储器 116 的所建立的可信 VM 306 中装入可信小应用程序 314。

响应于创立图 3 的可信环境 300，计算设备 100 还可以记录监视器 302、处理器 $102_1...102_P$、芯片组 104、BIOS 固件（未示出）和/或计算设备 100 的其他硬件/软件部件的量度。另外，计算设备 100 可以响应于例如系统启动、应用程序请求、操作系统请求等的各种事件创立可信环境 300。

现在参照图 4，示出了可以被用于本地证明的被密封的密钥二进制大对象 400 和受保护密钥二进制大对象 402。如所描绘的，被密封的密钥二进制大对象 400 可以包括一个或者多个完整性数据区 404 和一个或者多个加密数据区 406。完整性数据区 404 可以包括公共密钥 408、密封记录 410，并且可能还有其他非敏感数据，例如辅助标识二进制大对象和/或加载二进制大对象的密钥的二进制大对象头。另外，加密数据区 406 可包括使用授权数据 412、私有密钥 414 以及摘要值 416。完整性数据区 404 的

密封记录 410 可以表明非对称密钥对 408、414 对哪些 PCR 寄存器 210、相应的量度、证据值以及可能的其他敏感数据密封。另外，摘要值 416 可证明完整性数据区 404 的数据并还可证明加密数据区 406 的数据，以帮助防止通过改变被密封的密钥二进制大对象 400 的一个或者多个部分来获取对加密数据区 406 数据的访问的攻击。在一个实施例中，摘要值 416 可通过对完整性数据区 404、使用授权数据 412 和私有密钥 414 进行散列来生成。在一个实施例中，数据以纯文本或者不加密的形式被存储在完整性数据区 404 中，这样使得完整性数据区的数据被读取或者改变而不需要密钥来解密数据。另外，在一个实施例中加密数据区 406 的数据利用固定令牌 110 的公共密钥 206 被加密。如参照图 6 所详细描述的，没有与固定令牌 110 建立会话以使用对应于被用来对数据加密的公共密钥 206 的私有密钥 206，请求部件就不能成功地将被密封的密钥二进制大对象 400 的非对称密钥对 408、414 加载到固定令牌 110 中。另外，没有向固定令牌 110 提供对于被密封的密钥二进制大对象 400 的使用授权数据 412 或者对具有使用授权数据 412 的证明以及满足了由密封记录 410 所规定的标准的环境，请求部件就不能成功地加载非对称密钥对 408、416。

受保护密钥二进制大对象 402 可以包括一个或者多个完整性数据区 418 和一个或者多个加密数据区 420。完整性数据区 418 可以包括非敏感数据，例如辅助标识二进制大对象的二进制大对象头。另外，加密数据区 420 可以包括使用授权数据 422、被密封的密钥二进制大对象 400 和摘要值 424。摘要值 424 可证明完整性数据区 418 的数据并还可证明加密数据区 420 的数据，以帮助防止通过改变受保护密钥二进制大对象 402 的一个或者多个部分来获取对加密数据区 420 数据的访问的攻击。在一个实施例中，摘要值 424 可通过对完整性数据区 418、被密封的密钥二进制大对象 400 以及使用授权数据 422 进行散列而生成。在一个实施例中，数据以纯文本或者非加密的形式被存储于完整性数据区 418 中，这样使得完整性数据区的数据被读取或者改变而不需要密钥来解密数据。另外，在一个实施例中利用可移动令牌 112 的公共密钥 216 对加密数据区 420 的数据加密。如参照图 6 所详细描述的，没有与可移动令牌 112 建立会话以使用对应的

私有密钥 216，请求部件就不能成功地从受保护密钥二进制大对象 402 获取被密封的密钥二进制大对象 400。另外，没有向可移动令牌 112 提供对于受保护密钥二进制大对象 402 的使用授权数据 422 或者具有使用授权数据 422 的证据，请求部件就不能成功地获取被密封的密钥二进制大对象 400。

现在参照图 5 和图 6，示出了创建受保护密钥二进制大对象 402 的方法和使用被密封的密钥二进制大对象的方法。一般，图 5 和图 6 的方法由请求者启动。为了简化下面的描述，假设请求者是监视器 302。但是，请求者可以是例如在监视器 302 允许下的可信内核 312 和/或可信小应用程序 314 的其他模块。另外，以下描述假设请求者和令牌 110、112 已经具有标识存储于受保护存储器 204、216 中的密钥 206、218 的一个或者多个密钥句柄和相关的使用授权数据。例如，作为以前执行的密钥创建和/或密钥加载命令的结果，请求者和令牌 110、112 可以已经获取了这些信息。具体而言，以下描述假设请求者能够成功地建立会话以使用令牌 110、112 的密钥对。但是，应该认识到如果请求者没有被授权使用密钥对，则请求者将不能建立会话，从而将不能使用这样的密钥对生成对应的密钥二进制大对象并且将不能加载利用这样的密钥对创建的密钥二进制大对象的密钥对。

