

## (12) 发明专利申请

(10) 申请公布号 CN 102986161 A

(43) 申请公布日 2013. 03. 20

(21) 申请号 201180035364. 8

(72) 发明人 M. 迈德尔 S. 泽尔茨萨姆

(22) 申请日 2011. 06. 22

(74) 专利代理机构 中国专利代理(香港)有限公司 72001

(30) 优先权数据

102010027586. 7 2010. 07. 19 DE

代理人 杜荔南 刘春元

(85) PCT申请进入国家阶段日

2013. 01. 18

(51) Int. Cl.

H04L 9/08 (2006. 01)

(86) PCT申请的申请数据

PCT/EP2011/060487 2011. 06. 22

(87) PCT申请的公布数据

W02012/010380 DE 2012. 01. 26

(71) 申请人 西门子公司

地址 德国慕尼黑

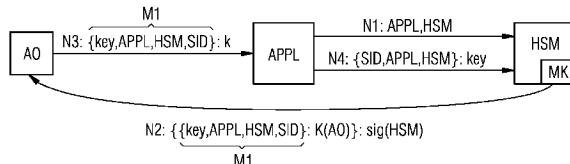
权利要求书 2 页 说明书 6 页 附图 2 页

## (54) 发明名称

用于对应用进行密码保护的方法

## (57) 摘要

本发明涉及一种用于对应用(APPL)进行密码保护的方法，其中应用(APPL)被分配给应用所有者(AO)并且在计算中心中实施，该计算中心由外部的不属于应用所有者(AO)的服务运营商管理，其中在计算中心中设置应用所有者(AO)的安全模块，在该安全模块上存储应用所有者(AO)的私有密码材料(MK)。本发明方法的特征在于，采用安全模块(HSM)与应用所有者(AO)之间的第一安全通道以及应用所有者(AO)与应用(APPL)之间的第二安全通道，通过它们传送或者由安全模块(HSM)或者由应用所有者(AO)生成的密码秘密。密码秘密通过这些安全通道自动提供给安全模块(HSM)以及应用(APPL)，而服务运营商不具有访问该秘密的可能性。借助秘密(key)可以在安全模块(HSM)中对应用(APPL)进行验证，从而接着可以通过由密码秘密保护的通道将密码材料从安全模块(HSM)传输到应用(APPL)。于是利用所传输的密码材料可以对应用数据加密，其中外部计算中心的服务运营商不具有访问该应用数据的可能性。



1. 一种用于对应用(APPL)进行密码保护的方法,其中应用(APPL)被分配给应用所有者(AO)并且在计算中心中实施,该计算中心由外部的不属于应用所有者(AO)的服务运营管理,其中在计算中心中设置应用所有者(AO)的安全模块(HSM),在该安全模块上存储应用所有者(AO)的私有密码材料(MK),其中:

- 通过应用所有者(AO)的生成装置或者通过安全模块(HSM)生成密码秘密(key);
- 密码秘密(key)通过保护在应用(APPL)与应用所有者(AO)的计算机装置之间的通信的第一安全通道在该计算机装置与安全模块(HSM)之间传送,由此密码秘密(key)对于所述计算机装置和安全模块(HSM)是可接近的;
- 密码秘密(key)通过保护在应用(APPL)与应用所有者(AO)的计算机装置之间的通信的第二安全通道从该计算机装置传送到应用(APPL),由此密码秘密(key)对于应用(APPL)是可接近的;
- 基于对于应用(APPL)和安全模块(HSM)可接近的密码秘密(key)来执行相对于安全模块(HSM)对应用(APPL)的验证,其中在成功的验证之后应用所有者(AO)的密码材料(MK)通过由密码秘密(key)保护的通道从安全模块(HSM)传输到应用(APPL)。

2. 根据权利要求1的方法,其中应用(APPL)的验证按照以下方式进行,即利用对于应用(APPL)可接近的密码秘密(key)对应用(APPL)的信息进行加密并且传送给安全模块(HSM),其中成功验证的条件在于,安全模块(HSM)能够用对于安全模块(HSM)可接近的密码秘密(key)对所述信息解密。