图 5 中示出了生成图 4 的被密封的密钥二进制大对象的方法。在框 500 中，监视器 302 和固定令牌 110 可为固定令牌 110 的非对称密钥对建立会话，所述非对称密钥对包括存储于固定令牌 110 的受保护存储器 204 中的私有密钥 206 和对应的公共密钥 206。在框 502 中，监视器 302 可通过所建立的会话请求固定令牌 110 创建被密封的密钥二进制大对象 400。具体而言，监视器 302 可以向固定令牌 110 提供对于被密封的密钥二进制大对象 400 的使用授权数据 412。另外，监视器 302 可以向固定令牌 110 提供标识了固定令牌 110 将被密封的密钥二进制大对象 400 的密钥 408、414 密封到其中的 PCR 寄存器 210 的一个或多个索引或者标识，并可向固定令牌 110 提供预期被存储于被标识的 PCR 寄存器 210 中的量度。

在框 504 中，固定令牌 110 可以创建并返回所请求的被密封的密钥二

进制大对象 400。具体而言，固定令牌 110 可以生成包括了私有密钥 414 和对应的公共密钥 408 的非对称密钥对 408、414，并可以将非对称密钥对 408、414 存储于其受保护存储器 204 中。另外，固定令牌 110 可将非对称密钥对 408、414 以及使用授权数据 412 密封到由被监视器 302 标识的 PCR 寄存器 210 的量度所规定的环境。密封的结果是，固定令牌 110 可生成标识了 PCR 寄存器 210 的密封记录 410、被标识的 PCR 寄存器 210 的量度、证据值以及证明非对称密钥对 408、414、使用授权数据 412 和密封记录 410 的摘要值 416。固定令牌 110 还可通过利用所建立的会话的公共密钥 206，对被密封的密钥二进制大对象 400 的私有密钥 414、使用授权数据 412、摘要值 416 以及任何其他敏感数据加密，来创建被密封的密钥二进制大对象 400 的加密数据区 406。通过利用会话的公共密钥 206 创建加密数据区 406，固定令牌 110 可以防止对该加密数据区 406 的数据的访问，因为这些数据只可利用固定令牌 110 控制之下的对应的私有密钥 206 来解密。固定令牌 110 然后可将所请求的被密封的密钥二进制大对象 400 返回给监视器 302。

在框 506 中，监视器 302 和可移动令牌 112 可以为包括了存储于可移动令牌 112 的受保护存储器 216 中的私有密钥 218 和对应的公共密钥 218 的非对称密钥对建立会话。在框 508 中，监视器 302 可以通过所建立的会话请求可移动令牌 112 从被密封的密钥二进制大对象 400 生成具有使用授权数据 422 的受保护密钥二进制大对象 402。具体而言，监视器 302 可以向可移动令牌 112 提供被密封的密钥二进制大对象 400 和使用授权数据 422。

在框 510 中，可移动令牌 112 可以创建并返回所请求的受保护密钥二进制大对象 402。具体而言，可移动令牌 112 可将使用授权数据 422 和被密封的密钥二进制大对象 400 密封到可移动令牌 112。密封的结果是，可移动令牌 112 可以生成证明使用授权数据 422 和被密封的密钥二进制大对象 400 的摘要值 424。可移动令牌 112 还可以通过利用所建立的会话的公共密钥 218，对受保护密钥二进制大对象 402 的使用授权数据 422、被密封的密钥二进制大对象、摘要值 424 以及任何其他敏感数据加密，来创建

加密数据区 420。通过利用会话的公共密钥 218 创建加密数据区 420，可移动令牌 112 可防止对加密数据区 420 的数据的访问，因为这些数据只可利用可移动令牌 112 控制之下的对应的私有密钥 218 来解密。可移动令牌 112 然后可将所请求的受保护密钥二进制大对象 402 返回给监视器 302。

现在参照图 6，示出了加载受保护密钥二进制大对象 402 的非对称密钥对 408、414 的方法。在框 600 中，监视器 302 和可移动令牌 112 可为被用来创建受保护密钥二进制大对象 402 的可移动令牌 112 的非对称密钥对建立会话。在框 602 中，监视器 302 可请求可移动令牌 112 返回存储于受保护密钥二进制大对象 402 中的被密封的密钥二进制大对象 400。为此，监视器 302 可以向可移动令牌 112 提供受保护密钥二进制大对象 402 和认证代码，该认证代码提供了拥有对受保护密钥二进制大对象 402 的使用授权数据 422 或者具有对受保护密钥二进制大对象 402 的使用授权数据 422 的知识的证据。监视器 302 可以若干不同的方式向可移动令牌 112 提供认证代码。在一个实施例中，监视器 302 可简单地利用所建立的会话的公共密钥 218 对使用授权数据 422 的拷贝加密，并向可移动令牌 112 提供其使用授权数据 422 的加密拷贝。

在另一个实施例中，监视器 302 可生成提供了拥有使用授权数据 422 的证据和对请求的一个或者多个参数的证明的消息认证代码（MAC）。具体而言，监视器 302 可以向可移动令牌 112 提供 MAC，该 MAC 是通过对包括或者基于第二个使用授权数据的共享秘密和包括了请求的一个或者多个参数的消息应用 HMAC 算法而得到的。在题为“HMAC：用于消息认证的加密钥散列（Keyed-Hashing for Message Authentication）”的请求注释（RFC）2104 中详细说明了 HMAC 算法。HMAC 算法主要基于共享秘密和被传送的消息利用密码散列函数，例如 MD5 或者 SHA-1 算法，来生成 MAC。在一个实施例中，监视器 302 和可移动令牌 112 可生成用于 HMAC 计算的共享秘密，该计算基于第二个使用授权数据和由监视器 302 和可移动令牌 112 为所建立的会话而生成的滚动现时标志。此外，监视器 302 可生成请求的参数的一个或者多个散列并利用所计算的共享秘密和参数散列作为消息通过 HMAC 算法计算 MAC。

在框 604 中，可移动令牌 112 可以验证受保护密钥二进制大对象 402 和对被密封的密钥二进制大对象 400 的请求。在一个实施例中，可移动令牌 112 可计算可移动令牌 112 期望从监视器 302 接收的认证代码。具体而言，可移动令牌 112 可对受保护密钥二进制大对象 402 解密以获取受保护密钥二进制大对象 402 的被密封的密钥二进制大对象 400 和使用授权数据 422。可移动令牌 112 然后可以使用从请求中接收到的参数和从受保护密钥二进制大对象 402 获取的使用授权数据 422，以与监视器 302 同样的方式，计算认证代码或者 MAC。响应于确定了所计算的认证代码或 MAC 与从监视器 302 接收到的认证代码或 MAC 不具有预定的关系（例如，相等），在框 606 中，可移动令牌 112 可返回出错消息，可关闭所建立的会话，可从可移动令牌 112 中擦去受保护密钥二进制大对象 402 和相关的数据，并且可停用可移动令牌 112。另外，在框 604 中可移动令牌 112 可验证受保护密钥二进制大对象 402 没有被改变过。具体而言，可移动令牌 112 可基于使用授权数据 422 和被密封的密钥二进制大对象 400 计算摘要值并可确定所计算的摘要值是否与受保护密钥二进制大对象 402 的摘要值 424 具有预定关系（例如，相等）。响应于确定了所计算的摘要值不具有预定关系，在框 604 中可移动令牌 112 可返回出错消息，可关闭所建立的会话，可从可移动令牌 112 中擦去受保护密钥二进制大对象 402 和相关的数据，并且可停用可移动令牌 112。

响应于确定了请求是有效的，在框 608 中可移动令牌 112 可向监视器 302 提供被密封的密钥二进制大对象 400。在框 610 中，监视器 302 和固定令牌 110 然后可为被用来创建被密封的密钥二进制大对象 400 的固定令牌 110 的非对称密钥建立会话。在框 612 中，监视器 302 可请求固定令牌 110 加载被密封的密钥二进制大对象 400 的非对称密钥对 408、414。为此，监视器 302 可向固定令牌 110 提供被密封的密钥二进制大对象 400 和认证代码或 MAC，所述认证代码或 MAC 提供拥有与被密封的密钥二进制大对象 400 相关的使用授权数据 412 或具有与被密封的密钥二进制大对象 400 相关的使用授权数据 412 的知识的证据。在一个实施例中，监视器 302 可向固定令牌 110 提供 MAC，该 MAC 是通过 HMAC 计算得到的，所述

HMAC 计算以与上述参照框 602 所描述的相同的方式使用了基于使用授权数据 412 的共享秘密。

在框 614 中，固定令牌 110 可验证加载被密封的密钥二进制大对象 400 的非对称密钥对 408、414 的请求。在一个实施例中，固定令牌 110 可计算固定令牌 110 期望从监视器 302 接收的认证代码。具体而言，固定令牌 110 可利用所建立的会话的私有密钥 206 对被密封的密钥二进制大对象 400 解密以获取被密封的密钥二进制大对象 400 的非对称密钥对 408、414、使用授权数据 412、密封记录 410 以及摘要值 416。固定令牌 110 然后可以使用从请求接收到的参数和从第一被密封的密钥二进制大对象获取的第一个使用授权数据，以与监视器 302 同样的方式，计算认证代码或 MAC。响应于确定了所计算的认证代码或 MAC 与从监视器 302 接收到的认证代码或 MAC 不具有预定关系（例如，相等），在框 616 中固定令牌 110 可返回出错消息，可关闭所建立的会话，可从固定令牌 110 上擦去第一个被密封的密钥二进制大对象和相关的数据，并可停用可移动令牌 112。另外，在框 614 中固定令牌 110 可以验证被密封的二进制大对象 400 没有被改变过。具体而言，固定令牌 110 可基于使用授权数据 412、非对称密钥对 408、414 以及密封记录 410 计算摘要值，并可确定所计算的摘要值是否与被密封的密钥二进制大对象 400 的摘要值 416 具有预定关系（例如，相等）。响应于确定了所计算的摘要值不具有预定关系，在框 616 中固定令牌可返回出错消息，可关闭所建立的会话，可从固定令牌 110 上擦去被密封的密钥二进制大对象和相关的数据，并可停用可移动令牌 112。