3. 根据权利要求1或2的方法,其中生成会话标识(SID),该会话标识在通过第一安全通道和/或通过第二安全通道传送密码秘密(key)时和/或在验证应用(APPL)的范围中一起传输,其中在该方法执行期间检验该会话标识(SID)是否保持不变。

4. 根据权利要求2和3的方法,其中会话标识是由应用(APPL)在其验证时加密并且被传送给安全模块(HSM)的信息。

5. 根据上述权利要求之一的方法,其中密码秘密(key)由安全模块(HSM)生成并且通过第一安全通道传输给应用所有者(AO)的计算机装置,其中第一安全通道通过以下方式形成,即用服务运营商不能访问的第一加密对第一消息(M1)加密,并且接着将第一消息(M1)传输到应用所有者(AO)的计算机装置,其中第一消息(M1)包含所述密码秘密(key)。

6. 根据权利要求5的方法,其中用安全模块(HSM)的签名(sig(HSM))对被加密的第一消息(M1)进行签名。

7. 根据权利要求5或6的方法,其中用应用所有者(AO)的公共密钥(K(AO))或者用只有应用所有者(AO)和安全模块(HSM)知道的私有密钥执行第一加密。

8. 根据权利要求5至7之一的方法,其中对传输到应用所有者(AO)的计算机装置的加密的第一消息(M1)进行解密并且接着通过第二安全通道传输到应用(APPL),其中第二安全通道通过以下方式形成,即用服务运营商不能访问的第二加密对解密的第一消息(M1)加密并且接着发送到应用(APPL)。

9. 根据上述权利要求之一的方法,其中密码秘密(key)由应用所有者(AO)的生成装置生成并且通过第一安全通道传输到安全模块(HSM),其中第一安全通道通过以下方式形成,即通过服务运营商不能访问的第二加密对第二消息(M2)加密,并且接着将第二消息(M2)传输到安全模块(HSM),其中第二消息(M2)包含所述密码秘密(key)。

10. 根据权利要求 9 的方法, 其中用应用所有者的签名( $\text{sig}(A0)$ )对被加密的第二消息(M2)进行签名。

11. 根据权利要求 9 或 10 的方法, 其中用安全模块(HSM)的公共密钥( $K(HSM)$ )或者用只有应用所有者(A0)和安全模块(HSM)知道的私有密钥执行第二消息(M2)的第二加密。

12. 根据上述权利要求之一的方法, 其中通过应用(APPL)来对第一安全通道建立隧道。

13. 根据权利要求 12 结合权利要求 9 至 11 之一的方法, 其中第一安全通道通过以下方式形成, 即加密的第二消息(M2)与至少密码秘密(key)一起首先通过第二安全通道传输到应用(APPL), 其中该应用(APPL)接着将所接收的加密的第二消息(M2)传输到安全模块。

14. 一种用于对应用(APPL)进行密码保护的系统, 其中该应用(APPL)被分配给应用所有者(A0)并且能在由外部的不属于该应用所有者(A0)的服务运营商管理的计算中心中实施, 其中所述系统包括应用所有者(A0)的设置在计算中心中的安全模块(HSM)以及生成装置和应用所有者的计算机装置, 在所述安全模块上存储应用所有者(A0)的私有密码材料(MK), 其中该系统被构成为, 在应用(APPL)在所述计算中心中实施时执行以下步骤:

- 通过应用所有者(A0)的生成装置或者通过安全模块(HSM)生成密码秘密(key);

- 密码秘密(key)通过保护在应用(APPL)与应用所有者(A0)的计算机装置之间的通信的第一安全通道在该计算机装置与安全模块(HSM)之间传送, 由此密码秘密(key)对于所述计算机装置和安全模块(HSM)是可接近的;

- 密码秘密(key)通过保护在应用(APPL)与应用所有者(A0)的计算机装置之间的通信的第二安全通道从该计算机装置传送到应用(APPL), 由此密码秘密(key)对于应用(APPL)是可接近的;

- 基于对于应用(APPL)和安全模块(HSM)可接近的密码秘密(key)来执行相对于安全模块(HSM)对应用(APPL)的验证, 其中在成功的验证之后应用所有者(A0)的密码材料(MK)能通过由密码秘密(key)保护的通道从安全模块(HSM)传输到应用(APPL)。