在框 618 中，固定令牌 110 还可验证环境 300 适于加载被密封的密钥二进制大对象 400 的非对称密钥 408。具体而言，固定令牌 110 可确定密封记录 410 的量度是否与 PCR 寄存器 210 的量度具有预定关系（例如，相等）并确定密封记录 410 的证据值是否表明固定令牌 110 创建了被密封的密钥二进制大对象 400。响应于确定了密封记录 410 的量度与 PCR 寄存器 210 不具有预定关系或者确定了固定令牌 110 没有创建被密封的密钥二进制大对象 400，在框 616 中，固定令牌可返回出错消息，可关闭所建立的

会话，可从固定令牌 110 上擦去被密封的密钥二进制大对象和相关的数据，并可停用可移动令牌 112。

响应于确定了请求和环境是有效的，在框 620 中，固定令牌 110 可向监视器 302 提供被密封的密钥二进制大对象 400 的公共密钥 408 和引用存储于固定令牌 110 的受保护存储器 204 中的非对称密钥对 408、414 的密钥句柄。监视器 302 以后可将该密钥句柄提供给固定令牌 110 以建立会话来使用由该密钥句柄标识的非对称密钥对 408、414。

图 5 和图 6 的方法一般结果是建立非对称密钥对，该密钥对仅当可移动令牌 112 出现并且,可选地,环境 300 如由 PCR 寄存器 210 的量度所表明的那样合适的时候，才可被使用。计算设备 100 和/或远程代理 $118_1...118_R$ 从而可基于被密封的密钥二进制大对象 400 的密钥 408 是否被固定令牌 110 成功地加载和/或解密秘密的能力来确定可移动令牌 112 的用户出现，所述秘密只可利用被密封的密钥二进制大对象 400 的密钥 408 被解密。

另外，用户可使用可移动令牌 112 来确定计算设备 100 满足被密封的密钥二进制大对象 400 的密钥被密封于其中的环境的标准。具体而言，用户可基于被密封的密钥二进制大对象 400 的密钥 408 是否被固定令牌 110 成功地加载和/或解密秘密的能力来确定计算设备 100 满足环境标准，所述秘密只可利用被密封的密钥二进制大对象 400 的密钥 408 被解密。

计算设备 100 可响应于执行机器可读介质的指令进行图 5 和图 6 所示的所有方法或者其一部分，其中机器可读介质是例如只读存储器（ROM）、随机访问存储器（RAM）、磁盘存储介质、光存储介质、闪存设备和/或电、光、声或其他形式的传播信号，例如，载波、红外信号、数字信号、模拟信号的介质。此外，尽管图 5 和图 6 的方法被示为系列操作，然而在一些实施例中，计算设备 100 可以并行或按不同次序来进行该方法的各种所示的操作。

尽管本发明的某些特征已经参考示例实施例被描述，然而该描述并不是用来在限定的意义上被解释。示例实施例以及本发明其他实施例的对于与本发明相关的领域的技术人员是显而易见的各种修改，被视为落在本发明的精神和范围之内。

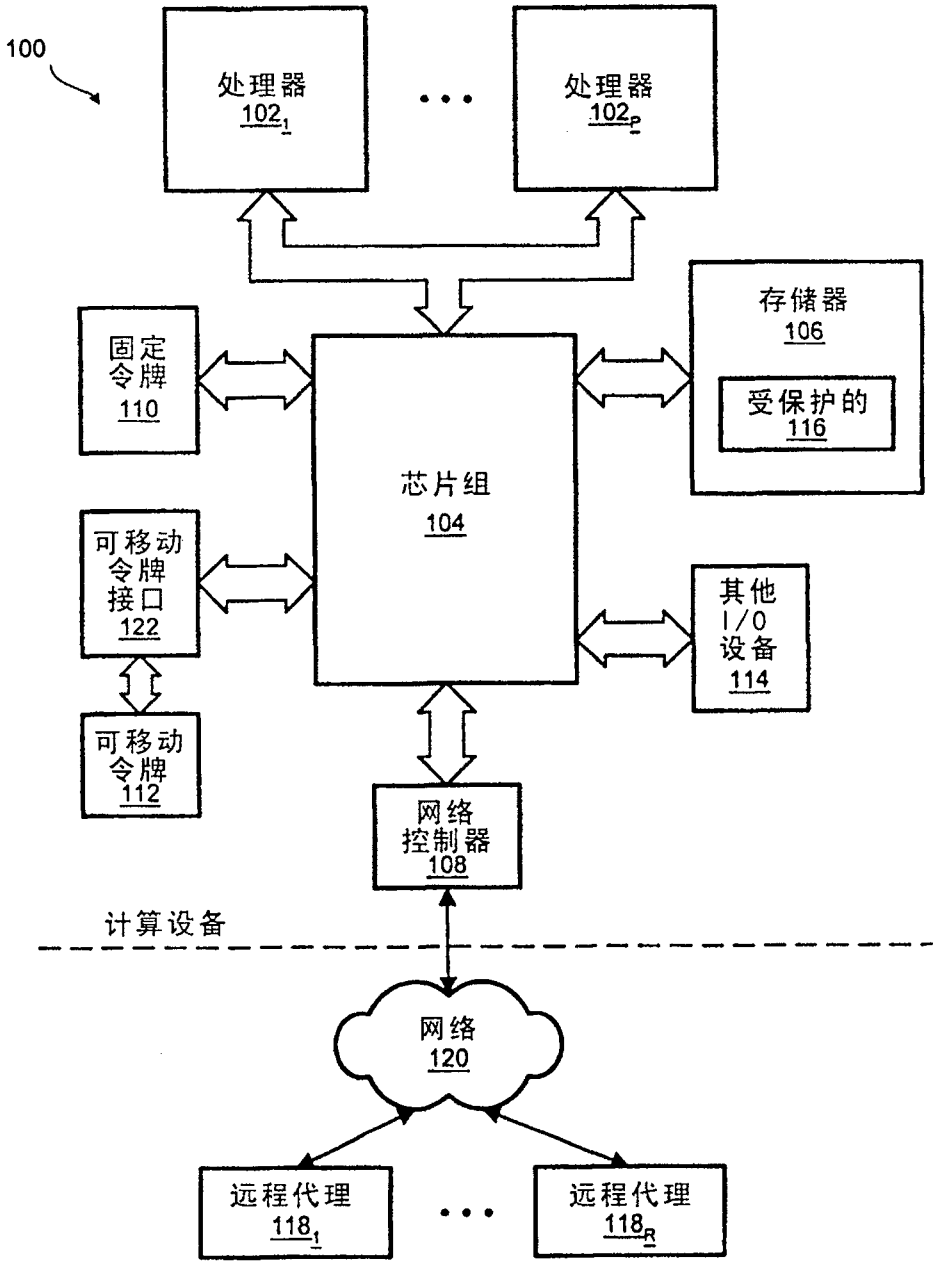

100
处理器
102$_1$
处理器
102$_P$
存储器
106
受保护的
116
固定
令牌
110
芯片组
104
可移动
令牌
接口
122
其他
I/O
设备
114
可移动
令牌
112
网络
控制器
108
计算设备
网络
120
远程代理
118$_1$
远程代理
118$_R$

图1

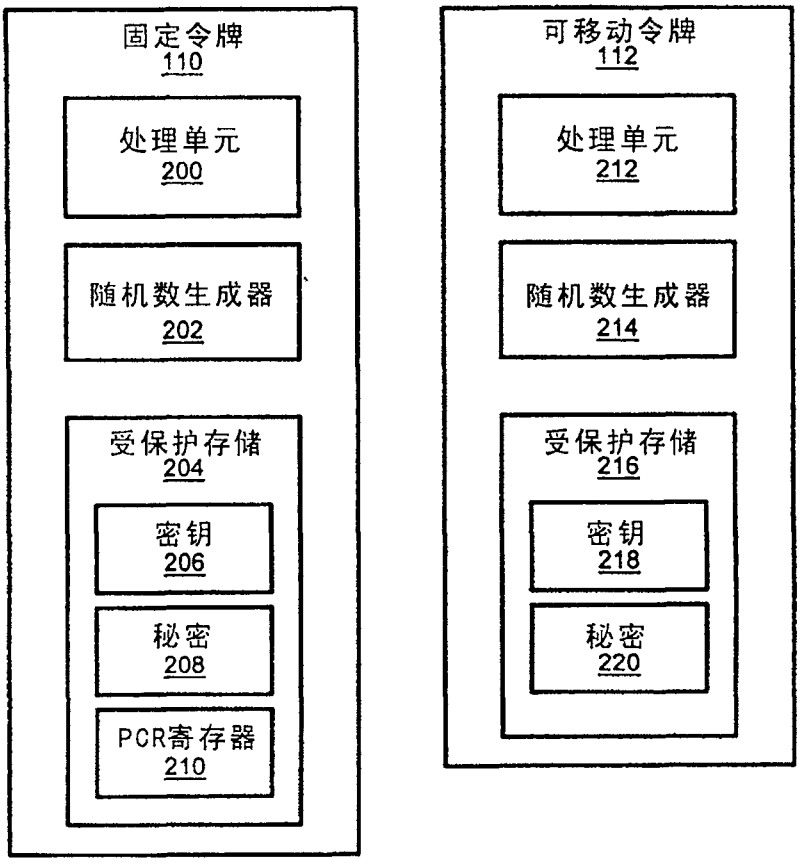

固定令牌
110
处理单元
200
随机数生成器
202
受保护存储
204
密钥
206
秘密
208
PCR寄存器
210
可移动令牌
112
处理单元
212
随机数生成器
214
受保护存储
216
密钥
218
秘密
220