15. 根据权利要求 14 的系统, 其被构成为能利用该系统执行根据权利要求 2 至 13 之一的方法。

## 用于对应用进行密码保护的方法

### 技术领域

[0001] 本发明涉及用于对应用进行密码保护的方法和系统。

### 背景技术

[0002] 由现有技术已知在所谓的云计算的范围内通过服务运营商向第三方提供计算性能,所述第三方将所述计算性能用于实施应用。这些应用在此在服务运营商的计算中心上运行,所述计算中心或者可以集中地位于一个地点或者也可以分布式地互连以引入灵活的服务。

[0003] 服务运营商的应用所有者形式的客户对服务运营商不具有能够访问该应用或通过该应用所产生的应用数据的可能性感兴趣,其中该客户想要属于他的应用可以在服务运营商的计算中心上运行。由此必须采取保护措施,利用该保护措施在服务运营商侧对系统管理员屏蔽应用。该屏蔽的措施例如是关键数据的加密,应用将所述关键数据存储在服务运营商的计算中心的相应存储器装置上,尤其是在硬盘上。由此可以防止由计算中心的系统管理员不被察觉地访问该应用的数据。在此问题是用于加密的密码密钥的保管。

[0004] 由现有技术已知所谓的安全模块,尤其是硬件安全模块的形式。安全模块使得可以在更安全的环境中尤其是以芯片卡或安全令牌的形式存储秘密密钥,其中仅能通过验证实现对所存储的密钥的访问。通常,为了进行验证使用所谓的 PIN,该 PIN 必须由安全模块的拥有者输入以访问存储在安全模块上的数据。如果在将应用搁置到外部服务运营商的计算中心上的范围中使用安全模块来存储对应用数据进行加密的密码密钥,则被证明为不利的是在常规的验证中通过 PIN 在每次访问安全模块时都必须手动输入该 PIN。

### 发明内容

[0005] 因此本发明的任务是,通过安全模块保护在外部服务运营商的计算中心中的应用所有者的应用免遭服务运营商的未授权访问,其中可以实现该应用对安全模块的数据的自动的安全的访问。

[0006] 该任务通过根据权利要求 1 的方法或根据权利要求 14 的系统解决。本发明的扩展在从属权利要求中限定。

[0007] 本发明的方法用于对应用进行密码保护,该应用被分配给应用所有者并且在由外部的不属于该应用所有者的服务运营商管理的计算中心中实施。应用所有者在此应当被理解为诸如企业的实体或机构。所述应用属于该实体或机构,尤其是该应用也由该实体或机构开发。在本发明的含义下,术语“计算中心”应当宽泛地理解并且可以包括在一个固定位置或分布在不同位置的一个或多个计算机,其中通过这些计算机提供用于实施计算过程的计算性能。对计算中心的管理又通过实体或机构(尤其是企业)进行,所述实体或机构是服务运营商。由于服务运营商运行该计算中心,因此服务运营商也具有访问该计算中心的管理员权限。

[0008] 在本发明方法的范围中使用安全模块,该安全模块虽然属于应用所有者,但是该

安全模块设置在计算中心中,即该安全模块通过相应的(本地)接口(例如USB)连接到计算中心的计算机。在该安全模块上存储了应用所有者的私有(永久)密码材料(例如私有密钥),所述私有密码材料用于对应用的应用数据进行适当的加密。安全模块在此尤其是被实现为所谓的硬件安全模块,该硬件安全模块由现有技术充分已知。

[0009] 根据本发明,通过应用所有者的生成装置或者通过安全模块生成密码秘密。术语“生成装置”在此应当宽泛地理解并且可以包括在应用所有者的安全的计算环境中的每一个基于软件或硬件实现的单元。密码秘密首先通过保护在应用和应用所有者的计算机装置之间的通信的第一安全通道在所述计算机装置和安全模块之间传送,由此密码秘密对于计算机装置和安全模块是可接近的。这样的第一安全通道例如可以通过用安全模块的公共密钥进行相应的加密来实现,如下面还要详细描述的。与生成装置类似,上面提到的计算机装置是应用所有者的安全计算环境中的硬件或软件形式的任意单元。该单元可以通过相应的接口与应用通信。

[0010] 密码秘密在本发明方法的范围中还通过保护在应用与应用所有者的计算机装置之间的通信的第二安全通道从计算机装置传送到应用,由此该密码秘密对于所述应用是可接近的。在此前提是在应用所有者与应用之间建立第二安全通道。这样的第二安全通道可以毫无问题地实现,因为该应用属于应用所有者,从而按照合适的方式例如可以由应用和应用所有者生成共同的私有密钥以建立第二安全通道。

[0011] 根据本发明,最后基于对于应用和安全模块可接近的密码秘密相对于安全模块来验证应用,其中在成功验证的情况下可通过由密码秘密保护的通道将应用所有者的密码材料从安全模块传输到应用。

[0012] 本发明的方法的特征在于,自动实现在计算中心上运行的应用对应用所有者的密码材料的访问,而计算中心的服务运营商具有读取该密码材料的可能性。这通过使用应用所有者的安全模块来实现,其中通过在中间连接应用所有者条件下的安全通道传送密码秘密,从而该秘密既向应用又向安全模块提供。该秘密然后可以被用于将安全模块的密码材料传输到应用。

[0013] 在本发明方法的特别优选的实施方式中,相对于安全模块验证应用,使得利用对于应用可接近的密码秘密来对应用的信息进行加密并且传送给安全模块,其中成功验证的条件在于,安全模块可以用对于安全模块可接近的密码秘密对所述信息解密。由此通过特别简单的方式执行检验,使得应用以及安全模块都包含相同的密码秘密。

[0014] 在本发明方法的另一个优选实施方式中,尤其是在该方法的开始生成会话标识,该会话标识在通过第一安全通道和 / 或通过第二安全通道传送密码秘密时和 / 或在相对于安全模块验证应用的范围中一起传输。在此,在该方法执行时检验该会话标识是否保持不变。这例如可以通过以下方式进行,即在该方法的开始就产生了会话标识的单元(例如应用或安全模块)检查在稍后的时刻传送给它的会话标识是否与原始生成的会话标识一致。如果不是这样的情况,则优选中断该方法。根据本发明的该变型,实现保护免遭所谓的重放攻击,在该重放攻击中尝试将在早期的会话中使用的秘密引入该方法中。在优选的变型中,还将会话标识用作由应用在其验证时加密并且被传输给安全模块的信息。

[0015] 在本发明方法的另一种实施方式中,密码秘密由安全模块生成并且通过第一安全通道传输给应用所有者的计算机装置,其中第一安全通道通过以下方式形成,即用服务运

营商不能访问的第一加密对第一消息加密，并且接着将第一消息传输到应用所有者的计算机装置，其中第一消息包含所述密码秘密。优选的，在此用安全模块的签名对被加密的第一消息进行签名，从而可以检验第一消息也来自安全模块。在优选的变型中，用应用所有者的公共密钥或者必要时也用只有应用所有者或安全模块知道的私有密钥进行第一加密。

[0016] 在本发明方法的另一变型中，对传输到应用所有者的计算机装置的加密的第一消息进行解密，其中该解密优选通过计算机装置进行。接着第一消息通过第二安全通道被传输到应用，其中第二安全通道通过以下方式形成，即用服务运营商不能访问的第二加密对解密的第一消息加密，并且发送到应用。通过这种方式将密码秘密通过受保护的连接传递到应用，其中该应用拥有对第二加密进行解密的相应密钥。

[0017] 在本发明方法的另一种设计中，密码秘密由应用所有者的生成装置生成并且通过第一安全通道传输到安全模块，其中第一安全通道通过以下方式形成，即通过服务运营商不能访问的第二加密对第二消息加密，并且接着将第二消息传输到安全模块，其中第二消息包含所述密码秘密。优选的，在此用应用所有者的签名对被加密的第二消息进行签名。此外，优先用安全模块的公共密钥或者必要时也用只有应用所有者和安全模块知道的私有密钥进行第二消息的第二加密。