图2

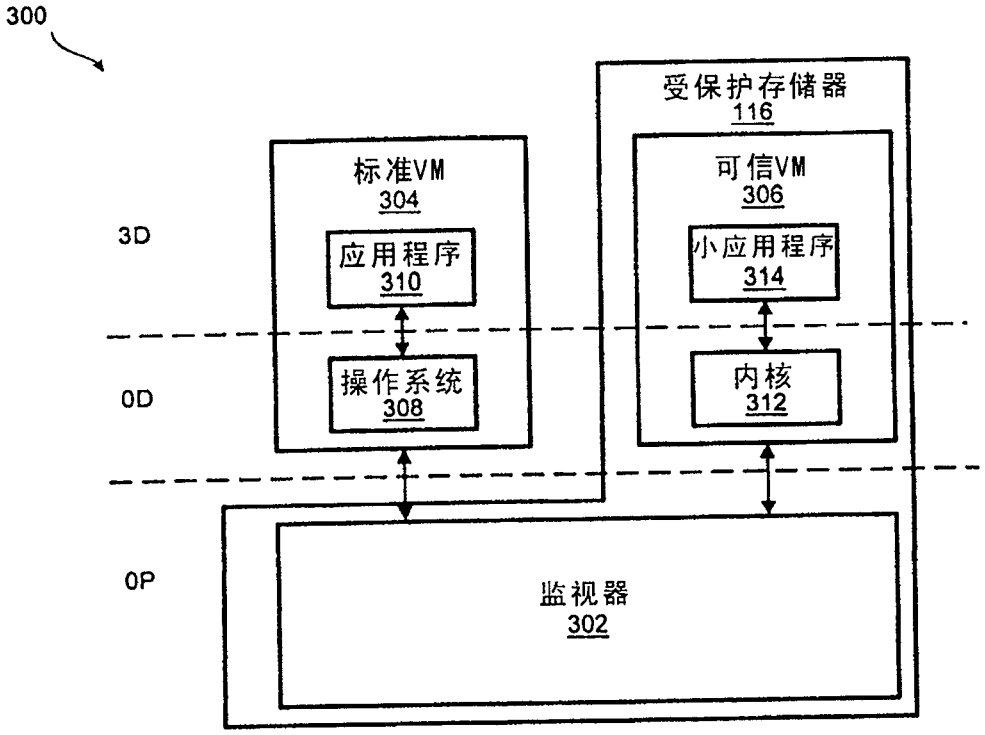

300
受保护存储器
116
标准VM
304
可信VM
306
3D
应用程序
310
小应用程序
314
0D
操作系统
308
内核
312
0P
监视器
302