[0018] 在本发明方法的另一个特别优选的实施方式中，通过应用来对第一安全通道建立隧道。也就是说，在第一安全通道的范围内，在中间连接所述应用的条件下进行消息传送，但是其中该应用不具有访问该第一安全通道或其中传送的信息的可能性。在一种特别优选的变型中，被形成隧道的第一安全通道通过以下方式形成，即加密的第二消息与至少密码秘密一起首先通过第二安全通道传输到应用，其中该应用接着将所接收的加密的第二消息传输到安全模块。通过这种方式，既通过第一安全通道又通过第二安全通道实现并行的传输。

[0019] 除了上述方法之外，本发明还涉及一种用于对应用进行密码保护的系统，其中该应用被分配给应用所有者并且可在由外部的不属于该应用所有者的服务运营商管理的计算中心中实施，其中所述系统包括应用所有者的设置在计算中心中的安全模块以及生成装置和应用所有者的计算机装置，在该安全模块上存储应用所有者的私有密码材料。该系统在此被构成为，使得在应用在所述计算中心中执行时实施上述本发明方法或该方法的一种或多种变型。

## 附图说明

[0020] 下面借助附图详细描述本发明的实施例。

[0021] 图 1 示出根据本发明方法的第一实施方式的消息交换的示意图；以及  
图 2 示出根据本发明方法的第二实施方式的消息交换的示意图。

## 具体实施方式

[0022] 下面描述的本发明方法的实施方式涉及对应用 APPL 的密码保护，该应用属于在图 1 和图 2 中通过附图标记 A0 表示的应用所有者。应用所有者在此是应用 APPL 所属的实体或机构，例如企业。例如，应用 APPL 可以是由该应用所有者开发的。通过该应用，应用所有者向其客户提供相应的服务，其中应用所有者不自己实施所述应用来提供该服务，而是

为此操作计算中心,所述应用就在该计算中心上运行。该计算中心由此是由不属于应用所有者 A0 的服务运营商管理的外部单元。因此存在以合适的方式保护应用 APPL 或相应的应用数据免遭服务运营商的未授权访问的需要。为此使用主密钥 MK 形式的私有密钥,利用该私有密钥对通过应用产生的、在计算中心的相应存储器中(例如在计算中心中的硬盘上)的数据进行适当加密。在此要保证,虽然应用能访问主密钥 MK,但是该主密钥被密码地保护以免遭服务运营商的访问。

[0023] 为了提供主密钥 MK,在下面描述的实施方式中使用所谓的硬件安全模块 HSM,该硬件安全模块本身由现有技术已知,其中该安全模块属于应用所有者并且是一种被密码保护的环境,主密钥 MK 就存储在该环境中。硬件安全模块 HSM 设置在计算中心中,即该硬件安全模块以合适的方式与计算中心中的相应计算机通过无线或有线的接口连接,其中对硬件安全模块的密码保护保证对计算中心进行管理的服务运营商不具有访问在该硬件安全模块上存储的数据的可能性。

[0024] 本发明方法的目的现在是在应用所有者 A0 的控制下实现对主密钥 MK 的自动访问,从而应用 APPL 接收主密钥以用于对数据加密,而计算中心的服务运营商不具有访问主密钥的可能性。为了实现这一点,执行相对于硬件安全模块 HSM 对应用 APPL 的可靠验证,其中该验证也被保护免遭在计算中心中具有管理员权限的攻击者。在此边界条件是,对应用的验证应当在硬件安全模块上自动地、即没有人员干预地进行。通过该边界条件保证应用在系统崩溃之后马上又可以自动启动。

[0025] 在下面,应用所有者 A0 应被理解为被分配给应用所有者的相应安全的计算机环境。也就是说,当下面的步骤通过应用所有者执行或与应用所有者通信时,意味着通过软件或硬件实现的相应的计算机装置参与方法步骤或通信,该计算机装置的一部分就是安全的计算机环境。下面还要以下条件为前提:在应用正在运行中在应用所有者 A0 与应用 APPL 之间存在安全通道,应用所有者 A0 可以通过该安全通道与应用 APPL 交换消息,从而没有第三方、即使是计算中心的系统管理员也不能读取该消息。这样的在权利要求的意义上与第二安全通道相应的安全通道可以毫无问题地在应用所有者 A0 与应用 APPL 之间实现,因为该应用属于应用所有者并且由此是该应用所有者所知道的。因此能以适当的方式在该应用在计算中心中运行结束时生成相应的、仅由应用所有者和应用知道的秘密,然后为了在应用所有者与应用之间建立安全通道使用该秘密。

[0026] 下面借助图 1 和图 2 描述本发明方法的两个变型,其中在方法的范围中交换相应的消息 N1, N2, N3 和 N4。在此,符号 {N}:k 表示位于大括号中的消息 N 被用相应的密钥 k 或相应的签名 k 加密或签名。此外在图 1 和图 2 的范围中使用以下表示:

-sig(HSM) :硬件安全模块 HSM 的签名,利用 HSM 的相应私有密钥;

-sig(A0) :应用所有者 A0 的签名,利用 A0 的相应私有密钥;

-K(A0) :应用所有者 A0 的公共密钥;

-K(HSM) :硬件安全模块 HSM 的公共密钥;

-k: 用于对应用所有者 A0 与应用 APPL 之间的通信加密的密钥;

-key: 在应用 APPL 与硬件安全模块 HSM 之间的共同秘密,该秘密在下面描述的本发明变型的范围中生成和交换;

-SID: 在该方法开始时生成的会话标识。

[0027] 只要附图标记 APPL 和 HSM 在所交换的消息内使用，则它们就表示应用或硬件安全模块的单义标识符，例如应用的哈希码或硬件安全模块的序列号。

[0028] 在图 1 的实施方式的范围中，由应用 APPL 通过消息 N1 发起消息交换，所述消息 N1 由应用 APPL 发送到硬件安全模块 HSM 并且包含应用 APPL 和硬件安全模块 HSM 的标识符。接着硬件安全模块生成对称密钥“key”，该对称密钥在该方法结束时表示应用与硬件安全模块之间的共同秘密。该对称密钥通过基于消息 N2 的第一安全通道由硬件安全模块 HSM 发送到应用所有者 A0。在消息 N2 中包含消息 M1，该消息 M1 包含密钥 key、应用 APPL 和安全模块 HSM 的标识符以及会话标识 SID。该会话标识由 HSM 产生。消息 M1 在此被用应用所有者的公共密钥 K(A0) 加密并且还用硬件安全模块的签名 sig(HSM) 签名。基于消息 M2 保证所生成的密钥 key 不能被计算中心的系统管理员读取，因为系统管理员不能访问应用所有者的用于对消息 M1 解密的私有密钥。通过用 sig(HSM) 来对消息 M2 签名，应用所有者 A0 可以确信该消息以及由此还有密钥 key 都来自安全模块 HSM。

[0029] 在接收到消息 N2 之后，应用所有者 A0 将消息 N3 通过在应用所有者 A0 和应用 APPL 之间建立的安全通道发送到应用。消息 N3 在此包含事先在消息 N2 的范围内传送的消息 M1，该消息 M1 现在通过对 A0 与 APPL 之间的通信进行保护的相应密钥 k 来加密。通过应用所有者 A0 与应用 APPL 之间的安全通道，保证只有应用 APPL 才能从消息 N3 中读取密钥 key。

[0030] 最后在下一个步骤中，相对于安全模块 HSM 进行对应用 APPL 的验证，其中基于消息 N4 进行该验证，所述消息 N4 包含应用 APPL 和安全模块 HSM 的标识符以及会话标识 SID，并且被用在 HSM 中原始生成的密钥 key 加密。该验证在此仅当 HSM 可以用由其原始生成的密钥对消息解密时才是成功的。另一个安全特征通过以下方式实现，即此外所传送的会话标识 SID 必须与由 HSM 原始生成的会话标识一致。通过这种方式保证免遭所谓的重放攻击，在重放攻击中在先前验证的范围内已经传送过一次的消息被再次使用。

[0031] 如果能用 HSM 的密钥 key 对消息 N4 解密并且此外会话标识 SID 与原始的会话标识一致，则验证是成功的。现在硬件安全模块 HSM 可以确信，由应用 APPL 在该硬件安全模块中接收并用密钥 key 加密的消息真的是来自该应用。根据图 1 的变型，在此实现了秘密 key 通过在中间连接所述应用所有者 A0 条件下的可信连接到达应用 APPL，而计算中心的系统管理员不具有访问该秘密的可能性。