图3

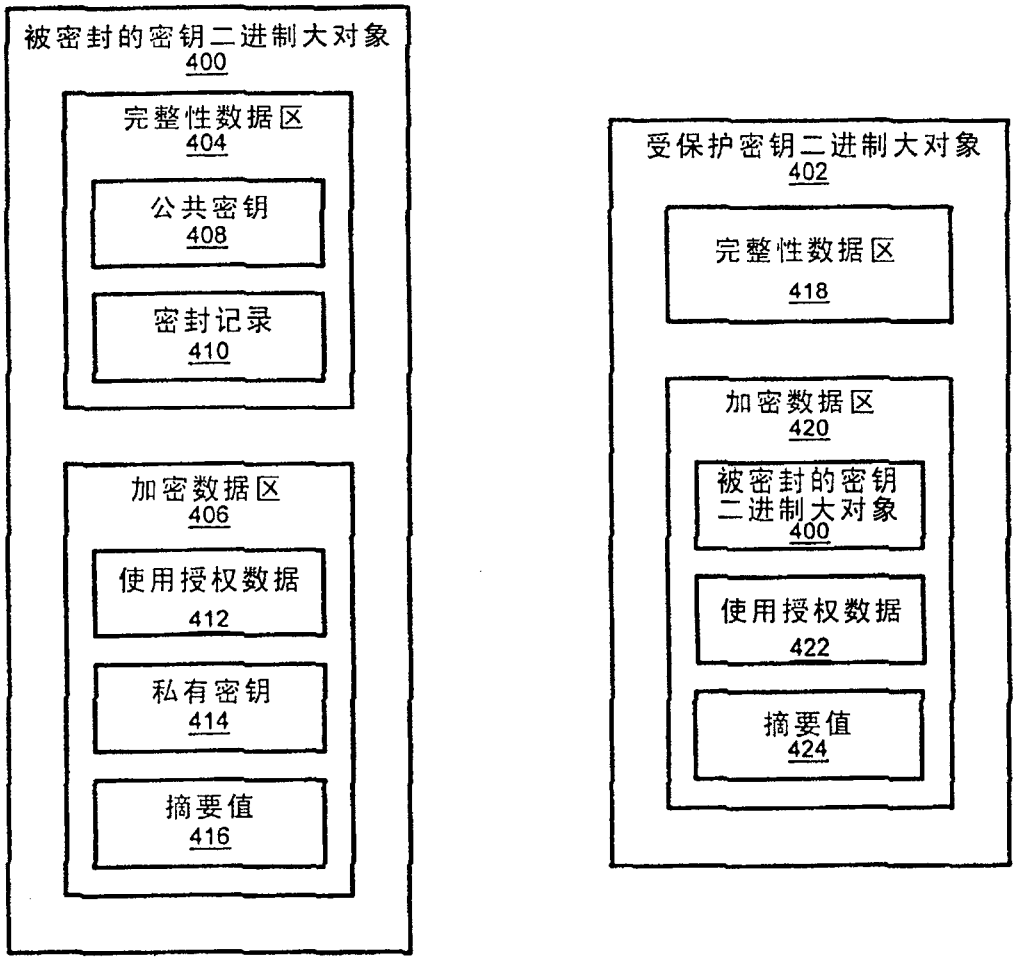

被密封的密钥二进制大对象
400
完整性数据区
404
公共密钥
408
密封记录
410
加密数据区
406
使用授权数据
412
私有密钥
414
摘要值
416
受保护密钥二进制大对象
402
完整性数据区
418
加密数据区
420
被密封的密钥二进制大对象
400
使用授权数据
422
摘要值
424

图4

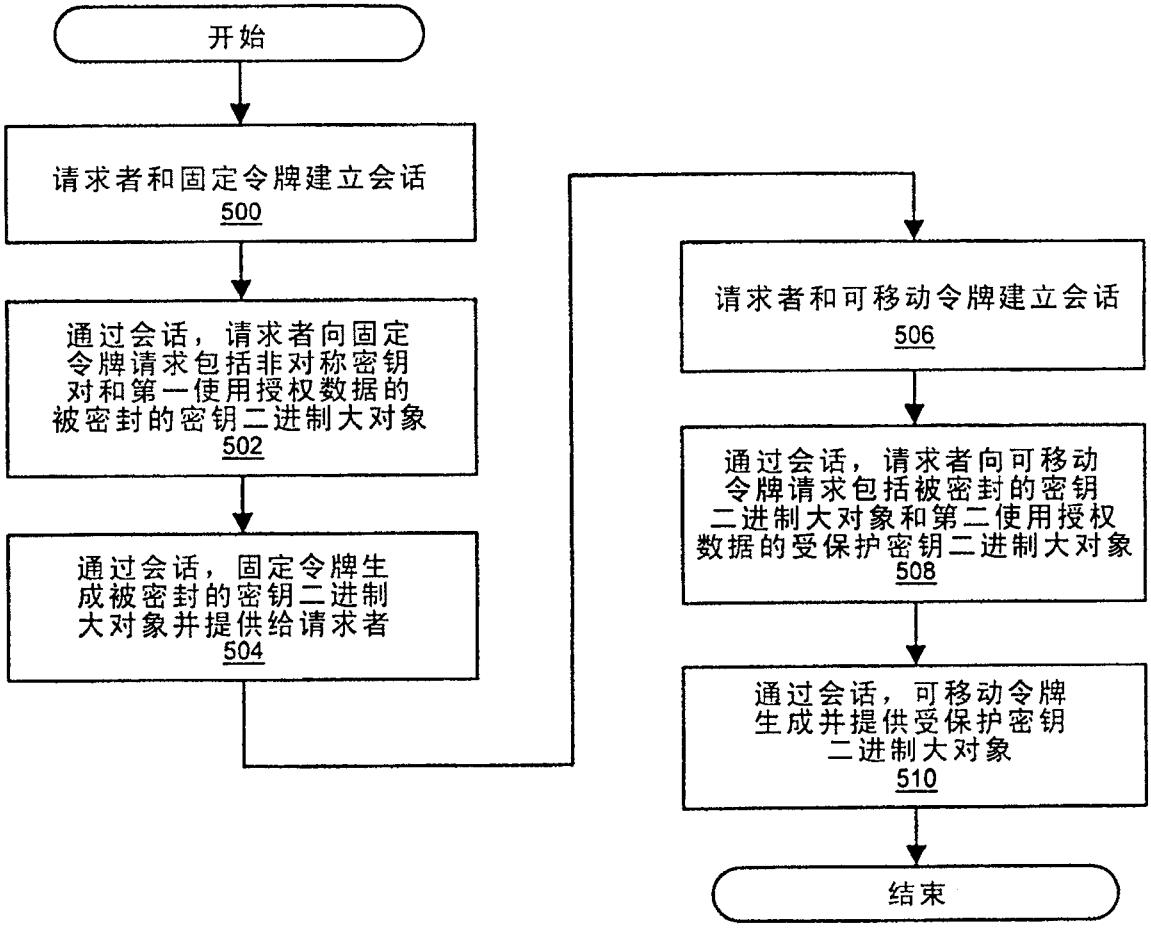

开始
请求者和固定令牌建立会话
500
通过会话，请求者向固定令牌请求包括非对称密钥对和第一使用授权数据的被密封的密钥二进制大对象
502
通过会话，固定令牌生成被密封的密钥二进制大对象并提供给请求者
504
请求者和可移动令牌建立会话
506
通过会话，请求者向可移动令牌请求包括被密封的密钥二进制大对象和第二使用授权数据的受保护密钥二进制大对象
508
通过会话，可移动令牌生成并提供受保护密钥二进制大对象
510
结束

图5

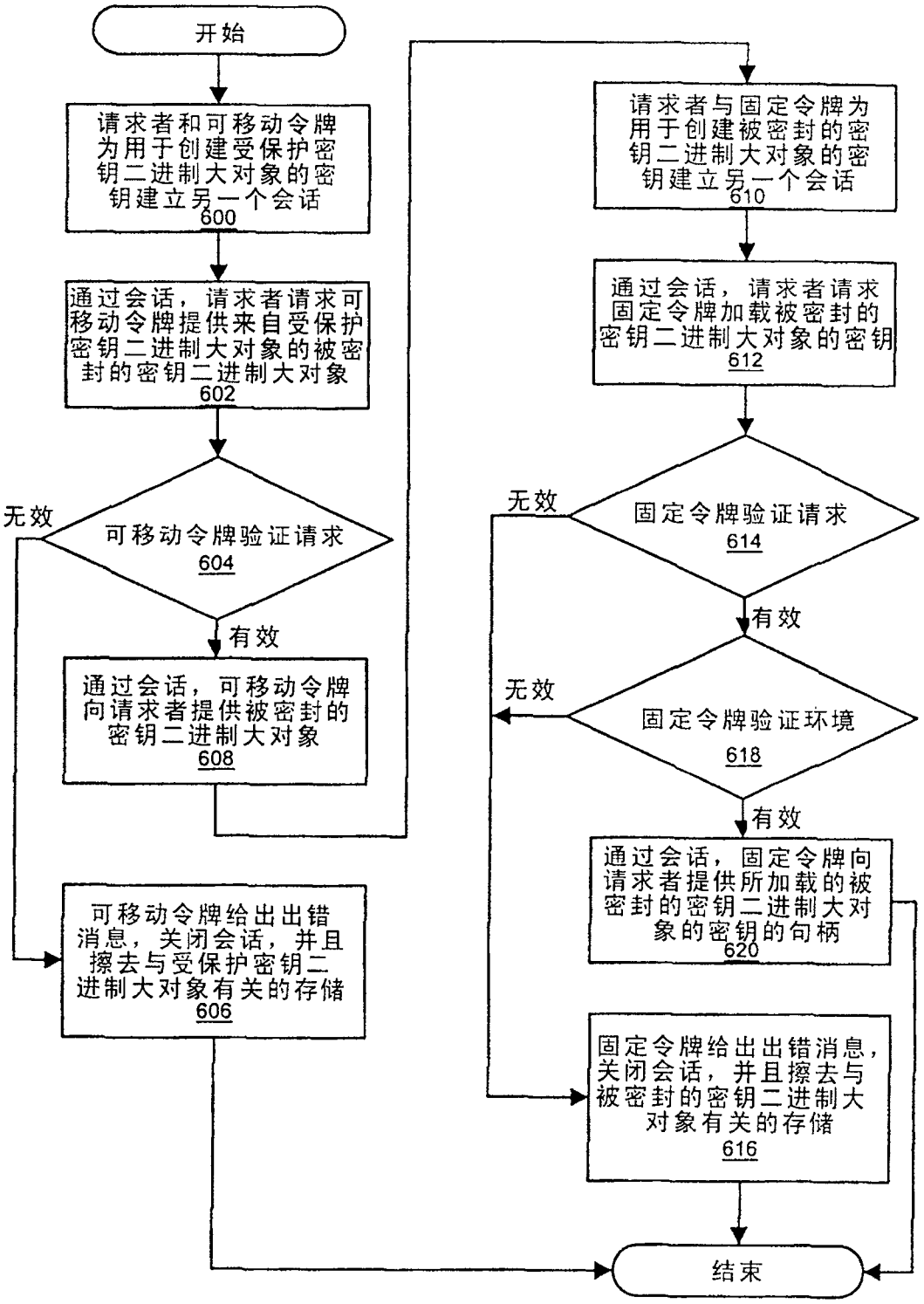

开始
请求者和可移动令牌为用于创建受保护密钥二进制大对象的密钥建立另一个会话
600
通过会话，请求者请求可移动令牌提供来自受保护密钥二进制大对象的被密封的密钥二进制大对象
602
可移动令牌验证请求
604
无效
有效
通过会话，可移动令牌向请求者提供被密封的密钥二进制大对象
608
可移动令牌给出出错消息，关闭会话，并且擦去与受保护密钥二进制大对象有关的存储
606
请求者与固定令牌为用于创建被密封的密钥二进制大对象的密钥建立另一个会话
610
通过会话，请求者请求固定令牌加载被密封的密钥二进制大对象的密钥
612
固定令牌验证请求
614
无效
有效
固定令牌验证环境
618
无效
有效
通过会话，固定令牌向请求者提供所加载的被密封的密钥二进制大对象的密钥的句柄
620
固定令牌给出出错消息，关闭会话，并且擦去与被密封的密钥二进制大对象有关的存储
616
结束

图6