[0032] 在成功的验证之后，借助密钥 key 建立应用 APPL 与安全模块 HSM 之间的安全通道。然后通过该通道将主密钥 MK 传送到应用 APPL，该应用接着可以用该密钥对应用数据加密。

[0033] 图 2 示出本发明方法的第二变型。在该变型中，与图 1 的实施方式不同以密钥 key 形式的共同秘密不由硬件安全模块 HSM 生成，而由应用所有者 A0 生成。在第一步骤中，首先由将相对于硬件安全模块 HSM 被验证的应用 APPL 把安全的消息 N1 发送到应用所有者 A0。通过密钥 k 加密的该消息包含现在由应用 APPL 生成的会话标识 SID 以及硬件安全模块 HSM 和应用 APPL 的标识符。

[0034] 在接收消息 N1 之后，应用所有者 A0 产生对称密钥 key。该密钥是在该方法结束时相对于安全模块 HSM 验证应用 APPL 的共同秘密。为了实现该验证，必须将密钥 key 安全地传输给应用 APPL 和安全模块 HSM。这在图 2 的范围内通过将消息 N2 从应用所有者 A0 传递给应用 APPL 以及将消息 N3 从应用 APPL 传送给安全模块 HSM 来实现。与图 1 不同，在此在

应用所有者 AO 与安全模块 HSM 之间不建立单独的安全通道。而是通过应用 APPL 为应用所有者 AO 与安全模块 HSM 之间的安全通道建立隧道。

[0035] 在上面提到的消息 N2 的范围中,消息 M2 与所生成的密钥 key、会话标识 SID 和硬件安全模块 HSM 的标识符一起被传送。消息 M2 在此还是包含会话标识 SID 和密钥 key 以及应用 APPL 的标识符。该消息在此被用安全模块的公共密钥 K(HSM) 加密并且还被用应用所有者的签名 sig(AO) 签名。由加密的并且签名的消息 M2 与 SID、HSM 和 key 构成的组合通过 AO 与 APPL 之间的安全通道传送到应用 APPL。接着 APPL 对该消息解密并且由此获得保持在工作存储器中的密钥 key。通过在该消息中包含的会话标识 SID,应用可以检验该消息是当前的,因为该应用可以将所传送的会话标识与由该应用原始生成的会话标识相比较。

[0036] 接着应用 APPL 将消息 N3 发送到安全模块 HSM,其中该消息包括包含在先前接收的消息 N2 中的消息 M2,该消息 M2 被用 sig(AO) 签名并且用安全模块 HSM 的公共密钥加密,从而该消息不能被应用解密。此外,应用 APPL 用密钥 key 对会话标识加密并且将结果添加到消息 N3。

[0037] 在接收到消息 N3 之后,安全模块 HSM 通过签名 sig(AO) 检验应用所有者 AO 已产生该消息并且也已将密钥 key 安全地传送给应用 APPL。接着, HSM 可以将加密的会话标识通过存储在该 HSM 中的密钥 key 解密,这证实了 APPL 拥有共同秘密 key。然后基于成功的解密相对于安全模块 HSM 对应用 APPL 进行验证,即安全模块 HSM 可以确信用密钥 key 加密的消息来自 APPL。通过将消息 N3 中的会话标识 SID 与通过 key 加密的会话标识进行比较,安全模块 HSM 还可以确定消息 N3 不是旧消息的重放。然后在验证之后在应用 APPL 与安全模块 HSM 之间可以在使用密钥 key 形式的共同秘密的条件下建立安全通道,于是可以接着将主密钥 MK 从 HSM 传输到应用 APPL,从而应用接着能用该主密钥对应用数据加密。

[0038] 在前面描述的发明具有一系列优点。尤其是使得可以在应用所有者 AO 的安全模块 HSM 中验证应用 APPL,而外部服务运营商一应用就在该外部服务运营商的计算中心上运行一不具有访问在验证的范围中产生的在应用与安全模块之间的共同秘密的可能性。这通过使用分配给应用所有者的安全模块以及通过在中间连接应用所有者条件下的安全通道的通信来实现。在此,对安全模块的主密钥的访问自动进行,而无需由应用所有者的授权人员手动输入密码。

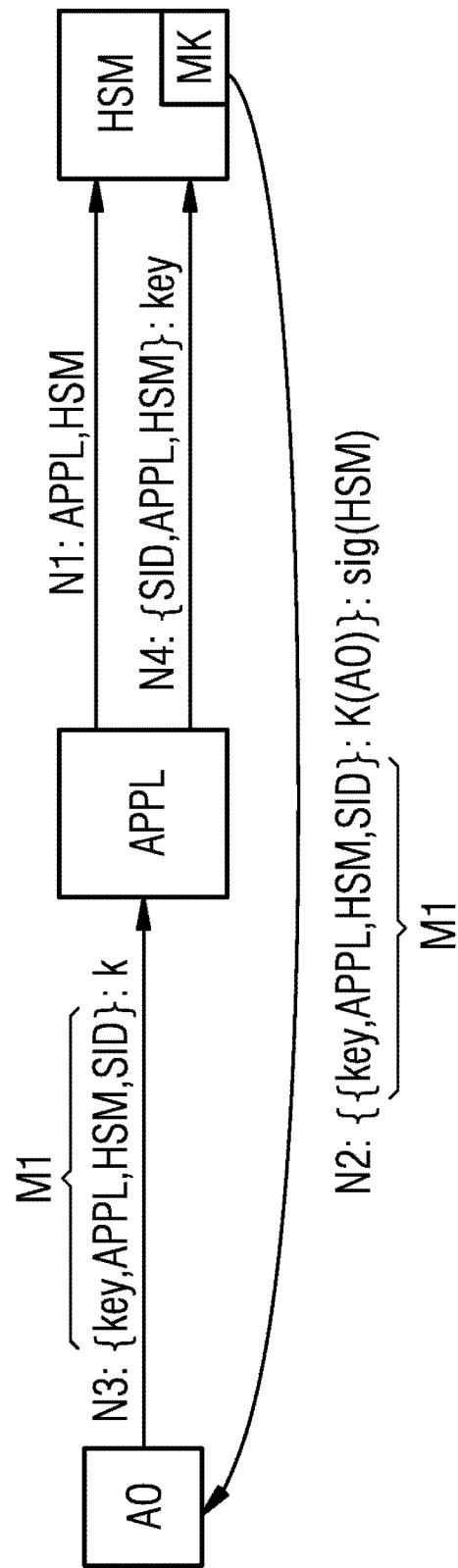


图 1

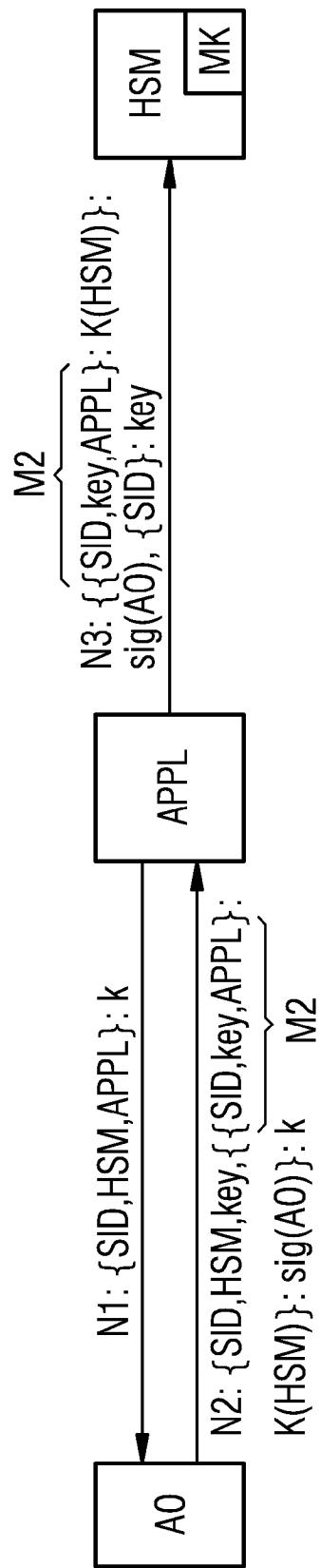


图 2